Univerzita Karlova v Praze
Právnická fakulta

Michaela Pobořilová

VIRTUÁLNÍ TRESTNÉ ČINY

Diplomová práce

Vedoucí diplomové práce: JUDr. Bc. Tomáš Gřivna, PhD.

Katedra: trestního práva

Datum vypracování práce (uzavření rukopisu): 1. 7. 2010

6. 9. 2010

Prohlašuji, že jsem předkládanou diplomovou práci vypracovala samostatně za použití zdrojů a literatury v ní uvedených.

V Praze dne 23. srpna 2010

Michaela Pobořilová

Hluboce děkuji váženému JUDr. Bc. Tomáši Gřivnovi, PhD., za ochotu a vstřícnost při zpracování diplomové práce

Obsah:

Úvod

V dnešní době se v čím dál větší míře setkáváme s pojmy virtuální prostředí neboli též kyberprostor, které bezprostředně zasahují do běžného lidského života prostřednictvím informačních technologií. Vývoj tohoto odvětví dosahuje neustálého pokroku a rozmachu.

Diplomová práce je zaměřena na problematiku virtuálního prostředí v oblasti práva, a to odvětví práva trestního. Kyberprostor vzhledem ke svým charakteristickým vlastnostem jako je jeho přístupnost, územní neomezenost, časová nereálnost, dostupnost, nízké náklady, anonymita aj., představuje místo, v němž dochází k páchání společensky škodlivých jednání různého charakteru.

Z teoretického hlediska je obsahem této práce vymezení virtuálního trestného činu, včetně jeho jednotlivých znaků, a dále jeho rozdělení dle různých kritérií. Pro potřeby této práce a vzhledem k jejímu rozsahu byly vybrány pouze nejpodstatnější konkrétní trestné činy, jichž je možné se dopustit v kyberprostoru.

Kyberprostor, pod něž zahrnujeme různorodou škálu informačních technologií (počítače, Internet, mobily apod.), je prostředím velice širokým, a proto není pokryt veškerý jeho rozsah. Diplomová práce se zaměřuje na nejčastější a nejběžnější část virtuálního prostředí, a to Internet, který je v současné době již nedílnou součástí každodenního života. V rámci internetového prostředí pak vznikla specifická oblast, tzv. virtuální světy, které v posledních letech získaly u svých uživatelů nevídaný ohlas. Virtuální světy tvoří samostatná prostředí, v nichž dochází k vzájemné interakci jejich uživatelů, kteří vytváří novou subkulturu společnosti a řídí se vlastními pravidly.

Praktická část diplomové práce je věnována případovým studiím a komparaci právních úprav jiných států. Případové studie jsou založeny na skutečných kauzách, které byly předmětem soudních řízení, přičemž se jedná o případy upravující otázky jednání spáchaných přímo v kyberprostoru nebo v souvislosti s ním. Reakce zahraničních států jsou různorodé a nejednotné, což dokazuje i právní úprava této oblasti. V rámci mezinárodní spolupráce se můžeme setkat s dokumenty, které upravují dílčí otázky, jenž státy považovaly za natolik důležité, že vznikla potřeba je regulovat. Tyto dílčí snahy znamenají uvědomění si jednotlivých států, že kyberprostor vedle

svých nepochybných pozitiv má i negativa, která díky místní neomezenosti virtuálního prostředí mají přeshraniční charakter a mohou být velice nebezpečná. Zájem států o regulaci této problematiky získává na stále větším významu a nepochybně povede k rozsáhlejší mezinárodní spolupráci.

Cílem této diplomové práce je především podat základní obraz problematiky virtuálních trestných činů, pokusit se vymezit jejich charakteristické rysy a nastínit možné problematické právní otázky, které virtuální prostředí vyvolává.

1. Základní pojmy

1.1. Kyberprostor, virtuální prostředí

Jedná se o česky užívaný termín pocházející z překladu anglického výrazu cyberspace, který nemá ustálený význam. Poprvé byl pojem kyberprostor použit na počátku 80. let 20. století v povídce prozaika Williama Gibsona „Jak vypálit Chrome“ a následně v románu Neuromancer, v němž kyberprostor popsal jako datovou halucinaci v podobě imaginárního prostoru, který je tvořen počítačově zpracovanými daty a přístupného pouze vědomí uživatelů[1].

Kyberprostor představuje prostředí, které je vytvářeno informačními technologiemi a můžeme zde řadit nejen počítače, ale i například mobilní telefony a jiné novodobé technologie, které přináší možnost vzniku dalších prostorů, v nichž budou moci probíhat na určité úrovni společenské vztahy. Pojem kyberprostor není přesně definovatelný a lze na něj pohlížet z různých úhlů pohledu, tj. jako na prostředí sociální, technologické nebo právní. Teoretiky je pak definován různými způsoby, přičemž se vychází ze stejné obsahové podstaty. Kybernetický prostor nemá hmotnou podstatu, je imaginární. Jeho vznik a další existence je závislá na světě reálném, je spojena s určitou úrovní technologické vyspělosti společnosti, s rozvojem informačních a telekomunikačních technologií, přičemž jednotliví uživatelé vytvářejí určitý druh společného prostoru, který lze nazvat „kyberprostorem“[2].

Kyberprostor má své specifické charakteristické znaky, které přináší řadu výhod, na druhou stranu skýtá mnoho negativ. Především se jedná o imaginární prostor, který nemá pevné hranice, je ve své podstatě nekonečný a neomezený, tzn. že se může neustále rozrůstat (elasticita). Tento prostor rovněž není omezen státními hranicemi, v nichž by jednotlivé státy mohly uplatňovat svou státní moc a vynucovat právními normami požadované chování. Vzniklo tak prostředí, které je vhodné pro společensky škodlivá jednání.

[1] Polčák, R., Škop, M., Macek, J. *Normativní systémy v kyberprostoru.* Masarykova univerzita, Brno, 2005, str. 7.
[2] Křivna, T. Závazky k ochraně kyberprostoru vyplývající z evropského a mezinárodního práva. In: Acta universitatis carolinae – Iuridica 4, 2008, str. 21-34.

Dalším specifikem je rychlost. Jakékoliv interakce uskutečňované ve virtuálním prostředí probíhají ve velmi krátkých časových intervalech, s nízkými finančními náklady a nízkou možností odhalení v případě páchání škodlivých jednání. Škoda, která takovými jednáními může být způsobena, může mít dalekosáhlé a nezvratné následky. Pro pachatele je výhodná i fyzická nepřítomnost jeho osoby a anonymita kyberprostoru. Tato anonymita může být odstraněna samotným uživatelem na základě poskytnutí údajů o své osobě (zpravidla však nevzniká možnost ověřit pravdivost uvedených údajů), anebo jistou formu identifikace představuje zjištění tzv. IP adresy[3].

Z hlediska technického se kyberprostor skládá ze stovek tisíců vzájemně propojených počítačů, serverů, směšovačů (router), přepínačů (switch) a optických kabelů. Jedná se o prostor, do něhož vstupují sociální aktéři, kteří používají ke vzájemné sociální interakci pokročilé informační technologie[4].

Na kyberprostor lze dále nazírat, zejména v očích laické veřejnosti, jako na prostředí sociální, v němž dochází ke vzájemné interakci jeho uživatelů, tj. komunikaci, rozvoji osobnosti, realizaci potřeb, představ apod. V návaznosti na to si musíme uvědomit, že se jedná zároveň i o prostředí právní, v němž zejména vznikají, mění se a zanikají právní vztahy. Takovéto pojetí bývá vzhledem k vlastnostem kyberprostoru opomíjeno. Důvodem je zejména proměnlivost prostředí, jeho neohraničitelnost neboli neomezenost, globální využití, vysoká anonymita apod. Kyberprostor tvoří samostatné prostředí a představuje nový pohled na rozsah právní teorie, tj. jeho pokrytí právními normami. Pro uplatnění práva ve virtuálním prostředí je potřebná znalost pojmů, které jsou vlastní oboru informatiky a technologii, s nimiž právo běžně neoperuje. I zde však existují normy, které regulují chování uživatelů, ať již přímo nebo zprostředkovaně. Z právního hlediska nás především bude zajímat, zda lze určitou okolnost, stav či skutečnost zařadit do kyberprostoru. Hranici mezi světem skutečným a kyberprostorem není těžké vymezit, resp. v konkrétním případě vždy poznáme, v jakém prostoru se pohybujeme. Základním rozlišovacím znakem bude druh technologie, který bude použit jako zprostředkovatel kyberprostoru (nejčastěji

[3] V informatice IP (internetový protokol) adresa představuje číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti, která používá internetový protokol. Informace dostupná z: http://cs.wikipedia.org/wiki/IP_adresa.

[4] Blíže srov. Polčák, R., Škop, M., Macek, J.: Normativní systémy v kyberprostoru. Masarykova univerzita, Brno, 2005. str. 9.

půjde o počítač či obdobné zařízení, mobil). Zvláštní význam je pak přičítán určení hranic v rámci kyberprostoru pro otázku trestní jurisdikce, která je v této práci ponechána stranou, neboť tvoří jednu z nejsložitějších otázek vyvstalých s problematikou informačních technologií[5].

Totožnost nemůžeme spatřovat ani mezi pojmy virtuální prostředí (kyberprostor) a virtuální svět, přestože mají společné rysy. Hlavní rozdílnost spočívá v kyberprostorovém (prostorovém) zaměření, kdy virtuální prostředí chápeme z tohoto pohledu jako kyberprostor, naproti tomu virtuální svět je chápán jako svět existující v rámci virtuálního prostředí, který je (ale nemusí být) přenesením, resp. odrazem světa reálného. Pro dostatečné rozlišení lze uvést příklad, kdy virtuálním prostředím je síť Internet (mobilní síť), virtuálním světem je například Second Life[6] (jiné tzv. trojrozměrné virtuální světy, online game hry).

Můžeme tedy shrnout, že kyberprostor je sociální, technologický a normativní systém využívající ke své funkčnosti informační technologie, a v jehož rámci dochází k vytváření jednotlivých vazeb a vztahů, které jsou charakteristické pro dané prostředí.

1.2. Kyberkriminalita

Stejně jako kyberprostor nemá ani tento pojem ustálenou definici. Již podle samotného názvu můžeme dovodit, že se jí rozumí kriminalita páchána v kyberprostoru nebo v souvislosti s ním. Pojem kyberkriminalita bývá často zaměňován s pojmem počítačová kriminalita nebo internetová kriminalita, nejedná se však o pojmy totožné.

[5] Zcela okrajově jako příklad otázky trestní jurisdikce lze uvést případ státu Minnesota, jejíž generální prokurátor prohlásil, že jurisdikci státu Minnesota podléhají všechny internetové stránky, které jsou dostupné z počítače, který se nachází ve státě Minnesota. Blíže viz: Polčák, R., Škop, M., Macek, J. *Normativní systémy v kyberprostoru.* Masarykova univerzita, Brno, 2005, str. 31. Minnesota Attorney General, *Statement of Minnesota Attorney General on Internet Jurisdiction.* http://world.std.com/goldberg/minn.html.

[6] Second Life je považován za MMORPG, na druhé straně se můžeme setkat s názorem, že Second Life není považován za MMOPRG, ale pouze za virtuální svět, který slouží jako prostředek komunikace a interakce s ostatními uživateli v reálném čase a trojrozměrném prostoru. Blíže viz Havlena, O. Komunikace virtuálně – Masarykova Univerzita a Second Life. Brno, 2009. Dostupný z: http://www.havlena.net/blog/komunikace-virtualne-masarykova-univerzita-a-second-life-sl/.

Na druhé straně tyto kategorie nelze od sebe přísně oddělovat, ale naopak se navzájem podmiňují a prolínají.

Virtuální kriminalita neboli kyberkriminalita představuje pojem nejširší, neboť v sobě zahrnuje veškerou trestnou činnost, pro níž je vždy charakteristické virtuální prostředí, a zároveň subsumuje veškeré informační technologie, které lze použít ke spáchání takovéto činnosti.

Počítačová kriminalita tvoří výseč kyberkriminality. Přestože nebývá jednoznačně definována, přinesl výbor Evropského parlamentu oficiální definici a označuje za ni nelegální, nemorální a neoprávněná jednání zahrnující užití dat získaných prostřednictvím výpočetní techniky nebo jejich změnu[7]. Na počítačovou kriminalitu je nadále nahlíženo jako na trestnou činnost, které je možné se dopustit jen ve virtuálním prostředí prostřednictvím specifického prostředku, tj. počítače.

Mylné by rovněž bylo spojovat kyberkriminalitu pouze s novým fenoménem - Internetem, jenž se rozmohl na přelomu 90. let 20. století. Internetová kriminalita je relativně samostatným podoborem kyberkriminality, jedná se o pojem užší a můžeme ji definovat jako trestnou činnost páchanou v síti Internet, prostřednictvím sítě Internet, resp. v souvislosti s jeho užíváním.

1.3. Internet

Za nejtypičtějšího představitele kyberprostoru bývá považován Internet. Z technického hlediska jde o soustavu serverů, sítí a k nim připojených počítačů[8]. Jedná se o virtuální prostředí s globálním charakterem, které nemá centralizované řízení a není právnickou osobou. Internet je v současné době jednou z nejkomerčněji a nejběžněji využívanou informační technologií, v níž se právo uplatňuje specifickým způsobem. Jedná se prostor regulovaný vlastními pravidly, autorita státu se zde prakticky neprojevuje a vzhledem k prozatímní neurčitelnosti trestní jurisdikce neexistují žádné účinné nástroje k vynucení právní poslušnosti[9].

[7] Kuchta, J., Válková, H. a kol. Základy kriminologie a trestní politiky. 1. vydání. Praha: C. H. Beck, 2005, str. 504.
[8] Informace dostupná z: http://cs.wikipedia.org/wiki/Internet
[9] Kuchta, J., Válková, H. a kol. Základy kriminologie a trestní politiky. 1. vydání. Praha: C. H. Beck, 2005, str. 514.

Počet uživatelů Internetu již překonal hranici 580 miliónů, přičemž tento počet den za dnem neustále narůstá.

Vznik Internetu můžeme rozdělit do tří fází[10]:

- I. fáze (60. léta 20. století – 1982)
- II. fáze (rozvoj Internetu včetně jeho komercionalizace, tj. od roku 1983)
- III. fáze (tzv. boom – 1995 až současnost)

Počátkem 60. let 20. století se ve Spojených státech amerických objevily první pokusy na vytvoření sítě, která by propojovala nejdůležitější vojenské, vládní a akademické počítače, a která by byla schopna přežít jaderný úder. Jednalo se o vojenský projekt americké armády během studené války, přičemž tato síť měla být schopná fungovat i v případě výpadku jednotlivých uzlů. Roku 1969 za finanční podpory Pentagonu agentura DARPA (Defence Advanced Research Project Agency) zprovoznila čtyři uzly sítě nazvané ARPANET, kdy všechny uzly byly umístěny na amerických univerzitách. Postupně se ARPANET rozrůstal o další uzly, avšak hlavním využitím nebylo používání vzdálených počítačů, ale komunikace prostřednictvím elektronické pošty a elektronické konference. V roce 1973 byly připojeny do sítě první dvě neamerické instituce, a to britská University College of London a norská univerzita Royal Radar Establishment. V roce 1974 pak byla zveřejněna první specifikace protokolu TCP/IP, který se začal oficiálně používat od roku 1983.

Druhá a třetí fáze je spojena s prudkým rozvojem Internetu a jeho komercionalizací. Na počátku 90. let 20. století měl Internet již přes více než milion uživatelů a došlo k jeho expanzi mimo americký kontinent. Avšak do roku 1993 zůstával Internet doménou především vědeckých a akademických pracovišť. Důležitým mezníkem se stal rok 1989, kdy se na půdě ústavu částicové fyziky objevil dokument HyperText and CERN, jenž popisoval možnosti vytvoření interního distribuovaného systému jako jednotné nástavby nad mnoha různorodými informačními zdroji. V listopadu 1990 byl předveden první prototyp WWW serveru a od této doby můžeme

[10] Informace dostupná z: http://en.wikipedia.org/wiki/Internet.

pozorovat nejrozsáhlejší expanzi této technologie, která dnes tvoří součást našich každodenních životů.

V České republice můžeme považovat za průkopníky Internetu zakladatele internetového vyhledávače www.seznam.cz pana Lukačeviče a méně známého pana Liebermana, iniciátora prvního českého portálu pro podnikatele www.tradenet.cz.

1.4. Virtuální světy, MMORPG

Relativně nově se v současné době setkáváme ve stále větší míře s prostředím tzv. virtuálních světů. Virtuální světy představují nereálná prostředí existující perzistentně s vlastní komunitou a vlastními specifickými (přizpůsobenými) pravidly. Tyto světy mohou vznikat jen v rámci kyberprostoru, přesněji Internetu, od nějž se na jednu stranu výrazně odlišují, na druhé straně mají společné znaky. Výrazným odlišujícím znakem je skutečnost, že virtuální světy existují v rámci kyberprostoru ve formě webových stránek[11], které mají svého vlastníka, kterým může být fyzická nebo právnická osoba. Naproti tomu Internet jako celek není nikým centrálně řízen, pouze jednotlivé servery[12] jsou ve vlastnictví konkrétních osob.

Virtuální světy jsou typické zejména pro MMORPG[13]. Jedná se o prostředí sui generis, které se vyvinulo z běžných online počítačových her[14]. MMORPG jsou představovány perzistentními trojrozměrnými (3D) světy zpřístupněnými prostřednictvím Internetu velkému počtu hráčů (uživatelů)[15], kteří vstupují v závislosti na konkrétním druhu hry do vzájemných interakcí. V každé MMORPG hráč přebírá

[11] World wide web = označení pro aplikace internetového protokolu http, tj. soustavu propojených hypertextových dokumentů. V češtině se slovo web často používá nejen pro označení celosvětové sítě dokumentů, ale i pro označení jednotlivé soustavy dokumentů dostupných na tomtéž webovém serveru nebo na téže internetové doméně nejnižšího stupně (internetové stránce). Informace dostupná z: http://cs.wikipedia.org/wiki/Web.

[12] V informatice termín užívaný pro obecné označení počítače, který poskytuje nějaké služby nebo počítačový program, který tyto služby realizuje. Servery jsou buď umístěny volně nebo ve speciální místnosti. Informace dostupná z: http://cs.wikipedia.org/wiki/Server.

[13] Vzhledem ke skutečnosti, že virtuální světy a MMORPG vychází ze stejného principu, jsou v dále uvedeném textu tyto pojmy používány jako synonymum.

[14] MMORGP patří do základní (výchozí) skupiny tzv. MOG (Multiplayer Online Game), která se dále diferencuje do různých podob podle typu hry (př. MMOG - Massively Multiplayer Online Game; MMORPG - Massively Multiplayer Online Role-playing Game; aj.).

[15] V případě hry RuneScape je možné, aby současně bylo připojeno až 250 tisíc hráčů.

určitou roli, tj. vytváří svou herní postavu, kterou řídí a kontroluje. Tyto hry jsou založeny na různých tématech, mezi nejčastější patří fantasy/sci-fi, jiné jsou založeny na odrazu běžného reálného života do virtuálního prostředí[16]. Lze konstatovat, že primárním všeobecným cílem je rozvoj hráčovy postavy, tzv. avatara, prostřednictvím vývojového sytému, který bývá specifický pro každou hru zvlášť[17].

Jednotlivé MMORPG můžeme rozdělit na hry zpoplatněné a nezpoplatněné, tzv. free to play. Zpoplatnění může mít formu jednorázového vstupního příspěvku, formu pravidelně placeného předplatného nebo se může jednat o poskytnutí poplatku přímo při prodeji softwaru a souvisejících datadisků. Tyto peněžní prostředky slouží k údržbě a rozvoji hry.

MMORPG, stejně jako virtuální světy, jsou založeny na společné interakci, tj. představují určitý druh sociálního prostředí a komunikace. Hráči mohou vystupovat buď jako jednotlivci, nebo se mohou, pokud to konkrétní hra umožňuje, sdružovat ve formě herního společenství. Hráči také často musejí na části hry spolupracovat s ostatními, kdy v takto uměle vytvořené skupině přijímají určitou roli (ochrana ostatních hráčů nebo jejich tzv. hojení v případě poškození nepřáteli aj.). Jednotlivé hry pak mají nástroje, kterými vzájemnou komunikaci mezi uživateli usnadňují[18]. Vzniká tak samostatná společenská kultura, která je tvořena hráči pocházejícími z různých koutů světa a kteří mají odlišné zvyky a tradice. Přesto má tato kultura vytvořena všeobecně uznávaná pravidla, která mohou být formulována jako pravidla hry či podmínky použití hry.

Některé internetové hry mají vlastní peníze, popř. kredity. „Virtuální měna“ slouží převážně k obchodování, zejména je jejím prostřednictvím umožněno získat určité virtuální zboží či služby. Takovéto kredity/peníze mají v závislosti na konkrétní hře různé postavení. V některých případech nemají vlastní hodnotu a nejsou soukromým vlastnictvím hráče, nebo v opačné situaci mají reálnou hodnotu, která je vyjádřena ve formě kurzu vůči konkrétní měně jako zákonnému platidlu příslušného

[16] Sci-fi téma: World of Warcraft. Téma reálného prostředí: Second Life.
[17] Může být založen na získávání tzv. zkušenostních bodů za provedení úkolů nebo činností (tzv. questy), přičemž po získání určitého jejich počtu avatar dosahuje vyšší úrovně (levelu). Typickým příkladem jsou vzájemné souboje (fantasy, sci-fi) a získávání různých doplňků, čímž herní postava akumuluje své bohatství a schopnosti.
[18] Např. chat, moderátoři nebo tzv. game mastři.

státu, a tvoří vlastnictví hráče. Virtuální měna z tohoto důvodu podléhá významným omezením, která stanovuje vlastník příslušné internetové hry, a navíc může stanovit další omezení vyplývající z právního řádu země, odkud hráč pochází. Mezi tato omezení patří především nabývání a vykoupení virtuální měny[19], stanovení maximální částky, kterou lze mít na uživatelském účtu, anebo vlastník může rozhodnout o ukončení tohoto produktu, avšak jen s dopadem pro všechny hráče. Je-li tedy možné, aby virtuální měna byla směněna za skutečné peníze, dochází zde k propojení skutečného a virtuálního světa, a může tak snadněji docházet k zasažení majetkové podstaty skutečných osob.

Některé online hry uvádějí, že virtuální majetek má reálnou hodnotu a lze ho za určitých podmínek směnit za reálné peníze. V současné době se lze proto setkat s tezí zaměřující se na oblast daňového práva a kyberprostoru. Podle některých názorů[20] by zdanění měly podléhat i virtuální výdělky mající určitou reálnou hodnotu, aniž by ke směně za peníze došlo. Darované virtuální předměty by tak podléhaly darovací dani, děděný virtuální majetek zase dani dědické. Předmětná situace by znamenala daňové povinnosti pro „výdělečné“ hráče, ale také zodpovědnost provozovatelů za správné a ověřitelné zúčtování a převody.

Každá internetová hra má stanovena určitá pravidla, která jsou vyjádřena v tzv. podmínkách použití hry (Terms/Conditions of use) stanovených samotným vlastníkem hry. Hráči bývají nejčastěji k akceptaci vyzvání při zakládání uživatelského účtu, nebo přímo na internetovém serveru je uvedena informace, že použití webové stránky se řídí podmínkami a pravidly stanovenými vlastníkem. V podmínkách použití se uvádí základní informace o vlastníkovi, ustanovení o použitelnosti webové stránky osobami mladšími 18 let, která je vázána na souhlas zákonného zástupce, dále řeší otázky bezpečnosti a zneužití produktů patřících vlastníkovi internetové hry. Podmínky se vyjadřují rovněž k právům duševního vlastnictví, založení účtu a vytvoření uživatelského jména (nickname), které nesmí porušovat práva třetí strany, nesmí být

[19] Výměnu virtuální měny za hráčem vybrané zboží lze ve lhůtě stanovené vlastníkem hry, v opačném případě by došlo k jejímu vymazání. V případě, že dojde k jejímu vymazání, není za ni poskytována žádná hotovost či jiná náhrada.

[20] Tuto teorii zastává americký Kongres. Informace dostupná z: http://news.cnet.com/IRS-taxation-of-online-game-virtual-assets-inevitable/2100-1043_3-6140298.html.

urážlivé, rasistické, obscénní či jinak nevhodné[21]. Hráč pak v rámci podmínek musí souhlasit s pravidly hry, a to se současnou platnou verzí, která může být změněna v návaznosti na různé okolnosti (například změna právní úpravy, technických dovedností apod.).

V mnoha případech vlastník při stanovení podmínek upozorňuje, že nemůže zabránit situaci, kdy ostatní uživatelé nebudou jednat ve shodě se stanovenými podmínkami nebo pravidly hry. Rovněž nemůže zcela zabránit nevhodnému či protiprávnímu obsahu zveřejňovanému hráči přímo ve hře, ale při zjištění takovéhoto jednání si vyhrazuje právo provést patřičná opatření. Vlastník internetové hry tedy počítá s tím, že ze strany uživatelů může docházet k porušování podmínek a pravidel hry. Většina internetových her má pro takové situace vybudován tzv. offence systém[22], který je určen k ochraně ostatních hráčů, kteří se porušení pravidel nedopustili. Tento ochranný systém má variabilitu možností pro případ, že se setkáme s jiným hráčem, jehož chování se příčí pravidlům hry[23].

2. Virtuální trestné činy

2.1. Pojem

Základem pro vymezení pojmu virtuální trestný čin je důležité vymezení slov *virtuální* a *trestný čin*, neboť pro celkovou složeninu nenalezneme v současné době žádnou jednotnou legální definici. Často používaným synonymem bývá virtuální zločin neboli kyberzločin[24].

[21] Zvolené uživatelské jméno ve většině případů podléhá posouzení, kdy vlastník si v rámci podmínek vyhrazuje možnost z jakéhokoliv uvedeného důvodu uživatelské jméno změnit nebo provést jiná vhodná opatření.
[22] Volně překládáno jako „ochranný systém“.
[23] Ochrana spočívá v možnosti přidat „závadného“ hráče do vlastního seznamu ignorovaných nebo v možnosti nastavit upravení chatu, čímž dojde k zabránění další interakce. Další možností je funkce ohlášení zneužití přímo vlastníkovi hry, který posoudí situaci a přijme vhodná opatření, aby nedošlo k dalšímu porušování pravidel.
[24] Jedná se o pojmy totožné. Pro účely diplomové práce byl vybrán pojem virtuální trestný čin, neboť pojem virtuální zločiny není vzhledem k současné definici vycházející z účinného trestního zákoníku zcela přesný.

Virtuální neboli virtualita je termín, který nacházíme ve většině moderních slovnících a v komunikaci je již běžně používán. Nejčastěji bývá stavěn do protikladu ke slovu „reálný - realita“, která předpokládá hmotné hmatatelné ztělesnění, tj. vlastnost náležející jevům, kterým přisuzujeme existenci nezávislou na vlastní vůli[25]. Z toho lze dovodit, že pro virtualitu je typická imaginárnost, tj. nehmatatelnost a nemožnost ztělesnění ve skutečném světě.

S pojmem „virtuální“ úzce souvisí pojem *kyberprostor*, který je označením virtuálního světa vytvářeného moderními technologiemi (počítači, telekomunikačními sítěmi apod.) paralelně ke světu „reálnému“[26].

Podstatně jednodušší je vymezení pojmu *trestný čin*. Legální definici obsahuje trestní zákoník v ustanovení § 13 odst. 1, který jej definuje jako protiprávní čin, který trestní zákon označuje za trestný a který vykazuje znaky uvedené v takovém zákoně. V současné době je trestný čin tvořen těmito znaky:

a/ protiprávnost
b/ typové znaky tvořící skutkovou podstatu trestného činu
c/ obecné požadavky kladené na subjekt

Z výše uvedených znaků je patrné, že se musí jednat o trestný čin, jehož základem je jednání, které je právním řádem zakázané a nedovolené, přičemž tuto protiprávnost posuzujeme z hlediska celého právního řádu. Typové znaky charakterizují jednotlivé trestné činy a navzájem je odlišují od trestných činů ostatních.

Pro každý trestný čin je charakteristické, že je vymezen znaky tvořícími jeho skutkovou podstatu, která představuje abstraktní popis určitého druhu trestného činu[27]. Skutková podstata se skládá z obligatorních znaků, které musí být přítomny vždy, abychom mohli mluvit o trestném činu, a dále mohou být součástí fakultativní znaky, které pokud je skutková podstata vyžaduje, stávají se znaky obligatorními. Fakultativní

[25] Berger, P., L. Luckmann, T. *Sociální konstrukce reality.* Praha: Centrum pro studium demokracie a kultury, 1999, str. 9.
[26] In *Pocta Otovi Novotnému k 80.narozeninám.* Praha: ASPI, Wolters Kluwer, 2008, str. 30
[27] Novotný, O., Vanduchová, M., Šámal, P. a kol. *Trestní právo homotné. Obecná část.* 6. vydání, Praha: Wolters Kluwer ČR, a.s., 2010, str. 117.

znaky na rozdíl od znaků obligatorních nejsou vyžadovány u všech trestných činů[28]. Tato obecně platná teorie se použije i pro virtuální trestné činy.

Virtuální trestný čin je tedy trestný čin spáchaný ve virtuálním prostředí nebo v souvislosti s ním, tj. jedná se o protiprávní jednání, které naplňuje jednotlivé znaky skutkové podstaty. Jako každý trestný čin je chápán jako negativní společensky škodlivé jednání, na jehož právní regulaci existuje právní zájem.

2.2. Klasifikace virtuálních trestných činů

Dříve než budou rozebrány jednotlivé znaky virtuálních trestných činů, je vhodné provést jejich rozdělení. Jelikož neexistuje jednotná legální definice, neexistuje ani jejich jednotná klasifikace. Virtuální trestné činy lze členit dle různých kritérií.

Stěžejním členěním pro diplomovou práci je členění dle prostředí, v němž je uskutečněno společensky škodlivé jednání zakládající trestný čin:

a/ **pravé virtuální trestné činy (čistě virtuální)**, pro něž je charakteristickým znakem, že tyto trestné činy mohou být spáchány jen ve virtuálním prostředí (kyberprostoru) a není možné se jich dopustit mimo něj. Typicky se bude jednat o trestné činy uvedené v ustanoveních §§ 230 až 232 zvláštní části trestního zákoníku, sniffing, spamming, stejně jako jiná protiprávní jednání, která doposud nemáme v českém trestním právu upravena.

b/ **nepravé virtuální trestné činy**, pro něž je charakteristickým znakem, že se jedná o trestné činy, které mohou být spáchány i mimo virtuální prostředí, tj. v běžném životě. Jedná se o trestné činy, jenž nalezneme v příslušných právních předpisech týkajících se ochrany společnosti před společensky škodlivými jednáními.

[28] Cílem této kapitoly není přinést výklad jednotlivých znaků trestného činu, ale provést bližší vymezení rozdílností charakteristických pro virtuální trestné činy. Pro bližší výklad je odkázáno na právní teorii.

Pod tuto kategorii lze subsumovat například krádež, dětskou pornografii a další trestné činy, u nichž to jejich povaha připouští.

Zaměřením této práce jsou obě uvedené kategorie, tj. pravé i nepravé virtuální trestné činy. Z hlediska trestního práva nelze přehlédnou fakt, že převážná pozornost je věnována zejména pravým virtuálním trestným činům (v užším pojetí můžeme hovořit o počítačové kriminalitě). Stále častěji se však setkáme s případy, které jsou s virtuálním prostředím spojeny nepřímo, tj. prostřednictvím využívání kyberprostoru, zejména pak sítě Internet (internetová kriminalita), a které jsou typické pro každodenní život. Tato skutečnost souvisí s prolínáním virtuálního a reálného prostředí. Takovéto situace se mohou dotknout, resp. mohou se stát kterémukoliv uživateli virtuálního prostředí, tzn. že není zapotřebí žádných zvláštních znalostí.

Virtuální trestné činy z hlediska kyberprostoru můžeme dále rozdělit na[29]:

a. trestné činy páchané v kyberprostoru, tj. situace, kdy kyberprostor je nástrojem páchání trestného činu,
b. trestné činy zaměřené proti kyberprostoru, tj. situace, kdy kyberporstor je předmětem útoku.

Výše uvedená dělení můžeme blíže rozdělit, a to na virtuální trestné činy[30]:

a. *typické* – do této relativně nejširší skupiny budou spadat pravé virtuální trestné činy a rovněž některé z nepravých virtuálních trestných činů, jejichž spáchání v rámci kyberprostoru můžeme řadit mezi nejčastější. Informační technologie zde bude použita či využita jednak jako nástroj, jednak jako předmět útoku. Patří zde zejména trestné činy uvedené v §§ 230 až 232, neoprávněné nakládání s osobními údaji (§ 180), porušení tajemství dopravovaných zpráv (§ 182), pomluva (§ 184) a další.
b. *netypické* – do této skupiny lze zařadit zbývající nepravé virtuální trestné činy, pro něž není charakteristická určitá míra běžnosti (častnosti). Bude se jednat

[29] Uvedené dělení je shodné s členěním internetové kriminality uvedené v Kuchta, J., Válková, H. a kol. Základy kriminologie a trestní politiky. 1. vydání. Praha: C. H. Beck, 2005, str. 515.
[30] Uvedené dělení virtuálních trestných činů nestanovuje pevnou hranici mezi jednotlivými kategoriemi, jedná se o dělení proměnlivé podle současného vývoje technologií a společenských hodnot příslušné kultury.

o trestné činy, kdy informační technologie bude použita zejména jako nástroj. Jelikož se jedná v právu o nový fenomén, převládá v teorii skepse ke stíhání takovýchto společensky škodlivých jednání, přestože právní zájem na jejich stíhání v současné době nabývá na stále větším významu. Do této kategorie bychom mohli například řadit krádež, čistě virtuální dětskou pornografii aj.

c. *polemické* – tato kategorie odpovídá trestným činům, u nichž není možné, aby byly spáchány virtuálně, neboť to jejich povaha či účel nepřipouští, popř. půjde o skupinu jednání ve virtuálním prostředí, o níž z morálního hlediska víme, že není správná, ale není shledán dostatečný právní zájem na jejím postihu. Jako příklad lze uvést jednání naplňující skutkové podstaty trestných činů proti životu a zdraví[31]. Vražda (zabití) uskutečněné ve virtuálním prostředí je zcela irelevantní, neboť zde není přítomna společenská škodlivost, která by vyvolávala potřebu trestního postihu[32]. V opačném případě bychom se museli pozastavit nad situací, že nejsou trestné vraždy ve filmech. Společenská škodlivost zde není přítomna právě z důvodu, že se jedná o fikci.

   Polemiku takovýchto jednání lze však spatřovat ve smyslu reálného naplnění znaků příslušné skutkové podstaty, kdy kyberprostor, resp. i informační technologie obecně, je pouze pohnutkou či motivem[33].

2.3. Jednotlivé znaky virtuálních trestných činů

2.3.1. Objekt

Objektem trestného činu rozumíme právní hodnoty a zájmy, na jejichž zachování má společnost zvláštní zájem, takže jim stát poskytuje trestněprávní ochranu. Jedná se o abstraktní duchovní hodnoty společenského řádu, které jsou předmětem ochrany v trestním právu, nikoli o konkrétní reálné předměty. Obligatorním znakem je tzv. konkrétní (individuální) objekt, tj. konkrétní právní statek, který je příslušným

[31] Hlava I. zvláštní části trestního zákoníku.
[32] Stranou je ponecháno vnitřní morální přesvědčení týkající se propagace násilí ve virtuálním prostředí.
[33] Pro lepší pochopení lze uvést například situaci, kdy ve skutečnosti bude zavražděn majitel uživatelského účtu z důvodu, že v on-line hře vyhladil pachatelovu vesnici.

ustanovením jednotlivého trestného činu chráněn. V teorii pak rozlišujeme různé dělení objektů[34].

Konkrétní objekt u virtuálních trestných činů pak bude odvislý od každého jednotlivého případu, resp. rozhodující bude, jaká skutková podstata bude jednáním naplněna. Právní zájem, který bude chráněn, může být různý.

V případě pravých virtuálních trestných činů může být objektem ochrana počítačových systémů a jejich částí, dat v nich uložených, ochrana počítačů nebo jiných druhů informačních technologií před neoprávněnými přístupy a zásahy apod. U nepravých virtuálních trestných činů bude ochrana poskytována (v návaznosti na vlastnosti virtuálního prostředí) nejčastěji osobnosti, soukromí a majetku, nejsou však vyloučeny objekty další. Základním kritériem bude, jakého „tradičního" trestného činu se pachatel v kyberprostoru nebo v souvislosti s ním dopustí.

Zcela nereálná je představa, že by v rámci virtuálních trestných činů byl primárním objektem život osoby. Situace, kdy by byl například v online hře zavražděn avatar a uživatel, který jej zabil, by měl být trestně stíhán, je nepravděpodobná, a to vzhledem k absenci zájmu společnosti na ochraně před takovýmito jednáními z důvodu neexistence společenské škodlivosti. Základní skutečností zůstává, že avatar není z právního hlediska považován za osobu, ale virtuální věc patřící k uživatelskému účtu. Reálné přenesení živé osoby do kyberprostoru není možné, a proto není možné dopustit se virtuálního trestného činu směřujícího k porušení nebo ohrožení života. Na druhé straně si však lze představit situaci, kdy dojde k vraždě skutečné osoby v souvislosti s kyberprostorem[35].

[34] K tomu blíže: Novotný, O., Vanduchová, M., Šámal, P. a kol. *Trestní právo homotné. Obecná část.* 6. vydání, Praha: Wolters Kluwer ČR, a.s., 2010, str. 132; Jelínek, J. a kol.: *Trestní právo hmotné.* 1. vydání. Praha: Leges, 2009, str. 152 a násl.

[35] V Číně se odehrál případ, kdy dva přátelé Qiu a Zhu získali v rámci internetové hry unikátní meč, jenž potom Zhu bez souhlasu svého přítele prodal na internetové aukci za 7200 juanů. Qiu šel tento skutek oznámit na policii, kde mu bylo sděleno, že na virtuální vlastnictví se zákony nevztahují a odmítli tento případ řešit. Qiu byl však natolik rozčílen počínáním svého přítele, že jej napadl a několika bodnými ranami usmrtil. Blíže viz: Polčák, R. K problémům působnosti trestního práva na internetu. In Acta universitatis carolinae – Iuridica 4, 2008, str. 91-106.

2.3.2. Objektivní stránka

Objektivní stránka trestného činu je charakterizována způsobem spáchání trestného činu a jeho následky. Mezi tzv. obligatorní znaky patří jednání, následek a příčinná souvislost mezi nimi. Mezi fakultativní znaky pak můžeme řadit například místo a čas jednání, způsob spáchání, použitý prostředek apod.[36]

Z hlediska virtuálních trestných činů zde budou rozdíly oproti platné teorii nejméně patrné. Pro jednání, tj. konání i opomenutí, bude platit obecná charakteristika s tím rozdílem, že projev vůle učiněný navenek bude muset mít určitou návaznost na kyberprostor. V daném kontextu bychom mohli fakultativní znak „místo" vázat jako znak obligatorní, neboť místem spáchání v případě pravých virtuálních trestných činů bude kyberprostor.

Následkem se rozumí porušení nebo ohrožení objektu. Vzhledem ke globálnímu rozměru a neomezenému prostoru virtuálního prostředí mohou společensky škodlivá virtuální jednání způsobit negativní následky různého charakteru a intenzity, přičemž k neexistenci státních hranic mohou zasahovat i do více států. V neposlední řadě i zde pak musí být příčinná souvislost mezi jednáním a následkem.

2.3.3. Subjekt

V rámci skutkové podstaty trestného činu je nutné odlišovat konkrétního pachatele od obecných znaků kladených na subjekt (věk, příčetnost), které jsou vyžadovány u všech trestných činů. Obecně můžeme pachatele definovat jako fyzickou osobu, která svým jednáním naplnila všechny znaky trestného činu, v době jeho spáchání dovršila patnáctý rok svého věku a byla příčetná[37]. Z hlediska skutkové podstaty pak může být vyžadována zvláštní vlastnost, způsobilost nebo postavení pachatele, v takovém případě hovoříme o tzv. speciálním či konkrétním subjektu. V současné době se v trestním právu vychází ze zásady, že trestní odpovědnost může být dána jen u fyzické osoby, tzn. že i virtuálního trestného činu stíhatelného dle české

[36] Novotný, O., Vanduchová, M., Šámal, P. a kol. *Trestní právo homotné. Obecná část.* 6. vydání, Praha: Wolters Kluwer ČR, a.s., 2010, str. 151 a násl.
[37] Tamtéž, str. 185 a násl.

právní úpravy se může dopustit pouze konkrétní fyzická osoba. Přestože doposud nemáme upravenu trestní odpovědnost právnických osob, můžeme se setkat s pokusy jejího zavedení[38].

Pro virtuální trestné činy má osoba pachatele specifický význam. Nenalezneme zde typický příklad osob pachatelů, naopak je lze rozdělit do jednotlivých skupin, pro něž jsou vždy charakteristické určité vlastnosti.

Podle některých názorů je kyberkriminalita spojována s kriminalitou tzv. bílých límečků, tj. kriminalitou středních a vyšších vrstev. Pro pachatele je dle statistických dat příznačné, že v průměru dosahují vysokoškolského stupně vzdělání a ke spáchání těchto trestných činů potřebují značné technické znalosti[39].

V dnešní době není jednoduché vymezit typického pachatele virtuálních trestných činů. Byl překonán názor, že se jedná o kriminalitu bílých límečků, a došlo k rozšíření této skupiny. Statisticky bylo zjištěno, že nejčastějšími pachateli jsou osoby ve věku 15 až 35 (i více) let. Věková kategorie souvisí především s rozvojem samotných informačních technologií, které jsou používány zejména mladší a střední generací. Dalším typickým znakem je pohlaví pachatele, a to v tom smyslu, že tento druh kriminality je běžný pro mužskou populaci. Tento fakt bývá vysvětlován různými teoremi. Důvody jsou spatřovány v náhražce sexuální aktivity[40] nebo v neochotě a nezájmu žen o technické a programátorské obory.

V literatuře je pachatel kyberkriminality obvykle vymezován jako osoba se středoškolským, jiným vyšším nebo vysokoškolským vzděláním, zejména v technických oborech, speciálně v oboru informačních technologií. Jedná se o osobu inteligentní s potřebnou mírou přizpůsobivosti a ovládající potřebné dovednosti a znalosti spojené s informačními technologiemi[41].

Důležitým faktorem pro vymezení osoby pachatele je skutečnost, zda se jedná o virtuální trestný čin pravý či nepravý. U pravých virtuálních trestných činů

[38] Parlament České republiky. Poslanecká sněmovna. 2004 IV. volební období. Tisk 745 – Vládní návrh zákona o trestní odpovědnosti právnických osob a řízení proti nim. Návrh byl zamítnut.
[39] Završnik, A. Definiční problémy a kriminologická specifika kyberzločinu. In: Gřivna, T., Polčák, R. (eds.). Kyberkriminalita a právo. Praha: Auditorium, 2008, str. 26-48.
[40] Blíže tamtéž, str. 42.
[41] Kuchta, J., Válková, H. a kol. Základy kriminologie a trestní politiky. 1. vydání. Praha: C. H. Beck, 2005, str. 507.

je z povahy těchto činů pravděpodobné, že pachatel bude muset disponovat určitým stupněm informačně-technologických dovedností a znalostí, aby se mohl dopustit příslušného jednání vymezeného skutkovou podstatou. Naproti tomu u nepravých virtuálních trestných činů nejsou tyto dovednosti a znalosti podstatné, tzn. že pachatel je nemusí mít, resp. musí mít pouze obecné znalosti ohledně používání konkrétní informační technologie (např. počítače, Internetu), jejichž získání v dnešní společnosti nečiní problém.

Lze shrnout, že pro všechny druhy pachatelů je typická určitá míra přizpůsobivosti a schopnosti ovládat informační technologie.

Kyberprostor skýtá řadu výhod pro páchání škodlivých jednání a pachatelé jsou si toho plně vědomi. Pachatelé využívají anonymity, kterou kyberprostor přináší, a fyzické nepřítomnosti jejich osoby, která snižuje možnost odhalení a dopadení. Většinou jednají individuálně s minimálním možným rizikem a psychickým tlakem pro sebe. Rovněž využívají nízkou nákladovost spočívající v používání informační technologie a její rychlost. Z určitého místa, které je v rámci kyberprostoru obtížně lokalizovatelné, páchají trestnou činnost ve velmi krátkém čase.

Motivy pachatelů mohou být různé, například ziskuchtivost, překonání sebe sama, pomsta aj. Vždy bude rozhodující o jakou skupinu pachatelů se bude jednat. Na předním místě motivace je touha po zisku, a proto virtuální trestné činy nejčastěji zasahují do majetkové sféry. V současné době se však můžeme setkat i s motivací dokazování si vlastních schopností a snahou překonat ostatní pachatele a získat si tak jejich respekt a uznání.

2.3.3.1. Klasifikace pachatelů

Nejrozšířenějším obecným členěním je členění z hlediska jejich vztahu k informacím, a to na amatéry, profesionály a teroristy[42].

[42] Předmětná klasifikace je přebrána z Kuchta, J., Válková, H. a kol. Základy kriminologie a trestní politiky. 1. vydání. Praha: C. H. Beck, 2005, str. 507 a násl.

Amatéři jsou osoby pronikající do informačních systémů náhodně nebo cílevědomě tak, že vyhledávají zranitelná místa. Osobnostně jde zpravidla o osoby s vyšší jednostranně rozvinutou inteligencí, jsou přizpůsobiví (lehce se naučí manipulaci s počítačem), vytrvalí a vynalézaví, většinu úkonů provádějí i automaticky a jsou neustále schopní vstřebávat nové informace, analyzovat je a pružně reagovat na změněnou situaci. Do této skupiny řadíme tzv. průnikáře neboli hackery, což je v rámci kyberprostoru nejčastější pojem, s nímž se lze z pohledu osobnosti pachatele setkat, a je veřejností používán v širokém významu. Hacker je označení pro pachatele kyberkriminality, jehož cílem je prokázání jeho schopností a znalostí, aniž by měl zájem získávat informace, poškozovat systém či získávat jiný osobní profit. S rozvojem informačních technologií se všeobecně a široce užívaný pojem hacker začal štěpit. Vyčlenila se další samostatná skupina pachatelů nazývaných tzv. crackeři. Cracker představuje označení pro pachatele, jenž využívá své technické znalosti k páchání kyberkriminality za účelem hromadění zisku[43].

Dále do této kategorie můžeme řadit i tzv. neúspěšné kritiky, jejichž motivace je ovlivněna neúspěšným poukazování na závady a nedostatky v informačních systémech bez zištného cíle, a tzv. mstitele a škodiče, jimž nejde jen o překonání ochranných překážek, ale ze způsobení škody a destrukce systému mají spíše radost.

Další skupinou jsou *profesionálové*, kteří tvoří specifickou kategorii s vyšší mírou inteligence a technických znalostí typických pro kyberprostor. Jejich náplň práce je dána informačním procesem a k počítačovým prostředkům mají prakticky neomezený přístup. Tuto činnost nevykonávají většinou pro sebe, ale pro zaměstnavatele, není však vyloučeno, že se jedná o individuální osoby. Motivací je zejména zisk. Patří sem například pracovníci managementu, programátoři nebo softwaroví piráti.

Teroristé tvoří zvláštní skupinu pachatelů, kteří jsou zpravidla spjatí s organizovaným zločinem, operují většinou vlastními zpravodajskými sítěmi, a to jak pro získávání potřebných informací, tak i pro vlastní ochranu zločinecké organizace. Mohou být velice kvalifikovaní, obdobně jako pracovníci oficiálních zpravodajských služeb. Odlišné bývá jejich zaměření, cíle, způsoby a prostředky dosažení těchto cílů.

[43] Završnik, A. Definiční problémy a kriminologická specifika kyberzločinu. In: Gřivna, T., Polčák, R. (eds.). Kyberkriminalita a právo. Praha: Auditorium, 2008, str. 26-48.

Počítačoví teroristé ke svým nekalým aktivitám využívají stále častěji prostředí mezinárodní sítě Internet, neboť jim poskytuje dostatečnou anonymitu[44].

Podle práva duševního vlastnictví se můžeme setkat s dělením pachatelů na tzv. černé uživatele a piráty. První skupina porušuje práva duševního vlastnictví pouze se záměrem získat produkt pro své vlastní užití, naproti tomu druhá skupina je motivována ziskem, který lze realizovat z prodeje příslušného produktu[45].

Černí uživatelé tvoří širokou škálu pachatelů. Můžeme zde řadit tzv. domácího uživatele jako konkrétní fyzickou osobu, která získala, případně dále nelegálně získaná práva duševního vlastnictví využívá pro svou vlastní potřebu, anebo tzv. potencionálního pachatele, pod nímž se skrývá osoba, která svůj čas tráví ve virtuálním prostředí a příležitostně se jí naskytne možnost získat nějaký profit.

Na základě výše uvedených poznatků bychom mohli dále členit pachatele virtuálních trestných činů na ty, kteří kyberkriminalitu páchají cílevědomě, a na tzv. příležitostné typy, jejichž jednání lze považovat za nahodilé. Příležitostní pachatelé budou pravděpodobně nejrozšířenější skupinou, neboť v sobě zahrnují i jednotlivé fyzické osoby, které ani nemusí vědět, že jsou pachateli kyberkriminality.

2.3.4. Subjektivní stránka

Jediným obligatorním znakem je zde zavinění, které je chápáno jako vnitřní psychický vztah pachatele k určitým skutečnostem, jež zakládají trestný čin. Rozlišujeme dvě základní formy zavinění, a to zavinění úmyslné a nedbalostní. Fakultativními znaky pak mohou být například pohnutka, cíl, záměr aj.[46]

Obecná charakteristika subjektivní stránky se uplatní i u virtuálních trestných činů, přičemž se zpravidla bude jednat o úmysl, avšak podle konkrétního druhu

[44] Musil, S. Počítačová kriminalita. Nástin problematiky. Institut pro kriminologii a sociální prevenci, Praha 2000, str. 246 a násl.
[45] Završnik, A. Definiční problémy a kriminologická specifika kyberzločinu. In: Gřivna, T., Polčák, R. (eds.). Kyberkriminalita a právo. Praha: Auditorium, 2008, str. 26-48.
[46] Novotný, O., Vanduchová, M., Šámal, P. a kol. *Trestní právo homotné. Obecná část.* 6. vydání, Praha: Wolters Kluwer ČR, a.s., 2010, str. 219 a násl.

trestného činu může postačovat nedbalost za uplatnění pravidla, že příslušná právní norma tak výslovně stanoví.

3. Právní úprava

Jak již bylo uvedeno v úvodní kapitole, kyberprostor je imaginární prostor, který je spojován s informačními technologiemi a má specifické vlastnosti. Jedná se o prostor, který nemá stanoveny pevné reálné hranice a z místního (geografického, teritoriálního) hlediska jej nelze omezit, neboť se jedná o prostředí globální. Spolu s anonymitou, která je pro něj rovněž typická, přináší možnost dopouštět se v něm pro společnost škodlivých jednání, která mohou být z hlediska časového spáchána v nepředstavitelně krátkém čase („jedním klikem“).

Dnes si je již většina moderních států vědoma negativ kyberprostoru a snaží se na tento jev reagovat změnou právní úpravy, která by eliminovala hrozící rizika. Vnitrostátní zákonodárství je však vzhledem k uvedeným specifikům nedostačující, neboť státy jsou omezeny svým územím, tj. státními hranicemi, které nemohou z vlastní iniciativy překročit. Z těchto důvodů vznikla celosvětová, resp. přeshraniční potřeba právní regulace, která se zejména orientuje na problematiku pravých virtuálních trestných činů. Stěžejním oblastí, která je mezinárodně (nadnárodně) právně regulována, je zejména problematika internetového prostředí. I zde se však potýkáme s problémy, které mezinárodní spolupráci doprovázejí od samého počátku, a těmi jsou rozmanitost jednotlivých národních právních úprav a neochota států omezovat svou trestní jurisdikci. Z mezinárodního pohledu jsou proto upravena jen ta jednání, jenž jsou považována za nejnebezpečnější (např. trestné činy v majetkové sféře, ochrana osob, ochrana před útoky na počítačové systémy, dětská pornografie aj.) Přestože k dané problematice vznikají právně závazné dokumenty, jejichž počet neustále narůstá, není současná situace dostatečně uspokojivá[47].

[47] Dále jsou uvedeny právně závazné dokumenty, které jsou považovány z hlediska této práce za nejpodstatnější. Širší výčet obsažen např. In: Gřivna, T. Závazky k ochraně kyberprostoru vyplývající z evropského a mezinárodního práva. In: Acta universitatis carolinae – Iuridica 4, 2008, str. 21-34.

3.1. Mezinárodní úprava

Nejvýznamnějším mezinárodním dokumentem vzniknuvším na půdě Rady Evropy, který upravuje problematiku virtuálního prostředí, je Úmluva o kybernetické kriminalitě (dále jen „Úmluva“)[48], jejímuž přijetí předcházelo doporučení Rady Evropy č. R (89) 9 z 13.9.1989, které se týká trestných činů souvisejících s počítači. Úmluva byla přijata dne 8.11.2001 a k podpisu byla otevřena dne 23.11.2001 v Budapešti, přičemž v platnost vstoupila dne 1.7.2004. Ke dni 1.6.2010 Úmluvu podepsalo 44 států, z nichž ji ratifikovalo 29 států. V roce 2010 Úmluvu ratifikovali Ázerbájdžán a Portugalsko, v blízké době by měla být ratifikována i Španělskem[49]. Česká republika podepsala Úmluvu dne 9.2.2005, doposud ji však neratifikovala.

Úmluva obsahuje preambuli a dále se člení na 4 kapitoly, v nichž je obsaženo 48 článků. Vymezuje základní pojmy jako jsou počítačový systém nebo počítačová data, dále vymezuje opatření přijímaná na národní úrovni, tj. upravuje závazky států v oblasti trestního práva hmotného i procesního, včetně působnosti vnitrostátních norem. Z hlediska hmotněprávního charakteru obsahuje Úmluva skutkové podstaty 9 trestných činů, které dělí do čtyř kategorií[50]. U každého trestného činu je výslovně uveden znak protiprávnosti a žádný z nich není možné spáchat z nedbalosti. U některých z těchto jednání se vyžaduje tzv. druhý specifický úmysl a v řadě případů je možné omezit trestní odpovědnost jen na nejzávažnější jednání, kdy smluvní státy mají možnost vyžadovat naplnění dodatečné okolnosti (např. nečestný úmysl pachatele, spáchání činu ve vztahu k počítačovému systému, který je propojen s jiným počítačovým systém, vznik závažnější škody apod.).

Z hlediska procesního se Úmluva dotýká vytvoření nových, resp. úpravy stávajících procesních institutů, které povedou k zajištění elektronických důkazů a odhalení pachatele. Řeší rovněž některé otázky základní trestní odpovědnosti jako odpovědnost právnických osob, účastenství, pokusu a v neposlední řadě se zabývá otázkami mezinárodní spolupráce. V rámci dalšího výkladu je důležité podotknout,

[48] Convention on Cybercrime. Lze se setkat i s překladem „Úmluva o počítačové kriminalitě“, který je však nepřesný.
[49] Informace dostupná z: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=01/06/2010&CL=ENG.
[50] Viz Příloha č. 1 . Blíže viz Gřivna, T. K ustanovením Úmluvy o počítačové kriminalitě. In: Gřivna, T., Polčák, R. (eds.). Kyberkriminalita a právo. Praha: Auditorium, 2008.

že Úmluva dává smluvním státům relativní volnost, neboť ponechává na jejich vůli, zda příslušná ustanovení Úmluvy do vnitrostátní úpravy promítnou či nikoliv. Smluvní stát, který nehodlá aplikovat některá z těchto ustanovení Úmluvy, musí prohlásit formou písemného oznámení, že si ponechává možnost učinit výhradu, popř. výhrady, které jsou samotnou Úmluvou připuštěny. Výčet ustanovení, ke kterým lze vznést výhradu, je však taxativní.

Česká právní úprava se snaží na tuto Úmluvu reagovat, avšak ne ve všech ohledech je s ní v souladu. Z hlediska hmotněprávního byla v trestním zákoníku nově upravena zejména ustanovení § 230 až 232, jimž je věnována následná podkapitola. Z procesního hlediska je však situace neuspokojivá, neboť současný platný trestní řád má pouze omezené možnosti, které jsou často nevyhovující (§§ 78, 79, 86 až 87c, 88 a 88a), a v návaznosti na Úmluvu dosud nezavádí žádné nové specifické instituty, které by procesní postup usnadňovaly[51].

K Úmluvě byl přijat Dodatkový protokol[52], který se týká kriminalizace činů rasistické a xenofobní povahy spáchané prostřednictvím počítačových systémů. K podpisu byl otevřen 28.1.2003 a v platnost vstoupil 1.3.2005. Ke dni 1.6.2010 jej podepsalo 34 států, z toho ratifikovalo 17[53]. Česká republika Dodatkový protokol prozatím nepodepsala.

Dodatkový protokol rozšiřuje Úmluvu o možnost harmonizace skutkových podstat trestných činů, které mají postihovat rasistickou a xenofobní propagandu šířenou prostřednictvím počítačových sítí a zlepšit metody mezinárodní spolupráce. Smluvní státy se zavázaly přijmout taková legislativní a další opatření, která mohou být nezbytná k tomu, aby následující jednání byla označena podle národního práva za trestné činy, pokud k jejich spáchání dojde prostřednictvím počítačového systému, úmyslně a neprávem[54]:

a. šíření rasistických a xenofobiích materiálů,

b. rasisticky a xenofobně motivovaná pohrůžka,

[51] K tomu blíže viz: Gřivna, T. Závazky k ochraně kyberprostoru vyplývající z evropského a mezinárodního práva. In: Acta universitatis carolinae – Iuridica 4, 2008, str. 21-34.
[52] Dodatkový protokol (ETS No. 189) k Úmluvě Rady Evropy o počítačové kriminalitě ze dne 28.1.2003.
[53] Informace dostupná z: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=1&DF=01/06/2010&CL=ENG.
[54] Blíže viz Herczeg, J. Dodatkový protokol k Úmluvě o počítačové kriminalitě. In: Gřivna, T., Polčák, R. (eds.). Kyberkriminalita a právo. Praha: Auditorium, 2008.

c. rasisticky a xenofobně motivovaná urážka

d. popření, hrué snižování, schvalování nebo ospravedlnění genocidy nebo zločinů proti lidskosti,

e. návod a pomoc k jednáním a. až d.

Dalšími prameny upravující otázky kyberkriminality je Úmluva o prevenci terorismu ze dne 16.5.2005, která mimo jiné stanovuje povinnost členským státům kriminalizovat veřejné, tj. i internetové (popř. jiný druh technologie, která je veřejně přístupná) podněcování k teroristickému činu[55]. V platnost vstoupila dne 1.6.2007, podepsalo ji 43 států, z nichž ratifikovalo 24. Česká republika není signatářem této úmluvy.

Významné postavení, zejména z hlediska mezinárodní spolupráce, zaujímá Rezoluce Hospodářské a sociální Rady OSN týkající se mezinárodní spolupráce v oblasti prevence, vyšetřování, stíhání a trestání hospodářských podvodů a trestných činů souvisejících s identitou osob, která byla přijata dne 26.7.2007. Apeluje na členské státy, aby upravily své národní úpravy s ohledem na stíhání trestných činů nedovoleného získání, kopírování, padělání a zneužívání dokumentů, které identifikují osoby, a osobních údajů.

Řada významných dokumentů vzniká i na poli dětské pornografie. Patří mezi ně například Úmluva o ochraně dětí před sexuálním vykořisťováním a zneužíváním ze dne 25.10.2007 (v platnost vstoupila dne 1.7.2010), která zavazuje smluvní státy mimo jiné k postihu výroby, nabízení, distribuce, získání, držení a vědomého získání přístupu k dětské pornografii prostřednictvím informačních a telekomunikačních technologií. Tuto úmluvu podepsalo 39 států, z nichž ratifikovalo 7[56].

3.2. Evropská úprava – právo EU

Právo Evropské unie představuje oproti úpravě mezinárodní mnohem širší záběr problematiky kyberkriminality. Na půdě EU vznikají právní dokumenty, které mají

[55] Gřivna, T. Závazky k ochraně kyberprostoru vyplývající z evropského a mezinárodního práva. In: Acta universitatis carolinae – Iuridica 4, 2008, str. 21-34.

[56] Informace dostupná z: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=201&CM=8&DF=08/08/2010&CL=ENG.

pro smluvní státy různou závaznost. Problematika trestního práva do přijetí Lisabonské smlouvy spadala převážně do třetího pilíře, a proto v právní regulaci EU převažují zejména rámcová rozhodnutí, doporučení a směrnice.

Rámcové rozhodnutí Rady 2005/222/SV ze dne 24.2.2005 o útocích proti informačním systémům je zaměřeno na účinný boj smluvních států proti vyspělým technologiím (tzv. high technology), které jsou používány k páchání trestné činnosti. Rámcové rozhodnutí zavádí jednotnou terminologii a vypočítává trestné činy, které by měly smluvní státy stíhat[57]. Základní charakteristika vyjmenovaných trestných činů spočívá v jejich neoprávněnosti, úmyslné formě zavinění a musí být stíhána jednání, alespoň pokud se nejedná o případy menšího významu. Smluvní státy mají tedy povinnost stíhat veškerou trestnou činnost většího významu, v případě menšího významu je postih ponechán na jejich vůli. Rámcové rozhodnutí stanovuje jako jeden ze svých cílů zamezení přílišné kriminalizaci, zejména v případech menšího významu. Definici slovního spojení „menšího významu“ však nevymezuje, naproti tomu Komise ve své zprávě ze dne 14.7.2008[58] uvádí, že pojetí „případu menšího významu“ musí odkazovat na případy, kdy došlo k protiprávnímu přístupu menší důležitosti nebo kdy porušení důvěrnosti informačního systému je menšího stupně.

I v právu EU je velká pozornost věnována boji proti dětské pornografii. Mezi významné právní dokumenty patří Rámcové rozhodnutí Rady 2000/375/JHA ze dne 29.5.2000 o boji proti dětské pornografii na internetu, jehož podstatou je stanovení opatření, která mají přispět k odhalení a regulaci dětské pornografie v prostředí Internetu. Předmětné Rámcové rozhodnutí nevypočítává žádné skutkové podstaty trestných činů, ale v čl. 1 stanovuje závazek členským státům přijmout nezbytná opatření, která podpoří uživatele internetu, aby přímo nebo nepřímo oznamovali donucovacím orgánům podezření o šíření dětského pornografického

[57] Výčet trestných činů: protiprávní přísup k informačním systémům, protiprávní zásah do systému a protiprávní zásah do dat. Rámcové rozhodnutí dostupné na: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:CS:HTML.

[58] KOM (2008) 448 v konečném znění, dostupná z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52008DC0448:CS:HTML, vznikla v návaznosti na povinnost smluvních států informovat Komisi a Generální sekretariát o postupu provádění Rámcového rozhodnutí do vnitrostátní úpravy.

materiálu na internetu, pokud se s takovým materiálem setkají[59]. Smluvní státy na takové oznámení mají reagovat a příslušnou situaci začít řešit. V České republice lze v současné době nahlásit dětskou pornografii přímo orgánům činným v trestním řízení (Policii ČR či státnímu zástupci) nebo společnostem (organizacím) vznikajícím v rámci různých projektů, jejichž úkolem je zamezit šíření dětské pornografie a dalšího nelegálního obsahu Internetem[60]. Problematikou ochrany před přístupností k dětské pornografii se věnuje i řada firem zabývajících se komunikačními technologiemi. Příkladem je firma Vodafone, která blokuje přístup svých uživatelů k nelegálnímu obsahu, přičemž blokování těchto stránek je automatické a zákazník nemá možnost jej zrušit.

Další Rámcové rozhodnutí Rady 2004/68/SVV ze dne 22.12.2003 o boji proti pohlavnímu vykořisťování dětí a dětské pornografii[61] se věnuje problematice dětské pornografie jednak z obecného hlediska, jednak v rámci prostředí počítačových systémů. Rámcové rozhodnutí vymezuje základní pojmy (dítě, pornografický materiál) a v čl. 3 vypočítává jednotlivé trestné činy, přičemž po smluvních státech je vyžadováno, aby přijaly nezbytná opatření k založení své příslušnosti pro stíhání uvedených jednání, případně též pro účastenství a pokus. Tento postih má být zaručen bez ohledu na to, zda se počítačový systém nachází na území daného státu či nikoliv.

3.3. Česká právní úprava

Česká právní úprava se snaží na problematiku kyberkriminality pozitivně reagovat, zejména z hlediska pravých virtuálních trestných činů. Pravé virtuální trestné činy, tj. ty, kterých se lze dopustit jen v rámci kyberprostoru, máme v současném trestním zákoníku upraveny zejména v ustanoveních § 230 až 232, přičemž dané problematiky se dotýkají i jiná ustanovení, jako například ustanovení § 182. Naproti tomu na nepravé virtuální trestné činy lze vztáhnout kteroukoliv skutkovou podstatu

[59] Dokument dostupný z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:138:0001:01:CS:HTML.
[60] Projekt E-bezpečí, Internet Hotline (www.internethotline.cz)
[61] Dokument dostupný z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:013:0044:01:CS:HTML.

uvedenou ve zvláštní části trestního zákoníku, pokud to její povaha připouští (tradiční trestné činy). Na škodlivá jednání, která mají souvislost s kyberprosterem se použijí tradiční ustanovení trestných činů, jejichž skutkovou podstatu lze naplnit i v reálné situaci, tzn. že nebyla vytvořena za účelem postihu kyberkriminality. V právní praxi ovšem převládá dosavadní neochota subsumovat jednání spáchaná v souvislosti s virtuálním prostředím pod tradiční skutkové podstaty trestných činů.

3.3.1. Vybrané pravé virtuální trestné činy

Pravé virtuální trestné činy, tj. takové, které byly vytvořeny za účelem ochrany společnosti proti škodlivým jednáním, které kyberkriminalita skýtá, jsou upraveny zejména v Hlavě V. nazvané Trestné činy proti majetku v ustanoveních § 230 až 232 trestního zákoníku. Tato úprava byla provedena na základě Úmluvy o kybernetické kriminalitě.

Objektem výše uvedených trestných činů je zájem na ochraně počítačových systémů a jejich částí, dat v nich uložených a dat uložených na nosičích informací a také na ochraně počítačů nebo jiných technických zařízeních pro zpracování dat před neoprávněnými přístupy a zásahy. Chráněn je z hlediska majetkové stránky jak substrát hmotný, jehož prostřednictvím informace a data vznikají, ukládají se a používají, tak i nehmotný obsah informací a dat před jejich zneužitím, zničením, poškozením, změnou nebo učiněním je neupotřebitelnými. Zprostředkovaně pak tato ustanovení chrání rovněž soukromí osob, osobní údaje, obchodní tajemství, autorská díla a jiné nehmotné statky, údaje o zaknihovaných cenných papírech aj[62].

Základ těchto trestných činů tvoří počítačový systém či jeho část anebo jiné technické vybavení sloužící ke zpracování informací a dat (dále jen „počítačový sytém“). Je podstatné si uvědomit, že se nejedná o objekt trestného činu, ale o předmět útoku anebo nástroj sloužící k jeho spáchání.

[62] Novotný, O., Vanduchová, M., Šámal, P. a kol. *Trestní právo homotné. Obecná část.* 6. vydání, Praha: Wolters Kluwer ČR, a.s., 2010, str. 209.

Počítačovým systémem se rozumí jakékoli zařízení nebo skupina vzájemně propojených nebo souvisejících zařízení, z nichž jedno nebo více provádí na základě programu automatické zpracování dat. Sestává se z technického (hardware) a programového (software) vybavení, které je určené k automatickému zpracování digitálních dat., tj. bez přímého lidského zásahu. K počítačovému systému bývá často jako synonymum používáno slovo počítač. Ve skutečnosti je pojem počítačový systém širší, neboť zahrnuje i síťově připojená zařízení, která pojmově nesplňují atributy počítače, který je představován zařízením. Více navzájem propojených počítačů tvoří síť založenou na konkrétním druhu propojení (bezdrátové, kabelové aj.). Na principu propojení jednotlivých počítačů, jež všechny používají stejné protokoly, je postavena síť Internet[63].

Vedle pojmu počítačový systém trestní zákoník užívá i pojem nosič informací, pod kterým si představujeme jakýkoliv nosič v informační technologii, tj. materiál, do kterého nebo na který lze zaznamenávat data a z kterého lze data zpět získat (pevný disk, operační paměť, mobilní telefon aj.)[64].

Objektivní stránka, jenž charakterizuje způsob spáchání trestného činu a jeho následky, je pro každou skutkovou podstatu stanovena odchylně.

Po subjektivní stránce se vyžaduje úmyslné zavinění, z čehož vyplývá, že pachatel v daném případě ví, že svým jednáním může takové porušení nebo ohrožení způsobit, a pro případ, že se tak skutečně stane, je s tím srozuměn, tj. je s tím smířen. Výjimku představuje ustanovení § 232, který je vázán na nedbalostní formu zavinění.

Pachatelem výše uvedených trestných činů může být kdokoliv, s výjimkou ustanovení § 232, kde pachatelem může být kterákoli fyzická osoba, vykonávající zaměstnání, povolání, postavení nebo funkci (z něhož ji vyplývá určitá povinnost, již porušila), ale i jakákoli jiná taková osoba, která porušila zákonem uloženou nebo smluvně převzatou povinnost.

[63] Šámal, P. a kol. Trestní zákoník II. § 140 až 421. Komentář. 1. vydání. Praha: C. H. Beck, 2010, str. 2087.
[64] Tamtéž, str. 2089.

3.3.1.1. Neoprávněný přístup k počítačovému systému a nosiči informací (§ 230)

Toto ustanovení obsahuje dvě samostatné základní skutkové podstaty. V odstavci 1 je předmětem ochrany důvěrnost počítačových dat a počítačového systému (jeho části). V odstavci 2 jsou pak primárně chráněny integrita a dostupnost počítačových dat a systémů před neoprávněnými zásahy, které mohou mít vliv na existenci, kvalitu, správnost dat, a rovněž chrání před neoprávněným užíváním uložených počítačových dat.

Objektivní stránka v odstavci 1 spočívá v neoprávněném přístupu k počítačovému systému za podmínky, že pachatel překoná bezpečnostní opatření. Bezpečnostním opatřením se rozumí každé opatření, jehož cílem je zabránit volnému přístupu k počítačovému systému nebo nosiči informací, přičemž nezáleží na stupni zabezpečení, nýbrž postačí, že pachatel musí překonat nějakou překážku (například heslo)[65].

V kybernetickém prostředí se neoprávněný přístup běžně nazývá jako hacking[66] (osoba, která se jej dopustí se označuje „hacker“). Z hlediska trestního práva jsou jako hacking označována škodlivá jednání spočívající v neoprávněném průniku do konkrétního informačního systému, který je proveden zpravidla ze vzdáleného počítače. Tento průnik nevzniká přímou cestou, ale prostřednictvím více internetových serverů umístěných v různých částech světa, což znesnadňuje odhalení pachatele, resp. počítače, ze kterého pachatel průnik provádí. Neoprávněný přístup může a zároveň nemusí být cílem sám o sobě. V případě hackingu bývá často záměrem pachatele samotný průnik bez jakéhokoliv dalšího zištného úmyslu[67], naproti tomu osoby, které neoprávněně pronikají do počítačových systému za účelem spáchání protiprávních jednání, získání majetkového nebo jiného osobního prospěchu, nazýváme termínem *cracker*.

---

[65] Šámal, P. a kol. Trestní zákoník II. § 140 až 421. Komentář. 1. vydání. Praha : C. H. Beck, 2010, str. 2085 a násl.

[66] Anglický termín pro neoprávněný přístup do počítačového systému jiné osoby za účelem prohlížení a/nebo změny informací. Oxford University Press - OALD dictionary. Dostupný z: http://www.oup.com.

[67] Např. touha hackera dokázat, že je chytřejší než ostatní a že překoná bezpečností opatření, jejichž účelem je právě zabránit vniknutí. Viz Šámal, P. a kol. Trestní zákoník II. § 140 až 421. Komentář. 1. vydání. Praha : C. H. Beck, 2010, str. 2086.

Hacking však nemusí být vždy protiprávní, neboť v současné době se můžeme setkat i s tzv. legálním hackingem. Všeobecně se jedná o situace, kdy ochránci zákona (příslušné státní orgány) postupují stejným způsobem jako hackeři, tj. pronikají na dálku do podezřelých počítačových systémů bez vědomí a souhlasu jejich majitelů[68].

Praxe řeší otázku, zda trestným činem má být každý neoprávněný přístup, nebo zda se má kriminalizovat jen průnik, který má umožnit spáchání jiného trestného činu nebo je jeho součástí. Vzhledem k výše uvedenému je tato otázka diskutabilní. Odpověď spočívá v právní úpravě a škodlivosti daného jednání. Legální hacking představuje průnik do počítačového systému, který požívá právní ochrany a nemůže být tudíž trestný. Takovéto situace jsou v jednotlivých státech pokryty právními předpisy[69]. V České republice nemáme legální hacking uzákoněn.

V ostatních případech hackingu bude východisko představovat škodlivost jednání a princip ultima ratio. Společenská škodlivost se bude muset posuzovat v každém jednotlivém případě a bude dána různými okolnostmi, zejména významem a intenzitou zasaženého zájmu. V teorii se setkáváme s názorem[70], že významný faktor společenské škodlivosti je dán mírou zabezpečení počítačového systému, do něhož pachatel pronikl. V případě, že počítačový systém nebude nikterak zabezpečen a pachatel nemusí překonávat žádné bezpečnostní opatření, lze takový případ posoudit s menší intenzitou škodlivosti pro společnost, než v případě zabezpečeného systému, kdy pachatel musí použít svých specifických znalostí a ve většině případů použít prostředky či nástroje, které nejsou běžné.

V odstavci 2 spočívá společenská škodlivost v získání přístupu k počítačovému systému nebo nosiči informací spolu s naplněním alespoň jedné z dalších okolností,

[68] Tento postup je např. uzákoněn ve Velké Británii. Současně se jedná i o novou strategii Evropské unie v boji proti kyberkriminalitě. Blíže viz *Council Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime* (Závěry Rady EU o vzájemné pracovní strategii a praktických opatřeních proti kybernetické trestné činnosti), 2987th JUSTICE and HOME AFFAIRS Council meeting Brussels, 27-28 November 2008. Dokument dostupný na www.eu2008.fr, http://eur-lex.europa.eu aj.

[69] První zemí, která se hlásí k legálnímu hackingu je Velká Británie. Tento postup umožňuje Regulation of Investigatory Powers Act 2000. Dostupný z: http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1. Naproti tomu např. v Německu se legální hacking do právní úpravy nezdařilo zavést.

[70] Viz Šámal, P. a kol. Trestní zákoník II. § 140 až 421. Komentář. 1. vydání. Praha: C. H. Beck, 2010, str. 2086.

které jsou uvedeny pod písmeny a) až d)[71]. Zde již však není podstatné, zda pachatel má přístup oprávněný či neoprávněný, ale stěžejní je neoprávněné užití a ostatní vyjmenované způsoby dispozice. Získáním přístupu (u obou odstavců) se pak rozumí takové jednání, které umožní pachateli volnou dispozici s počítačovým systémem nebo jeho částí a využití jeho informačního obsahu.

a) *neoprávněné užití dat* – tzv. počítačová špionáž, je jakákoliv nedovolená manipulace s daty uloženými v počítačovém systému nebo na nosiči informací, přičemž musí jít o takové užití, které je v rozporu s právní normou z hlediska celého právního řádu, popř. je činěno v rozporu se stanoveným účelem, tj. bez vědomí či souhlasu oprávněného.

b) *vymazání nebo jiné zničení, poškození, změna, potlačení, snížení kvality dat nebo učinění je neupotřebitelnými* – tzv. počítačová sabotáž, která spočívá v neoprávněné manipulaci s daty, která vede k jejich odstranění, nebo se snižuje jejich upotřebitelnost. K počítačové sabotáži se využívá celá řada škodlivých software programů (tzv. malware[72]), jako jsou viry, červi a tzv. trojští koně mající celou řadu funkcí, které mohou počítačový systém nezvratně poškodit.

c) *padělání nebo pozměnění dat, tak aby byla považována za pravá nebo s nimi bylo jednáno tak, jako by to byla data pravá* – jedná se o tzv. falzifikaci počítačových údajů, která spočívá v získání přístupu k počítačovému systému a k vytvoření či úpravě falešných dat, která mají vyvolat dojem, že jsou pravá. Toto jednání je obdobné falzifikaci listin s tím rozdílem, že zde mají data elektronickou podobu.

d) *neoprávněné vložení dat nebo učinění jiného zásahu do programového či technického vybavení počítače* – jedná se o jednu z podob počítačové

[71] Viz Příloha č. 2. Pro další výklad použita literatura: Šámal, P. a kol. Trestní zákoník II. § 140 až 421. Komentář. 1. vydání. Praha: C. H. Beck, 2010, str. 2086. Novotný, O., Vanduchová, M., Šámal, P. a kol. *Trestní právo homotné. Obecná část.* 6. vydání, Praha: Wolters Kluwer ČR, a.s., 2010. Gřivna, T., Polčák, R. (eds.). Kyberkriminalita a právo. Praha: Auditorium, 2008.

[72] Anglický termín pro počítačový program, který je určen ke vniknutí nebo poškození počítačového systému. Informace dostupná z: http://cs.wikipedia.org/wiki/Malware.

sabotáže, která směřuje jednak proti programovému vybavení počítače (softwaru), tak i technickému vybavení počítače (hardwaru), přičemž takovýto zásah nespadá pod jednání uvedená pod písmeny a) až c).

Trestný čin dle ustanovení § 230 trestního zákoníku vyžaduje formu úmyslného zavinění, jako následek však není uvedeno způsobení škody. Ta je až součástí kvalifikovaných skutkových podstat.

3.3.1.2. Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231)

Objektem tohoto ustanovení je zájem na ochraně před možným ohrožením vyplývajícím z nekontrolovaného opatření a přechovávání zařízení, nástrojů a prostředků. Jedná se o předčasně dokonaný trestný čin, tzn. že jednání, které spočívá ve výrobě, uvedení do oběhu, dovozu, vývozu, provozu, nabídce, zprostředkování, prodeji nebo jiného zpřístupnění sobě či jinému nebo přechovávání zařízení, postupu, nástroje či jiného prostředku, anebo počítačového hesla, přístupového kódu či dat[73], je pouze jednáním přípravným, které je povýšeno na dokonaný trestný čin. Účelem bylo uzákonit takovéto jednání, neboť by jeho příprava nebyla dle trestního zákoníku trestná.

V rámci ustanovení § 231 se vyžaduje zavinění ve formě úmyslu, který však přesahuje objektivní stránku, neboť pachatel zde jedná v tzv. druhém úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 trestního zákoníku, který charakterizují cíl pachatele[74].

[73] Výklad pojmů: *Přístupovým zařízením* se rozumí hardware, pomocí něhož lze získat neoprávněn přístup. *Počítačové heslo* je tvořeno řetězcem zanků, který umožňuje úplný nebo omezený přístup k počítačovému systému. *Přístupový kód* je založen na podobném principu jako heslo, rozdíl je v tom, že si jej uživatel obvykle nemůže vybrat volně, ale je mu přidělen (př. PIN). Blíže viz Viz Šámal, P. a kol. Trestní zákoník II. § 140 až 421. Komentář. 1. vydání. Praha: C. H. Beck, 2010, str. 2099 a násl.

[74] Novotný, O., Vanduchová, M., Šámal, P. a kol. *Trestní právo homotné. Obecná část.* 6. vydání, Praha: Wolters Kluwer ČR, a.s., 2010, str. 214.

3.3.1.3. Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232)

Tento trestný čin je nedbalostní alternativou k ustanovení § 230 trestního zákoníku, jehož podstatou je postih některých nedbalostních zásahů do dat či vybavení počítače. Zavinění je vázáno na hrubou nedbalost[75] a na následek ve formě způsobení značné škody. Objektivní stránka spočívá v porušení povinnosti pachatele, která vyplývá z jeho zaměstnání, povolání, postavení nebo funkce, popř. povinnosti mu uložené dle zákona nebo smluvně převzaté, přičemž dojde k manipulaci s daty uloženými v počítačovém systému, anebo je učiněn zásah do vybavení počítače nebo jiného technického zařízení pro zpracování dat. Odlišnost od ustanovení § 230 spočívá právě v porušení pachatelovy povinnosti uvedené výše a způsobení značné škody na cizím majetku.

3.3.1.4. Porušení tajemství dopravovaných zpráv (§182)

Tento trestný čin lze podřadit pod pravé virtuální trestné činy a je řazen ve zvláštní části trestního zákoníku v Hlavě II. dílu 2 nazvaném Trestné činy proti právům na ochranu osobnosti, soukromí a listovního tajemství. Důvodem je objekt, který je tímto ustanovením chráněn, tj. tajemství dopravovaných zpráv.

Trestný čin má dvě samostatné základní skutkové podstaty, jejichž součástí je i mimo jiné ochrana ,,virtuálního prostředí“[76]. V odstavci 1 je ochrana poskytována proti úmyslnému porušení tajemství posílané zprávy prostřednictvím sítě elektronických komunikací[77] nebo neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková počítačová data. Nejvyšší soud ČR k tomuto konstatoval: *„…ochrana je dopravované zprávě poskytována v době jejího „podávání“, tj. v průběhu doručování. Jedná se o proces, jehož počátek je možno ohraničit odesláním zprávy*

[75] Hrubá nedbalost je upravena v ustanovení § 16 odst. 2 trestního zákoníku: „Trestný čin je spáchán z hrubé nedbalosti, jestliže přístup pachatele k požadavku náležité opatrnosti svědčí o zřejmé bezohlednosti pachatele k zájmům chráněným trestním zákonem.“

[76] Ustanovení je mimo jiné též zaměřeno i na ochranu listovního tajemství, které je z důvodu zaměření práce ponecháno stranou.

[77] Např. e-mailová zpráva, přenos prostřednictvím Internetu (Skype, ICQ, Facebook aj.).

z počítače odesílatele (nebo z jiného počítače, se kterým právě odesílatel pracuje) a konec procesu je pak nutno vnímat v okamžiku doručení zprávy do emailové schránky příjemce, čímž je proces dopravy zprávy ukončen. Takto časově vymezený proces přepravy trvá zpravidla řádově zlomky vteřiny a je tedy téměř vyloučeno v jeho průběhu zprávu zachytit, přečíst a její tajemství tak porušit. Zpráva prochází během své dopravy zpravidla komunikačními uzly, ve kterých její text navíc zůstává zachován, a lze si proto představit možnost jeho automatického zkopírování pomocí zvláštního programu a odeslání např. do emailové schránky pachatele, tzn. že pachatel zachytil zprávu v průběhu jejího podávání…"[78]. V takovém případě by došlo k naplnění skutkové podstaty trestného činu porušování tajemství dopravovaných zpráv.

Porušením tajemství se rozumí jakékoli neoprávněné narušení posílané zprávy nebo neveřejného přenosu počítačových dat se snahou zjistit jejich obsah, přičemž není relevantní, zda byl tento obsah sdělen někomu dalšímu či nikoliv. Dojde-li k přečtení zprávy až po jejím doručení, není možné, aby byla naplněna skutková podstata trestného činu porušování tajemství dopravovaných zpráv, neboť řádně doručená elektronická zpráva, tj. bez neoprávněného narušení doručování, je již zcela v dispozici jejího příjemce, který se s ní může seznámit, aniž by vstoupil do e-mailové schránky, například prostřednictvím upozorňující zprávy na mobilním telefonu, která může obsahovat text zprávy elektronické[79]. Takovéto jednání však může být v návaznosti na konkrétní okolnosti případu posuzováno jako trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací.

V odstavci 2 je kriminalizováno jednání spočívající v prozrazení či využití tajemství, o němž se pachatel dozvěděl z telefonního hovoru nebo z přenosu prostřednictvím sítě elektronických komunikací, který byl určen jiné osobě. Prozrazením tajemství se rozumí sdělení obsahu zprávy jiné osobě než adresátovi. Tajemství pak využije ten, kdo jakýmkoliv způsobem uplatní jeho znalost a přitom

[78] Usnesení Nejvyššího soudu České republiky ze dne 21. 5. 2009 sp. zn. 11 Tdo 349/2009, ASPI - Nejvyšší soud ČR řešil otázku, zda přeposlání e-mailové zprávy ze schránky poškozeného, do níž pachatel vnikl bez jeho souhlasu a poslal další osobě, naplňuje skutkovou podstatu tohoto trestného činu.
[79] Usnesení Nejvyššího soudu České republiky ze dne 21. 5. 2009 sp. zn. 11 Tdo 349/2009, ASPI.

je veden záměrem způsobení škody jinému či opatřením neoprávněného prospěchu pro sebe nebo jiného[80].

Jedná se o úmyslný trestný čin, jehož pachatelem může být kdokoliv. Zvláštní skutková podstata uvedená v odstavci 5 však vyžaduje, aby pachatel byl zaměstnancem provozovatele telekomunikační služby nebo počítačového systému anebo osoby vykonávající komunikační činnost.

3.3.2. Vybrané nepravé virtuální trestné činy

Nepravé virtuální trestné činy jsou od virtuálních trestných činů pravých odlišné v mnoha směrech. Jejich vytvořením nebyl sledován účel ochrany virtuálního prostředí a v něm vznikajících vztahů, ale jedná se o ustanovení „tradičních" trestných činů, jež zákonodárce zavedl pro ochranu před jednáními, která se odehrávají v reálném světě. Tato rozdílnost, která spočívá v tom, že „tradiční" trestné činy nejsou přizpůsobeny virtuálnímu prostředí, neboť s tím zákonodárce v době jejich tvorby nepočítal, s sebou přináší řadu výkladových problémů. V teorii a praxi pak dochází k situacím, kdy zažité pojmosloví a jeho význam musí dostát změn a přizpůsobovat se současnému trendu[81].

3.3.2.1. Virtuální krádež

Virtuální krádež se vztahuje k trestnému činu krádeže, jenž je upraven v trestním zákoníku v Hlavě V. nazvané Trestné činy proti majetku, konkrétně v ustanovení § 205[82].

[80] Šámal, P. a kol. Trestní zákoník II. § 140 až 421. Komentář. 1. vydání. Praha: C. H. Beck, 2010, str. 1623 a násl.
[81] Veškeré tradiční trestné činy lze považovat za nepravé virtuální trestné činy, pokud to jejich povaha připouští. Z tohoto důvodu a z důvodu rozsahu diplomové práce byly dále vybrány trestné činy vztahující se k případovým studiím, které jsou součástí této práce.
[82] V rámci dalšího výkladu čerpáno z: Šámal, P. a kol. Trestní zákoník II. § 140 až 421. Komentář. 1. vydání. Praha: C. H. Beck, 2010, str. 1786 a násl.

3.3.2.1.1. Obecné vymezení trestného činu krádeže

Objektem tohoto trestného činu je vlastnictví věci, její držba, popř. faktické držení. Objektivní stránka je rozložena do dvou samostatných základních skutkových podstat, přičemž obě vychází ze základní definice krádeže, za kterou se považuje jednání pachatele spočívající v tom, že si přisvojí cizí věc, tím, že se jí zmocní, a doplňuje ji některým dalším alternativním znakem.

Po subjektivní stránce se vyžaduje úmysl, který musí zahrnovat všechny znaky objektivní stránky včetně přisvojení, nikoliv však jen na přechodnou dobu. Na druhé straně pachatel nemusí mít úmysl věc trvale užívat, ale o krádež jde v případech, kdy si věc přisvojí, tj. trvale vyloučí možnost dispozice oprávněné osoby s věcí.

Pachatelem může být kdokoliv[83].

Jedním ze základních pojmů trestného činu krádeže je cizí věc, která je předmětem útoku. V právním prostředí České republiky nemá věc v právním smyslu legální definici a její vymezení bylo ponecháno teorii a praxi[84].

Věc je předmětem právních vztahů, a to spolu s právy a povinnostmi, pokud to jejich povaha připouští, ale i jinými majetkovými hodnotami a nehmotnými statky. Obecnými znaky vymezujícími věc v právním smyslu jsou její ovladatelnost a použitelnost pro potřeby lidí, tj. užitečnost, kdy obě tyto vlastnosti se vždy posuzují objektivně. Nejasnost, zda se jedná o věc v právním smyslu či nikoliv, je vždy nutné posuzovat konkrétně se zřetelem na okolnosti a povahu jednotlivého případu[85]. Vedle těchto dvou základních znaků se věcmi v právním smyslu obecně rozumí věci odlišné od osoby, obchodovatelné, způsobilé k přivlastnění a způsobilé být objektem práv. Za věc v právním smyslu se dále považuje i ovladatelná přírodní síla (energie vodní, parní, sluneční, elektrická, jaderná), která slouží potřebám lidí, tj. má užitnou hodnotu.

Dle současné teorie se cizí věcí v případě krádeže rozumí jen movitá věc, jež nenáleží pachateli buď vůbec, nebo nenáleží jen jemu, a kterou pachatel nemá ve své

[83] V návaznosti na výklad v kapitole „Jednotlivé znaky virtuálních trestných činů - subjekt“.
[84] Legální definice věci má být obsažena v novém návrhu občanského zákoníku: „Věcí se rozumí vše, co není osobou a slouží potřebě lidí.“ Návrh nového občanského zákoníku dostupný na: http://obcanskyzakonik.justice.cz/cz/uvodni-stranka.html.
[85] Švestka, J., Spáčil, J., Škárová, M., Hulmák, M. a kol. Občanský zákoník I, II, 2. vydání, Praha 2009, str. 637.

dispozici. Ustanovení o věcech se vztahují i na živá zvířata, peněžní prostředky na účtu a na cenné papíry, nevyplývá-li z jednotlivých ustanovení trestního zákoníku něco jiného. Naopak z povahy věci vyplývá, že předmětem krádeže nemůže být nemovitá věc.

Přisvojením si cizí věci se rozumí získání možnosti trvalé dispozice s cizí věcí, nikoliv však získání takové věci do vlastnictví, neboť trestným činem nelze nabýt vlastnické právo. Přisvojení zároveň znamená vyloučení dosavadního vlastníka nebo faktického držitele z držení, užívání a nakládání s věcí. Pachatel získává možnost trvalé dispozice s cizí věcí, přičemž není rozhodné, jak poté s věcí skutečně nakládá. K přisvojení si cizí věcí dochází tím, že se jí pachatel zmocní, tzn. že věc odejme z dispozice vlastníka, oprávněného nebo faktického držitele, přičemž si tak zjedná možnost s věcí trvale nakládat podle své vůle sám či takovou možnost zjedná i dalším osobám.

3.3.2.1.2. Předmět virtuální krádeže

Obecně platná teorie ohledně cizí věci a věci v právním smyslu se bude v převážné míře vztahovat i na virtuální krádež, avšak lze najít některé odlišnosti, které vyvolávají řadu otázek. Co je předmětem virtuální krádeže a lze tento předmět podřadit pod definici cizí věci?

Veškeré věci nacházející se v kyberprostoru nazýváme virtuálními předměty. Nejtypičtější oblastí, kde se s nimi můžeme setkat, budou virtuální světy a hry.

Virtuální předměty jsou nereálnými, nehmatatelnými a imateriálními věcmi. Z hlediska definice věci v právním smyslu nemůžeme virtuální předměty zařadit ani mezi věci (hmotné a nehmotné), ani práva či povinnosti. Vzhledem k jejich charakteristickým rysům je lze však subsumovat buď pod jiné majetkové hodnoty, nebo pod nehmotné statky.

Virtuální předměty jsou převážně považovány za nehmotné statky, tj. statky, které nejsou demonstrovány v určité hmotné podobě, ale obvykle jsou vyjádřeny

objektivně seznatelnou formou, tj. na displeji počítače, v dokumentaci apod.[86] Nehmotné statky, tzn. i virtuální předměty, mohou být též jinými majetkovými hodnotami, pokud to jejich povaha připouští. Majetkovou hodnotu lze spatřovat zejména v případech, kdy je možné virtuální předměty určitým způsobem ocenit (např. hodnota v rámci online hry) a tuto hodnotu vyjádřit v penězích, resp. virtuální měně. V případě, že virtuální měna je směnitelná za skutečné peníze, můžeme mluvit o majetkové hodnotě reálné.

Určitou podobnost virtuálních předmětů můžeme spatřovat též v cenných papírech, zejména v zaknihované podobě, kdy podstatou je inkorporace určitého práva do cenného papíru, který fyzicky neexistuje, ale je evidován jako položka ve Středisku cenných papírů. Dispozice se zaknihovaným cenným papírem má dle teorie formu dispozice s movitou věcí (tradice, prodej, zástava aj.)[87]. U virtuálních předmětů pak můžeme spatřovat podobnost v inkorporaci práva vlastnického, resp. práva držby, a dále taky v jejich nereálné formě.

Podobnost existuje i u peněz jako zákonných platidel. Peníze jsou movité věci, a to i v případě, že se nachází na bankovním účtu, tzn. že nemají hmatatelnou podobu. Vlastníky těchto peněz není banka, ale majitel příslušného bankovního účtu.

3.3.2.1.3. Virtuální vlastnictví

Virtuální předměty jsou součástí příslušné online hry, tvoří s ní specifický celek, kdy mimo něj by zcela ztrácely svůj význam. Lze je považovat za produkt, který je výsledkem určitého ztvárnění vnitřní duševní činnosti, stejně jako celá hra, která je považována za autorské dílo. Virtuální předmět se pak konkrétně nachází na uživatelském účtu. Další otázka, která vyvstává je, kdo je vlastníkem předmětů, vlastník internetové hry či majitel účtu?

Virtuální věci mají pro hráče často stejnou hodnotu jako věci skutečné. Hodnota těchto věcí je pak určována nejen jejich množstvím a herní hodnotou, od níž se následně odvozuje postavení hráče ve hře, ale i podle toho, o jakou internetovou hru (herní

[86] Švestka, J., Spáčil, J., Škárová, M., Hulmák, M. a kol. Občanský zákoník I. § 1 až 459. Komentář. 2. vydání. Praha : C. H. Beck, 2009, 1394 s.
[87] Tamtéž, str. 639.

pravidla) se jedná, může být hodnota virtuálních věcí vyjádřena i prostřednictvím skutečných peněz.

Virtuální věc je plně v dispozici online hráče. V případě, že se hráč nachází v režimu offline, tj. není v dané chvíli připojen, jsou virtuální předměty i nadále na jeho uživatelském účtu, který je spravován vlastníkem hry. Po přihlášení se na uživatelský účet může hráč s věcmi libovolně nakládat, tzn. že je může směnit, darovat, prodat jinému hráči nebo s nimi činit jiné úkony, které jsou v souladu s herními pravidly příslušné hry.

Dříve než je povoleno hráči založit jeho uživatelský účet, musí akceptovat pravidla internetové hry, které jsou dostupné, resp. měly by být dostupné přímo na příslušném serveru (webové stránce). Každá hra má vlastní pravidla. Lze se setkat s pravidly, která stanovují, že veškerá práva duševního vlastnictví náleží vlastníku hry, nikoliv samotnému uživateli, na druhé straně se lze setkat s pravidly, která stanovují, že veškerý obsah účtu náleží jeho uživateli, který za něj rovněž odpovídá. Z trestněprávního hlediska je však tato otázka zcela nepodstatná, neboť ať už je vlastníkem kdokoliv, bude pachatel odcizovat cizí věc, s výjimkou případů, kdy by byl vlastníkem virtuální věci právě on. V rámci internetové hry však nelze vyloučit, že bude povoleno věc odcizit jinému hráči, resp. jeho virtuální postavě. Taková „krádež“ by v daném případě trestná nebyla, neboť každý hráč musí souhlasit před započetím online hry s jejími pravidly, s nimiž má povinnost se seznámit.

Jednotliví hráči jsou si plně vědomi skýtajících výhod, které příslušná hra nabízí. Běžně se na internetu setkáváme s nabídkami na odkup virtuálních předmětů, virtuální měny a jiných produktů internetové hry, se kterými je možné obchodovat. Jedná se o tzv. real-world trading[88], který některé internetové hry povolují, některé ho zakazují[89]. Někteří vlastníci her ve svých podmínkách a pravidlech uvádí, že veškerá práva duševního vlastnictví nebo jiných práv týkající se herní postavy, účtu a herních položek

[88] Tento pojem lze volně přeložit jako obchodování ve skutečném světě. Patří zde zejména obchodování s jednotlivými položkami (například virtuální zlato), koupě uživatelského účtu s dosaženým alter egem herní postavy aj.

[89] Pravidla hry RuneScape dovolují provést výměnu herních položek za jiné předměty/služby, které hra nabízí. Není však možné provést jejich výměnu za výhody v jiných online hrách, za reálné peníze či jiné výhody reálného světa.

jsou a také vždy zůstanou jejich vlastnictvím. Uživatelé účtu získávají od vlastníka oprávnění s těmito věcmi disponovat, ale jen v rámci předem stanovených pravidel.

Nelze tedy učinit jednoznačný závěr, že vlastníkem všech práv a věcí souvisejících s internetovou hrou z právního hlediska zůstává její majitel a hráč získává pouze oprávnění s tímto majetkem disponovat, ale rozhodující bude úprava duševního vlastnictví v rámci pravidel (podmínek použití) příslušné hry. Právní ochrana však bude poskytována vždy, a to nejen vlastníkům internetové hry, ale také jejím hráčům. Jedná se o vztah podobný vlastnickému právu a právu držby, kdy vlastník i držitel požívají příslušné právní ochrany. Vlastník hry navíc bude chráněn i pro situace, že se hráč dopustí v tomto směru porušení pravidel, kdy v případě, že je i majitelem práv duševního vlastnictví, získá právo na náhradu škody, vrácení bezdůvodného obohacení a není vyloučena ani trestní odpovědnost.

Odebrání virtuálních předmětů z uživatelského účtu hráče bez jeho souhlasu (ať již dle pravidel hry je nebo není jejich vlastníkem) znamená, že se dostávají z dosahu jeho moci do sféry osoby jiné, která získává možnost dispozice. Tímto jednáním osoba naplňuje znak zmocnění se cizí věci v rámci virtuálního prostředí, přičemž tak nečiní vlastní rukou, ale prostřednictvím nástroje v technickém (informačním) slova smyslu.

Na základě všech výše uvedených skutečností vyplývá závěr, že současná česká právní úprava trestného činu krádeže umožňuje trestně stíhat i tzv. virtuální krádež. Virtuální předměty nacházející se v kyberprostoru lze subsumovat pod definici věci v právním smyslu, a to jako nehmotné statky, popř. jiné majetkové hodnoty, a tudíž mohou být předmětem virtuálního trestného činu krádeže, pokud se nebude jednat o věc náležející do vlastnictví pachatele.

3.3.2.1.4. Virtuální postava jako osoba blízká nebo věc?

Praktickou otázkou, která může vyvstat ve virtuální právní oblasti, je, zda virtuální postava (avatar) je považována za věc v právním smyslu, anebo na ni lze pohlížet jako na osobu blízkou?

Osoba blízká je definována v ustanovení § 125 trestního zákoníku jako příbuzný v pokolení přímém, osvojitel, osvojenec, sourozenec, manžel a partner, jiné osoby v poměru rodinném nebo obdobném se pokládají za osoby sobě navzájem blízké jen tehdy, kdyby újmu, kterou utrpěla jedna z nich, druhá důvodně pociťovala jako újmu vlastní. Toto vymezení je obsahově shodné s vymezením osoby blízké v ustanovení § 116 občanského zákoníku.

Pojem osoby v právním smyslu je v teorii i praxi ustálen, přičemž rozlišujeme osoby fyzické a právnické. Pokud se jedná o pojem osoby blízké, objevil se v posledních letech trend, že právnickou osobu lze považovat za osobu blízkou[90].

Pro právnickou osobu je charakteristické, že svou vůli nevytváří sama o sobě, ale jen prostřednictvím fyzických osob, které jsou k tomu dle práva povolány. Je nepochybné, že mezi právnickou osobou a fyzickou osobou vznikají vztahy, přičemž musí jít o vztahy určité kvality, tj. nejen vztahy právní, ale i ekonomické. Za anologického použití § 116 občanského zákoníku bylo v současné praxi dovozeno, že za osobu blízkou může být považována i právnická osoba, a to v případě, že fyzická osoba, která je jejím společníkem by důvodně pociťovala újmu, kterou právnická osoba utrpěla, jako újmu vlastní[91]. Je v této souvislosti možné, aby byl avatar považován za osobu blízkou?

Virtuální postava má mnohé shodné znaky s právnickou osobou. V obou případech se jedná o osoby, které jsou dílem fikce, tzn. že nemají reálný hmatatelný základ, jsou „řízeny“ fyzickou osobou a k oběma si lze vytvořit určité vztahy (právní, ekonomické, emocionální). Na základě těchto vztahů by bylo možné dovodit, že hráč ovládající avatara by mohl pociťovat újmu, která mu vznikla, jako újmu vlastní. V tomto případě, by bylo na virtuální postavu pohlíženo jako na osobu blízkou. Na druhé straně však lze spatřovat i významná negativa. Předně by muselo dojít k rozšíření pojmu osoby v právním smyslu, což by znamenalo, že by na virtuální postavu bylo nazíráno jako například na právnickou osobu, a měla by tudíž požívat podobných práv a povinností. Přestože mají právnická osoba a virtuální postava společné rysy, není možné avatara považovat za osobu v právním smyslu, a tudíž ani

[90] Např. Usnesení Nejvyššího soudu ČR ze dne 20.11.2008 sp.zn. 32 Cdo 3852/2007, ASPI; Usnesení Nejvyššího soudu ČR ze dne 1.8.2001 sp.zn. 21 Cdo 2192/2001, ASPI.
[91] Čech, P., Pavela, L. Obchodní společnost jako osoba blízká? Právní rádce, 2007, č. 1, s. 27 a násl.

za osobu blízkou, neboť veškeré úkony, které činí, nezpůsobují v reálném světě právní následky či jiné právní účinky, jako je tomu u osob právnických či fyzických.

Virtuální postava tvoří jednu z herních položek náležejících k uživatelskému účtu hráče, a proto se na něj uplatní výklad týkající se virtuálních věcí jako věcí v právním smyslu. Vztah hráče k této věci může být nejen hodnotový (hodnota avatara v rámci dosažení určité úrovně), ale lze si představit i vztah emocionální, který ovšem nezakládá možnost považovat jej za osobu blízkou.

3.3.2.1.5. Virtuální krádež vloupáním?

Zajímavá otázka vzniká u jednoho z alternativních znaků, který se vyžaduje pro naplnění objektivní stránky krádeže, a to vloupání. Vloupání je blíže vymezeno v ustanovení § 121 trestního zákoníku, kdy se jím rozumí vniknutí do uzavřeného prostoru lstí, nedovoleným překonáním uzamčení nebo překonání jiné jistící překážky s použitím síly.

Uzavřeným prostorem se rozumí prostor, který může být uzavřen například v domě, bytě, skladu apod., oplocený či jinak uzavřený prostor, anebo jím může být i menší prostor, který je možné přemisťovat. Uzavření se vykládá jako ochrana věci proti odcizení, přičemž nejčastějšími způsoby je uzamčení pomocí zámku, oplocení nebo zajištění automatickým elektronickým zařízením. Za vniknutí se pak považuje vstup do takto uzavřeného prostoru, otevření nebo jiné narušení, a sáhnutí do něj, třeba i za pomoci potřebného nástroje, přičemž věc, která je předmětem útoku, se musí v tomto prostoru nacházet[92].

Smysl předmětného výkladového ustanovení vztahujícího se k vloupání je především vázán na fyzický akt. Přesto však lze zvážit možnost rozšiřujícího výkladu i na kyberprostor, přičemž musíme přihlédnout k tomu, že v době vzniku významu tohoto ustanovení zákonodárce nepočítal s problematikou virtuálního prostředí.

Vezměme si však konkrétní případ odebrání virtuálních věcí z uživatelského účtu. Uživatelský účet v rámci online hry můžeme považovat za uzavřený prostor ve smyslu výše uvedené definice. Přestože u něj nemůžeme určit pevně hmatatelné hranice, z technického hlediska kyberprostoru se jedná o jeho přesně vymezenou část,

[92] Šámal, P. a kol. Trestní zákoník I. § 1 až 139. Komentář. 1. vydání. Praha: C. H. Beck, 2010, str. 1167.

do níž mají přístup jen oprávněné osoby (majitel účtu, popř. vlastník hry). Jedná se o prostor imaginární, do něhož může být „vstoupeno – sáhnuto“ jen prostřednictvím nástroje v informačním (technickém) slova smyslu. Prostor uživatelského účtu online hry je pak zajištěn bezpečnostním opatřením ve formě hesla, resp. přihlašovacích údajů. Můžeme tedy mluvit o uzavřeném prostoru.

V rámci virtuálního prostředí připadá v úvahu vloupání jen prostřednictví lsti nebo nedovoleného překonání uzamčení. Na situaci nedovoleného překonání uzamčení ve formě bezpečnostního opatření bychom spíše mohli pohlížet jako na trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací (§ 230 trestního zákoníku). Pokud by však byl mimo jiné naplněn ještě některý další alternativní znak krádeže, bylo by možné mluvit o souběhu těchto trestných činů (§ 205 a 230 trestního zákoníku).

V případě vloupání lstí teorie považuje za lest vyvolání omylu u cizí osoby nebo využití omylu této osoby s úmyslem dosáhnout nějakého cíle, např. vlastního obohacení[93]. Výkladové ustanovení § 120 trestního zákoníku uvádí, že uvést někoho v omyl či využít něčího omylu lze i provedením zásahu do počítačových informací nebo dat, zásahu do programového vybavení počítače nebo provedením jiné operace na počítači, zásahu do elektronického nebo jiného technického zařízení, včetně zásahu do předmětů sloužících k ovládání takového zařízení, anebo využitím takové operace či takového zásahu provedeného jiným. Z uvedených možností pro spáchání krádeže vloupáním z hlediska virtuálního prostředí připadá v úvahu provedení zásahu do počítačových informací nebo dat, neboť virtuální předměty jako imateriální věci jsou v rámci kyberprostoru zaznamenány právě ve formě informací či dat. Data v obecné podobě představují interpretovatelnou a formalizovanou reprezentaci informace vhodnou pro komunikaci, interpretaci nebo zpracování. Informací se pak rozumí poznatek týkající se jakýchkoli objektů, jakou jsou fakta, události, věci, procesy nebo myšlenky. Nositelem informací je signál, který umožňuje získání, přenos, uchování v paměti a další zpracování informací, přičemž informační tok je realizován sledem kódových znaků[94].

[93] Šámal, P. a kol. Trestní zákoník I. § 1 až 139. Komentář. 1. vydání. Praha: C. H. Beck, 2010, str. 1167.
[94] Tamtéž, str. 1165.

Ve světle zmíněných pojmů a úvah je možné připustit výklad, že krádež virtuálních předmětů může být spáchána vloupáním, neboť uživatelský účet vytvořený v online hře, tj. ve virtuálním prostředí, je uzavřeným prostorem, do něhož lze vniknout lstí, a tudíž jsou naplněny definiční znaky pojmu vloupání.

3.3.2.2. Virtuální loupež

Virtuální loupež se vztahuje k trestnému činu loupeže, jenž je upraven v trestním zákoníku v Hlavě II. Dílu 2 nazvaném Trestné činy proti svobodě, konkrétně v ustanovení § 173[95].

3.3.2.2.1. Obecné vymezení loupeže

Tento trestný čin má některé společné výkladové pojmy s trestným činem krádeže. Objektem tohoto trestného činu je ochrana osobní svobody ve smyslu svobody rozhodování a zájem na ochraně majetku. Objektivní stránka spočívá v použití násilí nebo pohrůžky bezprostředního násilí v úmyslu zmocnit se cizí věci.

Pojem násilí není přímo v zákoně definován. Z hlediska praxe a v souladu s judikaturou se za násilí považuje fyzický útok na určitou osobu nebo věc. Může jím být jednání, které zcela vylučuje jiné než žádané chování, anebo kterým pachatel působí psychicky na jednání donucované osoby, takže ta se podrobuje nátlaku. Násilí zpravidla směřuje proti tomu, kdo má věc u sebe, lze je však spáchat i proti jiné osobě nebo věci, pokud je prostředkem nátlaku na vůli poškozeného.

Pohrůžka násilím spočívá v psychickém působení na vůli jiného, pohrůžka bezprostředního násilí pak znamená hrozbu násilím, které má být vykonáno ihned, např. násilím proti životu, zdraví nebo majetku, čímž je omezena volnost vlastního rozhodování. Hrozba bezprostředního násilí rovněž může směřovat i proti životu, zdraví nebo majetku jiné osoby než napadeného[96].

[95] Viz Příloha č. 2.
[96] Jelínek, J a kol. Trestní právo hmotné. 3.přepracované a aktualizované vydání, Linde Praha, Praha 2008, str. 677 a násl.

Zmocněním se rozumí, že pachatel si zjedná možnost s takovou věcí nakládat s vyloučením toho, kdo ji měl dosud ve své moci, tj. jedná se o převedení faktické moci nad ní z oprávněné osoby na pachatele, přičemž napadený nemusí být vlastníkem věci a není rozhodná ani cena věci[97].

3.3.2.2.2. Virtuální loupež

V případě virtuální loupeže lze vycházet z výkladu uvedeného výše, tj. že virtuální předměty nacházející se v kyberprostoru lze subsumovat pod definici věci v právním smyslu. Lze se však dopustit násilí nebo pohrůžky bezprostředního násilí ve virtuálním prostředí?

Reálně si lze představit situaci, kdy pachatel použije násilí vůči konkrétní skutečné fyzické osobě, aby z ní vymámil například přístup do aplikace internetového bankovnictví. Naproti tomu si představme následující situaci. Pachatel bude sedět v jedné místnosti s poškozeným, oba budou připojeni k internetové hře, v níž bude svádět souboj s avaterem poškozeného[98]. Jelikož poškozený tráví celé dny hraním předmětné internetové hry, ztotožnil se svým avatarem natolik, že si k němu vytvořil emocionální vztah. Vedle toho se jedná o avatara vyšší úrovně (levelu), který má v rámci internetové hry velkou hodnotu, jíž lze rovněž finančně vyčíslit, neboť hra povoluje obchodování s herními položkami a její virtuální měna je směnitelná za skutečné peníze. Pachatel bude mít úmysl získat informaci, kde se v místnosti nachází finanční hotovost, a za tímto účelem oznámí poškozenému, že pokud mu informaci nesdělí, tak jeho avatara v souboji zabije. Aby této situaci poškozený zabránil, sdělí pachateli, kde se finanční hotovost nachází.

Jednání pachatele naplňuje skutkovou podstatu trestného činu loupeže, neboť došlo ke zmocnění se cizí věci na základě pohrůžky bezprostředního násilí proti majetku poškozeného. Bude však takovéto jednání skutečně trestné?

Ke zmocnění se cizí věci došlo tím, že si pachatel zjednal možnost nakládat s finanční hotovostí, čímž vyloučil z dispozice toho, kdo ji měl oprávněně po celou

[97] Šámal, P. a kol. Trestní zákoník II. § 140 až 421. Komentář. 1. vydání. Praha: C. H. Beck, 2010, str. 1553.
[98] Předpokladem je vytvoření kriminální situace k naplnění skutkové podstaty trestného činu loupeže (tj. v místnosti se nachází dva počítače, z něhož jsou připojeni k internetové hře apod.).

dobu u sebe. Za tímto účelem bylo použito pohrůžky bezprostředního násilí ve formě psychického nátlaku na vůli poškozeného, která směřovala vůči jeho věci, tj. majetku. Tímto majetkem byl avatar, ke kterému si poškozený jednak vytvořil emocionální vztah, jednak se jednalo v rámci internetové hry o hodnotného avatara. Jelikož hra umožňuje směnu virtuální měny za měnu skutečnou, dochází zde nepochybně k zásahu do majetkové sféry ve skutečném světě, neboť avatar je virtuální věcí. Informační technologie byla prostředkem (nástrojem) použitým k dosažení cíle pachatele.

Z formálního hlediska došlo k naplnění všech obligatorních znaků skutkové podstaty trestného činu loupeže. Do popředí se však dostává otázka společenské škodlivosti tohoto jednání. Společenská škodlivost je poměřována podle hodnot, které daná společnost uznává a shledává zájem na jejich ochraně. Ve smyšleném případě by společenská škodlivost byla obsažena, a to vzhledem k úmyslu pachatele získat finanční hotovost prostřednictvím využití jeho vědomosti o vztahu poškozeného k avatarovi a jeho majetkové hodnotě.

3.3.2.3. Virtuální dětská pornografie

Virtuální dětská pornografie je oproti výše uvedené virtuální krádeži a loupeži virtuálním trestným činem, jenž má relativně dobrý základ právní regulace. Dětská pornografie je na celém světě (i když v různé míře) chápána jako negativní společenský jev, jenž zasahuje jedny z nejcitlivějších a nejbezbrannějších osob vůbec. Jedná se zároveň i o jeden z mála trestných činů, kterému je věnována velká pozornost na mezinárodní právní úrovni. Jednotlivé státy si začínají uvědomovat jeho následky v rámci virtuálního prostředí a snaží se je regulovat.

3.3.2.3.1. Klasifikace

Základem pro tuto práci je dělení dětské pornografie na skutečnou, tj. takovou, která zobrazuje skutečné dítě (dítě z masa a kostí), a virtuální, tj. takovou, která nezobrazuje žádné skutečné dítě, ale jedná se o díla, jejichž ústředním motivem je zobrazení

nereálného dítěte (jedná se např. o literární, kreslené a animované postavy, kyborgy[99], androidy[100] aj.).

Na virtuální dětskou pornografii lze pohlížet ze dvou směrů:

a/ v širším slova smyslu – do této kategorie lze zařadit jednak virtuální dětskou pornografii vytvořenou v rámci kyberprostoru, a jednak zde můžeme zařadit dětskou pornografii všeobecně, které je dále v rámci kyberprostoru (zejména Internetu) rozšiřována,

b/ v užším slova smyslu – zde patří pouze čistě virtuální dětská pornografie vytvořená v rámci kyberprostoru

Obsahem dalšího výkladu je jen virtuální dětská pornografie v užším slova smyslu, tj. na dětská pornografie bez zneužití skutečných dětí, a vytvořená v rámci kyberprostoru, zejména se zaměřením na animace.

Další členění virtuální dětské pornografie, resp. její podoby, může být dělena na:

1/ dětskou pornografii vytvořenou v rámci kyberprostoru (např. animace, fotografie nezobrazující skutečné dítě vytvořené pomocí počítačového programu – fotomontáž, vytvoření filmových postav jako tzv. kyborgů nebo androidů)

2/ chápání jejího vytvoření jako fikce, tj. i zde nevystupuje skutečné dítě, avšak jedná se o vytvoření mimo kyberprostor (např. literární díla, sochy)

Základem virtuální dětské pornografie tedy je, že zde nedochází ke zneužívání či jinému využití skutečného dítěte. Pro bližší pochopení virtuální dětské pornografie je podstatné vymezit její základní pojmy.

[99] Původně živé-přírodní tělo obohacené o mechanické či elektronické, jejichž montáž, popř. demontáž se provádí pomocí chirurgického zákroku. Podstatou je zde představa techniky parazitující na živém těle. Definice dostupná z: http://cs.wikipedia.org/wiki/Kyborg.

[100] Umělá, mechanická napodobenina člověka. Akademický slovník cizích slov, I. díl A-K. Academia Praha 1995, s. 51.

3.3.2.3.2. Pornografie, pornografické dílo, dítě

Pornografii z pohledu trestního práva můžeme chápat jen jako negativní společenský jev, jinak by v tomto oboru nebyla upravena. Obecně můžeme pornografii rozdělit do 3 kategorií (dle obsahu pornografického díla)[101] na tzv.:

a/ *pornografii tvrdou*, do které spadají pornografická díla, v nichž se projevuje násilí či neúcta k člověku nebo která znázorňují pohlavní styk se zvířetem,

b/ *pornografii dětskou*, kde řadíme taková pornografická díla, které zobrazují, popř. jinak využívají dítě,

c/ *pornografii prostou*, kterou tvoří ostatní pornografická díla.

V současné době trestní zákoník, ani žádný jiný právní předpis nedefinuje, co se pornografickým dílem rozumí. Vymezení definice, resp. její vyjádření, je ponecháno trestněprávní teorii a judikatuře.

„Dílo“ je obecně definováno v ustanovení § 2 autorského zákona[102], tj. je zde vymezeno dílo autorské jako předmět autorského práva. Předmětné ustanovení obsahuje demonstrativní výčet děl, která jsou pod autorskou ochranou, přičemž jsou rozdělena do jednotlivých kategorií (díla literární, jiná umělecká a díla vědecká). Dle autorského zákona mohou požívat autorskoprávní ochrany i díla pornografická, avšak z hlediska trestního práva se výrazem „dílo“ nemyslí dílo autorské. Reprobace takovýchto společensky nevhodných či nepřípustných jevů je povahy veřejnoprávní, která nemá autorskoprávní (soukromoprávní) obsah, tzn. že se nejedná o žádný druh děl ve smyslu autorského práva.[103] Podmínkou, aby pornografické dílo bylo považováno za dílo umělecké, tj. autorské, je nutné, aby mělo alespoň minimální tvůrčí charakter. Pokud tento tvůrčí prvek chybí, není možno mluvit o díle ve smyslu autorském.[104]

V teorii a praxi se za pornografické dílo považuje „*dílo, které zvláště intenzivním a vtíravým způsobem zasahuje a podněcuje sexuální pud, přičemž současně překračuje uznávané morální normy příslušné společnosti, čímž u většiny jejich členů vzbuzuje*

[101] Šámal, P. a kol. Trestní zákoník II. § 140 až 421. Komentář. 1. vydání. Praha: C. H. Beck, 2010, str. 1695.
[102] Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.
[103] Telec, I. Tůma, P. Autorský zákon. Komentář. 1.vydání. Praha: C. H. Beck, 2007, str. 25.
[104] Usnesení Nejvyššího soudu České republiky ze dne 18. 6. 2003, sp. zn. 5 Tdo 631/2003, ASPI.

stud.“[105] Ústavní soud v této otázce judikoval, že pro účely trestního zákona je pornografickým dílem jakákoliv věc, pokud uráží, způsobem, který lze stěží akceptovat, cit pro sexuální slušnost. Pornografické dílo může u normální osoby vyvolávat sexuální vzrušení, vedle toho však může tuto osobu sexuálně znechucovat či odpuzovat.[106]

Pornografické dílo je rovněž vyjádřeno jako „jakýkoli předmět, který, je-li pozorován ať přímo nebo prostřednictvím technického zařízení, zvláště intenzivním a vtíravým způsobem zasahuje a podněcuje samotný sexuální pud. Současně takové dílo hrubě porušuje uznávané morální normy společnosti a vyvolává pocit studu.“[107]

Podmínkou pornografického díla je, že takové dílo musí mít pornografický charakter, tzn. že musíme mluvit o pornografické povaze díla, neboť ne každé takové dílo je předmětem trestního postihu. Takovým příkladem jsou například historicky cenné předměty, předměty určené k vědeckým, vzdělávacím a osvětovým cílům, nebo umělecká díla, která i když zobrazují i ty nejintimnější chvíle člověka, nejsou považována za díla pornografická, a to i v případě, že mají pornografický charakter. Musí se naopak jednat o dílo, které bude hrubě porušovat morální hodnoty dané společnosti a na průměrného člověka bude dílo jako celek působit tak, že u něj vyvolá pocit studu, popř. takovou osobu bude znechucovat či odpuzovat, a celkově bude v rozporu s morálními hodnotami uznávanými v dané společnosti. Klíčovým momentem tedy bude určení, zda se jedná o dílo pornografické (bez pornografického díla nemůže být nikdo trestně stíhán pro trestné činy uvedené v příslušných ustanoveních trestního zákoníku) či nikoliv. Závěr o pornografickém charakteru díla musí být dovozován z celého obsahu díla, nikoli jen z určité části vytržené z kontextu (pasáže, kapitoly, úryvku, z jednotlivé fotografie vytažené z kolekce na sebe navazujících fotografií). Závěr o pornografickém charakteru díla naopak nelze dovozovat bez dalšího jen z toho, že je prezentováno za účelem uspokojení osob trpících sexuální deviací, pro které jsou sexuálně atraktivní nedospělé osoby, např. nelze

[105] Usnesení Nejvyššího soudu České republiky ze dne 28. 12. 2004 sp. zn. 7 Tdo 1077/2004-I, ASPI.
[106] Usnesení Ústavního soudu České republiky ze dne 19. 4. 2004, sp. zn. IV. ÚS 606/03, ASPI.
[107] Herczeg, J. Virtuální dětská pornografie: Zločin bez oběti? In Vanduhová, V., Gřivna, T. (eds.).: Pocta Otovi Novotnému k 80. narozeninám. ASPI, Wolters Kluwer, Praha 2008, s. 38.

paušálně hodnotit fotografické materiály jako pornografické jen z důvodu, že jsou na nich zachyceny děti a proto, že byly prezentovány na serveru určeném pedofilům.[108]

Posouzení charakteru díla musí být věnována pečlivá pozornost, neboť v předmětné věci může dojít ke kolizi s právem na svobodu projevu stanovenou v čl. 17 Listiny základních práv a svobod (čl. 10 Evropské úmluvy o ochraně lidských práv a základních svobod), která je jedním ze základů každé demokratické společnosti a znamená rovněž významný prostředek seberealizace jedince. V případě dětské pornografie je pak svoboda projevu úzce spjata s hodnotami, které příslušná společnost považuje za morální. Pokud tedy bude u díla shledán pornografický charakter (ve smyslu veřejnoprávním), bude stát mimo rámec ochrany svobody projevu. Test pornografické povahy díla spočívá na posouzení, zda jeho celkový dojem způsobuje morální pohoršení osobě s běžným cítěním.[109] Morální pohoršení by však mělo být intenzivnějšího významu, neboť například některá umělecká díla mohou svým obsahem být díly pornografickými, avšak ne stíhatelnými podle trestního práva. Abychom mohli mluvit o pornografickém díle z pohledu trestního práva, musí jít o dílo, které nemá vážnou uměleckou, politickou nebo vědeckou hodnotu. Pokud dílo bude mít seriózní uměleckou hodnotu, pak nemůže být předmětem dětské pornografie.[110]

Důležitý předpoklad, ze kterého bude nutné vycházet, představují morální hodnoty společnosti, tzv. obecné standardy morálky. Morální hodnoty se mohou v jednotlivých společnostech odlišovat. Jiné chápání (z pohledu dětské pornografie) se projevuje v Evropě a jiné v asijských zemích.[111] Jednotné pojetí morálních standardů nenalezneme ani v případech menšího geografického určení zaměřeného třeba jen na Evropu. Ústavní soud ČR však v této věci konstatoval, že svoboda projevu se vztahuje nejen na informace nebo ideje, které jsou vnímány příznivě či neutrálně, ale také na ty, které uráží, pohoršují, šokují či rozrušují stát nebo jakoukoliv část populace.[112] Tímto bylo deklarováno, že svoboda projevu je zaručena všem bez ohledu na hranice státu a současně Ústavní soud ČR stanovil podmínku, že se musí jednat

[108] Usnesení Nejvyššího soudu České republiky ze dne 28. 12. 2004 sp. zn. 7 Tdo 1077/2004-I, ASPI.
[109] Usnesení Ústavního soudu České republiky ze dne 19. 4. 2004, sp. zn. IV. ÚS 606/03, ASPI.
[110] Tento názor zastává např. JUDr. Michal Bartoň, Ph.D. Srov. Bartoň, M.: Virtuální pornografie, limity svobody umělecké tvorby a svobody projevu a trestní zákon. Právní rozhledy, 2008. roč. 16, č. 17, s. 617-627.
[111] V evropských zemích je dětská pornografie přísněji posuzována než je tomu v Japonsku. Srov. Poremská, M.: Pornografie v USA. In Trestněprávní revue, č. 8/2008, str. 237.
[112] Usnesení Ústavního soudu České republiky ze dne 19. 4. 2004, sp. zn. IV. ÚS 606/03, ASPI.

alespoň o část populace, která bude informace či ideje vnímat negativně. Otázkou pak zůstává, jak budou soudy posuzovat mínění části populace ohledně toho, co je v souladu s morálkou a co nikoliv. Jedním ze způsobů posuzování, zda informace či ideje má negativní dopad na společnost, a tudíž se vymyká obecným standardům morálky, může být vedle průzkumů a anket prováděných různými institucemi i vyjádření relevantního počtu občanů na internetových stránkách.[113]

Pornografické dílo může mít různou podobu, přičemž trestní zákoník[114] uvádí jejich demonstrativní výčet. Podoba demonstrativního výčtu byla zvolena zejména proto, aby reflektovala možný budoucí technický vývoj, čímž vložením slovního spojení „jiné pornografické dílo“ otevřela možnost extenzivního výkladu podob pornografického díla, resp. možnost subsumovat pod tento pojem např. nová technická zařízení, která v budoucnu vzniknou.

Pornografické dílo může mít formu písemnou, fotografickou, filmovou, počítačovou, elektronickou nebo jinou.[115] Pokud se jedná o vyjádření rozdílu mezi dílem počítačovým a elektronickým, tak prvým dílem se rozumí dílo vytvořené pomocí počítače, elektronickým dílem to, které má podobu čitelnou jen strojově.[116] Podmínkou počítačového díla je, že musí být vytvořeno pomocí počítače, tzn. že půjde o dílo vytvořené ve virtuálním prostředí, které pak dále bude moct být rovněž dílem elektronickým, tj. jeho obsah bude moct být produkován pomocí elektronické podoby zaznamenané na technickém zařízení.

Listina základních práv a svobod, jakožto právní norma nejvyšší právní síly, stanovuje v čl. 32 odst. 1, že dětem a mladistvým je zaručena zvláštní ochrana. Z hlediska dětské pornografie je důležité vyložit, co (resp. kdo) se rozumí pod pojmem dítě. Trestní zákoník v ustanovení § 126 uvádí, že dítětem se rozumí osoba mladší

[113] Srov. usnesení Nejvyššího soudu České republiky ze dne 12.7.2006, sp. zn. 8 Tdo 763/2006, ASPI. Ve věci uložení trestu odnětí svobody na doživotí bylo konstatován závěr, že lze připustit jako pramen důkazu i vyjádření občanů na internetových stránkách. Dle mého názoru by bylo možné tento případ analogicky vztáhnout i na případ, kdy by se zjišťovala otázka, zda se jedná o dílo pornografického charakteru, tj. zjištění aktuálního stavu vnímání obecných standardů morálky ve společnosti.
[114] Srov. § 191 a § 192 zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.
[115] K výkladu jednotlivých pojmů viz Šámal, P. a kol. Trestní zákoník II. § 140 až 421. Komentář. 1. vydání. Praha: C. H. Beck, 2010, 1695 s.
[116] Gřivna, T. Trestné činy proti lidské důstojnosti v sexuální oblasti v novém trestním zákoníku. Bulletin advokacie, 2009, č. 10, s. 70

osmnácti let, pokud trestní zákon nestanoví jinak. V dřívějších trestněprávních předpisech pojem dítě definován přímo nebyl, výjimku bylo relativně možné spatřovat v ustanovení § 216b zákona č. 140/1961 Sb., trestní zákon, který stanovoval, že dítětem se rozumí osoba mladší než osmnáct let. Toto vymezení se ovšem vztahovala pouze k trestnému činu únosu a obchodování s dětmi. Přestože pojem dítěte nebyl dříve legislativně přímo vymezen, nečinil jeho výklad v praxi problémy.

Pojem dítě je dále vymezen v čl. 1 Úmluvy o právech dítěte[117], která jej definuje jako každou lidskou bytost mladší 18 let, pokud podle právního řádu, jenž se na dítě vztahuje, není zletilosti dosaženo dříve. V této souvislosti je třeba zmínit, že náš právní řád dovoluje nabýt zletilosti ještě před dosažením 18. roku věku, a to uzavřením manželství za podmínek stanovených zákonem.[118] Takto lze nabýt zletilosti již od dovršení věku 16 let. Takovéto nabytí zletilosti však z hlediska trestního práva nemá vliv a osoba bude i nadále považována za dítě, dokud reálně, tj. plynutím času, nedosáhne 18. roku života.

Pojem dítě vymezuje i Rámcové rozhodnutí Rady EU o boji proti pohlavnímu vykořisťování dětí a dětské pornografii.[119] Podle čl. 1 písm. a) se pro účely tohoto rámcového rozhodnutí rozumí dítětem každá osoba mladší 18 let. Jiným významným dokumentem vymezujícím pojem dítě z hlediska dětské pornografie je Úmluva o kybernetické kriminalitě.[120] Tato úmluva však nepoužívá pojem dítě, ale „nezletilá osoba“. V čl. 9 odst. 3 se uvádí, že pojem nezletilá osoba zahrnuje všechny osoby mladší 18 let. Smluvní strana může stanovit nižší věkovou hranici, která však nesmí být nižší než 16 let. Tímto vymezením Úmluva reaguje na situace, kdy zletilost je v jednotlivých státech nabývána dříve než dosažením 18. roku života, tj. stanovují nižší věkovou hranici pro chápání osoby jako dítěte.

Osoba, která se nachází v životním období od 15. do 18. roku života, je v trestněprávní nauce nazývána jako osoba mladistvá, i ta je však považována za dítě ve výše vyloženém významu. V České republice je zákonné provádění sexuálních aktivit limitováno věkovou hranicí 15 let. I když od dosažení tohoto věku lze žít

[117] Úmluva o právech dítěte byla podepsána 20.11.1989 v New Yorku, pro ČR závazná od 6.2.1991 (sdělení č. 104/1991 Sb.).
[118] Ustanovení § 8 odst. 2 zák.č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů.
[119] Rámcové rozhodnutí Rady 2004/68/SVV ze dne 22.12.2003 o boji proti pohlavnímu vykořisťování dětí a dětské pornografii.
[120] Úmluva o kybernetické kriminalitě byla podepsána dne 23.11.2001, ČR ji podepsala dne 4.2.2005, doposud nedošlo k její ratifikaci, a tudíž není prozatím pro ČR závazná.

sexuálním životem, je nezbytnou podmínkou, aby takovéto jednání bylo beztrestné, souhlas osoby provádějící jakoukoliv sexuální aktivitu. Výjimku představuje dětská pornografie, neboť pokud by osoba mladší18 let dala souhlas například se záznamem na videokameru, pak takovýto souhlas je zcela bezvýznamný a osoba, která stiskne nahrávání na videokameře, bude stíhána za trestný čin výroby dětské pornografie dle ustanovení § 192 trestního zákoníku. Osoba mladší 18 let si tedy může zvolit, že se zapojí do sexuálního života, ale nemůže si zvolit, že bude subjektem pornografického díla.

3.3.2.3.3. Dětská pornografie

Pojem dětské pornografie není v našem právním řádu vyjádřen žádnou přímou legální definicí, a proto je její výklad ponechán trestněprávní nauce a judikatuře. Za dětskou pornografii se považují taková pornografická díla, která znázorňují nebo jinak využívají dítě. Česká judikatura pak vymezila dětskou pornografii jako jakékoli zobrazování dítěte libovolnými prostředky při skutečných nebo předstíraných zřejmých sexuálních aktivitách či jakékoli zobrazování pohlavních orgánů dítěte k prvotně sexuálním účelům. Nejvyšší soud uvedl demonstrativní výčet děl, která se považují za dětskou pornografii. Jedná se např. o snímky obnažených dětí v polohách vyzývavě předvádějících pohlavní orgány za účelem sexuálního uspokojení, snímky dětí zachycující polohy skutečného či předstíraného sexuálního styku s nimi, popř. i jiné obdobně sexuálně dráždivé snímky dětí. Za pornografické dílo však není možno označit snímky, byť i zachycující částečně či plně obnažené děti, které působí sexuálně stimulujícím způsobem na jedince pohlavně deviantního, pokud nesplňují kritéria pornografického charakteru.[121]

Dětskou pornografii vymezují i mezinárodní dokumenty. Rámcové rozhodnutí o boji proti pohlavnímu vykořisťování dětí a dětské pornografii v čl. 1 písm. b) vymezuje dětskou pornografii jako pornografický materiál, který zobrazuje skutečné dítě, skutečnou osobu se vzhledem dítěte a realistické znázornění neexistujícího dítěte,

[121] Usnesení Nejvyššího soudu České republiky ze dne 28. 12. 2004 sp. zn. 7 Tdo 1077/2004-I, ASPI.

které se aktivně nebo pasivně účastní jednoznačně sexuálního jednání, a to včetně dráždivého vystavování přirození nebo ohanbí dítěte.

Úmluva o kybernetické kriminalitě vymezuje dětskou pornografii v čl. 9 odst. 2 jako pornografický materiál, který vizuálně zobrazuje nezletilého při zjevném sexuálním chování nebo sobu, která se jeví jako nezletilá při zjevném sexuálním chování

či realistické obrázky ukazující nezletilého při zjevném sexuálním chování. Výkladový problém by mohl vzniknout při vymezení pojmu „vizuální zobrazení“, kterým se pravděpodobně rozumí každé zobrazení, které může být pozorovatelné zrakem, tj. je viditelné jedním ze smyslů člověka. Smluvním státům je pak ponechána možnost trestně nepostihovat jednak obstarávání dětské pornografie pomocí počítačového systému pro svou potřebu či pro jiného, a jednak držení dětské pornografie v počítačovém systému. Možnost výjimky je upravena i pro případ pornografického materiálu, jehož aktérem je osoba starší 18 let, avšak vypadající jako nezletilá, a také materiálu zobrazujícího realistické znázornění neexistujícího dítěte.

3.3.2.3.4. Virtuální dětská pornografie - specifika

Základem virtuální dětské pornografie tedy je, že zde nedochází ke zneužívání či jinému využití skutečného dítěte. Vyvstává však otázka, zda virtuální pornografická díla, resp. jejich tvůrce, lze trestně stíhat, neboť důvodem proč problematika dětské pornografie byla upravena, byl zájem na ochraně skutečných dětí před jejich zneužíváním a vykořisťováním v sexuální oblasti. V případě virtuální dětské pornografie však zájem na ochraně před sexuálním zneužíváním dětí nemůžeme přímo dovodit, neboť zde nevystupuje konkrétní skutečný jednotlivec, a proto primárním objektem je ochrana mravního vývoje dětí. Lze se setkat i s názorem, že individuálním objektem je ochrana společnosti před potencionálně nebezpečným jednáním, které může vést až ke skutečnému zneužívání dětí.[122] Někteří teoretici zabývající se touto otázkou

[122] Volevecký, P., Šubrt, M.: Dětská pornografie jako kybernetický trestný čin ve světle Úmluvy o počítačové kriminalitě. Trestní právo, roč. 2009, č. 4, s. 16.

dovozují, že objektem ochrany v případě virtuální dětské pornografie nemá být mravnost, nýbrž ochrana dětí.[123]

Pro ochranu mravního vývoje dítěte a tedy skutečnosti, jak může virtuální pornografie ovlivnit vztah dítěte k sexuálnímu životu, lze uvést argument, že když dítě uvidí sexuální animaci, v níž bude v sexuálním aktu jako aktér vystupovat například Lisa Simpson, která je vykreslena v seriálu Simpsonovi[124] jako kladná postava s pozitivními lidskými vlastnostmi, a tudíž v očích dítěte chápána jako „správná osoba", přičemž můžeme předpokládat, že dítě nižšího věku není rozumově natolik vyspělé a sexuálně zralé, aby si bylo plně vědomo toho, co vidí, a danou animaci může vnímat tak, že když „to" dělá Lisa, tak na tom není nic špatného a můžu „to" dělat i já. Stejný vliv by samozřejmě mohla mít i animace pro dospělé, tj. animace, v níž by aktérem sexuálního chování byla dospělá osoba (např. Sněhurka, která je rovněž v očích dětí chápána jako kladná postava). Argumentem proti této možnosti výše uvedeného chápání animace je, že se jedná pouze o předpoklad, že animace ze strany dítěte bude tímto způsobem vykládána.[125] Podobný argumentem je rovněž pozitivní možnost ovlivnění pohlavních deviantů, neboť virtuální pornografie by mohla být pro řadu z nich alternativou, která by jim umožnila realizovat své potřeby na úrovni masturbačních fantazií, a tím by se snížilo riziko, že své potřeby skutečně realizují. Opačný argument, který se nabízí, je názor, že virtuální dětská pornografie jen zvyšuje chuť pedofilů a dodává jim odvahu účastnit se nezákonných činů.[126] V tomto případě již do popředí vystupuje zájem na ochraně dětí před jejich zneužíváním. V dané věci se jedná pouze o předpoklady. Tuto situaci můžeme srovnat s tvrzeními, která byla a jsou v poslední době prezentována vědci, teoretiky, sdělovacími prostředky apod., a to konkrétně, že násilí prezentované ve filmech a videohrách ovlivňuje chování a vnímání dětí ve skutečném životě. Samozřejmě i zde máme zastánce, kteří tuto teorii podporují, a na druhé straně ty, kteří ji nezastávají. Reálným faktem ovšem zůstává, že ve světě již existuje případ, kdy jednání osob bylo ovlivněno počítačovými hrami, a to s přímým

[123] Srov. Bartoň, M.: Virtuální pornografie, limity svobody umělecké tvorby a svobody projevu a trestní zákon. Právní rozhledy, 2008. roč. 16, č. 17, s. 624.
[124] Americký animovaný televizní seriál. Více: http://www.csfd.cz/film/72489-simpsons-the/.
[125] Srov. McEWEN v. SIMMONS & ANOR (2008), New South Wales Supreme Court, NSWSC 1292, dostupné z: http://lawlink.nsw.gov.au/scjudgments/2008nswsc.nsf/2008ns.
[126] Herczeg, J. Virtuální dětská pornografie: Zločin bez oběti? In Vanduhová, V., Gřivna, T. (eds.).: Pocta Otovi Novotnému k 80. narozeninám. ASPI, Wolters Kluwer, Praha 2008, s. 47.

odkazem pachatelů na jejich názvy. Jedná se o případ tzv. Kolumbijského masakru[127], kdy dva studenti, po předchozím naplánování a přípravě, v kafetérii střední školy usmrtili několik svých spolužáků a jednoho profesora střelnými zbraněmi, které si s sebou přinesli do školy. Ještě před spácháním svého činu natočili domácí video, v němž přímo odkazují na počítačovou hru slovy: „Bude to jako ten podělanej Doom,…Tahle podělaná brokovnice je jako vystřižená z Dooma!“[128] Zastánci teorie, že násilí ve virtuálním světě ovlivňuje chování dětí ve světě reálném, teď mají v ruce skutečný argument, kterým mohou operovat. Tímto případem mělo být demonstrováno, že i v případě virtuální dětské pornografie by neměl být opomíjen fakt, že virtuální svět je dnes každodenní běžnou součástí života, že se může promítat do reality a ovlivňovat chování a vnímání osob.

Abychom mohli mluvit o dětské virtuální pornografii, musí být splněna podmínka, že se musí jednat o dílo, které má pornografický charakter ve smyslu trestního práva, tzn. že se musí jednat o charakter veřejnoprávní. Při takovém hodnocení totiž i zde vystupuje otázka zásahu do ústavně zaručeného práva na svobodu projevu[129]. Musí se jednat o dílo, jehož obsahem bude sexuální aktivita zneužívající nebo jinak využívající neexistující dítě. Z tohoto důvodu nemůžou být trestné animace, které zobrazují sexuální chování dospělých animovaných osob, tj. starších 18 let.

Jelikož v rámci virtuální dětské pornografie nejde o skutečné dítě, vyvstává otázka co, popř. kdo, bude jejím předmětem. Možnost, že subjektem dětské pornografie bude neexistující dítě, upravuje Rámcové rozhodnutí Rady o boji proti pohlavnímu vykořisťování dětí a dětské pornografii. Čl. 1 písm. b) vymezuje pojem dětské pornografie, přičemž v bodě iii) uvádí, že jí je pornografický materiál, který zobrazuje realistické znázornění neexistujícího dítěte[130], které se aktivně nebo pasivně účastní jednání uvedeného v bodě i), tj. účastní se jednoznačně sexuálního jednání, a to včetně

[127] Informace dostupná z: http://cs.wikipedia.org/wiki/Masakr_na_Columbine_High_School.
[128] Informace dostupná z: http://www.project-syndicate.org/commentary/singer26/Czech.
[129] Srov. Miller v. California 413 U.S. 15 (1973). Srov. též Bartoň, M.: Virtuální pornografie, limity svobody umělecké tvorby a svobody projevu a trestní zákon. Právní rozhledy, 2008. roč. 16, č. 17, s. 619-620.
[130] Srov. Herczeg, J. Virtuální dětská pornografie: Zločin bez oběti? In Vanduhová, V., Gřivna, T. (eds.).: Pocta Otovi Novotnému k 80. narozeninám. ASPI, Wolters Kluwer, Praha 2008, s. 43 (pasáž:Situace ve Spolkové republice Německo).

dráždivého vystavování přirození nebo ohanbí dítěte. V rámci Evropské Unie je tedy připuštěno, že předmětem dětské pornografie mohou být i virtuální pornografická díla (i ta vytvořená mimo kyberprostor). V daném případě je však podmínkou, že se musí jednat o realistické znázornění dítěte, tj. případ, kdy dílo z hlediska průměrného pozorovatele vypadá jako dokument o skutečném pohlavním zneužívání dítěte.[131] Důležitá bude míra realističnosti virtuálního pornografického díla. S ohledem na stále pokračující technický vývoj bude čím dál obtížnější rozeznat dítě skutečné a nereálné (tuto úvahu nelze vztáhnout na animace, neboť zde vždy víme, že se nebude jednat o skutečné dítě). Konzumenti takového díla by se mohli obhajovat právě tím, že se nejedná o skutečné dítě.[132] Jako příklad lze uvést situaci, kdy bude natočen film se skutečnými lidskými bytostmi, přičemž jedním z aktérů bude virtuálně upravený a do filmu přidaný android nebo kyborg, který bude prokazatelně mladší 18 let, a u tohoto díla nebude pochybnost, že se jedná o dílo zachycující dětskou pornografii.[133] V tomto konkrétním případě by určitě bylo možné vzít v potaz hledisko společenské škodlivosti, které by zde mělo pravděpodobně větší váhu než v případě animace.

Základní otázkou je, zda virtuální dítě (osoba) může mít věk. V daném kontextu není možné hovořit o věku v rámci plynutí času, ale v potaz lze brát tzv. „zdánlivý věk“, tj. věk, který může být virtuální osobě přisouzen na základě pozorovatelných tělesných znaků. Věk virtuálního dítěte lze odvodit z jeho vzhledu, přičemž může být jasné, že se jedná o dítě mladší 18 let (např. animované batole), a nebo nebude jisté, zda animovaná osoba je dítětem. Tato otázka bude v praxi představovat problém, který bude muset být řešen na základě konkrétních okolností a rysů animované postavy (tj. rysů vzhledových, přičemž v potaz by mělo být bráno i vystupování a chování takové postavy, její oblečení apod.). Uvedené rysy pak bude nutné vykládat ve vzájemné souvislosti, nikoliv jednotlivě.

Další způsob určení věku představuje jeho odvození z charakteru animace, resp. souvislostí dějové linie. Konkrétně se může jednat o situaci, kdy přímo v animaci bude

[131] Tamtéž, s. 43.

[132] Srov. Bartoň, M.: Virtuální pornografie, limity svobody umělecké tvorby a svobody projevu a trestní zákon. Právní rozhledy, 2008. roč. 16, č. 17, s. 621.

[133] Jako příklad lze pro srovnání uvést filmové zpracování Jaws 3-D (Čelisti 3), ve kterém vystupují skuteční herci a počítačově je zde pak upraven žralok. Dostupné z: http://www.csfd.cz/film/19676-jaws-3d/.

jasně řečeno, že se jedná o virtuální osobu mladší let (např. Mach a Šebestová, kdy se ve znělce uvádí „my jsme žáci 3.B“ a současně lze z charakteru a vzhledu poznat, že se jedná o děti mladší 18 let). Takovéto určení věku však musí být v konkrétním případě nesporné. V případě, že by otázka věku animované postavy nebyla určena napevno, měla by být uplatněna zásada in dubio pro reo.[134]

3.3.2.3.5. Trestní postih v české právní úpravě

Základní otázkou je, zda je možné virtuální dětskou pornografii v České republice trestně stíhat. Trestní zákoník nerozlišuje mezi dětskou pornografií skutečnou a virtuální. Virtuální dětská pornografie však dle ustanovení § 192 a § 193 trestního zákoníku stojí mimo dosah trestního stíhání, a to s ohledem na objekt těchto trestných činů, kterým je zájem společnosti na ochraně dětí před sexuálním zneužíváním a ochrana jejich mravního vývoje. Rovněž s ohledem na princip subsidiarity trestní represe lze mít za to, že držení pornografie, v němž je prezentováno virtuální dítě (nikoliv skutečné), trestné není.[135] Naproti tomu někteří teoretici zastávají názor, že výrobci a distributoři animované dětské pornografie se nevyhnou postihu za trestný čin šíření a výroby dětské pornografie, přičemž v konkrétním případě bude nutné zvážit hledisko společenské škodlivosti.[136] Pro skutečnost, že by virtuální dětská pornografie mohla být předmětem trestního stíhání, svědčí i její vymezení v ustanovení § 192 trestního zákoníku, v němž se uvádí výraz „jinak využívá dítě“, který ponechává určitou alternativu extenzivního výkladu. Tento výraz se má zřejmě vztahovat na pornografický materiál, u něhož z povahy věci chybí prvek zobrazení, avšak na druhé straně tento výraz vyžaduje, aby dítě bylo nějakým způsobem v díle přítomno, byť ne přímo zobrazeno.[137] Ke stíhání virtuální dětské pornografie by mohlo dojít jen v případě, že bude připuštěno, že virtuální dítě lze subsumovat pod pojem dítě používaný

[134] Císařová, D., Fenyk, J., Gřivna, T. a kol. *Trestní právo procesní.* 5. vydání. Praha: ASPI, 2008, 83 s.
[135] Šámal, P. a kol. Trestní zákoník II. § 140 až 421. Komentář. 1. vydání. Praha: C. H. Beck, 2010, str. 1705.
[136] Herczeg, J. Virtuální dětská pornografie: Zločin bez oběti? In Vanduhová, V., Gřivna, T. (eds.).: Pocta Otovi Novotnému k 80. narozeninám. ASPI, Wolters Kluwer, Praha 2008, s. 42.
[137] Bartoň, M.: Virtuální pornografie, limity svobody umělecké tvorby a svobody projevu a trestní zákon. Právní rozhledy, 2008. roč. 16, č. 17, s. 623.

v předmětném ustanovení trestního zákoníku. Tato otázka je spojena s chápáním významu pojmu dítě jako osoby z právního hlediska.

Není pochyb o tom, že dítě je zároveň osobou, a proto další otázkou, která v souvislosti s virtuální dětskou pornografií vyvstala, je, zda kreslená postava může být považována za „osobu" z právního hlediska. I zde se názory různí. Jedním z takových názorů je, že se o „osobu" jednat nemůže, neboť by se jednalo o extenzivní rozšiřování trestní odpovědnosti na situace, které neměl zákonodárce v úmyslu postihovat.[138] Pojem osoby v právním významu lze považovat za pojem historický a obecně se jím rozumí fyzické a právnické osoby, přičemž z hlediska českého trestního práva máme upravenu pouze trestní odpovědnost fyzických osob. Při zavádění pojmu fyzické osoby rozhodně nebylo možné počítat s variantou virtuálního prostředí, neboť zákonodárci pravděpodobně nebyla známa. Fyzická osoba je dnes chápána jako jednotlivec z masa a kostí, tj. jako skutečná osoba. Pokud se na danou problematiku podíváme všeobecně, můžeme konstatovat, že i právnické osoby jsou dílem fikce a nejsou skutečné, ale jejich chápání jako právních subjektů je již zažité, i když do oblasti trestního práva u nás doposud nepronikly jako je tomu v jiných státech. V případě, že by trestní odpovědnost právnických osob byla do trestního práva zavedena, je nezbytné podotknout, že by se právnická osoba některých skutkových podstat trestných činů nemohla dopustit. Stejným směrem lze uvažovat i v případě chápání kreslených postav jako osob z hlediska práva. Právo by nemělo být rigidní, resp. nemělo by být vykládáno zcela rigidně, ale naopak by mělo pružně reagovat na situace a prostředí v daném čase a místě. Rovněž by mělo reflektovat chápání a standardy společnosti. Jelikož virtuální svět překračuje pomyslnou hranici světa reálného, stává se jeho každodenní součástí, je možné brát v potaz i úvahy směřující k chápání kreslených postav jako právních entit, a tudíž by bylo možné rozšířit pojem osoby v právním významu. Samozřejmě i zde by musely platit určité hranice, kdy takové chápání kreslených postav by nebylo možné z povahy věci použít u všech skutkových podstat trestných činů (např. únos dítěte, dvojí manželství apod.).

[138] Volevecký, P., Šubrt, M.: Dětská pornografie jako kybernetický trestný čin ve světle Úmluvy o počítačové kriminalitě. Trestní právo, roč. 2009, č. 4, s. 19. Dále srov.: McEWEN v. SIMMONS & ANOR (2008), New South Wales Supreme Court, NSWSC 1292 (blíže pojednáno v kapitole Případové studie).

4. Případové studie

Tato kapitola je věnována vybraným kauzám, které se odehrály mimo státní hranice České republiky, tj. v rámci jurisdikce zahraničních států. Na těchto případech má být demonstrováno, jak se jiné státy vypořádávají s problematikou virtuálních trestných činů.

4.1. Amulet

Velice známou a celosvětově rozšířenou MMORPG je RuneScape[139]. Jedná se o volně dostupnou internetovou online hru, tzn. že je možné ji hrát bez poplatků a bez jakékoliv instalace. RuneScape je trojrozměrný virtuální svět založený na předloze fantasy[140]. Hra se hraje na více serverech rozmístěných po celém světě. Hráči jsou rozděleni na členy (pay to play) a nečleny (free to play). Rozdílnost spočívá v tom, že platící členové mají úplný a neomezený přístup do všech služeb hry. V rámci pravidel hry je dovoleno provádět výměny herních položek za jiné předměty či služby, které hra nabízí, není však možné provést jejich výměnu za výhody v jiných online hrách, za reálné peníze či jiné výhody reálného světa. I tato hra má svou vlastní měnu, která však není směnitelná za skutečné peníze. Veškerá práva duševního vlastnictví nebo jiných práv týkající se herní postavy, účtu a herních položek jsou a vždy zůstanou ve vlastnictví vlastníka hry.

Předmětná kauza[141] nazývána „amulet“ se odehrála v Holandsku v listopadu 2009 a byla projednávána odvolacím soudem v Leeuwardenu. Obžalovaný spolu s dalšími osobami si protiprávně přivlastnili virtuální amulet a masku, jakož i virtuální peníze, vše pocházející z internetové hry RuneScape. Tyto předměty náležely jinému

[139] Tato hra je vlastněna a provozována společností JAGEX LIMITED („Jagex“) se sídlem ve Velké Británii.
[140] Děj hry se odehrává na území země Gillinor rozdělené na více království.
[141] Rozhodnutí LJN: BK2773, Gerechtshof Leeuwarden. Dostupný z: www.rechtspraak.nl/ljn.asp?ljn=BK2773.

uživateli (poškozený), kterého nutili otevřít svůj uživatelský účet ve hře RuneScape, a tím umožnit převedení virtuálních předmětů na uživatelský účet vlastní. Předmětnému jednání předcházelo týrání, vyhrožování a užití násilí, které spočívalo v úderech pěstí do hlavy, kopání do hrudníku, žeber a beder. Obžalovaný se rovněž postavil proti poškozenému s nožem, s nímž prováděl pohyby spočívající v mávání, bodání a vrhání. Poškozenému hrozil slovy „zabiju tě“ a jinými slovy výhružné povahy. Obžalovaný strhnul poškozeného ze židle na podlahu, ovázal mu šátek kolem krku a stisknul mu hlavu, čímž způsobil poškozenému bolest a zranění. Z provedeného dokazování rovněž vyplynulo, že se jednalo o předem připravený plán.

Výše popsané jednání bylo kvalifikováno jako krádež za použití násilí podle čl. 310 a 312 nizozemského trestního zákoníku, přičemž čl. 312 nese označení loupež[142]. Trestné činy krádeže a loupeže jsou zařazeny společně do stejné hlavy XXII. nazvané Krádež. Dalo by se říci, že na loupež je pohlíženo jako na těžší formu krádeže, což lze dovodit přímo z předmětného čl. 312. Rozdílnost spočívá v použití násilí nebo pohrůžky násilím proti osobě se záměrem krádež připravit nebo usnadnit, nebo v případě přistižení při činu se záměrem zajistit sobě nebo dalším spolupachatelům únik nebo získání odcizeného majetku. Z tohoto důvodu odvolací soud hovoří o trestném činu krádeže, přičemž pod něj zahrnuje i loupež. Naproti tomu podle české úpravy by se jednalo pouze o loupež. Výkladově jsou ustanovení obou trestních zákoníků relativně shodná. Důležité je rovněž upozornit na fakt, že odebrání věcí bylo spácháno mimo kontext hry. Z tohoto důvodu se nejedná o virtuální jednání spáchané ve virtuálním světě (tj. nejde o pravý virtuální trestný čin), ale o skutečné jednání, jenž virtuální svět ovlivnilo.

Jednou ze základních otázek, kterou musel holandský odvolací soud řešit, byla námitka založená na rozsudku Evropského soudu pro lidská práva ze dne 27. listopadu 2008 ve věci Salduz proti Turecku. Pachatelem výše popsané události byl mladistvý podezřelý, který nebyl upozorněn na možnost právní pomoci během policejního výslechu. Rovněž nebyla podezřelému dána možnost poradit se svým právním zástupcem ještě před začátkem výslechu. Soud došel k závěru, že se jedná

[142] Viz příloha č. 3.

o porušení základní trestněprávní zásady a rozhodl, že výpověď podezřelého na policii musí být vyloučena z dokazování.

Z hlediska virtuálního prostředí řešil odvolací soud otázku, zda virtuální předměty pocházející z internetové hry RuneScape jsou věcmi v právním slova smyslu podle článku 310 nizozemského trestního zákoníku, který obsahuje skutkovou podstatu trestného činu krádeže, jejíž předmětem je neoprávněné přisvojení si cizí věci.

Základním problémem se stala otázka, zda virtuální předmět splňuje definiční znaky cizí věci. Relevantní bylo posouzení, zda takovéto předměty mají pro vlastníka uživatelskou hodnotu. V předmětné hře si hráči vytváří prostřednictvím osobního účtu své alter ego, přes které mohou vyvíjet různé aktivity, rozvíjet dovednosti, mohou bojovat či komunikovat se spoluhráči a plnit individuální úkoly. Za uskutečněná jednání dostávají body a získávají „předměty“ jako např. virtuální amulet a masku.

Soud v daném případě rozhodl, že virtuální předměty jsou věcmi ve smyslu čl. 310 nizozemského trestního zákoníku, a to na základě prohlášení všech stran sporu, že virtuální věci pro ně nepochybně hodnotu měly. Soud opřel svůj závěr o uživatelské hodnotě a o tom, že věc nemusí být jen hmotná, o rozhodnutí Nejvyššího soudu o elektřině z roku 1921, neboť virtuální předměty a elektřina mají společné rysy. V rozhodnutí o elektřině Nejvyšší soud konstatoval, že elektřina jako nehmotná věc je předmětem s uživatelskou (ekonomickou) hodnotou, přičemž tuto tezi lze vztáhnout i na problematiku virtuálních předmětů.

Další otázkou bylo, zda poškozenému věc v trestněprávním smyslu patřila a zda mu mohla být neoprávněně odebrána. Závěr o vlastnictví vyzněl pro poškozeného kladně. Pro soud byla rozhodující skutečnost, že poškozený měl vždy po přihlášení se na svůj účet ve hře jako jediný možnost skutečně a výlučně s virtuálními předměty nakládat, tj. realizoval nad nimi svou dispoziční moc. Po jejich převedení na uživatelský účet pachatele poškozený tuto dispoziční možnost ztratil a pachatelé ji naopak získali. Za irelevantní bylo považováno, že internetová hra má svého vlastníka, což zdůvodnil příkladem cestovního pasu, který je ve vlastnictví Holandska, ale může být krádeží odcizen svému držiteli z jeho dispoziční moci. Kdo je majitelem práv k internetové hře, není tedy podle rozhodnutí soudu relevantní.

Základem pro vyřešení této otázky se stala skutečnost, že věc byla odebrána z dispoziční moci jednoho do dispoziční moci druhého, a tudíž se u virtuálních předmětů jedná o situaci odlišnou od odcizení softwaru (počítačových dat, PIN atd.), kdy poškozený neztrácí dispoziční moc a nejedná se tedy o krádež. Pro odvolací soud byla rovněž relevantní skutečnost, že herní pravidla RuneScape nepředpokládají nabytí předmětů takovým způsobem, jakým se to stalo v tomto případě.

Ve výše uvedeném rozhodnutí nizozemský odvolací soud ustálil závěr, že virtuální předměty, které nemají hmotný hmatatelný základ, jsou v trestněprávním významu věcmi. Virtuální předměty a předměty skutečné tak byly postaveny na stejnou úroveň. Mohou být jinou osobou, která nemá k virtuálním věcem žádné relevantní vlastnické oprávnění, odcizeny a mohou tak naplnit skutkovou podstatu trestného činu krádeže.

4.2. Habbo hotel

Habbo hotel je název pro virtuální svět, který je vlastněn a provozován finskou společností Sulake Corporation, která má řídící centrum ve Spojených státech amerických. Habbo hotel může být považován rovněž za online hru, která je zpřístupněna prostřednictvím Internetu[143], ale spíše se lze setkat s názorem, že se jedná o pouze o virtuální sociální prostředí, v němž dochází k vzájemné interakci mezi jeho uživateli. Základním tématem je prostředí hotelu, které se skládá z veřejných a soukromých místností (hotelové pokoje). Nejprve si hráč založí uživatelský účet a vytvoří svou identitu. Následně si zařizuje svůj hotelový pokoj, komunikuje s ostatními hráči na virtuálních prostranstvích a využívá virtuální služby. Vybavení hotelového pokoje si hráči pořizují za kredity, jenž se pořizují za skutečné peníze. Na základě této skutečnosti dochází k vzájemnému propojení mezi světem virtuálním a skutečným.

V rámci hry existují dva druhy měn, a to tzv. kredity (mince), které se používají na nákup nábytku pro vybavení hotelového pokoje z katalogu, a tzv. pixely, které hráč

[143] www.habbo.com, www.habbo.nl aj. Ke dni 1.7.2010 existuje celkem 19 webových stránek.

získává za dobu, po kterou je připojen ke hře, za něž si pořizuje ostatní virtuální předměty. Kredity lze získat různými způsoby (například koupí, prostřednictvím SMS zprávy aj.), mohou být vyměněny ve směnárně, tzn. že podstatou jejich pořízení jsou skutečné peníze. Hráči mohou s těmito kredity libovolně obchodovat. Naproti tomu pixely jsou čistě virtuální měnou, kterou nelze za reálné peníze pořídit a není možné s ní obchodovat. Jejich použitelnost je vázána nejčastěji na nákup účinků pro své avatary nebo pro nájem nábytku se speciálními efekty apod.

Oproti internetové hře RuneScape má Habbo hotel řadu odlišností v rámci podmínek používání. Účastnit se tohoto virtuálního světa smí pouze osoba starší 13 let a podle právní úpravy státu, ze kterého pochází, je zapotřebí souhlasu zákonného zástupce v případě, že nemá plnou způsobilost k právním úkonům. Uživatel zodpovídá třetím stranám za veškerý obsah, který bude uveřejněn, a současně dává vlastníkovi souhlas s jeho případným užitím. Používání webových stránek Habbo hotelu je bez záruky vlastníka, který nenese žádnou odpovědnost.

Uživatelský účet, avatar i uveřejněný obsah je vytvořen uživatelem, který za ně odpovídá. V případě porušení pravidel má vlastník pouze právo, nikoliv povinnost, odstranit obsah bez předchozího upozornění. Mezi další vlastníkova oprávnění patří možnost zmrazit nebo zrušit účet ze stanovených důvodů, přičemž uživateli nebude náležet žádná náhrada za nakoupené kredity. Veškeré aktivity, předměty a služby zpřístupněné na webových stránkách jsou určeny pouze pro hru a je zakázáno je prodávat, směňovat či jinak s nimi disponovat, avšak pokud tak chce hráč učinit, má možnost požádat vlastníka hry o předchozí svolení.

Holandský trestní soud v Amsterdamu v dubnu 2009 řešil případ[144], kdy se mladistvý obžalovaný dopustil jednání, která byla kvalifikována jako zásah do počítačového systému dle čl. 138a a krádež dle čl. 311 nizozemského trestního zákoníku[145].

Protiprávní jednání spočívalo v úmyslném proniknutí na servery internetových stránek www.habbohotel.com a www.hotmail.com. Obžalovaný odeslal uživatelům

[144] Rozhodnutí LJN: BH9789, Rechtbank Amsterdam. Dostupný z: www.rechtspraak.nl/ljn.asp?ljn=BH9789.
[145] Viz příloha č. 3.

uvedených internetových stránek e-mailovou zprávu s odkazem na předem vytvořenou falešnou stránku (fake-site), která vypadala jako originální internetová stránka, a jenž byla přílohou elektronické zprávy. Falešná stránka byla vytvořena speciálním programem, který si obžalovaný stáhnul na Internetu. Uživatele vždy požádal, aby odkaz otevřel. Otevřením odkazu byl uživatel převeden na falešnou stránku www.habbohotel.com a www.hotmail.com, přičemž zadal originální přihlašovací údaje. Tímto způsobem obžalovaný získal originální uživatelské jméno a heslo. Následně tyto údaje použil na originální webové stránce, čímž se dostal do příslušného uživatelského účtu a požádal Habbohotel, aby mu zaslal přihlašovací údaje nové. Poté, co obžalovaný obdržel nové údaje, přihlásil se na habbohotelový účet podvedeného uživatele, kde se zmocnil virtuálního nábytku a jiných virtuálních předmětů z virtuálního hotelového pokoje, přičemž je přesunul na svůj uživatelský účet. Virtuální nábytek, který byl takto převeden, měl hodnotu přibližně 4000 eur.

Soud prvního stupně v Amsterdamu se v dané kauze musel vypořádat s několika otázkami. Nejprve se zabýval otázkou, zda pachatelé svým jednáním spáchali jeden trestný čin, a to konkrétně zásah do počítačového systému[146], či zda byl tento trestný čin spáchán v souběhu s trestným činem krádeže[147].

Soudce ve věcech mládeže se nakonec přiklonil k druhé variantě a shledal obžalované vinným z trestných činů zásahu do počítačového systému v souběhu s trestným činem krádeže. Při odůvodnění svých závěrů vycházel holandský soud z interpretace pojmů „převzetí, odposlech a zaznamenání“, které skutková podstata čl. 138a nizozemského trestního zákoníku používá. Tyto pojmy mají již v holandském trestním právu ustálený výklad a jsou používány pro zachycení a uchování proudících údajů.

Termíny „odposlech a zaznamenání“ jsou používány pro úkony spočívající v zachycení a uchování proudících údajů. Termín „převzetí“ je používán ve významu okopírování takto zaznamenaných údajů. Těchto jednání se pachatelé

[146] Zásah do počítačového systému je v České republice kvalifikován jako trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací dle ustanovení § 230 trestního zákoníku (dále jen „neoprávněný přístup k počítači“).

[147] Dle obhajoby byl zásah do počítačového systému v tomto případě speciálním trestným činem k trestnému činu krádeže. Obhájce současně uvedl, že pokud by čl. 138a nebyl považován za lex specialis, pak zmocnění se virtuálních předmětů je pokračování v jednání, jenž spočívalo v zásahu do účtu jiného prostřednictvím převzetí a odposlechu přihlašovacích údajů jiného.

dopustili pouze ve vztahu k údajům týkajících se e-mailových a hotelových účtů uživatelů, které byly zkopírovány prostřednictvím falešně vytvořené internetové stránky. Ani pod jeden z těchto pojmů se podle soudu nedá podřadit jednání, které spočívá v odcizení věci jejímu vlastníkovi, jenž je obsažené v ustanovení o trestném činu krádeže, neboť data v podobě virtuálního nábytku nebyla pachateli zachycena či uchována. Pravděpodobně jiná by byla situace, kdy by tyto předměty byly v době odcizení proudícími údaji.

V daném případě nedošlo ani k tzv. „převzetí" dat, neboť při tomto jednání, jak již bylo řečeno výše, dochází ke kopírování údajů, avšak jejich majitel s nimi neztrácí možnost nakládat. Zde však byly virtuální předměty protiprávně převedeny z dispoziční moci svého majitele do dispoziční moci pachatelů, tj. byly odcizeny ve smyslu ustanovení nizozemského trestního zákoníku o trestném činu krádeže.

Nizozemský soud svým rozhodnutím odlišil zásah do počítačového systému spojeného se zachycením a kopírováním dat v tomto systému uložených a krádeží virtuálních předmětů. Zatímco při „krádeži dat" zůstávají tyto data v dispozici poškozeného a pachatel získá pouze jejich kopii, při krádeži virtuálních předmětů se jedná o odebrání možnosti poškozeného s věcí nakládat, přičemž pachatel tuto možnost dispozice naopak získává.

Z výše uvedených důvodů a s ohledem na stále rostoucí význam internetového prostředí a závislosti na něm považoval soud za nezbytné chránit pokojné uživatele[148], a proto uznal obžalovaného vinným z trestného činu zásahu do počítačového systému a trestného činu krádeže.

Tato kauza je příkladem tzv. phishingu. Útočník "uloví" heslo uživatele tak, že mu zobrazí falešnou stránku, která se vydává vzhledově za stránku originální. To se v praxi děje nejčastěji posláním falešné e-mailové zprávy, která taktéž dodržuje obvyklou vzhledovou strukturu originální e-mailové zpávy[149], s žádostí k odeslání hesla z důvodu například poškození databáze. Pokud poškozený zadá svá přístupová hesla na odkazované falešné stránce, jsou okamžitě uložena a útočník tím získává možnost manipulovat s účtem.

[148] Soud nazval toto jednání tzv. hackerstvím.
[149] V ČR je nejznámějším případem phishing aplikace internetového bankovnictví České spořitelny a.s.

4.3. Virtuální dětská pornografie v Second Life

Jedním z diskutovaných problémů ohledně virtuální dětské pornografie, je její dostupnost v Second Life.[150]

Second Life má dvě základní formy, a to Basic a Premium. Basic verze je zcela zdarma a je pro ty uživatele, kteří nehodlají vlastnit půdu, obchodovat nebo se například prezentovat a pořádat různé akce. Vlastník Basic účtu má možnost stavět a skriptovat objekty pouze na speciálních pozemcích, které jsou označovány jako dočasné stavební zóny, tzv. sandboxy. Dále má možnost létat, oblékat se nebo ovládat své výtvory a ukládat je do svého inventáře. Naproti tomu účet Premium je určen pro všechny, kteří chtějí vlastnit půdu a kteří se chtějí více angažovat. Premium verze je zpoplatněna měsíčním poplatkem, který uživateli umožní stavět, ukládat a zobrazovat projekty přímo na své půdě, kterou si zakoupil, tzn. že má možnost plné realizace svého virtuálního života a postavy.

Vedle výše uvedých forem je Second Life rozdělen ještě do dvou virtuálních světu podle věku skutečného uživatele, a to na tzv. MainGrid, určený pro uživatele od dosažení věku 18 let a více, a na tzv. TeenGrid, určený pro věkovou skupinu v rozmezí od 13 do 18 let. Věk se zjišťuje při registraci, kdy uživatel je povinen vyplnit kolonku „age“, přičemž poté již v reálné situaci není nadále zkoumáno, zda je tato informace pravdivá či nikoliv. Není tedy vyloučeno, aby se v MainGrid nacházely osoby mladší 18 let a v TeenGrid osoby starší 18 let. Po registraci do příslušné verze Second Life si uživatel volí svou herní postavu, pod níž bude nadále vystupovat. Uživatelé si vytváří a průběžně mohou měnit svou identitu, tzv. virtuální totožnost, tj. i osoba starší 18 let si může zvolit vzhled batolete, pokud bude mít zájem.

Tvorba tohoto světa je plně v rukou samotných uživatelů. Veškeré výtvory uživatelů Second Life jsou zcela jejich vlastnictvím a vztahuje se na ně autorskoprávní ochrana. Uživatelé mají možnost obchodování s vytvořenými produkty nebo se službami, a to prostřednictvím existence vlastní vnitřní měny, tzv. Linden dolaru,

[150] Třírozměrný virtuální svět přístupný přes Internet, který měl na počátku roku 2008 více než 20 miliónů uživatelů. Second Life je obrazem skutečného světa ve virtuálním prostředí.. Informace dostupná z: http://cs.wikipedia.org/wiki/Second_life.

na kterém stojí veškerá ekonomika Second Life. Největší výhodou Linden dolaru je jeho volná směnitelnost za skutečné peníze[151].

V roce 2007 německá stanice ARD odvysílala reportáž o dostupnosti dětské pornografie v Second Life[152], a to jednak ve formě tradičního obrazového záznamu, a jednak přímo online jako hru, ve které byl avatar buď hlavním aktérem nebo se hry mohl účastnit jako divák, a to kdokoli, tj. kterýkoliv avatar. V některých případech bylo nutné zaplatit vstupné.[153] Reportáž odhalila skupinu obchodující s dětskou pornografií a vyšetřování bylo rovněž zaměřeno na uživatele, kteří za virtuální sex zaplatili. Důvodem, proč se německé vyšetřovací orgány a státní zástupce (prosecutor) touto kauzou zabývali, je skutečnost, že podle německého trestního práva je držení virtuální dětské pornografie trestné.[154] Společnost Linden Lab, která je tvůrcem Second Life, poskytla německým orgánům součinnost při zjišťování identity uživatelů, a to jednak těch, kteří zaplatili za virtuální sex, a jednak majitelů pozemků, na kterých se dětská pornografie uskutečňovala.[155] Současně se zavázala upravit hru tak, aby bylo zabráněno virtuálním dětem (tj. uživatelům mladším 18 let, ale i uživatelům, jejichž virtuální totožnost představuje dítě) v provozování sexuálního jednání a zaměřila se na ověřování identity.

Případ virtuální dětské pornografie v Second Life ukazuje nové prostředí a nebezpečnost, která je spojena s kyberprostorem, zejména možnost pohybovat se ve virtuálním světě bez větších obtíží a nízké možnosti dozoru. Virtuální dětská pornografie není brána na lehkou váhu. Naopak je v určitých státech chápána jako závažný negativní jev, který je nutné omezit a regulovat.

---

[151] Pro české uživatele byla v rámci Second Life vytvořena oblast Bohemia, tj. česko-slovenské město, v němž je mimo jiné zřízena funkce směnárny českých korun za Linden dolary prostřednictvím Raiffeisenbank. Kurz činí: 1Kč = 8,3000 L$.

[152] Reportáž je dostupná na: http://www.youtube.com/watch?v=Wk8uNWF77gg.

[153] V Second Life se obchoduje s virtuálními penězi, které je možné následně přeměnit ve skutečnou měnu a opačně.

[154] Informace dostupná z: http://news.bbc.co.uk/2/hi/technology/6638331.stm.

[155] V Second Life je možné vlastnit pozemky tohoto virtuální světa, které si je možné koupit, a to buď za účelem bydlení nebo obchodování s nimi.

4.4. Simpsonovi

Jedním ze zajímavých soudních rozhodnutích zabývajících se otázkou virtuální dětské pornografie je rozhodnutí australského Nejvyššího soudu (Nového jižního Skotska) McEwen v. SIMMONS & ANOR[156], které se zabývá otázkou, zda kreslené animované postavy (cartoon figures) mohou zobrazovat nebo vyjadřovat osobu (person). Pornografický materiál, který byl posuzován, zobrazoval dětské členy rodiny Simpsonů při sexuálních aktivitách, přičemž měly jasně vyobrazeny lidské pohlavní orgány. McEwen byl soudem nižšího stupně v předmětné věci shledán vinným z trestného činu držení dětské pornografie (dle státního zákonodárství – State legislation) a trestným činem šíření a zpřístupnění dětské pornografie (dle zákonodárství Společenství – Commonwealth legislation)[157].

V odůvodnění uvedeného rozhodnutí se Nejvyšší soud nejprve vypořádal s otázkou posouzení věku dětských kreslených postav (Bart a Lisa), kdy konstatoval, že předpokládaný věk uvedených postav lze odvodit z televizního seriálu a není žádná pochybnost o tom, že se jedná o postavy ve věku nižším než 18 let[158], a pravděpodobně také o postavy mladší 16 let.[159] Základní faktickou otázku, kterou Nejvyšší soud posuzoval, bylo, zda fiktivní kreslená postava může být považována za osobu ve smyslu zákonem stanovených trestných činů.[160] Postavy nenapodobovaly žádnou skutečnou nebo fiktivní lidskou bytost. I když se vyznačovaly čtyřmi prsty, obličejem, tj. měly oči, nos a ústa, odlišovaly se od kterékoliv možné lidské bytosti. Nejvyšší soud spatřoval základní rozdíl mezi zobrazením skutečné lidské bytosti a zobrazením fiktivní osoby. Pro objasnění rozdílu uvedl, že osoby zobrazené ,například ve videohrách a komiksech, jsou osobami fiktivními, které jsou zapojeny do strašného násilí zahrnujícího mučení a smrt. Kdyby tyto osoby byly skutečné, takové zobrazení by nebylo nikdy povoleno a jejich vytvoření by zakládalo trestný čin, tzn. že zobrazení jsou povolována jenom

[156] McEWEN v. SIMMONS & ANOR (2008), New South Wales Supreme Court, NSWSC 1292, dostupné z: http://lawlink.nsw.gov.au/scjudgments/2008nswsc.nsf/2008ns.

[157] V Austrálii se uplatňuje jednak státní zákonodárství (State legislation), jednak zákonodárství Společenství (Commonwealth legislation).

[158] Commonwealth legislation pod pojmem dítě chápe osobu mladší 18 let [Section 9H(3) of Crimes Act 1900].

[159] State legislation pod pojmem dítě chápe osobu mladší (zdánlivě mladší) 16 let [Section 474.19 of Criminal Code Act 1995].

[160] Přestože se soud s touto otázkou vypořádal, konstatoval, že žádná jasná linie zahrnutí nebo vyloučení kreslených postav ve smyslu posouzení, zda se jedná o osoby z právního hlediska, nemůže být popsána.

proto, že se jedná o fiktivní konstrukce. Skuteční lidé můžou být fiktivní a v tomto smyslu přijmout nebo hrát roli jiných než sebe samých či fiktivních postav, ale stále jsou to skuteční lidé.

Z pohledu „Commonwealth legislation" mohou být kresby a jiná zobrazení vyobrazením fiktivních nebo imaginárních postav.[161] Ačkoli hlavním cílem zákonodárství je boj proti přímému sexuálnímu vykořisťování a zneužívání dětí, zákonodárství rovněž počítá se zabráněním výroby takového materiálu (zahrnujícího i materiál kreslený) a jeho zpřístupněním na trh. V tomto ohledu Nejvyšší soud neshledal žádný důvod omezit význam osoby pouze na osobu skutečnou a do zobrazení nebo ztvárnění osob, na které definice odkazuje, zahrnuje jak kresby osob fiktivních (model, socha), tak i kreslených.

Rovněž Nejvyšší soud poukázal na fakt, že postava odchylující se od rozpoznatelné podoby lidské existence, se může stát více méně osobou, a nebo také nemusí ztvárňovat osobu vůbec. Pouhé přiřazování lidských vlastností například králíkovi nebo kachně, nelze chápat tak, že se jedná o vyjádření osoby, dokonce i když králík nebo kachna mají povahové rysy, které jsou zřetelně lidské. Na druhé straně mnoho kreslených postav, ačkoli ne všechny, jsou kresleny, aby se podobaly skutečné lidské existenci. V případě, že se kreslená postava odchyluje od ztvárnění člověka, je nutné posoudit, zda se stále ještě jedná o zobrazení osoby, a zda je způsobilé založit trestný čin. Nejvyšší soud připustil, že kreslená postava, která se bude odchylovat od ztvárnění člověka, může být zobrazením osoby ve smyslu zákonné definice, avšak je nutné, aby zde byla přinejmenším nějaká podobnost lidské podoby. Pouhý symbol by ztvárněním osoby nebyl.

Pokud jde o posuzování významu slova „osoba" z pohledu State legislation, vychází se z definice dětské pornografie, která používá pojem „zobrazuje nebo popisuje" (depicts or describes). Při zavádění State legislation bylo konstatováno, že zobrazení nebo popis dítěte v sexuálním kontextu je široká kategorie, která by měla pokrýt jednak situace, ve kterých je dítě zobrazeno v nemravné pozici nebo sledující jinou osobu zabývající se sexuální aktivitou. Požadavek, že materiál musí za všech okolností pohoršovat rozumné osoby zajistí, že nevinné rodinné fotografie nahých dětí

[161] Fiktivní = vymyšlený, existující jen v příbězích; imaginární = smyšlený, existující pouze v mysli či vlastní představivosti. Oxford University Press - OALD dictionary. Dostupný z: http://www.oup.com/elt/catalogue.

nebudou považovány za dětskou pornografii. Rovněž je pod tuto definici zařazován materiál, ve kterém je dítě obětí mučení, krutého nebo psychického zneužívání, i když se nejedná o čistě sexuální zneužívání, přesto však je takové jednání považováno za pohoršující. Nejvyšší soud se přiklonil k názoru, že slovo získává svůj význam až v daném kontextu, přičemž kontextem State legislation je ochrana dítěte před sexuálním vykořisťováním a zneužíváním. Na základě toho bylo konstatováno, že pojem osoba je v tomto kontextu způsobilá nejen k označení osoby skutečné, ale i fiktivní. V daném případě musí být kresba lidskou bytostí a jako taková musí být i rozpoznatelná, přičemž odklon od skutečnosti nemusí nutně znamenat, že nejde o zobrazení osoby v tomto smyslu. Jelikož je však zobrazení osoby základním znakem trestného činu, musí být prokázáno nade vší pochybnost. I zde bylo zdůrazněno, že pouhé přiřazovaní lidských vlastností králíkovi, kachně nebo květině, by bylo nedostačující, pokud by i nadále subjektem zůstal králík, kachna nebo květina. Z toho vyplývá, že fiktivní kreslené postavy, dokonce i ty, které se odlišují od rozpoznatelné lidské podoby, můžou být vyobrazením ve smyslu Crime Act.

Z výše uvedeného vyplývá závěr Nejvyššího soudu, že slovo „osoba“ (v rámci obou trestných činů) zahrnuje fiktivní nebo imaginární postavy a pouhý fakt, že postava je zobrazena odlišně od skutečného znázornění lidské bytosti, neznamená, že by taková postava nebyla osobou. Postavy v posuzovaném materiálu byly skutečně zobrazením osob ve smyslu zákonných definic. Za zmínku dále stojí, že v předmětném rozhodnutí Nejvyšší soud uvedl předchozí rozhodnutí ve věci Holland v. The Queen, v němž byl vyjádřen rozdíl mezi psaným dílem a dílem, jehož podstatou je zobrazení. V případě písemného díla nebude žádný rozdíl mezi tím, jestli spisovatel popisuje osobu, která je skutečná či nikoliv, neboť tento proces nevyžaduje přítomnost či dokonce existenci žádné skutečné osoby. V psaném díle není žádná osoba zobrazena, ale je popsána ve slovech. Psaný popis oku pozorovatele nikdy neposkytuje skutečně žijící osobu, může pouze předkládat její popis, přičemž osobou, která je v díle vylíčena, může být jak osoba skutečná, tak i osoba fiktivní nebo imaginární. Význam rozlišování mezi osobou skutečnou a fiktivní je základní pro zobrazení. Dostupné důkazy ukazují, že jednoznačné sexuální materiály mohou být škodlivé, ať už zobrazují skutečné dítě či nikoli, a to zejména z důvodu, že s rostoucí stupněm technologického pokroku může být

velice obtížné rozeznat skutečnou osobu od počítačové tvorby (výtvoru) nebo kompozice.

V rámci případu Simpsonovi měl být demonstrován vztah jiných států k virtuální dětské pornografii, zvláště pak skutečnost, že i v praxi dochází k rozšiřování pojmu osoby z právního hlediska.

4.5. Sexuální lekce pro mladé dívky

Posledním virtuálním příkladem, který bych ráda zmínila, je případ okresního soudu v Holandsku (Distrikt Court of ´s-Hertogenbosch) z roku 2008[162], jehož pachatel byl odsouzen k podmíněnému trestu odnětí svobody, přičemž zkušební dobu soud stanovil na 10 let.[163] V minutovém klipu nazvaném „Sexuální lekce pro mladé dívky" (Sex lessons for young girls) bylo ukázáno, jak virtuální dívka provádí manuální sex na dospělé (rovněž virtuální) osobě. Animace byla zaměřena na mladé dívky a měla sloužit jako návod. Po dosažení orgasmu dospělého virtuálního muže se dívka usmívá do kamery, spustí se lavina nafukovacích balónků a muž tleská. Tato atmosféra animace měla demonstrovat, že se jedná o zábavnou činnost, kterou mladé dívky mohou provozovat. Otázka, která byla předmětem rozhodování, zněla, zda se jedná o realistické zobrazení neexistujícího dítěte, jak uvádí Úmluva o kybernetické kriminalitě[164] a holandský trestní zákoník.[165]

Holandský trestní zákoník byl v roce 2002 novelizován. Z důvodové zprávy k trestnímu zákoníku vyplývá, že novela měla za cíl rozšířit čl. 240b o virtuální dětskou pornografii, což bylo učiněno včleněním pojmu „zdánlivý účastník". Vláda v předmětném ustanovení záměrně ponechala slovo „zdánlivě" (se zřetelem na věk), poněvadž důkaz týkající se věku virtuální osoby není možný podat, neboť ta žádný opravdový věk nemá. Odhad věku zobrazené osoby pak musí být proveden se zřetelem na všechny tělesné

[162] BC3225, Rechtbank 's-Hertogenbosch , 01/845400-07. Dostupný z: www.rechtspraak.nl/ljn.asp?ljn= BC3225.

[163] Nutno dodat, že pachatel byl stíhán současně za trestný čin ohrožování mravnosti a pohlavního zneužívání.

[164] Holandsko Úmluvu o kybernetické kriminalitě podepsalo dne 23.11.2001, ratifikována byla dne 16.11.2006 a v účinnost vstoupila dne 1.3.2007.

[165] Čl. 240b (Artikel 240b Wetboek van Strafrecht).

znaky (včetně pohlavních), které jediné mohou naznačovat věk této osoby. K posouzení „zdánlivé účasti“ ve virtuální pornografii je dle důvodové zprávy postačující, že se zobrazená osoba podobá opravdovému dítěti. Naproti tomu se dají vyloučit zobrazení, na nichž je ihned patrné, že se jedná o upravovaná nerealistická zobrazení či o kreativní výtvor lidského ducha, a které tudíž nespadají pod čl. 240b. V daném případě byl věk virtuální dívky odhadnut podle tělesných znaků, konkrétně podle nevyvinutých prs, ochlupení a nedorostlé postavy. Na základě toho soud konstatoval, že v animaci se jedná o virtuální dívku takřka pubertálním věku, která však nedosáhla věku 18 let. Z hlediska virtuální dětské pornografie je v Holandsku důvodem trestního postihu nejen ochrana vyobrazených mladistvých, ale i ochrana proti jednání, které může děti povzbudit nebo svést k tomu, aby se zúčastnili sexuálního chování nebo jednání, které je určeno pro subkulturu, která sexuální zneužívání dětí podporuje. V předmětné kauze soud usoudil, že dospělá osoba je sice schopná rozeznat zobrazené chování a osoby od pravých, avšak průměrné dítě tohoto schopno není.

Tento případ nám naznačuje pohled úvahy soudu, jak lze v konkrétních situacích z hmotněprávního a procesního hlediska postupovat. Posuzování věku virtuálních osob by ve zřejmých případech nemělo činit problémy, příp. je možné si vyžádat odborné vyjádření či znalecký posudek. Soud rovněž do popředí postavil velice významnou otázku, a to objekt virtuální dětské pornografie. Ochrana byla poskytnuta jednak proti jednáním, která děti v souvislosti se svou rozumovou vyspělostí nemusí vždy zcela chápat, resp. správně posoudit či vyvodit si správný úsudek v této věci, jednak samotným vyobrazeným mladistvým.

Závěr

Informační technologie díky jejich globálnímu a neudržitelnému rozvoji představují v dnešní společnosti běžnou součást každodenního života většiny lidí. Vedle výhod, které s sebou tento rozmach přináší, však na druhé straně stojí řada nevýhod a problému s tím spojených. Kyberprostor jako prostředí bez reálného času a prostoru, který nemá omezené hranice a lze se v něm „pohybovat“ bez jakékoliv kontroly, skýtá rovněž útočiště pro širokou škálu negativních společensky škodlivých jednání. Tato negativní jednání jsou relativně nová a ve většině případů z hlediska trestního práva také těžko postižitelná právní úpravou. Důvodem této skutečnosti jsou především charakteristické rysy virtuálního prostředí (globálnost, reálná neomezenost, rychlost, anonymita apod.), které ztěžují jeho samotné poznání a vyjasnění specifik, a to i pro řadu odborníků pohybujících se v dané oblasti. Tato negativa především znesnadňují běžný vyšetřovací postup orgánů činných v trestním řízení.

Virtuální prostředí představuje nové odvětví, které není jednoduché poznat. Má svá specifika a zavádí zcela novou terminologii, se kterou se musí seznámit i právní odvětví. Tato skutečnost je důvodem, proč se kyberprostor dostává do právního povědomí relativně těžce a proč je na něj zaměřeno tak málo právních odborníků. Na druhé straně však existuje nová právní generace, jenž se na toto odvětví zaměřuje a přináší s sebou nový pohled, který pomůže přizpůsobit české zákonodárství dané problematice.

Případové studie byly zaměřeny na zahraniční kauzy, které nám měly ukázat přístup některých států k problematice virtuálních trestných činů. Zároveň měly otevřít nový obzor, který je pro naše právní prostředí neznámý a řekněme, že i nepředstavitelný, neboť v současné době neshledáváme právní zájem na postihu některých škodlivých jednání, která jsou ve světě podrobena určité míře regulace.

V současné době je nutné v České republice přistoupit k určité „technializaci“ trestněprávních norem a reagovat na celosvětovou právní otevřenost k informačním technologiím. Základem bude překonání rigidnosti českého právního řádu, snaha přizpůsobit se vyvíjející se době vzhledem k rozsáhlosti a dostupnosti informačních

technologií a jejich rostoucímu zneužívání při páchání trestné činnosti, včetně zavádění nových pojmů, popř. rozšiřování významu pojmů již zažitých a běžně používaných. Česká republika by měla být připravena k řešení konkrétních problémů, s kterými se již některé státy světa potýkají. V trestním právu by proto měly být stanoveny určité mantinely, které by dovolovaly na danou problematiku reagovat a nezaostávat za světovým standardem.

Seznam zkratek

ČR	Česká republika
ESLP	Evropský soud pro lidská práva
EU	Evropská unie
MMORPG	**M**assive(ly)-**M**ultiplayer **O**nline **R**ole-**P**laying **G**ame
Nizozemský trestní zákoník	Wetboek van Strafrecht <http://www.wetboek-online.nl/wet/Sr.html>
Občanský zákoník	Zákon č. 40/1964 Sb., občanský zákoník, v platném znění
Trestní řád	Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), v platném znění
Trestní zákon	Zákon č. 140/1961 Sb., trestní zákon, v platném znění
Trestní zákoník	Zákon č. 40/2009 Sb., trestní zákoník, v platném znění

Použitá literatura

Acta universitatis carolinae – Iuridica 4, 2008

Akademický slovník cizích slov, I. díl A-K. Academia Praha 1995

Bartoň, M.: Virtuální pornografie, limity svobody umělecké tvorby a svobody projevu a trestní zákon. Právní rozhledy, 2008. roč. 16, č. 17

Berger, P., L. Luckmann, T. *Sociální konstrukce reality.* Praha: Centrum pro studium demokracie a kultury, 1999

Císařová, D., Fenyk, J., Gřivna, T. a kol. *Trestní právo procesní.* 5. vydání. Praha: ASPI, 2008

Čech, P., Pavela, L. Obchodní společnost jako osoba blízká? Právní rádce, 2007, č. 1

Gřivna, T. K ustanovením Úmluvy o počítačové kriminalitě. In: Gřivna, T., Polčák, R. (eds.). Kyberkriminalita a právo. Praha: Auditorium, 2008

Gřivna, T. Trestné činy proti lidské důstojnosti v sexuální oblasti v novém trestním zákoníku. Bulletin advokacie, 2009, č. 10

Gřivna, T. Závazky k ochraně kyberprostoru vyplývající z evropského a mezinárodního práva. In: Acta universitatis carolinae – Iuridica 4, 2008

Gřivna, T. Závazky k ochraně kyberprostoru vyplývající z evropského a mezinárodního práva. In: Acta universitatis carolinae – Iuridica 4, 2008, str. 21-34.

Gřivna, T., Polčák, R. (eds.). Kyberkriminalita a právo. Praha: Auditorium, 2008

Havlena, O. Komunikace virtuálně – Masarykova Univerzita a Second Life. Brno, 2009

Herczeg, J. Dodatkový protokol k Úmluvě o počítačové kriminalitě. In: Gřivna, T., Polčák, R. (eds.). Kyberkriminalita a právo. Praha: Auditorium, 2008.

Herczeg, J. Virtuální dětská pornografie: Zločin bez oběti? In Vanduhová, V., Gřivna, T. (eds.).: Pocta Otovi Novotnému k 80. narozeninám. ASPI, Wolters Kluwer, Praha 2008

Jelínek, J a kol. Trestní právo hmotné. 3.přepracované a aktualizované vydání, Linde Praha, Praha 2008

Jelínek, J. a kol.: *Trestní právo hmotné.* 1. vydání. Praha: Leges, 2009

Kuchta, J., Válková, H. a kol. Základy kriminologie a trestní politiky. 1. vydání. Praha: C. H. Beck, 2005

Musil, S. Počítačová kriminalita. Nástin problematiky. Institut pro kriminologii a sociální prevenci, Praha 2000

Novotný, O., Vanduchová, M., Šámal, P. a kol. *Trestní právo homotné. Obecná část.* 6. vydání, Praha: Wolters Kluwer ČR, a.s., 2010

Pocta Otovi Novotnému k 80.narozeninám. Praha: ASPI, Wolters Kluwer, 2008

Polčák, R. K problémům působnosti trestního práva na internetu. In Acta universitatis carolinae – Iuridica 4, 2008

Polčák, R., Škop, M., Macek, J. *Normativní systémy v kyberprostoru.* Masarykova univerzita, Brno, 2005

Poremská, M.: Pornografie v USA. In Trestněprávní revue, č. 8/2008

Šámal, P. a kol. Trestní zákoník I. § 1 až 139. Komentář. 1. vydání. Praha: C. H. Beck, 2010

Šámal, P. a kol. Trestní zákoník II. § 140 až 421. Komentář. 1. vydání. Praha: C. H. Beck, 2010

Švestka, J., Spáčil, J., Škárová, M., Hulmák, M. a kol. Občanský zákoník I, II, 2. vydání, Praha 2009

Telec, I. Tůma, P. Autorský zákon. Komentář. 1.vydání. Praha: C. H. Beck, 2007

Volevecký, P., Šubrt, M.: Dětská pornografie jako kybernetický trestný čin ve světle Úmluvy o počítačové kriminalitě. Trestní právo, roč. 2009, č. 4

Završnik, A. Definiční problémy a kriminologická specifika kyberzločinu. In: Gřivna, T., Polčák, R. (eds.). Kyberkriminalita a právo. Praha: Auditorium, 2008, str. 26-48.

Acta universitatis carolinae – Iuridica 4, 2008

Akademický slovník cizích slov, I. díl A-K. Academia Praha 1995

Bartoň, M.: Virtuální pornografie, limity svobody umělecké tvorby a svobody projevu a trestní zákon. Právní rozhledy, 2008. roč. 16, č. 17

Berger, P., L. Luckmann, T. *Sociální konstrukce reality.* Praha: Centrum pro studium demokracie a kultury, 1999

Císařová, D., Fenyk, J., Gřivna, T. a kol. *Trestní právo procesní.* 5. vydání. Praha: ASPI, 2008

Čech, P., Pavela, L. Obchodní společnost jako osoba blízká? Právní rádce, 2007, č. 1

Gřivna, T. K ustanovením Úmluvy o počítačové kriminalitě. In: Gřivna, T., Polčák, R. (eds.). Kyberkriminalita a právo. Praha: Auditorium, 2008

Gřivna, T. Trestné činy proti lidské důstojnosti v sexuální oblasti v novém trestním zákoníku. Bulletin advokacie, 2009, č. 10

Gřivna, T. Závazky k ochraně kyberprostoru vyplývající z evropského a mezinárodního práva. In: Acta universitatis carolinae – Iuridica 4, 2008

Gřivna, T. Závazky k ochraně kyberprostoru vyplývající z evropského a

mezinárodního práva. In: Acta universitatis carolinae – Iuridica 4, 2008, str. 21-34.

Gřivna, T., Polčák, R. (eds.). Kyberkriminalita a právo. Praha: Auditorium, 2008

Havlena, O. Komunikace virtuálně – Masarykova Univerzita a Second Life. Brno, 2009

Herczeg, J. Dodatkový protokol k Úmluvě o počítačové kriminalitě. In: Gřivna, T., Polčák, R. (eds.). Kyberkriminalita a právo. Praha: Auditorium, 2008.

Herczeg, J. Virtuální dětská pornografie: Zločin bez oběti? In Vanduhová, V., Gřivna, T. (eds.).: Pocta Otovi Novotnému k 80. narozeninám. ASPI, Wolters Kluwer, Praha 2008

Jelínek, J a kol. Trestní právo hmotné. 3.přepracované a aktualizované vydání, Linde Praha, Praha 2008

Jelínek, J. a kol.: *Trestní právo hmotné.* 1. vydání. Praha: Leges, 2009

Kuchta, J., Válková, H. a kol. Základy kriminologie a trestní politiky. 1. vydání. Praha: C. H. Beck, 2005

Musil, S. Počítačová kriminalita. Nástin problematiky. Institut pro kriminologii a sociální prevenci, Praha 2000

Novotný, O., Vanduchová, M., Šámal, P. a kol. *Trestní právo homotné. Obecná část.* 6. vydání, Praha: Wolters Kluwer ČR, a.s., 2010

Pocta Otovi Novotnému k 80.narozeninám. Praha: ASPI, Wolters Kluwer, 2008

Polčák, R. K problémům působnosti trestního práva na internetu. In Acta universitatis carolinae – Iuridica 4, 2008

Polčák, R., Škop, M., Macek, J. *Normativní systémy v kyberprostoru.* Masarykova univerzita, Brno, 2005

Poremská, M.: Pornografie v USA. In Trestněprávní revue, č. 8/2008

Šámal, P. a kol. Trestní zákoník I. § 1 až 139. Komentář. 1. vydání. Praha: C. H. Beck, 2010

Šámal, P. a kol. Trestní zákoník II. § 140 až 421. Komentář. 1. vydání. Praha: C. H. Beck, 2010

Seznam příloh

Příloha č. 1 :

Systematika trestných činů obsažených v Úmluvě o kybernetické kriminalitě

1. Trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů
    a. Neoprávněný přístup (čl. 2)
    b. Neoprávněné zachycení informací (čl. 3)
    c. Zásah do dat (čl. 4)
    d. Zásah do systému (čl. 5)
    e. Zneužití zařízení (čl. 6)

2. Trestné činy související s počítači
    a. Falšování údajů související s počítači (čl. 7)
    b. Podvod související s počítači (čl. 8)

3. Trestné činy související s obsahem
    a. Trestné činy souvisejíc s dětskou pornografií (čl. 9)

4. Trestné činy související s porušením autorského práva a práv příbuzných autorskému právu
    a. Trestné činy související s porušením autorského práva a práv příbuzných autorskému právu

Příloha č. 2 :

Český trestní zákoník – vybrané trestné činy

Hlava II.
TRESTNÉ ČINY PROTI SVOBODĚ A PRÁVŮM NA OCHRANU OSOBNOSTI, SOUKROMÍ A LISTOVNÍHO TAJEMSTVÍ

Díl 1
Trestné činy proti svobodě

§ 173
Loupež

(1) Kdo proti jinému užije násilí nebo pohrůžky bezprostředního násilí v úmyslu zmocnit se cizí věci, bude potrestán odnětím svobody na dvě léta až deset let.
(2) Odnětím svobody na pět až dvanáct let bude pachatel potrestán,
a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny,
b) způsobí-li takovým činem těžkou újmu na zdraví,
c) způsobí-li takovým činem značnou škodu, nebo
d) spáchá-li takový čin v úmyslu umožnit nebo usnadnit spáchání trestného činu vlastizrady (§ 309), teroristického útoku (§ 311) nebo teroru (§ 312).
(3) Odnětím svobody na osm až patnáct let bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu.
(4) Odnětím svobody na deset až osmnáct let bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 smrt.
(5) Příprava je trestná.

Díl 2
Trestné činy proti právům na ochranu osobnosti, soukromí a listovního tajemství

§ 182
Porušení tajemství dopravovaných zpráv

(1) Kdo úmyslně poruší tajemství

a) uzavřeného listu nebo jiné písemnosti při poskytování poštovní služby nebo přepravované jinou dopravní službou nebo dopravním zařízením,
b) datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli, který zprávu přijímá, nebo
c) neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková počítačová data,

bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.

(2) Stejně bude potrestán, kdo v úmyslu způsobit jinému škodu nebo opatřit sobě nebo jinému neoprávněný prospěch

a) prozradí tajemství, o němž se dozvěděl z písemnosti, telegramu, telefonního hovoru nebo přenosu prostřednictvím sítě elektronických komunikací, který nebyl určen jemu, nebo
b) takového tajemství využije.

(3) Odnětím svobody na šest měsíců až tři léta nebo zákazem činnosti bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny,
b) spáchá-li takový čin ze zavrženíhodné pohnutky,
c) způsobí-li takovým činem značnou škodu, nebo
d) spáchá-li takový čin v úmyslu získat pro sebe nebo pro jiného značný prospěch.

(4) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako úřední osoba,
b) způsobí-li takovým činem škodu velkého rozsahu, nebo
c) spáchá-li takový čin v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu.

(5) Zaměstnanec provozovatele poštovních služeb, telekomunikační služby nebo počítačového systému anebo kdokoli jiný vykonávající komunikační činnosti, který

a) spáchá čin uvedený v odstavci 1 nebo 2,
b) jinému úmyslně umožní spáchat takový čin, nebo
c) pozmění nebo potlačí písemnost obsaženou v poštovní zásilce nebo dopravovanou dopravním zařízením anebo zprávu podanou neveřejným přenosem počítačových dat, telefonicky, telegraficky nebo jiným podobným způsobem,

bude potrestán odnětím svobody na jeden rok až pět let, peněžitým trestem nebo zákazem činnosti.

(6) Odnětím svobody na tři léta až deset let bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 5 škodu velkého rozsahu, nebo
b) spáchá-li takový čin v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu.

Hlava V.
TRESTNÉ ČINY PROTI MAJETKU

§ 205
Krádež

(1) Kdo si přisvojí cizí věc tím, že se jí zmocní, a
a) způsobí tak na cizím majetku škodu nikoliv nepatrnou,
b) čin spáchá vloupáním

c) bezprostředně po činu se pokusí uchovat si věc násilím nebo pohrůžkou bezprostředního násilí,
d) čin spáchá na věci, kterou má jiný na sobě nebo při sobě, nebo
e) čin spáchá na území, na němž je prováděna nebo byla provedena evakuace osob,

bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Kdo si přisvojí cizí věc tím, že se jí zmocní, a byl za čin uvedený v odstavci 1 v posledních třech letech odsouzen nebo potrestán, bude potrestán odnětím svobody na šest měsíců až tři léta.

(3) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 nebo větší škodu.

(4) Odnětím svobody na dvě léta až osm let bude pachatel potrestán,
a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny,
b) spáchá-li takový čin za stavu ohrožení státu nebo za válečného stavu, za živelní pohromy nebo jiné události vážně ohrožující život nebo zdraví lidí, veřejný pořádek nebo majetek, nebo
c) způsobí-li takovým činem značnou škodu.

(5) Odnětím svobody na pět až deset let bude pachatel potrestán,
a) způsobí-li činem uvedeným v odstavci 1 nebo 2 škodu velkého rozsahu, nebo
b) spáchá-li takový čin v úmyslu umožnit nebo usnadnit spáchání trestného činu vlastizrady (§ 309), teroristického útoku (§ 311) nebo teroru (§ 312).

(6) Příprava je trestná.

§ 230
Neoprávněný přístup k počítačovému systému a nosiči informací

(1) Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Kdo získá přístup k počítačovému systému nebo k nosiči informací a

a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,
b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,
c) padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo
d) neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat,

(3) bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(3)Odnětím svobody na šest měsíců až tři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 nebo 2

a) v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch, nebo
b) v úmyslu neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat.

(4)Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny,
b) způsobí-li takovým činem značnou škodu,
c) způsobí-li takovým činem vážnou poruchu v činnosti orgánu státní správy, územní samosprávy, soudu nebo jiného orgánu veřejné moci,
d) získá-li takovým činem pro sebe nebo pro jiného značný prospěch, nebo
e) způsobí-li takovým činem vážnou poruchu v činnosti právnické nebo fyzické osoby, která je podnikatelem.

(5)Odnětím svobody na tři léta až osm let bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 1 nebo 2 škodu velkého rozsahu, nebo
b) získá-li takovým činem pro sebe nebo pro jiného prospěch velkého rozsahu.

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

(1)Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 180 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 228 odst. 1, 2 vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává

a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo
b) počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačového systému nebo jeho části,

bude potrestán odnětím svobody až na jeden rok, propadnutím věci nebo jiné majetkové hodnoty nebo zákazem činnosti.

(2) Odnětím svobody až na tři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny, nebo
b) získá-li takovým činem pro sebe nebo pro jiného značný prospěch.

(3) Odnětím svobody na šest měsíců až pět let bude pachatel potrestán, získá-li činem uvedeným v odstavci 1 pro sebe nebo pro jiného prospěch velkého rozsahu.

§ 232

Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

(1) Kdo z hrubé nedbalosti porušením povinnosti vyplývající ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté

a) data uložená v počítačovém systému nebo na nosiči informací zničí, poškodí, pozmění nebo učiní neupotřebitelnými, nebo
b) učiní zásah do technického nebo programového vybavení počítače nebo jiného technického zařízení pro zpracování dat,

a tím způsobí na cizím majetku značnou škodu, bude potrestán odnětím svobody až na šest měsíců, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu.

Příloha č. 3:

Nizozemský trestní zákoník – vybrané trestné činy

Hlava V.
PŘEČINY PROTI VEŘEJNÉMU POŘÁDKU

Čl. 138a
Porušení počítačové svobody (zásah do počítačového systému)

1. Trestem odnětí svobody až na šest měsíců nebo peněžním trestem třetí kategorie bude za porušení počítačové svobody potrestán ten, kdo úmyslně protiprávně pronikne do automatizovaného systému k ukládání a zpracování dat, nebo do jeho části, jestliže:
   a) přitom pronikne jakýmkoli zabezpečením, nebo
   b) si přístup získá technickým zásahem, pomocí falešných signálů, paklíčem nebo pod falešnou totožností.
2. Trestem odnětí svobody až na čtyři roky nebo peněžním trestem čtvrté kategorie bude potrestáno porušení počítačové svobody, jestliže pachatel data uložená v automatizovaném systému, v němž se nezákonně nachází, pro sebe či jiného převezme, odposlechne nebo zaznamená.
3. Trestem odnětí svobody až na čtyři roky nebo peněžním trestem čtvrté kategorie bude potrestáno porušení počítačové svobody spáchané prostřednictvím veřejné telekomunikační sítě, jestliže pachatel poté:
   a) využije kapacity automatizovaného systému se záměrem se nezákonně obohatit;
   b) prostřednictvím automatizovaného systému, do něhož pronikl, získá přístup do automatizovaného systému třetích osob.

Hlava XXII.
KRÁDEŽ

Čl. 310
Krádež

Kdo odcizí majetek, který zcela nebo zčásti náleží jinému, se záměrem si jej nezákonně přivlastnit, bude obviněn z krádeže a potrestán trestem odnětím svobody až na čtyři roky nebo peněžním trestem čtvrté kategorie.

Čl. 311
Krádež za přitěžujících okolností

1. Trestem odnětí svobody až na šest let nebo peněžním trestem čtvrté kategorie bude potrestána:
   a) krádež dobytka z pastvy;

b) krádež u příležitosti požáru, výbuchu, povodně, ztroskotání, leteckého či železničního neštěstí, nepokojů, vojenské vzpouře nebo ohrožení válkou;
c) krádež v době nočního klidu, v obydlí nebo na uzavřeném pozemku, na němž se obydlí nachází, spáchaná osobou, která se v těchto místech zdržuje bez vědomí nebo proti vůli oprávněné osoby;
d) krádež ve spolčení dvou či více osob;
e) krádež, při níž pachatel pronikl na místo činu nebo odcizil majetek prostřednictvím vloupání, násilného vniknutí na cizí pozemek, paklíče, falešného příkazu nebo převleku.

2. Jestliže je krádež podle bodu 3 spáchána za okolností podle bodu 4 a 5, bude potrestána trestem odnětí svobody až na devět let nebo peněžním trestem páté kategorie.

Čl. 312
Loupež

1. Trestem odnětí svobody až na devět let nebo peněžním trestem páté kategorie bude potrestána krádež, které předchází, kterou provází nebo následuje násilí nebo pohrůžka násilím proti osobám se záměrem krádež připravit nebo usnadnit, nebo v případě přistižení při činu se záměrem zajistit sobě nebo dalším spolupachatelům únik nebo získání odcizeného majetku.
2. Trest odnětí svobody až na dvanáct let nebo peněžní trest páté kategorie bude uložen:
   a) jestliže je čin spáchán v době nočního klidu v obydlí nebo na uzavřeném pozemku, na němž se obydlí nachází, anebo v jedoucím vlaku;
   b) jestliže je čin spáchán ve spolčení dvou a více osob;
   c) jestliže pachatel pronikl na místo činu nebo odcizil majetek prostřednictvím vloupání, násilného vniknutí na cizí pozemek, paklíče, falešného příkazu nebo převleku;
   d) jestliže má čin za následek těžkou újmu na zdraví.
3. Trest odnětí svobody až na patnáct let nebo peněžní trest páté kategorie bude uložen, jestliže má čin za následek smrt.

Abstract

Virtual crimes are a new specific area in the law system, which is associated with information technologies (mobile, Internet etc.). These are crimes that can be committed in cyberspace or in connection with it. Generally, cyberspace can be defined from different perspectives most often as social, technological and legal environment in which there is mutual interaction of its users. This environment, in particular the Internet, due to its characteristics such as unlimited local, speed, low cost and anonymity, allowing the perpetrators to commit very serious harmful act. It is important that these negotiations are subject to certain legal regulations.

This thesis provides a basic overview of the subject, defines the concept of virtual crime and his characters - an object, objective side, the person (body) and the subjective side. The thesis also contains case studies which demonstrates solutions to this problem in the practice of foreign countries with different rules.

Legal regulation is important in terms of international standards, for example United Nations, Council of Europe and the European Union. There are a multitude of important legal documents, a leading position occupies Convention of Cybercrime. The issue of virtual environment and crimes is at the beginning and it involves many unresolved issues. It is important that states doesn´t leave this problem and they have begun to address it effectively.

Key words: virtual crime, cyberspace, Internet