Univerzita Karlova v Praze

Právnická fakulta

Katedra trestního práva

INTERNETOVÁ A POČÍTAČOVÁ KRIMINALITA

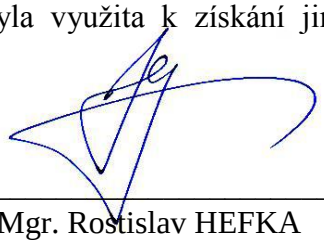
Diplomová práce

Mgr. Rostislav HEFKA

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

Datum vypracování práce (uzavření rukopisu): **29. března 2016**

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



V Praze dne 29. března 2016

Mgr. Rostislav HEFKA

Poděkování:

Chtěl bych tímto poděkovat vedoucímu své diplomové práce doc. JUDr. Bc. Tomáši Gřivnovi, Ph.D. za jeho cenné rady, připomínky, čas a také za ochotu, vstřícnost a vřelý vztah a porozumění k mé osobě při tvorbě této práce. Také bych chtěl velmi poděkovat své přítelkyni Veronice Blahnové za celkovou podporu při psaní práce a za závěrečnou slohovou korekturu.

Obsah

Úvod

Jako každý student vysoké školy, který si přeje, aby mohl úspěšně absolvovat, jsem se i já dostal do fáze studia, kdy bylo nutné zvolit jak oblast, tak i konkrétní téma diplomové práce, kterou bych mohl předložit a obhájit. Volba dané práce samozřejmě není snadná, přesto si dovolím tvrdit, že přinejmenším o oblasti práva, kterou bych se chtěl zabývat – právo trestní, jsem měl jasno již od prvního ročníku. Zbývalo mi tedy snad to lehčí, a to vybrat z nabízených témat dané katedry to, které by mi bylo svým oborem blízké, bylo nějakým způsobem zajímavé a aktuální, a které bych mohl studovat do hloubky včetně problematiky s ním spojené. Také vzhledem k tomu, že jsem již v minulosti na jiné vysoké škole měl téma diplomové práce spojené s internetem a počítači, více než patnáct let podnikám v oblasti informačních technologií a o internet a počítače se zajímám skutečně důkladně, nemohl jsem z nabízených témat zvolit žádné jiné, než právě téma „Internetová a počítačová kriminalita".

Téma jsem si tedy zvolil. Je to téma moderní, hodně aktuální, neboť informační a komunikační technologie jsou neoddělitelnou součástí našeho života v moderní společnosti. Spolu s výhodami technologického pokroku se dostává do popředí také problematika s tím související, a ač chceme či ne, dotýká se *de facto* každého z nás. Nicméně hned na začátku musím uvést, že pokud bych chtěl práci věnovat celé vybrané problematice, nabízely by se dvě varianty. Mohl bych psát povrchně/okrajově o každém faktu spojeném s vybraným tématem, což by mohlo svými parametry vystačit pro diplomovou práci, nicméně z mého hlediska by se jednalo pouze o nástin a neshledal bych v tom smysl, kromě splnění zadaného úkolu. Nebo bych mohl jít do hloubky a každému problému se věnovat důkladně, přičemž by se mohlo jednat o zajímavou práci, avšak svými parametry by mnohonásobně překročila požadavky pro diplomovou práci a nemohl bych ji bohužel předložit k obhajobě. Také doba na vypracování by byla značná a bylo by náročné takovou práci dokončit. Nezbývalo nic jiného než se pokusit najít variantu třetí, která by dle mého mohla být hlubším pohledem, a přesto by splňovala parametry závěrečné práce. Proto jsem se rozhodl, že tuto práci věnuji jen určité oblasti počítačové kriminality, kterou se budu snažit dostatečně rozebrat a pokud možno zahrnout většinu otázek a vlivů, které se v dané oblasti projevují. Chtěl bych se věnovat

trestným činům, které souvisí s ***rozmnožováním a šířením audio a audiovizuálních děl na internetu,*** ale i jejich nelegálním kopiím na případných nosičích, se kterými je možné obchodovat. S tím souvisí i případné rozmnožování a stahování počítačových programů a počítačových systémů, opět včetně jejich obchodování ve formě fyzického nosiče dat. To však neznamená, že bych ostatní oblasti kyberkriminality nezmínil. Rád bych uvedl alespoň některé všeobecně známé a ty, které působí značné škody, či ty, jejichž potenciální obětí může být téměř kdokoli. Některé jsou totiž zcela nové, rozvíjející se a budou značnou hrozbou budoucnosti, což je zkrátka spojeno s rozvojem moderních informačních technologií. Nicméně text týkající se těchto oblastí nebude tak podrobný. Pouze bych je rád zmínil, vypíchl neproblematičtější body a pokusil se naznačit, jak by případně bylo možné danou kriminalitu alespoň částečně omezit. Je totiž jasné, že úplné vymýcení dané kriminality je dnes již nemožné.

Hlavním smyslem mé práce bude tedy oblast obchodování s filmy, jejich šíření a také zajímavý pohled na případné vyčíslení škody, která jako v každé jiné oblasti práva danou kriminalitou vzniká. Hlavně šíření těchto děl na internetu je velký problém dnešní doby. Fenoménem této oblasti je šíření filmů, které měly premiéru v kině, tam někdo tajně pořídil záznam a tento poskytl na internet. Daný snímek je tak prostřednictvím internetu celosvětově šířen. Přičemž je v mnoha zemích k dispozici mnohem dříve, než je vůbec uveden do kin. Škody jsou v těchto případech opravdu značné, neboť mnoho potenciálních návštěvníků daného filmu v tomto případě již nemá důvod kino navštívit a zaplatit vstupné, protože film si zdarma na internetu stáhnou a zhlédnou.

Musíme si však uvědomit, že internetová kriminalita, jako zvláštní druh počítačové kriminality, má svá specifika, která činí subjekty v ní zapojené jedinečnými a v mnoha případech i anonymními. Internet se jen stěží bude držet národních hranic. I toto by sice bylo technicky možné, avšak z pohledu jiného práva, např. svobody slova, je takové technické omezení nepoužitelné. Je tedy nutné pokusit se objasnit právní a technologické aspekty páchání internetové kriminality ve světle mezinárodních a národních právních dokumentů, jejího dosavadního vývoje a dopadů na společnost. Není tedy možné, abych ve své práci vystačil pouze se zákonem č. 40/2009 Sb., trestní zákoník – TZ. Bude tedy potřeba užít i jiné právní prameny, a to nejen z oblasti práva

veřejného, neboť mnohdy i soukromoprávní normy jsou pro řešení nezbytné. Často je nutné užití i norem zahraničních a případně i rozhodnutí SDEU. Z českých norem to v mém případě bude zejména Autorský zákon – AZ – č. 121/2000 Sb., jenž mnou vybranou oblast značně upravuje. Z hlediska páchání trestného činu je samozřejmě zásadní osoba pachatele, kterou může být jak fyzická osoba, tak dnes i osoba právnická. Proto budu využívat také zákon č. 418/2011 Sb., zákon o trestní odpovědnosti právnických osob a řízení proti nim – ZTOPO. Ani právo však není vše řešící a všespásné, proto bude vhodné také posouzení z hlediska jiného oboru, protože tento nešvar ovlivňuje velmi mnoho faktorů. Vzhledem k mému předchozímu studiu na VŠE nemohu opomenout ekonomický prvek a prvek užitku, který je mnohdy pro potencionálního pachatele tím „hnacím motorem“ nebo motivací pro to, aby daný trestný čin spáchal. Ekonomický prvek může souviset také s přecházením kriminality, což se pokusím v práci objasnit. I samotné aspekty kriminologie a kriminalistiky jsou pro danou oblast důležité, proto bych se rád částečně věnoval i případnému vyšetřování dané trestné činnosti, nebo její prevenci či dozoru.

Také bych v práci rád uvedl několik skutečných případů, které dané odvětví ovlivnily. Nebude se vždy jednat pouze o medializované kauzy, i když těchto bude většina. Již téměř rok pracuji jako stážista na Obvodním státním zastupitelství pro Prahu 3, kde pod dozorem vykonávám práci státního zástupce a kde jsem se nedávno setkal s poměrně zajímavým případem spadajícím do této oblasti. Nicméně daná kauza ke dni uzavření této práce doposud nebyla soudně projednána, a tak je bohužel možné zveřejnění jen některých okrajových informací, které jsou veřejně dohledatelné či mohou být získány na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím

V neposlední řadě bych chtěl v práci uvést statistiky kybernetické trestné činnosti a její vývoj. Alespoň některých činů, které jsou statisticky zaznamenávány, neboť u počítačových a internetových činů tomu prozatím není vždy a statistiky cílené na tuto oblast zatím chybí.

1 Vymezení základních pojmů

Aby bylo možné přistoupit k popisu jádra této práce, je nejdříve nutné uvést výčet alespoň těch nejzákladnějších pojmů, které jsou pro práci nezbytné a to spolu s jejich popisem či alespoň vysvětlením jejich významu.

1.1 Počítač

Počítač, toto slovo nebo pojem jsou dnes téměř každým na naší planetě běžně používány a to již od útlého dětství. Používáme jej v běžné i odborné mluvě pro označení určitého stroje, který má jisté vlastnosti. Co však tento pojem skutečně znamená? A kdy tento pojem vznikl? Co je tedy to, čemu dnes říkáme PC?

Pod pojmem počítač budeme pro účely této práce chápat každý programovatelný stroj, jenž může provést naprogramovaný seznam instrukcí a reagovat na vnější pokyny zadávané prostřednictvím vstupních zařízení, a který je schopen zpracovat tyto pokyny jako jistá data, jež přetvoří ve výsledky prezentující pomocí výstupních zařízení. Z tohoto důvodu budeme mezi potenciální předměty útoku zahrnovat veškerá programovatelná zařízení, ta jež jsou jako „počítač“ označována, avšak i zcela jiná zařízení, jež mohou být skryta v původně zcela nepočítačových strojích. Například dnes vyráběné automobily mají jako standardní výbavu zabudovaný počítač, na což jsme si již zvykli. „Počítačem“ ale bude v budoucnu vybaveno daleko více zařízení, například všechny domácí přístroje, což dneska ještě takovým standardem není a ne každý by v nich dnes počítač očekával. Za okamžik, od kterého je možné považovat stroj za počítač splňující uvedenou definici je zřejmě možné považovat rok 1945, kdy John von Neumann navrhl první počítač s uloženým programem. Tento návrh publikoval v článku „First Draft of a Report on the EDVAC“ a vytvořil tím jakousi koncepci, jež tvoří základ architektury i současných počítačů.[1]

Definic pojmu počítač je velmi mnoho, některé jsou si blízce podobné, jiné i částečně rozdílné, pro naše účely však bude uvedená definice postačovat a zkráceně vystačí, zapamatujeme-li si, že počítač je stroj na zpracování informací.

---

[1] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. Pro praxi. ISBN 978-80-7380-501-2. s. 22-23

Každý počítač se skládá ze dvou základních druhů komponentů, kterými jsou hardware a software. A jeden bez druhého je vlastně zbytečný, neboť sami o sobě bez spojení s druhým sice mohou existovat, avšak nemohou pracovat.

1.1.1 Hardware

Hardwarem bychom mohli zjednodušeně nazvat takové součásti počítače, jaké je možno fyzicky „osahat“. Mají tedy hmotnou povahu. Každý počítač se skládá z různých komponent a tyto se mohou lišit dle toho, zda se jedná o počítač osobní – nepřenosný – PC, přenosný – laptop či notebook, server nebo sálový, nicméně ve všech případech u nich nalezneme některá ze vstupních (klávesnice, myš, scanner, webová kamera apod.) a výstupních (monitor, tiskárna, reproduktor apod.) zařízení, jeden či více procesorů, operační paměť – RAM, disk – ROM, grafickou, síťovou a zvukovou kartu a napájecí zdroj a u mnoha i základní desku, která předchozí zařízení propojuje.[2] Každá z těchto komponent je samostatně nefunkční, neboť právě potřebuje propojení s ostatními, avšak ve spojení s ostatními tvoří funkční celek. Toto je i drobná slabina každého počítače, protože když je byť i jen jedna z těchto komponent vadná, stává se celek, tedy počítač, nefunkčním.

1.1.2 Software – programové vybavení

Software neboli programové vybavení je druhou nezbytnou složkou pro funkční a použitelný počítač. Je to vlastně sada všech počítačových programů používaných v počítači, které provádějí nějakou činnost. Také je možné užít definici negací, že softwarem počítače je vše, co není jeho hardwarem. Dle funkce můžeme software rozdělit na systémový (firmware, operační systém) a aplikační (kancelářské balíky, grafické programy, hry apod.) a dle finanční dostupnosti na freeware, shareware a komerční software. Software je nezbytný pro chod počítače a řeší určité úlohy ve spolupráci s uživatelem. Program jako takový vzniká při programování jakožto zápis algoritmu v nějakém programovacím jazyce. Program, jenž je spuštěn, označujeme jako proces.[2,3]

---

[2] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. Pro praxi. ISBN 978-80-7380-501-2. s. 23-25

[3] Software. In: *Wikipedia: the free encyclopedia* [online]. Wikimedia Foundation, 2015 [cit. 2016-02-15]. Dostupné z: https://cs.wikipedia.org/wiki/Software

Na rozdíl od hardwarového vybavení, které je z hlediska práva možné považovat za věc, je software, tedy programové vybavení počítače, v právním významu mnohem zajímavější. Pojmy software, program, programové vybavení se v českém právním řádu vyskytují hned v několika zákonech.

§ 2 odst. 2 AZ uvádí, že za dílo se považuje též počítačový program. Toto ustanovení je zpřesněno obecnou úpravou počítačového programu a to v ustanovení § 65 AZ. § 22 odst. 1 písm. g) bod 1 zákona č. 586/1992 Sb. ze dne 20. listopadu 1992 o daních z příjmů užívá pojmu počítačového programu (software). Dále je možné tento pojem nalézt např. v zákoně č. 207/2000 Sb., o ochraně průmyslových vzorů, zákoně č. 527/1990 Sb., 527/1990, zákoně 478/1992 Sb., o užitných vzorech, zákoně 106/1999 Sb., o užitných vzorech, zákoně 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů a mnoha jiných. I v současnosti účinný OZ tento pojem v § 1811 a § 1837 užívá, přičemž ve všech těchto zákonech se pojem vyskytuje a je používán, přestože nikde v daných zákonech není tento pojem definován. Z tohoto důvodu se dá předpokládat, že je tento pojem všeobecně známý a proto není definice třeba. Stejně tak je tomu i v předpisech EU, kde se definice vyskytuje pouze zřídka, ačkoli s pojmem se pracuje velmi hojně. Ve Směrnici Evropského parlamentu a Rady 2009/24/ES ze dne 23. 4. 2009 o právní ochraně počítačových programů se „počítačovým programem" rozumí programy v jakékoliv formě, včetně těch, které jsou součástí technického vybavení (hardware). Jiné zákony využívají pojmu „programové vybavení počítače", jako např. zákon č. 62/2003 Sb., o volbách do Evropského parlamentu a další, přestože použitý pojem také nedefinují.[4]

Také TZ obsahuje pojmy „počítačový program" nebo „programové vybavení počítače" viz ustanovení § 103, § 120, § 231, § 232, § 236, § 264, § 267, § 348 a to opět bez jejich vymezení.

1.2 Pojem a definice kyberkriminality a kyberzločinu

Český právní řád pojem kyberkriminalita nikde nedefinuje a tak ji vlastně ani nezná a to i přesto, že se o ní hovoří čím dál častěji. I v právní teorii byl tento pojem s určitými výhradami akceptován až na základě mezinárodního vlivu Úmluvy o

[4] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. Pro praxi. ISBN 978-80-7380-501-2. s. 28

počítačové kriminalitě ze dne 23.11.2001, kterou Česká republika podepsala v roce 2005, nicméně k samotné ratifikaci došlo až v srpnu 2013 a účinnosti v našem právní řádu nabyl tento dokument 1. prosince 2013. Dřívější odborné debaty k vymezení toho správného názvu začínaly na základních pojmech „počítačová kriminalita“ a „internetová kriminalita“, kdy později byl používán přesnější pojem „informační kriminalita“ až po dnešní moderní název „kybernetická kriminalita“ či jinak „kybernalita“.[5,6]

Kybernetická kriminalita je poměrně nový interdisciplinární obor, jenž se zabývá nelegálními a závadnými činnostmi v kyberprostoru, které jsou založeny na použití nebo zneužití počítačové technologie. Kybernetická kriminalita vznikla až v okamžiku, kdy se na trh dostaly osobní počítače dostupné pro obyčejné lidi a k jejich dennímu užívání. Druhým, a patrně ještě důležitějším okamžikem, byl vznik počítačových sítí, zejména internetu a také možnosti vzdáleného přístupu k počítačům. Tímto vznikla poměrně unikátní situace, ve srovnání s do té doby běžně páchanou trestnou činností, neboť pachatel a oběť se mohou nacházet na zcela jiných místech od sebe vzdálených třeba i přes půl zeměkoule, což je fakt, který velmi stěžuje případné odhalení daného pachatele. Kybernetickou kriminalitou, neboli kybernalitou lze tedy rozumět páchání kybernetických trestných činů – kyberzločinů. Může být namířena přímo proti počítačům, proti datům apod. či může spočívat v použití počítačů jakožto prostředníka k páchání tradiční formy kriminality či je možné využít počítačovou síť jako prostředí, kde se kriminalita odehrává nebo k jejímu usnadnění. Jedná se o nemorální a neoprávněné jednání, jenž zahrnuje zneužití údajů získaných prostřednictvím informačních a komunikačních technologií nebo jejich změnu.[7,8,9,10]

---

[5] DUBENSKÁ, Petra. *Internetová a počítačová kriminalita*. Praha, 2013. Diplomová práce. PF UK. Vedoucí práce Doc. JUDr. Tomáš Gřivna, Ph.D. s. 7

[6] Česká republika po osmi letech ratifikovala Úmluvu o počítačové kriminalitě. *Ihned.cz* [online]. 2013 [cit. 2016-02-21]. Dostupné z: http://pravniradce.ihned.cz/c1-60516560-ceska-republika-po-osmi-letech-ratifikovala-umluvu-o-pocitacove-kriminalite

[7] BARTŮNĚK, Jan. *Kybernetická kriminalita*. Praha, 2014. Diplomová práce. PF UK. Vedoucí práce Doc. JUDr. Tomáš Gřivna, Ph.D. s. 7

[8] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2. s. 269-274

[9] ROSENZWEIG, Paul. *Cyber warfare: how conflicts in cyberspace are challenging America and changing the world*. Santa Barbara, Calif.: Praeger, 2013, xi, 290 p. ISBN 9780313398964. s. 85-95

[10] Kybernetická kriminalita - fenomén dneška. *Pravniprostor.cz* [online]. 2015 [cit. 2016-02-21]. Dostupné z: http://www.pravniprostor.cz/clanky/trestni-pravo/kyberneticka-kriminalita-fenomen-dneska

Kyberzločinem chápeme trestnou činnost, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení včetně dat, nebo pouze některá z jeho komponent. Jako takové dělíme kyberzločiny na čtyři okruhy:[11]

- zločiny narušující soukromí (nezákonný sběr údajů a jejich šíření)
- nelegální obsah (pornografie, vyzývání k násilí, rasismus apod.)
- ekonomické zločiny (napadení systémů, podvody, šíření virů atd.)
- porušování duševního vlastnictví (zejména v souvislosti s distribucí nelegálního softwaru a audio či video materiálů)

1.2.1 Kyberprostor

Kyberprostor (angl. výraz Cyberspace), tento pojem byl již v práci použit a bude se nepochybně ještě mnohokrát v práci vyskytovat, je dozajista na místě zde uvést, co tento význam představuje. Definice není zcela jednoduchá a jednoznačná. Mnoho odborníků i filozofů se v minulosti pokoušelo o jeho definici, z tohoto důvodu existuje několik pojetí. My však budeme vycházet z nejaktuálnější definice, která uvádí, že *„Kyberprostor je globální a vyvíjející se doména charakterizovaná užíváním elektrických sítí a elektromagnetického spektra, jejíž smysl je vytvářet, uchovávat, upravovat, vyměňovat, sdílet, vybírat, používat či vymazávat informace. Kyberprostor zahrnuje:*

a) fyzická i telekomunikační zařízení, která umožňují spojení technologií a komunikaci sítí systému, chápáno obecně (SCADA zařízení, smartphony / tablety, počítače, servery, atd.),

b) počítačové systémy a komplementární software, který zaručuje spojení a funkčnost systému,

c) spojení počítačových sítí,

d) uživatelské vstupy a uzly zprostředkovatelů spojení,

e) informace – uživatelská data.“[12,13]

---

[11] Internetová kriminalita. *Pcworld.cz* [online]. 2004 [cit. 2016-02-09]. Dostupné z: http://pcworld.cz/internet/internetova-kriminalita-14612

[12] How would you define Cyberspace? *Academia.edu* [online]. 2014 [cit. 2016-02-21]. Dostupné z: https://www.academia.edu/7096442/How_would_you_define_Cyberspace

[13] Kyberprostor. *Wikisofia.cz* [online]. 2015 [cit. 2016-02-21]. Dostupné z: https://wikisofia.cz/index.php/Kyberprostor

Jedna z nejvýznačnějších vlastností skladby kyberprostoru je otevřenost velkému množství uživatelů v interaktivním a virtuálním prostředí. Dalším a důležitým znakem, zejména pro právní či kriminalistické důsledky, je anonymita. Ta umožňuje téměř jakékoliv jednání bez zodpovědnosti. Kyberprostor umožňuje uživatelům komunikovat, sdílet a vyměňovat si informace a idey, hrát online hry i s mnoha spoluhráči ve stejný okamžik, účastnit se diskuzí na sociálních fórech, provádět obchodní transakce atd.[14]

1.3 Informace, informační systémy, data

Data jsou vyjádřením jak skutečností, tak i myšlenek, a to v takové podobě, aby s nimi bylo možno nakládat, tj. uchovávat, zpracovávat, ale i přenášet. To vše s cílem vytvářet z nich informace. Proto jsou data ukládána na nosičích dat (podkapitola 1.3.1), a pro snadnější přístup a práci, nějakým způsobem organizována. Pro ještě lepší uspořádání a přístup k nim podle zadaných kriterií se z dat utvářejí databáze, což jsou souhrny uspořádané podle pojmové struktury, v níž jsou popsány vlastnosti těchto dat a vztahy mezi odpovídajícími entitami. V našem případě je nutné připomenout, že je nutné užití počítače jakožto zprostředkovatele pro zpracování dat, resp. zpracování informací, které jsou těmito daty reprezentovány. Z tohoto důvodu je vhodnější hovořit o kriminalitě zaměřené na informační systémy, resp. informace, jenž jsou v informačních systémech zpracovávány prostřednictvím výpočetní a telekomunikační techniky. Pod pojmem informace nás bude, také díky vlivu kybernetiky, zajímat jeho reprezentační pojetí, kdy lidé i stroje mohou zpracovávat a ukládat informace představující poznání vnější reality, avšak i komunikační pojetí, kdy předpokládáme určitou komunikaci, s lidským či strojovým prvkem, která spojuje zdroj a přijímač informací. Pokud bude existovat systém, který jakoukoli informaci zpracovává, můžeme tento systém ve zjednodušení chápat jako informační systém. Jedná se o celek složený z počítačového hardwaru a souvisejícího softwaru, k němuž náleží i lidé, jež je využívají, a také procesy, které přitom vykonávají za účelem získávání, zpracování a šíření informací potřebných k plánování, rozhodování a řízení.[15]

---

[14] Kyberprostor. In: *Wikipedia: the free encyclopedia* [online]. 2015 [cit. 2016-02-21]. Dostupné z: https://cs.wikipedia.org/wiki/Kyberprostor

[15] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. Pro praxi. ISBN 978-80-7380-501-2. s. 31-44

Informačních systémů je dnes celá řada a slouží nejen samy sobě pro snadnější a efektivnější práci, ale hlavně lidem, kterým usnadňují každodenní činnosti. Příkladem by mohl být i Studijní informační systém UK, který napomáhá každému studentovi, ale i pedagogům a dalším zaměstnancům a bez nějž si dnes jen stěží dovedeme studentský život představit.

1.3.1 Nosič dat

Z hlediska trestního práva se jedná o dost zásadní pojem, neboť některá ustanovení TZ s ním pracují (§ 230 – § 232), třebaže pod označením „nosič informací“.

Za nosič dat je možné chápat jakýkoli nástroj, který umožňuje uchování informací určených jak uchovateli tak, aby mohly být využívány po dobu přiměřenou účelu těchto informací, a který umožňuje reprodukci těchto informací v nezměněné podobě. Jinými slovy je to vše, kam je možné data jakýmkoli způsobem uložit a později je využít. Je tedy zřejmé, že pod tuto definici je možné zahrnout i obyčejnou tužku s papírem. I na papír je možné zaznamenat informaci, která bude později použita. Je zřejmé, že v dnešní době je tento způsob uchovávání dat již poněkud „archaický“, přesto však je velmi snadný a hlavně levný. Nicméně za jeho nevýhody lze považovat to, kolik či jaké množství dat lze takto uchovat a také dobu, po kterou je možné data opětovně použít. Přesto se však i dnes tohoto způsobu využívá.

Pro naši potřebu však budeme za nosiče dat považovat poněkud modernější a výkonnější prostředky. Prostředky, na které je možné uložit mnohonásobně větší množství dat a to na téměř neomezenou dobu, a které „přežijí“ i v podmínkách, kde by jiné prostředky byly již dávno zničené a tudíž veškerá data a informace navždy ztracená. Jedná se o nosiče, které dnes chápeme jako přenosná výměnná datová média, jež umožňují ukládání datových souborů a jejich přenos mezi počítači a dalšími zařízeními, jako jsou mobilní telefony, fotoaparáty či moderní televize. V širším pojetí lze za datové nosiče považovat i vnitřní paměť počítače, disky zabudované do počítače nebo naopak síťová datová úložiště. Nosičem datového záznamu může být buďto digitální nebo analogový signál, přičemž v dnešní době se využívá v drtivé většině signál digitální, kdy se digitální hodnota uloží většinou v binární formě, což je složení nul a jedniček ve správném pořadí. Záznam dat na takovém nosiči pak může být permanentní – zapisovatelné CD-R, semipermanentní – přepisovatelné CD-RW nebo volatilní (nestálý,

kdy se po vypnutí napájení obsah ztratí) – paměť RAM počítače. Jak se vyvíjely samotné počítače, vyvíjely se i nosiče dat, přičemž se vždy využívalo fyzikálních vlastností daných nosičů. Z dnešního pohledu můžeme nosiče dělit na:

- **Magnetické** – disketa, pevný disk, magnetooptický disk, magnetická páska (audiokazeta, videokazeta, DAT kazeta, LTO 1 až N)
- **Optické** – CD, DVD, Blu-ray, HD DVD
- **Elektronické –** flash paměť (Secure Digital, Multimedia Memory Card, Memory Stick, Flash card, xDcard, USB flash paměť[16]

Dnes se v drtivé většině využívá nosičů elektronických, je to dáno jejich rychlostí přístupu k jednotlivým datům, přesto jsou oblasti, kde i nejstarší typ nosičů, tedy magnetické, nalezne své uplatnění. Pro zájemce o historický vývoj a případnou budoucnost nosičů je možné odkázat na zajímavý článek na internetu – viz pozn. pod čarou.[17]

1.3.2 ICT

ICT je zkratka oboru informačních a komunikačních technologií. Vychází z anglického názvu Information and Communication Technologies. Vzniklo z IT v momentě, kdy mezi sebou začaly počítače a celé počítačové sítě komunikovat. Z této komunikace se postupem času vyvinul internet (kapitola 1.4) či mobilní telefony, a proto ICT nejsou pouze počítače, ty představují jen jednu ze součástí. Jedná se nejenom o HW, ale i programy a aplikace, které zařízením říkají, jak pracovat či zpracovávat informace podle potřeb a přání lidského faktoru. Jedná se i o přenos informací, jemuž daly nový rozměr právě internet a mobilní sítě, po nichž neustále proudí neuvěřitelné množství dat. Spojení zprostředkovávají i telekomunikační sítě a satelity. Informační a komunikační technologie jsou v současnosti naprosto nezbytné. Dnes jsou využívány téměř ve všech oborech a bez jejich pomoci by dnes už jen těžko mohly fungovat úřady, banky, zdravotnictví, doprava, vědecké instituce, média či mnoho dalších.[18]

---

[16] Datové médium. In: *Wikipedia: the free encyclopedia* [online]. Wikimedia Foundation, 2014 [cit. 2016-02-21]. Dostupné z: https://cs.wikipedia.org/wiki/Datov%C3%A9_m%C3%A9dium

[17] zajímavý článek na internetu ohledně historie a budoucnosti nosičů – **Historie a současnost datových úložišť** – dostupný online na http://www.svethardware.cz/historie-a-soucasnost-datovych-ulozist/23935

[18] Co je ICT? *Zkusit.cz* [online]. 2010 [cit. 2016-02-21]. Dostupné z: http://www.zkusit.cz/proc-zkusit/co-je-ict.php

1.4 Internet

Každodenně jej využívají miliardy lidí po celém světě, avšak co to vlastně je? Internet je celosvětovou počítačovou sítí, která spojuje počítače a počítačové sítě všech kontinentů. Internet nabízí mnoho služeb, mezi nejznámější patří WWW, z anglického WorldWideWeb – kombinace textu, grafiky a multimédií propojených hypertextovými odkazy – tj. zobrazování webových stránek, elektronická pošta – e-mail či FTP protokol pro přístup a přenos vzdálených souborů, ale nabízí mnoho desítek dalších služeb. Propojené počítače komunikují pomocí protokolů TCP/IP (Transmission Control Protocol – Internet Protocol) a to na základě IP, ve kterém se počítače označují číselnými adresami tzv. IP adresy. Jedním s cílů lidí využívajících internet je bezproblémová komunikace a výměna dat.[19]

Jak již bylo uvedeno, tak kyberprostor či internet neznají hranic. Tedy co se týká hranic mezi státy, jak je chápeme jako občané toho či onoho státu. Samozřejmě, že i internet své hranice má, neboť jen těžko může být dostupný na izolovaném počítači, tedy tam, kde není připojen kabel, není v dosahu žádná Wi-Fi, mobilní či jiná síť a ani žádný satelit do daného zařízení internet nepřenáší. Proto je novým druhem interkulturní komunikace, kde geografická lokace nemá prakticky žádný význam. Přesto se však stává, že i tato lokace má na přístup k datům vliv. Některé stránky či provozovatelé webů filtrují veřejné IP adresy, tedy adresy, které jsou počítačům propůjčeny, aby se mohly k internetu připojit, a určité uživatele nežádoucích států na své stránky nepouští. Avšak toto je zřejmě zásah do principu internetu, tedy toho, že internet nemá hranice a jednou publikovaný materiál by měl být dosažitelný odkudkoli bez výjimky. V některých zemích by tato „filtrace“ či vlastně diskriminace mohla narážet na národní právní předpisy, které v těchto zemích IP adresu považují za „osobní údaj“, na který se vztahují příslušné zákony o ochraně osobních údajů, a proto by neměla být daná omezení aplikována na základě takto nezákonně získaných informacích. Jiná věc je případná cenzura státu, který může obsah internetu pro své občany a na svém území filtrovat.[20]

---

[19] Intermet. In: *Wikipedia: the free encyclopedia* [online]. Wikimedia Foundation, 2019 [cit. 2016-02-21]. Dostupné z: https://cs.wikipedia.org/wiki/Internet

[20] ROSENZWEIG, Paul. *Cyber warfare: how conflicts in cyberspace are challenging America and changing the world*. Santa Barbara, Calif.: Praeger, 2013, xi, 290 p. ISBN 9780313398964. s. 201-210

Internet má vzhledem k dříve uvedenému jednu podstatnou vlastnost. Tou je jeho obrovský informační dopad tím, že spojuje většinu počítačů, a nejenom počítačů, ale i jiných komunikačních zařízení na planetě. Cokoli je na internetu publikováno, stává se veřejným a to zcela v souladu s ustanovením § 117 písm. a) TZ, podle něhož je trestný čin spáchán veřejně, jestliže je spáchán obsahem tiskoviny nebo rozšiřovaného spisu, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem. Přesto je třeba odlišovat případy, kdy je internet využit jako komunikační nástroj mezi dvěma uživateli. Např. obsah emailové či chatové komunikace nemůže být chápán ve smyslu uvedeného paragrafu TZ jako veřejný, k čemuž se váže nález Ústavního soudu sp. zn. I. ÚS 1428/13 ze dne 20.8.2013, ale také rozsudek Krajského soudu v Brně ze dne 27.10.2010, sp. zn. 3 To 478/2010.[21]

1.5 Sociální sítě

Sociální síť, společenská síť nebo komunitní síť (anglicky social network nebo community network) je aplikace na internetu, jež umožňuje svým registrovaným uživatelům vytvářet osobní veřejný či částečně veřejný profil, komunikovat s jinými uživateli v rámci dané aplikace, sdílet informace, fotografie, videa, provozovat chat a mnoho dalších aktivit. Za „nižší“ formu sociální sítě lze považovat internetová diskusní fóra, kde si daní členové vyměňují názory a poznatky na vybraná témata. Komunikace mezi uživateli sociálních sítí může probíhat buď soukromě, tedy pouze mezi dvěma, nebo hromadně, tj. mezi uživatelem a skupinou s ním propojených dalších přátel či obchodnch partnerů. Pojmenování pochází ze sociologického pojmu sociální síť, což je skupina lidí, která spolu udržuje komunikační vztahy různými prostředky.[22]

Dnes jsou sociální sítě jedním z nejběžnějších komunikačních nástrojů. Lidé na nich tráví i hodiny denně, aby byli v kontaktu se svými známými. Dá se říci, že sociální sítě svět zmenšují, neboť ohromná vzdálenost již není takovou překážkou pro kontakt s ostatními lidmi. Mezi nejznámější sociální sítě patří Facebook, Twitter, Google+, MySpace, LinkedIn a několik dalších. V ČR jsou to např. Lidé.cz a Spolužáci.cz.[23]

---

[21] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. Pro praxi. ISBN 978-80-7380-501-2. s. 52-55

[22] Sociální síť. In: *Wikipedia: the free encyclopedia* [online]. 2016 [cit. 2016-02-22]. Dostupné z: https://cs.wikipedia.org/wiki/Soci%C3%A1ln%C3%AD_s%C3%AD%C5%A5

[23] BARTŮNĚK, Jan. *Kybernetická kriminalita*. Praha, 2014. Diplomová práce. PF UK. Vedoucí práce Doc. JUDr. Tomáš Gřivna, Ph.D. s. 6

1.6 Warez

Warez je termín počítačového slangu označující autorská díla, s nimiž je nakládáno nelegálně a to zejména v rozporu s autorským právem. Slovo bylo vytvořeno z anglického slova wares, zřejmě v souvislosti se slovem soft**wares**, tedy množné číslo počítačových programů. Někdy je možné warez dělit podle okruhu zájmů, na který se tedy daný zaměřuje, tj. hry, programy, filmy atd. Pro své šíření je nejvíce využíván internet a to právě pro svou vysokou anonymitu. Zjednodušeně jsou lidé, kteří zacházejí s warezem, označováni jako počítačoví piráti. Toto expresivní pojmenování těchto lidí prosazují zejména organizace zastupující zájmy držitelů autorských práv, což je v ČR ponejvíce Česká protipirátská unie (ČPU). Na rozdíl od prodejců nelegálních kopií her, programů či filmů, kteří konají pro své obohacení, nemají warezové skupiny ze svého počínání žádný finanční zisk. Motivace těchto skupin může být různá, přesto jako každý subjekt, i jim jde o jistý užitek, v ekonomickém významu. Nicméně ten není reprezentován penězi, tedy alespoň ne primárně. Může být představován i pouhým uznáním mezi ostatními členy skupiny. Bohužel však mnoho uploaderů (nahrávačů) sdílí warez na upload serverech (podkapitola 1.7), což je pro držitele autorských práv ten největší problém, se kterým se snaží, tu a tam i úspěšně, bojovat.[24]

I v ČR je možné zapojit se do několika warezových skupin, které právě na internetu utvářejí fóra. Jedním z největších je Warforum.cz. Na těchto fórech nejde pouze o warez, ačkoli jsou primárně za tímto účelem založena. Jedná se o komunitu lidí, vlastně jistou formu sociální sítě, kde dochází k mnohým diskuzím na všelijaká témata. Mnohdy ale i značně odborná, kdy si uživatelé mezi sebou vyměňují poznatky, ale i hodnotné rady pro řešení nejrůznějších problémů nejen ze světa počítačů, ale i ze světa skutečného. Je velmi zajímavé, že tyto rady jsou poskytovány nezištně, tedy bez protiplnění a často jsou to rady skutečně cenné. Rady zejména ze světa počítačů, kdy i samotný výrobce softwaru či hardwaru si neví se situací rady, je možné na těchto fórech získat. Což někdy může danému uživateli i legálního softwaru, ušetřit mnoho starostí a třeba i peněz. Z tohoto důvodu není možné označit dané skupiny či fóra jen za vyvrhele a tak k nim přistupovat, neboť se v nich nachází lidé, kteří jsou skutečnými odborníky v daném odvětví.

[24] Warez. *Superia.cz* [online]. 2015 [cit. 2016-02-22]. Dostupné z: http://cojeto.superia.cz/internet/warez.php

1.7 Upload servery, tzv. webová úložiště či filehostingy

Jedná se internetová úložiště, která umožňují velmi jednoduché i velmi rychlé sdílení jakýchkoli dat. To znamená, že je možné se po nahrání dat na server – uploadování, k nim dostat z jakéhokoliv počítače, telefonu nebo tabletu. Stačí znát přihlašovací údaje k úložišti a mít na zařízení nainstalovanou potřebnou aplikaci nebo webový prohlížeč. Takovýchto úložišť je mnoho a liší se pouze podmínkami, za jakých své služby nabízejí. Některé poskytují své služby zdarma, jiné za úhradu, většinou je to v kombinaci obojího, kdy např. zdarma je možné nahrát soubor do jisté velikosti, či stahování zdarma probíhá jen omezenou rychlostí. Pokud chce uživatel nahrávat větší soubory či stahovat neomezenou rychlostí, je nutné za tuto službu zaplatit. Také doba uložení je u souborů zdarma mnohonásobně kratší, než v případě placené služby.[25]

Mezi nejznámější a nejvyužívanější úložiště patřily RapidShare a Megaupload, avšak oba již podlehly tlaku držitelů autorských práv a jejich boji proti nim a proto dnes již neexistují. Dnes se ve světě využívá doposud funkčních serverů Turbobit.net, Uploaded.net či Filefactory.com. U nás patří mezi nejoblíbenější servery Uloz.to, kterému se snaží konkurovat Sdilej.cz, Datoid.cz, Fastshare.cz či Webshare.cz. Za vznikem Webshare.cz stojí warezová skupina již zmiňovaného fóra Warforum.cz, čili se jedná o servery, které jsou přímo vytvořené pro warez data. Specifickou úlohu na českém trhu hraje server Hellshare.cz, který jako jediný neumožňuje free, neboli volné či zdarma stahování a tak pouze uživatel, který serveru zaplatí, je oprávněn soubory stáhnout. Díky této změně v „politice“ stahování není mezi uživateli warez fór moc oblíben, neboť zdarma z něj nikdo nic nezíská. Přesto má oproti ostatním jednu nezanedbatelnou výhodu, tím že je zaměřen pouze na platící klienty, má více prostředků na zakoupení serverů, kde jsou data uložena a díky tomu je schopen nahrané soubory uchovat na delší dobu. Proto se v praxi stává, že ačkoli soubory na serverech, které volné stahování umožňují, již nejsou, Hellshare je stále nabízí a tím své klienty získává.

V dnešní době se však zdá, že klasická webová úložiště jsou na mírném ústupu a začíná se více využívat úložišť cloudových (kapitola 1.8), oproti nimž jsou v nevýhodě v tom, že soubor se musí nejdříve celý stáhnout, aby se uživatel dostal k obsahu, zatímco cloudy zpřístupňují data téměř v reálném čase a čas dnes hraje důležitou roli.

[25] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. Pro praxi. ISBN 978-80-7380-501-2. s. 55-56

1.8 Cloudy – cloudová (online) úložiště

Takzvaná „cloudová“ úložiště jsou úložiště pro ukládání či zálohování dat na serveru dostupném online na internetu. Data se ukládají aplikacemi pro automatickou synchronizaci těchto dat s jedním nebo více počítači a dalšími zařízeními (tablet, chytrý mobilní telefon). Umožňují tak uživateli *de facto* neomezený přístup ke svým datům, přičemž jedinou nutností je mít internetové připojení.[26]

Cloudová úložiště mají navíc zpravidla software např. pro počítače či mobily (v budoucnosti to jistě budou i jiná zařízení, určitě SMART TV či jakékoli jiné domácí elektronické spotřebiče, dnes fungující bez jakékoli potřeby být „chytré“ či online napojené na internet – viz pozn. pod čarou [27]), které umožňují synchronizaci a některé další zajímavé přídavné funkce, jenž je odlišují od výše zmíněných uploadových serverů. Mezi cloudová úložiště nepatří ani řešení pro online zálohování, byť se může zdát, že ano.[28]

Mezi nejvýraznější společnosti na trhu s cloudy patří bezesporu Microsoft OneDrive, který se tímto krokem snaží přilákat ještě více zájemců o své služby, ale také Apple iCloud, Dropbox či Google. U nás je to např. BeeScale či Webcloud.

Bohužel se však často stává, že tyto servery jsou terčem nelegálních útoků, které se snaží dostat k jejich obsahu, neboť ten mnohdy bývá značně soukromý a jako takový se stává zajímavým finančním zdrojem. K tomuto problému se však ještě dostaneme.

Zvláštním hráčem na trhu je server Youtube.com. Nejedná se o klasický cloud server, přesto se svou strukturou a možností přístupu k datům, přičemž se v jeho případě jedná pouze audio či video obsah, cloudům přibližuje. Jedná se o zvláštní způsob sdílení videa, tzv. přenos datovým tokem, anglicky **streaming**, ačkoli ještě lehce upravený do podoby **pseudostreaming**, což je obohacené progresivní stahování. Další možností, jak může být video přeneseno k uživateli je stahování, anglicky **download**. Takto fungují webová úložiště. Posledním způsobem je progresivní stahování, **progressive download**.

---

[26] Cloudové úložiště. *Wiki.ics.muni.cz* [online]. 2015 [cit. 2016-02-14]. Dostupné z: https://wiki.ics.muni.cz/cloudove_uloziste

[27] zajímavý článek na internetu ohledně budoucnosti domácích spotřebičů – **Kdy ovládnou naše domácnosti SMART spotřebiče?** – dostupný online na http://www.teshop.cz/novinky/kdy-ovladnou-nase-domacnosti-smart-spotrebice/

[28] Velký přehled cloudových úložišť. *Wordpress.com* [online]. 2015 [cit. 2016-02-14]. Dostupné z: https://365tipu.wordpress.com/2015/07/06/tip187-velky-prehled-cloudovych-ulozist-aneb-dropbox-onedrive-box-net-a-ti-dalsi/

1.9 P2P sítě a programy, které je využívají

Peer-to-peer = rovný s rovným, P2P nebo klient ⇔ klient je označení typu počítačových sítí, kdy spolu komunikují přímo jednotliví klienti, tedy počítače a to bez zapojení běžných webových serverů. Čistá P2P architektura vůbec pojem server nezná, protože všechny uzly sítě jsou na stejné úrovni a tudíž rovnocenné. Působí současně jako klienti i „servery" pro ostatní připojené klienty. Pro usnadnění počátečního spojení a navázání komunikace mezi klienty se však často v protokolu objevují specializované servery, které někdy slouží i jako proxy servery v případě, že spolu z nějakého důvodu nemohou koncové uzly komunikovat přímo. V dnešní době se označení P2P vztahuje hlavně na výměnné sítě, prostřednictvím nichž si velké množství uživatelů vyměňuje svá data. Jednou z nejpodstatnějších výhod P2P sítí je skutečnost, že s rostoucím množstvím uživatelů celková dostupná přenosová kapacita roste, neboť obsah se sdílí po částech. Celý obsah si tak klient stáhne od několika různých dalších klientů. Tyto části se pak v uživatelově PC spojí a vytvoří celý komplet. Díky tomuto dochází ke sčítání rychlostí a tedy i k růstu celkové přenosové kapacity. Samozřejmě připojený klient pak v síti sám funguje jako šiřitel a části, které má již stažené, sám dál po jiných částech poskytuje druhým. Toto u klasického modelu klient-server, tedy například při stahování z webového úložiště, nefunguje. Zde se musí uživatelé dělit o konstantní kapacitu serveru, takže při nárůstu uživatelů klesá průměrná přenosová rychlost a při obrovském množství napojených klientů může dojít i k přetížení, kdy data nejsou dostupná nikomu.[29]

Příkladem P2P sítí jsou např. Gnutella či původní verze Napsteru. Dnes je nejrozšířenější BitTorrent, jež bude ještě zmíněna. Programy, které umožňují připojení a stahování prostřednictvím P2P jsou např. uTorrent, BitComet či Strong DC++.

1.10 Internet a kriminalita

Již od samotného vzniku lidské civilizace se pachatelé snaží využívat k protispolečenským či protiprávním činům nové a nové prostředky, které jim poskytuje a umožňuje daná doba. Nejinak je tomu bohužel i dnes, kdy internet a informační

---

[29] Peer-to-peer. In: *Wikipedia: the free encyclopedia* [online]. 2015 [cit. 2016-02-22]. Dostupné z: https://cs.wikipedia.org/wiki/Peer-to-peer

technologie poskytují velké množství moderních prostředků pro nezákonné aktivity nebo se samy stávají předmětem útoku, nikoli jen jeho prostředkem. Internetová kriminalita, ještě nedávno nový či vlastně i neznámý pojem, v kriminalistice pomalu zdomácněl. [30]

Problém s „řízením" internetu je dán tím, že kybernetický prostor je kombinací virtuálních vlastností, které nejsou, jak již bylo v úvodu zmíněno, omezovány zeměpisnými hranicemi, a fyzické infrastruktury spadající do výsostné jurisdikce suverénních států. Je nutné si také uvědomit, že je právě možné z nízkonákladové virtuální sféry vést útoky proti sféře fyzické, jež tvoří i vzácné a drahé zdroje, o které útočníkům v největší míře jde. Ačkoli kybernetický prostor nabízí mnoho výhod, z nichž nejpodstatnější je volný přístup k informacím a snadná komunikace rostoucího počtu lidí odkudkoli na planetě, stal se zároveň i místem, kde je možné páchat téměř anonymně nejrůznější zločiny, hackerské útoky, ohrožovat vlády zemí i celé společnosti. [31]

Vše výše uvedené bohužel dokládají i statistiky spáchaných trestných činů v ČR, které eviduje Policie ČR. Ačkoli Policie ČR neeviduje odděleně statistiky výlučně internetové kriminality (Obr. 1), z prostudování celkových lze vyvodit závěr, že tento druh kriminality má značný nárůst. Dle informací právě z internetového zdroje plyne, že v roce 2014 vzrostla tato kriminalita oproti roku 2013 o více jak jednu třetinu[32], a nárůst v roce 2015 oproti roku 2014 byl dalších 15%[33]. Od roku 2011 do roku 2014 došlo dokonce k téměř trojnásobnému zvýšení internetových trestných činů (v absolutních číslech je to nárůst z 1500 na 4300 TČ)[34], což je dosti znepokojující vývoj, na který budou muset OČTŘ reagovat. Když se k tomu připočte i jistá míra latence, jsou tato

---

[30] Internetová kriminalita. *Pcworld.cz* [online]. 2004 [cit. 2016-02-09]. Dostupné z: http://pcworld.cz/internet/internetova-kriminalita-14612

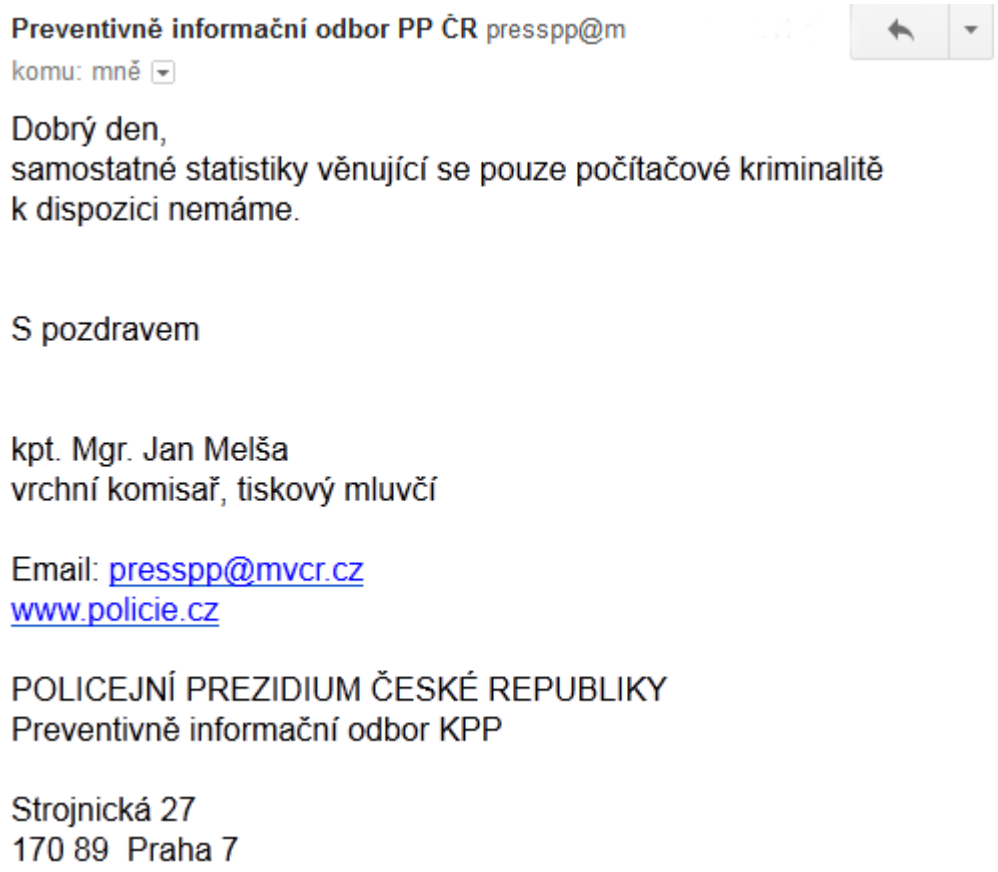
[31] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. Pro praxi. ISBN 978-80-7380-501-2. s. 72

[32] Na českém internetu přibývá podvodů. Loni škoda překročila miliardu korun. *Ihned.cz* [online]. 2015 [cit. 2016-02-10]. Dostupné z: http://archiv.ihned.cz/c1-63664110-na-ceskem-internetu-pribyva-podvodu-loni-skoda-prekrocila-miliardu-korun

[33] Kriminalita v ČR loni klesla, stalo se nejméně vražd od roku 2000. *Ceskenoviny.cz* [online]. 2016 [cit. 2016-02-10]. Dostupné z: http://www.ceskenoviny.cz/zpravy/kriminalita-v-cr-loni-klesla-stalo-se-nejmene-vrazd-od-roku-2000/1304705

[34] Internetová kriminalita roste, policie založí nový útvar. *Aktualne.cz* [online]. 2015 [cit. 2016-02-10]. Dostupné z: http://zpravy.aktualne.cz/domaci/kriminalita-na-internetu-se-od-roku-2011-ztrojnasobila/r~79c4ebd6b10d11e49f60002590604f2e/

čísla skutečně alarmující. Jen pro zajímavost je možné uvést, že v roce 2001 bylo v ČR spácháno, tedy evidováno, v oblasti kybernetické kriminality pouze 15 zločinů.[35]



Preventivně informační odbor PP ČR presspp@m
komu: mně

Dobrý den,
samostatné statistiky věnující se pouze počítačové kriminalitě k dispozici nemáme.

S pozdravem

kpt. Mgr. Jan Melša
vrchní komisař, tiskový mluvčí

Email: presspp@mvcr.cz
www.policie.cz

POLICEJNÍ PREZIDIUM ČESKÉ REPUBLIKY
Preventivně informační odbor KPP

Strojnická 27
170 89 Praha 7

Obr. 1

[35] Za poslední roky se kybernetická kriminalita ztrojnásobila. *Ceskatelevize.cz* [online]. 2015 [cit. 2016-02-10]. Dostupné z: http://www.ceskatelevize.cz/ct24/domaci/1501646-za-posledni-roky-se-kyberneticka-kriminalita-ztrojnasobila

2 Kybernetické zločiny

Jak již bylo v úvodu této práce zmíněno, je primárně zaměřena na trestné činy, které souvisí s rozmnožováním a šířením audiovizuálních děl na internetu spolu s případnými nezákonnými kopiemi počítačových programů a systémů. Avšak není od věci se seznámit i s jinými druhy útoků z či v kyberprostoru, které ovlivňují životy téměř každého. Je až zarážející, kolik trestných činů uvedených ve zvláštní části TZ je možné spáchat za použití počítače či využití internetového prostředí.

Vyvstává však otázka, zda se dají tyto protiprávní „útoky" nějakým způsobem zatřídit a pokud ano, tak jak. Jinými slovy, existuje jakási typologie kybernality? Na tuto otázku není odpověď až tak snadná. Mnoho odborníků v oblasti IT se o provedení klasifikace či typologie pokoušelo, avšak výsledky byly nejrůznější. Jiní odborníci odmítali možnost typologií vůbec a namítali, že používané typologie jsou pouze *ad hoc* sestavené na základě podobných znaků. Přesto se v této části o jisté zatřídění, alespoň některých kyberzločinů, pokusíme a k vybraným uvedeme případy ze života i s jejich trestněprávním posouzením. Výčet samozřejmě nebude úplný, neb možností, co skrze internet a za použití počítače napáchat je velké množství.

2.1 Hacking

V roce 1960 byl pojem hacking použit poprvé a za hackera byl tehdy považován skutečný programátor, člověk, jenž plně ovládl počítačové systémy a byl schopen je pozměnit k tomu, aby prováděly více nebo něco jiného, než k čemu byly původně určeny. V původním označení nebylo hackerství nezákonnou aktivitou, nýbrž činností směřující k počítačovému programování a k širšímu využití počítačů jejich uživateli. Bylo nutné ovládat značné počítačové znalosti, zejména v programování a postupně se rozvíjelo k nekonvenčnímu užití počítačových systémů. Hackerství vzniklo zejména díky základním principům kyberprostoru, tj. otevřenosti, volného přístupu k výsledkům duševní činnosti a jejich vzájemného sdílení za využití nadprůměrných počítačových znalostí. V dnešním významu však hacking reprezentuje činnost spočívající v průniku do počítačových systémů jinak než běžnou cestou bez úmyslu získávat či ničit informace nebo působit škodu. Motivem pachatelů je zejména vlastních uspokojení nad svými schopnostmi. Nejde primárně o nic jiného, než si něco dokázat a proniknutí do

počítačového systému je cílem sám o sobě. Bohužel se však informace, které jsou k takovým činům nutné, sdílí a dostávají se pak i mimo komunitu „pravých hackerů“. Díky tomuto pak mají takové znalosti i lidé, pro které je hacking pouhým nástrojem pro dosažení zcela jiného cíle. Tím je zneužití informací, k nimž se takový člověk dostane, pro účely dosažení ponejvíce nějakého finančního profitu či způsobení problémů, pokud ne rovnou újmy, oprávněnému uživateli daných dat.[36]

2.1.1 Trestné činy spojené s hackingem a jejich právní posouzení

Možný delikt: zaměstnanec se hackingem v počítačové síti svého zaměstnavatele dostane k jeho důležitým datům (k čemuž neměl původně oprávnění) a tato, jako pomstu za výpověď, opatří kvalitním heslem. Tímto jednáním se dopustil TČ dle § 230 odst. 2 písm. b) TZ – *Kdo získá přístup k počítačovému systému nebo k nosiči informací a data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými*.

Jiný příklad s malou obměnou: zaměstnanec banky se hackingem dostane do oblasti dat, kam mu přístup nenáleží. Tato data odcizí (není možné je obnovit), opět třeba jako pomstu, a svému zaměstnavateli sdělí, že pokud zaměstnavatel nesplní jeho podmínky, tak takto získaná data, která obsahují osobní údaje klientů banky, uveřejní. Tímto jednáním se dopustil vícečinného souběhu TČ dle § 230 odst. 2 písm. a) TZ – *Kdo získá přístup k počítačovému systému nebo k nosiči informací a neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací* a TČ dle § 175 TZ vydírání.

Medializovaným příkladem z nedávné doby se stalo pravděpodobné prolomení hesla k e-mailové schránce, či jinak nelegálně získaný přístup k tajným datům, premiéra – „*Hackeři tvrdí, že se nabourali do e-mailové schránky premiéra Sobotky*“[37]. Doposud neznámý pachatel se tímto dopustil typického TČ dle § 231 TZ Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat.

---

[36] DUBENSKÁ, Petra. *Internetová a počítačová kriminalita*. Praha, 2013. Diplomová práce. PF UK. Vedoucí práce Doc. JUDr. Tomáš Gřivna, Ph.D. s. 17

[37] Hackeři prolomili soukromou e-mailovou schránku premiéra Bohuslava Sobotky. Stáhli z ní desítky zpráv, ve kterých se projednávají státní i soukromé záležitosti. Případem se začala zabývat policie. Zdroj: http://zpravy.idnes.cz/hackeri-nabourali-e-mail-premiera-sobotky-fgd-/domaci.aspx?c=A160105_132452_domaci_fer

V podkapitole cloudových úložišť byly nastíněny problémy, které jejich užívání bohužel přináší. Dnešní moderní přístroje, ať už jsou to nové typy notebooků, tabletů či chytrých telefonů, synchronizují veškerá data právě s cloudy. U některých značek k tomuto dochází dokonce automaticky bez vědomí majitele. V případě, že majitel přístroj ztratí či mu bude odcizen, je díky tomuto schopen svá data získat zpět do nového přístroje, což je nesporná výhoda, avšak zabezpečení cloudů proti odcizení dat není a nikdy nebude dostatečné. Z toho důvodu bude v budoucnosti docházet stále častěji k případům, kdy se různé skupiny dostanou k jejich obsahům a tento budou dále šířit. Buďto pro uznání, nebo v horším případě pro finanční zisk. V ČR zatím k únikům dat z cloudů ve velkém měřítku nedošlo, nicméně to je pouze otázkou času. V zahraničí již k tomu několikrát došlo. V nejznámějších kauzách šlo hackerům ponejvíce o uložené telefonní seznamy známých lidí, které posléze zveřejnili, nebo o uložené soukromé fotky erotického charakteru známých hereček – „*Hacker zveřejnil nahé fotky celebrit, případ řeší FBI*“[38] či „*Hacker zveřejnil na internetu nahé fotky 101 celebrit! Ukradl je z úložiště iCloudu*“.[39] Je zřejmé, že cloudy budou bezpečnostní hrozbou budoucnosti a bude nutné jejich zabezpečení věnovat mnohem větší pozornost.

V uvedených případech by dané jednání, pokud by k němu došlo v ČR, bylo opět posuzováno jako TČ dle § 231 TZ Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat.

2.2 Cracking

Pojem cracking úzce souvisí s výše zmíněnými pojmy hacking a warez. Vyznačuje se prolamováním nebo obcházením ochranných prvků elektronických nebo programových produktů se záměrem jejich neoprávněného užití či případného kopírování, kteréžto bylo před tímto zásahem crackera technicky nemožné. Cracking používá celou řadu technik k nabourání systému, což vede nejen k porušování právě

[38] Obavy o zabezpečení tzv. cloudových úložišť vyvolal útok neznámého hackera, který ukradl choulostivé fotografie převážně amerických filmových celebrit a zveřejnil je na internetu. Zdroj: http://magazin.aktualne.cz/celebrity/hacker-ukradl-nahe-fotky-jennifer-lawrence-hodla-je-prodat/r~42377faa31b811e48a740025900fea04/

[39] Jennifer Lawrence, Kate Upton, Kaley Cuoco, Kirsten Dunst. To je jen malá část z dlouhého seznamu světových celebrit, které se staly obětí hackera, který jim z cloudového úložiště ukradl desítky kompromitujících fotografií. Zdroj: http://www.blesk.cz/clanek/celebrity-svetove-celebrity/271810/hacker-zverejnil-na-internetu-nahe-fotky-101-celebrit-ukradl-je-z-uloziste-icloudu.html

autorských práv, ale i k prolomení bezpečnostní ochrany systému.[40] Nejčastěji se jedná o tzv. password cracking, tedy zjišťování hesla pro přístup do programu. Nicméně v poslední době, kdy díky technickému rozvoji došlo k masivnímu nárůstu počtu Wi-Fi sítí, které aby zajišťovaly svým majitelům alespoň jistý pocit bezpečí, vysílají kódovaně, dochází tu a tam díky „crackingu" k narušení jejich bezpečnosti, odcizení toku dat či k neoprávněnému přístupu, tj. přímo k připojení neoprávněné osoby. Z tohoto důvodu je občas pod cracking zahrnováno pouze páchání zlovolných skutků a bezdůvodný vandalismus.[41]

2.2.1 Trestněprávní posouzení činů spojených s crackingem

Trestní klasifikace tohoto jednání může být různá. Např. uvedený případ přístupu do zabezpečené Wi-Fi sítě může být posouzen, za využití zásady *ultima ratio*, jako TČ neoprávněný přístup k počítačovému systému a nosiči informací dle § 230 odst. 1 TZ. Zde se však nabízí otázka, zda by šlo takto kvalifikovat jednání případného pachatele i v případě, kdy by daná Wi-Fi síť neužívala žádného šifrování. Bylo by možné tuto síť považovat za zabezpečenou? Skutková podstata uvedená v § 230 odst. 1 TZ *„Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci."* předpokládá jisté bezpečnostní opatření, kterým je dle komentářů TZ rozuměno:

> *Bezpečnostním opatřením je třeba rozumět každé opatření, jehož cílem je zabránit volnému přístupu k počítačovému systému nebo nosiči informací (např. heslo nebo použití firewallu). Na stupni, míře zabezpečení nezáleží. Úroveň zabezpečení nelze považovat za rozhodující, postačí, že pachatel musí překonat nějakou překážku. Existence jakéhokoli zabezpečení totiž najedná straně jasně signalizuje, že si uživatel nepřeje, aby někdo nepovolaný do systému vstupoval, na druhé straně musí pachatel vyvinout zvýšené úsilí, aby do systému vstoupil.*[42]
>
> *Bezpečnostním opatřením je každé opatření, které je způsobilé plnit ochrannou funkci počítačového systému, kupř. zabezpečovací software, hardware, užívání vstupních a*

[40] MATĚJKA, Michal. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, 2002. ISBN 80-7226-419-2. s. 73

[41] GŘIVNA, Tomáš a Radim POLČÁK (eds.). *Kyberkriminalita a právo*. Vyd. 1. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4. s. 39

[42] ŠÁMAL, Pavel. *Trestní zákoník: komentář – zvláštní část*. 2. vyd. V Praze: C.H. Beck, 2012. Velké komentáře. ISBN 978-80-7400-428-5. s. 2306

bezpečnostních hesel, systém vymezení uživatelských práv, režim užívaní počítačových systémů ve společnostech a stejně tak i ve veřejnoprávních institucích a přístup k nim i k jejich částem, zajištění pracovišť s počítačovým systémem pomocí technických zařízení s tím, že bezpečnostním opatřením je rovněž nastavení integrovaného firewallu, který brání neoprávněným průnikům a ovládání počítače prostřednictvím sítě Internet.[43]

Je tedy zřejmé, že i v případě, kdy síť bude nešifrována, ale server DNS bude vypnut, tj. nedojde k přidělení IP adresy připojeného zařízení a je tedy její ruční nastavení, i v tomto případě se jedná o zabezpečení, byť velmi slabé. Přesto by se dalo jednání v této síti považovat za TČ. Pokud však síť nemá ani šifrování a DNS automaticky IP adresy přiděluje, o zabezpečení se nejedná a případný přístup do systému bez jakékoli žádné jiné aktivity trestný nebude.

O jinou právní kvalifikaci však půjde v případě vlastního aktu prolomení technické ochrany datového nosiče a následné manipulace s takto zpřístupněnými daty, např. DVD s audiovizuálním obsahem, jež je chráněn proti kopírování. Opět může být trestně právně posouzeno jako trestný čin neoprávněného zásahu k počítačovému systému a nosiči informací, nicméně nyní dle § 230 odst. 2 písm. a) TZ – *Kdo získá přístup k počítačovému systému nebo k nosiči informací a neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací.*

Povětšinou však v případech crackingu půjde o porušení autorského práva, práv souvisejících s právem autorským a práv k databázi a jelikož takováto skutková podstata uvedená v § 270 TZ je hlavním cílem této práce, rozebereme si toto protiprávní jednání důkladněji ve 3. kapitole.

2.3 Spam

Zřejmě každý uživatel internetu, jenž má ve virtuálním světě zřízenu e-mailovou schránku, se se spamem setkal osobně. Spam je nevyžádané reklamní sdělení masově šířené internetem. Primárně bylo užíváno pro nevyžádané reklamní e-maily, postupem času však tento fenomén postihl i ostatní druhy internetové komunikace – diskusní fóra, komentáře pod různými články nebo i sociální sítě. Krom reklamního a vlastně i neškodného obsahu, však někdy může, v tom horším případě, spam sloužit k šíření

[43] DRAŠTÍK, Antonín. *Trestní zákoník: komentář*. Vydání první. Praha: Wolters Kluwer, 2015. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-790-4. s. 1477

potenciálně nebezpečného obsahu, kterým mohou být viry, ale může se jednat o tzv. phishing (podkapitola 2.5) či pharming (podkapitola 2.6) maily.[44]

Spam existuje déle nežli internet. První zmínka o spamu pochází z 19. století, nicméně s příchodem elektronické pošty, jež snižuje náklady na takovéto sdělení až na téměř nulu, začal se spam vyskytovat velmi hojně. E-mailové adresy jsou pro účel rozesílání nevyžádané pošty získávány z nejrůznějších zdrojů či jsou i náhodně generovány. Díky určitým společnostem, které poskytují schránky zdarma na svých doménách (Seznam.cz, Gmail.com) ve velkém množství, je i takovéto náhodné generování úspěšné. Poslední dobou se však zdá, že tako škodlivá činnost je přece jen na mírném ústupu.[45] V procentuálním vyjádření nepochybně a snad tomu tak bude brzy i v číslech absolutních. V červnu roku 2015 činil poměr spamu jen 49,7% z celkového počtu e-mailových zpráv[45], což je poměrně dobré číslo, neboť ještě před cca 10 lety tvořil spam přes 90% ze všech odeslaných zpráv na internetu.[46]

2.3.1 Právní posouzení spamu

Povětšinou lze rozesílání spamu klasifikovat jako přestupek (FO) či správní delikt (PO) a to hned dle několika zákonů. Odpovědnost ve správním řízení vyplývá z ustanovení § 118 odst. 1 písm. i) zákona č. 127/2005 Sb., o elektronických komunikacích, podle něhož se za správní delikt považuje zaslání nevyžádané zprávy nebo zpráv třetím osobám bez souhlasu držitele adresy elektronické pošty. § 10a a § 11 zákona č. 480/2004 Sb., o některých službách informační společnosti definuje přestupek, potažmo správní delikt, pokud je obchodní sdělení šířeno elektronickými prostředky hromadně nebo opakovaně bez souhlasu adresáta. Jisté prvky spamu naplňuje i tzv. nigerijský dopis, což je označení pro různé typy podvodných sdělení, jež jsou formou e-mailových zpráv rozesílána do poštovních schránek. Povětšinou obsahují sdělení o vysokém finančním podílu z určité majetkové operace. Po odpovědi na tuto

---

[44] Co je to: Spam. *Unet.cz* [online]. 2015 [cit. 2016-02-28]. Dostupné z: https://www.unet.cz/blog/2015/09/15/co-je-to-spam/

[45] Spamů ubylo, jejich podíl byl nejnižší za dvanáct let. *Aktualne.cz* [online]. 2015 [cit. 2016-02-28]. Dostupné z: http://zpravy.aktualne.cz/ekonomika/spamu-ubylo-jejich-podil-byl-nejnizsi-za-dvanact-let/r~cd41ff1e2dd211e5ae1b002590604f2e/

[46] Téměř 90 % e-mailů jsou spamy. *Isvs.cz* [online]. 2007 [cit. 2016-02-28]. Dostupné z: http://2011-2015.isvs.cz/temer-90-e-mailu-jsou-spamy/

zprávu však následují další sdělení, jež posléze vede až v žádost o převod určité finanční částky, ponejvíce na účet do zahraničí. Tímto je naplněna skutková podstata TČ podvodu dle § 209 TZ, přinejmenším ve stádiu pokusu dle § 21 TZ.[47]

2.4 Sniffing a právo

Sniffing (z anglického překladu čenichat, čmuchat nebo větřit) je zvláštní technika, která umožňuje „odposlouchávání" počítačů v lokální síti, jinými slovy sledování celkového chodu počítače, včetně toku příchozích i odchozích dat. Během tohoto sledování dochází k „odchytu" dat, kterými jsou používaná hesla či zprávy, které si oprávněný uživatele počítače v síti vyměňuje. Při dané činnosti je možné skrytě pozorovat provoz celé sítě, což generuje přínosné informace, jež mohou být použity při nasazení botnetu, síťového červa či DDoS (podkapitola 2.7).[48]

Již samotné pozorování průtoku dat je TČ porušování tajemství dopravovaných zpráv podle ustanovení § 182 TZ. Dále by mohlo dojít k TČ porušení tajemství listin a jiných dokumentů uchovávaných v soukromí dle § 183 TZ, neoprávněný přístup k počítačovému systému podle § 230 TZ či opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat podle § 231 TZ.

2.5 Phishing, pharming a jejich trestněprávní posouzení

Anglicky phishing, se foneticky vyslovuje stejně jako fishing, proto se dané jednání také někdy do češtiny překládá jako „rhybaření" nebo i „házení udic". I popis daných skutků rybaření připomíná, neboť útočník vyšle skrze e-mailovou zprávu „návnadu" a poté čeká, zda něco „uloví". Za předchůdce daných útoků lze považovat již zmiňované nigerijské dopisy.

Tento typ podvodů je charakterizován využitím důvěry oběti a skutečnosti, že drtivá většina uživatelů v kyberprostoru nemá příliš hluboké znalosti v oblasti výpočetní techniky a dobrého zabezpečení a bezpečného chování při práci v elektronickém světě. Hlavním motivem daného jednání je odcizit uživateli údaje, které by mohly být zneužity k podvodníkovu finančnímu zisku. Proto se útok zaměřuje na přihlašovací jména a hesla

---

[47] DUBENSKÁ, Petra. *Internetová a počítačová kriminalita*. Praha, 2013. Diplomová práce. PF UK. Vedoucí práce Doc. JUDr. Tomáš Gřivna, Ph.D. s. 24

[48] Sniffing. *Sprava-site.eu* [online]. [cit. 2016-02-28]. Dostupné z: http://www.sprava-site.eu/sniffing/

např. pro přístup k bankovním účtům na internetu, nebo údaje o kreditní kartě, PINu, avšak někdy uživatele vyzývá k úhradě rádoby oprávněné peněžní částky apod.

V podstatě jde o vytvoření falešného e-mailu, který je uživateli zaslán tak, aby se vydával za oficiální zprávu instituce, se kterou je uživatel v jistém vztahu. V dané zprávě je obvykle výzva, že uživatel má něco učinit pro svou „ochranu" a nejrychlejší cesta je kliknutí na přiložený hypertextový odkaz a přihlášení se do známé aplikace. Po daném kliknutí je uživateli otevřeno internetové okno, jež vypadá *de facto* stejně, jako je uživateli známo a tak své údaje zadá. Tyto údaje jsou však ihned odesílány útočníkovi. Jednou z cest jak toto odhalit bývá pozorné ověření e-mailové adresy, ze které daná zpráva dorazila, či adresa URL, na kterou byl dotyčný přesměrován. V obou případech bývá značný nebo i nepatrný rozdíl od údajů, které by tam být měly, pokud by byly pravé.

Oproti tomu existuje forma útoků, jež se snaží tento „nedostatek" odstranit. Takovéto útoky se nazývají pharming (někdy překládáno do češtiny jako „pharmaření") a principem je napadení DNS serveru a přepsání IP adresy, na kterou je potenciální oběť přesměrována a tato adresa pak není rozeznatelná od skutečné webové stránky, kterou uživatel předpokládá. Cílem útoku je i zde získání dat, ovšem sofistikovanější formou.[49]

Pokud bychom dané jednání chtěli právně klasifikovat, jednalo by se primárně o TČ podvodu dle § 209 TZ, dále pak TČ opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat dle ustanovení § 231 TZ a pokud byla cílem i platební karta, tedy údaje, které se dají použít pro platbu na internetu, došlo by k naplnění skutkové podstaty TČ neoprávněné opatření, padělání a pozměnění platebního prostředku podle § 234 TZ.

K phishingovým útokům dochází v ČR velmi často a je pravděpodobné, že se s nějakou jeho formou setkal každý z nás. Bohužel je ale také faktem, že i přes neustálé upozorňování jak v médiích, tak od dotčených institucí, jsou útočníci neustále úspěšní. Upozornění i rady je možné si přečíst na webových stránkách Národního centra kybernetické bezpečnosti, kde je možné nalézt i několik příkladů, včetně porovnání screen obrazů pravých a podvržených webových stránek.[50]

---

[49] Pharming. In: *Wikipedia: the free encyclopedia* [online]. 2015 [cit. 2016-02-28]. Dostupné z: https://cs.wikipedia.org/wiki/Pharming

[50] PHISHING – STÁLE AKTUÁLNÍ HROZBA - http://www.govcert.cz/cs/informacni-servis/hrozby/phishing---stale-aktualni-hrozba/

Poslední zajímavá forma phishingu „zaplavila“ internet v minulém týdnu. Nedochází při ní k odeslání podvodné zprávy, ale naopak při běžném prohlížení webové stránky, např. na facebooku se v reklamním banneru na okraji okna objeví nabídka na vyzkoušení nové verze internetového bankovnictví České spořitelny a.s. Pokud někdo bude o vyzkoušení této „nové verze“ stát a na odkaz klikne, bude přesměrován na podvodnou stránku s rozdílnou adresou a po přihlášení již standardně odešle své údaje podvodníkovi. Ukázka včetně uvedené podvodné URL adresy je zobrazena na obr. 2.[51]

Obr. 2 (zdroj: Česká spořitelna a.s.)

[51] Chtějí vybílit lidem účty, používají k tomu Facebook. *Novinky.cz* [online]. 2016 [cit. 2016-02-29]. Dostupné z: http://www.novinky.cz/internet-a-pc/bezpecnost/395029-chteji-vybilit-lidem-ucty-pouzivaji-k-tomu-facebook.html

2.6 Skimming a jeho právní posouzení

Jako skimming, nebo někdy i card skimming, je označováno podvodné jednání, při kterém pachatelé zkopírují údaje z magnetického proužku platebních, debetních, kreditních či jiných podobných karet bez vědomí právoplatného držitele karty. Takto získané údaje poté pachatelé použijí při výrobě jiné karty, kdy tyto nahrají na její magnetický proužek a vytvoří vlastně klon karty původní. Pachatelé tak mají k dispozici kartu, kterou mohou použít k platbě a začít tak odčerpávat finanční prostředky z účtu, k němuž je originální karta přidružena. Nicméně klonovaná karta sama o sobě k zisku nestačí. Každá karta je jištěna zadáním PINu, bez kterého není možné kartou platit. Z tohoto důvodu při získávání údajů z magnetického proužku dochází zároveň i k videozáznamu procesu zadávání PINu na klávesnici napadeného přístroje, což bývá ponejvíce bankomat. Jen pokud mají pachatelé k dispozici PIN a údaje z proužku, je možné kartu použít. Přesto se však banky snaží tomuto předcházet a karty vybavují čipem, který slouží k platbě. V zemích EU je drtivá většina platebních terminálů vybavena tak, aby platba probíhala spíše skrze čip než protažením karty z důvodu čtení proužku. Kvůli tomu dochází sice k odcizování údajů v Evropě, avšak k výrobě kartových kopií a odčerpávání prostředků dochází v zemích, kde je technická úroveň terminálů v počátcích. Využíván k placení je právě magnetický záznam a pachatelé mají možnost jeho užití. Většinou se jedná o státy Jižní Ameriky a je tak nutná spolupráce pachatelů téměř po celém světě.

Výhodou tohoto typu útoků oproti běžné krádeži karty je v tom, že majitel karty se mnohdy nemusí o zneužití dozvědět i několik dní, což dává pachatelům dostatečný čas na odčerpání prostředků. Banky se proto snaží všemožnými prostředky skimmingu zabránit a montují na bankomaty protiopatření. Jak však budou proti těmto útokům úspěšní, ukáže budoucnost. Cena zařízení potřebných pro skimming neustále klesá a stává se tak dostupnou i pro jednotlivce, jenž bude páchat tuto činnost v malém měřítku. Na stránce největšího aukčního portálu světa Ebay.com stačí zadat do vyhledávače správný dotaz a odpovědí je tazateli mnoho set stránek s rozsáhlou nabídkou od minimálních cen. Proto se dá předpokládat, že tyto útoky jen tak nevymizí a je tak nutná ostražitost každého z nás.

Na webových stránkách Policie ČR je možné nalézt mnoho návodů jak při výběru peněz z bankomatu postupovat, aby došlo k minimalizaci rizika případného

zneužití, ale také jsou tam fotografie skimmovacích zařízení a statistiky jejich použití na bankomatech v ČR (odkaz na obdobné stránky viz poznámka pod čarou[52]).

Z hlediska trestněprávní kvalifikace skimmingu jde o trestný čin neoprávněné opatření, padělání a pozměnění platebního prostředku podle § 234 TZ.

2.7 Útoky DoS (Denied of Service) a DDoS (Distributed Denied of Services)

V této kapitole je z hlediska právní úpravy tato podkapitola zcela jistě nejzajímavější, avšak o tom až za chvíli. Popis celého procesu Dos a DDoS je poměrně obsáhlý. Pro naše účely tak postačí stručnější nastínění dané problematiky.

Zkratka DoS znamená Denial of Service, neboli znepřístupnění či potlačení služby jakýmkoliv způsobem. Od fyzického odpojení serveru (vytržení kabelu od serveru), což se v praxi moc neuplatňuje, až po využití chyby v zabezpečení – odeslání specifického řetězce, po které server „zamrzne“ a přestane komunikovat. Lze ale najít i jiné slabiny, jako je dosažení limitu systému (nejčastější forma), síťové karty, aplikace, nebo systémových. V případě limitu systému se jedná o útok na internetové služby nebo stránky, při kterém dochází k přehlcení požadavky, tj. přichází jich větší počet, než na kolik je daný server dimenzován. Následkem je pád nebo alespoň nefunkčnost a nedostupnost pro ostatní uživatele. Jejich komunikace je buďto zcela nemožná nebo velmi pomalá. K napáchání větší škody však pachatelé využívají jiné techniky, jež umožňují distribuované útoky na vícero služeb v jednom čase. Distribuovaný DoS útok = DDoS (Distributed Denial of Service attack) je charakterizován větším množstvím počítačů, snažících se najednou zahltit cíl útoku. V drtivé většině případů je útok veden bez vědomí majitelů útočících počítačů. Při dnešních kapacitách serverů není ani reálné, že by sám útočník nashromáždil fyzicky tolik přístrojů, které by mu DDoS umožnily. Je

---

[52] Sdělení ÚOOZ SKPV ohledně skimmingu - http://www.policie.cz/clanek/skimming.aspx

Poznámka autora k tématu skimming – opatrnost je na místě a to nejenom při výběru z bankomatů, ale všude, kde se kartou platí. Na bankomatech dnes lidé skimming očekávají a jsou opatrnější. Pokud by autor byl v pozici případného pachatele a chtěl užít podobného přístroje, umístil by jej raději jinam. Např. na samoobslužné čerpací stanice (jejichž počet se neustále zvyšuje – mají levnější provoz, neb se neplatí lidský faktor a jsou rychlejší a pro zákazníky výhodnější), kde probíhá úhrada platební kartou skrze tankovací automat a lidé tady skimmovací zařízení nečekají. Nejsou zde tolik opatrní a k zadávání PINu skrytým způsobem jistě nedochází. Díky tomu by úspěšnost potřebného spárování dat z magnetického proužku a PINu byla daleko větší než při umístění zařízení na výběrní bankomat.

k tomu využíváno napadení a úspěšné infikování cizích systémů, např. malwarem, jenž v sobě nese uloženou IP adresu oběti útoku a také datum, kdy se má daný program pokusit zaútočit na cíl. Celý tento postup má tu výhodu, že útočník s daným systémem nemusí nijak komunikovat a útok proběhne automaticky. Systém může být také napaden programem (botem), který poté běží jako skrytý proces na pozadí. Nicméně není nastaven na automatické zahájení útoku. Musí čekat na příkazy útočníka, či programátora bota, který poté útok centrálně řídí. Takto napadený systém se nazývá zombie a společně s ostatními počítači, napadenými stejným programem, tvoří takzvaný botnet.[53, 54]

Intenzita a promyšlenost uskutečněných útoků je rok od roku vyšší a vyšší a tím pádem i jejich účinnost a nebezpečnost. Jestliže tu a tam útokem i na jediný server dochází ve značném měřítku k ovlivnění chodu internetu, je jen otázkou času, kdy podobné útoky získají mezikontinentální přesah. Z tohoto důvodu je nanejvýš důležité docílit uspokojivého a zejména závazného právního rámce pro potýkání se s tímto typem hrozeb. Jedním takovým rámcem zavádějícím jistý povinný standard ochrany pro všechny subjekty zodpovědné za poskytování služeb (ISP) je zákon o kybernetické bezpečnosti.[55]

V minulosti se řada českých serverů potýkala s nemalými problémy, které jim přinesly právě zmiňované útoky. Oblíbeným terčem se stávají poměrně známé servery, jako je Aukro.cz, Seznam.cz, ale i velké firmy jako např. Česká pošta s.p.

2.7.1 Trestněprávní posouzení útoků DoS a DDoS

Posouzení útoků z hlediska trestního práva není nic snadného. Mnohdy ani sama Policie ČR v případě trestního oznámení neví, jak je posoudit a tudíž pod znění jakého paragrafu zvláštní části trestního zákoníku toto jednání subsumovat, což s sebou přináší zmiňovanou zajímavost této podkapitoly. Přesto se o posouzení pokusíme.[56]

---

[53] DUBENSKÁ, Petra. *Internetová a počítačová kriminalita*. Praha, 2013. Diplomová práce. PF UK. Vedoucí práce Doc. JUDr. Tomáš Gřivna, Ph.D. s. 20

[54] Seznamte se – DoS a DDoS útoky. *Security-portal.cz* [online]. 2013 [cit. 2016-03-04]. Dostupné z: http://www.security-portal.cz/clanky/seznamte-se-%E2%80%93-dos-ddos-%C3%BAtoky

[55] CHUDĚJ, Radim. *Právní postih kybernetických útoků*. Brno, 2014. Diplomová práce. Právnická fakulta Masarykovy univerzity. Vedoucí práce Doc. JUDr. Radim Polčák, Ph.D. s. 28

[56] při konzultaci s vedoucím této práce doc. Gřivnou byl autor upozorněn na dvě možnosti, jak tato jednání trestněprávně posoudit, sám poté nalezl v odborných článcích ještě třetí možnost posouzení, se kterou však autor nesouhlasí

Vnější pohled je jednou z možností jak jednání posoudit je. Dívat se a chápat internet a celou strukturu jeho sítě jako prospěšné zařízení. Poté by bylo možné útok chápat jako poškození a ohrožení provozu obecně prospěšného zařízení dle § 276 TZ. Chráněným zájmem jsou v tomto případě obecně prospěšná zařízení uvedená v ustanovení § 132 TZ, a která svým vymezením zahrnují převážnou část prvků kritické infrastruktury. „*Obecně prospěšným zařízením se rozumí veřejné ochranné zařízení proti požáru, povodni nebo jiné živelní pohromě, obranné nebo ochranné zařízení proti leteckým a jiným podobným útokům nebo jejich následkům, ochranné zařízení proti úniku znečišťujících látek, zařízení energetické nebo vodárenské, podmořský kabel nebo podmořské potrubí, zařízení a sítě elektronických komunikací a koncová telekomunikační a rádiová zařízení, zařízení držitele poštovní licence, zařízení pro veřejnou dopravu, včetně součástí dráhy a drážních vozidel ve veřejné drážní dopravě a svislých zákazových nebo příkazových dopravních značek a dopravních značek upravujících přednost.“* Šámal jimi rozumí „*zařízení, která představují buď technicky složitější veřejná zařízení, která podle své povahy slouží potřebám velkého okruhu osob, nebo mohou sloužit i omezenému počtu osob za předpokladu, že jsou technicky složitější či mají velký význam z hlediska společnosti a mají veřejnou povahu*.“[57]

Škodlivým jednáním pak pro naše účely budeme rozumět ohrožení provozu nebo využívání zařízení, učinění zařízení neupotřebitelného a poruchu provozu obecně prospěšného zařízení. Ohrožení provozu znamená, že k poruše provozu obecně prospěšného zařízení zatím nedošlo, nicméně takové riziko hrozí. Méně účinné DoS útoky, jež jsou zaznamenány, a následně je riziku způsobení škodlivých následků zamezeno pomocí obranných opatření, by se takto daly posoudit. Pokud je však DoS, nebo spíše DDoS útok úspěšný, pak se jím podaří vyřadit obecně prospěšné zařízení z provozu, dostáváme se do režimu § 276 odst. 2 písm. b) TZ – způsobení poruchy provozu obecně prospěšného zařízení. V tento moment již došlo k vyřazení obecně prospěšného zařízení z provozu na dobu delší než zcela krátkou. Takovou poruchu není po dobu trvání ohrožení snadné odstranit. To vše odpovídá následkům zdařilého účinného DoS či DDoS útoku.[58]

---

[57] ŠÁMAL, Pavel. *Trestní zákoník: komentář – zvláštní část*. 2. vyd. V Praze: C.H. Beck, 2012. Velké komentáře. ISBN 978-80-7400-428-5. s. 1386

[58] CHUDĚJ, Radim. *Právní postih kybernetických útoků*. Brno, 2014. Diplomová práce. Právnická fakulta Masarykovy univerzity. Vedoucí práce Doc. JUDr. Radim Polčák, Ph.D. s. 73

Druhou možností jak jednání postihnout je pohled na dané konkrétní počítače, jež útok neboli dotazy vysílaly. Ty musely být k této činnosti nějakým způsobem donuceny. Většinou se tak stává, jak jsme již uvedli, po vniknutí nějakého malwaru. Někdo musel do počítače proniknout a příslušný škodlivý software do PC nainstalovat. Dané jednání je pak možné posoudit dle ustanovení § 230 odst. 2 písm. d) – „*Kdo získá přístup k počítačovému systému nebo k nosiči informací a 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.*“ A že k něčemu obdobnému došlo, jsme již vysvětlili.

Třetí variantou jak postihnout dané útoky je pohlížet na dané napadené servery jako na cizí věci, které se stávají neupotřebitelné. Některé odborné články tímto nabízí posouzení dle znění § 228 TZ, tj. jako poškození cizí věci – „*Kdo zničí, poškodí nebo učiní neupotřebitelnou cizí věc, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci.*“ Myšlenka zde je jednoduchá. Server chápeme dle ustanovení OZ za cizí věc a v případě útoku se stane neupotřebitelným. Škoda je zde chápána jako náklady spojené s obnovením provozu či ušlý zisk. Autor práce se však s tímto posouzením neztotožňuje. Dle jeho názoru se jednak server nestal neupotřebitelným a ohledně způsobené škody byla myšlenka zákonodárce jiná. Ke škodě musí dojít na dané věci, nikoli škodu vyčíslovat jako sekundární důsledek. Však také Šámal uvádí: „*Neupotřebitelnou se stane věc tehdy, kdy sice nadále existuje, avšak nelze ji použít k účelu, ke kterému byla určena (smíchání různých barev, vypuštění divokého zvířete). Škodou nikoli nepatrnou se podle § 138 odst. l rozumí škoda dosahující částky nejméně 5 000 Kč. Ušlý* ***zisk se do výše škody nezapočítává.*** *Pod touto hranicí škody se jedná o přestupek podle § 50 odst. l písm. a) zák. o přestupcích.*“[59] Věc, v našem případě nefungující server, sama o sobě není a nemůže být neupotřebitelná, neboť po ukončení útoku začne opět plnit svou funkci, a tak žádná primární škoda na věci nevznikla. Sporné by bylo i posouzení, od jakého momentu je věc neupotřebitelná. Jak stanovit, že tento stav nastal právě danými útoky a ne jinak. Představme si pro jednoduchost situaci, kdy server snese zátěž 500 dotazů. Útokem se podařilo docílit pouze 490 dotazů, neboť

[59] ŠÁMAL, Pavel. *Trestní zákoník: komentář – zvláštní část*. 2. vyd. V Praze: C.H. Beck, 2012. Velké komentáře. ISBN 978-80-7400-428-5. s. 1468

útočník „nenakazil“ více zařízení. Díky tomuto k naplnění kapacity nedošlo a server nadále funguje. Poté jiných 11 uživatelů s oprávněnými dotazy své požadavky na server vyšle, čímž dojde k překročení oné hranice 500 a server pak „spadne“. Nicméně jeho vyřazení nebylo způsobeno útokem nýbrž požadavkem jiného uživatele. Není snadné takto neupotřebitelnost definovat a server se DoS útoky neupotřebitelným nestává. Z výše vyřčeného se autor nedomnívá, že je možné použití § 228 TZ a DoS či DDoS útoky pod tuto skutkovou podstatu subsumovat.

Ve zvláštní části trestního zákoníku není uvedena skutková podstata, jež by dané jednání přímo vystihovala a z uvedeného je zřejmé, že subsumování útoků pod některý jiný uvedený skutek není nic snadného. Proto se skutečně není čemu divit, že ani OČTŘ nemají jasno, jak pachatele daných útoků postihovat.

Ze statistik vyplývá, že počty takovýchto útoků rostou geometrickou řadou, taktéž úroveň uskutečněných útoků se zvyšuje každým rokem a stejně tak jejich účinnost a nebezpečnost, jak jsme již uvedli. Toto může do budoucna znamenat velmi závažné problémy. V ČR se počet útoků uskutečněných za rok 2014 oproti roku 2013 zdvojnásobil.[60] Z další statistiky vyplývá, že celosvětově došlo v roce 2015 k nárůstu útoku oproti roku 2014 o 180%.[61] Tato čísla jsou vskutku alarmující, a jak počítačoví odborníci, tak i právní systém na toto musí co nejdříve reagovat. Proto se k těmto útokům vrátíme v sedmé kapitole – Vlastní návrhy – *De lege ferenda*, kde se pokusíme definovat skutkovou podstatu, jež by takováto jednání jednoznačně postihovala.

2.8 Keylogging a právo

Keylogging spočívá ve sledování všech stisknutých kláves v počítači[62], za pomoci vhodného softwarového nebo někdy i hardwarového zařízení. Je používán pro zisk informací z napadeného počítače, zejména přístupových údajů a hesel, ale někdy také získává informace pro přípravu jiného typu útoku. Nicméně i proti keyloggingu je možná obrana. Nejlepší obranou je instalace kvalitního antispywarového produktu,

---

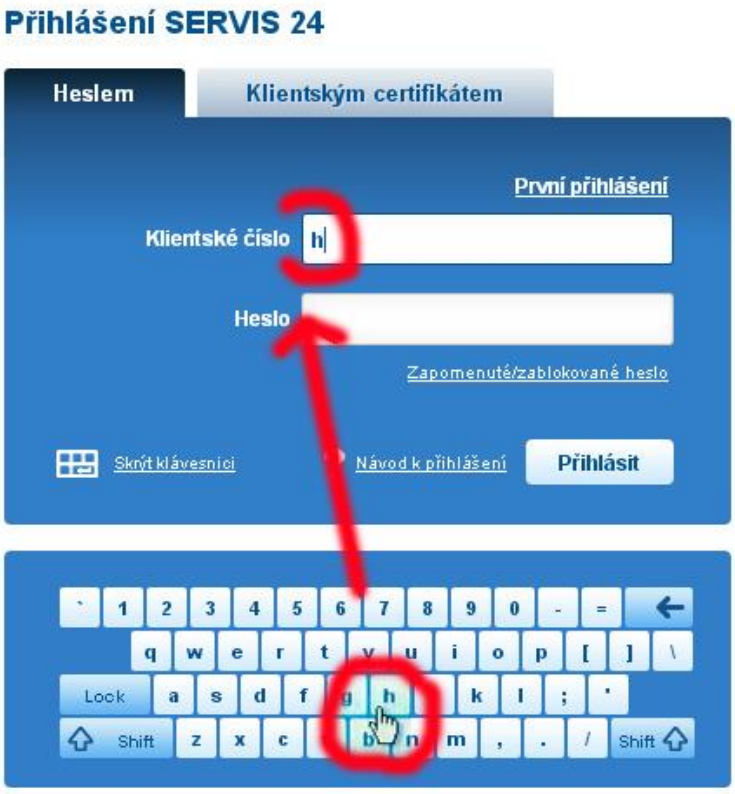
[60] DDoS útoků na české servery přibývá. Loni se jejich počet zdvojnásobil. *Lupa.cz* [online]. 2015 [cit. 2016-02-29]. Dostupné z: http://www.lupa.cz/clanky/ddos-utoku-na-ceske-servery-pribyva-loni-se-jejich-pocet-zdvojnasobil/

[61] Počet DDoS útoků vzrostl o 180%. *Kyberbezpecnost.cz* [online]. 2015 [cit. 2016-02-29]. Dostupné z: http://www.kyberbezpecnost.cz/?p=5701

[62] Co je keylogger? *Kaspersky.com* [online]. [cit. 2016-03-01]. Dostupné z: http://www.kaspersky.com/cz/internet-security-center/definitions/keylogger

který před keyloggery ochrání. Takovýto program je záležitost majitele počítače a ne vždy je tento zodpovědný. Některé banky proto mají snahu tento problém řešit tak, že pro přihlášení není nutné zadávat údaje na klávesnici, ale v procesu přihlašování je v internetovém okně zobrazena klávesnice, jež přihlašování ovládá. Uživatel místo na skutečnou klávesnici pouze kliká kurzorem, tj, myší nebo u dotykových zařízení přímo, na písmena takovéto nabídnuté virtuální klávesnice (obr. 3).

Při právním posouzení pak dané jednání naplňuje znaky TČ neoprávněný přístup k počítačovému systému podle § 230 TZ a TČ opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat podle § 231 TZ.



Obr. 3

2.9 Podvody

Doposud jsme se zabývali trestnou činností, k jejímuž páchání je nutné vlastnit poměrně odborné znalosti. Jednalo se o řadu technik, které jsou sofistikované a jsou způsobilé přivodit velké škody značnému počtu lidí. Je však nutné si uvědomit, že prostřednictvím internetu a počítače je možné páchat trestnou činnost i s poměrně malou odbornou znalostí. Drtivá většina uživatelů je totiž hodna být takto označována.

Jedná se skutečně o „pouhé uživatele“. Z tohoto důvodu je možné činit protiprávní jednání velice snadno. Jedním z nejčastějších trestných činů, jenž kyberprostor přináší a to již od svého vzniku, je podvod.

Již jsme se s tímto TČ v této kapitole setkali, avšak byl páchán mnohem důmyslněji. Podvést někoho na internetu je však velmi jednoduché, stačí k tomu např. chat na sociální síti, názorové fórum či inzertní server. Je ale také pravdou, že objasněnost takovýchto jednoduchých činů je mnohonásobně vyšší, než objasněnost dříve uvedených útoků páchaných počítačovými odborníky.

Kyberprostor svou anonymitou vytváří prostředí, jež svede na scestí i ty, kteří by v běžném životě něčeho podobného schopni nebyli. Skutečně zde platí, že „příležitost dělá zloděje“. Na dálku a v skrytu sítě je mnohem snazší uvádět zcela nepravdivé údaje či pravdivé elektronickou cestou pozměňovat.

Skutková podstata uvedená v § 209 odst. 1 TZ „*Kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci*“ vyžaduje, aby došlo v uvedení v omyl nebo využití něčího omylu a je-li toto možné provést v kyberprostoru, pak je zde možné spáchat tento trestný čin. Trestní zákoník s touto možností také počítá a tak v § 120 TZ definuje, 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.*“

V elektronickém světě je však možné naplnit skutkovou podstatu podvody i téměř „nevinně“. Budeme-li uvažovat o částce vyšší než 5.000,-Kč, aby šlo dle § 138 TZ o škodu nikoli nepatrnou, je možné TČ (při škodě nižší by se jednalo pouze o přestupek spáchaný dle § 50 odst. 1 písm. a) přestupkového zákona) spáchat i tak, že pro vlastní potřebu užijeme peníze z vlastního účtu (buďto je vybereme a utratíme nebo opět v elektronickém světě, tedy v internetovém bankovnictví, s nimi začneme disponovat), které však na tento účet dorazily bez právního titulu a tedy majiteli účtu nenáleží. Pokud v okamžiku jejich použití je majiteli známo, že peníze mu nenáleží, jedná se o podvod a nikoli o zatajení věci dle § 219 TZ, jak by se možná zdálo. Vyplývá

to z Usnesení Nejvyššího soudu ze dne 16. 5. 2007, sp. zn. 5 Tdo 538/2007.[63] Je to možná opět dáno anonymitou kyberprostoru, že by většina takovéto peníze použila. Pokud by se to stalo v běžném světě a někdo nám dával peníze z ruky do ruky, které nám nenáleží, asi bychom se divili a bránili se. Každopádně bychom váhali mnohem déle, zda je utratit. To zkrátka u anonymních peněz neplatí a opět bude platit, že „příležitost dělá zloděje".

Pro páchání podvodů na internetu dnes není nutný ani vlastní počítač. Vše se dá „vyřídit" v internetové kavárně a pravděpodobnost dopadení se tak snižuje, tedy pokud tato kavárna svůj provoz nesnímá kamerami a tyto záznamy nearchivuje. Pokud ano, je dopadení pachatele OČTŘ o něco snazší.[64]

2.10 Poškození cizích práv aneb voyeur v bytě či koupelně

V nedávné době informovala média o dvou právně zajímavých případech[65, 66]. V obou šlo o šmírování nájemníků v pronajatém bytě. Bylo použito webové kamery, která byla připojena k počítači a díky tomu bylo dění v bytě, zejména v koupelně, možné zaznamenat. V novějším případě bylo kamer rozmístěných po bytě více a byly velmi zdařile maskované. Nájemníci tak neměli po dlouhou dobu ponětí, že jsou pozorováni. Motiv byl téměř stejný. Vždy pronajímatel, muž, nabízel svůj byt dívkám, případně párům, aby je mohl skrytě pozorovat. Zda s případnými nahrávka dále obchodoval, či je zpřístupňoval na internetu, se prokázat nepodařilo.

---

[63] Jestliže si pachatel přisvojil peníze, které mu byly omylem zaslány na bankovní účet, s nímž disponoval, pak pro rozlišení, zda tím spáchal trestný čin podvodu (s využitím omylu jiného) nebo trestný čin zatajení věci (tj. věci, která se dostala do moci pachatele omylem) je rozhodující, zda pachatel věděl o omylu jiné osoby v době, kdy se peníze dostaly do jeho moci, tj. když se skutečně dozvěděl o takové platbě na bankovní účet (např. na základě výpisu z účtu). Věděl-li pachatel již v této době, že jde o peníze, které mu byly zaslány omylem, může spáchat jen trestný čin podvodu, nikoli trestný čin zatajení věci.

Uvědomí-li si pachatel omyl (nebo je-li na něj upozorněn) až poté, co již získal cizí věc, za níž se považují i peníze na účtu, do své dispozice (do své moci), nemůže naplnit skutkovou podstatu trestného činu podvodu. V takovém případě není vyloučena jeho trestní odpovědnost pro trestný čin zatajení věci.

[64] Podvodníci falšují doklady a nabízejí fiktivní zboží přes internetové kavárny – http://www.novinky.cz/krimi/395236-podvodnici-falsuji-doklady-a-nabizeji-fiktivni-zbozi-pres-internetove-kavarny.html

[65] „Šmírák z Jihlavy" se psychicky zhroutil. V pondělí dostal podmínku – http://jihlavsky.denik.cz/zlociny-a-soudy/smirak-z-jihlavy-se-psychicky-zhroutil-v-pondeli-dostal-podminku-20140513.html

[66] Sledoval nahé nájemnice kamerami. Byt může pronajímat dál – http://sumpersky.denik.cz/z-regionu/sledoval-kamerami-najemnice-byt-muze-dal-pronajimat-20160205-rzt1.html

Dané jednání je klasifikováno jako poškození cizích práv dle § 181 TZ. U staršího z případů již došlo k odsouzení pachatele. *Za přečin poškozování cizích práv dostal třiapadesátiletý Luboš Vondrák trest dvanáct měsíců s podmíněným odkladem na zkušební dobu třiceti měsíců. Kromě toho propadla státu zabavená kamera a nosiče. Třem ze šesti poškozených nájemníků navíc musí Vondrák zaplatit 130 tisícové odškodné za způsobené psychické trauma dohromady šedesát tisíc korun. Ostatní soud odkázal se svými nároky na civilní řízení.*[67,68]

Pokud rozebereme skutkovou podstatu daného TČ jak je uvedená v ustanovení § 181 odst. 1 TZ – „*Kdo jinému způsobí vážnou újmu na právech tím, že*

a) uvede někoho v omyl, nebo

b) využije něčího omylu,

bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti,“ je zřejmé, že musí dojít k vážné újmě na právech. Je nasnadě otázka, o jaká práva se jedná, zda jakákoli nebo zda zde existuje omezení. Objektem ustanovení § 181 TZ jsou jiná než majetková práva, neboť k ochraně majetkových práv před podvodným jednáním jsou úpravy v § 209 – 212 TZ tj. podvod, pojistný podvod, úvěrový podvod a dotační podvod, jak se dá vyvodit z usnesení Nejvyššího soudu ze dne 16. 7. 2008, sp. zn. 3 Tdo 848/2008. Také je důležité posoudit, co se rozumí vážnou újmou. Pokud použijeme komentář TZ, zjistíme, že: „*Vážná újma na právech vzniká porušením nebo ohrožením subjektivních občanských práv, především na lidskou důstojnost člověka, jeho osobní čest, dobrou pověst, jméno a soukromí. Tímto zásahem do právní sféry poškozeného, který se nedotýká přímo jeho majetkových práv, ale přesto je jím pravém pociťován úkorně, může dojit a často dochází k majetkové újmě, která vzniká buď současně, nebo následně v důsledku primární újmy.*“[69]

V případech šmírování tak došlo k uvedení v omyl, byla způsobena vážná újma na právech, zejména porušení soukromí, jsou zde i osoby pachatelů i o jejich zavinění

---

[67] „Šmírák z Jihlavy“ se psychicky zhroutil. V pondělí dostal podmínku. *Jihlavský deník* [online]. 2014 [cit. 2016-03-01]. Dostupné z: http://jihlavsky.denik.cz/zlociny-a-soudy/smirak-z-jihlavy-se-psychicky-zhroutil-v-pondeli-dostal-podminku-20140513.html

[68] Špehoval nájemníky při sexu! Dostal 2,5 roku a zaplatí 130 tisíc!. *TN.cz* [online]. 2014 [cit. 2016-03-01]. Dostupné z: http://tn.nova.cz/clanek/za-spehovani-najemniku-dostal-dva-a-pul-roku-zaplati-jim-130-tisic.html

[69] DRAŠTÍK, Antonín. *Trestní zákoník: komentář*. Vydání první. Praha: Wolters Kluwer, 2015. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-790-4. s. 996 - 997

nemůže být pochyb. Z uvedeného je zřejmé, že ve zmíněných případech došlo k naplnění všech znaků skutkové podstaty, proto se pronajímatelé dopustili TČ poškození cizích práv.

Bohužel těchto případů bude díky rozvoji techniky dozajista přibývat. Pokud se nechceme stát „hvězdami“ internetu, musíme se kolem sebe zřejmě lépe rozhlížet. Skryté kamery mohou dnes být téměř kdekoli a v čemkoli. Správným dotazem na Ebay.com vyjede nabídka špionážních kamer v cenách od stokoruny a ukrytých v tužce, věšáku, klíči, hodinách, knoflíku nebo i sprchové hlavici. Co vše nám ještě budoucnost přinese?

2.11 Možná budoucí ohrožení

Uvedli jsme několik technik a trestných činů, se kterými je dnes možno se v elektronickém světě setkat, nicméně jejich výčet není ani zdaleka konečný. Technik existuje ještě celá další řada stejně tak i trestných činů, jež jsou v tomto světě páchány. A co hůře, každým dnem se případní pachatelé snaží vymyslet stále propracovanější postupy, jak svých znalostí užít pro svůj prospěch a to i za cenu protiprávního jednání. Bohužel se jim to velmi daří. Není proto možné uvést výčet konečný a vlastně to ani není účelem tohoto díla, neboť by šlo o značně rozsáhlou práci. Přesto je dobré si uvědomit, že s tím, jak bude růst počet „chytrých služebníků a společníků“ nás lidí, bude takovýchto útoků přibývat a jejich cílem se právě tito důmyslní SMART společníci stanou.

V podkapitole 1.8 jsme zmínili fakt, že v domácnosti bude již brzy většina spotřebičů tzv. SMART. Toto se však týká i např. dopravních prostředků, jako jsou letadla, která umí sama létat i přistávat, plánované výstavby metra trasy D v Praze, kde by měly jezdit vlaky, jež budou fungovat bez lidského řidiče nebo brzy i osobní automobily napojené na internet. Vše uvedené se stane cílem útoků a lidstvo by se na to mělo připravit.

Dnešní automobily zatím do procesu řízení zasahují řidiči jen v omezení míře. To se však časem změní a díky jejich napojení na celosvětovou síť bude možné toto řízení ovlivnit, což zcela jistě způsobí nemalé problémy. V roce 2015 již došlo k prvním útokům na automobily, kdy byly skrze internet ovládány cizími útočníky pracujícími na notebooku – „Hacknout přes Internet už jdou i auta. Jako první to schytal Jeep

Cherokee“[70] či „Hackeři se zmocnili Jeepu Cherokee, na dálku ovládnou všechna auta FCA.“[71]

Útoky na mobilní telefony jsou dnes rozšířené a do budoucna toto číslo jistě ještě poroste. Je třeba si uvědomit, že pro některé praktiky je nutné jak napadení počítače, tak i telefonu a to zároveň. Např. v případě phishingu nestačí jen získat přihlašovací údaji k bankovnímu účtu na internetu, neboť banky jakékoli operace jistí skrze autorizační SMS. Pro úspěch je nutné získat kontrolu i nad daným telefonem a tuto autorizaci získat. Proto se dnes začínají útočníci na telefony zaměřovat ve velkém. Na trhu jsou tři hlavní operační systémy telefonů – Android (zcela otevřený systém), iOS (polouzavřený) a Windows Phone (uzavřený), který zřejmě bude nahrazen systémem pouze Windows. Každý ze systémů má své klady i zápory. Pro útočníky bude nejtěžší proniknout do Windows Phone, neboť do tohoto telefonu není možné téměř nic, krom ověřených programů z Windows Store, nainstalovat a tak jsou relativně bezpečné, avšak to se jistě v budoucnu změní[72]. Je nutné mít svůj telefon pod kontrolou, ale to dnes není vůbec snadné. Na pozadí je spuštěno velké množství aplikací a jen skutečný odborník je schopen vše analyzovat.

Hrozbám tak jsme a budeme vystaveni na každém kroku. Přestože jsme si uvedli jen několik málo možných hrozeb[73], jisté je jediné, cokoli v budoucnu bude schopné „komunikace,“ bude nepochybně terčem ataku. Musíme na to být připraveni.

---

[70] webová stránka věnující se této problematice – http://www.tyinternety.cz/novinky/hacknout-pres-internet-uz-jdou-auta-jako-prvni-schytal-jeep-cherokee/

[71] webová stránka věnující se této problematice – http://www.autoforum.cz/zivot-ridice/hackeri-se-zmocnili-jeepu-cherokee-na-dalku-ovladnou-vsechna-auta-fca/

[72] Trojský kůň cílí na Windows 10, útočníci mohou lidem vysát bankovní účty – http://www.novinky.cz/internet-a-pc/bezpecnost/395873-trojsky-kun-cili-na-windows-10-utocnici-mohou-lidem-vysat-bankovni-ucty.html

[73] poznámka autora – některé další možné hrozby a TČ, které nebylo možno, z důvodu obsáhlosti práce, uvést jsou např.: phreaking, cybersquatting, typosquatting, cyberstalking, denigration, masquerade, outing, kybergrooming, avšak opět i TČ bez zvláštních technik, jako je vydírání, porušení tajemství listin a jiných dokumentů uchovávaných v soukromý, porušení tajemství dopravovaných zpráv, šíření poplašné zprávy, padělání a pozměnění veřejné listiny, pak dosti závažné je šíření pornografie a zejména dětská pornografie, bohužel však i mnoho dalších TČ je v kyberprostoru pácháno

3 Porušování autorských práv v prostředí internetu

Jeden druh kriminality páchané v kyberprostoru jsme zatím nezmínili a to i přes nesporný fakt, že patří mezi nejrozšířenější (dá se předpokládat, že každý uživatel internetu se na páchání tohoto deliktu již alespoň jednou podílel) a způsobuje ohromné škody a ovlivňuje společnost jako celek i jeho dílčí části, obzvláště některé podnikatelské záměry. Tímto druhem je porušování autorských práv, jež by, jak bylo v úvodu zmíněno, mělo tvořit hlavní jádro této práce, a proto tuto kapitolu budeme věnovat tomuto nešvaru.

Než však bude možné posuzovat tuto trestnou činnost, je dobré si přiblížit některé pojmy, které jsou pro dané posuzování důležité.

3.1 Škoda, skutečná škoda, ušlý zisk, bezdůvodné obohacení

Za malou chvíli budeme pracovat s pojmem škoda. Je však důležité připomenout, že OZ_{2012} pojem škoda již nebere za východisko, nýbrž vychází z pojmu újma, kterou lze dělit na majetkovou a nemajetkovou. Bohužel však k jasné definici pojmu újma v OZ_{2012}. nedošlo. Jedná se však o právní pojem, tudíž za ni v právním smyslu považujeme jen takovou ztrátu, kterou osoba utrpí na právem chráněném statku. Nicméně zde nalezneme alespoň definici škody, kde z § 2894 odst. 1 vyplývá, že se jedná o újmu na jmění. Přičemž § 495 OZ stanovuje, že „*Souhrn všeho, co osobě patří, tvoří její majetek. Jmění osoby tvoří souhrn jejího majetku a jejích dluhů.*“ Právní ochrany se dostává souhrnu majetkových vztahů a za škodu je považován i vznik dluhu, což platí až od nabytí účinnosti OZ_{2012}, tedy až do 1.1.2014.[74]

Škoda se dělí na skutečnou škodu a ušlý zisk. Skutečná škoda je dle nálezu Ústavního soudu ze dne 30. dubna 2002, sp. zn. ÚS Pl. ÚS 18/01 vymezována jako majetková újma vyjádřitelná penězi, která spočívá ve zmenšení, ve snížení či v jiném znehodnocení již existujícího jmění poškozeného, jakož i ve vynaložení nákladů na odstranění tohoto znehodnocení. Projevuje se zpravidla zmařením podstaty věci (tj. zničením, uvedením do nepoužitelného stavu), její ztrátou či odcizením anebo

[74] HÁLEK, Jakub. *Autorské právo a jeho porušování na internetu z pohledu škody, náhrady škody a bezdůvodného obohacení* [online]. Praha, 2015 [cit. 2016-03-24]. Dostupné z: http://svoc.prf.cuni.cz/sources/8/17/519.pdf. SVOČ. PF UK. s. 6

poškozením. Též ji utváří skutečně vynaložené vedlejší náklady, jež jsou poškozenými vydávány smysluplně a účelně.[75]

„*Ušlý zisk je újmou spočívající v tom, že u poškozeného nedojde v důsledku škodné události k rozmnožení majetkových hodnot, ač se to dalo očekávat s ohledem na pravidelný běh věcí. Nepostačuje přitom pouhá pravděpodobnost zvýšení majetkového stavu v budoucnu, neboť musí být najisto postaveno a v tomto směru je důkazní břemeno na poškozeném, že nebýt protiprávního jednání škůdce (či škodní události u objektivní odpovědnosti) by se majetkový stav poškozeného zvýšil. Ušlým ziskem je nepochybně i jakákoliv ztráta na odměně, kterou lze odškodnit, jestliže škoda způsobená na zdraví znemožnila poškozenému vykonávat činnost vedoucí k dosažení prospěchu, kterého by se mu dostalo v případě, že by k protiprávnímu jednání nedošlo.*“[76]

Pro určení výše ušlého zisku nemůže být náhodné či libovolné. Ale mělo by výpočtem dojít k takovému určení, jež se skutečnosti přibližuje s velkou pravděpodobností. OZ v § 2955 udává, že „*nelze-li výši náhrady škody přesně určit, určí ji podle spravedlivého uvážení jednotlivých okolností případu soud.*“ Pro takovéto určení může být využito tvrzení o konkrétních smluvních vztazích, které měl po rozhodnou dobu poškozený sjednány. U podnikatelských subjektů lze užít i informace o pravidelně se opakujících obchodních příležitostech, o něž v té době přišel, o snížení zisku z podnikání o prostředky vynaložené na mzdu nebo na jiný příjem osoby, která v tomto období za poškozeného vykonávala činnost k dosažení zisku, zatímco předtím tyto prostředky nebyly vynakládány, apod.[77,78]

Bezdůvodné obohacení je definováno v ustanovení § 2991 odst. 1 OZ jež říká, že ten, „*kdo se na úkor jiného bez spravedlivého důvodu obohatí, musí ochuzenému vydat, oč se obohatil.*“ § 2991 odst. 2 OZ pak obsahuje výčet skutkových podstat bezdůvodného obohacení, nicméně tento výčet je pouze demonstrativní.

---

[75] HÁLEK, Jakub. *Autorské právo a jeho porušování na internetu z pohledu škody, náhrady škody a bezdůvodného obohacení* [online]. Praha, 2015 [cit. 2016-03-24]. Dostupné z: http://svoc.prf.cuni.cz/sources/8/17/519.pdf. SVOČ. PF UK. s. 6

[76] Rozsudek Nejvyššího soudu ze dne 28. ledna 2009, sp. zn. 25 Cdo 3586/2006

[77] Ušlý zisk. *Epravo.cz* [online]. 2002 [cit. 2016-03-06]. Dostupné z: http://www.epravo.cz/top/clanky/usly-zisk-15607.html

[78] Rozsudek Nejvyššího soudu ze dne 28. listopadu 2001, sp. zn. 25 Cdo 1920/99

3.2 Nehmotné statky

Nehmotný statek je zvláštní druh objektů právních vztahů. Má nehmotnou povahu, musí však být vyjádřen objektivně, pro člověka poznatelnou formou. Lze jej vymezit i jako statek tvořený konkrétním duševním obsahem, jehož objektivní vyjádření je způsobilé být předmětem společenských vztahů, aniž by bylo nutné jej ztělesnit v hmotné podobě. Přesto má-li být takovýto statek předmětem právní ochrany, musí být vnímatelnou podobu a tato podoba může být také nehmotná – např. zobrazení webové stránky prostřednictvím počítače. Díky této povaze má řadu zvláštních charakteristických znaků, jimiž se od statku hmotného odlišuje. Nehmotný statek je duševní povahy a jeho vnímání je neodvislé od existence hmotného podkladu. Může být kdykoli a kdekoli současně i následně vnímán a užíván neomezeným počtem subjektů a to bez újmy na jeho podstatě či funkci. A převod práva s privativními účinky pro převodce je jeho povahou buď zcela vyloučen, nebo omezen, případně vázán na zvláštní podmínky.[79] Do oblasti nehmotných statků patří především duševní vlastnictví.[80]

3.2.1 Duševní vlastnictví

Co vše chápat jako duševní vlastnictví? Na to nám dá odpověď např. Úmluva o zřízení Světové organizace duševního vlastnictví (WIPO), podepsaná ve Stockholmu dne 14.7.1967, změněná dne 2.10.1979 (vyhl. č. 69/1975 Sb. ve znění vyhl č. 80/1985 Sb.), konkrétně ustanovení článku 2, bod viii) říká, že „duševním vlastnictvím“ se rozumí práva: k literárním, uměleckým a vědeckým dílům; k výkonům výkonných umělců; ke zvukovým záznamům a k rozhlasovému vysílání; k vynálezům ze všech oblastí lidské činnosti; k vědeckým objevům; k průmyslovým vzorům a modelům; k továrním, obchodním známkám a známkám služeb, jakož i k obchodním jménům a obchodním názvům; na ochranu proti nekalé soutěži a všechna ostatní práva vztahující se k duševní činnosti v oblasti průmyslové, vědecké, literární a umělecké.

---

[79] např. ustanovení § 12 odst. 2 AZ – Poskytnutím oprávnění podle odstavce 1 (autor má právo své dílo užít v původní nebo jiným zpracované či jinak změněné podobě, samostatně nebo v souboru anebo ve spojení s jiným dílem či prvky a udělit jiné osobě smlouvou oprávnění k výkonu tohoto práva; jiná osoba může dílo užít bez udělení takového oprávnění pouze v případech stanovených tímto zákonem) právo autorovi nezaniká; autorovi vzniká pouze povinnost strpět zásah do práva dílo užít jinou osobou v rozsahu vyplývajícím ze smlouvy

[80] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. Pro praxi. ISBN 978-80-7380-501-2. s. 331-332

Avšak i předpis EU [81] v článku 2 obsahuje definici, co duševním vlastnictvím rozumí:

a) ochranná známka;

b) průmyslový vzor;

c) autorské právo nebo jakékoli související právo stanovené vnitrostátními nebo unijními právními předpisy;

d) zeměpisné označení;

e) patent stanovený vnitrostátními nebo unijními právními předpisy;

f) dodatkové ochranné osvědčení pro léčivé přípravky stanovené v nařízení Evropského parlamentu a Rady (ES) č. 469/2009 ze dne 6. května 2009 o dodatkových ochranných osvědčeních pro léčivé přípravky;

g) dodatkové ochranné osvědčení pro přípravky na ochranu rostlin stanovené v nařízení Evropského parlamentu a Rady (ES) č. 1610/96 ze dne 23. července 1996 o zavedení dodatkových ochranných osvědčení pro přípravky na ochranu rostlin;

h) odrůdové právo Společenství stanovené v nařízení Rady (ES) č. 2100/94 ze dne 27. července 1994 o odrůdových právech Společenství;

i) odrůdové právo stanovené vnitrostátními právními předpisy;

j) topografie polovodičového výrobku stanovená vnitrostátními nebo unijními právními předpisy;

k) užitný vzor, pokud je vnitrostátními nebo unijními právními předpisy chráněn jako právo duševního vlastnictví;

l) obchodní název, pokud je vnitrostátními nebo unijními předpisy chráněn jako výlučné právo duševního vlastnictví;

Práva k duševnímu vlastnictví dělíme na tvůrčí právo duševního vlastnictví (osobní majetková práva duševního vlastnictví jako výsledek tvorby FO) a na netvůrčí právo duševního vlastnictví (majetková ochranná práva nehmotných předmětů duševního vlastnictví). Pro účely práce nás však z celého výčtu budou v následujících částech zajímat pouze práva k dílům autorským, jež nějak souvisejí s ICT.[82]

3.2.2 Porušování autorských práv na internetu

Dle Smejkala se pachatelé dopouštějí neoprávněného užívání autorských děl v oblasti ICT dvěma způsoby:

- neoprávněným užíváním (a/nebo šířením) počítačových programů – čemuž se věnuje podkapitola 3.4

[81] Nařízení Evropského parlamentu a Rady (EU) č. 608/2013 ze dne 12. června 2013 o vymáhání práv duševního vlastnictví celními orgány a o zrušení nařízení Rady (ES) č. 1383/2003

[82] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. Pro praxi. ISBN 978-80-7380-501-2. s. 333 – 335

- neoprávněným užíváním (a/nebo šířením) jiných autorských děl, zejména pak audio a audiovizuálních děl (hudba, film) – čemuž se věnuje podkapitola 3.3

K takovémuto jednání může dojít jak fyzickým kontaktem (předáním nosiče informací, jako je počítač, USB flash disk, CD či DVD, na kterém se SW či film nachází), tak prostřednictvím internetu pouze v elektronické, tj. nehmotné podobě (zasláním mailem, stažením z ftp či filehostingového serveru, nebo jen sdělením odkazu, kde se nelegální SW či film nachází).[83]

Porušování autorských práv a práv souvisejících s právem autorským je dnes jedním z nejdiskutovanějších a největších problémů v oblasti kybernetické kriminality. Z tohoto důvodu je nutné autorská díla, do kterých řadíme i databáze, chránit. Tato ochrana je realizována prostřednictvím zákona č. 121/2000 Sb., autorského zákona – AZ, ve znění pozdějších předpisů. Ustanovení tohoto zákona odpovídá kontinentálnímu pojetí práva, což znamená, že právo k výsledkům duševní se přiznává fyzické osobě a je řazeno mezi základní lidská práva a jako takové je také chráněno. Ostatně ustanovení čl. 34 odst. 1 LZPS hovoří jasně: „*Práva k výsledkům tvůrčí duševní činnosti jsou chráněna zákonem.*“ Jako taková jsou nezcizitelná a nelze se jich vzdát. Současná právní úprava zákona reaguje na vliv komunitárního práva a posiluje dualismus práv osobnostních a práv majetkových. Nicméně reaguje i na mezinárodní úpravy, ke kterým se zavázala, jako je Bernská úmluva, Římská úmluva, dohoda TRIPS či již zmiňovaná smlouva WIPO. Mezi hlavní principy AZ patří:

1) AZ jako *lex specialis* vůči OZ přebírá jeho základní zásadu – smluvní volnosti; zákonná úprava platí pouze pokud si strany neujednají jinak
2) AZ upravoval jednotný smluvní typ – licenční smlouvu, nicméně tato úprava je dnes již v obecné normě v ust. § 2358 a násl. OZ
3) AZ rozšiřuje hmotněprávní nároky autora, kterých se může v případě porušení svého práva domáhat
4) AZ v souladu s legislativou práva ES přiznává některá nová související práva

[83] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. Pro praxi. ISBN 978-80-7380-501-2. s. 342

5) AZ poskytuje větší ochranu těm nositelům práv, jež investují do šíření svých děl prostřednictvím moderních technologií
6) AZ posiluje postavení investorů – zaměstnavatelů a zavádí nové kategorie děl
7) AZ stanovuje dobu ochrany autorských děl na 70 let po smrti autora[84]

Obsahem autorského práva, tak jak je uvedeno v AZ, jsou dle § 11 výlučná osobnostní práva a výlučná majetková práva dle § 12, což představuje již zmíněný dualismus.

Majetkovými právy jsou:

I) dle § 12 odst. 4 AZ – právo dílo užít a nechat užít (§ 12 AZ),
   a) právo na rozmnožování díla (§ 13 AZ),
   b) právo na rozšiřování originálu nebo rozmnoženiny díla (§ 14 AZ),
   c) právo na pronájem originálu nebo rozmnoženiny díla (§ 15 AZ),
   d) právo na půjčování originálu nebo rozmnoženiny díla (§ 16 AZ),
   e) právo na vystavování originálu nebo rozmnoženiny díla (§ 17 AZ),
   f) právo na sdělování díla veřejnosti (§ 18 AZ), zejména
      1. právo na provozování díla živě nebo ze záznamu a právo na přenos provozování díla (§ 19 a 20 AZ),
      2. právo na vysílání díla rozhlasem či televizí (§ 21 AZ),
      3. právo na přenos rozhlasového či televizního vysílání díla (§ 22 AZ),
      4. právo na provozování rozhlasového či televizního vysílání díla (§ 23

   AZ),
   g) další způsoby užití (§ 12 odst. 5 AZ)

II) dle § 96 odst. 1 písm. a) bod 5. AZ – právo na odměnu při opětovném prodeji originálu díla uměleckého (§ 24 AZ),

III) dle § 71 odst. 3 AZ – právo na odměnu v souvislosti s rozmnožováním díla pro osobní potřebu a vlastní vnitřní potřebu (§ 25 AZ).

---

[84] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. Pro praxi. ISBN 978-80-7380-501-2. s. 344 - 346

Uvedená ustanovení AZ stanovují, že pouze díla v hmotné podobě mohou být užita rozšiřováním, pronájmem, půjčováním a vystavováním originálů a rozmnoženin. Těmito způsoby užití díla tak vůbec nelze prostřednictvím internetu zasáhnout do autorského práva. Naopak na internetu dochází k porušování autorských práv především neoprávněným sdělováním děl veřejnosti. K tomuto sdělování může dojít mnoha různými způsoby, které se liší technologickým provedením. Takovéto možnosti jsme již v první kapitole naznačili, nicméně ještě se k jednotlivým typům vrátíme a právně je posoudíme.[85]

V souvislosti s porušováním AZ v prostředí kyberprostoru bylo, je a jistě ještě bude v ČR rozpoutáno několik zajímavých kauz. Všechny se týkaly „podvodů" s diplomovými pracemi studentů vysokých škol. Buďto byly tyto práce opsány zcela či částečně, přičemž k tomuto došlo díky internetu, kde je možné takovéto práce nalézt, nebo byly použity nezměněné články z webových stránek, které nebyly citovány, ani uvedeny jako zdroj pro dané práce. Díky těmto deliktům došlo k úspěšnému absolvování VŠ i u studentů, kteří k tomuto po takovémto selhání oprávněni nebyli. Poměrně zajímavé na těchto událostech je fakt, že k takovémuto jednání docházelo především od exponovaných lidí, jako jsou politici, čelní představitelé státní správy, nebo i mnoho policistů (státních i obecních) a zaměstnanců vězenství. I toto bohužel doba internetu přináší. Proto AZ musel na toto reagovat a tak v § 31, který upravuje citace, docházelo k mnoha změnám.

3.3 Úprava porušování autorského práva v trestním zákoníku – § 270

Při trestně právním posouzení musíme mít stále na paměti, že trestního práva by se mělo užívat až jako nástroje *ultima ratio*. Vždy je nutné citlivě posoudit, zda není možné protiprávní jednání v této oblasti postihnout dle jiného právního předpisu, tj. jako přestupek či správní delikt dle ustanovení § 105a AZ (přestupky) nebo § 105b (správní delikty právnických a podnikajících fyzických osob). Až teprve poté, pokud by potrestání dle uvedeného předpisu nebylo dostatečné, je vhodné použít nástrojů práva trestního, konkrétně ustanovení § 270 TZ a užití skutkové podstaty zde uvedené.

---

[85] HÁLEK, Jakub. *Autorské právo a jeho porušování na internetu z pohledu škody, náhrady škody a bezdůvodného obohacení* [online]. Praha, 2015 [cit. 2016-03-24]. Dostupné z: http://svoc.prf.cuni.cz/sources/8/17/519.pdf. SVOČ. PF UK. s. 12

§ 270

Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi

(1) Kdo neoprávněně zasáhne nikoli nepatrně do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovému záznamu, rozhlasovému nebo televiznímu vysílání nebo databázi, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.

(2) Odnětím svobody na šest měsíců až pět let, peněžitým trestem nebo propadnutím věci bude pachatel potrestán,

a) vykazuje-li čin uvedený v odstavci 1 znaky obchodní činnosti nebo jiného podnikání,

b) získá-li takovým činem pro sebe nebo pro jiného značný prospěch nebo způsobí-li tím jinému značnou škodu, nebo

c) dopustí-li se takového činu ve značném rozsahu.

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

a) získá-li činem uvedeným v odstavci 1 pro sebe nebo pro jiného prospěch velkého rozsahu nebo způsobí-li tím jinému škodu velkého rozsahu, nebo

b) dopustí-li se takového činu ve velkém rozsahu.

Pokud si rozebereme jednotlivé znaky skutkové podstaty uvedeného trestného činu § 270 TZ, pak dle Šámala je objektem ochrana především vědecké a literární, hudební, výtvarné, audiovizuální a jiné umělecké tvůrčí činnosti a požitků z ní plynoucích, ale i práva výrobců zvukových či zvukově obrazových záznamů, jakož i práva rozhlasového a televizního vysílatele a práva pořizovatelů databází. Objektivní stránka je charakterizována jednáním pachatele, jímž neoprávněně zasáhne nikoli nepatrně do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovému záznamu, rozhlasovému nebo televiznímu vysílání nebo databázi. V daném případě se jedná o blanketní odkaz na zákon upravující práva autora k jeho autorskému dílu, práva související s právem autorským a práva k databázi, což je v ČR již výše zmiňovaný autorský zákon. Výhodou takovéto blanketní úpravy je fakt, že v případě změny AZ nebude nutné měnit i toto ustanovení TZ.[86]

Autorským dílem je dle ustanovené § 2 odst. 1 AZ myšleno dílo literární a jiné dílo umělecké a dílo vědecké, které je jedinečným výsledkem tvůrčí činnosti autora a je vyjádřeno v jakékoli objektivně vnímatelné podobě včetně podoby elektronické, trvale

[86] ŠÁMAL, Pavel. *Trestní zákoník: komentář – zvláštní část*. 2. vyd. V Praze: C.H. Beck, 2012. Velké komentáře. ISBN 978-80-7400-428-5. s. 2737

nebo dočasně, bez ohledu na jeho rozsah, účel nebo význam. Autorským dílem je zejména dílo slovesné vyjádřené řečí nebo písmem, dílo hudební, dílo dramatické a dílo hudebně dramatické, dílo choreografické a dílo pantomimické, dílo fotografické a dílo vyjádřené postupem podobným fotografii, dílo audiovizuální, jako je dílo kinematografické, dílo výtvarné, jako je dílo malířské, grafické a sochařské, dílo architektonické včetně díla urbanistického, dílo užitého umění a dílo kartografické. Dle ustanovení § 2 odst. 2 AZ je za dílo chápán též, jak jsme si již uvedli, počítačový program. V této souvislosti je vhodné uvést, že ne všem dílům je dle AZ poskytována ochrana. Případní zájemci naleznou tyto výjimky v § 3 AZ. Z toho je zřejmé, že není možné spáchat TČ, který by se takovýchto děl týkal, neboť tato díla nespadají pod ochranné ustanovené § 270 TZ.

Dále je třeba mít na paměti, že ne všechny zásahy do práva autorského musí být nutně zásahy neoprávněné. Při splnění určitých podmínek autorský zákon připouští zásahy do autorských práv, aniž by se ten, kdo do těchto práv zasahuje, vystavoval nebezpečí trestního či jiného postihu. Tyto výjimky a omezení autorského práva se nazývají volné užití a bezúplatné zákonné licence. Dle ustanovení § 29 odst. 1 AZ je dílo užito v souladu se zákonem pouze tehdy, pokud takovéto užití vyhovuje tzv. **třístupňovému testu**. Čili výjimky a omezení práva autorského lze uplatnit pouze:

- ve zvláštních případech stanovených v AZ a pouze tehdy
  - pokud takové užití díla není v rozporu s běžným způsobem užití díla
  - a ani jím nejsou nepřiměřeně dotčeny oprávněné zájmy autora

Pokud jakékoli nakládání s dílem nesplňuje byť i jen jedinou z uvedených podmínek, pak se jedná o porušení práva autorského nebo práv souvisejících s právem autorským. Za volné užití díla se dle § 30 AZ považuje takové užití, jež užívá pro osobní potřebu fyzická osoba (zřejmě se netýká FO podnikatele, jež by dílo užíval v souvislosti se svou podnikatelskou činností), přičemž účelem užití díla není dosažení přímého nebo nepřímého hospodářského nebo obchodního prospěchu. Také do práva autorského nezasahuje ten, kdo pro svou osobní potřebu zhotoví záznam, rozmnoženinu nebo napodobeninu díla, nicméně i zde jsou výjimky, které tvoří počítačové programy, databáze, či architektonické dílo stavbou. Dále ustanovení § 30 odst. 3 AZ neumožňuje v rámci volného užití pořízení záznamu audiovizuálního díla při jeho provozování ze záznamu nebo jeho přenosu i pro osobní potřebu fyzické osoby. Jinými slovy nahrávky

v kině (podkapitola 3.4.7), ačkoli by byly opatřené pro vlastní potřebu, nejsou povolené. Volné užití díla však není nadřazeno právu autora opatřit své dílo ochrannými prvky pro ochranu svých práv, a proto autorovi umožňují své dílo opatřit např. prvky, které zabraňují jeho rozmnožování.[87]

Pro naše účely je ještě vhodné uvést, co je chápáno jako audiovizuální dílo. Dle Šámala jsou audiovizuálními díly především díla kinematografická (filmová) a díla televizní, dále jiná zvláštní díla audiovizuální (např. videoklipy, ale i ideografická díla a multimediální díla), jako zvláštní druh uměleckých děl spojených jednotným režijním vedením ke zpracování scénáře (zpravidla na bázi literární předlohy, filmové povídky, hudebního díla atd.) za použití filmové, televizní nebo jiné audiovizuální techniky. Zpravidla jde o dílo skládající se z tvůrčích příspěvků jednotlivých spolupracujících filmových nebo televizních pracovníků (scenáristy, kameramana, herců, architektů apod.), v důsledku toho je třeba rozeznávat na jedné straně audiovizuální dílo (např. filmové či televizní) a práva k němu a na druhé straně jednotlivá díla a výkony užité k jeho tvorbě a výrobě. V AZ je audiovizuální dílo podrobněji upraveno v § 62 – 64. I počítačové programy mají v AZ, oproti již uvedenému, své podrobnější zpracování v § 65 – 66.[88]

K právům souvisejícím s právem autorským jsou také řazena práva výkonného umělce k uměleckému výkonu, právo výrobců zvukového záznamu k jeho záznamu a právo výrobce zvukově obrazového záznamu k jeho prvotnímu záznamu a práva rozhlasového a televizního vysílatele k jeho vysílání. Důvodem zařazení těchto práv do AZ je věcná souvislost těchto práv s autorskými díly. Tato práva související s právem autorským jsou díky tomuto také chráněna prostřednictvím § 270 TZ.[89]

Vrátíme-li se zpět k ustanovení § 270 TZ, tak subjektem je osoba pachatele, která svým jednáním naplnila všechny znaky skutkové podstaty trestného činu. Např. v případě neoprávněného sdílení audiovizuálního díla je pachatelem ten, kdo film dále poskytl. Avšak v případě třeba softwarového deliktu, kterému se budeme věnovat v podkapitole 3.5, může být a často i bývá situace zajímavější, neboť trestného činu se

---

[87] DUBENSKÁ, Petra. *Internetová a počítačová kriminalita*. Praha, 2013. Diplomová práce. PF UK. Vedoucí práce Doc. JUDr. Tomáš Gřivna, Ph.D. s. 63-65

[88] ŠÁMAL, Pavel. *Trestní zákoník: komentář – zvláštní část*. 2. vyd. V Praze: C.H. Beck, 2012. Velké komentáře. ISBN 978-80-7400-428-5. s. 2739-2741

[89] tamtéž s. 2748

dopouští a pachatelem se tak stávají i osoby právnické. Je však takovéto právní posouzení možné? Odpověď, zda se tohoto trestného činu může dopustit i PO, nám poskytuje zákon o trestní odpovědnosti právnických osob a řízení proti nim. V ustanovení § 7 ZTOPO je možné nalézt taxativní výčet TČ, kterých se mohou PO dopustit, a protože zde porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle §270 TZ nalezneme, je odpověď kladná. Právnické osoby mohou tento TČ spáchat a také se tak v životě poměrně často děje.

Posledním typovým znakem je subjektivní stránka. V případě TČ porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 270 odst. l TZ se vyžaduje úmyslná forma zavinění. Úmysl se však musí vztahovat i na pachatelovo vědomí, že v jeho případě šlo o dílo jako výsledek tvůrčí činnosti autora, jako duševní výtvor spočívající v individuálním ztvárnění myšlenky. Obdobně i v případech výkonného umělce, zvukových nebo zvukově obrazových záznamů anebo rozhlasových či televizních vysílání.[90]

Pro rozbor základní skutkové podstaty § 270 TZ je nezbytné ještě uvést, co se rozumí neoprávněným zásahem nikoli nepatrným do zákonem chráněných práv. Znamená to především přivlastnění si autorství k dílu a jakékoli zveřejnění díla bez souhlasu autora anebo sice s jeho souhlasem, ale s provedením změn v díle, s nimiž autor neprojevil souhlas, eventuálně použití díla takovým způsobem, který snižuje uměleckou hodnotu díla. Neoprávněným zásahem do autorských práv je i jednání pachatele, který např. neoprávněně připojí českou zvukovou stopu do originálního video DVD, jež původně nebylo určené pro český trh, avšak po tomto zásahu je dostupnější i žádanější pro i od další veřejnosti.[91]

Pro posouzení trestnosti již zbývá pouze uvést, že zásah do autorských práv musí být nikoli nepatrný. K tomuto posouzení je třeba užít ustanovení § 138 odst. 1 TZ *a simili*, čili musí být způsobena škoda minimálně 5.000,-Kč. V případech kvalifikovaných skutkových podstat ustanovení § 270 TZ je přitěžující zejména vykazuje-li trestná činnost znaky obchodní činnosti nebo jiného podnikání, nebo získá-li pachatel činem pro sebe nebo pro jiného značný prospěch, potažmo prospěch velkého

---

[90] ŠÁMAL, Pavel. *Trestní zákoník: komentář – zvláštní část*. 2. vyd. V Praze: C.H. Beck, 2012. Velké komentáře. ISBN 978-80-7400-428-5. s. 2753

[91] tamtéž s. 2751

rozsahu, opět posouzený dle § 138 odst. 1 TZ. Nicméně se zde objevují ustanovení o způsobení značné škody, či škody velkého rozsahu, ale i páchání takového činu ve značném rozsahu či ve velkém rozsahu. Samozřejmě posouzení za užití § 138 odst. 1 TZ a rozřazení dle číselného určení je snadné, avšak to je až druhý krok. Primárně je nutné škodu či rozsah vyčíslit. A ačkoli by se vše mělo posuzovat na základě konkrétních okolností případu, není určení výše škody, natož pak rozsahu, vůbec nic snadného. Stávající judikatura soudů k danému určení neexistuje. Je pouze judikováno, jak se škoda vyčíslovat nemá, na což poukázal Nejvyšší soud ve svém usnesení ze dne 8. října 2014, sp. zn. 5 Tdo 171/2014, nicméně jak ano, zatím známo není. To je také důvod, proč ani OČTŘ neví, jak dané skutky posuzovat a také důvod, proč se tomuto tématu budeme ještě věnovat. Jednak si situaci rozebereme v souvislosti s judikaturou NS a pak v kapitole vlastních návrhů, kde se pokusíme definovat skutkovou podstatu, která by problém s výpočtem neměla.

3.4 „Pirátství“ audio a audiovizuálních děl

Pirátství, co to vlastně znamená? A proč a jak se vžilo toto pojmenování pro tuto nekalou činnost? „*Pirátstvím rozumíme neoprávněné užívání autorských děl či jiných předmětů ochrany dle práva autorského takovým způsobem, který přísluší pouze nositelům práv k těmto dílům resp. jiným předmětům ochrany. Pirátství je parazitování na duševním vlastnictví někoho jiného a to především za účelem zisku. Pojmenování pirátství vzniklo původně podle pojmenování černých rozhlasových stanic umístěných na lodích, které kotvily v mezinárodních vodách. Tyto stanice neoprávněně vysílaly hudbu, tedy autorská díla. Rozšíření tohoto názvu na celou oblast porušování práv k duševnímu vlastnictví je zcela příhodné. Také námořní pirát okrádal jiné lodě a bral majetek, který nebyl jeho.*“[92] Z tohoto vymezení již odvození pro definici audio a audiovizuálního pirátství nebude složité, a tak audio a „*audiovizuálním pirátstvím rozumíme jakékoli neoprávněné užití“* audio (díla hudebního) nebo *„audiovizuálního díla (tedy díla filmového nebo jiného díla, které se sestává z řady zaznamenaných spolu souvisejících obrazů, vyvolávajících dojem pohybu, ať již doprovázených zvukem či nikoli), zvukově obrazového záznamu a televizního vysílání.*“[93] Podle způsobu

[92] Digitální média a pirátství: Audiovizuální pirátství. *Česká protipirátská unie* [online]. 2007 [cit. 2016-03-11]. Dostupné z: http://www.cpufilm.cz/new/www/txt/audiovizualni_piratstvi.pdf. s. 10

[93] tamtéž s. 11

neoprávněného užití rozdělujeme audiovizuální pirátství do těchto nejčastějších typů:

- výrobkové pirátství (nelegální kopie CD, DVD…)
- neautorizované veřejné projekce (projekce z komerčních nosičů)
- televizní pirátství, krádeže signálu (neoprávněný přenos, či sdělování)
- internetové pirátství (patrně největší problém – viz dále tato podkapitola)
- nekalé pomůcky (pomůcky k prolomení oprávněné ochrany děl)
- paralelní import (oprávněné rozmnoženiny avšak bez licence pro území)

V páté kapitole se budeme zabývat vyšetřováním trestných činů páchaných na internetu, mezi které samozřejmě sdílení hudby a filmů bezpochyby patří. Jako pro každé jiné vyšetřování páchané kriminality je samozřejmě osoba pachatele tím nejdůležitějším. Aby bylo možné zvláště tento typ deliktů odhalovat, případně jim i předcházet, čemuž je věnována kapitola šestá, je nutné porozumět způsobům a důvodům, jak a proč k nim dochází.

Zajisté, odpověď by mohla znít, že se tak děje pro peníze či jiný užitek, a určitě by ve většině případů byla správná. Tato skupina je nejpočetnější a z hlediska trestního práva nejškodlivější. Takovíto lidé ve velkém rozmnožují veškeré filmy, které jen mohou a uploadují je na servery, které za stahování poskytují finanční protiplnění (nejvíce z českých serverů vyplácí Hellshare.cz), jež vždy po dosažení určité výše přepošlou na běžný účet uploadera. Proto tento „uploader“ své linky (odkazy na stažení nasdílených audiovizuálních děl) šíří, kde jen mohou, nejčastěji jako členové nejednoho warezového fóra. Jiná skupina si za účelem svého profitu zakládá webové stránky, kde tato díla distribuují pohromadě, za využití všech možných technických prostředků současného kyberprostoru. O všech těchto možnostech se ještě za malou chvíli zmíníme a právně je rozebereme. Nicméně existuje mnoho pachatelů, kteří ač jednají protiprávně, nemají ze svého konání žádný profit a dělají tak pro zájem skupiny, ve které se pohybují, což bývá povětšinou nějaké internetové fórum, nejčastěji warezové. Dnes již k této situaci dochází jen zřídka, ale ještě cca před 10 lety, kdy se do popředí zájmu dostala technologie DVD, jež přinášela možnosti kvalitního zvuku a obrazu, docházelo k situacím, kdy DVD byly v ČR dostupná, avšak bez české zvukové stopy. V lepším případě DVD obsahovalo české titulky, v horším ani ty ne. Jiné případy podobné situace nastaly v době expanze tzv. trafikových DVD, kdy na nosičích vycházely nejrůznější filmy za velmi zajímavé ceny. Důsledkem nižší prodejní ceny byl fakt, že zahraniční

filmy obsahovaly sice českou zvukovou stopu, nicméně se jednalo o nově pořízený dabing pro distribuci těchto levnějších DVD. Nový dabing byl levnější, než zakoupení práv ke zvukové stopě ke stejnému filmu, která byla již v minulosti pořízena, mnohdy i před rokem 1989. Vycházela tedy média, která byla pro uživatele dostupná, avšak pro filmové nadšence zcela neakceptovatelná. Co v obou případech dělat, pokud chce člověk zhlédnout film v dobré kvalitě, ale s dabingem, na který je zvyklý? Nezbývalo nic jiného, než použít trafiková DVD s českou stopou tvořenou novým dabingem, nebo DVD bez české stopy a technicky je upravit. Touto úpravou dojde k oddělení zvukové stopy od obrazu. Ze starých VHS kazet, které kolovaly, se zvuková stopa převede do digitální podoby. Dochází k jejímu „čištění" a poté synchronizaci s obrazem z DVD. Pokud vše „sedí", dojde ke spojení upravené zvukové stopy a obrazu v nové jiné DVD, které již obsahuje dabing, na který je divák zvyklý. Takovýto postup představuje mnohdy desítky hodin, u kreslených DVD dokonce i stovky hodin práce. Přesto vše tito nadšenci obětovali, aby se mohli se známými podělit. Většinou skutečně bez odměny. Občas sice docházelo k uploadům na servery, které nevyplácely peníze za stahování, nicméně těmto uploaderům pak umožňovaly zdarma stahování neomezenou rychlostí. Což byl „profit" a mnohdy i motivace. Jedním ze serverů, který takto postupoval, byl Rapidshare.com. Po změně tohoto přístupu a také problémům, které později zmíníme, došlo k odlivu klientů a server, který byl skutečnou jedničkou na trhu filehostingových úložišť, začátkem roku 2015 skončil. Jednalo se v těchto případech o protiprávní jednání? Ano, nepochybně. Postižitelné dle TZ? Na toto není odpověď tak jednoznačná, záleželo by na každém jednotlivém posouzení a leckdy by i trestně právní postih byl na místě. Avšak položme si otázku, proč takto tito lidé postupovali? Neměli jinou možnost. Rádi by zakoupili jistě kvalitnější DVD, než která sami „vyrobili", ale ta na trhu nebyla.

Potenciálním pachatelem se může stát i člověk, který touží zhlédnout film, zcela legálně, avšak tuto možnost nemá. Film prostě není v ČR k sehnání a ani česká kina jej nikdy nepromítala. Jak má takovýto „filmový nadšenec" postupovat? Začne se rozhlížet po webových úložištích, ale pokud nebude úspěšný, vyzkouší torrenty, skrze které je možné získat skutečně vše. Nicméně tato technologie znamená připojit se k síti P2P, což s sebou nese i možnost trestního postihu z důvodu, který bude uveden v podkapitole 3.4.2. Z poslední doby je takových dílem třeba film Regression 2015.[94] Česká kina tento

[94] http://www.csfd.cz/film/356862-regression/prehled/

film nenabízela a to i přes zjevný fakt, že divácký zájem by byl, neboť v něm hrají žádaní herci. Film není k dispozici ani na DVD, či v online půjčovnách.

Z uvedených případů je snad zřejmé, že „pirátství" vždy není jen o financích, ale hrají v něm svou roli i jiné faktory, které je třeba zohlednit. Držitelé autorských práv by i tyto důvody měli při určité prevenci vzít v úvahu.

Ačkoli producentům filmových a hudebních děl či softwaru vznikají vysoké škody, obrana či zadostiučinění je prakticky nedosažitelné. Na rozdíl od jiných porušení zákona, např. vraždy, je porušování autorského práva vnímáno mnohem rozporuplněji. Obzvlášť když z něj pachatelům neplyne finanční prospěch. Též případy odhalení pachatele, či jen pouhého zjištění, že dochází k trestné činnosti, nejsou tak snadné. V případě vraždy bude s velkou pravděpodobností nalezeno tělo. U krádeže se zřejmě přihlásí okradený, avšak při porušování autorských práv, ještě ke všemu v prostředí internetu, není možné vše ohlídat. Pokud si držitel práv, případně svaz, který držitele zastupuje, nelegálního obsahu na internetu nevšimne, je ohlášení od jiných uživatelů internetu jen velmi málo pravděpodobné, nicméně i toto se občas stane. Lidé chápou sdílení jako běžnou věc a škodlivost v tomto jednání nevidí. Může to být i náladou ve společnosti, či její kupní síle, kdy lidé na stanovenou cenovou hladinu některých děl nedosáhnou, či se domnívají, že někteří umělci si své odměny nezaslouží, neboť jsou nepřiměřené. Rozbor této problematiky by však sám o sobě mohl být námětem na diplomovou práci, nicméně zřejmě na jiné fakultě než právnické, z tohoto důvodu se my tomuto rozboru nebudeme více věnovat.

Ovšem i v těchto případech platí již zmiňované heslo „příležitost dělá zloděje". Pokud se má uživatel rozhodnout, zda na internetu zhlédne film z online půjčovny, ovšem až po jeho zaplacení, nebo zda se na film podívá zdarma prostřednictví stejné sítě, bude odpověď v drtivé většině jasná. To vše i přes fakt, že bude zřejmě muset chvíli čekat na stažení filmu z úložiště (i když jsou i postupy jak sledovat film, který se ve stejnou chvíli stahuje) a toto dílo bude možná i v horší kvalitě, než případné vypůjčené. Zkrátka cena na našem trhu rozhoduje. Z uvedeného je zřejmé, že kampaně typu „rohlík či auto byste také neukradli, tak proč film ano?", které společnosti, jež se snaží nelegálnímu stahování zabránit, používají v boji proti stahování, nemohou fungovat. Pokud by zmíněný rohlík, či auto, byly volně k dispozici, jistě by se jich brzy někdo zmocnil. Existuje mnoho studií či pokusů, kdy je ve městě odloženo nezajištěné

avšak monitorované kolo, a kolemjdoucí na tuto situaci reagují. V mnoha případech netrvá dlouho a kolo je odcizeno. Na celém je zajímavý i fakt, že se tohoto jednání dopouští lidé, kteří mají dobré příjmy a doposud nikdy nespáchali byť pouhý přestupek proti majetku. Přesto i tito využili příležitosti a kolo odcizili. Pokud je tedy film k dispozici zdarma, bude se stahovat. Pro řešení je nutné zaměřit se především na uploadery, kteří film distribuují nebo jinak motivovat downloadery, aby vyžadovali pouze legální zdroje. O nějaké návrhy, jak tohoto docílit se v šesté kapitole pokusíme.

Vraťme se ale zpět k deliktům souvisejícím s audio a audiovizuálními díly. V následujících podkapitolách si představíme některé způsoby, jakými dochází v prostředí internetu, k šíření těchto děl a pokusíme se právně posoudit postavení jednotlivých účastníků celého procesu sdílení. Poukážeme na postavení uploadera, tedy toho, kdo kopii díla na internet umístil, dále na downloadera, jenž si dílo prostřednictvím internetu opatřuje pro svou potřebu a v neposlední řadě i na postavení provozovatele serveru, kde je možné daná díla nalézt, tedy pokud se tento v procesu sdílení vyskytuje.

3.4.1 Webová úložiště

Jednu část první kapitoly jsme filehostingu již věnovali. Proč je ale tento prostor z hlediska pirátství tak důležitý? Odpověď je nasnadě. Tyto servery poskytují tolik žádané místo, kam je možné kopie hudby a filmů umisťovat. Samozřejmě tak nečiní jako dobrodinci, ale moc dobře si uvědomují, že jen díky žádanému obsahu budou jejich stránky navštěvované. Stránky, které jsou plné reklamy a tak poskytují provozovatelům značný finanční příjem. Dalším příjmem jsou uživatelé, kteří chtějí stahovat. Mají možnost využít omezené rychlosti či jiné limitace, službu která je zdarma, jen za navštívení stránky a zhlédnutí reklamy, nebo si připlatit za neomezené stahování, což přináší další zmiňovaný nemalý profit. Aby si provozovatelé serverů zajistili žádoucí obsah, motivují různými pobídkami uživatele, aby na servery data nahrávali, ale to jsme již zmiňovali. Zajímavý je i fakt, že se téměř všechny servery vymezují jako „legální“ úložiště, tedy pro data, jež jsou nahrána v souladu se zákony, např. fotografie z dovolené, které někdo nasdílí pro přátele, neboť je nechce nebo nemůže sdílet mailem. Tato činnost však skutečně představuje pouze 5 – 10 % celkového obsahu. Zbytek tvoří nelegální díla a jedině ta zajistí dostatečný počet návštěvníků, kteří „přináší“

provozovatelům finance. Statistika je jasná, z legálního sdílení by provozovatelé serverů nepřežili. A ačkoli provozovatelé hrdě prohlašují, že dělají vše pro ochranu autorských práv, sami však nelegálně nahraný obsah nikterak nevyhledávají a data mažou až po stížnostech.[95] Vzhledem k počtu souborů by to ani nebylo technicky proveditelné. Jak také zajistit stoprocentní účinnost, když metody sdílení jsou a vždy budou před jakýmkoli vyhledávačem. Málokterý uploader dnes nasdílí film pod jeho názvem a ještě ve formátu videa, tedy avi, mkv, mp4 či další možné. Dnes jsou filmy k nalezení jako různé abstraktní názvy s koncovkou např. PDF. Soubor se tedy vydává za textový dokument. Teprve po stažení do počítače dojde ke změně formátu, kdy je koncovka PDF zaměněna např. na ZIP či RAR. Tedy komprimovaný soubor, který je nutné za pomoci příslušného programu tzv. „rozbalit" a mnohdy je ještě k tomuto nutné heslo. Je jasné, že obyčejný uživatel tyto informace, natož heslo nezná a nemá, proto se k obsahu dostane jen ten, kdo je podle uploadera k tomuto oprávněn. Může to být člen skupiny, fóra nebo sociální sítě. Naopak majitelé autorských práv či zastupující organizace toto neví a tak ani na daný soubor upozornit nemohou. Tento tak zůstane k dispozici mnohem delší dobu než by tomu bylo, kdyby obsahoval název nějakého filmu.

Z uvedeného je zřejmé, že stahování díla z internetu, pro které se i v české informační společnosti vžil z angličtiny převzatý termín downloading, je další tradiční forma užití díla v celosvětové počítačové síti a vlastně i neuvěřitelný fenomén. S rozvojem techniky, rychlosti připojení a stále větším počtem děl umístěných na hostingových serverech (zejména MP3 hudebních souborů, videí, různých aplikací či počítačových programů) se stahování stalo vedle navštěvování a obyčejného prohlížení webových stránek naprosto běžnou činností většiny uživatelů internetu. S postupem času a nových technologií se rychle rozšiřuje výčet zařízení, pomocí kterých je možné k filehostingu přistupovat a poté soubory stahovat. Dnes je tak normální stahovat film či hudbu do SMART telefonu a rovnou si v něm tato díla přehrávat.[96]

Na úložištích se krom zmiňovaných děl objevují i různé „naskenované", ofocené či elektronické knihy a to jak učební, tak i jiná literatura, což pro držitele autorských

---

[95] Nelegální obsah sami nehledáme, smažeme ho až po stížnosti, říká spolumajitel Ulož.to.*Ihned.cz* [online]. 2012 [cit. 2016-03-12]. Dostupné z: http://byznys.ihned.cz/c1-54928870-nelegalni-obsah-sami-nehledame-smazeme-ho-az-po-stiznosti-rika-spolumajitel-uloz-to

[96] FRIČ, Antonín. *INTERNET A AUTORSKÉ PRÁVO*. Praha, 2011. Diplomová práce. PF UK. Vedoucí práce JUDr. Irena Holcová. s. 46-47

práv představuje obdobný problém, se kterým se také snaží bojovat. Nutno přiznat, že také marně.

3.4.1.1 Právní posouzení sdílení prostřednictvím webových úložišť

Uploader a jím nasdílený obsah. Zde je situace z hlediska právního posouzení nejjednodušší, neboť sdílení audio a audiovizuálních děl není bez souhlasu nositele práv možné a proto je za toto jednání uploader vždy právně odpovědný. Záleží jen na posouzení každého jednotlivého případu, o jakou odpovědnost se bude jednat.

Situace je zřejmá, kdo neoprávněně zpřístupňuje díla v nehmotné podobě (vymezení viz §18 AZ), tj. bez souhlasu nositele autorského práva a práv souvisejících s právem autorským, v našem případě, zvukově či obrazově-zvukovým záznamem nebo vysíláním rozhlasu nebo televize, která jsou předmětem ochrany podle autorského zákona, dopouští se porušení autorského práva a práv s ním souvisejících a měl by si být vědom možných nepříznivých důsledků, které pro něho z jeho jednání vyplývají. Odlišujeme tři základní typy odpovědnosti, které mohou v důsledku porušování autorského práva vyvstat, a to občanskoprávní, přestupkovou a trestní odpovědnost.

OBČANSKOPRÁVNÍ ODPOVĚDNOST: V § 40 AZ jsou vymezeny nároky, kterých se může autor domáhat v občanskoprávním řízení v případě, že bylo do jeho práva neoprávněně zasaženo, nebo pokud jeho právu hrozí neoprávněný zásah. Zejména dále AZ v § 40 odst. 4 stanoví, že právo na náhradu škody a na vydání bezdůvodného obohacení podle zvláštních právních předpisů tedy občanského zákoníku zůstává nedotčeno a že místo skutečně ušlého zisku se autor může domáhat náhrady ušlého zisku ve výši odměny, která by byla obvyklá za získání takové licence v době neoprávněného nakládání s dílem. Výše bezdůvodného obohacení vzniklého na straně toho, kdo neoprávněně nakládal s dílem, aniž by k tomu získal potřebnou licenci, pak činí dvojnásobek odměny, která by byla za získání takové licence obvyklá v době neoprávněného nakládání s dílem.

PŘESTUPKOVÁ ODPOVĚDNOST: V méně závažných případech, kdy neoprávněné jednání nenaplňuje znaky trestného činu porušení autorského práva, práv souvisejících s právem autorským a práv k databázi podle § 270 TZ, a je tak klasifikováno jako přestupek, hrozí narušiteli na základě § 105a – 105c AZ pokuta až 150 000,- Kč. OČTŘ posoudí intenzitu neoprávněného zásahu do

autorských práv, tedy počet a rozsah dílčích útoků. Také zahrnou a zhodnotí celkovou dobu trvání protiprávního jednání, počet a charakter předmětů ochrany, do jejichž práv bylo neoprávněně zasaženo, a dále i osobu pachatele, míru jeho zavinění a jeho pohnutku, význam chráněného zájmu, který byl činem dotčen, způsob provedení činu a jeho následky a okolnosti, za kterých byl čin spáchán, a rozhodne, zda se v konkrétním případě jedná o zločin, přečin či „pouze" o přestupek.

TRESTNĚPRÁVNÍ ODPOVĚDNOST: Pokud však intenzita porušení bude OČTŘ posouzena jako vyšší a čin pro společnost nebezpečnější, nebude již možné jednání posoudit dle jiného právního předpisu než je TZ a bude se jednat o TČ dle § 270 TZ, jež jsme si důkladně přiblížili v podkapitole 3.3. Posouzení se bude lišit pouze v subsumování pod jednotlivé odstavce dané skutkové podstaty.

Uploaderovi tedy za sdílení hrozí:

1. povinnost nahradit způsobenou škodu a vydat bezdůvodné obohacení (občanskoprávní odpovědnost, možno však požadovat i v adhezním řízení v rámci řízení trestního) – tato odpovědnost nastane vždy
2. pokuta až 150.000,- Kč pokud dojde k posouzení, že šlo o přestupek
3. možný i trest odnětí svobody, trest peněžitý, trest propadnutí věci – počítače, kamery, kopií díla atd. pokud bude jednání posouzeno jako TČ

Je třeba také připomenout, že jak návodce, tak i pomocník nebo i případný organizátor TČ budou trestně odpovědní stejně jako pachatel, a může jim být uložen stejný trest.[97]

Downloader, tedy osoba, jež si dílo stáhne a nebude jej dále šířit, pouze užije pro svou osobní potřebu, bude právně posouzen zcela jinak. Nutno však dodat, že názory na posouzení stahování se různí. Pohledy na situaci jsou dva. Jedno stanovisko chápe i téměř veškeré stahování jako nelegální a druhé naopak jako legální, neb se jedná o výjimku volného užití dle § 30 AZ. Oba názory porovnáme a pokusíme se vyslovit jasný závěr, jak to se stahováním, podotkněme pouze v ČR, vlastně je.

[97] Odpovědnost za porušení autorského práva. *Česká protipirátská unie (ČPU)* [online]. [cit. 2016-03-12]. Dostupné z: http://www.cpufilm.cz/new/www/odpovednost.html

Jeden pohled na právní posouzení stahování, tedy zhotovení kopie pro osobní potřebu, je, že za určitých podmínek je toto legální. Jedná se u využití § 29 odst. 1 AZ a již zmíněného třístupňového testu. Musí se jednat o dílo již zveřejněné a kopii si musí zhotovit ten, jehož osobní potřebě bude sloužit. Zároveň však takové jednání nesmí být v rozporu s běžným způsobem užití díla a ani jím nesmí být nepřiměřeně dotčeny oprávněné zájmy autora. Dále jednání nesmí být v rozporu s dobrými mravy dle § 2 odst. 3 OZ. Problém je však v tom, že soubory, které různé osoby uložily na filehostingové servery, nebyly zhotoveny se souhlasem nositele autorských práva a jsou sdělovány veřejnosti v rozporu se zákonem. Stahování z těchto serverů tak nesplňuje jednu z podmínek testu, neboť se jedná a stahování z nelegálních zdrojů v návaznosti na protiprávní jednání jiných osob. Navíc opakované a početné stahování z nelegálních zdrojů nesplňuje ani jednu z podmínek testu, a jedná se proto dokonce o více závažné protiprávní jednání.[98]

Tento názor, že stahovat z internetu v souladu s právem je možné jen tehdy, dochází-li ke stažení legálně umístěného díla, u nelegálně umístěných děl je stahování vždy nezákonné, zastává především ČPU a jí podobné organizace, které autory zastupují, avšak i řada právníků. „*Stahovat data z nelegálního zdroje není povolené ani pro osobní potřebu, říkají odborníci z TaylorWessing e|n|w|c Advokáti.*“[99]

Druhý pohled je tedy opačný. Po technické stránce se jedná o vytvoření elektronické kopie autorského díla v digitální podobě z pevného disku internetového serveru. Z ustanovení § 12 odst. 4 AZ přichází do úvahy pouze rozmnožování díla. Uživatel, který si na webové stránce úložiště vyhledá a stáhne prostřednictvím prohlížeče data představující dílo, jedná ve smyslu § 13 AZ, neboť stažením dat dojde k jejich rozmnožení. Jedná se o vědomé a cílené stahování určitého obsahu díla uživatelem z webové stránky. Autorský zákon říká, že zhotovování rozmnoženin v digitální podobě je užitím díla se všemi autorskoprávními důsledky. Naprostá většina stahovaných děl však bude spadat pod výjimku institutu volného užití díla, konkrétně tedy rozmnožováním díla pro osobní potřebu podle § 30 odst. 1 a 2 AZ. V zákoně není

[98] F.A.Q. - Často kladené otázky. *Česká protipirátská unie (ČPU)* [online]. [cit. 2016-03-12]. Dostupné z: http://www.cpufilm.cz/faq.html

[99] Stahovat data z nelegálního zdroje není povolené. *Stance.cz* [online]. 2015 [cit. 2016-03-12]. Dostupné z: http://www.stance.cz/stahovat-data-z-nelegalniho-zdroje-neni-povolene-ani-pro-osobni-potrebu-rikaji-odbornici-z-taylorwessing-enwc-advokati-1370/ - stanovisko právníka Petra Dobeše

stanoven žádný požadavek na právní povahu zdroje, ze kterého je možné rozmnoženinu zhotovit. Může se jednat jak o originál, tak i již o rozmnoženinu díla, což je pro aplikaci této výjimky v rámci internetu zásadní. Současně musí být tato výjimka vykládána i v souladu s již zmiňovaným třístupňovým testem, který je zakotven v § 29 odst. 1 AZ.[100]

Z uvedeného důvodu autor této práce zastává názor, že stahování pro vlastní potřebu splňuje podmínku třístupňového testu vždy, ať se jedná o dílo zpřístupněné legálně, či nasdílené v rozporu se zákonem, a proto je takové stažení v souladu se zákonem a neměl by za něj být nikdo postihován. Obdobné stanovisko zastává i Čermák[101], neboť během své přednášky na PF UK toto potvrdil.

Jednak je z hlediska práva jednodušší předpokládat, že stahování všech audiovizuálních děl pro svou potřebu je oprávněné, než dokazovat každému downloaderovi, že měl a mohl vědět, že jím stažené dílo je umístěno nelegálně. A pak je nutné zohlednit fakt, že v ČR jsou zákonem vymezené peněžní odvody – autorské poplatky, které byly stanoveny vyhláškou č. 488/2006 z listopadu 2006. Jejich smyslem je kompenzace ztrát z výdělků autorů způsobených rozmnožováním autorsky chráněných děl. Finanční prostředky získané z těchto poplatků spravuje OSA (Ochranný svaz autorský) a Integram (Nezávislá společnost výkonných umělců a výrobců zvukových a zvukově obrazových záznamů). Každý u nás platí při nákupu určitých produktů poplatky, již v ceně obsažené, které poté obdrží tvůrci děl. Jedná se např. o CD, DVD, HDD, ale i USB flash disky, avšak poplatky platíme také při nákupu tiskáren, notebooků i telefonů. Zákonodárce tedy primárně předpokládá, že každý v této zemi veškeré takto nakoupené zboží používá jen k účelu šíření nelegálního obsahu. Jinak není možné si danou normu vyložit. Dokonce i v situaci, kdy někdo podniká např. v oboru videostudio jako kameraman svateb, které po natočení sestříhá a připraví na DVD, musí při nákupu nosičů poplatky uhradit, ačkoli je jasné, že jeho prioritou není nelegální šíření. Náhradní odměny nemohou být ani vráceny po doložení situace, že DVD nebyla užita k nelegální činnosti, protože to neumožňuje AZ ani vyhláška 488/2006 Ministerstva kultury, která určuje typy přístrojů, nosičů a výši odměn. Tyto

[100] FRIČ, Antonín. *INTERNET A AUTORSKÉ PRÁVO*. Praha, 2011. Diplomová práce. PF UK. Vedoucí práce JUDr. Irena Holcová. s. 47-48

[101] přednáška Internet a autorské právo I. JUDr. Jiřího Čermáka konána dne 10. března 2016 na PF UK v rámci předmětu Právo duševního vlastnictví II. – HP2019

poplatky dle názoru autora musí něco kompenzovat a touto kompenzací je právě možný výklad nezákonně nasdílených děl, kdy tato budou spad po institut volného užití dle § 30 AZ, jak jsme si výše uvedli. Názor autora by mohl být podpořen i usnesením NS[102], které sděluje: „*Ze znění ustanovení § 30 odst. 1 písm. a) AZ nelze dovozovat, že se omezení autorského práva pro pořizování rozmnoženiny díla pro osobní potřebu vztahuje pouze na pořízení rozmnoženiny z originálu díla nebo z jeho legálně zakoupené kopie pořizovatelem rozmnoženiny, neboť v rámci omezení autorského práva pro pořizování rozmnoženin pro osobní potřebu nestanoví toto ustanovení nic o právní povaze zdroje, ze kterého je možno rozmnoženinu díla pro osobní potřebu pořizovat.*“

Bohužel však tento názor autora potažmo NS bude narážet na právo EU. Je totiž v rozporu s posledním rozsudkem SDEU, který se této záležitosti týkal. Autor práce s tímto rozsudkem souhlasí jen částečně a domnívá se, že zatím není reálné jeho uplatnění v praxi ve všech zemích EU, a proto způsobí v některých zemích spíše problémy. Více k rozsudku v následující podkapitole.

Provozovatelé filehostingových serverů nejsou za obsah svých úložišť primárně odpovědní. V České republice upravuje tuto oblast zákon č. 480/2004 Sb., o některých službách informační společnosti. Ten omezuje odpovědnost provozovatelů úložišť dle ustanovení § 5 tohoto zákona, neboť se v jejich případě jedná o služby spočívající v ukládání obsahu informací poskytovaných uživatelem, na 3 případy:

- jestliže provozovatel mohl vzhledem k okolnostem vědět o tom, že obsah je závadný
- jestliže se provozovatel prokazatelně dozvěděl o protiprávní povaze obsahu uživatele a neprodleně neučinil veškeré kroky, které lze po něm požadovat, k odstranění nebo znepřístupnění takovýchto informací
- jestliže provozovatel vykonával přímo či nepřímo rozhodující vliv na činnost uživatele.

Odpovědnost provozovatelů nastupuje jen ve výše uvedených třech případech. Zákon č. 480/2004 Sb. je implementací evropské směrnice[103], konkrétně její článku 14

[102] Usnesení Nejvyššího soudu ze dne 25. března 2009, sp. zn. 5 Tdo 234/2009

[103] Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. 6. 2000 o některých právních aspektech služeb informační společnosti, zejména na elektronickém obchodu na vnitřním trhu (směrnice o elektronickém obchodu)

obsahuje vzor pro § 5 našeho zákona. Omezení odpovědnosti provozovatele jak v naší, tak i evropské úpravě má sloužit k tomu, aby nebylo bráněno poskytování služeb prostřednictvím internetu. Není totiž rozumné ani reálné požadovat od poskytovatelů, aby při značném a stále se zvyšujícím počtu uživatelů a vysokém objemu uložených dat zjišťovali a posuzovali legálnost či nelegálnost veškerého uloženého obsahu. Toto musí zůstat v kompetenci samotných uživatelů, jaký obsah na poskytnutém serverovém prostoru uloží, včetně jejich případné odpovědnosti za obsah nezákonný. Poskytovatelé nemají povinnost aktivně sledovat materiály, jež jsou na jejich serverech uloženy. Jak Soudní dvůr Evropské unie, tak Evropský soud pro lidská práva, který je příslušný k výkladu Evropské úmluvy o ochraně lidských práv, přitom kladou důraz na to, že služby informační společnosti slouží i k šíření myšlenek a idejí a proto se na ně vztahuje také ochrana svobody projevu.[104]

3.4.1.2 Stahování v jiných zemích EU a stanovisko SDEU

Ačkoli je stahování audio a audiovizuálních děl pro vlastní potřebu dle mínění autora v ČR legální, situace v jiných zemích EU je mnohde zcela odlišná. Většina zemí výjimku v jejich autorském zákoně ohledně pořizování kopií pro vlastní potřebu zakotvenu nemá. Např. pokud si někdo v Německu, byť jen na návštěvě, z veřejného zdroje stáhne film, majiteli bytu brzy do schránky dorazí dopis od právníka, který zastupuje společnost, jejíž práva tímto stažením dotyčný porušil. Psaní bude obsahovat poučení, čeho se dopustil, výpis od ISP jaký soubor a jak dlouho stahoval a závěrem bude přiložena faktura, v námi dokládaném případě viz příloha č. 1, k úhradě 450€ za stažený film a 506€ za právní výlohy. Téměř tisíc euro na jeden film je cena, která by mnoho rodin v ČR ekonomicky zruinovala, a to jen za jeden film. Při počtu, v jakém dochází ke stahování u nás, by tyto sumy byly astronomické. Přesto takováto pravidla jsou v některých zemích EU akceptována.

Ve Velké Británii byla ještě nedávno situace obdobná té v České republice. Pro osobní potřebu bylo také možné si pořídit kopii díla. Nicméně v červenci 2015 londýnský Vrchní soud svým rozhodnutí toto změnil. Od tohoto rozhodnutí je kopie pro

---

[104] Jaká je odpovědnost provozovatelů internetových úložišť za obsah uložený jejich uživateli? Odpověď na tuto otázku je třeba hledat jak v českém, tak v evropském právu. *Idnes.cz*[online]. 2013 [cit. 2016-03-13]. Dostupné z: http://finance.idnes.cz/odpovednost-provozovatelu-internetovych-ulozist-fxr-/pravo.aspx

osobní potřebu nezákonná. Takže pokud si někdo koupí album a nahraje si některé skladby do telefonu nebo iPodu, tak porušuje zákon. S největší pravděpodobností se jednalo o jistou harmonizaci s rozhodnutím SDEU dle rozsudku Soudního dvora C-435/12 ze dne 10. dubna 2014, tedy s právem EU, které zřejmě brzy ovlivní rozhodování soudů i v zemích, které kopie pro vlastní potřebu zatím umožňují.[105,106]

Rozsudek C-435/12 ze dne 10. dubna 2014 Soudního dvora EU ve věci ACI Adam BV a další proti Stichting de Thuiskopie, Stichting Onderhandelingen Thuiskopie vergoeding. Předmětem byla žádost o rozhodnutí o předběžné otázce na základě článku 267 SFEU, podaná rozhodnutím Hoge Raad der Nederlanden (Nejvyšší soud Nizozemska) ze dne 21. září 2012, došlým Soudnímu dvoru dne 26. září 2012.

K otázce oprávněnosti zdroje, ze kterého je soukromá rozmnožena pořizována se před nedávnem vyjádřil čtvrtý senát SDEU ve rozsudku ve věci C‑435/12. Soud v rozsudku mimo jiné jednoznačně stanovil, že „*…unijní právo, konkrétně čl. 5 odst. 2 písm. b) směrnice 2001/29 ve spojení s odstavcem 5 tohoto článku, musí být vykládáno v tom smyslu, že brání takovým vnitrostátním právním předpisům, jaké jsou dotčeny v původním řízení, které situaci, kdy zdroj, z něhož je rozmnožena pro soukromé užití pořízena, je oprávněný, neodlišují od situace, kdy je tento zdroj neoprávněný.*“[107]

Rozsudek SDEU vyvolává otázku, zda něco pro nás v ČR znamená a bude se měnit trestněprávní posouzení stahování? Rozhodnutí s největší pravděpodobností zatím nemá a snad ani nebude mít přímý vliv na české trestní právo. Je zřejmě i nadále nutné posuzovat otázku právní povahy zdroje rozmnoženiny, tedy otázku, zda je relevantní, z jakého zdroje je rozmnožena pořízena. Jak jsme již uvedli, stávající právní předpisy a judikatura automaticky nezakládají trestněprávní odpovědnost při stažení díla chráněného autorským právem pro osobní potřebu z nelegálního zdroje. Rozhodnutí SDEU však může v budoucnu znamenat změnu české legislativy. Ve svém důsledku

---

[105] UK: Copyright – private copying exception falls. *Bird and Bird Lawyers* [online]. London, 2015 [cit. 2016-03-13]. Dostupné z: http://www.twobirds.com/en/news/articles/2015/uk/copyright-private-copying-exception-falls

[106] Británie se vrací do středověku a kopie hudby pro osobní potřebu je (znovu) nezákonná. *Wordpress.com* [online]. 2015 [cit. 2016-03-13]. Dostupné z: https://rychlofky.wordpress.com/2015/07/17/britanie-se-vraci-do-stredoveku-a-kopie-hudby-pro-osobni-potrebu-je-znovu-nezakonna/

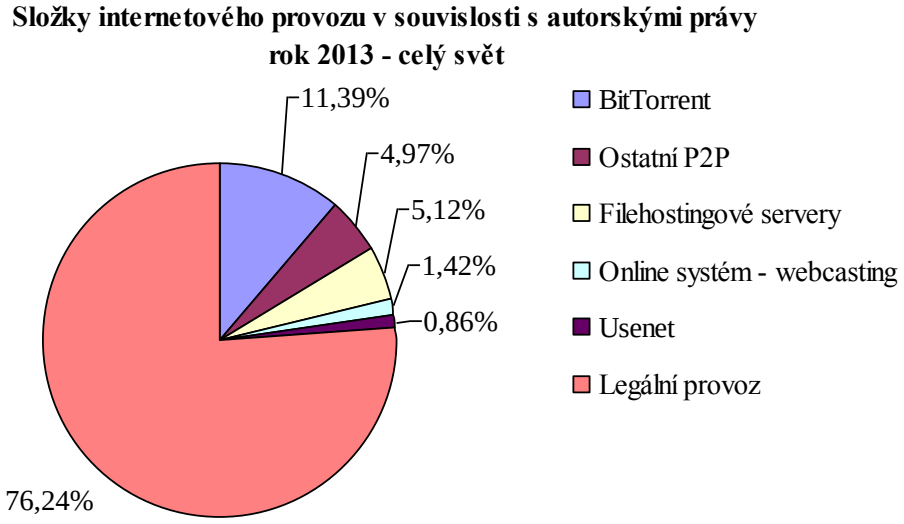
[107] Směrnice Evropského parlamentu a Rady 2001/29/ES ze dne 22. května 2001 o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti

může nepřímo zapříčinit změnu trestního práva a s tím i návaznost trestněprávní odpovědnosti na otázku oprávněnosti zdroje, ze kterého je rozmnožena pro užití pro osobní potřebu pořizována.[108]

3.4.2 P2P – BitTorrent sítě jako prostředek šíření nelegálního obsahu

I P2P sítím jsme se v úvodu věnovali, proto se nyní soustředíme hlavně na jednu z nich, tedy BitTorrent, neboť toto jsme avizovali, a opět se sdílení v rámci této sítě pokusíme právně posoudit.

Obecně platí, že sdílení a stahování autorských děl v rámci výměnných sítí typu P2P hraje co do objemu již nějakou dobu prim v užívání děl pomocí internetové sítě, a nutno říci, že hlavně v užívání neoprávněném. Právě síť BitTorrent je v současné době na celém světě tou nejužívanější (viz graf 1, autorem sestavený dle nalezených dat) pro šíření nelegálního obsahu, a z tohoto důvodu je pro držitele autorských práv tou „nejproblematičtější".



Graf 1

BitTorrent však původně nevznikl jako další ze systémů ke sdílení dat, nýbrž

[108] Trestněprávní odpovědnost za pořízení rozmnoženiny autorského díla pro osobní potřebu z nelegálního zdroje. *Davidzahumensky.cz* [online]. 2015 [cit. 2016-03-13]. Dostupné z: http://www.davidzahumensky.cz/2014/05/28/trestnepravni-odpovednost-za-porizeni-rozmnozeniny-autorskeho-dila-pro-osobni-potrebu-z-nelegalniho-zdroje/

jako distribuční mechanismus pro velké soubory, aby svým systémem provozu mohl předejít nutnosti použití silného serverem, odkud by šel případný velký soubor stahovat. Pořízení silného serveru by jednak zvyšovalo náklady na distribuci a jednak při enormním zájmu o soubor by byla jeho dostupnost snížena. Alternativou je tak nabídnout možnost stahovat nejen z jednoho serveru, ale současně z počítačů těch, kteří si jej již stáhli nebo právě stahují a některé části souboru se již nachází v jejich zařízeních. Avšak aby bylo možné stahovat jediný soubor z více zdrojů současně, je nutné jej nějakým vhodným způsobem rozdělit na určité množství menších částí. Každá tato část je kouskem skládačky, která se nakonec složí do původní podoby celku. Každá část může pocházet z jiného místa. V kontextu dělení pak hovoříme o dvou kategoriích uživatelů, o tzv. seedrech a leecherech. Seedři jsou ti uživatelé, kteří již mají celé zpřístupňované dílo uložené ve svém počítači a poskytují jej ke stažení. Leecheři jsou pak všichni ostatní uživatelé, kteří dílo stahují. Jediné, co je poté nutné k sestavení v původní soubor, je přesný popis celku. Tento popis je u technologie BitTorrent uložen v samostatném souboru s příponou **.torrent**. Jakmile je zahájeno stahování souboru, stává se tento stahující klient zároveň prvkem, který již stažené součásti nabízí dál a to je onen právní problém pro posouzení legálnosti P2P sítí, avšak o tom více v další podkapitole.[109]

Význam této technologie je patrný i z mediální odezvy, kterou vyvolala kauza ve věci švédského serveru The Pirate Bay, který provozoval BitTorrent tracker a též velmi obsáhlou databázi torrent souborů. S jistotou je možné označit kauzu za největší svého druhu v celé historii porušování autorských práv. Rozsáhlá společenská diskuze kolem ní eskalovala otázku nepřímé odpovědnosti provozovatelů obdobných serverů. My se však této kauze věnovat nebudeme a případné zájemce odkážeme na články na internetu, kterých je celá řada (viz poznámka pod čarou[110]).

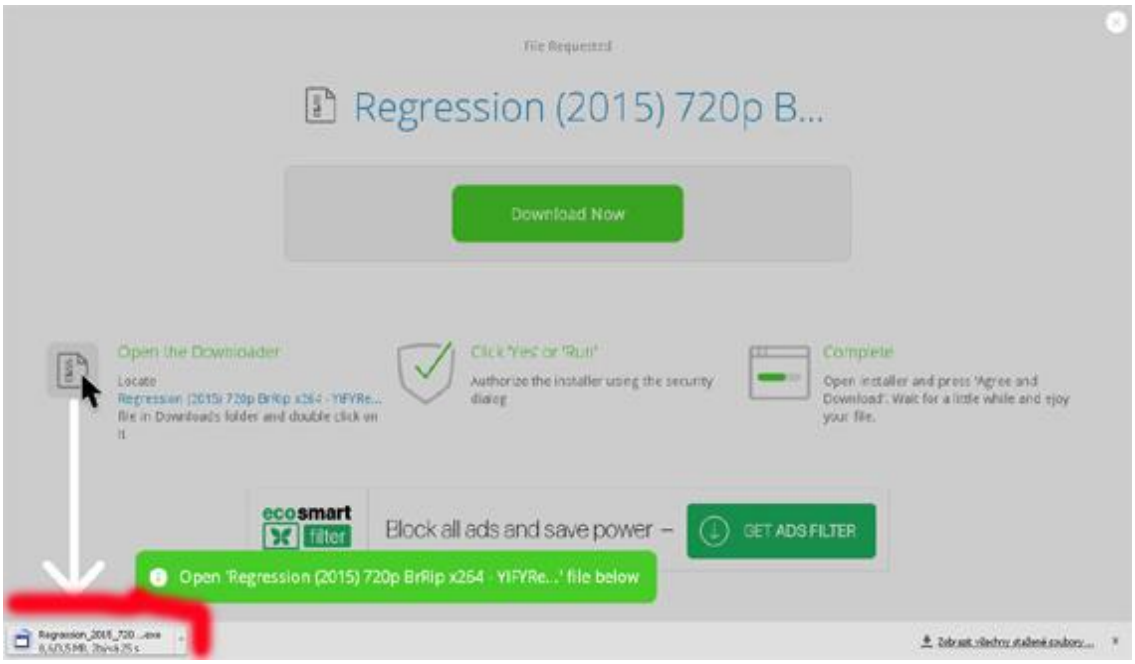
Než přistoupíme k právnímu rozboru sdílení prostřednictvím P2P sítí, nastíníme si i zde některé důvody, proč k němu dochází. Finanční motiv zde neobstojí, neboť není

---

[109] PFEFFER, Jan. *Softwarové pirátství*. Praha, 2009. Diplomová práce. PF UK. Vedoucí práce JUDr. Petra Malá Žikovská. s. 19-21

[110] na internetu je k nalezení nepřeberné množství článků, které jsou kauze The Pirate Bay věnovány – namátkou http://www.zive.cz/bleskovky/vzpominate-na-soud-s-the-pirate-bay-kauza-jeste-stale-neskoncila/sc-4-a-174431/default.aspx, nebo http://a2larm.cz/2014/06/the-pirate-bay-proces/, či http://zahranicni.eurozpravy.cz/eu/121027-server-the-pirate-bay-ma-dalsi-problemy-ztratil-domeny-ve-svedsku/

využíváno žádného serveru, který by toto plnění poskytoval. Přesto se dá využít příjmu z reklamy, nicméně tento bude přilepšením pouze výrobcům programů, které stahování v síti BitTorrent umožňují. V nastavovacím okně obslužného softwaru je prostor na její účelné zobrazování. Možným motivem pro seedry je uznání ve skupině a následná možnost stahovat jiná díla od ostatních členů. Méně poctiví uživatelé dávají ke sdílení tzv. fake (falešný) soubor, jenž neobsahuje požadované a pojmenované dílo, ale buďto nějaké reklamní sdělení, nebo i virus či malware. Toto se děje v případě nových žádaných filmů poměrně často. Mnoho uživatelů stahuje v domnění, že zhlédnou nejnovější hollywoodský „trhák“, avšak po stažení zjistí, že soubor obsahuje reklamu nebo virus. Občas je virus přibalen i ke skutečnému filmu. Pokud nemají uživatelé antivirovou ochranu, mohou se stát obětí jiného kyberzločinu, např. některého z druhé kapitoly práce. Virus může útočníkovi přinést nemalý finanční zisk a to je pro něho dobrý motiv, proč soubory sdílet. Také vyhledávání torrentových souborů přináší pro kyberzločince vhodný prostor na šíření závadných programů. Velmi často se děje, že místo žádaného torrentu dojde ke stahování viru či malwaru. Povětšinou místo koncovky .torrent má stažený soubor koncovku EXE (viz obr. 4 představující možnou hrozbu, ačkoli by se mělo jednat o torrentový soubor již zmiňovaného filmu Regression, je to virus). Nejde tedy o program ke stažení filmu, nýbrž o program, který je možné poklikem spustit. Poté je počítač již infikován a přináší útočníkovi možný zisk.



Obr. 4

3.4.2.1 Právní posouzení sdílení prostřednictvím sítě P2P – BitTorrent

Z pohledu uploadera, neboli seedra v tomto případě, neexistuje právní rozdíl mezi „klasickým“ zpřístupněním díla pomocí plnohodnotných filehostingových serverů nebo prostřednictvím peer to peer sítí. Opět se bude jednat o rozmnoženinu díla dle § 13 AZ a její sdělování veřejnost dle § 18 AZ. Pokud k tomuto dochází bez souhlasu nositele autorských práv, je jednání nezákonné a právní posouzení bude zcela totožné, jako při sdílení skrze filehostingy. Z tohoto důvodu odkážeme na právní rozbor v podkapitole 3.4.1.1., neboť bychom pouze opakovali již uvedené.

V případě downloadera, neboli leechera, je již situace oproti webovým úložištím odlišná. Základem pro posouzení bude ustanovení § 2 odst. 3 AZ, jež stanoví, že právo autorské se vztahuje na dílo dokončené, jeho jednotlivé vývojové fáze a části, včetně názvu a jmen postav. Autorský zákon tedy chrání i časti děl, a to je pro právní posouzení podstatné. V případě sítě BitTorrent každý uživatel, který stahuje data jejím prostřednictvím, zároveň ve stejný okamžik poskytuje jiná, již před tím stažená data, která tvoří část stahovaného celku, i ostatním uživatelům. Což jsme si již vysvětlili. Stává se tak alespoň na určitou dobu v celé, nebo omezené míře. Podstata těchto sítí totiž neumožňuje uživatelům být pouze příjemci dat. Jinými slovy, kdo chce stahovat, musí zároveň i sdílet. Omezení je možné pouze při nastavení rychlosti sdílení, přičemž nejpomalejší nastavení je 1 kbps. Zcela vypnout upload není možné, a tak některé části díla budou vždy šířeny, proto se leecher dostává do režimu sdělování díla veřejnosti podle § 18 AZ.[111]

Není tak možné využít institutu volného užití díla dle ustanovení § 30 AZ. Tím pádem ani třístupňový test nepřichází do úvahy a je jasné, že stahování prostřednictvím sítě BitTorrent je nezákonné. Dostáváme se do stejné právní situace jako v případě seedra a proto bychom pouze opakovali již uvedené. Právní posouzení je stejné jako v případě uploadera v podkapitole 3.4.1.1. Jen zdůrazníme, že pokud bude docházet ke značnému stahování, tím pádem i sdílení dat, dojde ke stíhání spíše dle předpisu trestního práva, než stíhání pro přestupek. A pokud dochází ke skutečně značnému

[111] ČERMÁK, Jiří. Ochrana autorského práva v prostředí peer to peer sítí typu BitTorrent s přihlédnutím k rozsudku ve věci The Pirate Bay. *Právní rozhledy: časopis pro všechna právní odvětví*. Praha: C. H. Beck, 2010, č. 8. ISSN 1210-6410. s. 272

porušování práva, může se pachatel, případně skupina pachatelů, dočkat „přátelské“ návštěvy od Policie ČR. Takový zásah proběhl v minulosti několikrát i v ČR a jednou dokonce na téměř akademické půdě, kdy OČTŘ koncem roku 2007 dorazily na studentské koleje na pražský Strahov [112], kde zadržely skupinu sedmi osob a značné množství HW a nosičů, neboť tyto osoby byly podezřelé, že prostřednictvím zejména P2P sítí sdílely nelegální obsah.

S nadsázkou je možné říci, že jediné využívání technologie BitTorrent, jež neporušuje autorská práva, je sdílení děl se souhlasem autora nebo šíření a stahování děl, která nepožívají autorskoprávní ochrany. Bohužel realita je zcela odlišná. Využívání BitTorrent sítí má díky své jednoduchosti, rychlosti a efektivitě jednoznačně za cíl šířit zejména žádaná a tudíž autorsky chráněná díla.[113]

Poslední možné právní posouzení, je odpovědnost provozovatelů či tvůrců systémů, které takovéto sdílení děl umožňují. Zhodnocení není úplně jednoznačné a na stanovisko má vliv, o jaký typ výměnné sítě se jedná. Peer-to-peer sítě, založené na zmíněném postupu, lze totiž rozdělit na centralizované, decentralizované a tzv. BitTorrenty. Tvůrci a provozovatelé P2P sítí se sami nedopouštějí užívání díla, ovšem svou činností umožňují uživatelům, aby neoprávněně díla zpřístupňovali. Tímto se tak určitou formou podílejí na porušování autorského práva. Vzhledem k tomu se tak autor díla či vykonavatel příslušných práv může u provozovatele P2P sítě domáhat zákazu poskytování jeho služby dle § 40 odst. 1 písm. f) AZ. Záleží ovšem, zda jde o centralizovaný systém či nikoliv, zda dochází k majetkovému prospěchu provozovatele a podobně. Zde by opět přicházela již zmiňovaná odpovědnost podle zákona č. 480/2004 Sb., o některých službách informační společnosti. Také v případě, kdy bychom dovodili, že provozovatel sítě tímto svým jednáním porušil obecnou povinnost předcházení škodám (*neminem laedere*) podle § 2900 občanského zákoníku, by toto porušení generální prevenční povinnosti mělo právní následek. Byla by jím povinnost k náhradě škody tímto jednáním způsobené podle § 2909 a násl. OZ. U provozovatelů P2P sítí s decentralizovaným vyhledáváním je tato odpovědnost sporná, neboť nikdo

[112] více k danému zásahu na vysokoškolských kolejích je možné nalézt na těchto webových stránkách: http://www.novinky.cz/krimi/128907-policie-provedla-zatah-na-piraty-na-strahovskych-kolejich.html

[113] FRIČ, Antonín. *INTERNET A AUTORSKÉ PRÁVO*. Praha, 2011. Diplomová práce. PF UK. Vedoucí práce JUDr. Irena Holcová. s. 60-61

kromě koncových uživatelů nemá žádnou kontrolu a vliv na sdílené soubory. A u samotných tvůrců protokolu pak v podstatě vyloučená. Trestní odpovědnost bychom provozovatelů nebo tvůrců systémů zřejmě nedovodili.[114,115,116]

3.4.3 Warezová fóra jako zdroj nelegálního obsahu – odkazy na weby

Již víme, co je warez i warezová fóra a tak jen v krátkosti zejména ono fórum vymezíme. Drtivá část warezu je na internetu distribuována takto. Uploader po nahrání svého „díla“ na nějaký filehosting, od něhož obdrží webový odkaz, tj. přesnou webovou adresu, kde je toto dílo k dispozici ke stažení. Sám tento odkaz dále šíří. Bez něj by o daném díle nikdo nevěděl a tak by jej nikdo nestahoval. Má možnost jej zaslat přátelům, ale to by stále nebyl dostatečný počet, aby mu to přineslo finanční zisk, o který uploadreům především jde, což již víme. Proto na internetu vznikají fóra, která takovéto odkazy, neboli linky sdružují. Jsou účelově uspořádána dle kategorií, jako např. film, software atd. a každá kategorie má i své podkategorie. Je zde tedy možné vše přehledně dohledat. Tento systém nás však přinutí k zamyšlení a položení otázky, zda jsou tedy fóra, která takto odkazy sdružují, legální a je možné dohledat odpovědnost vkladatele příspěvku s odkazem, nebo odpovědnost provozovatele fóra?

Než na tuto otázku odpovíme, ještě si odkazy rozdělíme na dva typy. První typ, tzv. pasivní odkaz. V tomto případě se jedná pouze o uspořádanou skupinu písmen, která sice nese informaci o místě, kde je dílo ke stažení, ale není s ním nikterak propojené. Pokud chce uživatel tuto informaci využít, musí celý odkaz zkopírovat a sám vložit do příkazového řádku. Teprve až poté dojde k jeho přesměrování na daný filehosting a bude mu umožněno dané dílo stáhnout. Oproti tomu aktivní odkaz, nebo někdy se užívá pojem „živý“, ten je ve své podstatě s úložištěm propojen. Stačí na tento odkaz najet kurzorem a pouze odkliknout. Ihned dojde k přesměrování a uživatel může stahovat. Jedná se tedy o pohodlnější formu sdílení. Bude však tento nepatrný rozdíl těchto odkazů mít vliv na právní posouzení? Odpověď nalezneme v následující části.

---

[114] FRIČ, Antonín. *INTERNET A AUTORSKÉ PRÁVO*. Praha, 2011. Diplomová práce. PF UK. Vedoucí práce JUDr. Irena Holcová. s. 60-61

[115] ČERMÁK, Jiří. *Internet a autorské právo*. 2. aktualiz. a rozš. vyd. Praha: Linde, 2003, 251 s. ISBN 80-7201-423-4. s. 97-98

[116] PRÁVNÍ ASPEKTY P2P. *Ifpi.cz* [online]. 2015 [cit. 2016-03-13]. Dostupné z: http://www.ifpi.cz/pravni-aspekty-p2p/

3.4.3.1 Warez fóra vs. právo

Odpověď na položenou otázku není jednoduchá. Sdílení odkazů na nabídky filmů, či jiných autorských děl ke stažení není bohužel nikde výslovně upraveno v žádném právním předpise. Lze však konstatovat, že se jedná o aktivitu přinejmenším problematickou. Zákon nám odpověď jasně neposkytne, judikatura týkající se odkazů, potažmo warez fór není a jak se říká, v této oblasti má každý právník svůj názor. Tyto názory jsou však dosti rozdílné. Z tohoto důvodu není *de facto* z čeho vycházet a tak je tato podkapitola právním názorem autora, který však nemusí, při případném projednání, být soudem akceptován.

Samotný pasivní odkaz sice nese informaci o místě díla, ale nelze jej dle autora chápat jako zpřístupňování díla v nehmotné podobě a tím tak subsumovat pod ustanovení § 18 odst. 1 AZ. Při pasivním odkazu je nutná uživatelova vůle, neboť bez ní se na patřičnou stránku s dílem nedostane. Oproti tomu aktivní odkaz, kdy může dojít k přesměrování, tedy i ke zpřístupnění díla, pouhým omylem. Nedopatřením při čtení webové stránky uživatel klikne jinam, než chtěl a bude přesměrován. To je onen podstatný rozdíl a proto autor této práce zastává názor, že právní posouzení obou typů odkazů je rozdílné. Posoudíme tedy každou situaci zvlášť.

V případě používání pasivních odkazů, je situace pro uploadera, který odkaz s nasdíleným dílem šíří, downloadera, jenž odkaz ke stažení použije a vlastně i provozovatele warezového fóra, právně totožná. Všechny tyto skupiny nejsou dle názoru autora nikterak za šíření těchto typů odkazů právně odpovědné, z důvodu výše uvedenému. Jedná se pouze o šíření „informací" nikoli zpřístupňování díla jako takového. Hovoříme však jen o právní stránce v záležitosti odkazů, neboť jinak je samozřejmě uploader za nasdílení právně odpovědný dle předchozích podkapitol.

Dle některých zdrojů[117] by situaci pasivního odkazu bylo pro ztížení možné posoudit i z pohledu, kdy je třeba link na data v internetovém úložišti chápat jako sdělování veřejnosti a to v případě, že samotné úložiště neumožňuje vyhledávat a tím i zpřístupňovat data bez znalosti konkrétní internetové adresy. Pouze ten, komu je znám přesný odkaz, se k obsahu dostane, nikdo jiný. V takové situaci by zveřejnění odkazu,

[117] tento názor je možné nalézt např. v této práci – FRIČ, Antonín. *INTERNET A AUTORSKÉ PRÁVO*. Praha, 2011. Diplomová práce. PF UK. Vedoucí práce JUDr. Irena Holcová. s. 54-55

ať už aktivního či pasivního, bylo nedílnou součástí sdělování veřejnosti, z důvodu nemožnosti přístupu k takto uloženému dílu jiným způsobem, než právě skrze hypertextový odkaz. U většiny úložišť je však vyhledávání možné, dílo je tak zpřístupněno samotným uploadováním na příslušný server. Je také nutné si uvědomit, že stejně vždy existuje univerzální vyhledávač, např. google, který dokáže webové stránky prohledávat a k obsahu uživatele dovede i přes uzamčená fóra. Proto je dle autora takovýto pohled, kdy by sdílení odkazů bylo nelegální, nesprávný a sdílení pasivných odkazů tak není nezákonné.

Zda by bylo možné dovodit odpovědnost provozovatelů fór např. dle zákona č. 480/2004 Sb. o některých službách informační společnosti, jako u provozovatelů filehostingu autor také pochybuje. Proč by měl mít správce fóra povinnost odstranit pasivní odkaz informující o jiném webu, když se nejedná o dílo jako takové. Pouze o informaci. Proto autor i s touto odpovědností nesouhlasí. Zcela jistě také nemají odpovědnost dle předpisu trestního práva. Zbývala by odpovědnost dle obecného předpisu občanského práva, avšak bylo by na žalujícím prokázat, že těmito informacemi byl poškozen, což by se zřejmě povedlo, ale také, že odpovědnost za obsah je na provozovateli a toto by se již dle autora, např. díky nezadatelnému právu svobody slova, nepodařilo.

Je skutečně nereálné dovozovat odpovědnost provozovatele fóra za celý obsah, byť zcela zřejmě cílený na oblast porušování autorských práv. Ale již v první kapitole jsme si uvedli, že tato fóra slouží i pro jiné účely a kde pak bude možné najít hranice mezi tím, co je a co není povolené? Pasivní odkazy jsou jen informace a záleží na každém z nás, jak s nimi naložíme. *Ad absurdum* by poté mohla být nezákonná i informace v podobě věty, jež by zněla: „Na internetu je možné nalézt odkazy na nezákonná díla“. Neboť i ta poskytuje uživateli cenné sdělení, že má hledat a pokud hledat bude, tak nalezne. Je to svým významem údaj vedoucí k nalezení díla, což je vlastně i pasivní odkaz na něj. Pokud nebude zákonem přesně definován linking nebo spíše deep-linking jako užití díla, bude autor práce zastávat názor výše uvedený.

Aktivní odkazy, to je však něco jiného. Autor práce je chápe jako jistou podkategorii tzv. embedded linků, ke kterým se již soudy, nejen v ČR, vyjádřily, a proto bude právní posouzení živých odkazů spadat do následující podkapitoly. Dá se říci, že i

sama fóra si tento rozdíl uvědomují a aktivní odkazy v příspěvcích netolerují (pravidla fór tyto zakazují) a jsou provozovateli aktivní linky mazány.

Každopádně by bylo z hlediska právní jistoty vhodné, kdyby zodpovědné orgány podaly závazné stanovisko, jak to se šířením odkazů je. Ať tak či tak, bylo by jasno a ČPU by opět mohla věnovat něčemu smysluplnějšímu, než je štvavá kampaň proti warez fórum. Buďto by mohly zasáhnout OČTŘ nebo by fóra byla ponechána svému osudu.

3.4.4 Embedded linky na webových stránkách jako nový způsob šíření děl

Nejprve opět krátké přiblížení problematiky, abychom věděli, co pojem embedded linky znamená. Jedná se o technický způsob umístění obsahu na internetových stránkách vložením připraveného kódu, jenž odkazuje na obsah umístěný na jiné internetové stránce, či spíše na jiný server umístěný v zemích, které autorské právo příliš nechrání, a to tak, že je tento odkazovaný obsah možné zobrazit na původní stránce, kde je embeddovaný link umístěn, bez nutnosti uživatele přejít na internetovou stránku, kde je umístěn obsah. Popsaný postup představuje jakési „vnoření“ jiné stránky do stránky zobrazované.[118]

3.4.4.1 Právní rozbor embedded linků

Právní problematika tohoto postupu není tak jednoduchá, jak by se na první pohled zdálo. Proč vlastně tento způsob zobrazení stránky zvolit? Odpověď je nasnadě. Vlastník webové stránky má v dnešní době oprávněné obavy z případného postihu za nelegálně šířená díla. Může tedy tvrdit, že jeho stránka je v souladu se zákony, pouze odkazuje na jinou stránku, která nelegální obsah nabízí a to není jeho problém. Dá se předpokládat, že právě z tohoto důvodu výše popsaný postup vznikl. Programátoři se tak snažili obejít autorskoprávní ochranu a zamezit tak svému postihu. Motivace je jasná, chtějí mít na stránkách žádaný obsah, který zajistí vysokou návštěvnost, potažmo finanční zisk z reklam, které tyto stránky ve vysoké míře doprovází, nicméně nechtějí být stíháni OČTŘ za nikoli nepatrný zásah do zákonem chráněných práv k

[118] Kybernetická kriminalita v judikatuře českých soudů. GŘIVNA, Tomáš. *Docplayer.cz* [online]. 2015 [cit. 2016-03-14]. Dostupné z: http://docplayer.cz/3912001-Kyberneticka-kriminalita-v-judikature-ceskych-soudu-doc-judr-tomas-grivna-ph-d-pravnicka-fakulta-uk-v-praze.html

autorskému dílu. Hlavním důvodem jsou v tomto případě peníze. Soudy v ČR však takovýto postup, kterým docházelo k obcházení litery zákona, striktně odmítly.

Opět si právně rozeberme jednání jednotlivých subjektů, jež se na systému sdílení podílí. Situace uploadera je opět právně totožná s podkapitolou sdílení díla u filehostignu. Z uvedného důvodu opět odkážeme na pasáž – podkapitola 3.4.1.1. V těchto případech však není využíváno klasického webového úložiště, ale úložiště online. Většinou jsou vybírány servery v zahraničí, které zaručují dostatečnou anonymitu. Dohledat v takových případech uploadera je téměř nemožné, ačkoli se dá předpokládat, že uploaderem bude v drtivé většině právě provozovatel stránky, která na videa odkazuje. Prokázat tento fakt by však při případném trestněprávním soudním řízení bylo povinností státního zástupce. Bohužel pokud by jednání nebylo prokázáno nade vší pochybnost, soud by za užití zásady *in dubio pro reo* obžalovaného zprostil. Možná i díky tomu došlo soudními rozhodnutími k „přenosu" odpovědnosti za nelegální obsah na provozovatele stránek. Podrobněji se tomu budeme věnovat v další podkapitole.

Právní posouzení downloadera, i když v tomto způsobu sdělování vlastně ke stažení díla ani nedochází a tak by se hodil spíše termín divák, je jednodušší. Situace je podobná jako při sledování děl na serveru YouTube. Tuto záležitost si přiblížíme v podkapitole 3.4.5.1.

3.4.4.2 Embedded linky a česká judikatura

Jak je to tedy s onou odpovědností provozovatelů stránek využívající embedded linky? K této problematice se již několikrát vyjádřil NS. Odmítl tvrzení provozovatelů, že oni chráněný zájem nenarušují, neboť pouze odkazují na jiné servery a tak nemohou naplnit skutkovou podstatu TČ dle § 270 TZ.

Prvním rozhodnutím ve věci embedded linků bylo usnesení Nejvyššího soudu ze dne 27. února 2013, sp. zn. 8 Tdo 137/2013, které se skrze podanou ústavní stížnost dostalo až před Ústavní soud. Avšak ÚS tuto ústavní stížnost, svým usnesením III.ÚS 1768/13 ze dne 10. 9. 2013, odmítl.

V této kauze se jednalo o případ takzvaného „libereckého piráta", šestnáctiletého studenta, jenž na webových stránkách, které provozoval, nabízel ke zhlédnutí 2470 audiovizuálních děl. NS v této věci ohledně embedded linků prohlásil: „*Za neoprávněný*

zásah do zákonem chráněných práv ve smyslu § 270 odst. 1 TZ lze považovat i takové jednání pachatele, který na Internetu v prostoru vyhrazeném pro své internetové stránky umístí odkazy (tzv. embedded linky) umožňující neoprávněný přístup k rozmnoženinám děl (např. filmových a televizních) umístěných na externích serverech tak, že kdokoli k nim může mít prostřednictvím takové internetové stránky přístup, aniž by k tomu měl souhlas nositelů autorských práv, a využije tzv. hostingu s možností uložení dat na serveru. V takovém případě totiž pachatel (umístěním tzv. embedded linku) umožnil přístup k rozmnoženině díla, a to jako osoba odlišná od osoby, která je vlastníkem této rozmnoženiny nebo jinou oprávněnou osobou, což je činnost, již je nutné považovat za porušení autorských práv k jednotlivým dílům a porušení práva na sdělování díla veřejnosti ve smyslu § 18 odst. 1, 2 autorského zákona."

Tato kauza však přinesla zajímavý pohled i na nároky uplatňované poškozenými oprávněnými nositeli autorských práv. Jak vyplývá z rozsudku soudu prvního stupně, měla být oprávněným nositelům autorských práv dle jejich sdělení způsobena škoda ve výši 122.106.045 Kč. ČPU vyčíslila škodu za jedno zhlédnutí filmu na 15 nebo 30 korun a za jedno zhlédnutí epizody seriálu na 5 nebo 10 korun. V samém závěru výpočtu byla škoda snížena a to dle výsledků dokazování. U každého filmu byl počet kliknutí (neboli zhlédnutí), na film vydělen stem a výsledná částka pak sloužila k výpočtu škody. Celkový nárok na náhradu škody byl tedy snížen na 3.914.595 Kč. A právě tato částka bude vymáhána občanskoprávní cestou. S daným systémem výpočtu však autor nesouhlasí. K samotnému výpočtu se také NS vyjádřil v jiné kauze. Samotná kauza i případné návrhy na vyčíslení škody budou ještě v této práci zmíněny.[119]

Vraťme se ale zpět k embedded linkům, neboť se objevily opět u NS v jiné kauze. I zde NS rozhodoval a vydal usnesení Nejvyššího soudu ze dne 29. května 2013, sp. zn. 5 Tdo 271/2013, ve kterém sdělil: „*Tzv. embedding použitý osobou odlišnou od vlastníka díla či jiného předmětu ochrany představuje neoprávněný zásah do zákonem chráněných práv jejich nositelů za předpokladu, že tato metoda je způsobilá zpřístupnit veřejnosti autorské dílo nebo jiný předmět ochrany. Z hlediska trestní odpovědnosti za trestný čin porušení autorského práva, práv souvisejících s právem autorským a práv k databázi podle § 270 trestního zákoníku má význam též okolnost, zda pachatel*

---

[119] HÁLEK, Jakub. *Autorské právo a jeho porušování na internetu z pohledu škody, náhrady škody a bezdůvodného obohacení* [online]. Praha, 2015 [cit. 2016-03-24]. Dostupné z: http://svoc.prf.cuni.cz/sources/8/17/519.pdf. SVOČ. PF UK. s. 23-24

neoprávněně zpřístupnil dílo nebo jiný předmět ochrany metodou vloženého kódu (tzv. embeddingu), anebo zda použil toliko prostý odkaz na autorské dílo či jiný předmět ochrany. Zatímco v případě prostého odkazu jiná osoba než autor díla nebo další nositel práv toliko informuje o umístění díla (resp. jeho rozmnoženiny) na příslušných internetových stránkách, aniž by zpřístupnila obsah díla (resp. jeho rozmnoženiny), použití metody vloženého kódu (tzv. embeddingu) představuje přímé zpřístupnění obsahu takového díla (resp. jeho rozmnoženiny) veřejnosti.“[120]

Embedding se k NS dostal ještě jednou a tak je k dispozici ještě další obdobné rozhodnutí. Ve svém usnesení Nejvyššího soudu ze dne 12. listopadu 2014, sp. zn. 5 Tdo 1136/2014 opět NS zachoval svůj postoj a svá dřívější rozhodnutí nerevokoval. I v tomto případě zpřístupňoval pachatel neoprávněně cizí autorská díla tak, že jako vlastník domény www.serialycesky.cz a její administrátor, bez souhlasu autorů nebo výrobců a v rozporu s ustanovením § 12, § 30 a § 80 AZ, sděloval prostřednictvím internetu lehce inovovanou metodou embeddingu. Díla již nebyla zobrazována v základním okně, ale po kliknutí na hypertextový odkaz se zobrazila v nové vrstvě, tzv. shadowboxu, který překryl stránku pod ním tmavou barvou. Audiovizuální záznamy epizod dvanácti seriálů tak poskytoval, aniž by k tomu měl souhlas nositelů práv. Pro posouzení coby činnosti nelegální je rozhodující skutečnost, že pachatel díla, jež zpřístupnil jiným uživatelům metodou vloženého kódu odkazující na stránky www.megaupload.com a www.megavideo.com, umístil i na webové stránky www. megaupload.com a www.megavideo.com bez souhlasu nositelů autorských práv, o čemž byl dobře informován. Svou roli zde sehrál i jeho zištný úmysl, neboť obviněný se chtěl primárně obohatit, což činil prostřednictvím reklamního systému ETAR-GET (pro zájemce více na http://www.etarget.cz/). Soud závěrem konstatoval, že obviněný nejenže záměrně neoprávněně zasáhl do autorsky chráněných práv, ale chráněná díla, respektive jejich rozmnoženiny, sděloval téměř tři měsíce v podstatě neomezenému počtu uživatelů kyberprostoru a činil tak se zištným motivem.[121]

Z výše uvedeného je zřejmé, že provozovatel webových stránek odpovídá za obsah, na který pomocí embedded linků odkazuje. Jedná se o přímé upozorňování na

---

[120] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. Pro praxi. ISBN 978-80-7380-501-2. s. 363

[121] tamtéž s. 365-366

dílo, obdobně jako je tomu u aktivního odkazu, na což jsme dříve upozorňovali, a právní odpovědnost je u nich zcela obdobná jako u uploadera v případě filehostingu. Z tohoto důvodu opět odkážeme na podkapitolu 3.4.1.1., neboť bychom právní závěry pouze opakovali. Skutečně se v jejich případě jedná o sdělování díla veřejnosti dle § 18 odst. 1, 2 AZ a proto jsou právně odpovědni za své jednání.

Autor podotýká, že se jedná o správná rozhodnutí, neboť pokud by závěry byly jiné, již nikdy by se pirátství nepodařilo regulovat, natož vymýtit. Každý provozovatel by jen odkazoval a byl by zcela z obliga. To by byla cesta k absolutnímu znemožnění ochrany autorských práv na internetu.

3.4.4.3 Judikatura EU – zejména rozsudek Soudního dvora EU C-466/12

Taktéž v jiných zemích EU se embedded linky dostaly do popředí zájmu soudů. Situace eskalovala v předložení případu čtvrtému senátu Soudního dvora EU. Ten se k dané problematice poměrně nedávno vyjádřil a zaujal doporučující stanovisko pro soudy zemí EU, ve věci C-466/12 Nils Svensson a další proti Retriever Sverige AB ze dne 13. února 2014.

Základem neshod v původním řízení bylo, že společnost Retriever Sverige zveřejňovala na svých webových stránkách odkazy mimo jiné na novinové články Nilse Svenssona a ostatních novinářů, zveřejněné na internetové stránce novin Göteborgs-Posten. Tyto články byly na web Göteborgs-Posten umístěny se souhlasem autorů a uživatelé stránek k nim měli volný přístup. Soudní dvůr po zvážení všech relevantních okolností došel k závěru, že poskytnutí hypertextového odkazu, k jakému došlo v původním řízení, není sdělováním veřejnosti ve smyslu čl. 3 odst. 1 Informační směrnice [122], ke kterému by bylo nutné svolení autorů, jelikož díla nejsou sdělována nové veřejnosti a je tudíž v souladu se zákonem.[123]

V podobném případě Soudního dvora ve věci C-348/13 BestWater International GmbH proti Michael Sebes a Stefan Potsch, ze dne 21. října 2014, nicméně jiné technologie, tzv. „framingu“, což je vložení videa nebo obrázku z jiné webové stránky, SDEU vydal usnesení, kde konstatoval: „*Pouhou skutečnost, že chráněné dílo, volně*

---

[122] Směrnice Evropského parlamentu a Rady 2001/29/ES ze dne 22. května 2001 o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti

[123] DVOŘÁK, Pavel. *Neoprávněné užití autorského díla*. Praha, 2015. Diplomová práce. PF UK. Vedoucí práce JUDr. Veronika Křesťanová, Dr. s. 62-66

dostupné na internetové stránce, je vloženo na jinou internetovou stránku prostřednictvím odkazu používajícího techniku „framing“, jako je i ta věc v původním řízení, nelze kvalifikovat jako „sdělování veřejnosti“ ve smyslu čl. 3 odst. 1 směrnice Evropského parlamentu a Rady 2001/29/ES ze dne 22. května 2001 o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti, jestliže tím dotčené dílo není sdělováno nové veřejnosti a ke sdělení nedochází za použití specifické technologie, která se liší od technologie původního sdělování.“ Opět se dá vyvodit, že SDEU v této činnosti problém neshledává.

Jedná se o nešťastná rozhodnutí nebo jsou jen nesprávně interpretována? Daná rozhodnutí se zcela jasně týkají odkazování na obsah, který je na internetu umístěn legálně, tedy se souhlasem autora. Avšak lze daná rozhodnutí vztáhnout i na případy, kdy je odkazováno na díla, jež byla na internetovou stránku umístěna bez souhlasu autorů, tedy nezákonně (což jsou právě případy pirátství v ČR)? Většina odborné veřejnosti[124] se domnívá, že rozhodnutí platí i pro tyto případy s čímž však autor této práce zásadně nesouhlasí. Dle jeho názoru by tímto krokem docházelo ke zlegalizování předchozí nezákonné činnosti a v poměrech ČR by to znamenalo v oblasti porušování autorských práv audio a audiovizuálních děl naprostý boom.

Však se již také mnoho obviněných z porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 270 TZ na radu svých obhájců na uvedený rozsudek C-466/12 odvolává. I v případu piráta, který se dovolával k NS ve zmíněné věci 5 Tdo 1136/2014, bylo tímto rozsudkem C-466/12 argumentováno. „*Obviněnému ale státní zástupce nepřisvědčil s poukazem na to, že zmíněné rozhodnutí řešilo problematiku vytvoření odkazů (linků) na volně a zcela legálně přístupné články na stránkách internetových novin Göteborgs-Posten.*“ Tato úvaha ohledně legálnosti odkazovaného zdroje je v tomto případě skutečně na místě, neboť pokud by takováto obrana byla připuštěna, znamenalo by to zásadní komplikace pro filmový průmysl.

Každopádně se jistě brzy dočkáme buďto potvrzení uvedených závěrů SDEU, nebo jejich revokace a to zásluhou rozhodnutí Soudního dvora ve věci C-160/15 GS

---

[124] např. CÍSAŘOVÁ, Zuzana. Pojem „nová veřejnost“ v rozhodovací praxi SDEU a slučitelnost s mezinárodními úmluvami v oblasti autorského práva. *Aktuální otázky práva autorského a práv průmyslových: nový občanský zákoník a vybrané problémy evropského práva duševního vlastnictví - dopady na českou legislativu a praxi*. Praha: Univerzita Karlova v Praze, Právnická fakulta, 2014, ISBN 9788087975152. s. 50-52

Media BV[125], jež čeká v Lucemburku na své rozuzlení.

3.4.5 YouTube

V souvislosti s rostoucí popularitou YouTube se vynořuje i fenomén tak zvaných youtuberů (youtubers). Jedná se o mladé tvůrce obsahu, převážně videí. Dá se říci, že pro tento typ sdílení byl server založen. Spolu s rapidním nárůstem počtu uživatelů internetu rostou též možnosti a služby, které lze na této unikátní celosvětové síti využívat. Jedná se o velice pohodlný způsob sledování audiovizuálních děl či poslechu děl hudebních, většinou přímo v rozhraní internetového prohlížeče, což představuje již zmiňovaný streaming. [126] Bohužel ruku v ruce s legálním sdělováním obsahu jde i sdělování nelegální. Jakmile lze někam nahrávat hudbu a videa, byť toto jednání má být v souladu se zákonem, okamžitě se začne využívat tento prostor i pro šíření obsahu nezákonného. Je tedy vhodné toto počínání právně klasifikovat. Opět se budeme věnovat jen obsahu nezákonnému, neboť šíření děl v souladu s právem není předmětem této diplomové práce.

3.4.5.1 YouTube a právo

Na rozdíl od non-streaming přenosů, tj. od běžného stahování z úložiště, nevyžaduje technologie streamingu zhotovení rozmnoženiny díla na pevném disku uživatele. Tento proces tak nepřesahuje rámec technických rozmnoženin podle zákonné licence uvedené v ustanovení § 38a AZ. Streaming tak představuje sdělování obsahu veřejnosti na vyžádání v individuálně zvoleném místě a čase, které popisuje ustanovení § 18 odst. 1, 2 AZ. Základem streamingu je vnímání díla uloženého na streamovém serveru, což je např. zmiňovaný YouTube, okamžitě při přenosu díla. To je dosaženo díky průběžnému ukládání dat ve vyrovnávací paměti počítače uživatele (tzv. buffering) a skládání v ucelený vnímatelný proud (stream) vjemů.[127]

Právní posouzení uploderů, jež umísťují zvukové nebo zvukově-obrazové záznamy na streamové servery, je obdobné jako při ukládání děl na webová úložiště.

---

[125] Žádost o rozhodnutí o předběžné otázce podaná Hoge Raad der Nederlanden (Nizozemsko) dne 7. dubna 2015 – GS Media BV v. Sanoma Media Netherlands BV a další (věc C-160/15).

[126] FRIČ, Antonín. *INTERNET A AUTORSKÉ PRÁVO*. Praha, 2011. Diplomová práce. PF UK. Vedoucí práce JUDr. Irena Holcová. s. 61

[127] tamtéž

Dochází ke sdělování díla veřejnosti a k rozmnožování díla. Opět tak odkážeme na podkapitolu 3.4.1.1.

V pozici diváka, tj. při sledování či poslechu děl uložených na streamovém serveru nemůže docházet a tedy ani nedochází k porušování autorských práv, neboť dočasné rozmnoženiny částí díla ve vyrovnávací paměti mají, jak je uvedeno, charakter rozmnoženin technických, popsaných v § 38a AZ. Proto je sledování děl na tomto portálu zcela v souladu se zákony.

Jak je to s odpovědností provozovatele? Je jasné, že samotný server YouTube si je své odpovědnosti vědom a tak je v sekci Autorská práva na Youtube možné nalézt prohlášení: „*Autorská práva představují důležité téma pro celou komunitu YouTube. V následujících odstavcích najdete přístup ke všem informacím a nástrojům potřebným ke správě vlastních práv na platformě YouTube a dozvíte se podrobnější informace ohledně respektování práv jiných tvůrců.*“ Každý, kdo nahrává nějaké dílo na tento server, musí respektovat jeho stanovené podmínky, jež musí stvrdit odkliknutím a každým přihlášením, pak opět konkludentně s těmito podmínkami, třeba i v upravené podobě z důvodu změny díky časovému vývoji, souhlasí. Touto metodou se server snaží minimalizovat svou odpovědnost a přenést ji na uploadera. To nicméně nelze. Jak jsme uvedli, uploader je samozřejmě za své jednání právně odpovědný, avšak YouTube se své odpovědnosti provozovatele zprostit nemůže. Odpovědnost je obdobná jako provozovatele filehostingu. Na YouTube je tak možné najít mnoho odkazů na videa, která byla, na základě požadavku autora či držitele práv, smazána. I v tomto případě odkážeme na právní rozbor provozovatele v podkapitole 3.4.1.1. na str. 64.

3.4.6 Online přenosy – TV či sport, tzv. webcasting

Webcasting zažívá v současné době značný rozmach. S rozvojem internetu a to zejména rychlosti jeho šíření a připojení nastala doba, kdy za stejný časový úsek je možné přenést stále větší množství dat. Toto množství je již dostatečné k tomu, aby obsahovalo např. jak zvukovou, tak i obrazovou složku.

Dnes jej chápeme jako zpřístupňování určitých dat prostřednictvím internetu v reálném čase tzv. real time streaming. Napodobuje klasické rozhlasové či televizní vysílání, které uživatel není oprávněn interaktivně ovlivňovat, a je v každou chvíli pro

všechny stejné. Původně byl tok dat technicky zabezpečen, aby nešel ukládat a nešlo si pořídit rozmnoženinu vysílaného díla, zejména u legálně šířeného vysílání, avšak každé zabezpečení v kyberprostoru se dá obejít a tak to dnes již neplatí. Například běžný webový prohlížeč Avant Browser umožňuje ukládání jakéhokoli video přenosu, který zobrazuje.[128]

Ovšem není webcasting jako webcasting. Pokud někdo přes internet vysílá obsah, ke kterému je oprávněn, tedy je držitelem autorských práv na jeho šíření či má jeho souhlas, není na tomto jednání nic protiprávního.[129] Bohužel je tomu ve většině případů naopak. Šířen je obsah bez souhlasu držitelů autorských práv. Toto nelegální šíření je možné rozdělit na dva případy. V prvním případě dochází k šíření programů, které jsou však volně dostupné v nabídce digitálního pozemního vysílání. Tento jev samozřejmě televizním stanicím vadí, nicméně vzhledem k faktu, že se jedná o volně dostupné kanály a k rozšiřování počtu diváků, kteří by k obsahu měli jinak přístup zdarma, díky internetu dochází jen v omezeném množství, podnikají kroky k zamezení šíření jen namátkou. Ovšem v druhém případě, kdy jsou šířeny kanály placené, tedy tzv. pay TV kanály, které jsou dostupné až po peněžní úhradě a tedy pouze omezenému okruhu diváků, podnikají TV stanice kroky k zamezení šíření ihned, jakmile se o takovémto šíření dozví, neboť přichází o peníze. I když i v tomto postupu se najdou výjimky a tak např. stanovisko televizní stanice NOVA je: „*Neděláme rozdíl v tom, zda jde či nejde o pay TV.*“[130] Z tohoto je zřejmé, že této stanici vadí internetové šíření obsahu stanic jinak zdarma dostupných.

Mezi nejžádanější obsahy pro občany ČR patří online vysílání českých televizních stanic (dostupné např. na stránkách http://mojetv.blbne.cz/) a sportovní přenosy (přenosy z celého světa a téměř každého sportu jsou dostupné např. na http://www.day.to nebo http://www.oleoletv.top/).

---

[128] ČERMÁK, Jiří. *Internet a autorské právo*. 2. aktualiz. a rozš. vyd. Praha: Linde, 2003, 251 s. ISBN 80-7201-423-4. s. 125

[129] poznámka autora – i legální vysílání prostřednictvím internetu však musí probíhat v souladu se zákony – nicméně vývoj právní úpravy přesahuje téma této diplomové práce, a proto se této problematice věnovat nebudeme, pouze odkážeme, že vysílání upravuje zákon č. 231/2001 Sb., o provozování rozhlasového a televizního vysílání a v případě záznamů také zákon č. 132/2010 Sb., o audiovizuálních mediálních službách na vyžádání a samozřejmě i AZ – zejména § 96 odst. 1 písm. c)

[130] zájemce je možné odkázat na tento článek, kde je možné si více o této problematice, včetně stanoviska právě TV NOVA, přečíst: http://www.digizone.cz/clanky/nelegalni-zive-streamovani-televizi-na-internetu-jak-to-vidi-samotni-provozovatele/

3.4.6.1 Právní náhled na webcasting

Právní posouzení webcastingu se týká pouze diváka a zprostředkovatele vysílání prostřednictvím jeho webové stránky. Je téměř vyloučeno, aby zde figurovala osoba třetí, tedy provozovatel webové stránky, který šíří přenos jiným zprostředkovaný. Toto se v praxi neděje, a proto se zaměříme na právní posouzení pouze dvou subjektů.

Pro právní posouzení odpovědnosti zprostředkovatele vysílání je vhodné uvést rozsudek čtvrtého senátu Soudního dvora EU ze dne 7. března 2013 ve věci C-607/11 ITV Broadcasting Ltd a další proti TV Catch Up Ltd., ve kterém SDEU prvně použil termín tzv. kriteria „specifických technologických prostředků", jakožto dalšího hlediska, jež je nutno vzít v potaz při interpretaci pojmu sdělování veřejnosti. Předmětem pro posouzení Soudního dvora bylo, zda podnikání společnosti TVCatchup naplňuje znaky sdělování veřejnosti ve smyslu čl. 3 odst. 1 Informační směrnice.[131] SDEU dospěl k závěru, že dochází-li k šíření děl, jež jsou součástí televizního vysílání, prostřednictvím specifické technologie odlišné od původního vysílání, kterou představuje internetový streaming, je takové šíření nutno považovat za „sdělování" ve smyslu čl. 3 odst. 1 Informační směrnice. Jestliže je tento zprostředkovaný přenos současně určen blíže neurčenému počtu eventuálních diváků a týká se vysokého počtu osob, jedná se naplnění požadavku „veřejnosti" a jde tudíž o sdělování veřejnosti. V případě následného sdělování tak užití specifických technologických prostředků navíc dle SDEU není významné, zda jsou díla zprostředkovávána „nové veřejnosti".[132]

Po celkové analýze je z rozsudku patrné, že *poskytovatelé televizního vysílání mohou zakázat další přenos svého vysílání jinou společností prostřednictvím internetu*, neboť *další přenos totiž za jistých podmínek představuje „sdělování děl veřejnosti", ke kterému musí autor udělit svolení.* Této možnosti *de facto* u nás všechny televizní stanice využívají a výjimky udělují pouze těm společnostem, se kterými mají sdílení smluvně dohodnuto. Ostatní sdílení skrze různé webové stránky, viz např. dříve uvedené, je z hlediska právního posouzení, nezákonné. A to i v případě, že dochází

---

[131] Směrnice Evropského parlamentu a Rady 2001/29/ES ze dne 22. května 2001 o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti

[132] DVOŘÁK, Pavel. *Neoprávněné užití autorského díla*. Praha, 2015. Diplomová práce. PF UK. Vedoucí práce JUDr. Veronika Křesťanová, Dr. s. 58-60

k šíření těch programů, které jsou jinak vysílány zdarma prostřednictvím televizních vysílačů a tudíž volně dostupné. Není tedy překvapivé, že je i sdílení programů, které jsou v samé podstatě placené, protizákonné. V těchto případech dokonce dochází ke sdělování obsahu i „nové veřejnosti“, neboť takovíto uživatelé by se k těmto programům za standardních podmínek pozemního vysílání stejně nedostali. Pokud situaci shrneme, jedná se v případě nenasmlouvaného webcastingu o činnost nelegální. Poskytovatel stránek, tedy i samotného obsahu živého vysílání, je právně odpovědný obdobně, jak je tomu v případě uploadera děl na filehosting. Je zde sice drobný rozdíl, avšak ten nemá vliv na právní posouzení odpovědnosti. U webcastingu dochází ke sdělování děl veřejnosti, jak nám ukázal rozsudek SDEU, tj. dle § 18 odst. 1, 2 AZ, nicméně nedochází k pořizování rozmnoženin dle ustanovení §13 AZ, avšak toto není pro posouzení odpovědnosti nezbytné. Z tohoto důvodu odkážeme na právní rozbor uploadera v podkapitole 3.4.1.1. na str. 60, jenž je obdobný pro zprostředkovatele webcastingu.

V této souvislosti se nabízí zmínit případ z října 2015, kdy si podanou žalobou u Městského soudu v Praze telekomunikační firma O2 vymohla vydání předběžného opatření, které zakazuje kabelovým a satelitním firmám, jež svůj obsah sdělují dále webcastingem na internetu, vysílat programy, kterými neoprávněně šíří zápasy fotbalové Ligy mistrů. Na tyto má v ČR práva jen O2 a Česká televize. Ačkoli nedocházelo k šíření obsahu společnosti O2, ale obsahu zahraničních televizních stanic, na českém internetu a TV byl fotbal jako takový k dispozici a to se O2 nelíbilo. Od vydání předběžného opatření je při vysílání fotbalových zápasů k dispozici pouze černá obrazovka s oznámením, že obsah není pro toto území k dispozici a to i v případě internetu. Což je dle autora sporné, neboť toto oznámení černé obrazovky je zobrazováno i na internetu v jiné zemi, např. Rakousku, kde by měl obsah k dispozici být. Webový prohlížeč je totiž schopen, na základě veřejné IP adresy, rozpoznat že uživatel se nachází na území jiného státu.

V pozici diváka, je situace obdobná jako v případě streamingu. Toto právní posouzení jsme si již uvedli, nicméně bez případného rozhodnutí SDEU, které sdělování streamingem, webcastingem, ale hlavně browsingem (tedy pouhým prohlížením jakékoli webové stránky) ovlivnilo. Tímto určujícím faktorem je rozsudek Soudního dvora EU ze dne 5. června 2014 ve věci C-360/13, Public Relations Consultants

Association Ltd proti Newspaper Licensing Agency Ltd a další. Předmětem byla žádost o rozhodnutí o předběžné otázce výkladu článku 5 odst. 1 a 5 opět Informační směrnice. Žádost byla předložena v rámci sporu v otázce povinnosti získat svolení nositele autorských práv k prohlížení internetových stránek, při němž dochází k vytváření kopie těchto stránek na obrazovce počítače uživatele a v internetové vyrovnávací paměti (tzv. „cache“) na pevném disku tohoto počítače. SDEU rozhodl, že článek 5 Informační směrnice musí být vykládán v tom smyslu, že veškeré kopie jak na obrazovce počítače uživatele, tak i ve vyrovnávací paměti pevného disku tohoto počítače vytvořené koncovým uživatelem při prohlížení internetové stránky, splňující podmínky, podle které musí být tyto kopie dočasné, musí být krátkodobé či akcesorické. Dále musí tvořit nedílnou a podstatnou součást technologického procesu, jakož i podmínky stanovené v článku 5 odst. 5 této směrnice, a jako takové mohou být vytvářeny bez svolení nositelů autorských práv. Současně platí, že není třeba majitelům těchto autorských práv hradit odpovídající odměnu. Jedním z hlavních argumentů, stojícím za daným rozhodnutím, je odůvodnění, že kopie ve vyrovnávací paměti počítače značně usnadňují prohlížení internetu, neboť bez těchto kopií by internet nebyl schopen pojmout stávající objem online datových přenosů. Bez vytvoření takovýchto kopií by byl proces používaný k zobrazování internetových stránek jednoznačně méně účinný.[133]

Z nastíněného případu je již snad dostatečně jasné, proč je streaming, webcasting i případný samotný browsing, možné právně posoudit tak, že nedochází k porušování autorských práv, jelikož dočasné rozmnoženiny částí díla ve vyrovnávací cache paměti mají charakter rozmnoženin technických. Tyto jsou popsány v § 38a AZ a z tohoto důvodu není sledování online obsahu nezákonné a divákovi tak nevzniká žádná odpovědnost.

3.4.7 Camcording aneb záznamy z kin

V oblasti porušování autorských práv k audiovizuálním dílům je velmi populární a vlastně i značně rozšířený tzv. camcording. Jedná se o neoprávněné pořizování záznamu filmu na kameru či obdobné technické zařízení a to přímo při jeho promítání v

[133] Rozsudek Soudního dvora EU C-360/13 se významným způsobem vztahuje i ke službám informační společnosti a zaručení jejich ochrany. *Ministerstvo průmyslu a obchodu* [online]. 2014 [cit. 2016-03-19]. Dostupné z: http://www.mpo.cz/dokument150669.html

kině. Bohužel i opatření, která tomuto zabraňují, značně zaostávají za možnostmi, jež mají lidé k dispozici a jsou tak neúčinná. Již v druhé kapitole jsme zmiňovali všelijaká zařízení, která jsou schopná videozáznamu např. v koupelně a to velmi skrytě. Takováto zařízení je bohužel možné použít i v případě kina k pořízení záznamu promítaného filmu. Například obyčejné brýle, které jsou schopny nahrávat, je velmi těžké odhalit. Již v roce 2014 byl takovýto případ v kině zaznamenán, kdy „*muž byl vyveden z kina kvůli údajnému nahrávání filmu přes Google Glass.*“[134] Camcording sice není ze své podstaty typickým internetovým pirátstvím, nicméně velmi úzce s ním souvisí. Jsou to právě tzv. kinoripy, tedy kopie filmu nahrané v kině, které jsou i přes svou obvykle nízkou kvalitu zdrojem prvních rozmnoženin těchto děl na internetu. Zde se pak následně masivně šíří prostřednictvím rozličných P2P sítí či filehostingových serverů. Mnohdy se stává, že film je pořízen na předpremiéře a okamžitě sdílen. Vzniká tak situace, kdy je dílo dostupné na internetu dříve, než má premiéru v kině v daném státě. Někdy je tento předstih i několik měsíců, pokud třeba distribuční společnost premiéru odloží. Protiprávnost pořizování záznamu filmu přímo při jeho promítání v kině výslovně upravila novela autorského zákona č. 216/2006 Sb., která v ustanovení § 30 odst. 3 AZ vyňala pořízení záznamu audiovizuálního díla při jeho provozování ze záznamu nebo jeho přenosu z práva na volné užití. Tímto výslovně stanovila protiprávnost jakéhokoliv pořizování záznamu filmu při promítání v kině, avšak tento fakt jsme si již dříve uvedli. V České republice camcording až tak častý není, nicméně tu a tam i u nás někdo poruší zákon. Nejznámější „camcordingovou“ kauzou v ČR byl případ z roku 2007, kdy za kopii filmu Simpsonovi byl obviněn 19letý mladík.[135] Nedochází k tomu možná z obavy přistižení, ale možná i důvodu, že filmy, které jsou u nás k vidění, jsou již i na internetu, tak proč riskovat. Jen v některých případech to význam má a to jsou případy filmu s českým dabingem, ty se shání hůře. Proto se tento způsob řeší poměrně bezpečnější metodou, kdy se v českém kině pořídí pouze zvuková stopa a ta se připojí k filmu, který na internetu koluje, avšak pořízen byl v jiné zemi. Poslední takovýto případ byl v ČR v prosinci 2015, kdy dva dny po premiéře filmu Star Wars: Síla se

[134] článek věnovaný této záležitosti si je možné přečíst např. zde: http://cdr.cz/clanek/muz-byl-vyveden-z-kina-kvuli-udajnemu-nahravani-filmu-pres-google-glass

[135] článek věnovaný této záležitosti si je možné přečíst např. zde: http://kultura.zpravy.idnes.cz/za-kopii-simpsonovych-je-obvinen-19lety-mladik-f4g-/filmvideo.aspx?c=A070818_125401_filmvideo_ton

probouzí, bylo možné si tento film z internetu stáhnout včetně českého dabingu, přičemž tento byl do filmu přidán již nastíněným způsobem. Původní nahrávka filmu byla pořízena v Rusku.[136]

Případ camcordingu si uvádíme hlavně z důvodu, že stačí jedno zcizené dílo a způsobená škoda může být ohromná. Protože při trestněprávním posouzení jednání uploadera nedochází ke sdílení děl ve značném rozsahu, rozhodující tak musí být způsobená škoda, neboť jinak by bylo možné užití maximálně základní skutkové podstaty (zásah nikoli nepatrný), nicméně spíše by se jednalo pouze o přestupek. Bez vyčíslené škody, která nebude dosahovat určité hodnoty, nedojde k naplnění skutkové podstaty TČ dle § 270 TZ. Avšak jak v tomto případě onu škodu vyčíslit? Odpověď není vůbec jednoduchá a pouhé vynásobení počtu stažení jistou cenou, např. ceny lístku v kině, nebude tím nejvhodnějším řešením. Pokusíme se i tento případ nějakým způsobem začlenit a to v podkapitole 3.7.2.

3.4.7.1 Právní rozbor camcordingu

Právní posouzení uploadera, který nahraný film z kina poskytne skrze filehosting, je tedy jasné, i včetně samotného, již výše právně posouzeného, nezákonného aktu pořizování záznamu. Taktéž odpovědnost downloadera i provozovatele filehostingu je zřejmá. Ve všech třech případech jde o obdobu odpovědnosti z podkapitoly 3.4.1.1 a nemá význam uvedené opakovat.

Nicméně v případě nahrávek z kina se v procesu vyskytuje ještě další subjekt. Tím je samotné kino, potažmo jeho provozovatel. Bylo by možné dovodit i jeho odpovědnost, třeba i trestní? Tedy bylo by možné stíhat buďto FO provozovatele nebo dokonce PO kino? Jako jediná možnost trestněprávního posouzení by se nabízela forma účastenství na případném TČ. Náš trestní zákoník rozlišuje tři druhy účastenství. Dle § 24 odst. 1 TZ je posouzení možné: buďto se na účastníka hledí jako na organizátora, návodce nebo pomocníka, přičemž jsou tyto tři typy řazeny dle závažnosti jejich podílení se na trestné činnosti v písm. a) až c) uvedeného prvního odstavce. Šámal uvádí, že jde „*o úmyslnou formu účasti na trestném činu, kdy účastník bezprostředně přispívá k naplnění znaků konkrétní skutkové podstaty trestného činu, i když účastník*

[136] VARJASSYOVÁ, Martina. *Díla audiovizuální*. Praha, 2009. Diplomová práce. PF UK. Vedoucí práce JUDr. Veronika Křesťanová, Dr. s. 50-51

sám tyto znaky přímo nenaplňuje.“ [137] Ustanovení § 111 TZ však tyto formy účasti chápe jako spáchání trestného činu. Z tohoto důvodu se trestní odpovědnost účastníka posoudí dle ustanovení, jež jsou užita pro postih pachatele nebo spolupachatele. Z uvedených tří druhů by pro náš případ bylo nejvhodnější označení kina jako pomocníka. Tato jediná forma by mohla být naplněna, neboť Šámal uvádí, že „*pomocník úmyslně umožňuje nebo usnadňuje hlavnímu pachateli spáchání trestného činu, čímž mu pomáhá nebo ho podporuje, a to ještě před spácháním činu nebo v době činu, jestliže došlo alespoň k pokusu trestného činu.*“ [138] Nicméně i tato nejméně závažná forma účasti vyžaduje úmyslné jednání a toho se pravděpodobně žádné kino dopustit nechce.

Nicméně odpovědnost dle obecného předpisu OZ a za užití AZ by možná byla, neboť tyto předpisy nevyžadují úmyslnou formu zavinění. Také případné dohledání v jakém kině byla nahrávka pořízena není složité, neboť každému kinu je sice doručena kopie stejného filmu, ale nikdy nejsou identické. Vždy jsou v ní skryté indexované pasáže, které umožní identifikovat, v jakém kině nahrávka vznikla. Díky tomuto by, dle autora, bylo možné po případném provozovateli kina požadovat částečnou náhradu za vzniklou majetkovou újmu.

3.5 Softwarové „pirátství“

Již jsme si vysvětlili pojem audio a audiovizuálního pirátství, avšak co chápat jako pirátství softwarové? Pro odpověď stačí navštívit webové stránky [139] organizace BSA a hned na první stránce je uvedena jedna z možných definic.

„*Softwarové pirátství je synonymem pro neoprávněné užívání softwaru, které je chráněného autorskými právy. K pirátství může dojít při kopírování, stahování, sdílení či prodeji softwaru. Další častou formou pirátství je instalace více kopií softwaru do osobního nebo pracovního počítače, než umožňuje zakoupená licence. Hodně lidí si neuvědomuje, že při nákupu softwaru si nekupují vlastní software (program), ale jen licenci na jeho užívání. Tato licence určuje, jakým způsobem lze se softwarem nakládat*

---

[137] ŠÁMAL, Pavel. *Trestní zákoník: komentář – zvláštní část*. 2. vyd. V Praze: C.H. Beck, 2012. Velké komentáře. ISBN 978-80-7400-428-5. s. 343

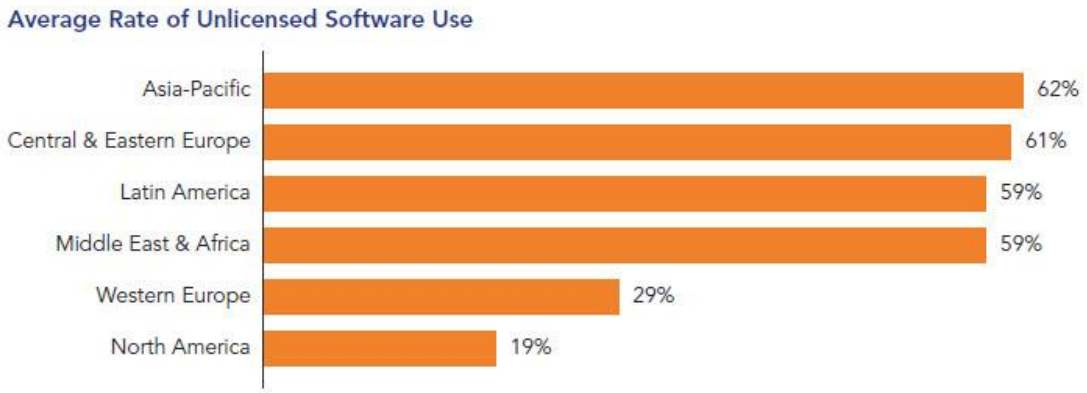
[138] tamtéž s. 349

[139] české webové stránky BSA: Co je softwarové pirátství? *BSA* [online]. [cit. 2016-03-20]. Dostupné z: http://ww2.bsa.org/country.aspx?sc_lang=cs-CZ

– například kolikrát lze software nainstalovat – takže je třeba si ji dobře přečíst. Pokud zhotovíte více kopií, než dovoluje licence, dopouštíte se pirátství.“

Již máme stanovenu určitou definici softwarového pirátství, ale stále nevíme, jakého druhu SW se tento nešvar týká, zda každého, nebo existuje pouze jistá skupina SW, jež je „ohrožena“. A pravdou je, že žádná skupina SW není ušetřena. Nelegální užívání i šíření se týká každého SW, tedy až na volně šiřitelný software, jež je možné volně používat, ale i dále upravovat a distribuovat tj. kopírovat a sdílet, a proto ani není možné jeho nelegální užití. Přestože se nešvar týká všech, vyjma volně použitelných programů, existují skupiny, které v žebříčku nelegálního nakládání dominují. Prim v této oblasti hrají zejména operační systémy, zejména Windows v jakékoli verzi, pak také grafické programy a kancelářské balíky. Hojně jsou v rozporu s licenční smlouvu také užívány „vypalovací“ programy a programy antivirové. V poslední době se problém týká i programů pro všechny typy navigací včetně jejich mapových podkladů.

Z různých průzkumů, často prováděných společností BSA, vyplývá, že průměrná míra nelegálního softwaru v Evropské unii za rok 2014 činí 31%. V České republice je procento užívaného nelegálního softwaru odhadované na 33%, což je zřejmě dvanáctá nejlepší hodnota ze všech zemí světa a dostáváme se v hodnocení i před vyspělejší západoevropské země jako jsou Francie, Itálie či Španělsko. Celosvětová míra se odhaduje na 44%, přičemž je známým faktem, že nejlépe jsou na tom s legálním užíváním SW země západní, zejména USA nebo Kanada. Naopak nejhůře si stojí země východní - Rusko, Čína, ale i země jižní Ameriky. Graf 2 zobrazuje průměrnou míru užití nelegálního SW v různých oblastech světa za rok 2014.



Graf 2 (zdroj: webové stránky organizace BSA)

Statistiky za rok 2015 nejsou zatím k dispozici, nicméně rozdíly budou zhruba v rozpětí jednoho, maximálně dvou procent.

I v případě SW je vhodné uvést důvody, jež jsou motivací k jeho nelegálnímu užívání a šíření. Důvody pro šíření SW jsou obdobné, jako pro šíření audio a audiovizuálních děl v podkapitole 3.4 a opakovat je nebudeme, jen zdůrazníme, že v případě SW je finanční motivace tou nejhlavnější. Užívání nelegálního SW je vlastně také motivováno penězi, neboť uživatel chce pracovat s určitým programem, ale není ochoten akceptovat jeho cenu a přijde mu jednodušší si jej opatřit nezákonně a hlavně zdarma. Je zajímavé, že zatímco cenu HW nikdo nerozporuje, s cenou SW problém mnozí mají. A zarážející je skutečnost, že peníze, byť mnohdy nemalé, za nákup HW bez problémů zaplatí, další obnos na SW vybavení již ale neakceptují. A to ani za nejzákladnější program, kterým je OS, natož za programy další.

Za jistou podobu programu lze považovat i počítačovou hru. Tento segment představuje ohromný byznys, a proto jsou také počítačové hry hojně nelegálně šířené a to nejenom prostřednictvím internetu, ale i ve fyzické podobě na různých datových nosičích. I touha po hře tak představuje jistou motivaci pro nelegální získání SW a samotné hry tak rovněž představují značnou část trhu nezákonného šíření.

3.5.1 Druhy softwaru a jeho užití

Než budeme moci nějakým způsobem a dle určitých kriterií rozdělit protiprávní činnost spojenou se SW, je vhodné si představit formy počítačových programů a zdůraznit jejich možné legální užití. Již víme, že autorský zákon vymezuje způsoby užití počítačových programů zejména v § 65 a 66, samozřejmě za užití ustanovení § 30. Právo na jeho užití lze, mimo výjimky u děl volně šiřitelných, nabýt pouze smlouvou. Jedná se o smlouvu licenční, jejíž uzavírání upravuje oddíl pátý OZ, konkrétně ustanovení § 2358 až § 2389 OZ. Softwarová licence je v informatice právní nástroj, jež umožňuje používat nebo redistribuovat software, který je chráněn zákonem.

3.5.1.1 Freeware

Freeware je formou počítačového SW. Jedná se volně dostupný a šiřitelný software, bez nároku autora na honorář, nicméně autor si ponechává svá autorská práva a například neumožňuje program upravovat nebo omezuje použití zdarma jen pro specifické účely, jako jsou nekomerční účely, osobní potřeba či třeba účely vzdělávací

atd. Veškerý rozvoj takového programu je plně v rukou autora a není ani možné, aby v něm kdokoli prováděl různé úpravy a modifikace. Zdrojový kód programu není zveřejněn a není dovoleno tento zdrojový kód zpětným způsobem z programu získávat. Nicméně pojem freeware nesmí být překládán či zaměňován za „volný software“. Volný software je program, ke kterému již nikdo nemá autorská práva, neboť ta zanikla uplynutím 70 let od smrti autora.[140,141]

3.5.1.2 Shareware

Další formou představuje shareware. Jedná se o autorským právem chráněný software, který lze volně distribuovat. Obvykle má v sobě zabudované jisté omezení, které uživateli umožňuje software na určitou dobu zdarma vyzkoušet a přesvědčit se, zda mu vyhovuje. Po uplynutí autorem stanovené lhůty je uživatel povinen řídit se licenčním ujednáním. Nejčastěji za program zaplatit, nebo v případě bezplatného shareware se například někde zaregistrovat. Pokud však o program nemá dále zájem, je povinen jej odinstalovat. Takovéto verze shareware se označují „trial“ a mají obvykle stanovenu zkušební lhůtu cca 30 dnů. V jiných případech, kdy není trial omezen časem, je stanoven počet užití cca 5-10, po kterých se chová stejně jako po uplynutí lhůty.[142,143]

3.5.1.3 Adware

Třetí formou je adware, z angl. advertising-supported software. Jedná se opět o volně šiřitelný software, nicméně práce s ním je znepříjemňována nějakou reklamní aplikací a to s různou úrovní agresivity – od běžných bannerů až po neustále vyskakující pop-up okna nebo ikony v oznamovací oblasti. Ani tento software nesmí být volně pozměňován zejména tím, že dojde k úpravě zdrojového kódu, aby bylo zabráněno zobrazování reklamy. Většinou však nejsou adware přímo nebezpečné jako spyware. Rozdíl mezi těmito je ve vědomí uživatele, neboť spyware se do počítače instaluje sám nebo jej instaluje např. hacker po proniknutí do PC, tedy bez vědomí

---

[140] PFEFFER, Jan. *Softwarové pirátství*. Praha, 2009. Diplomová práce. PF UK. Vedoucí práce JUDr. Petra Malá Žikovská. s. 8

[141] Freeware. In: *Wikipedia: the free encyclopedia* [online]. 2015 [cit. 2016-03-20]. Dostupné z: https://cs.wikipedia.org/wiki/Freeware

[142] PFEFFER, Jan. *Softwarové pirátství*. Praha, 2009. Diplomová práce. PF UK. Vedoucí práce JUDr. Petra Malá Žikovská. s. 8

[143] Shareware. In: *Wikipedia: the free encyclopedia* [online]. 2015 [cit. 2016-03-20]. Dostupné z: https://cs.wikipedia.org/wiki/Shareware

uživatel. Adware se instaluje v souladu s licenčními podmínkami a jeho funkce je čistě reklamní, jež zprostředkovává tvůrci finanční profit, díky kterému autor umožňuje volné šíření programu s adwarem spojeného.[144]

3.5.1.4 Volně šiřitelný neboli open source software

Čtvrtou a již zmiňovanou formou je open source software, neboli volně šiřitelný SW. Software s otevřeným a přístupným zdrojovým kódem. Otevřenost představuje jak technickou dostupnost kódu, tak legální dostupnost – licenci software, jež uživateli umožňuje, při dodržení podmínek, zdrojový kód využívat, tj. prohlížet i jej upravovat. Open source software má spojitost s free softwarem, avšak termín „Free Software" komerční firmy odrazuje a mate, a proto se již moc neužívá.[145,146]

3.5.1.5 OEM software

Další a zřejmě mezi běžnými uživateli PC, zejména notebooků, dobře známý typ SW je OEM software. OEM licence, z angl. Original Equipment Manufacture, je způsob užití počítačového program, kdy je licence k danému programovému vybavení získána koncovým uživatelem současně se zakoupením hardwaru či jiného softwarového produktu. Takovýto program pak může být užíván pouze s hardwarem, ke kterému byl dodán a nelze jej užívat samostatně. OEM software není možné instalovat na jiný počítač a při ztrátě nebo zničení takového počítače dochází k zániku OEM licence. Tedy alespoň takový dojem chtějí výrobci mezi uživateli šířit, přesto soudní rozhodnutí na území EU tento názor nesdílí, a proto se tomuto typu budeme v podkapitole 3.5.4.5 důkladněji věnovat. Nespornou výhodou OEM softwaru je jeho nižší pořizovací cena oproti tzv. krabicové verzi. Funkčnost OEM i krabicové verze je stejná, jen někdy bývá servis k OEM softwaru, jako např. technická podpora, poskytován pouze výrobcem počítače. Přesto všechno je cena OEM oproti verzi krabicové i o desítky procent nižší.[147,148]

---

144 Adware. In: *Wikipedia: the free encyclopedia* [online]. 2015 [cit. 2016-03-20]. Dostupné z: https://cs.wikipedia.org/wiki/Adware

145 Otevřený software. In: *Wikipedia: the free encyclopedia* [online]. 2015 [cit. 2016-03-20]. Dostupné z: https://cs.wikipedia.org/wiki/Otev%C5%99en%C3%BD_software

146 PFEFFER, Jan. *Softwarové pirátství*. Praha, 2009. Diplomová práce. PF UK. Vedoucí práce JUDr. Petra Malá Žikovská. s. 9

147 tamtéž

148 OEM produkce. In: *Wikipedia: the free encyclopedia* [online]. 2015 [cit. 2016-03-20]. Dostupné z: https://cs.wikipedia.org/wiki/OEM_produkce

3.5.1.6 Retail software

Posledním typem je, před malou chvílí zmiňovaný, komerční, jinak též krabicový či retail software. Jedná se o plnohodnotný, krabicový, zcela funkční a pouze licenčně omezený software. Tvůrce poskytuje užívání takového softwaru na základě licenční smlouvy, téměř vždy za úplatu a je možno jej libovolně přenášet z počítače na počítač. Program je zakázáno modifikovat, kromě zákonných výjimek. Většinou se jedná o nejkvalitnější, avšak cenově velmi nákladný, přesto uživateli vyhledávaný software. Z tohoto důvodu dochází k jeho značnému šíření a to všemi možnými způsoby porušování autorského práva, čemuž se budeme dále věnovat.[149,150]

3.5.2 Formy porušování autorských práv u softwaru

Trestná činnost, jež souvisí s nelegálním užíváním počítačových programů, může postihovat celý, jinak legální, proces distribuce. Tedy cestu od tvůrce či výrobce až k uživateli – např. tvorba plagiátu, jeho výroba šíření a využívání – nebo jen některé etapy tohoto procesu – např. užívání legálního software v rozporu s licenčními podmínkami. Jednotlivé etapy distribuce softwaru je možné využít jako kriteria klasifikace forem softwarového pirátství. Podle Smejkala je pak díky zobecněným poznatkům kriminalistické praxe možné rozčlenit typické formy softwarového pirátství dle čtyř způsobů:

A. nelegální zásahy do softwaru
B. nelegální výroba počítačových programů
C. nelegální šíření softwaru
D. nelegální užívání počítačových programů, resp. nelegální vytěžování nebo zužitkování databáze[151]

A. Nelegální zásahy do softwaru

I zde mohou poznatky kriminalistické praxe napomoci k rozčlenění této formy softwarového pirátství a to na typické způsoby jednání pachatelů, za které považujeme:

---

[149] Retail verze softwaru. In: *Wikipedia: the free encyclopedia* [online]. 2015 [cit. 2016-03-20]. Dostupné z: https://cs.wikipedia.org/wiki/Retail_verze_softwaru

[150] PFEFFER, Jan. *Softwarové pirátství*. Praha, 2009. Diplomová práce. PF UK. Vedoucí práce JUDr. Petra Malá Žikovská. s. 9

[151] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. Pro praxi. ISBN 978-80-7380-501-2. s. 342

- *plagiátorství* – úprava původního díla pachatelem bez souhlasu autora a vydávání takto pozměněného díla za dílo vlastní
- *tvorba národních verzí software* – překlad původního programového díla nebo databáze do jiného jazyka pachatelem bez svolení autora a jeho šíření
- *další úpravy, mající za cíl změny funkčností software, rozšíření licenčních omezení*

a ještě jiné zásahy, které sledují rozdílný účel, s nelegálním užíváním software přímo nesouvisejí, avšak právě u nelegálního SW se mohou vyskytnout. Příkladem je možné přidání dalších škodlivých programů za účelem poškození obsahu počítače - spyware.[152]

B. Nelegální výroba počítačových programů

I v tomto případě je možné nalézt typické způsoby páchání, kterými jsou:

- *nelegální průmyslová výroba softwaru* – činnost podniku schopného průmyslové výroby optických nosičů pro výpočetní techniku je pachatelem zneužita tím, že je zadána „legální" zakázka na základě neplatné licence pro výrobu standardního software, jež je poté distribuován, ovšem bez souhlasu autora
- *domácí výroba softwaru bez patřičné licence* – soukromá osoba pro svoji potřebu nebo za komerčním účelem nelegálně kopíruje určité programy a současně se je pokouší prodat nejčastěji prostřednictvím inzerátů na internetu, přičemž je možné pachatelovo spojení s dalšími spolupachateli, což utváří organizovanou skupinu
- *zneužití oficiálních kopírovacích služeb*[153]

C. Nelegální šíření softwaru (této činnosti se budeme dále věnovat)

Tato forma trestné činnosti představuje širokou škálu aktivit, přesto je možné jisté členění na tyto způsoby:

- *pašování a prodej nelegálního softwaru vyrobeného v zahraničí na našem trhu* – pachatelé (zpravidla organizovaná skupina) obstará nelegální dovoz CD/DVD s padělanými programy do České republiky a zde jsou poté distribuovány v podstatě jako originály, avšak za nižší ceny, přičemž se snaží v kupujících vzbudit dojem, prostřednictvím dokumentace i zdánlivě originálního obalu a licenčního ujednání, že se jedná o legální produkt, který je určený pro ČR

[152] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. Pro praxi. ISBN 978-80-7380-501-2. s. 342-343

[153] tamtéž s. 343

- *prodej softwaru bez svolení autora* – převážně spojen s nelegální výrobou software, kdy pachatel buď sám nelegálně kopíruje software, nebo získává nelegálně kopírovaný software a prodává jej zájemcům přes inzertní služby, kde zveřejňuje nabídky, přičemž v praxi se můžeme setkat i se zastřeným nelegálním prodejem software, kdy pachatel instaluje jako službu pro zákazníka software bez licence OEM opravňující jej k takovému postupu, avšak pachatel zákazníkovi nedodává licenční ujednání na užívání programu a na prodejním dokladu neuvádí, že s novým či repasovaným počítačem byl prodán i software
- *půjčování softwaru* – obecně není dovoleno, avšak můžeme se s ním nejčastěji setkat u mládeže, kdy si pachatelé půjčují originální software za tím účelem, aby si jej mohli instalovat na své osobní počítače, nicméně v současnosti je tato nezákonná činnost vytlačována stahováním na internetu, avšak s rostoucím využíváním cloudové technologie se může tento způsob distribuce opět zvýšit
- *nelegální šíření softwaru prostřednictvím internetu* – šíření SW prostřednictvím množství serverů, které poskytují prostor pro ukládání jakýchkoliv digitálních dat a které zneužívají principy formulované ve směrnici EU [154], podle které poskytovatel služby, jež spočívá v ukládání informací poskytnutých uživatelem, odpovídá za obsah informací uložených na žádost uživatele, jen:
    - mohl-li vzhledem k předmětu své činnosti, okolnostem a povaze případu vědět, že obsah ukládaných informací nebo jednání uživatele jsou protiprávní, nebo
    - dozvěděl-li se prokazatelně o protiprávní povaze obsahu ukládaných informací nebo o protiprávním jednání uživatele a neprodleně neučinil veškeré kroky, které lze po něm požadovat, k odstranění nebo znepřístupnění takovýchto informací[155]

  což jsme již zmiňovali v souvislosti s národní úpravou[156]

---

[154] Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. 6. 2000 o některých právních aspektech služeb informační společnosti, zejména na elektronickém obchodu na vnitřním trhu (směrnice o elektronickém obchodu)

[155] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. Pro praxi. ISBN 978-80-7380-501-2. s. 343-344

[156] zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti)

D. Nelegální užívání software (i této činnosti se budeme dále věnovat)

V tomto případě je činnost páchána dvěma typickými způsoby:

- *užívání legálně získaného programu nebo databáze, v rozporu s licenčním ujednáním* – užívání legálně nabytého program na více počítačích najednou v rozporu s licenčními podmínkami, což není otázkou jen drobných uživatelů v domácnostech a malých firem, avšak jsou známy případy, kdy takto postupovaly i poměrně velké firmy
- *užívání nelegálně získaného softwaru* – užívání bez jakéhokoliv oprávnění je typickým a velmi rozšířeným způsobem páchání a opět se s tímto nešvarem setkáváme nejen u osobního využití jednotlivcem, ale i v případech komerčního užívání a bohužel i při využití v různých nekomerčních institucích jako jsou např. školy, přestože tyto instituce mají mnohdy ceny licencí programů nastaveny velmi příznivě[157]

3.5.3 Rozmnoženina pro osobní potřebu není záložní rozmnoženina

Z předchozích pasáží víme, že v případě např. filmu je možné si pořídit rozmnoženinu pro osobní potřebu a to zcela v souladu s autorským zákonem dle ustanovení § 30 jako tzv. volné užití díla. V případě zvláštního druhu díla – počítačových programů (byť chráněných jako díla literární) však AZ v souladu se evropskou směrnicí[158] tvorbu kopie pro osobní potřebu vyloučil. V opačném případě se bude jednat o porušení autorského zákona, případně trestního zákoníku. Tato výjimka je absolutní a týká se veškerých počítačových programů a tedy i počítačových her. V důsledku z tohoto ustanovení vyplývá, že i v soukromí je užití jakéhokoliv počítačového programu možné pouze se svolením autora. Důvodem tohoto absolutního zákazu zřejmě byla potenciální hrozba nekontrolovatelného a masového šíření počítačových programů a s tím spojené narušení majetkových zájmů autorů počítačových programů. Zda je však ve skutečnosti tohoto cíle tímto ustanovením dosaženo, nechť si každý čtenář zhodnotí sám. K jistému obcházení daného znění dochází i jinak. V praxi se mnohokrát stalo a nepochybně se bude stávat i nadále, že úspěšný počítačový program je prozkoumán,

---

[157] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. Pro praxi. ISBN 978-80-7380-501-2. s. 344

[158] Směrnice Evropského parlamentu a Rady 2009/24/ES ze dne 23. 4. 2009 o právní ochraně počítačových programů

tedy zejména jeho zdrojový kód, jsou zjištěny jeho principy a další vlastnosti, jež z něj dělají úspěšný produkt, je popsán interní tvar datových struktur, s nimiž program pracuje a následně je vytvořen program zcela jiný, který se ale navenek tváří prakticky stejně, má stejnou strukturu dat, a je bud' levnější, nebo alespoň vylepšený, čímž začne ohrožovat tržní úspěšnost programu původního, na kterém *de facto* parazituje. A prokázat takovéto jednání není pochopitelně úplně jednoduché.[159,160]

Ale zpět k rozmnoženinám. Mnoho uživatelů, ale i odborníků často užívá pojem „záložní rozmnožena", který však nesprávně zaměňují s tvorbou rozmnoženiny pro osobní potřebu. Záložní rozmnožena je totiž definována v § 66 AZ, jež stanovuje omezení autorských práv ve vztahu k počítačovému programu. Tato úprava má ovšem zcela odlišný režim oproti § 30. V souladu se zněním § 66 AZ si záložní rozmnoženinu může zhotovit pouze oprávněný uživatel a to pouze za podmínky, že je taková rozmnožena nezbytná pro užívání počítačového programu. Tímto se rozumí např. možnost oprávněného uživatele nově instalovat počítačový program při změně HW nebo při změně OS apod. Pro tyto účely je pak zcela nepodstatné, je-li záložní rozmnožena pořizována pro osobní potřebu či nikoli. Dle § 66 odst. 6 AZ je „*oprávněným uživatelem rozmnoženiny počítačového programu oprávněný nabyvatel rozmnoženiny počítačového programu, který má vlastnické či jiné právo k rozmnoženině počítačového programu, a to za účelem jejího využití, nikoli za účelem jejího dalšího převodu, dále oprávněný nabyvatel licence nebo jiná osoba oprávněná užívat rozmnoženinu počítačového programu.*" Závěrem je nutné konstatovat, že oprávněný uživatel musí být držitelem, na rozdíl od tvorby rozmnoženiny pro osobní potřebu běžným uživatelem, specifického oprávnění k užití počítačového programu, které mu umožňuje záložní rozmnoženinu zhotovit.[161]

3.5.4 Nejčastější způsoby porušování softwarových autorských práv

V podkapitole 3.5.2 jsme si přiblížili způsoby, kterými dochází k porušování autorských práv v souvislosti se softwarem. Některé z nich podrobněji rozebereme a

---

[159] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. Pro praxi. ISBN 978-80-7380-501-2. s. 350

[160] PFEFFER, Jan. *Softwarové pirátství*. Praha, 2009. Diplomová práce. PF UK. Vedoucí práce JUDr. Petra Malá Žikovská. s. 10

[161] tamtéž s. 10-11

právně posoudíme.

3.5.4.1 Šíření SW prostřednictvím internetu – webové úložiště a P2P sítě

Tuto podkapitolu věnujeme šíření SW prostřednictvím filehostingu a P2P sítí. Stejně jako v sekci pirátství audio a audiovizuálního děl, hraje i u softwarového pirátství internet velmi významnou roli, jak z hlediska legálního, tak hlavně nelegálního sdílení. Opět bychom mohli posoudit roli a právní odpovědnost všech subjektů, které se celého procesu šíření SW účastní. Avšak z hlediska uploadera a také provozovatele serveru úložiště (u P2P sítí víme, že provozovatel sítě se objevuje jen zřídka a jen u některých typů, proto o něm nehovoříme) by právní posouzení pouze rekapitulovalo již jednou, celkem zevrubně, uvedený právní rozbor této problematiky těchto subjektů. Proto jej opět uvádět nebudeme, odkážeme na předchozí pasáže, a zaměříme se na posouzení role downloadera, tj. uživatele staženého softwaru. Nicméně pokud bychom dospěli k závěru, že i role uploadera by mohla být posouzena rozdílně, tuto drobnou úpravu v posouzení zde zmíníme.

Posouzení právní odpovědnosti downloadera SW z webových úložišť je oproti stahování filmů odlišné. U „běžných" děl, mezi které filmy patří, jsme legálnost jejich stahování pro svou vlastní potřebu podepřeli ustanovením § 30 AZ, tj. možností volného užití a samozřejmě nutností obstát v třístupňovém testu. Jak jsme si ale v předchozí podkapitole uvedli, v případě zvláštního druhu díla – počítačových programů, toto neplatí, ustanovení volného užití se programů netýká a tak ani třístupňový test nepřichází do úvahy. Pořídit rozmnoženinu díla, což samotné je již chápáno jako užití díla, je možné jen ve zvláštních případech a pouze v souladu s § 66 AZ. Z tohoto je jasné, že v případě downloadera, byť by si do svého počítače program pouze stáhl, se již jedná o užití díla a k takovémuto užití je nutné oprávnění, nejčastěji licence k danému programu. Pouhé stažení programu je protizákonné a nese s sebou veškerou právní odpovědnost za toto konání. O případné instalaci programu a jeho užití již ani není třeba hovořit, neboť i to je samozřejmě nelegální a budeme se tomu věnovat v další kapitole. Nyní však posoudíme situaci pouze z hlediska stahování. Stahování SW vybavení je protizákonné a jednání je možné posoudit obdobně jako v případě uploadera. Což již velmi dobře víme, neboť tento problém jsme již několikráte diskutovali.

Zaměříme se na malou odchylku, která v případě šíření SW může nastat. Autor práce se domnívá, že ačkoli trestní právo je nástrojem *ultima ratio,* v těchto případech by se jej mělo užívat častěji než při šíření filmů. A to jak z hlediska downloadera, tak především uploadera, což je ona drobná odchylka, na kterou jsme upozorňovali. Je to způsobeno rozdílnou cenou jednoho filmu či songu a jednoho programu, kdy tento rozdíl je mnohdy v rámci několika řádů. Cena například jednoho DVD filmu se totiž pohybuje od cca 50 do cca 500 Kč, zatímco programy na DVD začínají v řádu tisíců korun, ale mohou dosahovat i desítky či někdy dokonce i stovky tisíc korun, v případě speciálních grafických programů. Pokud dochází ke sdílení, tak velikostně z hlediska soborů se jedná v obou případech o to samé, avšak výše škody je nesrovnatelná. Přitom však sdílení programů o tolik za sdílením filmů nezaostává, je tedy jasné, že SW pirátství způsobuje vyšší škody a užití trestního práva je tímto, zejména v případě uploadera, ale častěji i downloadera, dle autorova mínění, opodstatněné. Vyvstává zde však jeden problém, obdobně jako u filmů či hudby, kterým je stanovení správné výše škody, od čehož se odvíjí správná trestněprávní klasifikace. Zda je možné vyčíslení škody vypočítat jako vynásobení počtu stáhnutí díla jeho cenou, na to se pokusíme odpovědět v podkapitole 3.7.

U P2P sítí by se zdálo, že rozdílnost posouzení situace uploadera – seedra a downloadera – leechera při šíření audio a audiovizuálních děl a SW by nastat neměla a posouzení by mělo být totožné. Občas se však objevuje právní názor, který autor práce sice nesdílí, přesto si jej uvedeme. Rozdílnost se týká posouzení situace leechera. Již víme, že autorské právo se vztahuje nejen na dílo dokončené, avšak i na jeho jednotlivé vývojové fáze a části, čehož jsme pro posouzení šíření prostřednictvím P2P sítí využili.

Autorské právo k počítačovému programu se tedy vztahuje jak na celý program, tak na jeho jednotlivé části – podprogramy, procedury, pasáže textu. Nabízí se ovšem otázka, kdy se rysy autorského díla vytrácejí natolik, že s nimi mizí i ochrana autorským zákonem. Postupná atomizace u počítačových programů vede ke stálému snižování prvků individuality a originality, takže na úrovni jednotlivých příkazů již prakticky nelze hovořit o autorském díle, rozhodně nikoliv ve smyslu § 2 odst. l AZ. Čili zachovávat ochranu jednotlivým příkazům programu chráněného ve významu § 2 odst. 2 AZ by opět smysl nemělo, neboť poté by byly chráněny i ty nejzákladnější a běžně užívané programové příkazy typu „IF A=B THAN DO C“. Je jasné, že originalita

programu, nebo i jeho části, je rovněž vlastností, jež se v jistém okamžiku při vytrvalém rozdělování programu na stále menší části vytrácí.[162] Z této myšlenky poté vychází názor, že u P2P, kdy leecher sdílí jisté drobné části, jak již víme, sdílí vlastně jen jednoduché binární příkazy, které není možné chránit AZ. V souladu s uvedeným poté nemůže porušovat AZ a stahování skrze P2P síť tedy není nezákonné. Jak jsme již uvedli, autor práce s takovýmto posouzením nesouhlasí. Míra ochrany je vždy záležitostí konkrétního posouzení každé jednotlivé kauzy a to při sdílení u P2P je zcela jasné. Cílem je dosáhnout stažení celého kompletního díla, nikomu při tom nejde o pouhé dílky, neboť by nebyly k ničemu, jde o celý program a je tedy nutné situaci takto posuzovat. Z uvedeného je jak seeding, tak i leeching nelegální s právním posouzením uvedeným v podkapitole 3.4.2.1 na str. 70 této práce.

U šíření odkazů na stažení SW skrze warezová fóra zastává autor názor, že jde o obdobu warezu běžných děl a proto není nutné se situaci SW warezu více věnovat.

3.5.4.2 Používání počítačového programu bez licence

Dalším a dle statistik poměrně značně rozšířeným deliktem je užívání SW bez licence, tj. vlastně kradeného programového vybavení. V kapitole o komerčním softwaru, jsme zmiňovali, že k legálnímu užití programů je třeba souhlasu autora, nejčastěji ve formě licence k danému počítačovému programu. Pokud je počítačový program užíván bez licence, jedná se o porušení AZ. K tomuto porušování dochází obzvláště u koncových uživatelů, tedy v domácnostech a ve firmách. Autor se proti těmto osobám může domáhat ochrany na základě § 40 AZ, může také požadovat náhradu škody či vydání bezdůvodného obohacení podle obecných právních předpisů, zejména OZ.[163] Většinou se tak děje prostřednictvím adhezního řízení, avšak jen pokud probíhá řízení trestní. Málokdy se autor domáhá svého práva skrze podanou civilní žalobu, neboť v tomto případě musí zcela, nebo alespoň z části, unést důkazní břemeno a to z hlediska vyčíslení škody není jednoduché. Využití adhezního řízení je pro vymáhání škody jednodušší, třebaže ne vždy dosáhne poškozený na odškodnění v požadované výši.

---

[162] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. Pro praxi. ISBN 978-80-7380-501-2. s. 351-352

[163] PFEFFER, Jan. *Softwarové pirátství*. Praha, 2009. Diplomová práce. PF UK. Vedoucí práce JUDr. Petra Malá Žikovská. s. 12

Pokud bychom využili norem veřejného práva pro posouzení jednání koncového uživatele, jež používá program bez řádné licence, záleželo by na posouzení každé jednotlivé situace. Avšak již jsme uvedli, že u SW pirátství dochází k vyšším škodám, proto je užití trestního práva více pravděpodobné. Také se dá předpokládat, že uživatel, který užívá jeden program nelegálně, bude mít i některé další programy na svém počítači v rozporu se zákony, čímž se škoda opět zvyšuje. Přesto v méně závažných případech, kdy neoprávněné jednání nebude naplňovat znaky trestného činu porušení autorského práva, práv souvisejících s právem autorským a práv k databázi podle § 270 TZ, bude klasifikováno jako **přestupek** a narušiteli bude hrozit na základě § 105a – 105c AZ pokuta až 150 000,- Kč. Pokud však intenzita porušení bude OČTŘ posouzena jako vyšší, což se pro uvedené dá předpokládat, bude se jednat o **trestný čin** dle § 270 TZ, jež jsme si důkladně přiblížili v podkapitole 3.3. Posouzení se bude lišit pouze v subsumování pod jednotlivé odstavce dané skutkové podstaty a to zejména dle výše způsobené škody.

3.5.4.3 Překročení licencí

Dalším způsobem porušování autorskoprávně chráněných děl je překročení počtu licencí. Toto se děje zejména v různých firmách, nicméně je možné i v případě domácnosti s více počítači nebo notebooky. Jedná se o případy, kdy společnost má sice určitou licenci na užívání počítačového programu legálně zakoupenu, nicméně následně překročí meze této licence. Obvykle je totiž licence určena k užití na jednom počítači. Porušení tak spočívá v jakési falešné domněnce, že je vlastně vše v pořádku a k žádnému porušování práv nedochází. Opak je ovšem pravdou a takové jednání bezpochyby odporuje licenčnímu ujednání a autor díla se může opětovně domáhat ochrany, jak jsme již výše uvedli. Odpovědnost za vzniklou škodu a celkovou situaci ponese jednak společnost, tedy její statutární orgány, a případně i jiné osoby v možném zaměstnaneckém poměru, které jsou vzhledem ke své pozici za řádný provoz počítačových programů a jejich licencování odpovědné.[164]

Z hlediska právního posouzení by oproti předchozí podkapitole mohl být rozdíl v rozšíření odpovědnosti na právnickou osobu, tedy firmu, která program používá na

---

[164] PFEFFER, Jan. *Softwarové pirátství*. Praha, 2009. Diplomová práce. PF UK. Vedoucí práce JUDr. Petra Malá Žikovská. s. 12-13

více počítačích, než by měla, a to právě díky ZTOPO, neboť posouzení daného jednání jako přestupku, spíše ale správního deliktu, není příliš pravděpodobné. Ustanovení § 270 odst. 2 písm. a) TZ totiž udává, že „*vykazuje-li čin uvedený v odstavci 1 znaky obchodní činnosti nebo jiného podnikání,*“ dojde tímto k naplnění skutkové podstaty TČ, čímž je jednání trestné a není možné jej posoudit jako správní delikt. Díky tomuto je možné užití ZTOPO a firmu jako PO trestně stíhat. A že v případě firmy se o podnikání bude jednat, o tom není v celku pochyb. Výjimky a posouzení jako správního deliktu by mohly nastat např. u škol, kdy tato instituce, jež primárně není založena pro obchodní činnost či podnikání, překročí užití licence. Zde by mírnější posouzení, dle autora práce, možné bylo.

3.5.4.4 Předinstalovaný SW výrobcem počítače aneb prodej HW bez legálního SW

Dalším způsobem, kterým dochází k porušování AZ, je prodej počítače bez legálního programového vybavení. Prodej samotného počítače bez SW, či dokonce pouze komponent, ze kterých si uživatel počítač sám sestaví, již v dnešní době téměř neexistuje. Názorným příkladem jsou notebooky, které dnes bez SW není ani možné sehnat. Uživatel tak téměř vždy zaplatí alespoň za licenci OS Windows, tedy pokud nemá zájem o NTB firmy Apple. I v případě, že poté na notebook nainstaluje vlastní OS, má přesto licenci jiného OS. Pro zvýšení hodnoty prodávaného stroje či jeho vyšší konkurenceschopnost se tak jeho prodejci snaží na počítač již před jeho prodejem umístit značné množství počítačových programů. Pokud ale k umístění těchto programů nemají povolení autora nebo osoby vykonávající správu autorských práv k redistribuci, prodeji, instalování daného počítačového programu, dopouští se opět porušování AZ. Tímto jednáním však oproti konkurenci získávají určitou výhodu, jelikož v případě oprávněné instalace těchto programů by se náklady zvýšily a tím zcela logicky i cena prodávaného produktu. Autor díla by se opět mohl domáhat ochrany podle AZ i podle OZ.[165] Nabízí se však otázka, po kom případné odškodnění vyžadovat. Po prodejci nebo po kupujícím, který posléze programy bude využívat? Pokud kupující byl v dobré víře, že kupuje celý komplet i s programy, které mohou mnohdy být uvedené i na falešném prodejním dokladu, pak asi pouze na prodejci. Pokud ale kupující mohl předpokládat, že

---

[165] PFEFFER, Jan. *Softwarové pirátství*. Praha, 2009. Diplomová práce. PF UK. Vedoucí práce JUDr. Petra Malá Žikovská. s. 13

SW není nainstalován legálně, poté i po něm je možné odškodnění požadovat.

Obdobně lze posoudit subjekt přestupkové nebo trestní odpovědnosti. A pokud již máme subjekt, je možná klasifikace, která pro prodejce bude totožná s tou v předchozí podkapitole, jen s rozdílem případného posouzení jako přestupku (u FO podnikatele) a správního deliktu (u PO). U prodejce jde opět o obchodní činnost, což je přitěžující okolnost a jednání bude hodnocené spíše jako trestný čin. Pokud byl kupující v dobré víře, je jeho jednání beztrestné, pokud o problému věděl, pak by záleželo na rozsahu a množství SW, zda by šlo o přestupek, nebo o trestný čin.

3.5.4.5 OEM licence Microsoft operačních systémů a jejich další užití

V sekci OEM licence jsme uvedli, že se k jejich problematice ještě vrátíme. Následující část budeme tedy věnovat problematice dalšího prodeje OEM licence. Zda je legální či ne. Licenční podmínky všech výrobců ho totiž zakazují.

K prodeji použitého softwaru dochází celkem běžně. Jednak spolu s prodejem použitého hardwaru a časté jsou rovněž prodeje v různých internetových aukcích či inzertních serverech. Zpravidla je tak prodávána jedna licence získaná s prodávaným počítačem nebo jedna licence softwaru, který byl zakoupen zvlášť na CD nosiči. Nicméně výrobci softwaru proti takovému jednání brojili, neboť jej chápali jako rozpor s licenčním ujednáním. Zda právem či ne již dnes díky rozhodnutí SDEU víme, avšak než jednoznačně odpovíme, je nutné si vysvětlit zejména pojem vyčerpání autorských práv, který je definován v § 14 odst. 2 AZ. [166] Princip vyčerpání se vztahuje pouze na rozšiřování, nikoliv na rozmnožování, originálu. Z ustanovení AZ vyplývá, že k vyčerpání autorských práv dochází prvním prodejem originálu nebo rozmnoženiny autorského díla. Nicméně je nutné uvést, že princip vyčerpání se nepoužije na on-line zpřístupňování autorských děl, což je pro současný způsob prodeje licencí velmi důležité. Pokud totiž autor či držitel autorských práv umožňuje download autorského díla, užije se zásada zakotvená především v evropské směrnici[167], podle které je každá

[166] znění § 14 ost. 2 AZ – Prvním prodejem nebo jiným prvním převodem vlastnického práva k originálu nebo k rozmnoženině díla v hmotné podobě, který byl uskutečněn autorem nebo s jeho souhlasem na území některého z členských států Evropské unie nebo některého ze států tvořících Evropský hospodářský prostor, je ve vztahu k takovému originálu nebo rozmnoženině díla právo autora na rozšiřování pro území členských států Evropské unie a států tvořících Evropský hospodářský prostor vyčerpáno; právo na pronájem díla a právo na půjčování díla zůstává nedotčeno.

[167] Směrnice Evropského parlamentu a Rady 2014/26/EU ze dne 26. února 2014 o kolektivní správě autorského práva a práv s ním souvisejících a udělování licencí pro více území k právům k užití hudebních děl online na vnitřním trhu

on-line služba úkonem, který musí podléhat schválení. Na tomto principu nic nemění fakt, že si konečný uživatel může stažené autorské dílo vypálit na CD či DVD nebo vytisknout a zhotovit si rozmnoženinu. Stále bude platit, že bez výslovného souhlasu nelze takovou „rozmnoženinu“ rozšiřovat.[168]

Problémy s dalším prodejem OEM licence v právním světě vyvstaly již v roce 2000 v Německu, kdy Nejvyšší soud aplikoval princip vyčerpání i na tzv. OEM verze softwaru od Microsoftu a rozhodl, že OEM verze lze rozšiřovat i samostatně, aniž by byly součástí nově zakoupených počítačů.[169] Avšak konečné, zásadní a doporučující stanovisko k tomuto problému vydal až červenci 2012 SDEU ve svém rozsudku ve věci C-128/11 UsedSoft GmbH v. Oracle International Corp. Z daného rozsudku vyplývá, že „*tvůrce programového vybavení nemůže bránit dalšímu prodeji svých „použitých“ licencí umožňujících užívat jeho programy stažené z internetu*“ a také, že „*výlučné právo na rozšiřování rozmnoženiny počítačového programu, na kterou se taková licence vztahuje, se vyčerpá prvním prodejem této rozmnoženiny.*“ Z uvedené tak vyplývá důležitý závěr, který je možné shrnout do věty: „*Pasáže licenčních smluv, které obsahují případný zákaz dalšího prodeje OEM licencí, neplatné*.“[170]

Ohledně převodu OEM licencí probíhala v Česku, na rozdíl od jiných evropských států, diskuse ohledně možnosti „přenosu“ OEM licencí, tedy možnosti odprodat zvlášť OEM licence, např. pokud dojde ke zničení HW počítače, nicméně s nejasným výsledkem. Tento problém soudní rozhodnutí s konečnou platností ukončilo ve prospěch zákazníků a ve prospěch trhu s volným obchodováním nepoužívaných softwarových licencí. Od daného rozhodnutí se téměř veškerý software stává přenositelným. Hlavní myšlenkou rozhodnutí je, aby uživatel využíval pouze tolik softwarových licencí, kolik je potřebné a to v takových verzích, jež odpovídají skutečným potřebám daného uživatele. Ne vždy je nezbytné pořizovat nejnovější dostupné verze softwaru, ale běžní prodejci starší verze nabídnout nedokáží.[171]

Autor práce se pokusil toto rozhodnutí ověřit, zda-li v praxi výrobci SW dodržují

---

[168] Právní aspekty prodeje použitého softwaru. *Systemonline.cz* [online]. 2007 [cit. 2016-03-21]. Dostupné z: http://www.systemonline.cz/sprava-it/pravni-aspekty-prodeje-pouziteho-softwaru.htm

[169] tamtéž

[170] Poznejte druhotný software. *Vyhodny-software.cz* [online]. 2013 [cit. 2016-03-21]. Dostupné z: http://www.vyhodny-software.cz/pro-media/poznejte-druhotny-software/

[171] tamtéž

vše uvedené a informují zákazníky, že mohou OEM licence dále nabízet. I v případě kdy byl OS dodán s notebookem a ten již nefunguje. Na obr. 5 je tak emailová odpověď

Od: "Czech Customer Service" <CNTUS.PRSL.EU.CZ.CS.ARV.BRN.CS.T01.CUS.00.EM@css.one.microsoft.com>

Komu: "mně"

Předmět: RE: SRX1126944360ID - Dotaz ohledně přenosu OEM licence Windows

Datum: 10.03.2015 09:50

Velikost: 30,6 kB

Vazeny pane Hefko,

dekujeme Vam, ze jste kontaktoval Zakaznicke centrum spolecnosti Microsoft

Vec: Moznosti prenositelnosti licence

Reseni:

Prenositelnost softwaru je zavisla na licenci, tzn. zalezi na tom jak jste zakoupil Vas operacni system:

FPP verze (krabicova): tuto verzi je mozno prenaset na jiny PC. Nejdrive je nutne licenci odinstalovat z puvodniho pocitace a nasledne je mozne licenci nainstalovat na jine zarizeni. Take je mozne menit jakekoliv komponenty v PC. Verze se pote aktivuje pres nasi aktivacni linku: 800 100 074.

- http://www.microsoft.com/cze/licence/fpp/default.mspx

OEM verze (predinstalovana v novem PC nebo zakoupena samostatne - to bylo mozne do konce roku 2008) : tato verze je neprenositelna a plne vazana na zakladni desku PC. Dale je mozno menit veskere komponenty krome zakladni desky. Tu smi zakaznik vymenit pouze v pripade poniceni nebo poskozeni. Pokud je nutna vymena behem dvoulete zaruky PC, je mozno produkt opet aktivovat na nasi aktivacni lince na cisle 800 100 074 nebo 261 197 665.

- http://www.microsoft.com/cze/licence/oem/default.mspx

V pripade prokazani servisnim dokladem, ze je notebook nepouzitelny, je mozne licenci znovu nainstalovat a telefonicky zaktivovat.

Pokud mate dalsi dotazy, nevahejte se na nas prosim obratit.

S pozdravem,

Petra Urbankova

Microsoft s.r.o.
Zakaznicke centrum
BB Centrum, budova Alpha
Vyskočilova 1461/2a
140 00 Praha 4

Tel.: + 420 841 300 300
Fax: + 420 543 550 342
E-mail: czinfo@microsoft.com
Web: http://support.microsoft.com
Spolecnost Microsoft poskytuje vsem svym zakaznikum unikatni sluzbu technicke poradny on-line a to zdarma! Technickou poradnu on-line najdete na adrese http://support.microsoft.com/start.

Stranky obsahuji tipy a triky, ktere zprijemni a zjednodussi vasi praci se softwarem spolecnosti Microsoft, a tisice rad a navodu na reseni ruznych problemu prave s timto softwarem.

Mate pripominky, ci podnety ke spolecnosti Microsoft? Nenechavejte si je pro sebe. Napiste nam, co bychom mohli zlepsit ma adrese http://www.microsoft.cz/podnety/register.aspx

Obr. 5

na dotaz, který autor této práce zaslal společnosti Microsoft, zda je možné legální užití a aktivace OS, který původně sloužil na jiném počítači. Je zřejmé, že Microsoft rozhodnutí respektuje a zcela v souladu s právním stavem odpověděl. Škoda jen, že této odpovědi se dostane jen tomu, kdo se zeptá, neboť jinak jsou OEM licence prezentovány jako dále neprodejné a hlavně nepřenosné.

Pokud je tedy takovéto nakládání s OEM programem v souladu s výše uvedeným rozhodnutím, nemůže být postihováno jako přestupek, natož jako trestný čin. Výrobcům programů se však takovéto rozhodnutí nezamlouvá. Nechtějí akceptovat přenos licencí na jiné stroje, a to ani za předpokladu, že původní HW již nefunguje, protože tím přicházejí o peníze z prodeje jiné licence. Z tohoto důvodu od OEM licencí spjatých s HW ustupují a současnost nabízí produkty tzv. Click-to-Run.

Click-to-Run představuje Microsoft streamovací a virtualizační technologii určenou pro instalaci, spouštění a aktualizaci Microsoft Office aplikací. Princip fungování je založen na technologii Microsoft Application Virtualization (App-V). Virtualizační technologie vytvářejí na lokálním počítači izolované prostředí, ve kterém jsou aplikace Microsoft Office na spouštěny. Po dokončení úvodní instalace může uživatel s produkty Office pracovat i bez připojení k internetu, protože všechny aplikace jsou staženy na lokální počítač, a nejsou tak spouštěny z žádného internetového nebo lokálního serveru.[172] Vzhledem k tomu nemusí být SW šířen prostřednictvím fyzického nosiče a prodávám např. jako OEM licence, ale uživatel si program stáhne on-line. A jak již víme, princip vyčerpání se na on-line zpřístupňování autorských děl nepoužije. Tímto tak Microsoft zamezil případnému přeprodávání licencí. A ačkoli je tato služba prezentována jako zlepšení pro uživatele, autor práce se domnívá, že hlavním důvodem je právě snaha o finanční profit z dalších a dalších licencí za své produkty.

3.5.4.6 Cracking podruhé

Již z první kapitoly víme, že cracking představuje činnost, jež obecně souvisí s kybernetickou bezpečností. Nicméně představuje i jistou formu softwarového pirátství. Z tohoto důvodu se této aktivitě, jak bylo zmíněno, budeme věnovat ještě jednou a to z pohledu právě této podkapitoly. Cracker je též osoba porušující autorská

[172] Týdny s Office - Office 365 a instalace Office Click-to-Run. *Optimalizovane-it.cz* [online]. 2015 [cit. 2016-03-21]. Dostupné z: http://www.optimalizovane-it.cz/technet-cz/sk/tydny-s-office-office-365-a-instalace-office-click-to-run.html

práva. Za cracking je pak v tomto smyslu označováno jednání crackera spočívající v obcházení ochranných prvků, které jsou ve smyslu § 43 odst. 1 AZ označovány jako účinné technické prostředky ochrany. Jsou jimi:

- *registrační číslo* (serial number), jež je mnohdy nezbytné k úspěšnému nainstalování aplikace
- *časové omezení* (time limit), které umožňuje program využívat jen po předem stanovenou dobu, nebo jen se stanovenými funkcemi, např. trial
- *registrační soubor* (key file), který se užívá k úspěšné instalaci místo registračního čísla
- *samostatný program*, který je potřebný k běhu programu jiného
- *hardwarový klíč* (dongle), což je technický prostředek, který je připojen ke komunikačnímu portu počítače a bez kterého nelze program spustit, využíváno portu USB, dříve to býval port LPT a klíč byl „průchozí"
- *kontrola originálního CD/DVD*, což je způsob kontroly, zda je v mechanice počítače vložen originální nosič
- *demoverze* neboli programy, jejichž jednotlivé části a funkce jsou pro uživatele zablokovány, nebo odstraněny, což je činí nezajímavými pro kopírování
- *další typy ochrany*, kombinace předchozích, nebo též metody používané hackery ke zpřístupnění plné funkce programu[173]

Tímto způsobem pak pachatel může software chráněný copyrightem užívat bezplatně a velmi často ho i šířit dál prostřednictvím internetu. Mezi nejčastěji crackovaný software patří počítačové hry. Potřebné cracky (ať již kódy či sériová čísla) se dají poměrně snadno vyhledat na internetu v různých fórech, jež vyžadují registraci, čímž se chrání před odpovědností za obsah. Mimo jiné často nabízejí i podrobné návody, nebo přímo speciální program na vygenerování požadovaného cracku, tzv. keygen, takže cracknout programu nevyžaduje žádnou zvláštní znalost či počítačovou obratnost. Tímto se zvyšuje množství veřejnosti, které může spáchat trestný čin.[174]

---

[173] ZEMAN, Daniel. *Počítačová a internetová kriminalita*. Praha, 2011. Diplomová práce. PF UK. Vedoucí práce Doc. JUDr. Tomáš Gřivna, Ph.D. s. 78-79

[174] VIRDZEKOVÁ, Alica. *Trestoprávna úprava internetovej kriminality*. Brno, 2011. Diplomová práca. Právnická fakulta Masarykovy univerzity. Vedoucí práce Doc. JUDr. Josef Kuchta, CSc. s. 33

Vlastní akt prolomení technické ochrany může být trestněprávně posouzen jako trestný čin neoprávněného zásahu k počítačovému systému a nosiči informací podle § 230 TZ, což již víme, avšak překonávání technických prvků ochrany je charakterizováno jako trestný čin porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 270 TZ. Stejně tak jako případné užívání daného programu bez licence s eventuálně možným posouzením přitěžujících okolností pro užití kvalifikované skutkové podstaty.

3.5.5 Judikatura NS pro softwarové pirátství

Jedním z důležitých rozhodnutí pro posuzování trestnosti v oblasti softwarového pirátství je usnesení Nejvyššího soudu ze dne 26. března 2014, sp. zn. 5 Tdo 62/2014. V dané věci šlo o případ, kdy byl rozsudkem Obvodního soudu jistý jednatel uznán vinným přečinem porušení autorského práva, práv souvisejících s právem autorským a práv k databázi podle § 270 odst. 1, 2 písm. b) TZ. Jednání se dopustil tím, že instaloval a užíval na firemním hardwarovém zařízení za účelem podnikatelské činnosti u celkem 98 kusů počítačů a 2 serverů komerční software bez licence a souhlasu nositelů autorských práv k mnoha počítačovým programům, čímž uvedeným poškozeným nositelům autorských práv k uvedeným počítačovým programům způsobil škodu v celkové výši 1.495.076,- Kč. Nutno poznamenat, že se jednalo o součet částek, které představovaly prodejní ceny licencí daných nainstalovaných programů. Obžalovaný se hájil tvrzením, že společnost, ve které k danému jednání došlo, byla součástí programu BizSpark, v rámci kterého mělo být k dispozici veškeré portfolio všech produktů společnosti Microsoft k vlastnímu využívání zdarma. Toto tvrzení vyvrátila zpráva zástupce společnosti Microsoft, ve které bylo uvedeno, že tento program sice existuje a obviněný se do tohoto programu pokusil přihlásit, ale protože nesplňoval podmínky programu, nebyl vstup této společnosti do programu schválen a registrace byla smazána. NS poznamenal, že jednáním způsobil jinému značnou škodu a tím se přiklonil k výpočtu výše škody. Také souhlasil s uloženou výší trestu a to ve výměře 1 roku s odkladem na zkušební dobu v trvání 18 měsíců. Případ byl zajímavý i z hlediska posouzení právní odpovědnosti PO, na což také obžalovaný poukazoval. Nicméně v době páchání TČ byl sice již ZTOPO platným zákonem právního řádu ČR, avšak nebyl zatím zákonem účinným. Další obranou bylo tvrzení, zda je možné každý

počítačový program považovat za autorské dílo ve smyslu AZ, na což dané usnesení také dává odpověď. A v neposlední řadě byla na obranu „povolána“ zásada *ultima ratio,* tj. že se soud nedostatečně vypořádal s tím, zda není v tomto případě možné na porušování autorského práva použít v prvé řadě prostředky práva civilního. A ještě bylo namítnuto, že soudy nepřihlédly ke stupni nebezpečnosti činu pro společnost. I s těmito námitkami se NS soud v daném usnesení vypořádal a dává nám tím na tyto případné otázky i odpovědi. NS poté posoudil dané dovolání jako zjevně neopodstatněné, a proto je podle § 265i odst. 1 písm. e) TŘ odmítl.

3.5.6 SW programy a podklady pro autonavigace

Autor práce nemůže nepoznamenat, že ne každý zásah do SW, ač může mít značný rozsah, by měl být posuzován jako čin trestný. Na příkladu autonavigace DVD Carminat montované do automobilů značky Renault si můžeme demonstrovat případ, jež by měl být místo TČ posuzován podle mírnějších právních prostředků.

Zabudovaná navigace v autě, která s autosystémy spolupracuje, se dnes chápe jako jistý standard. Pro správnou funkčnost je nutná aktuálnost mapových podkladů. Jak má ale vlastník daného automobilu postupovat, když firma Renault nový programový systém s aktuálními podklady neprodává? Nezbývá nic jiného, než jiný obdobný systém rozebrat a použít jako „mustr“ k sestavení programu pro jiný, avšak kompatibilní systém. Stejně tak použít jiné mapové podklady a do tohoto systému je zakomponovat. Není zřejmě překvapením, že tímto jednáním se bude zaobírat jistá podskupina warezového fóra. Daný nově sestavený systém se pak začne komerčně prodávat a tím pádem dojde k naplnění, dokonce kvalifikované, skutkové podstaty TČ. I přes uvedené, autor práce stále trvá na názoru, že takovéto jednání by nemělo být posuzováno jako trestné.

V celé záležitosti je totiž důležitým faktem, že tento systém byl ještě v roce 2011 do vozidel značky Renault montován za poměrně vysokou částku cca 70.000,-Kč. Přesto však společnost Renault vydala poslední mapový SW pro tento systém v roce 2012 a od té doby, ani přes značné naléhání uživatelů minimálně z celé Evropy, nikoli. Proto znovu zopakujeme, že každou kauzu je nutné posoudit individuálně a to ze všech možných pohledů na danou věc.

3.6 Pirátství optických disků

Následující podkapitola spojuje obě oblasti zmiňovaného pirátství. Ačkoli je v dnešní době tento typ deliktů již za svým vrcholem, i tak stále ještě dokáže napáchat ohromné škody. Tímto typem zločinu je pirátství optických disků, kdy hmotným substrátem díla je optický disk (zejména DVD-/+R, DVD a CD-R). Pirátství se začalo v České republice vyskytovat v průběhu roku 2000, nicméně jeho značný rozvoj nastal až v roce 2002 zejména v souvislosti s rozšířením DVD technologie. V počátcích chránily český trh kromě malého rozšíření příslušné technologie také další skutečnosti, zejména nízká jazyková vybavenost zákazníků, kteří navíc dávali přednost dabovaným filmům před titulkovými a poměrně malý počet česky hovořícího obyvatelstva, pro které se pirátům nevyplatilo průmyslově vyrábět národní verzi. Obdobné poznatky jsme již zmínili v případě jazykových úprav DVD. S rozšířením technologie DVD rostl zároveň počet lidí, disponujících nejen přehrávačem DVD, ale i jiných formátů, zejména video kompaktních disků a v některých případech i CD-R či CD-RW. I běžné přehrávače DVD totiž umožňovaly a stále ještě umožňují přehrát film všech možných formátů, i vypálené CD, pokud je vypáleno ve formátu VCD, ale i vypálené DVD, opět všech možných formátů, včetně média dvouvrstvého.[175]

Z hlediska pirátských aktivit stále ještě představuje DVD v dnešní době lehce dostupný, kvalitní a aktuální vzor k výrobě jiných pirátských nosičů. Zároveň také reprezentuje ideální nosič k distribuci do velkého počtu jazykově odlišných regionů, neboť vzhledem ke své kapacitě umožňuje současné zaznamenání velkého počtu titulů a dokonce i zvukových stop. Globální digitální pirátství má v zásadě dvě hlavní podoby. Jednou je výroba a distribuce pirátských lisovaných DVD, druhou úprava záznamů filmů do formátu pro DVD-R a CD-R a jejich šíření prostřednictvím internetu. Boj proti oběma těmto problémům musí být zaměřen především proti zdroji pirátství a jeho příčinám. Náš trh však ponejvíce zasahuje zejména internetová forma pirátství a následného přepalování v DVD, tj. prostřednictvím internetu dojde ke stažení DVD obrazu, který je poté zpětně vypálen na DVD a ten získá opětovně fyzickou podobu.[176]

---

[175] Digitální média a pirátství: Audiovizuální pirátství. *Česká protipirátská unie* [online]. 2007 [cit. 2016-03-11]. Dostupné z: http://www.cpufilm.cz/new/www/txt/audiovizualni_piratstvi.pdf. s. 12

[176] tamtéž s. 13

Bohužel jsou však optické nosiče i vhodným médiem, zejména pro svou velikost, k šíření programů a i tento nelegální trh má značný odbyt a páchá stejně nemalé škody. Přičemž z programů na nosičích hrají prim počítačové hry. A i tyto nosiče jsou prostřednictví svých „obrazů“ šířeny skrze internet.

Pokud bychom právně posoudili nastíněné situace, tak v případě stahování díla z internetu již máme jasno a nic na tom nemění ani ten fakt, že poté dojde k jeho vypálení na optický nosič. Jednání není protizákonné, tedy v případě filmových a zvukových obrazů. U softwarových forem je i stahování nezákonné a postižitelné dle zákona, jak jsme již několikrát zmínili, stejně jako sdílení jakýchkoli děl.

V případě prodeje a nákupu fyzické podoby nosiče autor práce zastává názor, již jednou vyslovený, že pokud kupující v dobré víře nosič zakoupí, tak jeho jednání nemůže být postižitelné ani v případě nákupu SW. Pokud však kupující věděl, že se jedná o padělek, pak v případě SW by se o přestupek, potažmo trestný čin, v případě mnoha programů, jednat mohlo. U filmu či hudby ani tehdy ne, pro právní důvody dříve v této práci uvedené. U prodejců je situace jasná, jednání je nezákonné, vykazující obchodní znaky, čili minimálně se jedná o TČ dle § 270 odst. 2 písm. a) TZ, ale v případě rozsáhlého prodeje a tedy i vyšší škody, připadá v úvahu i klasifikace dle odstavce třetího. Díky fyzické podobě disku je také snazší stanovení výše případného prospěchu, který prodejce svým jednáním získal.

3.6.1 Judikatura NS související s posouzením díla pro vlastní potřebu

Ještě jednou se vrátíme k usnesení NS[177], se kterým jsme se již v předchozí části seznámili, nicméně mělo vliv i na posouzení situace případného obchodování s optickými nosiči.

Rozsudkem Okresního soudu ve Zlíně ze dne 9. 4. 2008, sp. zn. 3 T 246/2004, byl obviněný uznán vinným trestným činem porušování autorského práva, práv souvisejících s právem autorským a práv k databázi, neboť bez souhlasu vlastníků autorských práv k užití díla neoprávněně nabízel prostřednictvím internetu na stránkách www.annonce.cz s odkazem na adresu své elektronické pošty k prodeji kopie některých filmů na nosičích DVD-R a CD-R za cenu 150 Kč za kus. Poté, co byl zájemcem

[177] Usnesení Nejvyššího soudu ze dne 25. března 2009, sp. zn. 5 Tdo 234/2009

prostřednictvím elektronické pošty osloven s dotazem, zda nabízí i jiné filmy, zaslal mu seznam celkem 61 filmů. Na základě tohoto seznamu si u něj zájemce elektronicky nějaké filmy objednal. Tyto pak v souladu s objednávkou obviněný poštou odeslal na adresu objednatele na nosičích DVD-R. V době domovní prohlídky přechovával obviněný v místě svého trvalého bydliště 236 kusů DVD-R a CD-R nosičů s kopiemi filmů, počítačových her, hudebních záznamů a počítačových programů.

Krajský soud v Brně, pobočka ve Zlíně, který rozhodoval jako soud odvolací o odvolání obviněného, rozhodl usnesením ze dne 29. 7. 2008, sp. zn. 6 To 320/2008, tak, že odvolání obviněného podle § 256 TŘ jako nedůvodné zamítl.

Nejvyšší soud ČR zrušil rozsudky obou soudů a mj. konstatoval, že:

- co se týká skutku, že bez souhlasu vlastníků autorských práv k užití díla neoprávněně nabízel prostřednictvím internetu na stránkách www.annonce.cz s odkazem na adresu své elektronické pošty k prodeji kopie filmů na nosičích DVD-R a CD-R za cenu 150 Kč za kus, o jeho vymezení a právní kvalifikaci nevznikají žádné pochybnosti
- pokud jde o posouzení další části skutku kladeného obviněnému za vinu spočívající v tom, že přechovával v místě svého trvalého bydliště 236 kusů DVD-R a CD-R nosičů s kopiemi filmů, počítačových her, hudebních záznamů počítačových programů, nelze se závěry soudů obou stupňů ohledně výkladu ustanovení § 30 AZ, upravujícího volné užití díla, zcela souhlasit

Z předchozí části víme, že zhotovovat kopie pro vlastní potřebu není trestné, avšak toto se týká pouze nosičů, jež obsahují počítačové programy. U kopií programového vybavení nelze § 30 užít. V daném případě tak není možné na základě domovní prohlídky předpokládat, že byly veškeré disky připraveny k prodeji a tím je automaticky zahrnout do skutkové podstaty. Ačkoli se to zdá pravděpodobné, je přesto možné, že tyto nosiče sloužili pouze pro osobní potřebu obviněného. Pod trestní posouzení je možné zahrnout pouze ty disky, jejichž případné kopie jsou samy o sobě nezákonné (počítačové programy) a pak ty, ačkoli zdánlivě pořízeny legálně, o jejichž prodeji není žádných pochybností. Jinými slovy: u zvukových a zvukově-obrazových disků je možné stíhat pouze takové jednání, kterým nepochybně došlo k jejich prodeji či předání

(třebaže zdarma) jiné osobě, neboť jen tehdy nebyla splněna podmínka užití pro vlastní potřebu.

3.7 Důležitá judikatura pro vyčíslení škody

V této části práce se nejdříve seznámíme s důležitým rozhodnutím NS[178], jež má značný vliv na posouzení výpočtu výše škody, kterou lze porušením autorského zákona způsobit. Poté se pokusíme nastínit kriterium, dle jakého by se škoda počítat mohla, na což poté v sedmé kapitole vlastními návrhy navážeme.

3.7.1 Usnesení NS ze dne 8. října 2014, sp. zn. 5 Tdo 171/2014

Začátkem roku 2015 byla českými médii věnována značná pozornost zveřejněnému usnesení Nejvyššího soudu ze dne 8. října 2014, sp. zn. 5 Tdo 171/2014, kterým bylo rozhodnuto o dovolání obviněného R.R., jenž byl rozsudkem Městského soudu v Brně ze dne 23. 7. 2013, sp. zn. 89 T 69/2013, uznán vinným zločinem porušení autorského práva, práv souvisejících s právem autorským a práv k databázi podle § 270 odst. 1, 2 písm. c), odst. 3 písm. a) TZ. Za tento zločin byl odsouzen podle § 270 odst. 3 TZ k trestu odnětí svobody v trvání 3 let. Výkon trestu mu byl podle § 81 odst. 1 a § 82 odst. 1 TZ podmíněně odložen na zkušební dobu 5 let. Současně mu byla podle § 82 odst. 2 TZ uložena přiměřená povinnost podle svých sil ve zkušební době nahradit škodu, kterou trestným činem způsobil.

Uvedeného zločinu se podle zjištění soudu prvního stupně dopustil tím, že ze svého počítače v rozporu s § 12, 13, 18, 76 a 80 AZ prostřednictvím internetu bez souhlasu oprávněných nositelů autorských práv vložil na dvě veřejná úložiště **372 filmových audiovizuálních děl** nebo **zvukově obrazových záznamů** a rozmnoženiny **33 hudebních děl**, ačkoli věděl, že jde o díla chráněná autorským právem a k jejich šíření mu nebyl majiteli autorských práv udělen souhlas. Na různých internetových diskusních fórech pak zveřejnil odkazy, na kterých bylo možno uvedená díla stáhnout. Dle názoru soudu prvního stupně tak ve značném rozsahu zasáhl do práv k autorským dílům, která takto neoprávněně rozmnožil a zpřístupnil, čímž způsobil škodu v celkové výši **11.041.514 Kč**. Obviněný uznal svou vinu, nesouhlasil ovšem s výpočtem výše vzniklé škody.

[178] Usnesení NS ze dne 8. října 2014, sp. zn. 5 Tdo 171/2014

NS shledal postup soudu prvního stupně a i postup odvolacího soudu jako nesprávný a to zejména v závěru, který se týkal kvalifikačního znaku škody velkého rozsahu podle § 270 odst. 3 písm. a) TZ, neboť soud prvního stupně pochybil především v tom, jakým způsobem **vyčíslil výši škody,** protože soud postavil závěr o ušlém zisku z neprodaných legálních nosičů na tom, že uživatelé počítačové sítě internet si stáhli z datového úložiště dílo chráněné autorským zákonem, které tam obviněný bez souhlasu oprávněných distributorů umístil, takže si ho v podstatě pořídili, ovšem oprávněným distributorům za to nezaplatili obvyklou cenu. Obvyklou cenu legálního nosiče v době neoprávněného stažení díla zjistil z prodejních katalogů jednotlivých poškozených a ušlý zisk stanovil jako násobek této ceny počtem neoprávněně rozmnožených kopií a počtem jejich stažení jinými uživateli internetu. Výše škody tak byla vyčíslena na částku 11.041.514 Kč. Soud však neopatřil žádné skutkové podklady pro zjištění, že nelegální zpřístupnění chráněných děl uživatelům internetu mělo vliv na prodejnost originálních nosičů. Soud se nezabýval ani tím, že díla, která obviněný neoprávněně sdílel uživatelům internetu prostřednictvím datových úložišť, byla bez jeho přičinění údajně již dříve dostupná prostřednictvím jiných internetových serverů. NS vyslovil názor, že tvrzení soudu prvního stupně o konkrétní finanční ztrátě jednotlivých nositelů práv chráněných autorským zákonem stojí na čistě hypotetickém a nijak nepodloženém základě, že každý uživatel internetu, který si zdarma stáhl z datového úložiště konkrétní film nebo jiný audiovizuální nebo hudební záznam, by si jinak koupil jeho legální DVD nebo CD nosič, s čímž NS, ani autor této práce, nesouhlasí.

Jestliže je výše škody možným znakem základní skutkové podstaty nebo podmínkou podmiňujících použití vyšší trestní sazby, z trestněprávního hlediska nemůže být výše škody vymezena ryze hypotetické. Při rozhodování o vině v trestním řízení musí být totiž všechny znaky skutkové podstaty trestného činu objektivně a bez důvodných pochybností prokázány, a není-li to možné alespoň v minimální míře, pak nelze dospět k závěru o jejich naplnění volnými úvahami, jež mohou být jinak akceptovatelné při rozhodování o náhradě škody. Odvolacím soudem pak byla bez výhrady uznána tato spekulativní a nevhodná konstrukce výpočtu výše škody.[179,180]

---

[179] Usnesení NS ze dne 8. října 2014, sp. zn. 5 Tdo 171/2014

[180] HÁLEK, Jakub. *Autorské právo a jeho porušování na internetu z pohledu škody, náhrady škody a bezdůvodného obohacení* [online]. Praha, 2015 [cit. 2016-03-24]. Dostupné z: http://svoc.prf.cuni.cz/sources/8/17/519.pdf. SVOČ. PF UK. s. 19-22

Nejvyšší soud také odmítl podobnost s překupníkem kradeného zboží, jež soud prvního stupně stroze reagoval na obhajobu obviněného, který namítal, že uživatelé internetu by si legální nosič pravděpodobně vůbec nekoupili. Dle NS je tak třeba přizvat znalce, jehož úkolem bude kvalifikovaně stanovit alespoň minimální výši ušlého zisku oprávněných nositelů práv v návaznosti na to, jaký výnos by jim plynul v případě, pokud by v rozhodné době a za srovnatelných podmínek sami zpřístupnili dílo uživatelům internetu prostřednictvím filehostingových serverů.[181]

V závěru usnesení poukázal NS na to, že v úvahách o tom, v jakém rozsahu byl čin spáchán, se vždy odráží povaha a intenzita narušení chráněných práv včetně toho, že pachatel zvolil k nelegálnímu zpřístupnění chráněných děl veřejně přístupnou počítačovou síť internet a vybízel mnoha odkazy na možnost stažení těchto děl v podstatě neomezený počet uživatelů internetu. Za čin spáchaný ve značném nebo velkém rozsahu lze přitom ukládat trest ve stejné sazbě, jako za čin, kterým pachatel způsobil značnou škodu nebo škodu velkého rozsahu.[182]

Autor práce se domnívá, že Nejvyšší soud v podstatě poskytl jakési doporučení soudům nižších instancí, aby se v případě trestného činu porušení autorského práva, práv souvisejících s právem autorským a práv k databázi nepouštěli do složitého prokazování skutečně způsobené škody na ušlém zisku, nýbrž aby jakožto okolnost podmiňující použití vyšší trestní sazby posuzovali rozsah trestné činnosti.[183] NS sice učinil určitá doporučení, nestanovil však přesný návod, což se od něj nejspíše očekávalo. Přesný způsob výpočtu škody, který mohl NS soud stanovit, by byl vždy objektivním pravidlem, takto zůstalo u posouzení subjektivního. Možná i ne zcela přesné pravidlo, by bylo lepší, než stále nejistý způsob určování výše škody. Takto jsme vlastně na půli cesty. Bylo řečeno, jak to není, ale ne, jak to je. Což pro další případy, kterých jistě bude přibývat není, dle mínění autora, vůbec dobře.

S tímto rozhodnutím NS ale nesouhlasí ředitelka ČPU Markéta Prchalová, která označila některé úvahy NS za zavádějící ba přímo nesprávné. Uvedla, že v rámci

---

[181] HÁLEK, Jakub. *Autorské právo a jeho porušování na internetu z pohledu škody, náhrady škody a bezdůvodného obohacení* [online]. Praha, 2015 [cit. 2016-03-24]. Dostupné z: http://svoc.prf.cuni.cz/sources/8/17/519.pdf. SVOČ. PF UK. s. 19-22

[182] Usnesení NS ze dne 8. října 2014, sp. zn. 5 Tdo 171/2014

[183] HÁLEK, Jakub. *Autorské právo a jeho porušování na internetu z pohledu škody, náhrady škody a bezdůvodného obohacení* [online]. Praha, 2015 [cit. 2016-03-24]. Dostupné z: http://svoc.prf.cuni.cz/sources/8/17/519.pdf. SVOČ. PF UK. s. 19-22

argumentace pravděpodobně došlo k záměně služeb zpřístupňujících nelegální obsah s legálními audiovizuálními mediálními službami na vyžádání, ale také to, že NS nerozlišoval mezi stažením a zhlédnutím díla. Dále zmínila, že o rozsahu trestné činnosti vypovídá i výše škody na ušlém zisku stanovená alternativními způsoby, pokud skutečně vzniklou škodu není možné objektivně vyčíslit.[184]

Ačkoli se dá nesouhlasné stanovisko organizace, která zastupuje autory, s rozhodnutím NS pochopit, neboť jde o peníze, je třeba zdůraznit, že závěry NS o výpočtu výše škody se týkají pouze oblasti trestního práva, nikoliv občanskoprávních nároků na náhradu škody a na vydání bezdůvodného obohacení. Jinými slovy, případný způsob výpočtu škody, který bude v možném nesouladu s názorem ČPU neznamená, že ČPU se nemůže této požadované sumy domáhat v občanskoprávním sporu. Výpočet slouží právu trestnímu, aby bylo možné jednání pachatele subsumovat pod ustanovení některé základní nebo kvalifikované skutkové podstaty TČ. ČPU však chce finance v jí požadované výši, ale s minimem námahy, neboť adhezní řízení je pro ni jednodušším řešením.

3.7.2 Možné způsoby vyčíslení škody

Co odmítl rozhodnout NS, se nyní, alespoň zhruba, pokusíme v této kapitole stanovit. Tedy nějaké možné kriterium pro výpočet výše škody, kterým bychom mohli jednání jednoznačně klasifikovat. Z tohoto nastínění se poté v sedmé kapitole pokusíme vymezit případné nové znění ustanovení § 270 TZ, jehož objektem bude i nadále právo duševního vlastnictví.

Autor předestírá, že se jedná pouze a jeho návrh, se kterým jistě může mnoho čtenářů nesouhlasit, přesto se domnívá, že i nedokonalé pravidlo je pro danou situaci mnohem lepší, než nejistota, která nyní panuje. A pokud by případná poškozená strana s tímto nesouhlasila, má možnost se obrátit v civilním řízení na soud se zbytkem svého nároku způsobené škody. Je přece možnost stanovit pravidlo a to postupem času a za užití nových poznatků pozměňovat.

Problém porušování autorských práv se dnes krom hudby, filmu a počítačových programů týká ve velkém i knih a to jak v podobě nafocené či naskenované, nebo

[184] Soud se zastal internetového piráta, který měl platit vysokou škodu. *E15.cz* [online]. 2015 [cit. 2016-03-24]. Dostupné z: http://e-svet.e15.cz/it-byznys/soud-se-zastal-internetoveho-pirata-ktery-mel-platit-vysokou-skodu

rovnou v podobě tzv. e-knihy, nicméně vzhledem k tématu této práce se zaměříme pouze na hudbu, film a počítačové programy.

Vhodné subsumování nežádoucího jednání pod ustanovení skutkové podstaty trestného činu souvisejícího s právem autorským, by dle mínění autora, bylo možné ve třech různých případech:

1. **výše škody by byla určena soudním znalcem**
2. **výše škody by byla určena dle daných kritérií:** a) podkladem je cena licence
   b) fixně stanovený výpočet
3. **výše škody není pro právní kvalifikaci nutná** – skutková podstata ji nevyžaduje,

přičemž pouze ve dvou z těchto případů by bylo nutné stanovení výše způsobené škody daným nezákonným jednáním. Ve třetím případě by ustanovení skutkové podstaty výši škody nevyžadovalo.

Ad 1 **Výši škody určí soudní znalec**

Skutková podstata trestného činu by jako doposud vycházela ze způsobené škody, kterou by stanovil soudní znalec z oboru ekonomika, odvětví ceny a odhady, specializace oceňování duševního vlastnictví. Zároveň by zohledňoval stáří díla a aktuální situaci na trhu. Více o možném zohledňování v podkapitole 5.4 věnované znalcům.

Tento systém určení by nejvěrněji a nepřesněji určil cenu díla a tím pádem i škodu. Proti tomuto posudku by poškození neměli mít námitek a v rámci adhezního řízení by jim mohla být přiznávána znalcem určená výše škody. Nicméně případné bezdůvodné obohacení by stejně museli žalovat u soudu civilního. Upravené znění trestního zákoníku související s tímto způsobem výpočtu si přiblížíme v podkapitole 7.2 věnované vlastním návrhům autora spjatým s touto problematikou.

Je však nutné zmínit, že ačkoli by stanovená výše škody soudním znalcem nejvíce odpovídala skutečnosti, byl by tento systém v případě rozsáhlého pirátství nejenom značně zdlouhavý (možná až nemožný), ale hlavně velmi nákladný. A jelikož náklady na znalce hradí stát (potažmo složky státu, které si o znalecký posudek požádaly), nutně by znamenaly navýšení prostředků daných složek, které znalci faktury proplácí. Z tohoto důvodu by autor tento systém nepreferoval.

Ad 3 **Výše škody není pro právní kvalifikaci nutná**

Tento způsob klasifikace nežádoucího jednání by nebyl založen na výši způsobené škody, ale na rozsahu, v jakém k nežádoucímu jednání došlo. Tj. stát by přesně definoval nezákonný zásah, kolik počítačových programů, zvukových nebo zvukově obrazových děl, nebo jejich kombinací, by znamenalo naplnění skutkové podstaty, která by musela mít jiné znění, než doposud. Toto znění a případné návrhy, kolik jakých děl by znamenalo naplnění skutkové podstaty, si opět představíme v podkapitole 7.2.

Tento systém by z hlediska právní kvalifikace byl naprosto jasný (pokud by byla stanovená pravidla počtu děl), čímž by jednak znamenal naprostou právní jistotu a také úsporu oproti využití systému se soudním znalcem. Nicméně by se daly očekávat nesouhlasné návrhy ze strany poškozených a jejich zástupců. Tento systém by výši škody nevyčísloval a tak by ani nebylo možné v rámci adhezního řízení přiznat poškozeným finanční náhradu. Veškeré nároky by museli uplatnit před soudem v civilním řízení. Navrhovaný systém by sloužil jen pro řízení trestní.

Ad 2 písm. a) **Výše škody by byla určena dle přesně stanovených kritérií, s přihlédnutím k ceně případné licence k dílu**

V první řadě je nutné rozdělení na 2 kategorie. Na SW a audio a audiovizuální díla, neboť sdílení či kopírování SW nutně přináší jiný systém výpočtu, zejména díky vyšší ceně SW. U SW je tak nutné zohlednit počet jeho stažení nebo prodaných nosičů, zatímco u filmů atd. toto nutné není. V takovém případě by počet stažení nebyl pro stanovení výše podstatný (vyjma camcordingu, kde by toto zohlednění nutné bylo).

I. Zaměříme se na výpočet výše škody způsobené šířením SW. Základem ceny je hodnota licence předmětného programu. Jak získat tuto hodnotu si ukážeme hned v další části u bodu 2 b). Dalším určujícím faktorem by bylo počet stažení z filehostingu a prostřednictvím P2P sítě. Počet stažení lze v případě sledování subjektu či při jiném vyšetřování zjistit. Chybovost při získávání dat z filehostingu se rovná 3 – 5% z celkového počtu započatých procesů stahování. Je dána možnou chybou serveru, připojení uživatele či jiným problémem. U P2P sítě je chybovost, díky sdílení po částech a ne vždy od jednoho uživatele, cca 15%. K úplnému stažení tak u filehostingu dojde v přibližně 95% případů, u P2P je to cca 85%. Pokud bychom zhruba stanovili průměrnou chybovost, bude desetiprocentní, čili v 9 z 10 případů dojde k úplnému

stažení dat. Posledním krokem by bylo stanovení koeficientu tržní ceny programu. Nelze použít fixní cenu, neboť SW se cenově značně odlišují. Na rozdíl od filmů, kde by přibližně mohla být stanovena. Při tomto typu výpočtu autor koeficient navrhuje na jednu třetinu, neboť by mohl zohlednit prostředí trhu. Vysvětleno níže. Tímto bychom měli stanovena jistá kritéria, ze kterých by šla výše škody určit, a proto autor práce navrhuje tento výpočet

$$\mathbf{Š_{SW} = P_S \times K_{CH} \times PrC_{LSW} \times K_L}$$

kde $Š_{SW}$ bude výše škody u SW deliktů, P_S bude počet zjištěných stažení či sdílení daného díla, K_{CH} je koeficient akceptující chybovost, v tomto případě 0,9, jak jsme si vysvětlili, PrC_{LSW} je prodejní cena licence v době nasdílení díla (zjištěná dle návodu níže) a konečně K_L je koeficient zahrnující vliv trhu, tedy jedna třetina, po dosazení koeficientů dostaneme vzorec pro výši škody

$$\mathbf{Š_{SW}} = P_S \times 0{,}9 \times PrC_{LSW} \times \frac{1}{3} = \mathbf{P_S \times PrC_{LSW} \times 0{,}3}$$

II. V případě výše škody u filmu či hudby bychom vycházeli z ceny licence pro toto dílo, ale z licence k půjčování děl na internetu nikoli z licence pro koncového uživatele. Např. cena filmu na DVD je pro názornost 300 Kč. Avšak ten samý film na DVD pro možnost půjčení je 1500 Kč. Tato cena je vyšší a zohledňuje případný možný profit půjčovatele. Neurčuje pro něj však cenu za půjčení ani rozmezí, na jak dlouho dílo zapůjčí. Na internetové sdílení bychom poté mohli nahlížet jako na on-line zapůjčení díla, avšak bez protiplnění - tedy bez platby pro osobu, která dílo nasdílela. A nikomu nemůžeme určovat, za kolik musí půjčovat. Když někdo koupí licenci k filmu a poté jej dobrovolně zdarma poskytuje, je to jeho volba. Výše škody by byla dána výpočtem

$$\mathbf{Š_{AAV} = P_D \times PrC_{LAAV}}$$

kde $Š_{AAV}$ bude výše škody při sdílení audio a audiovizuálního díla, P_D bude počet zjištěných nelegálně poskytnutých děl – na internetu či prostřednictvím nosiče (v případě jednoho filmu pak bude $P_D = 1$), PrC_{LAAV} je prodejní cena licence pro půjčování v době nasdílení díla, zjistitelná z ceníků či přímo od nositele autorských práv.

Jediným problémem zůstává šíření děl získaných camcordingem, kde výši škody určíme dle níže uvedeného pravidla.

Samozřejmě pokud pachatel porušuje autorská práva k počítačovým programům i k audio a audiovizuálnímu dílu, je celková výše škody dána součtem škod dílčích pro každou kategorii, tedy **Š = $Š_{SW}$ + $Š_{AAV}$ +** (případná škoda za camcording)**.** Tento model dle autora má již jisté prvky přesnosti, což je výhodou. Také se vyčísluje škoda, kterou lze přiznat poškozeným. I v tomto případě je však mnoho faktorů, které je nutné zjišťovat, proto by ani jej autor nezvolil jako nejvhodnější.

Ad 2 písm. b) **Výše škody by byla určena dle přesně stanovených kritérií, tj. byly by fixně stanoveny způsoby výpočtu**

Rovněž v této situaci je nutné rozdělení způsobů výpočtu výše škody pro SW a audio a audiovizuální díla.

I. I zde se nejdříve zaměříme na výpočet výše škody způsobené šířením SW. Základem ceny je opět hodnota licence v době nasdílení. Tu bychom mohli zjistit z internetových serverů, které sledují statistiky prodejních cen (např. heureka.cz, zbozi.cz atd.). Tyto servery dokáží ve svých statistikách archivovat a zobrazovat ceny až 5 let zpět. Přičemž zobrazují ceny minimální, maximální a průměrné. Vycházeli bychom z cen průměrných ke dni nasdílení a to na základě dat minimálně ze dvou serverů. Měli bychom tedy dvě průměrné hodnoty licence, ze kterých bychom stanovili aritmetický průměr, jež by představoval cenu PrC_{LSW}**.** Nebo by byl ustanoven úřad, např. ČSÚ, který by ceny monitoroval (což možná určitým způsobem dělá) a jako základ by sloužila jím sdělená cena licence. Také koeficient tržní hodnoty SW by v tomto případě autor navrhoval hodnotu 0,2. A to na základě zkušeností autora, které budou zmíněny a komentovány v části podkapitoly 6.3.2.

Z uvedeného autor navrhuje vzorec pro výpočet škody i SW na

$$Š_{SW} = P_S \times K_{CH} \times PrC_{LSW} \times K_L$$

kde $Š_{SW}$ bude výše škody u SW deliktů, P_S bude počet zjištěných stažení či sdílení daného díla, K_{CH} je koeficient akceptující chybovost, v tomto případě 0,9, jak jsme si vysvětlili v předchozí části, PrC_{LSW} je prodejní cena licence v době nasdílení díla dle uvedeného návodu a konečně K_L je koeficient zahrnující vliv trhu, pro tuto část je koeficient 0,2. Po dosazení koeficientů dostaneme vzorec pro výši škody

$$\mathbf{Š_{SW} = P_S \times 0{,}9 \times PrC_{LSW} \times 0{,}2 = P_S \times PrC_{LSW} \times 0{,}18}.$$

II. V případě výše škody u filmu či hudby bychom vycházeli z ceny pevně stanovené. Přičemž cena by jistým způsobem zohledňovala vývoj, tj. jiná cena filmu je v době promítání v kině, jiná pokud je dostupný na DVD a jiná po odvysílání v TV. Vycházelo by se z počtu stažení, opět zohledněného koeficientem. V případě filmů se tyto navíc šíří framingem či skrze embedded linky. Jejich chybovost je cca 10%, jež zohledňuje chyby, ale i případné nedokoukání filmu a jeho nové spuštění, sice jen od části doposud nezhlédnuté. Ačkoli jde vlastně o zhlédnutí jedno, dojde tímto způsobem k navýšení počtu zhlédnutí. Díky tomu může zůstat koeficient chybovosti na hodnotě 0,9. Z výše uvedeného důvodu by autor práce navrhoval následující výpočet pro výši škody

$$\mathbf{Š_{AAV} = P_S \times K_{CH} \times C_D}$$

kde $Š_{AAV}$ bude výše škody při sdílení audio a audiovizuálního díla, P_S bude počet zjištěných stažení či sdílení daného díla – na internetu či prostřednictvím nosiče, K_{CH} je koeficient akceptující chybovost, v tomto případě 0,9, jak jsme si vysvětlili, C_D je pevně stanovená cena díla. Pro sdílení camcordingu, tedy odcizeného snímku z kina bude $\mathbf{C_D = 10}$. Pro díla, jež jsou dostupná na DVD, v on-line půjčovně, či jiné formě, kterou určí distributor, tedy po skončení promítání v kinech, bude $\mathbf{C_D = 0{,}5}$, po odvysílání na volně dostupné televizní stanici se koeficient změní $\mathbf{C_D = 0{,}05}$, a pro jednotlivé songy (jeden MP3 soubor) bude $\mathbf{C_D = 0{,}01}$. Pokud by došlo k nasdílení celého alba, tedy celé hudební CD či DVD, pak $\mathbf{C_D = 0{,}5}$, což je stejné jako v případě běžného filmu. Koeficienty stanovují ke všem dílům *de facto* shodné ceny, s čímž by někdo mohl nesouhlasit, ale v kině je také cena lístku jednotná, DVD stojí obdobně a ceny v on-line půjčovnách jsou také shodné, proto je toto stanovení, dle autora, možné. K určení koeficientu C_D je rozhodná doba nasdílení. Po dosazení do vzorce dostaneme výpočet výše škody:

Camcording	$\mathbf{Š_{CAM} = P_S \times 0{,}9 \times 10 = P_S \times 9}$
DVD díla	$\mathbf{Š_{DVD} = P_S \times 0{,}9 \times 0{,}5 = P_S \times 0{,}45}$
TVdíla	$\mathbf{Š_{TV} = P_S \times 0{,}9 \times 0{,}05 = P_S \times 0{,}045}$
Songy	$\mathbf{Š_{MP3} = P_S \times 0{,}9 \times 0{,}01 = P_S \times 0{,}009}$
Alba	$\mathbf{Š_{Alba} = P_S \times 0{,}9 \times 0{,}5 = P_S \times 0{,}45}$

Celková výše škody pak bude dána součtem dílčích škod. Autor samozřejmě chápe, že ne každý s tímto bude souhlasit, on však tento systém považuje za nejvhodnější ze všech jím představených a navrhoval by jeho zavedení do praxe.

Škoda je zcela jasně spočítatelná, tím pádem je možné v rámci adhezního řízení vydat rozsudek ve prospěch poškozeného na náhradu v této výši. Posudek znalce není potřebný, ušetří se náklady a čas. Odpadají debaty o nevhodně stanovené výši škody, neboť pravidla jsou jasně dána, což přináší další úsporu času. A v neposlední řadě, výpočet je tak snadný, že jej zvládne každý.

Jen doplníme, že výsledný výpočet ve všech případech je hodnota stanovená v čekcýh korunách.

4 Případy „pirátství“ nejen v ČR

V této kapitole si představíme některé zajímavé kauzy, které s pirátstvím souvisí a staly se známými díky medializaci, nebo je s nimi autor obeznámen a domnívá se, že by svou zajímavostí a případným dopadem uvedeny být měly.

4.1 Kuky se vrací

Známá kauza, jež se týkala filmu Jana Svěráka, Kuky se vrací a jeho zpřístupnění na filehostingovém serveru www.share-rapid.cz, přinesla zajímavé rozhodnutí, které bylo v mnoha médiích označováno jako průlomové. „Svěrák porazil piráty“[185], „Svěrák a "Kuky" u soudu: Server bude tvrdě platit za porušení autorských práv“[186] či „Jan Svěrák má dostat půl milionu za nelegální stahování Kukyho“[187] jsou názvy některých článků v českých médiích, které se snaží vzbudit dojem, že situace je zcela jasná a piráti byli navždy poraženi.

Ve všech článcích chybí to nejpodstatnější, nikde není uvedeno, proč Jan Svěrák vyhrál, také že nešlo o řízení trestní, ale civilní. V dané kauze byli žalováni provozovatel daného portálu a osoba, jež měla registrovanou příslušnou doménu. Rozsudkem byli zavázáni k vydání bezdůvodného obohacení celkem ve výši 535.880,-Kč.[188] Nicméně se jednalo o rozsudek pro uznání, jenž byl vydán na základě fikce uznání nároku žalovanými. A nešlo o průlomový rozsudek na základě speciálního zákona, který Jan Svěrák objevil, jak bylo na webových stránkách uvedeno – „*Svěrák však našel zákon, který říká, že pokud se provozovatel o nelegálním obsahu dozví, musí jej odstranit*“.[189] Nejedná se však o zvláštní zákon, ale o zákon o některých službách informační společnosti, který jsme již rozebírali a to včetně daného ustanovení, jež provozovatele zavazuje k odstranění nelegálního obsahu, pokud se o něm dozví.

---

[185] více na stránkách – http://objevit.cz/sverak-porazil-piraty-t29809

[186] více na stránkách – http://kultura.eurozpravy.cz/film-a-tv/72939-sverak-a-kuky-u-soudu-server-bude-tvrde-platit-za-poruseni-autorskych-prav/

[187] více na stránkách – http://www.lidovky.cz/hn-sverak-ma-dostat-odskodneni-za-nelegalni-stahovani-kukyho-p5v-/zpravy-domov.aspx?c=A130702_081150_ln_domov_tep

[188] více na stránkách – http://blog.eisionline.org/2013/09/01/rozhodnutia-prazskych-sudov-vo-veci-share-rapid-cz/

[189] Svěrák porazil piráty. *Objevit.cz* [online]. 2013 [cit. 2016-03-24]. Dostupné z: http://objevit.cz/sverak-porazil-piraty-t29809

Rozsudkem bylo žalobě v plném rozsahu vyhověno, aniž by soud posuzoval nárok žalobce z pohledu hmotného práva. Chybí tak právní názor soudu, kterým by bylo v dalších podobných případech možné výši bezdůvodného obohacení vyčíslit. Pro provozovatele serveru bylo zřejmě jednodušší zaplatit, než se dále soudit. Dá se předpokládat, že na filmu vydělali více, proto nárok žalující strany nerozporovali. Nicméně autor je přesvědčen, že jinak by prokázání nároku pro Jana Svěráka nebylo tak snadné. Samozřejmě také záleží na faktu, kdy a jak byl server o nelegálním obsahu informován a kdy dílo odstranil. Pokud by tak totiž učinil neprodleně po upozornění, nebylo by možné dovodit jeho odpovědnost a žalovat je. Toto potvrzuje i výrok tehdejšího advokáta a dnešního ministra spravedlnosti: „*Ten verdikt není průlomový. Jednak jsme se nedozvěděli žádné odůvodnění, žalovaný se nebránil. I kdyby se ale někdo bránil, neučí nás to nic nového. Nešlo tam o samotný problém vyvěšení filmu na web.*“

4.2 Vratné lahve

Dalším filmem z produkce syna a otce Svěrákových, který se objevil na internetu ještě dříve, než byla zahájena jeho oficiální distribuce na příslušném nosiči, byl film Vratné lahve.[190] Na této kauze je zajímavé, že unikl DV disk, který byl jako jediný zapůjčen Ministerstvu kultury ČR. Při sledování tohoto disku byl několikráte vidět vodoznak – „*Pouze pro potřeby MK ČR, nekopírovat*“.

V tomto případě se již jednalo o kauzu trestní, bohužel k soudnímu projednání, které by mohlo dát nějaký návod na výpočet výše škody u „nových“ filmů nedošlo. Dle internetových zpráv[191] se dá předpokládat, že bylo využito ustanovení § 307 odst. 1 TŘ, které umožňuje podmíněné zastavení trestního stíhání.

4.3 „Nerez“ a jeho „TVORBA“

Další kauzou, se způsobenou škodou v astronomické výši, alespoň podle ČPU,

[190] více na webových stránkách – http://www.novinky.cz/krimi/122681-muz-obvinen-za-unik-filmu-vratne-lahve-na-internet.html nebo http://kultura.zpravy.idnes.cz/unikla-kopie-vratnych-lahvi-s-puncem-ministerstva-fw5-/filmvideo.aspx?c=A070719_102010_filmvideo_kot

[191] „Bylo rozhodnuto o podmíněném zastavení trestního stíhání. Usnesení nabylo právní moci 11. července. Zkušební doba byla u obou obviněných stanovena na 18 měsíců, řekla mluvčí Obvodního soudu pro Prahu 5 Vanda Činková“ a „S jedním z nich došlo k uzavření dohody o náhradě škody“ – citováno z webové stránky http://art.ihned.cz/c1-26062070-stihani-piratu-kteri-sirili-film-vratne-lahve-bylo-pozastaveno dne 24.3.2016.

byl případ moderátora warezového fóra warcenter.cz, jenž používal přezdívku „Nerez“. Tento uživatel působil se stejným nickem i na konkurenčním, v práci již zmiňovaném, fóru warforum.cz, zde pouze jako řadový člen. V obou případech však dával k dispozici odkazy na audiovizuální díla, která sám na filehostingy nahrával. Veškeré jeho nahrávky byly snadno identifikovatelné, neboť užíval v názvu díla svou přezdívku, tedy např. XYZ_Nerez.avi.

Podle obžaloby zpřístupnil během 4,5 let na internetu 2 066 audiovizuálních děl[192], což díky zdvojování a ztrojování činilo přes 14 tisíc nelegálních kopií audiovizuálních děl – filmů a epizod seriálů.[193] Okresní soud ve Zlíně jej uznal vinným z porušení autorského práva, práv souvisejících s právem autorským a práv databázi, za což mu uložil trest odnětí svobody ve výměře 18 měsíců s podmíněným odkladem výkonu trestu na zkušební dobu v trvání 3 let a trest propadnutí věci. ČPU vyčíslila škodu na více než 80 milionů Kč, nicméně zlínský soud ČPU odkázal s nárokem na náhradu škody na občanskoprávní řízení. Je tedy zřejmé, že výši škody vyčíslovala standardně, počet stažení násobeno cenou díla na trhu. Je proto dobře, že samosoudce škodu posoudil jako nepřiměřenou a odkázal poškozené na civilní řízení. Další důkaz vhodnosti jakéhokoli pravidla pro stanovení výpočtu výše škody.

4.4 Případ náhradního plnění za způsobenou škodu

Zajímavým případem z přelomu roku 2015/2016 byla kauza skladníka, který na internetu sdílel převážně počítačové programy a hry, ale neopomněl ani filmy a hudbu, i když ne v takové míře. Pozoruhodné na celém bylo dohodnutí prvního alternativního trestu za toto nelegální šíření hudby, filmů a programů.

I zde byla vyčíslena škoda v ohromné výši cca 9 milionů[194] korun, nicméně zástupci poškozených společností byli odkázáni s nárokem k civilnímu soudu, neboť soud výpočet škody opět neakceptoval. „*Přesto právníci BSA Froňkovi nadále*

[192] Počítačový pirát Nerez nabízel ke stažení tisíce filmů, dostal podmínku. *Idnes.cz* [online]. 2012 [cit. 2016-03-24]. Dostupné z: http://zpravy.idnes.cz/soud-s-pocitacovym-piratem-miroslavem-ocelikem-f5v-/krimi.aspx?c=A120523_162415_zlin-zpravy_sot

[193] Nad piráty se i v Čechách stahují mračna: Moderátor Nerez byl za nelegální uploady odsouzen. *Kinobox.cz* [online]. 2012 [cit. 2016-03-24]. Dostupné z: http://www.kinobox.cz/clanek/7059-moderator-nerez-odsouzen

[194] POČÍTAČOVÝ PIRÁT UŽ SI TREST ODPRACOVAL. KAJÍCNÉ VIDEO VIDĚL MILION LIDÍ. *Respekt.cz*[online]. 2015 [cit. 2016-03-24]. Dostupné z: http://www.respekt.cz/spolecnost/pocitacovy-pirat-uz-si-trest-odpracoval-kajicne-video-videl-milion-lidi

vyhrožovali soudem o pět a půl milionu, na třímilionovém vyrovnání trvala i ČPU. „Živím se jako skladník, to jsem v životě nemohl zaplatit," říká Froněk. Firmám rozeslal omluvné dopisy a návrh, že místo pokuty natočí protipirátské video. ČPU trvala na finanční odplatě a vymohla si nakonec čtvrt milionu, který si Froněk půjčil v bance, ale BSA se spokojila s 60 tisíci – a zmiňovaným spotem. Ovšem pod podmínkou, že video získá nejméně 200 tisíc zhlédnutí." [195] Odsouzený natočil tříminutový snímek popisující útrapy způsobené návštěvou policie, výslechů a soudních obsílek a umístil jej na server YouTube.com s prosbou o sdílení videa, neboť potřebuje 200.000 zhlédnutí, aby nemusel hradit škodu v řádu milionů. Taktéž založil webovou stránku http://www.mojepiratstvi.cz/, kterou nazval příznačně „*Stahuji (pirátskou vlajku) a sdílím (svůj příběh)*". Video se stalo hitem a během 14 dní jej vidělo více než milion uživatelů, čímž došlo ke splnění podmínky a škoda tím pádem byla uhrazena.

Objevily se sice i názory, že je celé video a kauza je podvod (fake), které nastrojily společnosti zastupující autory, avšak to nic nemění na faktu, že se tento případ stal zajímavým milníkem v oblasti náhrady za stanovenou škodu.

4.5 Embedded linky v praxi

V této podkapitole si přiblížíme kauzu, která doposud není veřejná, neboť zatím ani není soudně projednávána [196] (jak autor v úvodu zmínil). Tato kauza se týká webových stránek http://sledujufilmy.cz/, kde bylo a bohužel stále ještě je možné nalézt nepřeberné množství filmů a seriálů. Pro sdílení je zjevně využívána technologie embedded linků a framingu, kterémuž problému jsme již jednu podkapitolu věnovali.

---

[195] POČÍTAČOVÝ PIRÁT UŽ SI TREST ODPRACOVAL. KAJÍCNÉ VIDEO VIDĚL MILION LIDÍ. *Respekt.cz*[online]. 2015 [cit. 2016-03-24]. Dostupné z: http://www.respekt.cz/spolecnost/pocitacovy-pirat-uz-si-trest-odpracoval-kajicne-video-videl-milion-lidi

[196] poznámka autora: Ještě v den uzavření práce navštívil autor OSZ P3, kde se dotázal na základě zákona o svobodném přístupu k informacím, zda bude brzy nařízeno hlavní líčení, neboť dle prvotních informací již toto projednáváno být mělo. Bohužel došlo ke zpoždění a ke dni uzavření této práce je většina informací stále neveřejná. Z tohoto důvodu musel autor práce na poslední chvíli tuto podkapitolu, která měla více než 3 stránky, zcela přepracovat. Ačkoli byly použity pouze údaje, jež u soudu stejně veřejně zazní, doposud podléhají utajení a není možné je použít. Podkapitola tak bude podložena veřejně dostupnými informacemi, avšak v budoucnu autor tuto pasáž jistě uveřejní.

Autor práce si nemůže odpustit ještě jeden komentář, že pokud dojde ke zprošťujícímu rozsudku s odkazem na zmiňovaný případ Svensson, nejenom že s tímto nebude právně souhlasit, ale zřejmě zváží, že si obdobnou stránku pracující na tomto principu co nejdříve založí, neboť dle níže uvedených možných příjmů z reklamy to bude finančně výnosnější, než jakákoli „běžná" práce byť i dobrého právníka.

Dle informací uvedených v kontaktech na této stránce (http://sledujufilmy.cz/kontakt/) je zřejmé, že zakladatelem a vlastníkem webové stránky je právnická osoba, ovšem nikoli česká, ale anglická, se sídlem v Londýně. Z anglického obchodního rejstříku (http://wck2.companieshouse.gov.uk/ je možné dohledat, že zakladatelem této právnické osoby je osoba zřejmě české národnosti. Lze tak usuzovat dle jména a také jejího českého telefonního čísla, které ještě začátkem března 2016 bylo volně k dispozici u kontaktů na webové stránce. Z rejstříku je zjistitelné, že firma byla založena pouze s minimálním základním kapitálem £100. Vše ukazuje na účelové jednání s účelem ztížit dopadení případného pachatele.

Na předmětných stránkách je značné množství reklamy, která je také přítomna ještě před spuštěním požadovaného filmu, což zřejmě přináší provozovateli stránek nemalý finanční profit. V měsících lednu až březnu 2016 dominovaly bannery firmy Seznam.cz. Dle ceníku této firmy, kolik vyplácí za uveřejňování svých bannerů na cizích webových stránkách v závislosti na počtu návštěvnosti stránek, je možné odhadnout, kolik peněz je měsíčně provozovateli stránek vypláceno. Dle hrubého výpočtu autora práce, na základě dostupných informací o návštěvnosti předmětných stránek a ceníku firmy Seznam.cz, by se mohlo jednat o částku v rozmezí 250.000,-Kč až 300.000,-Kč za každý jeden měsíc provozování stránek.

Zda i v tomto případě bude u soudu použita obhajoba odkazující na námi probíranou kauzu SDEU ve věci C-466/12 – Svensson, která jak víme, byla SDEU posouzena jako oprávněné odkazování na již dostupná díla na internetu, ukáže až čas. Nicméně autor se domnívá, že vzhledem k tomu, že se tomu tak poslední dobou v obdobných případech děje s naprostou pravidelností, což jsme si již přiblížili, bude i zde tohoto způsobu obhajoby využito.

Kauza je zajímavá i z hlediska, že zřejmě bude stíhána jak FO, tak i PO. Bohužel rozhodnuto ve věci zatím není a už vůbec není zřejmé, jak soudy dané jednání posoudí. Na závěr celé kauzy si tedy budeme muset ještě počkat.

4.6 Nepodmíněný trest za prodej nelegálního SW

I v případě nezákonného nakládání s počítačovými programy již došlo na soudní rozhodnutí. Proto si i tuto skutečnou kauzu uvedeme. Je zajímavá i z pohledu rozsudku, neboť poprvé došlo na odsouzení k nepodmíněnému trestu odnětí svobody. Doposud jak za sdílení SW, tak i za sdílení filmů padaly pouze tresty s podmíněným odkladem, což

poměrně často kritizovala ředitelka ČPU, které vadí nejenom výpočet výše škody, ale i mírné tresty. Nejraději by viděla všechny odsouzené minimálně na 5 let ve vězení.

Softwarový pirát z Mostecka byl odsouzen na 20 měsíců do vězení kvůli prodeji nelegálních kopií softwaru od Microsoftu a Adobe. Pirát programy opakovaně nabízel a inzeroval na internetových inzertních portálech a od podvedených kupujících vybral přes 89 tisíc korun. Výrobcům tímto jednáním však způsobil škodu přesahující půl milionu korun, kterou musí uhradit. Své kupující lákal na podezřele nízkou cenu a nelegální kopie vydával za použitý software z druhé ruky. Peníze inkasoval bezhotovostním převodem nebo na dobírku.[197]

Dalšími případy, kdy se soudy zabývají nelegálním softwarem, bývají případy firem, které buďto nemají legální SW vůbec, nebo překročí počet licencí. O takovýchto případech jsou orgány nejčastěji informovány od bývalých, většinou propuštěných zaměstnanců, jež na toto upozorňují zejména z pomsty za dané propuštění.

4.7 Nelegální sdílení filmů s jejich rozsudky

Příkladem odsouzeného piráta z kina, tzv. camcordingu, byl únik filmu „Rafťáci“, natočeného v kině Cinema City Flora. A jelikož byl skutkový stav sdílení spolehlivě prokázán opatřenými důkazy, bylo rozhodnutí vydáno, bez projednání věci v hlavním líčení, trestním příkazem, který si je možné přečíst v příloze č. 2.

I za sdílení hudby a filmů prostřednictvím P2P sítí je možné být trestním příkazem odsouzen. V příloze č. 3 je možné si danou kauzu přečíst.

Do třetice byl trestným příkazem odsouzen pirát za sdílení převážně her pro zařízení Play Station. Opět podmíněně, avšak zároveň s peněžitým trestem. Trestní příkaz s popisem skutku je možné nalézt v příloze č. 4.

4.8 Únik filmu před premiérou v DVD kvalitě

Pirátství se projevuje skutečně po celém světě. Únik filmů, dokonce ve vysoké kvalitě DVD, poznamenal letošní udílení cen akademie Oscar v USA. Velmi očekávané a žádané filmy na přelomu roku 2015/2016 zahltily nejen úložné servery, ale i P2P sítě.

Dva z nejočekávanějších filmů roku, Osm hrozných a Zmrtvýchvstání, se ocitly

---

[197] V Česku padl první nepodmíněný trest za softwarové pirátství. *Ceskatelevize.cz* [online]. 2013 [cit. 2016-03-25]. Dostupné z: http://www.ceskatelevize.cz/ct24/domaci/1059807-v-cesku-padl-prvni-nepodmineny-trest-za-softwarove-piratstvi

14 dní před oficiální premiérou v kinech. Okamžitě je sdílelo na internetu více než dva miliony unikátních IP adres. Sdílení se již nepodařilo zabránit, proto jsou tato díla dnes téměř všude a to v té nejlepší kvalitě. Dá se říci, že filmy se kradou běžně, ale tahle masivní dávka vánočních „upirátěných" snímků byla přece jen v něčem unikátní. Problém byl o to větší, že v obou případech bylo zjištěno (díky FBI), odkud snímky unikly. Podle „watermarků" (skrytých značek, o kterých jsme diskutovali v tématu camcordingu) na digitálních kopiích byl únik rychle vystopován do kanceláře vysoce postaveného člověka z filmové společnosti Alcon Entertainment, do které dorazily ve formě oscarových „screeners" – tedy kopií, které jsou rozesílány masivní porotě Filmové akademie k ohodnocení, aby filmy mohly být do soutěže o zlatou sošku zařazeny. Škoda, která tímto únikem vznikla, je zřejmě jen stěží vyčíslitelná, neboť oba filmy patří mezi tzv. kasovní trháky a návštěvnost kin je v takovýchto případech enormní. Únik v maximální kvalitě je proto pro distribuční společnosti katastrofou.[198]

[198] Pirátské vánoce: Na internet unikla bezprecedentní halda filmů včetně Osmi hrozných od Tarantina. *Reflex.cz* [online]. 2015 [cit. 2016-03-25]. Dostupné z: http://www.reflex.cz/clanek/kultura/68238/piratske-vanoce-na-internet-unikla-bezprecedentni-halda-filmu-vcetne-osmi-hroznych-od-tarantina.html

5 Odhalování a vyšetřování kyberkriminality

Již ve třetí kapitole jsme uvedli několikeré důvody, jež motivují lidi, aby se dopouštěli protiprávního jednání. Pokusíme se tuto kapitolu věnovat postupům a metodám, jež mohou napomoci odhalování a vyšetřování kybernetické kriminality. Je však nutné si uvědomit, že již tolikrát zmiňovaná anonymita, bezhraničnost a tím pádem i možná neuvěřitelná vzdálenost překonatelná prostřednictvím internetu, veškeré kroky vedoucí k okrytí možného zločinu a dopadení pachatele, značně ztěžují.

Z toho důvodu se těmito trestnými činy zabývá zvláštní část kriminalistiky.[199] Po dlouhodobém zkoumání nových trestných činů, způsobu jejich páchání, obzvláště jejich značné variabilitě, pachatelů a jejich obětí, vznikly zásluhou kriminalistické vědy nové metody a postupy, díky nimž je možné úspěšněji odhalovat nové trestné činy, kterými kyberzločiny jistě jsou. Je nutné si však uvědomit, že právě v této oblasti, tj. kyberprostoru, budou mít zločinci před OČTŘ značný náskok, tedy minimálně v blízké budoucnosti. Nicméně tato smutná skutečnost nesmí boj proti nim ovlivnit a úsilí pro potírání této nezákonné činnosti nesmí polevit.

5.1 Pachatelé a motivy

Jedním ze znaků, které charakterizují skutkovou podstatu trestného činu, je subjekt trestného činu, tj. pachatel. Na pachatele je možno nahlížet v užším významovém pojetí, pak je pachatelem ten, kdo sám naplnil všechny typové znaky skutkové podstaty trestného činu nebo se o trestný čin pokusil či trestný čin připravoval za předpokladu, že je tato příprava trestná (§ 22 odst. 1 TZ), a též nepřímý pachatel. V širším významu je pachatelem, vedle pachatele v užším slova smyslu, též spolupachatel, organizátor, návodce a pomocník, nicméně tuto formu pachatelství jsme již zmiňovali. Při vyšetřování počítačové kriminality je naprosto nezbytné, aby se OČTŘ zabývaly problematikou pachatele trestného činu, a to samozřejmě z pohledu trestního práva, ale i z pohledu kriminalistické psychologie. V případě pachatele počítačového trestného činu bude totiž v praxi docházet k tomu, že pachatelem budou mnohdy osoby mladistvé a v blízké budoucnosti, díky masivnímu rozvoji počítačů v mnohé podobě a jejich

[199] GŘIVNA, Tomáš a Radim POLČÁK (eds.). *Kyberkriminalita a právo*. Vyd. 1. Praha: Auditorium, 2008, 220 s. ISBN 978-80-903786-7-4. s. 86

zasahování do lidského života od čím dál útlejšího věku, i osoby mladší patnácti let, díky čemuž jejich trestní odpovědnost nebude dána.[200] Je skutečně nutné se připravit na stav, kdy děti budou nejenom ohroženou skupinou na internetu, ale naopak i těmi, kteří trestnou činnost budou páchat. V souvislosti s osobou pachatele je nutné připomenou, že kyberzločinů se může dopustit i osoba právnická a je tak nutné i s touto variantou v případě vyšetřování počítat.

Ještě před nedávnem byly počítačové delikty považovány za kriminalitu středních a vyšších vrstev či za kriminalitu podivínů a specialistů. Tato kriminalita nebyla považována za originální zločin, nebyla příliš zjevná, nebyla na očích veřejnosti, čímž vzbuzovala dojem menší nebezpečnosti. I dnes platí, že počítačové delikty vyžadují jistou schopnost přizpůsobivosti, odpovídající „know-how" a určitou míru inteligence. Klasifikace pachatelů počítačové kriminality může vycházet jednak z hledisek psychologických, ale také z hledisek kriminologických. Z tohoto pohledu pak rozlišujeme cílevědomé kriminogenní osobnosti nebo příležitostné typy. Příležitostné typy pachatelů však v kyberprostoru zatím převažují. Tito pachatelé využívají dané situace nebo vlastních zkušeností. Často pracují na místech, která vzbuzují respekt i důvěru společnosti. Je možné je dále rozdělit podle určitých detailních charakteristik. Jedná se o pachatele, kteří se zaměřují na dosažení co největšího zisku z páchání trestné činnosti tím, že překonávají překážky ochrany systémů. Hlavní motivací je zvýšení prestiže v kolektivu sobě rovných nebo pocit vlastního uspokojení z utajené trestné činnosti. A pak je skupina pachatelů, kteří pouze využívají příhodných podmínek k uskutečnění trestné činnosti.[201, 202]

Kromě převažující touhy po nějaké formě užitku, nejvíce finančním profitu však existují i jiné motivy, např. získat domnělou převahu nad zaměstnavatelem, pocit beztrestnosti nebo neodhalitelnosti, kompenzovat pocit ukřivděnosti, osobního neuznání, nedostatečného ocenění práce, odstranit pocit vykořisťování nejčastěji od

---

[200] MENDEL, Aleš. *Technická a infrastrukturní počítačová kriminalita* [online]. Brno, 2008 [cit. 2016-03-24]. Dostupné z: https://is.muni.cz/th/328211/pravf_r/rigorozni_prace.pdf. Rigorózní práce. Právnická fakulta Masarykovy univerzity. s. 19-21

[201] MATOUŠKOVÁ, Ingrid. *Aplikovaná forenzní psychologie*. 1. vyd. Praha: Grada, 2013. Psyché (Grada). ISBN 978-80-247-4580-0. s. 159-160

[202] MENDEL, Aleš. *Technická a infrastrukturní počítačová kriminalita* [online]. Brno, 2008 [cit. 2016-03-24]. Dostupné z: https://is.muni.cz/th/328211/pravf_r/rigorozni_prace.pdf. Rigorózní práce. Právnická fakulta Masarykovy univerzity. s. 19-21

zaměstnavatele apod. V neposlední řadě bývá motivem touha po uplatňování rizika nebo dobrodružství. Avšak díky věkové rozmanitosti, je nutné přihlédnout k faktu, že motivy pachatelů se budou měnit především s ohledem právě na jejich věk, osobnostní vyspělost, případně příležitost, daleko méně pak s ohledem na okolnosti spáchání TČ z hlediska technických vědomostí a dovedností pachatele.[203]

Kyberprostor se stává důležitým kriminogenním faktorem. Každý den vznikají a objevují se nové formy počítačové kriminality, nové aspekty osobnosti pachatelů a tak je nezbytné zkoumat jejich účinky z kriminologického i kriminalistického a samozřejmě též právního pohledu.[204]

A právě právní pohled, nebo spíše příslušná legislativa, je dalším specifikem týkajícím se oblasti počítačové kriminality. V posledních cca dvaceti letech se objevilo mnoho nových škodlivých jednání adresovaných proti počítači nebo s počítačem související, z nichž některé jsou natolik společensky závadné, že je nutné na ně reagovat. To je však úkolem pro zákonodárce, jenž musí rozhodnout, která z těchto jednání jsou ještě v mezích zákona, a jaká tuto mez překračují a měla by být tudíž postihnuta normami správního, posléze trestního práva či případně na základě jiných právních předpisů. Jedním z doposud neupravených deliktů je zmiňovaný DoS útok. Najít tak ideální variantu není jednoduché, neboť je obtížné vymezit nežádoucí jednání v právních normách tak, aby byl postih efektivní a účinný. K vyšetřování a odhalování těchto protiprávních jednání samozřejmě nestačí jen jejich vymezení v zákoně, nýbrž je nutné příslušným OČTŘ svěřit pravomoc k tomu, aby mohly počítačovou kriminalitu odhalovat a trestat. I toto je úkol nelehký, neboť na jedné straně existuje zájem na tom, aby byly počítačové delikty řádně odhaleny a efektivně potrestány, na druhé je třeba dbát na to, aby nebylo vyšetřováním neúměrně zasahováno do ústavních a jiných zaručených práv a oprávněných zájmů osob. Příslušné vyšetřovací orgány by měly mít přístup pouze k těm informacím a údajům, jež jsou nezbytně nutné pro vyšetřování.[205]

---

[203] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. Pro praxi. ISBN 978-80-7380-501-2. s. 486

[204] MENDEL, Aleš. *Technická a infrastrukturní počítačová kriminalita* [online]. Brno, 2008 [cit. 2016-03-24]. Dostupné z: https://is.muni.cz/th/328211/pravf_r/rigorozni_prace.pdf. Rigorózní práce. Právnická fakulta Masarykovy univerzity. s. 21

[205] *Počítačová kriminalita* [online]. 40-50 [cit. 2016-03-25]. Dostupné z: https://theses.cz/id/zctjxg/Diplomova__prace_cast_2.pdf. s. 41

5.2 Digitální stopy

Počítačová kriminalita má jisté charakteristické rysy, které ji odlišují od ostatních druhů kriminality. Zjistit totiž počítačové stopy, či spíše stopy digitální po spáchání některé ze zločinů, je často velmi obtížné a k jejich identifikaci i případnému dešifrování je nezbytný kvalitní software a hardware, což bývá mnohdy velmi finančně náročné. Dalším problémem spojeným s těmito stopami je fakt, že stopy mohou mít krátkou životnost a proto je třeba je zajistit ihned pro případ jejich zničení. Škody způsobené počítačovými delikty jsou v mnoha případech těžko zjistitelné a někdy se jen obtížně vyčíslují, což není problémem jen počítačové kriminality a softwarové pirátství, ale duševního vlastnictví obecně.[206]

Je však nutné si uvědomit, že ačkoli je získávání digitálních stop obtížné, není nemožné. Každé technologické zařízení, jež získává, zpracovává, předává nebo uchovává data, zanechává záznamy o své činnosti. Jakmile uživatel navštíví jakoukoli webovou stránku, ihned se zaznamená nejenom IP adresa, odkud přistoupil, ale i OS, který užívá, stejně tak i verze webového prohlížeče a mnoho dalších informací o daném PC ve formě záznamu. Tyto záznamy jsou z kriminalistického hlediska stopami. Jedná se o digitální stopy, které je možné definovat jako jakékoli informace s vypovídající hodnotou, uložené nebo přenášené v digitální podobě. Z jiného pohledu je možné digitální stopu chápat jako fyzikální interpretaci nehmotné informace, zakódované do digitálního formátu. Z hlediska trestního či správního je digitální stopa jakákoli informace, uložená nebo přenášená v binární podobě, jež může být předložena u soudu jako věcný důkaz. Přičemž fyzické a datové objekty se stávají důkazy pouze tehdy, akceptují-li je OČTŘ a podstatná je právě otázka, zdali se stopa nacházela na určitém místě a také zda nebyla od jejího zjištění do ukončení znaleckého zkoumání nikterak modifikována. Proto se z opatrnosti pracuje s duplikátem, tedy přesnou digitální reprodukcí všech vlastností stopy. Jednou ze základních zásad při zajišťování digitálních stop je zachování jejich integrity a postup předpokládající pořízení identických binárních kopií originálů. Tento postup představuje tzv. digitální forenzní analýzu, která je charakterizována tím, že po zajištění pracuje s takovými daty, jež jsou uložena na médiích s dlouhou dobou životnosti, což umožňuje detailní prozkoumání,

[206] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2. s. 251-252

opakování jednotlivých pokusů testování, nebo i dodatečné provedení analytických kroků a v případě potřeby i s odstupem několika let.[207]

Pokud bychom hovořili konkrétně, tak v našem případě nelegálního šíření filmů prostřednictvím webových stránek, by za takovouto stopu mohla být považována uloženina každé jednotlivé webové stránky, kde se tato díla nachází. V případě inzerátu nabízejícího nelegální SW, pak uloženina této stránky s nabídkou. Je totiž pravděpodobné, že takový obsah daných stránek může být velmi rychle změněn. Tyto kopie webových stránek je možné vypálit na CD či DVD a nosič poté bude představovat další typ digitální stopy a ta může sloužit jako případný důkaz v trestním řízení. Však také ČPU tento postup shromažďování důkazů využívá, neboť většinou, jakmile se podezřelý dozví o aktivitách ČPU, které se jej týkají, dojde k okamžité změně jím provozovaných stránek a prokázat původní nelegální činnost by bez této stopy bylo mnohem obtížnější.

5.3 Vyšetřování a dokazování

Vyšetřováním se nazývá úsek od zahájení trestního stíhání do podání obžaloby nebo jiného způsobu vyřízení.[208] V případě počítačových deliktů představuje složitou činnost a je proto vhodné jej svěřit týmu odborníků zabývajícím se informačními technologiemi. Ne vždy OČTŘ takovýmto týmem kompetentních a vzdělaných odborníků disponují, nicméně se dá říci, že situace v této oblasti se rok od roku přece jenom zlepšuje. Pokud chceme vyšetřovat i složitější kyberdelikty, je vhodné, aby i vyšetřující osoby měly potřebné schopnosti a znalosti. Je také žádoucí, aby tyto orgány spolupracovaly s počítačovými experty a odborníky z IT oblasti. Pokud se má počítačové kriminalitě účinně čelit, je vhodné, aby poškozené osoby oznamovaly OČTŘ, že došlo ke spáchání možného trestného činu a poskytly jim náležitou spolupráci.[209] To se ale vždy neděje a proto jedním z charakteristických rysů počítačové kriminality je její vysoká latence. Buďto poškození nechtějí dané nezákonné jednání nahlásit a to z nejrůznějších důvodů, strach, obava o dobré jméno, stud apod., nebo

---

[207] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. Pro praxi. ISBN 978-80-7380-501-2. s. 492-493

[208] tamtéž s. 507

[209] *Počítačová kriminalita* [online]. 40-50 [cit. 2016-03-25]. Dostupné z: https://theses.cz/id/zctjxg/Diplomova__prace_cast_2.pdf. s. 41

poškození ani netuší, že se stali obětí nějakého útoku. A bohužel v této oblasti obzvlášť platí, „kde není žalobce, není ani soudce“. Zejména pro audio a audiovizuální pirátství je situace obtížnější, neboť o nelegálním zásahu do svých práv se autor díla dozví jen v mizivém procentu. Není reálné mít celý obsah internetu pod kontrolou a tak pokud sdílení nebude příliš „drzé“, např. u hodně žádaného díla, kdy se případ sdílení medializuje, autor díla se o porušování svých práv vlastně ani nedozví. Na porušování narazí autor, nebo organizace, které jej zastupují povětšinou náhodou, i když samozřejmě tyto organizace navštěvují warezová fóra a prohledávají obsah filehostingových úložišť, úspěšnost je v řádu procent. Sami uploadeři nebo downloadeři na nelegální obsah upozorňovat zkrátka nebudou.

V případě nelegálního užívání a/nebo distribuce programového vybavení je toto zjištěno obvykle na základě oznámení svědka, nejčastěji současného či bývalého zaměstnance firmy nebo prostřednictvím tzv. kontrolního nákupu.[210]

K úspěšnému vyšetřování je důležité zvolit správný postup. V kriminalistice se správný postup nazývá **metodika vyšetřování**. Metodika má několik fází, kdy každá představuje jiné úkony, jež se musí učinit. Bohužel celý rozbor metodiky vyšetřování internetové a počítačové kriminality by byl značné rozsáhlý a je proto nad rámec této diplomové práce. Proto se jí hlouběji zabývat nebudeme.

Dokazování dle ustanovení § 89 TŘ je vedle rozhodování nejdůležitější procesní činností OČTŘ, neboť umožňuje skutkový základ pro jejich rozhodování a pro další případný postup tak, aby mohl být naplněn účel trestního řízení.[211] Směřuje k prokázání určitých skutečností uvedených v písm. a) – f) odst. 1 § 89 TŘ, o nichž nejsou důvodné pochyby, a to v rozsahu, který je nezbytný pro každé rozhodnutí OČTŘ.

Soud hodnotí důkazy provedené v průběhu soudního řízení dle zásady volného hodnocení důkazů. Za důkaz se považuje vše, co může objasnit skutkový stav, zejména výpověď obviněného, svědků, znalecké posudky (další podkapitola – pro oblast ICT deliktů mají nezastupitelnou roli), materiální důkazy (např. zmiňované digitální stopy) atd.

---

[210] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. Pro praxi. ISBN 978-80-7380-501-2. s. 350

[211] tamtéž s. 507

Existuje několik rozhodnutí soudů, které se vztahují k dokazování a mohly by být *per analogiam* aplikovatelné i na problematiku elektronických dokumentů, resp. pro oblast ICT deliktů. Bohužel tolik prostoru pro jejich rozbor tato práce neposkytuje. Přesto jsou daná rozhodnutí pro případné zájemce v poznámce pod čarou.[212]

5.4 Znalci

Významnou, a v případě internetové a počítačové kriminality zřejmě i nezastupitelnou, úlohu pro opatřování důkazů představují soudní znalci a jejich posudky. Postavení znalců je upraveno v zákoně č. 36/1967 Sb. ze dne 6. dubna 1967 o znalcích a tlumočnících a případně vyhláškou Ministerstva spravedlnosti.

OČTŘ rozhodne o přibrání znalce dle ustanovení § 105 odst. 1 TŘ, je-li k objasnění skutečností důležitých pro trestní řízení třeba odborných znalostí. Pro kriminalitu, jež souvisí s porušováním autorských práv, je téměř nezbytné přibrání znalce, ponejvíce z oboru kybernetika – odvětví výpočetní technika. Bývá výhodné znalce přibrat k účasti na prováděné domovní prohlídce, neboť je schopen přímo na místě konzultovat nebo řešit technické problémy, jež mohou při prohlídce vzniknout. Zdárným příkladem je pořizování identických otisků dat a jejich zálohování, pokud není možné výpočetní techniku zajistit přímo včetně jejího datového obsahu. V rámci trestního řízení je nejpodstatnější působení znalce dáno jeho vlastní znaleckou činností, z níž vyplývá stanovisko v jím zpracovaném znaleckém posudku, kde znalec odpovídá na otázky, které mu zadavatel při zadání položil. Úlohou znalce však není hodnotit důkazy a řešit právní otázky, to je úkolem OČTŘ, k čemuž jim právě znalecké posudky napomáhají. Posudek je zpracováván zpravidla písemně, nicméně v oblasti audiovizuální a softwarové kriminality se znalec nevyhne tomu, aby k posudku připojil vybraná zajištěná data v elektronické podobě na datových médiích, jako je např. zajištění elektronické pošty či obrazových dokumentů, jejichž vytištění na papír by zřejmě způsobilo nepřehlednost. Kromě standardních otázek, které směřují ke zjištění softwarového vybavení počítače, by se měl policejní orgán dožadovat odpovědí, jež by osvětlily zejména, kdo je nositelem autorských práv ke konkrétnímu dílu, kdy byl tento

[212] Nález Ústavního soudu ze dne 20. dubna 2007, sp. zn. III. ÚS 299/06
Rozsudek Nejvyššího soudu ze dne 17. ledna 2001, sp. zn. 8 Tz 287/2000
Usnesení Nejvyššího soudu ze dne 11. dubna 2012, sp. zn. 5 Tdo 275/2012
Usnesení Ústavního soudu ze dne 28. března 2002, sp. zn. IV.ÚS 2/02

produkt do počítače nainstalován či stažen nebo nahrán na webový server. Možná nejdůležitější odpovědí je stanovení hodnoty softwarového vybavení či předmětného audiovizuálního díla, s čímž souvisí stále diskutovaná otázka v řízeních před soudem. A to že hodnotu u softwarového produktu a s tím spojená odborná vyjádření poskytují jednotliví výrobci softwaru, kteří jsou v dané věci v postavení poškozeného, potažmo autoři filmů, či jejich zástupci, pro něž platí obdobné. Při určování ceny výrobku ze strany poškozeného nebývá zohledněno stáří či verze produktu, nebo počet licencí, které pachatel neoprávněně užíval, nebo zda byl daný film, třeba již několikrát, vysílán na volně dostupné televizní stanici. Všechny tyto okolnosti totiž aktuální cenu ovlivňují. V mnoha případech dochází k výraznému nadhodnocení ceny díla oproti skutečné situaci na trhu. Naznačené situace by měl být znalec schopen v rámci své činnosti vyřešit, neboť může získat informace o ceně produktu nejen od jeho výrobce a distributora, ale i z jiných zdrojů, jako jsou např. informace o cenách, za které je produkt prodáván na elektronických burzách s přihlédnutím k tomu, zda se již konkrétní verze programu nestala freewarem nebo nemá program modernější verzi, která se však příliš neliší, nebo z případných cen zapůjčení filmu v on-line půjčovnách. Soudní znalec je v takovém případě prakticky jediným objektivním arbitrem, jenž je schopen určit, jaká je skutečně aktuální hodnota jednotlivých děl, které pachatel neoprávněně užíval či rozšiřoval. Toto zjištění má zásadní vliv na trestněprávní kvalifikaci skutku.[213]

I pro znalce a jejich znalecké posudky existuje několik důležitých rozhodnutí, které tuto oblast ovlivňují z hlediska právního názoru. Bohužel opět máme prostor pouze pro uvedení některých těchto rozsudků v poznámce pod čarou.[214]

5.5 Mezinárodní spolupráce při vyšetřování počítačové kriminality

Propojování počítačů do stále větších centrálních sítí přináší situace, kdy k některým počítačovým deliktům nedochází pouze na území jednoho státu, ale jejich příprava, páchání a následky mohou nastat na území dvou či více států. Pro řádné odhalení a vyšetření této trestné činnosti je nezbytné, aby jednotlivé státy a hlavně

---

[213] PLECITÝ, David. *Prostředky dokazování softwarové kriminality*. Praha, 2006. Bakalářská práce. PA ČR. Vedoucí práce JUDr. Jan Kolouch. s. 31-33

[214] Nález Ústavního soudu ze dne 14. března 2002, sp. zn. III. ÚS 346/01
Rozsudek Nejvyššího soudu ze dne 13. listopadu 2012, sp. zn. 4 Tz 77/2012
Usnesení Nejvyššího soudu ze dne 12. prosince 2012, sp. zn. 6 Tdo 1372/2012
Usnesení Nejvyššího soudu ze dne 23. června 2010, sp. zn. 3 Tdo 1483/2010, ale i několik dalších

OČTŘ těchto zemí mezi sebou spolupracovaly. Jak jsme již zmínili, bez této spolupráce budou pachatelé počítačové delikty páchat prostřednictvím kyberprostoru v jiném státě bez možnosti je za tyto útoky potrestat. Případná spolupráce může probíhat jednak formou vzájemné právní pomoci, např. Interpol či Europol pro země EU, nebo neformální cestou, jíž si státy navzájem poskytují důležité informace a spolupracují, což je zejména v dnešní době, nejen pro ICT delikty, velmi důležité. Součinnost formou vzájemné právní pomoci je ustavována na základě mezinárodních dohod uzavřených mezi dvěma či více státy. Interpol ustanovil několik expertních pracovních skupin pro oblast ICT a také vydal příručku počítačové kriminality, jež obsahuje metodiku instrukce vyšetřování ICT trestných činů, popis nástrojů a technik k zajištění případných digitálních stop. Obdobně i OSN vydala příručku týkající se prevence a kontroly trestné činnosti související s počítači. Bez vzájemné spolupráce a podpory je boj s kybernalitou téměř nemožný. Bylo nutné přijmout stěžejní mezinárodní dokument, který by boji s počítačovou kriminalitou napomáhal. Tímto dokumentem se stala Úmluva o počítačové kriminalitě, přijata v roce 2001 na Mezinárodní konferenci o počítačové kriminalitě, o níž jsme se již zmiňovali.[215]

[215] GŘIVNA, Tomáš a Radim POLČÁK (eds.). *Kyberkriminalita a právo*. Vyd. 1. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4. s. 97-99

6 Jak bojovat proti kyberzločinům či preventivně působit

Jak bojovat nebo jak působit preventivně je vcelku snadné napsat, nicméně vymyslet systém, který by byl funkční, je zřejmě nesplnitelný úkol. Přesto každá snaha se cení a je nutné zkusit cokoli, co by mohlo pomoci. Na druhou stranu je nutné si uvědomit, že již zmiňovanou bezhraničností kyberprostoru žádný stát či instituce nemá samostatně v boji proti kybernalitě téměř žádnou šanci. Jediná naděje je celosvětová spolupráce. Pokud se však některé státy odmítnou podílet na boji proti kybernetickým zločinům, bude výsledek vždy nejistý. V systému touto absencí vznikne mezera, kterou pachatelé využijí a státy, které nehodlají internetovou zločinnost stíhat, budou využívány jako sídla pro své servery, z nichž budou své útoky díky propojenosti šířit.

Dalším faktorem ovlivňujícím kriminalitu kyberprostoru je nepoměr rozvoje informačních technologií a právního řádu, jež ICT upravuje. Zatímco jeden měsíc může v případě technologického vývoje znamenat neuvěřitelný pokrok, úprava právního řádu se bude počítat spíše na roky a není jisté, s jakým výsledkem. Právo bude neustále za technikou zaostávat, a proto nebude možné kyberzločiny vymýtit úplně. Vždy se objeví nový, do té doby nepopsaný a tedy i zákonem neupravený, způsob, jakým se budou páchat zločiny v oblasti ICT. To je nutné si uvědomovat a také na tuto skutečnost reagovat. Je dobře, že i vláda ČR se o oblast kybernality zajímá[216] a činí některé kroky, které by mohly přivodit alespoň částečnou eliminaci některých negativních skutečností z oblasti ICT. Dle mínění premiéra ČR bude nutné posílit týmy expertů na počítačové útoky a obranu proti nim[217], což lze považovat za správné rozhodnutí.

Jednou z cest boje proti zločinu je i v odvětví ICT prevence. V oblasti porušování autorských práv na internetu to dle autora této práce platí dvojnásob. V některých případech je skutečně nejlepší cestou v boji proti pirátství prevence, tj. předcházení situacím, kdy k porušení práv dochází a těmto situacím se vyvarovat. Níže nějaké možnosti zmíníme.

---

[216] předseda vlády koncem března 2016 jedná s ředitelem NBÚ – http://www.vlada.cz/cz/media-centrum/aktualne/premier-sobotka-stupnujici-kyberneticke-utoky-ukazuji--ze-prijata-prisnejsi-vladni-opatreni-maji-smysl-141285/

[217] Česko se obává kyberútoků. Posílí obranu a přibere IT agenty!. *Tn.cz* [online]. 2016 [cit. 2016-03-26]. Dostupné z: http://tn.nova.cz/clanek/cesko-se-obava-kyberutoku-posili-obranu-a-pribere-it-agenty.html

6.1 Kybernetická bezpečnost – Policie ČR. NCKB, CERT, CSIRT

V případě potřeby vyšetřování počítačové kriminality je tento úkol svěřen ze strany státu v České republice, stejně jako v případě jiné trestné činnosti, Policii ČR. Od roku 2005 začaly při jednotlivých Krajských ředitelstvích vznikat oddělení informační kriminality, která sama aktivně na internetu vyhledávají důkazy o páchání počítačové kriminality. Při jejich vlastním vyšetřování jsou tato oddělení podporována útvary služby kriminální policie a vyšetřování.[218]

Dne 19. října 2011 přijala vláda ČR usnesení o ustavení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast. Na základě přijatého usnesení vzniklo Národní centrum kybernetické bezpečnosti (NCKB), jako součást Národního bezpečnostního úřadu, se sídlem v Brně. Úlohou centra je koordinace spolupráce na národní i mezinárodní úrovni při předcházení kybernetickým útokům i při návrhu a přijímání opatření pro řešení incidentů i proti probíhajícím útokům. Mezi hlavní oblasti činnosti centra náleží:

- provozovat Vládní CERT České republiky (GovCERT.CZ)
- spolupracovat s ostatními národními CERT týmy a CSIRT týmy
- spolupracovat s mezinárodními CERT týmy a CSIRT týmy
- příprava bezpečnostních standardů pro jednotlivé kategorie organizací v ČR
- osvěta a podpora vzdělávání v oblasti kybernetické bezpečnosti
- výzkum a vývoj v oblasti kybernetické bezpečnosti [219]

Od svého zřízení mimo jiné pracovalo na vytvoření zákona o kybernetické bezpečnosti (podkapitola 6.2), který byl dne 2. ledna 2014 schválen vládou k předložení Parlamentu ČR, kde byl posléze přijat a stal se tak platnou součástí právního řadu ČR s účinností od 1.1.2015.[220]

---

[218] GLYKNER, Martin. *Počítačová kriminalita a ČR*. Praha, 2012. Bakalářská práce. VŠE. Vedoucí práce Mgr. Ing. Tomáš Sigmund, Ph.D. s. 26

[219] CO JE NCKB. *Govcert.cz* [online]. [cit. 2016-03-26]. Dostupné z: http://www.govcert.cz/cs/

[220] Národní bezpečnostní úřad. In: *Wikipedia: the free encyclopedia* [online]. 2015 [cit. 2016-03-26]. Dostupné z: https://cs.wikipedia.org/wiki/N%C3%A1rodn%C3%AD_bezpe%C4%8Dnostn%C3%AD_%C3%BA%C5%99ad

Z hlediska bezpečnosti síťové infrastruktury jsou podstatné týmy CSIRT (Computer Security Incident Response Team) a CERT (Computer Emergency Response Team). Praktický rozdíl mezi těmito týmy *de facto* není. Jedné se o obecné označení bezpečnostních týmů, jejichž cílem je minimalizovat počet bezpečnostních incidentů v přidělené síti, a případně spolupracovat s dalšími CSIRT a CERT týmy. Mezi tyto incidenty se řadí například rozesílání spamu, DoS útoky, či případy phishingu a pharmingu. Bezpečnostní týmy jsou vytvářeny v jednotlivých organizacích, které buďto připojení k internetu zprostředkovávají (např. ISP), nebo ho značně využívají (velké firmy). V Čechách na nejvyšší úrovni figuruje tým CSIRT.CZ, který je provozován sdružením CZ.NIC. V gesci tohoto týmu je pak především pomoc s vytvářením bezpečnostních týmu na nižší úrovni a usnadňování jejich vzájemné komunikace. CSIRT.CZ také obstarává komunikaci s národními CSIRT týmy dalších států a české bezpečnostní týmy tento tým chápou „institut poslední záchrany“, kam je možné se obrátit s žádostí o pomoc a spolupráci. Na vládní úrovni vznikl v květnu 2011 GovCERT.CZ, který se specializuje na sítě orgánů veřejné správy a provozovatelů kritické infrastruktury. Jeho provoz zajišťuje NBÚ.[221,222]

6.2 Zákon o kybernetické bezpečnosti

„Novým“ zákonem přijatým pro boj proti kyberzločinům je zákon č. 181/2014 Sb. o kybernetické bezpečnosti, přijatý v roce 2014 a účinný od 1.1.2015. Již při svém přijetí se setkal s rozporuplnými reakcemi a to zejména z důvodu obtížné identifikace osob, na něž zákon ve skutečnosti dopadá, a důvodu přenechání úpravy poměrně značné části klíčových záležitostí podzákonným předpisům – dvěma vyhláškám a jednomu nařízení vlády. Hlavním důvodem přijetí zákona bylo dle důvodové zprávy[223] vyhodnocení dosavadního stavu, kdy ochrana kybernetického prostoru byla vykonávána vesměs osobami soukromého práva bez jednotné regulace, nutné koordinace informací a institucionálního dohledu apod. V důvodové zprávě vláda výslovně poukazuje na DDoS útoky na zpravodajské servery, bankovní a finanční instituce, stránky telekomunikačních operátorů a dalších subjektů z března 2014. Dále, že každý

[221] GLYKNER, Martin. *Počítačová kriminalita a ČR*. Praha, 2012. Bakalářská práce. VŠE. Vedoucí práce Mgr. Ing. Tomáš Sigmund, Ph.D. s. 27

[222] Úvod. *Csirt.cz* [online]. [cit. 2016-03-26]. Dostupné z: https://csirt.cz/

[223] důvodová zpráva dostupná např. zde: https://www.nbu.cz/download/nodeid-806/

informační a komunikační systém je spravován jiným správcem, v odlišných právních režimech, a tudíž jejich společný postup v kritických situacích nelze zajistit jinak než zákonem.[224]

Zákon zavádí výše zmiňovaná dohledová pracoviště v podobě vládního a národního CERT. K označení dotčených subjektů zákon používá termín „orgány a osoby v oblasti kybernetické bezpečnosti“, přičemž se vždy musí jednat o orgány a osoby spravující dostatečně důležité komunikační nebo informační systémy a sítě, které splňují stanovená kritéria. Zákon však bohužel žádným způsobem nereguluje obsah přenášených informací, a nevztahuje se tudíž na otázky počítačové kriminality, dětské pornografie, softwarového pirátství, nelegálního šíření autorských děl (což by pro téma této práce bylo zajímavé) apod. V rámci plnění kontrolních pravomocí tak stát v žádném okamžiku nemá na základě zákona možnost jakkoli kontrolovat obsah informací přenášených prostřednictvím informačních sítí. Subjekty, které spravují specifické informační a komunikační systémy, jsou právě ty, jichž se zákon dotýká. Stav kybernetického nebezpečí je dalším kriteriem pro stanovení okruhu dotčených osob, neboť za standardní situace dopadají přímé povinnosti dle zákona pouze na subjekty, jejichž systémy, sítě nebo služby mají zásadní význam pro fungování státu nebo informační společnosti. Pouze v případě kybernetického nebezpečí je tento okruh osob rozšířen i na ostatní poskytovatele služeb a správce systémů a sítí. Pro lepší představu je toto znázorněno v příloze č. 5. Lze tak rozlišit dvě skupiny dotčených osob. Tou první, které se zákon dotýká pouze okrajově a v přesně stanovených situacích a pouze za stavu kybernetického nebezpečí nebo za nouzového stavu přijmout reaktivní opatření ve smyslu § 11. Do druhé skupiny osob, na něž zákon dopadá v celé své šíři, patří správci informačních systémů kritické informační infrastruktury, správci komunikačních systémů kritické informační infrastruktury a správci významných informačních systémů. Tyto osoby jsou (vedle povinností uvedených výše) povinny plnit informační povinnosti vůči vládnímu CERT, zavádět bezpečnostní opatření a provádět opatření v rozsahu dle zákona.[225]

Pokud bychom provedli shrnutí tohoto zákona, tak většina soukromoprávních

---

[224] Právní aspekty přijetí zákona o kybernetické bezpečnosti. *Systemonline.cz* [online]. 2015 [cit. 2016-03-26]. Dostupné z: http://www.systemonline.cz/clanky/pravni-aspekty-prijeti-zakona-o-kyberneticke-bezpecnosti.htm

[225] tamtéž

subjektů bude spadat do výše zmíněné první skupiny osob s užším okruhem povinností. Tyto subjekty měly bezprostředně po nabytí účinnosti hned povinnost, díky které musely do 30 dní od nabytí účinnosti zákona (tedy do 30.1.2015) nahlásit své kontaktní údaje národnímu CERT. Nicméně všechny subjekty provozující informační a komunikační systémy musely vyhodnotit, zda se jich zákon nějakým způsobem dotýká a pokud ano, do které ze skupin dotčených subjektů patří. Díky tomu mohly včas přijmout potřebná opatření.[226]

6.3 Možné způsoby řešení problému „pirátství“

Doposud jsme diskutovali bezpečnost v kyberprostoru obecně pro veškerá možná konání. Nyní se však pokusíme zaměřit na problémy spojené s pirátstvím, tj. jak tyto nezákonné aktivity potlačovat, či jak působit preventivně, aby k nim vůbec nedocházelo.

6.3.1 HADOPI – elektronická gilotina

Jedním ze způsobů, jak trestat pirátství a vlastně i zneužívání celosvětové počítačové sítě, je řešení zavedené ve Francii, o kterém se dnes hovoří jako o tzv. „elektronické gilotině“ nebo také jako o systému „třikrát a dost“ či „Hadopi[227] law“.

Tento systém představuje zákonnou úpravu, jež zřizuje speciální instituci[227], která má za úkol monitorovat uživatele internetu. Jestliže úřad zjistí, že některý uživatel porušil autorská práva, tak jej upozorní a vyzve, aby v takovém jednání nepokračoval. Pokud bude upozorněn i potřetí, může následovat vedle dalších sankcí i odpojení od internetové sítě na určitou dobu. Dle všeho je tento model v boji s piráty účinný, neboť dvě třetiny lidí, kteří obdrží první upozornění prostřednictvím elektronické pošty, s nelegálním stahováním přestane. V případě druhé zprávy s tímto špatným způsobem využívání internetu skončí se svou nelegální činností více než 95 % uživatelů.[228]

Takto tvrdě represivní přístup má i své stinné stránky. Odpojení od internetu je

---

[226] Právní aspekty přijetí zákona o kybernetické bezpečnosti. *Systemonline.cz* [online]. 2015 [cit. 2016-03-26]. Dostupné z: http://www.systemonline.cz/clanky/pravni-aspekty-prijeti-zakona-o-kyberneticke-bezpecnosti.htm

[227] Higher Authority for the Distribution of Works and the Protection of Copyright on the Internet = HADOPI = francouzský úřad pro jistý způsob monitorování – více případně na: http://hadopi.fr/

[228] Ve Francii začal platit protipirátský zákon „HADOPI“. *Itbiz.cz* [online]. 2010 [cit. 2016-03-26]. Dostupné z: http://www.itbiz.cz/zakon-hadopi-zacal-platit

v současné společnosti velice omezujícím opatřením, jež přináší i řadu problémů. Pokud by odpojení postihovalo pouze delikventa, bylo by pochopitelné a akceptovatelné a složilo by i jako preventivní prvek, neboť by tento akt byl jistě medializován (pouze s údaji, jež je možné zveřejnit). Nicméně často by zasáhlo i další subjekty, zejména členy společné domácnosti. Dle Gřivny a Herczega by byl takovýto zásah do významných politických práv v evropském právním státě těžko ospravedlnitelný, snad jen převažujícím veřejným zájmem orientovaným na dodržování autorských práv. Je jednoduché stanovit za porušování peněžitý trest 300 000 EUR a/nebo odnětí svobody až na 3 roky, avšak jak dopadnout skutečného viníka? To tak snadné není, proto zákon obsahuje ustanovení, že pokud není možné identifikovat konkrétní osobu na určité přípojce, která práva porušuje, lze odsoudit toho, kdo si přípojku nechal zřídit.[229] Autorovi práce však toto trochu připomíná naši úpravu zákona č. 361/2000 Sb., o provozu na pozemních komunikacích, která stanovuje, že provozovatel vozidla má zákonnou odpovědnost za dodržování povinností řidiče, s čímž autor nesouhlasí, neboť zákonodárce se tímto exkulpuje z povinnosti prokázat hříšníkovi vinu, aby si ušetřil námahu, která by v mnoha případech mohla být marná.

Zákon je ve Francii platný již více než 5 let. Ačkoli od počátku byla uživatelům masivně odesílána varování, první „hříšník“ byl odpojen až po téměř třech letech. Podle statistik bylo odesláno více než 5,4 milionu prvních varování, druhých varování byla necelá desetina, přibližně 504 tisíc. Do závěrečné třetí fáze, tedy odpojení od internetu, dospělo jen 2900 uživatelů; trestní řízení bylo údajně zahájeno se zhruba 400 uživatelů. Na úřad HADOPI aktuálně přichází denně okolo 100 tisíc hlášení o porušení práv, z nich ale úřad zvládne vyřídit jen přibližně polovinu, ostatní jsou odložena.[230]

Je však otázkou, zda by tento systém fungoval i u nás. Ne vždy ISP pro každou přípojku využívá jinou IP adresu. Mnoho uživatelů má adresu sdílenou a poté identifikovat správný PC není nemožné, nicméně je to nákladné. Také mnohdy dochází ke změně IP adresy, jež ISP klientovi poskytuje, při každém restartování přípojného zařízení. I změna samotné IP adresy není obtížná, čili i tento fakt by systém ovlivňoval. Taktéž přístup občanů ke státním orgánům, zejména jejich respektování, je u nás na jiné

---

[229] GŘIVNA, T.; HERCZEG, J. Právo na přístup k Internetu, blokace stránek a digitální gilotina. *Trestněprávní revue*. 2010, roč. 9, č. 05, s. 141-146. ISSN 1213-5313. s. 143

[230] Pět let francouzského „třikrát a dost“. *Linuxexpres.cz* [online]. 2015 [cit. 2016-03-26]. Dostupné z: http://www.linuxexpres.cz/novinky/pet-let-francouzskeho-trikrat-a-dost

úrovni. Nehledě na to, že systém by šel obcházet i jinými způsoby a kde je cesta pro jednoho, tak je v Čechách cesta pro každého. Pokud by například došlo k odeslání výzvy, uživatel by změnil poskytovale a tím pádem by měl jinou IP adresu. Musel by vzniknout buď přímo úřad, jako ve Francii, který by vedl registr těchto deliktů, nebo by musel vzniknout jen samotný registr a o agendu by se staral jiný úřad. Nicméně v našich podmínkách, kdy se přes 20 let hovořilo o registru přestupků, který není doposud v provozu (až od 1. října 2016 by měla být zřízena celostátní evidence přestupků), je takové opatření pravděpodobně neproveditelné.

Pokud bychom přikročili k určité míře omezení internetu, navrhoval by autor práce použití tohoto přístupu v případech sdílení dat skrze P2P sítě, neboť v jejich případě by se omezení nabízelo v jiném systému, než využívá HADOPI. Tyto sítě využívají pro přenos souborů porty v určitém rozmezí. Tyto porty nejsou *de facto* k jiné činnosti potřebné a bylo by tak možné i technicky snadně proveditelné, aby ISP tyto porty uživatelům blokoval. P2P sítě by poté nefungovaly. Je ovšem otázkou, zda by takováto služba neporušovala zákazníkova práva na volný internet.

6.3.2 Cena jako prostředek prevence

Autor práce se domnívá, že cena je velmi dobrým prostředkem prevence v oblasti pirátství. Například v době tzv. stánkových DVD, jejichž cena byla od 40 do 50 Kč, se sice občas někdo pokoušel tato díla uploadovat, ale stahování bylo téměř nulové a tak soubory velmi rychle expirovaly (po určité době bez stažení je soubor na filehostingu smazán). Důvod je jednoduchý, pokud chtěl někdo DVD, tak cena prázdného média byla cca 15 Kč, připočteme-li práci a dobu stažení, dostaneme se na cenu cca 30 Kč. Tedy téměř shodnou jako má nové vylisované DVD, které vydrží déle. Lisovaná DVD mají díky použité technologii delší životnost než DVD vypalovaná. V případě dvouvrstvého DVD filmu, kdy velikost originálního disku je více než 4,7GB musí dojít buď ke zmenšení a tím snížení kvality filmu, nebo musí dojít k vypálení na dvouvrstvé médium, které je však mnohem dražší a dosahuje ceny originálního nosiče. Sice tak získáme film, avšak bez potisku povrchu DVD, což jeho hodnotu snižuje. V dalším kroku musí být DVD potištěno a to navyšuje jeho cenu. Z uvedeného je zřejmé, že v takovém případě cena díla ovlivnila počet jeho nelegálních sdílení o minimálně devadesát procent, neboť již cenově bylo výhodnější koupit originál.

Obdobně tomu bylo před několika lety u prodejní akce antivirového programu Nod32. Běžná cena roční licence je cca 1.000,-Kč. Před 6 lety však byla po dobu jednoho měsíce stanovena akční cena roční licence na 199,-Kč. V té době autor práce (při podnikatelské činnosti v IT oboru) prodal za jeden měsíc zhruba 50 licencí. Ačkoli tento produkt doporučoval klientům ve stejné míře a stejným způsobem, tak po zbylých 16 let podnikání prodal stejné licence pouze 3. V ostatních případech nebyl o produkt zájem a klienti volili zřejmě cestu nelegálního užití. V tomto příkladu se promítne, že za měsíc se prodalo 16krát tolik licencí, jako za zbývajících 16 let. Výrobce by si to tedy měl při úvahách o výši ceny produktu uvědomit a případně si trh i nějakým způsobem „vyzkoušet“. Ve smyslu - co se stane, pokud stanoví cenu například na 20% původně zamýšlené. Možná by byl překvapen a zjistil by, že prodal výrobek tolika lidem, že zisk převýší hodnotu z prodeje za plnou cenu ovšem minimu zákazníků. To je také důvod pro rozhodnutí ustanovit koeficient rovný 0,2. Koeficient byl využit při výpočtu výše škody u SW pirátství, kterou autor použil v podkapitole 3.7.2. Velká část obyvatel by akceptovala cenu 20% a produkt zakoupila. Proto je možné podle autora pro určení výše škody takto stanovený koeficient použít.

Obdobná byla situace před několika lety, kdy OEM verze OS Windows XP měly stanovenu cenu na cca 4.000,-Kč, retail verze pak cenu 7.000,-Kč. Microsoft tuto cenu vysvětloval rovností cen stejného produktu na trzích všech zemí. Tento argument sice zní rozumně, nicméně nezohledňuje kupní sílu obyvatel jednotlivých zemí. A předpokládat, že v případě levnější české verze, oproti např. německé, by obyvatelé Německa kupovali produkt český (v českém jazykovém vyhotovení), je dle autora nesmyslné. Proto patřil OS Windows XP mezi nejvíce nelegálně šířené programy své doby. Uživatelé cenu v žádném případě neakceptovali a situaci řešili jinak.

6.3.3 Maďarský model či myšlenka MV ČR – registrace

Pro omezení sdílení metodou ceny existují různé myšlenky. Jednou z nich byla snaha v Maďarsku zatížit poplatkem přenos internetových dat. Vládní návrh daní pro Maďarsko na rok 2015 počítal i s poplatkem za internetové přenosy. Za gigabajt přenesených dat měly společnosti platit 150 forintů (asi 14 korun).[231] Tento poplatek by

[231] Zaplaťte 14 Kč za každý gigabajt: Maďarsko plánuje zdanit internet. *Idnes.cz* [online]. 2014 [cit. 2016-03-26]. Dostupné z: http://technet.idnes.cz/madarsko-planuje-zdanit-internet-dqv-/sw_internet.aspx?c=A141022_172733_sw_internet_pka

samozřejmě pirátství ovlivnil, neboť průměrně velký stažený film z internetu by na oněch 14 korun vyšel, což by jistě mnoho uživatelů neakceptovalo. Tento systém by však přinesl i některé problémy a tak zatím poplatek přijat nebyl.

Další případnou myšlenou, jak potlačit pirátství, se pokusil představit ministr vnitra ČR. V jeho podání jde o jakousi potřeby „deanonymizovat“ internet[232]. Připojení k internetu by bylo možné až po určitém „zalogování“ do systému, neboť bez přihlášení se stránky nenačtou. Tím pádem bude vždy zcela zřejmé, co který uživatel učinil. Alespoň by tomu tak být mělo, neboť získat cizí uživatelské přihlašovací údaje nebude v prostředí internetu obtížné a situaci to jen posune do další fáze, krom pirátství bude páchán ještě další trestný čin. Autor práce, stejně jako mnoho dalších uživatelů, tak s tímto principem nesouhlasí.

6.3.4 Weby s vlastní s tvorbou a kontrola uploadových serverů

Proti pirátství se dá bojovat i systémem sdílení vlastních děl zdarma. Tento systém aplikují např. některé televize, které svou tvorbu, převážně seriály, poskytují uživatelům zdarma na svých webových stránkách. Na stránkách je pak značné množství reklamy, která je pak i v každém díle, přičemž se zobrazuje i během přehrávání. Příjem z této reklamy zcela jistě vynahradí případnou hodnotu jednoho zhlédnutí, neboť systém je nastaven tak, že reklama přeskakovat v podstatě nejde. Důležitá je i kontrola filehostingových úložišť, aby se přesto zdarma nabízená díla na serverech neobjevila a pokud ano, ihned z pozice držitele autorských práv provozovatele serverů vyzvat k odstranění těchto děl. Příkladem takového systému jsou webové stránky TV Prima a TV Nova, přičemž TV Nova stanovuje jistý poplatek, který je dalším příjmem. Ale poplatek je kompenzován přístupem i k dalším službám.

Dle autora práce by tento systém jistě fungoval i v případě filmů. Pokud by distributoři nabízeli filmy zdarma, opět za reklamu na stránkách, je velmi pravděpodobné, že systém by byl více ziskový, než zavedený model prodeje filmů. Naznačený reálný příklad, který autor popsal ve čtvrté kapitole z vlastní zkušenosti

---

[232] "Chovanec je zločin" znělo před ministerstvem vnitra na demonstraci Pirátů. *Lidovky.cz*[online]. 2016 [cit. 2016-03-27]. Dostupné z: http://www.lidovky.cz/pirati-demonstrovali-za-svobodny-internet-fko-/zpravy-domov.aspx?c=A160220_185941_ln_domov_ELE

dokládá, že za reklamu utržil pachatel přes 300.000,-Kč měsíčně. Kolik by poté musely vydělávat filmové společnosti? A nabízela by se i možnost úpravy filmu, zdarma by byl k dispozici pouze v nízkém rozlišení, například jen SD. Tento formát je vhodný jen pro malá zařízení, např. notebooky, ale nejnovější velké televize s rozlišením HD, nebo dnes již i 4K, by toto dílo zobrazily značně „kostičkovaně" a tím i nekvalitně. Pokud by přesto uživatel o dílo stál ve větším rozlišení pro svou velkou televizi, byl by k dispozici za poplatek, ale stanovený v rozumné výši, třeba 5,-Kč. I tento systém by dle autora mohl velmi dobře prosperovat.

6.3.5 Akceptace pirátství jako způsob prevence

I určitý stupeň akceptování softwarového pirátství může představovat jistý druh prevence. Pokud je v některých rodinách užíván nějaký počítačový program neoprávněně, jedná se o podobu pirátství. Nicméně společnosti vyrábějící programy si uvědomují, že v těchto rodinách jsou děti, které jednoho dne vyrostou. Na daný systém si již zvykly, tak proč jej měnit. A protože se dá předpokládat jistý vývoj ve společnosti, co se náhledu na nelegální užívání SW týká, mohou tyto společnosti předpokládat, že nová generace bude jejich systém využívat zcela v souladu s licencí a tudíž program zakoupí.

S tímto samozřejmě souvisí i výchova nejmladší generace, a to nejen v rodinách, ale i ve školách, které mohou preventivně působit zdůrazňováním těch správných hodnot, mezi které zákonné jednání jistě patří. Pokud totiž společnost zaznamená v tomto směru určitý vývoj, bude to mít vliv i na její kriminalitu, nejenom internetovou, ale i v jejím celkovém pojetí.

Případné ovlivnění názoru na pirátství ve společnosti by mohlo být způsobeno i spojením určitých dominantních firem s nelegální činností. Těmto firmám by se takové spojení jistě nelíbilo, případy by byly medializované a o problému by se hovořilo, což by názory obyvatel ovlivňovalo. Pokud se ještě jednou vrátíme k příkladu embedded linky v praxi, který autor uvedl v podkapitole 4.5, tak zde pachatel zřejmě získává prostředky nejvíce od společnosti Seznam.cz. Je to firma svým způsobem ovlivňující český trh, a pokud by existoval nějaký seznam finančních přispěvatelů nelegální činnosti, kde by tato firma byla uvedena, jistě by se jí to nelíbilo. A svou podporu

nelegálním stránkám by jistě zvážila. Medializace problémů s nezákonnou činností má neuvěřitelný vliv na společnost i na samotné firmy, které totiž o tento typ reklamy nestojí. Příkladem je nedávné odhalení dopingového prohřešku známé sportovkyně. „*Tenisová hvězda Maria Šarapovová ztrácí velké sponzory. Nejlépe placenou sportovkyni loňského roku přestaly podporovat kvůli dopingu, ke kterému se ruská hráčka nečekaně přiznala.*“ [233] Toto jen dokládá již vyřčené. Pokud bychom pirátům odebrali finance, jejich nezákonná činnost bude rapidně snížena, protože zdarma pracuje jen málokdo.

6.4 Budoucnost

I v budoucnu budou kyberzločiny znamenat značnou hrozbu. Dá se dokonce předpokládat, že situace se bude ještě zhoršovat. Z tohoto důvodu EU připravuje nové směrnice a nová nařízení, kterými se snaží na případný vývoj reagovat.

Do konce roku 2017 by měly vstoupit v platnost dva nové právní předpisy EU, které upravují informační bezpečnost a ochranu dat. Zásadním způsobem ovlivní, jak organizace v členských státech EU řeší svou ochranu a jak oznamují narušení bezpečnosti a případnou ztrátu dat. Kyberbezpečnostní směrnice o bezpečnosti sítí a informací (Network and Information Security, NIS) a Nařízení o obecné ochraně údajů (General Data Protection Regulation, GDPR) zasáhnou všechny organizace v rámci všech států EU bez ohledu na jejich velikost. Stanoví standard pro zabezpečení informací a ochranu údajů a sjednotí předpisy v rámci jednotlivých členských států. Snahou je snížit počet bezpečnostních incidentů a úniků osobních dat.[234]

Připravovaná směrnice reaguje na obavy z případných kybernetických útoků, určuje bezpečnostní i ohlašovací závazky společností v rizikových oblastech, jako jsou doprava, energetika, zdravotnictví či finance. Internetové firmy budou předmětem méně přísných povinností než například letiště nebo provozovatelé produktovodů. Podle směrnice budou společnosti jako Google, Amazon, eBay či Cisco muset nahlásit vážné bezpečnostní incidenty národním úřadům, které budou mít pravomoc uvalit na firmy

[233] Šarapovová přichází o miliony, na početný tým vinu nesvádí. *Rozhlas.cz* [online]. 2016 [cit. 2016-03-27]. Dostupné z: http://www.rozhlas.cz/zpravy/tenis/_zprava/sarapovova-prichazi-o-miliony-na-pocetny-tym-vinu-nesvadi--1591744

[234] Co vyžadují nové předpisy EU o kybernetické bezpečnosti? *Computerworld.cz* [online]. 2015 [cit. 2016-03-27]. Dostupné z: http://computerworld.cz/securityworld/co-vyzaduji-nove-predpisy-eu-o-kyberneticke-bezpecnosti-52594

sankce, pokud dané závazky nesplní.[235] Nabízí se jistá podoba zmiňovaného zákona o kybernetické bezpečnosti, který je již v ČR více než rok účinný.

6.5 Vliv kyberkriminality na některé obory podnikání

Pro některé obory podnikání bohužel existuje vyšší riziko ovlivnění kriminalitou, což případným podnikajícím subjektům může přinést nemalé problémy. Ovlivnění trhu může být jak v pozitivním, tak i v negativním směru. Uvedeme si několik příkladů, kdy kriminalita měla na podnikání vliv.

Internetová kriminalita měla zcela jistě rozhodný účinek na vývoj podnikání v oblasti videopůjčoven (včetně DVD nosičů). Pirátství předznamenalo tomuto oboru téměř konec. Ve fyzické podobě, kdy uživatel musí do půjčovny osobně, konec skutečně nastal, ale objevila se varianta on-line videopůjčoven, která stále ještě na trhu přežívá a dle posledního vývoje možná i zažívá nový rozmach. Sledování televize na základě vlastního výběru pořadů z on-line videotéky je způsob zábavy, který si stále častěji volí český divák[236]. Přes tento fakt je možné udělat závěr, že jen o málokteré nezákonné činnosti se dá říci, že tak zásadně ovlivnila činnosti v souladu se zákonem. Problémy pro videopůjčovny nastaly se zvyšující se dostupností technologie, která umožňovala kopírování obsahu na médiích uložených. Klesaly ceny počítačů a tak je začalo mít doma stále více lidí. A vypalovací mechanika se začala stávat jejich běžnou součástí.[237] To vše byly důvody konce klasických půjčoven.

Určitý vliv na podnikání a hlavně placení v kyberprostoru mělo zavedení kryptoměny Bitcoin, o které se uvažuje i jako o možné oficiální měně[238]. Touto

---

[235] EU má první směrnici o kybernetické bezpečnosti. Firmy jako Google budou muset hlásit nebezpečné incidenty. *Ihned.cz* [online]. 2015 [cit. 2016-03-27]. Dostupné z: http://zahranicni.ihned.cz/evropa-slovensko/c1-64952760-eu-ma-prvni-smernici-o-kyberneticke-bezpecnosti-internetove-firmy-budou-muset-hlasit-nebezpecne-incidenty

[236] Češi se vracejí do videopůjčoven, tentokrát on-line. *Ceskatelevize.cz* [online]. 2015 [cit. 2016-03-27]. Dostupné z: http://www.ceskatelevize.cz/ct24/media/1606311-cesi-se-vraceji-do-videopujcoven-tentokrat-line

[237] Úspěch podnikatelského nápadu není zaručen na věky. *Ipodnikatel.cz* [online]. 2011 [cit. 2016-03-27]. Dostupné z: http://www.ipodnikatel.cz/Hledani-podnikatelskeho-napadu/uspech-podnikatelskeho-napadu-neni-zarucen-na-veky.html

[238] Z bitcoinu se možná stane legální měna. Japonsko uvažuje o zdanění. *Novinky.cz* [online]. 2016 [cit. 2016-03-27]. Dostupné z: http://www.novinky.cz/internet-a-pc/395970-z-bitcoinu-se-mozna-stane-legalni-mena-japonsko-uvazuje-o-zdaneni.html

měnou je možné provádět platby na internetu. Nicméně se stala platidlem i za nelegální operaci a to má na její pověst, jíž se prezentuje, neblahý vliv. Některé země tak považují bitcoiny za jasný symbol trestné činnosti. Např. „Kreml chce za bitcoiny posílat až na čtyři roky do vězení. Je to prý prostředek pro zločince“[239].

Jistý dopad má kybernalita i na oblast pojišťovnictví. Některé pojišťovny zařadily do svého portfolia produkty, které nabízí pojištění kybernetických rizik. Jako první v ČR koncem března 2016 zařadily mezi nabízené produkty tuto službu Kooperativa a ČSOB Pojišťovna a to za cenu cca 900 Kč / rok. Přičemž pojištění lze sjednat pro případ:

- úniku osobních údajů, dat a informací z informačního systému nebo počítače společnosti (náhodného nebo z nedbalosti)
- cíleného napadení informačního systému třetími osobami nebo zaměstnanci společnosti za účelem získání přístupu k datům společnosti a způsobení škody[240]

Již brzy (zřejmě od 1.11.2016) vejde v platnost povinnost podnikatelů evidovat každou platbu on-line [241]. Autor se domnívá, že i tento systém se stane terčem kyberzločinců. Něco podobného se totiž v daňové oblasti stalo na Slovensku [242]. Finanční správa by se na možný útok tedy měla důkladně připravit.

Zajímavý dopad má kyberkriminalita i na oblast vzdělávání. Zatím se sice jedná o soukromou vysokou školu, nicméně již se připravuje nový studijní obor pro příští rok, který bude na kybernalitu zaměřen. Potenciální studenty láká na heslo: „Staňte se nepostradatelným pro kybernetickou bezpečnost firmy“ [243]. To jen dokazuje, že kybernalita ovlivňuje téměř vše kolem nás.

---

[239] Kreml chce za bitcoiny posílat až na čtyři roky do vězení. Je to prý prostředek pro zločince.*Ihned.cz* [online]. 2016 [cit. 2016-03-27]. Dostupné z: http://archiv.ihned.cz/c1-65205180-kreml-chce-za-bitcoiny-posilat-do-vezeni

[240] Pojištění kybernetických rizik. *Vitovec.cz* [online]. 2016 [cit. 2016-03-27]. Dostupné z: http://www.vitovec.cz/pojisteni-kybernetickych-rizik

[241] Senát schválil evidenci tržeb. *Eltrzby.cz* [online]. 2016 [cit. 2016-03-27]. Dostupné z: http://www.eltrzby.cz/cz/aktuality/85-senat-schvalil-evidenci-trzeb

[242] Na Slovensku odhalili manipulace s registračními pokladnami, jde o miliardy. *Novinky.cz*[online]. 2016 [cit. 2016-03-27]. Dostupné z: http://www.novinky.cz/ekonomika/397422-na-slovensku-odhalili-manipulace-s-registracnimi-pokladnami-jde-o-miliardy.html

[243] BEZPEČNOST A TECHNOLOGIE KOMUNIKACE. *Mup.cz* [online]. 2016 [cit. 2016-03-27]. Dostupné z: http://www.mup.cz/btk/

7 Vlastní návrhy – *De lege ferenda*

V této kapitole si přiblížíme možné právní ustanovení skutkové podstaty, které by postihovalo zmiňované problémové DoS a DDoS útoky a v druhé části, ve spojitosti s uvedeným výpočtem výše škody u pirátství či náhledem posouzení z podkapitoly 3.7.2, si představíme autorův návrh změny ustanovení § 270 TZ, jež by vyhovovalo nově nastaveným kriteriím a případně definujeme ustanovení nového § 270a TZ.

7.1 DoS a DDoS útoky

Ačkoli je pravidlem, že skutková podstata by měla zachovávat dostatečnou obecnost a neměla by tak být zaměřena pouze na jeden typ konání, v tomto případě si situace v kyberprostoru zaslouží výjimku a tyto útoky by měly být postižitelné svou vlastní skutkovou podstatou. Sice se jedná o jediný unikátní typ činnosti, přesto si svou četností, která se dle statistik uvedených v podkapitole 2.7.1 bude pravděpodobně jen zvyšovat, tuto výjimku zaslouží.

Nyní se pokusíme navrhnout znění skutkové podstaty, jež by umožňovalo trestat DoS a DDoS útoky, dle názoru autora práce. Mělo by být uvedeno v trestním zákoníku v hlavě V věnované trestným činům proti majetku a snad i bezprostředně za dalšími počítačovými trestnými činy. Mohlo by se jednat o znění § 232a TZ. Zároveň se budeme snažit zahrnout do vymezení všechny varianty těchto útoků při zachování dostatečné obecnosti, aby bylo ustanovení použitelné i v případě možných technologických změn v budoucnosti. Dané ustanovení ještě krátce okomentujeme.

§ 232a

Nedovolený zásah do provozu informačního systému

(1) Kdo v úmyslu podstatně omezit nebo zcela vyřadit z provozu cizí informační systém nebo službu tohoto systému vytvoří a poté cíleným způsobem nasměruje datový proud či silný telekomunikační provoz nebo zužitkuje jinou možnost za účelem zahlcení kapacity určené pro přenos nebo využije hardwarové nebo softwarové chyby informačního systému, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.

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

a) způsobí-li takovým činem škodu nikoli malou,
b) spáchá-li čin uvedený v odstavci 1 proti více subjektům
c) způsobí-li tímto činem vážnou poruchu v činnosti právnické osoby nebo fyzické osoby, která je podnikatelem.

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

a) způsobí-li takovým činem značnou škodu,
b) získá-li takovým činem pro sebe nebo pro jiného značný prospěch,
c) omezí-li tímto činem funkčnost sítě elektrotechnických komunikací,
d) bude-li mít takový čin dopad na státem garantovanou službu.

(4) Odnětím svobody na pět až dvanáct let bude pachatel potrestán

a) způsobí-li takovým činem škodu velkého rozsahu,
b) získá-li takovým činem pro sebe nebo pro jiného prospěch velkého rozsahu,
c) bude-li mít čin uvedený v odstavci 1 dopad na kritickou informační infrastrukturu
d) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny.

(5) Příprava je trestná.

V prvním odstavci jsme definovali způsob možného škodlivého jednání, které v současnosti vystihují jen zmiňované DoS útoky, nicméně v budoucnu by se mohlo jedna např. o zahlcení GSM sítě s úmyslem poškodit zákazníky i provozovatele, nebo narušit satelitní vysílání. V druhém odstavci se pak zaměřujeme na možnou škodu, kterou je možné zásahem způsobit, také na rozsah možných útoků na více subjektů a na poškozování podnikatelské činnosti, což si jistě zaslouží udělení vyššího trestu. Třetí odstavec krom výše škody zohledňuje i případný profit pachatele a také služby důležitější pro fungování společnosti, jako jsou některé státem garantované služby a komunikační systémy. Čtvrtý odstavec pak naráží na nejzávažnější problém, jednak organizované pachatelství a pak na problémy s kyberútoky obecně, kterým se snaží zabraňovat výše zmiňovaný zákon o kybernetické bezpečnosti, proto je pojem kritické informační infrastruktury převzat z tohoto zákona, konkrétně z jeho ustanovení § 2 písm. b), kterážto jednání, spolu s vysokou škodou či ziskem lze považovat za zvlášť závažné zločiny díky čemuž je i jejich příprava trestná.

7.2 Návrhy na změnu znění § 270 TZ a znění nového TČ § 270a TZ

V podkapitole 3.7.2 jsme nastínili některé možnosti, jak přistupovat k problému pirátství. Pokusili jsme se stanovit jisté způsoby výpočtu pro stanovení výše způsobené škody. Také jsme uvedli jednu možnost, kdy výši škody nevyžadovat. Nyní se pokusíme definovat skutkovou podstatu, která by tuto naší přípravu zohlednila.

7.2.1 Varianta založená na výši škody

Pro tuto variantu je známa výše způsobené škody, přesto není možné využít aktuální ustanovení § 270 TZ, neboť se vztahuje i na jiná díla (knihy, obrazy, atd.), než potřebujeme. Dojde k jeho změně v prvním odstavci, kdy odebereme definici pro počítačové programy a audio a audiovizuální díla, která budou mít svou úpravu v § 270a, jež bude ve vztahu *lex specialis* k ustanovení § 270.

§ 270

Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi

(1) Kdo neoprávněně zasáhne nikoli nepatrně do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, rozhlasovému nebo televiznímu vysílání nebo databázi, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.

§ 270a

Porušení autorského práva souvisejícího s počítačovým programem a zvukovým či zvukově obrazovým záznamem

(1) Kdo neoprávněně zasáhne nikoli nepatrně do zákonem chráněných práv ke zvukovému či zvukově obrazovému záznamu nebo počítačovému programu a tímto zásahem způsobí jinému škodu nikoli nepatrnou nebo získá takovým činem pro sebe nebo pro jiného prospěch v nikoli nepatrné výši, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.
(2) Odnětím svobody na šest měsíců až pět let, peněžitým trestem nebo propadnutím věci bude pachatel potrestán,

a) vykazuje-li čin uvedený v odstavci 1 znaky obchodní činnosti nebo jiného podnikání,
b) získá-li takovým činem pro sebe nebo pro jiného značný prospěch nebo způsobí-li tím jinému značnou škodu.

(3) Odnětím svobody na tři léta až osm let bude pachatel potrestán, získá-li činem uvedeným v odstavci 1 pro sebe nebo pro jiného prospěch velkého rozsahu nebo způsobí-li tím jinému škodu velkého rozsahu.

(4) Odnětím svobody na pět až dvanáct let bude pachatel potrestán, dopustí-li se činu uvedeného v odstavci 1 jako člen organizované skupiny, která nese znaky obchodní činnosti.

Autor práce skutkovou podstatu orientuje na výši způsobené škody, případně na výši prospěchu, který lze nelegální činností získat. Pokud máme stanoven vzorec výpočtu škody (podkapitola 3.7.2), jedná se o nejobjektivnější posouzení.

Obdobně u trestného činu krádeže nás také zajímá výše škody určená znalcem na odcizené věci v době krádeže. Případně si pokládáme otázku, zda pachatel měl a mohl vědět, že cena je vyšší, ačkoli předmět se jevil jako bezcenný, ale ve skutečnosti je jeho hodnota nikoli nepatrná či vyšší.

V dalších odstavcích zohledňujeme možnou rostoucí výši škody či zisku, ale také chápeme jako škodlivé, pokud činnost vykazuje znaky podnikání, neboť podnikání s nelegálním produktem chápe autor jako společensky škodlivé. Poslední odstavec je cílen na nejzávažnější typ kriminality, kterou představují organizované skupiny, jež mohou díky propracované organizaci napáchat škody astronomické výše.

Výhodou varianty je již zmiňované vyčíslení výše škody, která může být v rámci trestního řízení poškozeným přiznána.

7.2.2 Varianta založená na rozsahu škody

Zde je nutné oddělit případy běžně spojené s právem autorským a případy pro tuto práci důležité. Opět upravíme znění § 270 a vytvoříme novou skutkovou podstatu, obdobně jako v minulé podkapitole. Nicméně nyní již skutková podstata nebude založená na způsobené škodě ale na rozsahu zpřístupnění děl (i na fyzických nosičích).

§ 270

Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi

(1) Kdo neoprávněně zasáhne nikoli nepatrně do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, rozhlasovému nebo televiznímu vysílání nebo databázi, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.

§ 270a

Porušení autorského práva souvisejícího s počítačovým programem a zvukovým či zvukově obrazovým záznamem

(1) Kdo neoprávněně v míře škodlivé zasáhne do zákonem chráněných práv ke zvukovému či zvukově obrazovému záznamu nebo počítačovému programu nebo získá takovým činem pro sebe nebo pro jiného prospěch v nikoli nepatrné výši, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.

(2) Odnětím svobody na šest měsíců až pět let, peněžitým trestem nebo propadnutím věci bude pachatel potrestán,

a) vykazuje-li čin uvedený v odstavci 1 znaky obchodní činnosti nebo jiného podnikání,
b) získá-li takovým činem pro sebe nebo pro jiného značný prospěch nebo
c) dopustí-li se takového činu v míře nebezpečné.

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

a) získá-li činem uvedeným v odstavci 1 pro sebe nebo pro jiného prospěch velkého rozsahu nebo
b) dopustí-li se takového činu v míře kritické.

(4) Odnětím svobody na pět až dvanáct let bude pachatel potrestán, dopustí-li se činu uvedeného v odstavci 1 jako člen organizované skupiny, která nese znaky obchodní činnosti.

Do základní skutkové podstaty autor nepoužil spojení „nikoli nepatrně“, které je obsaženo v současné úpravě § 270 TZ, neboť jej v tomto případě nepovažuje, ve spojení s posuzováním jednání co do rozsahu, za vhodné.

Nezbytné však naopak je, pro případné uplatnění, jasné definování pojmů míry škodlivé, nebezpečné a kritické.

Za míru škodlivou bude považováno zpřístupnění alespoň 50 songů nebo 20 epizod seriálů nebo 10 filmů nebo 10 hudebních alb nebo 5 počítačových programů a jejich možné kombinace.

Za míru nebezpečnou bude považováno zpřístupnění alespoň 200 songů nebo 50 epizod seriálů nebo 30 filmů nebo 30 hudebních alb nebo 15 počítačových programů a jejich možné kombinace.

Za míru kritickou bude považováno zpřístupnění alespoň 500 songů nebo 200 epizod seriálů nebo 100 filmů nebo 100 hudebních alb nebo 30 počítačových programů a jejich možné kombinace.

Tato varianta možná není nejvhodnější, neboť nezohledňuje aktuálnost filmu. Ačkoli i při jednom nejnovějším nasdíleném filmu (camcording) by mělo být jednání klasifikováno jako trestný čin (způsobená škoda, nejen majetková, bude značná), uvedené znění toto neřeší. Na druhou stranu však s sebou přináší možnost velice jednoduchého právního posouzení.

Primárně jde o rozsah sdílení, přičemž u softwaru je vždy nejnižší hodnota co do počtu zpřístupnění (i na optickém nosiči), neboť autor chápe počítačové programy jako nejcennější díla z nabízených. Díky přesné definici počtu produktů nebude při právním posouzení problém určit, do jaké kategorie daný čin spadá. Zároveň ale skutková podstata zohledňuje i možný profit pachatele, který je taktéž nežádoucí, stejně jako případná podnikatelská činnost. V posledním odstavci je pak opět zmíněna nebezpečnost organizovaných skupin, stejně jako v předcházející podkapitole.

8 Závěr

Co říci závěrem? Snad jen to, že autor se v této práci pokusil popsat několik problémů, které kráčí ruku v ruce s kyberprostorem. Nicméně je nutné si uvědomit, že ačkoli se autor připravoval, sbíral odborné i naučné články a novinky a dělal si poznámky k přípravě více než jeden rok s cílem sepsat práci s co možná nejaktuálnějšími fakty, je vývoj v oblasti ICT tak překotný, že ve chvíli kdy práce bude tištěna, budou v oboru používány zcela nové přístupy a poznatky. Každým dnem vznikají nové způsoby, jak trestnou činnost prostřednictvím počítače a internetu páchat. Přesto autor doufá, že práce obsahuje dostatek podnětných materiálů, které danou problematiku vystihují. Určitě si ale nečiní iluze, že by se v práci podařilo postihnout kompletní problematiku s naprosto všemi souvislostmi.

Hlavní jádro práce, které představuje třetí kapitola, tedy problematika pirátství, je shrnuto na cca 80 stranách a snad podrobně vystihuje skutky, kterých se lze v souvislosti s autorským právem dopustit. Autor nechtěl sepsat práci, jež by byla pouhým povrchním popisem či nástinem situace a tak přistoupil k poněkud hlubší analýze celé problematiky. Nevýhodou tohoto přístupu je fakt, že celá práce je obsáhlejší, než by zřejmě dle požadavků na diplomovou práci být měla, avšak snad to nebylo ke škodě. I tak musel autor přistoupit k omezení práce, zvláště u páté a šesté kapitoly vyřadil některé pasáže, které měl připravené, neboť by práce měla přes 200 stran a to by bylo skutečně mnoho. Přesto by se k dané problematice v budoucnu rád vrátil s novými poznatky, jež jistě vývoj, jak práva, tak hlavně informačních technologií, přinese. Také by rád využil možnosti zahrnout rovněž problematiku trestního řízení a postupů OČTŘ (jako je zajištění důkazů, či možnost „zmrazit“ obsah webových serverů a úložišť do konce vyšetřování) v daných konkrétních případech a tuto práci jimi doplnil. Zejména kapitola věnovaná pachateli, tedy odhalování a vyšetřování kybernality, by si podrobnější rozbor zasloužila, neboť prostoru v tomto zpracování mnoho nedostala, z důvodů výše uvedených.

Pro některé pasáže této práce zvolil autor přiměřeně volnější výrazovou formu, neboť se domnívá, že je čtivější a k dané problematice více přináleží. Avšak v práci jsou

obsaženy rovněž statě, jež jsou psány prostřednictvím odborných faktů, které jsou adekvátní vědecké práci.

V této souvislosti je nutné připomenout, že díky blanketnímu odkazu v ustanovení § 270 TZ bylo nutné v práci popisovat i jinou právní problematiku, než pouze problematiku trestněprávní. Problém trestněprávního posouzení těchto zločinů je právě díky odkazu na jiné normy, které nemají vždy tak jednoznačný a jednotný výklad. Ten poté představuje komplikaci, zda je možné jednání posoudit jako protiprávní. Bylo tedy nezbytné, krom právu trestnímu, se věnovat i právu autorskému, občanskému a správnímu, ale také mnoha technickým údajům, jež s oblastí souvisí a podílejí se na jejím utváření. Stejně tak nebylo možné vše posuzovat jen z hlediska práva, ale i z jiných odvětví lidské činnosti, neboť nejen právo je pro tyto činy určujícím faktorem. Přesto autor doufá, že se se vším obstojně vypořádal a práce přináší nové pohledy do diskutované problematiky, stejně tak i jeho právní názory a stanoviska a není jen pouhým povrchním nástinem, což si sám autor, ani vedoucí práce, nepřáli.

Poslední připomínku, se kterou se rozloučíme a kterou si autor nemohl odpustit, je opětovná novinka v problematice skimming z druhé kapitoly. V předposledním březnovém týdnu roku 2016 se objevila novinka, které tyto činy opět modifikuje. Nový přístroj na skimming již není pouhým jednoduchým zařízením, proti kterému se dá bránit skrytím PINu při zadávání. Jedná se o důmyslné provedení, kdy je na celý bankomat, nasazena svrchní část, jež jej celý přikryje jako „maska na obličej“ a není tak možné zakrýt klávesnici při zadávání PINu, neboť i deska pro zadávání je snímána a nepotřebuje kameru, protože se snímá každé jednotlivé stisknuté klávesnice. Proti tomuto typu zřejmě obrana není. Více v případně ve videu[244] nebo na obr. 6. Do druhé kapitoly již nechtěl autor zasahovat a tak je tato novinka zde, jako poslední tečka, která demonstruje neustálý vývoj a modifikaci kyberzločinů.

Obr. 6

[244] video představující novou a zřejmě velmi účinnou metodu – bylo objeveno policií v polovině března 2016 – zde je možné zhlédnout více než na obr. 6 – http://www.navratdoreality.cz/?p=view&id=22786

9 Seznam zkratek

AZ	autorský zákon
BSA	mezinárodní „protipirátská organizace“, sdružující výrobce software v boji proti jeho nelegálnímu užívání, založena 1998
CD	Compact Disc – pro uložení optických, digitálních dat
CERT	Computer Emergency Response Team
ČPU	Česká protipirátská unie
DNS	Systém doménových jmen
DVD	Digital Versatile (Video) Disc – formát digitálního optického datového nosiče, který může obsahovat filmy ve vysoké obrazové a zvukové kvalitě
ES	Evropská společenství
EU	Evropská unie
FBI	Federální úřad pro vyšetřování (anglicky Federal Bureau of Investigation – yšetřovací orgán amerického ministerstva spravedlnosti
FO	fyzická osoba
FTP	File Transfer Protokol – protokol pro přenos souborů mezi počítači pomocí počítačové sítě
HDD	pevný disk (zkratka HDD, anglicky Hard Disk Drive)
HW	hardware
ICT	informační a komunikační technologie
IT	informační technologie
ISP	poskytovatel internetového připojení
LPT	paralelní port
LZPS	Listina základních práv a svobod
NBÚ	Národní bezpečnostní úřad
NS	Nejvyšší soud
OČTŘ	orgány činné v trestním řízení
OS	operační systém, zejména Windows

OZ	občanský zákoník
PC	osobní počítač, nepřenosný (z anglického „personal computer“)
PIN	akronym z anglického personal identification number, což znamená osobní identifikační číslo, užití k autorizaci např. u platební karty
PO	právnická osoba
SDEU	Soudní dvůr Evropské unie v Lucemburku
SMART	chytré spotřebiče se síťovou konektivitou
SW	software
TZ	trestní zákoník
TŘ	trestní řád
URL	Unified Resource Locator
USB	Universal Serial Bus – způsob připojení periferií k počítači
Úmluva	Úmluva o kybernetické (počítačové) kriminalitě
ÚOOZ SKPV	Útvar pro odhalování organizovaného zločinu Služby kriminální policie a vyšetřování
VŠ	vysoká škola
VŠE	Vysoká škola ekonomická
Wi-Fi	Wireles Fidelity – Bezdrátová technologie pro šíření dat („vzduchem“), vhodná pro tvorbu sítových infrastruktur
WIPO	Světová organizace duševního vlastnictví
WWW	world wide web = v překladu celosvětová síť
ZTOPO	zákon o trestní odpovědnosti právnických osob a řízení proti nim

10 Zdroje

10.1 Seznam použité české a anglické literatury

BARTŮNĚK, Jan. *Kybernetická kriminalita*. Praha, 2014. Diplomová práce. PF UK. Vedoucí práce Doc. JUDr. Tomáš Gřivna, Ph.D.

CÍSAŘOVÁ, Zuzana. Pojem „nová veřejnost“ v rozhodovací praxi SDEU a slučitelnost s mezinárodními úmluvami v oblasti autorského práva. *Aktuální otázky práva autorského a práv průmyslových: nový občanský zákoník a vybrané problémy evropského práva duševního vlastnictví - dopady na českou legislativu a praxi*. Praha: Univerzita Karlova v Praze, Právnická fakulta, 2014, ISBN 9788087975152. s. 44-52

ČERMÁK, Jiří. *Internet a autorské právo*. 2. aktualiz. a rozš. vyd. Praha: Linde, 2003, 251 s. ISBN 80-7201-423-4.

DRAŠTÍK, Antonín. *Trestní zákoník: komentář*. Vydání první. Praha: Wolters Kluwer, 2015. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-790-4.

DUBENSKÁ, Petra. *Internetová a počítačová kriminalita*. Praha, 2013. Diplomová práce. PF UK. Vedoucí práce Doc. JUDr. Tomáš Gřivna, Ph.D.

DVOŘÁK, Pavel. *Neoprávněné užití autorského díla*. Praha, 2015. Diplomová práce. PF UK. Vedoucí práce JUDr. Veronika Křesťanová, Dr.

FRIČ, Antonín. *INTERNET A AUTORSKÉ PRÁVO*. Praha, 2011. Diplomová práce. PF UK. Vedoucí práce JUDr. Irena Holcová.

GÁBRIŠ, Tomáš. *Law & technology*. 1. vydanie. Bratislava: Comenius University, 2015. Učebnice Právnickej fakulty. ISBN 978-80-7160-397-9.

GLENNY, Misha. *Temný trh: kyberzloději, kyberpolicisté a vy*. 1. vyd. v českém jazyce. Praha: Argo, 2013, 270 s. Zip (Argo: Dokořán). ISBN 978-80-7363-522-0.

GLYKNER, Martin. *Počítačová kriminalita a ČR*. Praha, 2012. Bakalářská práce. VŠE. Vedoucí práce Mgr. Ing. Tomáš Sigmund, Ph.D.

GRAGIDO, Will, John PIRC a Russ ROGERS. *Cybercrime and espionage: an analysis of subversive multivector threats*. Oxford: Elsevier Science [distributor], 2011, xv, 254 p. ISBN 1597496138.

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

GŘIVNA, Tomáš. Existují virtuální trestné činy? *Pocta Otovi Novotnému k 80. narozeninám*. s.28-35, , 28-35. ISSN 978-80-7357-365-2.

CHUDĚJ, Radim. *Právní postih kybernetických útoků*. Brno, 2014. Diplomová práce. Právnická fakulta Masarykovy univerzity. Vedoucí práce Doc. JUDr. Radim Polčák, Ph.D.

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

MAREŠOVÁ, Alena. *Resortní statistiky - základní zdroj informací o kriminalitě v České republice*. Vyd. 1. Praha: Institut pro kriminologii a sociální prevenci, 2011, 148 s. Studie (Institut pro kriminologii a sociální prevenci). ISBN 978-80-7338-110-3.

MATĚJKA, Michal. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, 2002. ISBN 80-7226-419-2.

MATOUŠKOVÁ, Ingrid. *Aplikovaná forenzní psychologie*. 1. vyd. Praha: Grada, 2013. Psyché (Grada). ISBN 978-80-247-4580-0.

PFEFFER, Jan. *Softwarové pirátství*. Praha, 2009. Diplomová práce. PF UK. Vedoucí práce JUDr. Petra Malá Žikovská.

PLECITÝ, David. *Prostředky dokazování softwarové kriminality*. Praha, 2006. Bakalářská práce. PA ČR. Vedoucí práce JUDr. Jan Kolouch.

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

PORADA, Viktor a Zdeněk KONRÁD. *Metodika vyšetřování počítačové kriminality*. Vyd. 1. Praha: Policejní akademie České republiky, 1998. ISBN 80-85981-75-0.

ROSENZWEIG, Paul. *Cyber warfare: how conflicts in cyberspace are challenging America and changing the world*. Santa Barbara, Calif.: Praeger, 2013, xi, 290 p. ISBN 9780313398964.

SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. Pro praxi. ISBN 978-80-7380-501-2.

SUMMERS, Sarah J, Christian SCHWARZENEGGER, Gian EGE a Finlay YOUNG. *The emergence of EU criminal law: cybercrime and the regulation of the information society*. Portland, Oregon: Hart Publishing, 2014. Studies in international and comparative criminal law, volume 14. ISBN 978-1-84113-727-8.

SVATOŠ, Roman. *Prevence kriminality*. České Budějovice: Vysoká škola evropských a regionálních studií, 2014. ISBN 978-80-87472-76-7.

ŠÁMAL, Pavel. *Trestní zákoník: komentář – zvláštní část*. 2. vyd. V Praze: C.H. Beck, 2012. Velké komentáře. ISBN 978-80-7400-428-5

VANDUCHOVÁ, Marie a Tomáš GŘIVNA (eds.). *Pocta Otovi Novotnému k 80. narozeninám*. Vyd. 1. Praha: ASPI, 2008, 491 s. ISBN 978-80-7357-365-2.

VARJASSYOVÁ, Martina. *Díla audiovizuální*. Praha, 2009. Diplomová práce. PF UK. Vedoucí práce JUDr. Veronika Křesťanová, Dr.

VIRDZEKOVÁ, Alica. *Trestoprávna úprava internetovej kriminality*. Brno, 2011. Diplomová práca. Právnická fakulta Masarykovy univerzity. Vedoucí práce Doc. JUDr. Josef Kuchta, CSc.

ZEMAN, Daniel. *Počítačová a internetová kriminalita*. Praha, 2011. Diplomová práce. PF UK. Vedoucí práce Doc. JUDr. Tomáš Gřivna, Ph.D.

10.2 Seznam zákonů nejen České republiky

Code Penal, Francouzský trestní zákoník, loi 92-686 du 22 juillet 1992

HADOPI, loi n°2009-669 du 12 juin 2009

Vyhláška č. 488/2006 Sb., kterou se stanoví typy přístrojů k zhotovování rozmnoženin, typy nenahraných nosičů záznamů a výše paušálních odměn

zákon č. 141/1961 Sb. ze dne 29. listopadu 1961 o trestním řízení soudním (trestní řád)

zákon č. 36/1967 Sb. ze dne 6. dubna 1967 o znalcích a tlumočnících

zákon č. 200/1990 Sb. ze dne 17. května1990 o přestupcích

zákon č. 586/1992 Sb. ze dne 20. listopadu 1992 o daních z příjmů

zákon č. 1/1993 Sb. ze dne 16. prosince 1992 Ústava České republiky

zákon č. 2/1993 Sb. ze dne 16. prosince 1992 o vyhlášení Listiny základních práv a svobod (Listina základních práv a svobod)

zákon č. 123/1998 Sb. ze dne 13. května 1998 o právu na informace o životním prostředí

zákon č. 106/1999 Sb. ze dne 11. května 1999 o svobodném přístupu k informacím

zákon č. 121/2000 Sb. ze dne 7. dubna 2000 o právu autorském, o právech souvisejících s právem autorským (autorský zákon)

Zákon č. 361/2000 Sb. ze dne 14. září 2000 o provozu na pozemních komunikacích

zákon č. 365/2000 Sb. ze dne 14. září 2000 o informačních systémech veřejné správy a o změně některých dalších zákonů

zákon č. 480/2004 Sb. ze dne 29. července 2004 o některých službách informační společnosti

zákon č. 127/2005 Sb. ze dne 22. února 2005 o elektronických komunikacích

zákon č. 40/2009 Sb. ze dne 8. ledna 2009 trestní zákoník

zákon č. 418/2011 Sb. ze dne 3. února 2012 o trestní odpovědnosti právnických osob a řízení proti nim

zákon č. 89/2012 Sb. ze dne 3. února 2012 občanský zákoník

zákon č. 181/2014 Sb. ze dne 23. července 2014 o kybernetické bezpečnosti

(zákony České republiky citované v této práci jsou v jejich původním označení, ale chápány jsou ve znění pozdějších předpisů)

10.3 Seznam mezinárodních právních předpisů a předpisů ES / EU

Bernská úmluva o ochraně literárních a uměleckých děl z 9.9.1886, doplněná v Paříži dne 4. května 1896, revidovaná v Berlíně dne 13. listopadu 1908, doplněná v Bernu dne 20. března 1914 a revidovaná v Římě dne 2. června 1928, v Bruselu dne 26. června 1948, ve Stockholmu dne 14. července 1967 a v Paříži dne 24. července 1971 (viz. vyhl.č. 133/1980 Sb.), ve znění změny ze dne 28.9. 1979 (viz vyhl. č. 19/1985 Sb.)

Dohoda o obchodních aspektech práv k duševnímu vlastnictví, která je jednou z příloh Dohody o zřízení Světové obchodní organizace (WTO) – viz sděl. č. 191/1995 Sb., (TRIPS – Trade Related Aspects of Intellectual Property Rights)

Konsolidované znění Smlouvy o Evropské unii a Smlouvy o fungování Evropské unie - Smlouva o Evropské unii (konsolidované znění) - Smlouva o fungování Evropské unie (konsolidované znění) - Protokoly - Přílohy - Prohlášení připojená k závěrečnému aktu mezivládní konference, která přijala Lisabonskou smlouvu podepsanou dne 13. prosince 2007

Mezinárodní úmluva o ochraně výkonných umělců, výrobců zvukových záznamů a rozhlasových organizací ze dne 26. října 1961 (vyhl. č. 192/1964 Sb., ve znění opravy č. 157/1965 Sb.) – Římská úmluva

Nařízení Evropského parlamentu a Rady (EU) č. 608/2013 ze dne 12. června 2013 o vymáhání práv duševního vlastnictví celními orgány a o zrušení nařízení Rady (ES) č. 1383/2003

Rámcové rozhodnutí rady 2001/413/SVV ze dne 28. 5. 2001 o potírání podvodů a padělání bezhotovostních platebních prostředků

Rámcové rozhodnutí Rady 2005/222/SVV ze dne 24:2:2005 o útocích proti informačním systémům – posun ke směrnici Evropského parlamentu a Rady 2013/40/EU

Rozhodnutí rady 92/242/EHS ze dne 31. 3. 1992 o bezpečnosti informačních systémů

Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. 6. 2000 o některých právních aspektech služeb informační společnosti, zejména na elektronickém obchodu na vnitřním trhu (směrnice o elektronickém obchodu)

Směrnice Evropského parlamentu a Rady 2001/29/ES ze dne 22. května 2001 o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti

Směrnice Evropského parlamentu a Rady 2009/24/ES ze dne 23. 4. 2009 o právní ochraně počítačových programů

Směrnice Evropského parlamentu a Rady 2013/40/EU, o útocích proti informačním systémům

Směrnice Evropského parlamentu a Rady 2014/26/EU ze dne 26. února 2014 o kolektivní správě autorského práva a práv s ním souvisejících a udělování

licencí pro více území k právům k užití hudebních děl online na vnitřním trhu

Smlouva Světové organizace duševního vlastnictví o právu autorském vyhlášena pod číslem 33/2002 Sb.m.s.

Smlouva Světové organizace duševního vlastnictví o právu autorském Ženeva 1996 ze dne 20. prosince 1996 (viz sděl. 33/2002 Sb. m. s.), (WCT – WIPO Copyright Treaty)

Smlouva Světové organizace duševního vlastnictví o výkonech výkonných umělců a o zvukových záznamech Ženeva 1996 ze dne 20. prosince 1996 (viz sděl. 48 / 2002 Sb. m. s.), (WPPT – WIPO Performances and Phonograms Treaty)

Úmluva o ochraně výrobců zvukových záznamů proti nedovolenému rozmnožování jejich zvukových záznamů ze dne 29. října 1971 (viz vyhl. 32/1985 Sb.) – Ženevská úmluva

Úmluva o zřízení Světové organizace duševního vlastnictví (WIPO), podepsaná ve Stockholmu dne 14.7.1967, změněná dne 2.10.1979 (vyhl. č. 69/1975 Sb. ve znění vyhl č. 80/1985 Sb.)

Úmluva Rady Evropy č. 185 ze dne 23. 11. 2001 o kybernetické (počítačové) kriminalitě

10.4 Internetové zdroje

"Chovanec je zločin" znělo před ministerstvem vnitra na demonstraci Pirátů. *Lidovky.cz*[online]. 2016 [cit. 2016-03-27]. Dostupné z: http://www.lidovky.cz/pirati-demonstrovali-za-svobodny-internet-fko-/zpravy-domov.aspx?c=A160220_185941_ln_domov_ELE

„Šmírák z Jihlavy“ se psychicky zhroutil. V pondělí dostal podmínku. *Jihlavský deník* [online]. 2014 [cit. 2016-03-01]. Dostupné z: http://jihlavsky.denik.cz/zlociny-a-soudy/smirak-z-jihlavy-se-psychicky-zhroutil-v-pondeli-dostal-podminku-20140513.html

ACTA skončila. Europoslanci ji definitivně zamítli drtivou většinou. In: *IDNES.cz* [online]. 2012 [cit. 2016-02-03]. Dostupné z: http://technet.idnes.cz/acta-skoncila-europarlament-zamitl-actu-fdq-/sw_internet.aspx?c=A120704_132333_sw_internet_pka

Adware. In: *Wikipedia: the free encyclopedia* [online]. 2015 [cit. 2016-03-20]. Dostupné z: https://cs.wikipedia.org/wiki/Adware

BEZPEČNOST A TECHNOLOGIE KOMUNIKACE. *Mup.cz* [online]. 2016 [cit. 2016-03-27]. Dostupné z: http://www.mup.cz/btk/

Británie se vrací do středověku a kopie hudby pro osobní potřebu je (znovu) nezákonná.*Wordpress.com* [online]. 2015 [cit. 2016-03-13]. Dostupné z: https://rychlofky.wordpress.com/2015/07/17/britanie-se-vraci-do-stredoveku-a-kopie-hudby-pro-osobni-potrebu-je-znovu-nezakonna/

Cloudové úložiště. *Wiki.ics.muni.cz* [online]. 2015 [cit. 2016-02-14]. Dostupné z: https://wiki.ics.muni.cz/cloudove_uloziste

Co je ICT? *Zkusit.cz* [online]. 2010 [cit. 2016-02-21]. Dostupné z: http://www.zkusit.cz/proc-zkusit/co-je-ict.php

CO JE NCKB. *Govcert.cz* [online]. [cit. 2016-03-26]. Dostupné z: http://www.govcert.cz/cs/

Co je softwarové pirátství? *BSA* [online]. [cit. 2016-03-20]. Dostupné z: http://ww2.bsa.org/country.aspx?sc_lang=cs-CZ

Co je to: Spam. *Unet.cz* [online]. 2015 [cit. 2016-02-28]. Dostupné z: https://www.unet.cz/blog/2015/09/15/co-je-to-spam/

Co vyžadují nové předpisy EU o kybernetické bezpečnosti? *Computerworld.cz* [online]. 2015 [cit. 2016-03-27]. Dostupné z: http://computerworld.cz/securityworld/co-vyzaduji-nove-predpisy-eu-o-kyberneticke-bezpecnosti-52594

Česká republika po osmi letech ratifikovala Úmluvu o počítačové kriminalitě. *Ihned.cz* [online]. 2013 [cit. 2016-02-21]. Dostupné z: http://pravniradce.ihned.cz/c1-60516560-ceska-republika-po-osmi-letech-ratifikovala-umluvu-o-pocitacove-kriminalite

Česko se obává kyberútoků. Posílí obranu a přibere IT agenty!. *Tn.cz* [online]. 2016 [cit. 2016-03-26]. Dostupné z: http://tn.nova.cz/clanek/cesko-se-obava-kyberutoku-posili-obranu-a-pribere-it-agenty.html

Češi se vracejí do videopůjčoven, tentokrát on-line. *Ceskatelevize.cz* [online]. 2015 [cit. 2016-03-27]. Dostupné z: http://www.ceskatelevize.cz/ct24/media/1606311-cesi-se-vraceji-do-videopujcoven-tentokrat-line

Datové médium. In: *Wikipedia: the free encyclopedia* [online]. Wikimedia Foundation, 2014 [cit. 2016-02-21]. Dostupné z: https://cs.wikipedia.org/wiki/Datov%C3%A9_m%C3%A9dium

DDoS útoků na české servery přibývá. Loni se jejich počet zdvojnásobil. *Lupa.cz* [online]. 2015 [cit. 2016-02-29]. Dostupné z: http://www.lupa.cz/clanky/ddos-utoku-na-ceske-servery-pribyva-loni-se-jejich-pocet-zdvojnasobil/

Digitální média a pirátství: Audiovizuální pirátství. *Česká protipirátská unie* [online]. 2007 [cit. 2016-03-11]. Dostupné z: http://www.cpufilm.cz/new/www/txt/audiovizualni_piratstvi.pdf.

EU má první směrnici o kybernetické bezpečnosti. Firmy jako Google budou muset hlásit nebezpečné incidenty. *Ihned.cz* [online]. 2015 [cit. 2016-03-27]. Dostupné z: http://zahranicni.ihned.cz/evropa-slovensko/c1-64952760-eu-ma-prvni-smernici-o-kyberneticke-bezpecnosti-internetove-firmy-budou-muset-hlasit-nebezpecne-incidenty

F.A.Q. - Často kladené otázky. *Česká protipirátská unie (ČPU)* [online]. [cit. 2016-03-12]. Dostupné z: http://www.cpufilm.cz/faq.html

Freeware. In: *Wikipedia: the free encyclopedia* [online]. 2015 [cit. 2016-03-20]. Dostupné z: https://cs.wikipedia.org/wiki/Freeware

HÁLEK, Jakub. *Autorské právo a jeho porušování na internetu z pohledu škody, náhrady škody a bezdůvodného obohacení* [online]. Praha, 2015 [cit. 2016-03-24]. Dostupné z: http://svoc.prf.cuni.cz/sources/8/17/519.pdf. SVOČ. PF UK.

How would you define Cyberspace? *Academia.edu* [online]. 2014 [cit. 2016-02-21]. Dostupné z: https://www.academia.edu/7096442/How_would_you_define_Cyberspace

Chtějí vybílit lidem účty, používají k tomu Facebook. *Novinky.cz* [online]. 2016 [cit. 2016-02-29]. Dostupné z: http://www.novinky.cz/internet-a-pc/bezpecnost/395029-chteji-vybilit-lidem-ucty-pouzivaji-k-tomu-facebook.html

Intermet. In: *Wikipedia: the free encyclopedia* [online]. Wikimedia Foundation, 2019 [cit. 2016-02-21]. Dostupné z: https://cs.wikipedia.org/wiki/Internet

Internetová kriminalita roste, policie založí nový útvar. *Aktualne.cz* [online]. 2015 [cit. 2016-02-10]. Dostupné z: http://zpravy.aktualne.cz/domaci/kriminalita-na-internetu-se-od-roku-2011-ztrojnasobila/r~79c4ebd6b10d11e49f60002590604f2e/

Internetová kriminalita. In: *Pcworld.cz* [online]. 2004 [cit. 2016-02-09]. Dostupné z: http://pcworld.cz/internet/internetova-kriminalita-14612

Jaká je odpovědnost provozovatelů internetových úložišť za obsah uložený jejich uživateli? Odpověď na tuto otázku je třeba hledat jak v českém, tak v evropském právu. *Idnes.cz*[online]. 2013 [cit. 2016-03-13]. Dostupné z: http://finance.idnes.cz/odpovednost-provozovatelu-internetovych-ulozist-fxr-/pravo.aspx

Je stahování pirátského obsahu z webu legální? *Lupa.cz* [online]. 2014 [cit. 2016-03-12]. Dostupné z: http://www.lupa.cz/clanky/je-stahovani-piratskeho-obsahu-z-webu-legalni/

Kreml chce za bitcoiny posílat až na čtyři roky do vězení. Je to prý prostředek pro zločince. *Ihned.cz* [online]. 2016 [cit. 2016-03-27]. Dostupné z: http://archiv.ihned.cz/c1-65205180-kreml-chce-za-bitcoiny-posilat-do-vezeni

Kriminalita v ČR loni klesla, stalo se nejméně vražd od roku 2000. *Ceskenoviny.cz* [online]. 2016 [cit. 2016-02-10]. Dostupné z: http://www.ceskenoviny.cz/zpravy/kriminalita-v-cr-loni-klesla-stalo-se-nejmene-vrazd-od-roku-2000/1304705

Kybernetická kriminalita - fenomén dneška. *Pravniprostor.cz* [online]. 2015 [cit. 2016-02-21]. Dostupné z: http://www.pravniprostor.cz/clanky/trestni-pravo/kyberneticka-kriminalita-fenomen-dneska

Kybernetická kriminalita v judikatuře českých soudů. GŘIVNA, Tomáš. *Docplayer.cz* [online]. 2015 [cit. 2016-03-14]. Dostupné z: http://docplayer.cz/3912001-Kyberneticka-kriminalita-v-judikature-ceskych-soudu-doc-judr-tomas-grivna-ph-d-pravnicka-fakulta-uk-v-praze.html

Kyberprostor. In: *Wikipedia: the free encyclopedia* [online]. 2015 [cit. 2016-02-21]. Dostupné z: https://cs.wikipedia.org/wiki/Kyberprostor

MENDEL, Aleš. *Technická a infrastrukturní počítačová kriminalita* [online]. Brno, 2008 [cit. 2016-03-24]. Dostupné z: https://is.muni.cz/th/328211/pravf_r/rigorozni_prace.pdf. Rigorózní práce. Právnická fakulta Masarykovy univerzity.

Na českém internetu přibývá podvodů. Loni škoda překročila miliardu korun. *Ihned.cz* [online]. 2015 [cit. 2016-02-10]. Dostupné z: http://archiv.ihned.cz/c1-63664110-na-ceskem-internetu-pribyva-podvodu-loni-skoda-prekrocila-miliardu-korun

Na Slovensku odhalili manipulace s registračními pokladnami, jde o miliardy. *Novinky.cz*[online]. 2016 [cit. 2016-03-27]. Dostupné z: http://www.novinky.cz/ekonomika/397422-na-slovensku-odhalili-manipulace-s-registracnimi-pokladnami-jde-o-miliardy.html

Nad piráty se i v Čechách stahují mračna: Moderátor Nerez byl za nelegální uploady odsouzen. *Kinobox.cz* [online]. 2012 [cit. 2016-03-24]. Dostupné z: http://www.kinobox.cz/clanek/7059-moderator-nerez-odsouzen

Národní bezpečnostní úřad. In: *Wikipedia: the free encyclopedia* [online]. 2015 [cit. 2016-03-26]. Dostupné z: https://cs.wikipedia.org/wiki/N%C3%A1rodn%C3%AD_bezpe%C4%8Dnostn%C3%AD_%C3%BA%C5%99ad

Nelegální obsah sami nehledáme, smažeme ho až po stížnosti, říká spolumajitel Ulož.to.*Ihned.cz* [online]. 2012 [cit. 2016-03-12]. Dostupné z: http://byznys.ihned.cz/c1-54928870-nelegalni-obsah-sami-nehledame-smazeme-ho-az-po-stiznosti-rika-spolumajitel-uloz-to

Odpovědnost za porušení autorského práva. *Česká protipirátská unie (ČPU)* [online]. [cit. 2016-03-12]. Dostupné z: http://www.cpufilm.cz/new/www/odpovednost.html

OEM produkce. In: *Wikipedia: the free encyclopedia* [online]. 2015 [cit. 2016-03-20]. Dostupné z: https://cs.wikipedia.org/wiki/OEM_produkce

Otevřený software. In: *Wikipedia: the free encyclopedia* [online]. 2015 [cit. 2016-03-20]. Dostupné z: https://cs.wikipedia.org/wiki/Otev%C5%99en%C3%BD_software

Peer-to-peer. In: *Wikipedia: the free encyclopedia* [online]. 2015 [cit. 2016-02-22]. Dostupné z: https://cs.wikipedia.org/wiki/Peer-to-peer

Pět let francouzského „třikrát a dost“. *Linuxexpres.cz* [online]. 2015 [cit. 2016-03-26]. Dostupné z: http://www.linuxexpres.cz/novinky/pet-let-francouzskeho-trikrat-a-dost

Pharming. In: *Wikipedia: the free encyclopedia* [online]. 2015 [cit. 2016-02-28]. Dostupné z: https://cs.wikipedia.org/wiki/Pharming

Pirátské vánoce: Na internet unikla bezprecedentní halda filmů včetně Osmi hrozných od Tarantina. *Reflex.cz* [online]. 2015 [cit. 2016-03-25]. Dostupné z: http://www.reflex.cz/clanek/kultura/68238/piratske-vanoce-na-internet-unikla-bezprecedentni-halda-filmu-vcetne-osmi-hroznych-od-tarantina.html

Počet DDoS útoků vzrostl o 180%. *Kyberbezpecnost.cz* [online]. 2015 [cit. 2016-02-29]. Dostupné z: http://www.kyberbezpecnost.cz/?p=5701

Počítačová kriminalita [online]. s. 40-50 [cit. 2016-03-25]. Dostupné z: https://theses.cz/id/zctjxg/Diplomova__prace_cast_2.pdf

Počítačový pirát Nerez nabízel ke stažení tisíce filmů, dostal podmínku. *Idnes.cz* [online]. 2012 [cit. 2016-03-24]. Dostupné z: http://zpravy.idnes.cz/soud-s-pocitacovym-piratem-miroslavem-ocelikem-f5v-/krimi.aspx?c=A120523_162415_zlin-zpravy_sot

POČÍTAČOVÝ PIRÁT UŽ SI TREST ODPRACOVAL. KAJÍCNÉ VIDEO VIDĚL MILION LIDÍ. *Respekt.cz*[online]. 2015 [cit. 2016-03-24]. Dostupné z: http://www.respekt.cz/spolecnost/pocitacovy-pirat-uz-si-trest-odpracoval-kajicne-video-videl-milion-lidi

Pojištění kybernetických rizik. *Vitovec.cz* [online]. 2016 [cit. 2016-03-27]. Dostupné z: http://www.vitovec.cz/pojisteni-kybernetickych-rizik

Poznejte druhotný software. *Vyhodny-software.cz* [online]. 2013 [cit. 2016-03-21]. Dostupné z: http://www.vyhodny-software.cz/pro-media/poznejte-druhotny-software/

PRÁVNÍ ASPEKTY P2P. *Ifpi.cz* [online]. 2015 [cit. 2016-03-13]. Dostupné z: http://www.ifpi.cz/pravni-aspekty-p2p/

Právní aspekty prodeje použitého softwaru. *Systemonline.cz* [online]. 2007 [cit. 2016-03-21]. Dostupné z: http://www.systemonline.cz/sprava-it/pravni-aspekty-prodeje-pouziteho-softwaru.htm

Právní aspekty přijetí zákona o kybernetické bezpečnosti. *Systemonline.cz* [online]. 2015 [cit. 2016-03-26]. Dostupné z: http://www.systemonline.cz/clanky/pravni-aspekty-prijeti-zakona-o-kyberneticke-bezpecnosti.htm

Retail verze softwaru. In: *Wikipedia: the free encyclopedia* [online]. 2015 [cit. 2016-03-20]. Dostupné z: https://cs.wikipedia.org/wiki/Retail_verze_softwaru

Rozsudek Soudního dvora EU C-360/13 se významným způsobem vztahuje i ke službám informační společnosti a zaručení jejich ochrany. *Ministerstvo průmyslu a obchodu* [online]. 2014 [cit. 2016-03-19]. Dostupné z: http://www.mpo.cz/dokument150669.html

Senát schválil evidenci tržeb. *Eltrzby.cz* [online]. 2016 [cit. 2016-03-27]. Dostupné z: http://www.eltrzby.cz/cz/aktuality/85-senat-schvalil-evidenci-trzeb

Seznamte se – DoS a DDoS útoky. *Security-portal.cz* [online]. 2013 [cit. 2016-03-04]. Dostupné z: http://www.security-portal.cz/clanky/seznamte-se-%E2%80%93-dos-ddos-%C3%BAtoky

Shareware. In: *Wikipedia: the free encyclopedia* [online]. 2015 [cit. 2016-03-20]. Dostupné z: https://cs.wikipedia.org/wiki/Shareware

Sniffing. *Sprava-site.eu* [online]. [cit. 2016-02-28]. Dostupné z: http://www.sprava-site.eu/sniffing/

Sociální síť. In: *Wikipedia: the free encyclopedia* [online]. 2016 [cit. 2016-02-22]. Dostupné z: https://cs.wikipedia.org/wiki/Soci%C3%A1ln%C3%AD_s%C3%AD%C5%A5

Software. In: *Wikipedia: the free encyclopedia* [online]. Wikimedia Foundation, 2015 [cit. 2016-02-15]. Dostupné z: https://cs.wikipedia.org/wiki/Software

Soud se zastal internetového piráta, který měl platit vysokou škodu. *E15.cz* [online]. 2015 [cit. 2016-03-24]. Dostupné z: http://e-svet.e15.cz/it-byznys/soud-se-zastal-internetoveho-pirata-ktery-mel-platit-vysokou-skodu

Spamů ubylo, jejich podíl byl nejnižší za dvanáct let. *Aktualne.cz* [online]. 2015 [cit. 2016-02-28]. Dostupné z: http://zpravy.aktualne.cz/ekonomika/spamu-ubylo-jejich-podil-byl-nejnizsi-za-dvanact-let/r~cd41ff1e2dd211e5ae1b002590604f2e/

Stahovat data z nelegálního zdroje není povolené. *Stance.cz* [online]. 2015 [cit. 2016-03-12]. Dostupné z: http://www.stance.cz/stahovat-data-z-nelegalniho-zdroje-neni-povolene-ani-pro-osobni-potrebu-rikaji-odbornici-z-taylorwessing-enwc-advokati-1370/

Svěrák porazil piráty. *Objevit.cz* [online]. 2013 [cit. 2016-03-24]. Dostupné z: http://objevit.cz/sverak-porazil-piraty-t29809

Šarapovová přichází o miliony, na početný tým vinu nesvádí. *Rozhlas.cz* [online]. 2016 [cit. 2016-03-27]. Dostupné z: http://www.rozhlas.cz/zpravy/tenis/_zprava/sarapovova-prichazi-o-miliony-na-pocetny-tym-vinu-nesvadi--1591744

Špehoval nájemníky při sexu! Dostal 2,5 roku a zaplatí 130 tisíc!. *TN.cz* [online]. 2014 [cit. 2016-03-01]. Dostupné z: http://tn.nova.cz/clanek/za-spehovani-najemniku-dostal-dva-a-pul-roku-zaplati-jim-130-tisic.html

Téměř 90 % e-mailů jsou spamy. *Isvs.cz* [online]. 2007 [cit. 2016-02-28]. Dostupné z: http://2011-2015.isvs.cz/temer-90-e-mailu-jsou-spamy/

Trestněprávní odpovědnost za pořízení rozmnoženiny autorského díla pro osobní potřebu z nelegálního zdroje. *Davidzahumensky.cz* [online]. 2015 [cit. 2016-03-13]. Dostupné z: http://www.davidzahumensky.cz/2014/05/28/trestnepravni-odpovednost-za-porizeni-rozmnozeniny-autorskeho-dila-pro-osobni-potrebu-z-nelegalniho-zdroje/

Týdny s Office - Office 365 a instalace Office Click-to-Run. *Optimalizovane-it.cz* [online]. 2015 [cit. 2016-03-21]. Dostupné z: http://www.optimalizovane-it.cz/technet-cz/sk/tydny-s-office-office-365-a-instalace-office-click-to-run.html

UK: Copyright – private copying exception falls. *Bird and Bird Lawyers* [online]. London, 2015 [cit. 2016-03-13]. Dostupné z: http://www.twobirds.com/en/news/articles/2015/uk/copyright-private-copying-exception-falls

Úspěch podnikatelského nápadu není zaručen na věky. *Ipodnikatel.cz* [online]. 2011 [cit. 2016-03-27]. Dostupné z: http://www.ipodnikatel.cz/Hledani-podnikatelskeho-napadu/uspech-podnikatelskeho-napadu-neni-zarucen-na-veky.html

Ušlý zisk. *Epravo.cz* [online]. 2002 [cit. 2016-03-06]. Dostupné z: http://www.epravo.cz/top/clanky/usly-zisk-15607.html

Úvod. *Csirt.cz* [online]. [cit. 2016-03-26]. Dostupné z: https://csirt.cz/

V Česku padl první nepodmíněný trest za softwarové pirátství. *Ceskatelevize.cz* [online]. 2013 [cit. 2016-03-25]. Dostupné z: http://www.ceskatelevize.cz/ct24/domaci/1059807-v-cesku-padl-prvni-nepodmineny-trest-za-softwarove-piratstvi

Ve Francii začal platit protipirátský zákon „HADOPI". *Itbiz.cz* [online]. 2010 [cit. 2016-03-26]. Dostupné z: http://www.itbiz.cz/zakon-hadopi-zacal-platit

Velký přehled cloudových úložišť. *Wordpress.com* [online]. 2015 [cit. 2016-02-14]. Dostupné z: https://365tipu.wordpress.com/2015/07/06/tip187-velky-prehled-cloudovych-ulozist-aneb-dropbox-onedrive-box-net-a-ti-dalsi/

Warez. *Superia.cz* [online]. 2015 [cit. 2016-02-22]. Dostupné z: http://cojeto.superia.cz/internet/warez.php

Z bitcoinu se možná stane legální měna. Japonsko uvažuje o zdanění. *Novinky.cz* [online]. 2016 [cit. 2016-03-27]. Dostupné z: http://www.novinky.cz/internet-a-pc/395970-z-bitcoinu-se-mozna-stane-legalni-mena-japonsko-uvazuje-o-zdaneni.html

Za poslední roky se kybernetická kriminalita ztrojnásobila. *Ceskatelevize.cz* [online]. 2015 [cit. 2016-02-10]. Dostupné z: http://www.ceskatelevize.cz/ct24/domaci/1501646-za-posledni-roky-se-kyberneticka-kriminalita-ztrojnasobila

Zaplaťte 14 Kč za každý gigabajt: Maďarsko plánuje zdanit internet. *Idnes.cz* [online]. 2014 [cit. 2016-03-26]. Dostupné z: http://technet.idnes.cz/madarsko-planuje-zdanit-internet-dqv-/sw_internet.aspx?c=A141022_172733_sw_internet_pka

10.5 Periodika

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

GŘIVNA, T.; HERCZEG, J. Právo na přístup k Internetu, blokace stránek a digitální gilotina. *Trestněprávní revue*. 2010, roč. 9, č. 05, s. 141-146. ISSN 1213-5313.

VOLEVECKÝ, Petr. Kybernetické hrozby a jejich trestně právní kvalifikace (dokončení z čísla 12/2010). *Trestní právo*. 2011, 15(1), 11-23. ISSN 12112860.

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

10.6 Judikatura

Nález Ústavního soudu ze dne 14. března 2002, sp. zn. III. ÚS 346/01

Nález Ústavního soudu ze dne 30. dubna 2002, sp. zn. ÚS Pl. ÚS 18/01

Nález Ústavního soudu ze dne 20. dubna 2007, sp. zn. III. ÚS 299/06

Nález Ústavního soudu ze dne 20. srpna 2013, sp. zn. I. ÚS 1428/13

Rozsudek Krajského soudu v Brně ze dne 27. října 2010, sp. zn. 3 To 478/2010

Rozsudek Nejvyššího soudu ze dne 17. ledna 2001, sp. zn. 8 Tz 287/2000

Rozsudek Nejvyššího soudu ze dne 28. listopadu 2001, sp. zn. 25 Cdo 1920/99

Rozsudek Nejvyššího soudu ze dne 5. listopadu 2008 sp. zn. 32 Cdo 3629/2008

Rozsudek Nejvyššího soudu ze dne 28. ledna 2009, sp. zn. 25 Cdo 3586/2006

Rozsudek Nejvyššího soudu ze dne 13. listopadu 2012, sp. zn. 4 Tz 77/2012

Rozsudek Soudního dvora EU C-128/11 ze dne 3. července 2012

Rozsudek Soudního dvora EU C-607/11 ze dne 7. března 2013

Rozsudek Soudního dvora EU C-466/12 ze dne 13. února 2014

Rozsudek Soudního dvora EU C-435/12 ze dne 10. dubna 2014

Rozsudek Soudního dvora EU C-360/13 ze dne 5. června 2014

Usnesení Nejvyššího soudu ze dne 16. května 2007, sp. zn. 5 Tdo 538/2007

Usnesení Nejvyššího soudu ze dne 16. července 2008, sp. zn. 3 Tdo 848/2008

Usnesení Nejvyššího soudu ze dne 25. března 2009, sp. zn. 5 Tdo 234/2009

Usnesení Nejvyššího soudu ze dne 23. června 2010, sp. zn. 3 Tdo 1483/2010

Usnesení Nejvyššího soudu ze dne 11. dubna 2012, sp. zn. 5 Tdo 275/2012

Usnesení Nejvyššího soudu ze dne 12. prosince 2012, sp. zn. 6 Tdo 1372/2012

Usnesení Nejvyššího soudu ze dne 27. února 2013, sp. zn. 8 Tdo 137/2013

Usnesení Nejvyššího soudu ze dne 29. května 2013, sp. zn. 5 Tdo 271/2013

Usnesení Nejvyššího soudu ze dne 11. prosince 2013, sp. zn. 4 Tdo 1315/2013

Usnesení Nejvyššího soudu ze dne 26. března 2014, sp. zn. 5 Tdo 62/2014

Usnesení Nejvyššího soudu ze dne 8. října 2014, sp. zn. 5 Tdo 171/2014

Usnesení Nejvyššího soudu ze dne 12. listopadu 2014, sp. zn. 5 Tdo 1136/2014

Usnesení Soudního dvora EU C-348/13 ze dne 21. října 2014

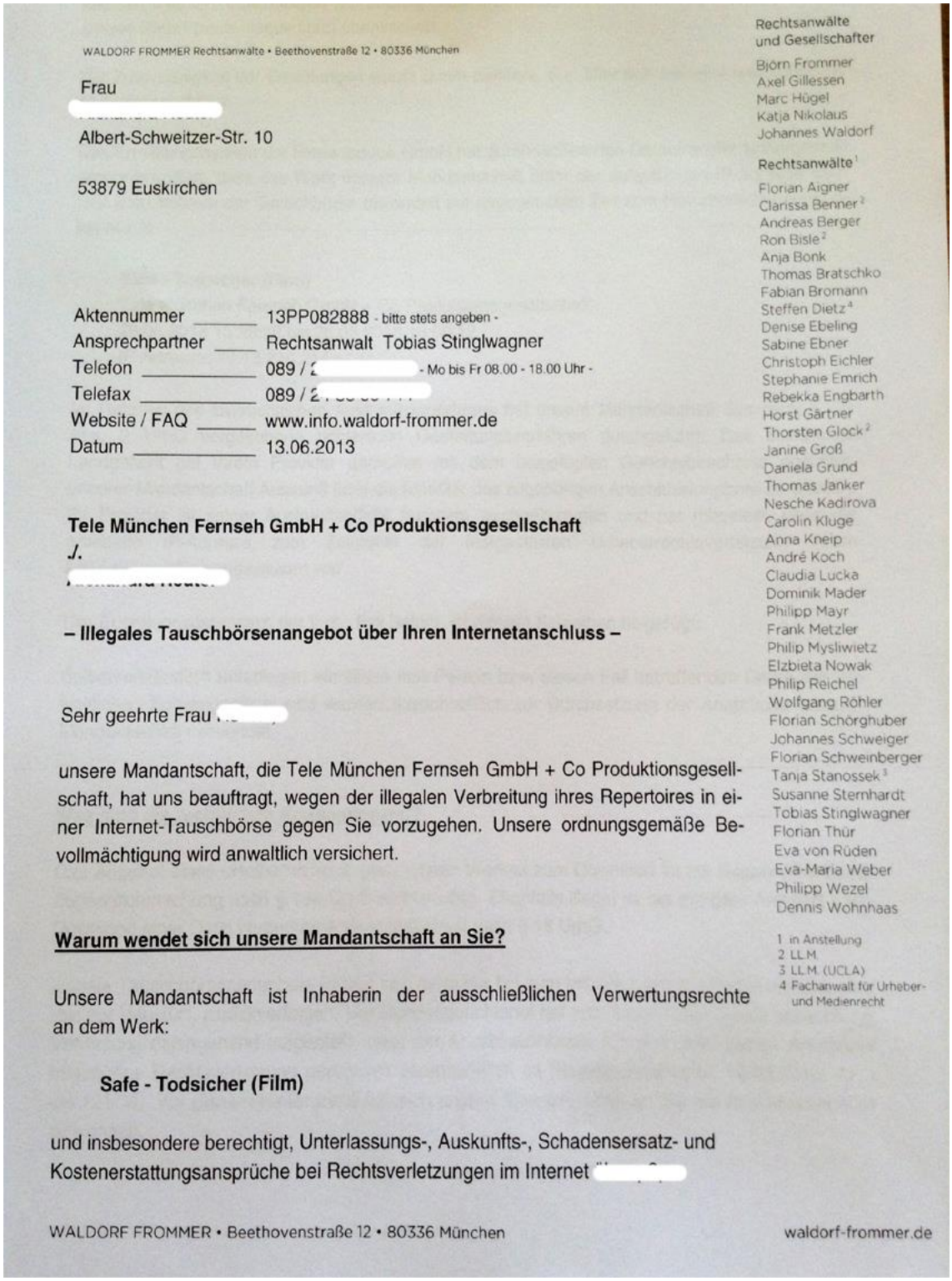
Usnesení Ústavního soudu ze dne 28. března 2002, sp. zn. IV.ÚS 2/02

Usnesení Ústavního soudu ze dne 10. září 2013, sp. zn. III.ÚS 1768/13

Žádost o rozhodnutí o předběžné otázce podaná Hoge Raad der Nederlanden (Nizozemsko) dne 7. dubna 2015 – GS Media BV v. Sanoma Media Netherlands BV a další (věc C-160/15).

Přílohy

Příloha č. 1 – A



WALDORF FROMMER Rechtsanwälte • Beethovenstraße 12 • 80336 München

Frau
[redacted]
Albert-Schweitzer-Str. 10

53879 Euskirchen

Aktennummer _____ 13PP082888 - bitte stets angeben -
Ansprechpartner ____ Rechtsanwalt Tobias Stinglwagner
Telefon _____ 089 / [redacted] - Mo bis Fr 08.00 - 18.00 Uhr -
Telefax _____ 089 / [redacted]
Website / FAQ _____ www.info.waldorf-frommer.de
Datum _____ 13.06.2013

Tele München Fernseh GmbH + Co Produktionsgesellschaft
./.
[redacted]

– Illegales Tauschbörsenangebot über Ihren Internetanschluss –

Sehr geehrte Frau [redacted]

unsere Mandantschaft, die Tele München Fernseh GmbH + Co Produktionsgesellschaft, hat uns beauftragt, wegen der illegalen Verbreitung ihres Repertoires in einer Internet-Tauschbörse gegen Sie vorzugehen. Unsere ordnungsgemäße Bevollmächtigung wird anwaltlich versichert.

Warum wendet sich unsere Mandantschaft an Sie?

Unsere Mandantschaft ist Inhaberin der ausschließlichen Verwertungsrechte an dem Werk:

Safe - Todsicher (Film)

und insbesondere berechtigt, Unterlassungs-, Auskunfts-, Schadensersatz- und Kostenerstattungsansprüche bei Rechtsverletzungen im Internet [redacted]

WALDORF FROMMER • Beethovenstraße 12 • 80336 München waldorf-frommer.de

Rechtsanwälte und Gesellschafter
Björn Frommer
Axel Gillessen
Marc Hügel
Katja Nikolaus
Johannes Waldorf

Rechtsanwälte[1]
Florian Aigner
Clarissa Benner[2]
Andreas Berger
Ron Bisle[2]
Anja Bonk
Thomas Bratschko
Fabian Bromann
Steffen Dietz[4]
Denise Ebeling
Sabine Ebner
Christoph Eichler
Stephanie Emrich
Rebekka Engbarth
Horst Gärtner
Thorsten Glock[2]
Janine Groß
Daniela Grund
Thomas Janker
Nesche Kadirova
Carolin Kluge
Anna Kneip
André Koch
Claudia Lucka
Dominik Mader
Philipp Mayr
Frank Metzler
Philip Mysliwietz
Elzbieta Nowak
Philip Reichel
Wolfgang Röhler
Florian Schörghuber
Johannes Schweiger
Florian Schweinberger
Tanja Stanossek[3]
Susanne Sternhardt
Tobias Stinglwagner
Florian Thür
Eva von Rüden
Eva-Maria Weber
Philipp Wezel
Dennis Wohnhaas

1 in Anstellung
2 LL.M.
3 LL.M. (UCLA)
4 Fachanwalt für Urheber- und Medienrecht

Příloha č. 1 – B

streitwert) angemessen. Die zu erstattende Geschäftsgebühr liegt unterhalb der gesetzlichen Regelgebühr. Die Gebühren sind nicht nach § 97a Abs. 2 UrhG zu begrenzen, da es sich vorliegend bereits um keine nur unerhebliche Rechtsverletzung handelt.

Bei außergerichtlicher Klärung belaufen sich die von Ihnen geschuldeten Rechtsverfolgungskosten inklusive Auslagenpauschale auf **EUR 506,00**.

- Konkrete Zahlungshöhe -

Insgesamt beläuft sich die Forderung unserer Mandantschaft auf einen Betrag von **EUR 956,00**, der sich aus folgenden Einzelbeträgen zusammensetzt:

Schadenersatz	EUR	450,00
Rechtsanwaltskosten	EUR	506,00
Gesamtsumme	**EUR**	**956,00**

- Zu beachtende Fristen -

Die **Frist** zum **Eingang der Unterlassungserklärung** endet am	**24.06.2013.**
Die **Zahlungsfrist** endet am	**03.07.2013.**

Die unterzeichnete Unterlassungserklärung muss bis spätestens zum angegebenen Zeitpunkt hier eingegangen sein. Die Zahlung muss ebenfalls bis spätestens zum genannten Zeitpunkt auf dem Konto der Kanzlei als Empfangsvertreter eingegangen sein. Um eine reibungslose Zuordnung Ihrer Zahlung gewährleisten zu können, verwenden Sie zur Zahlung bitte den **beiliegenden Überweisungsträger**.

Wann ist die Auseinandersetzung beendet?

Mit fristgerechtem Eingang der Unterlassungserklärung sowie vollständiger Zahlung der offenen Forderung sind sämtliche Ansprüche unserer Mandantschaft in vollem Umfang erledigt und die vorliegende juristische Auseinandersetzung mit Ihnen vollständig beendet.

Wo finde ich weitere Informationen?

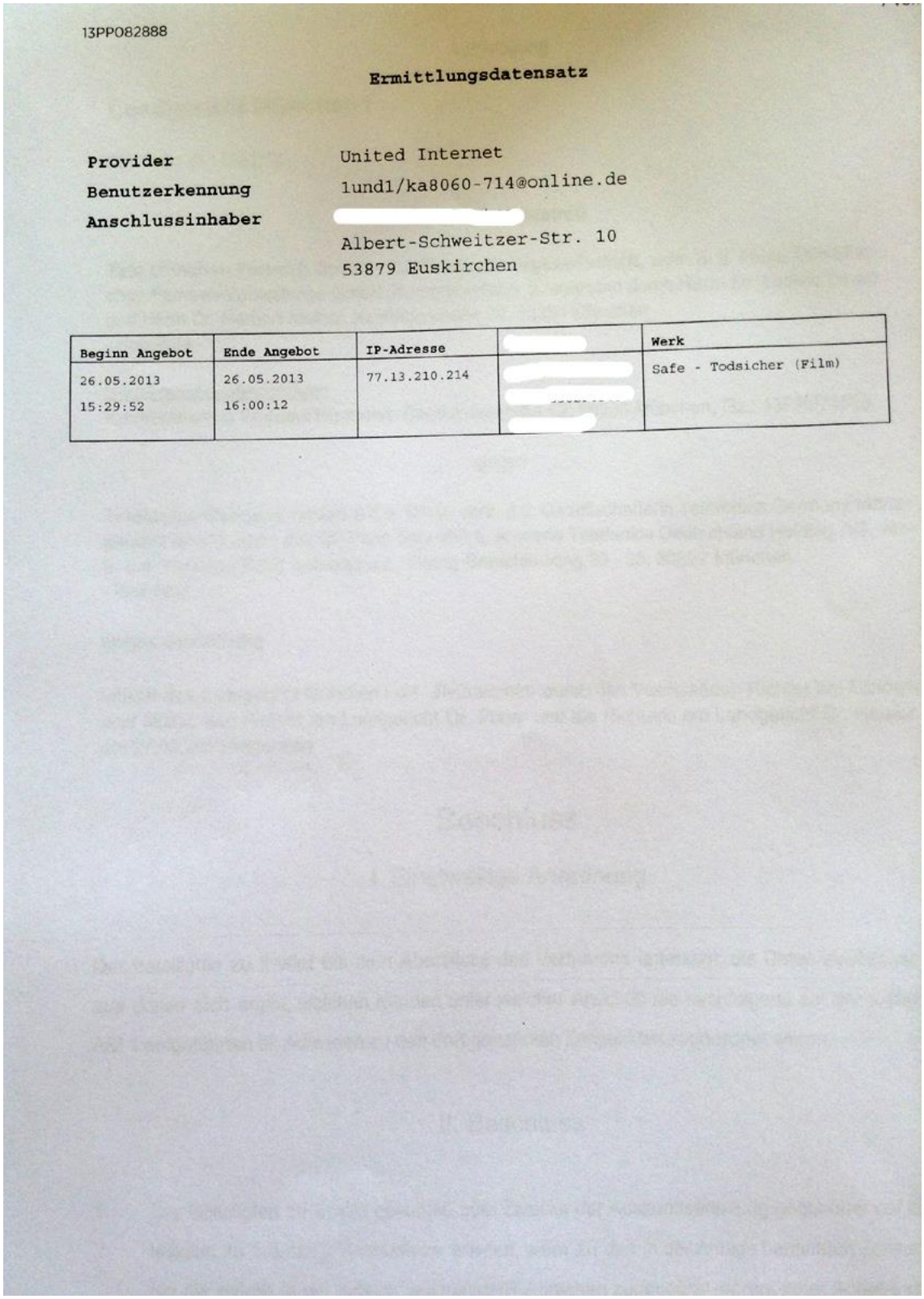
Informationen zu aktuellen Gerichtsverfahren der Kanzlei sowie Antworten auf häufig gestellte Fragen finden Sie unter

www.info.waldorf-frommer.de

Gern stehen wir Ihnen auch telefonisch zur Verfügung:

089 / 24 88 99 010

Příloha č. 1 – C



13PP082888

Ermittlungsdatensatz

Provider	United Internet
Benutzerkennung	1und1/ka8060-714@online.de
Anschlussinhaber	[redacted]
	Albert-Schweitzer-Str. 10
	53879 Euskirchen

Beginn Angebot	Ende Angebot	IP-Adresse	[redacted]	Werk
26.05.2013 15:29:52	26.05.2013 16:00:12	77.13.210.214	[redacted]	Safe - Todsicher (Film)

Příloha č. 2 – A (zdroj http://www.cpufilm.cz/rozsudky.html)

Spisová značka: **6 T 46/2007**

Toto rozhodnutí nabylo právní moci:
25. 5. 2007
OKRESNÍ SOUD V MOSTĚ
dne 9. května 2007

POLICIE ČR – okresní ředitelství
služba kriminální policie a vyšetřování
434 75 Most
Došlo: 15. V. 2007
Č. j.:
Přílohy:

ČESKÁ REPUBLIKA

TRESTNÍ PŘÍKAZ

Samosoudce Okresního soudu v Mostě vydal dne 22.3.2007 v Mostě podle § 314e odst. 1 tr. řádu následující **t r e s t n í p ř í k a z :**

Obviněný

M Z ,

nar. 1988 v Mostě, bytem trvale Most, ,

j e v i n e n , ž e

1) dne 12.3.2006 v kině Cinema City Flora v paláci Flora v Praze 3, ul. Vinohradská čp. 130, při promítání filmu „Rafťáci" pořídil kamerou bez souhlasu vlastníka práv k tomuto filmu, spol. Cinemania s.r.o. Praha 2, nelegální záznam tohoto filmu, který poté převedl ve svém počítači v místě svého trvalého bydliště v Mostě, , do souboru s názvem „Raftaci_CAM_by_b-s-h.wmv", a dne 13.3.2006 ho nabídnul ke stažení na veřejnou počítačovou síť Internet a tento soubor s výše uvedeným filmem zpřístupnil neomezenému množství dalších osob a v následujících dnech opakovaně zveřejňoval na internetu odkazy na webové stránky, z nichž bylo možno jím natočený a upravený film kopírovat,

2) v době od 12.1.2006 do 30.4.2006 měl ve svém počítači umístěném v místě svého bydliště v Mostě, , vědomě nainstalovány k užívání počítačové programy Adobe Photoshop v7.0 CE Czech, Dreamweaver 4, Dreamweaver MX, Microsoft Office Professional Edition 2003, Microsoft Windows XP Professional, Norton Internet Security 2005, Auto CAD 2006 Z.54.10, Avast! Antivirus Professional v.4.6, Borland C++ Application Frameworks 3.1, MOBILedit! 2.00, Total Commander v.6.03a, Autoškola professional 20.2, Autoškola professional 2002 v11.2, Autoškola professional v20.5, Autoškola professional 2002 11.9, PC Translator 2005 a HALF-LIFE COUNTERSTRIKE, aniž by získal právo k jejich instalaci koupí příslušných licencí od společností ADOBE SYSTEMS INCORPORATED, 345 Park Avenue, San Jose, California USA, MICROSOFT INC., One Microsoft Way, Redmont, USA, SYMANTEC CORPORATION, 20330 Stevens Creek Blvd., Cupertino, California, USA, AUTODESK INC., 111 McInnis Parkway, San

Příloha č. 2 – B (zdroj http://www.cpufilm.cz/rozsudky.html)

Rafael, California, USA, ALWIL Software, Praha 10, BORLAND spol. s.r.o., Praha 4, COMPELSON Trade, spol. s.r.o. Praha 9, JIMAZ, spol. s r.o., Praha 7, Bc. Jana Dobeše, Dačice, a LangSoft spol. s.r.o. Korytná, přičemž těmto vlastníkům autorských práv ke shora uvedenému komerčnímu software způsobil škodu ve výši 248.750,- Kč,

t e d y neoprávněně zasáhl do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovanému záznamu,

č í m ž s p á c h a l

trestný čin porušování autorského práva, práv souvisejících s právem autorským a práv k databázi podle § 152 odst. 1 tr. zákona,

a o d s u z u j e s e

Podle § 152 odst. 1 tr. zákona s přihlédnutím k § 314e odst. 2 tr. řádu k trestu odnětí svobody v trvání **t ř í /3/** měsíců.

Podle § 58 odst. 1 a § 59 odst. 1 tr. zákona se výkon tohoto trestu podmíněně odkládá a stanoví se zkušební doba na **j e d e n /1/** rok.

Podle § 55 odst. 1 písm. a) tr. zákona se obviněnému zároveň ukládá **trest propadnutí věci**, a to 1 ks počítačové skříně šedé (metalové) barvy a 1 ks kazety DVC zn. Panasonic, které byl zajištěny při domovní prohlídce konané dne 3.5.2006.

Podle § 228 odst. 1 tr. řádu se obviněnému ukládá povinnost uhradit poškozeným zastoupeným advokátní kanceláří Voborník a Nigrini se sídlem Praha 1, Štupartská 9, částku ve výši **247.750,- Kč** (spol. Adobe 63.452,- Kč, spol. Autodesk 153.110,- Kč, spol. Microsoft 29.620,- Kč, spol. Symantec 1.568,- Kč).

P o u č e n í : Proti tomuto trestnímu příkazu mohou obviněný, osoby, které jsou oprávněny podat v jeho prospěch odvolání, a státní zástupce podat do osmi dnů ode dne doručení příkazu odpor u Okresního soudu v Mostě.

Byl-li podán proti trestnímu příkazu oprávněnou osobou v lhůtě odpor, trestní příkaz se ruší a samosoudce nařídí ve věci hlavní líčení; přičemž při projednávání věci v hlavním líčení není samosoudce vázán právní kvalifikací a ani druhem a výši trestu obsaženými v trestním příkazu.

Jinak se trestní příkaz stane pravomocným a vykonatelným.

Po doručení trestního příkazu může se oprávněná osoba odporu výslovně vzdát.

V Mostě dne 22.3.2007

JUDr. Benno Eichler, v.r.
samosoudce

Za správnost vyhotovení:

Příloha č. 3 – A (zdroj http://www.cpufilm.cz/rozsudky.html)

DOŠLO 11. 04. 2007

Jednací číslo: **3 T 160/2006**

Toto rozhodnutí nabylo právní moci
ke dni 26-03-2007
OBVODNÍ SOUD PRO PRAHU 10

ČESKÁ REPUBLIKA

TRESTNÍ PŘÍKAZ

Samosoudce Obvodního soudu pro Prahu 10 vydal dne 29.září 2006 podle § 314e odst.1 trestního řádu tento t r e s t n í p ř í k a z:

Obviněný

L R ,

nar. 1972 ve Varnsdorfu, trvale bytem Bořanovice,

j e v i n e n, ž e

v době nejméně od roku 2002 do 16.1.2006 na svém pracovišti v Praze 10 ve společnosti se na pracovním počítači jako uživatel internetové výměnné sítě vystupující pod přezdívkou LUBOSOFT připojoval k Internetu, kde v rámci výměnných sítí za použití speciálního programu DC++ sdílel a tím ostatním uživatelům těchto výměnných sítí nabízel ke stažení hudební a audiovizuální soubory, a to bez vědomí a souhlasu nositelů autorských práv, ke škodě České národní skupiny Mezinárodní federace hudebního průmyslu z celkem 717 šířených a zajištěných komerčních titulů, Ochranného svazu autorského pro práva k dílům hudebním z počtu 621 skladeb a České protipirátské unii za provedení rozmnožení filmových titulů,

t e d y: zasáhl neoprávněně do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému a zvukově obrazovému záznamu a dopustil se takového činu ve značném rozsahu,

TRR082 - (Tr.ř. 82 - trestní příkaz)

Příloha č. 3 – B (zdroj http://www.cpufilm.cz/rozsudky.html)

čímž spáchal

trestný čin porušování autorského práva, práv souvisejících s právem autorským a práv k databázi podle § 152 odst. 1, odst. 2 písm. b) trestního zákona,

a za to se odsuzuje

Podle § 152 odst. 2 tr. zákona k trestu odnětí svobody **v trvání 7 měsíců**.

Podle § 58 odst. 1 tr. zákona a § 59 odst. 1 tr. zákona se výkon trestu podmíněně odkládá **na zkušební dobu 14 měsíců**.

Podle § 229 odst. 1 tr. řádu se poškozená Česká protipirátská unie se sídlem Praha 8, Sokolovská 37/24 odkazuje s nárokem na náhradu škody na řízení ve věcech občanskoprávních.

Poučení: Proti tomuto trestnímu příkazu lze do osmi dnů od jeho doručení podat u zdejšího soudu odpor. Právo podat odpor nenáleží poškozenému. Pokud je odpor podán včas a oprávněnou osobou, trestní příkaz se ruší a ve věci bude nařízeno hlavní líčení. Při projednání věci v hlavním líčení není samosoudce vázán právní kvalifikací ani druhem a výměrou trestu obsaženými v trestním příkaze. Nebude-li odpor řádně a včas podán, trestní příkaz se stane pravomocným a vykonatelným. V případě, že obviněný odpor nepodá, vzdává se tím práva na projednání věci v hlavním líčení.

V Praze dne 29.září 2006

Mgr. Radek Mařík v.r.
samosoudce

OBVODNÍ SOUD PRO PRAHU 10
16

Za správnost vyhotovení:
Andrea Šléglová

TRR082 - (Tr.ř. 82 - trestní příkaz)

Příloha č. 4 – A (zdroj http://www.cpufilm.cz/rozsudky.html)

DOŠLO 27. 06. 2006

2 T 24/2006

ČESKÁ REPUBLIKA

Trestní příkaz

Samosoudce Okresního soudu v Trutnově Mgr. Jan Steinmetz vydal dne 15. února 2006 v Trutnově podle § 314e odst. 1 tr.ř. následující **t r e s t n í p ř í k a z**:

Obviněný

M Š ,

nar. 1967 v Teplicích, nástrojař trvale bytem , okr. Trutnov,

j e v i n e n , ž e

v období nejméně od března 2004 do srpna 2004 v Žacléři, okr. Trutnov, prostřednictvím internetu a e-mailové schránky nelegálně a bez vědomí či souhlasu nositelů autorských práv nabízel pod hlavičkou různé filmy a hry na Play Station, na základě následných objednávek tato autorsky chráněná díla, rozmnožená na nosičích CD-R, rozeslal oproti finanční úhradě nejméně šesti objednatelům, čímž poškozeným společnostem Sony Czech se sídlem v Praze 4, Bontofilm, a.s. se sídlem v Praze 5, Hollywood C.E., s.r.o. se sídlem v Říčanech, Intersonic Taunus Production, s.r.o. se sídlem v Břeclavi, SPI International Czech republic, s.r.o. se sídlem v Praze 4, Warner Bros., s.r.o. se sídlem v Praze 1 a Cenega Czech, s.r.o. se sídlem v Praze 5, způsobil škodu ve výši celkem nejméně 21.441,- Kč,

t e d y

neoprávněně zasáhl do zákonem chráněných práv k autorskému dílu,

Příloha č. 4 – B (zdroj http://www.cpufilm.cz/rozsudky.html)

čímž spáchal

trestný čin porušování autorského práva, práv souvisejících s právem autorským a práv k databázi podle § 152 odst. 1 tr. z.,

a odsuzuje se

podle § 152 odst. 1 tr. z. s přihlédnutím k § 314e odst. 2 tr. ř. k trestu odnětí svobody v trvání **šesti (6) měsíců.**

Podle § 58 odst. 1 tr. z. a § 59 odst. 1 tr. z. se výkon trestu **podmíněně** odkládá na zkušební **dobu dvou (2) let.**

Podle § 59 odst. 2 tr. z. se obviněnému ukládá, aby podle svých sil, v nejkratší možné době, nahradil škodu, kterou trestným činem způsobil.

Podle 53 odst. 1 tr. z. se obviněnému ukládá peněžitý trest ve výši **15.000,- Kč (patnáct tisíc)** a pro případ, že by tento trest nebyl ve stanovené lhůtě vykonán, podle § 54 odst. 3 tr. z. se stanovuje náhradní trest odnětí svobody v trvání **dvou (2) měsíců.**

Podle § 229 odst. 1 tr. ř. se poškození Česká protipirátská unie, se sídlem Pobřežní 22, Praha 8 – Karlín, CENEGA CZECH s.r.o., se sídlem Naskové 3, Praha 5 a SONY CZECH, se sídlem V Parku 2309/6, Praha 4 – Chodov odkazují se svými nároky na náhradu škody na řízení ve věcech občanskoprávních.

Poučení: Proti tomuto trestnímu příkazu lze do osmi dnů od jeho doručení podat u zdejšího soudu odpor. Právo podat odpor nenáleží poškozenému. Pokud je odpor podán včas a oprávněnou osobou, trestní příkaz se ruší a ve věci bude nařízeno hlavní líčení. Při projednání věci v hlavním líčení není samosoudce vázán právní kvalifikací ani druhem a výměrou trestu obsaženými v trestním příkaze. Nebude-li odpor řádně a včas podán, trestní příkaz se stane pravomocným a vykonatelným. V případě, že obviněný odpor nepodá, vzdává se tím práva na projednání věci v hlavním líčení.

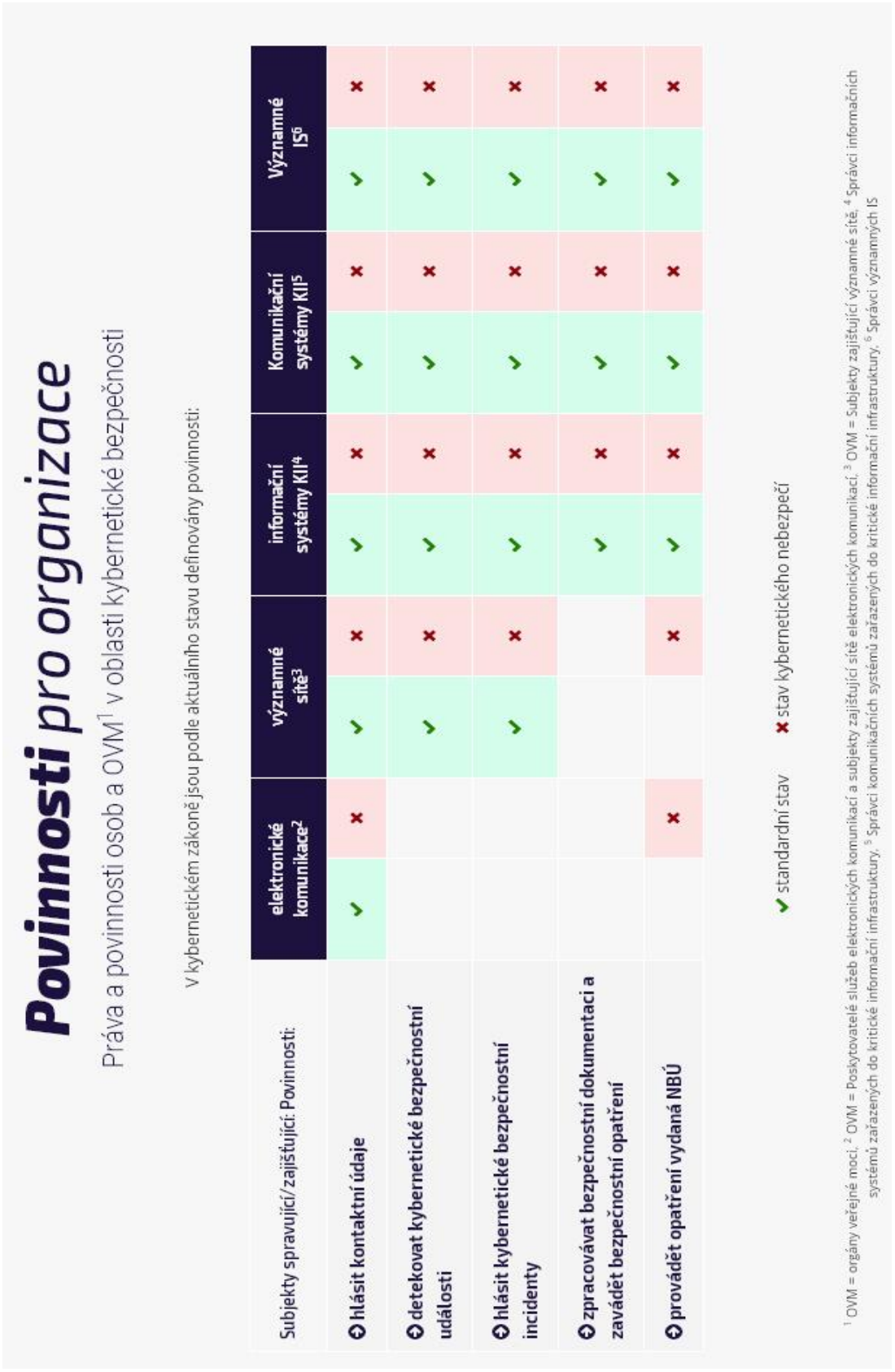
V Trutnově dne 15. února 2006

Mgr. Jan Steinmetz, v. r.
samosoudce

Za správnost vyhotovení: Jana Vlášková

OKRESNÍ SOUD V TRUTNOVĚ

Příloha č. 5 (zdroj http://www.kybernetickyzakon.cz/)



Resumé

Tato diplomová práce, jak už její název napovídá, pojednává o problému současné doby spojeném s počítači a internetem, díky kterým je možné páchat nejrůznější protiprávní jednání. Počítače jsou součástí našeho denního života a oblast informačních a komunikačních technologií se neustále rychle rozvíjí, což dává prostor případným pachatelům nalézat stále nové postupy. Práce je rozdělena do osmi kapitol.

Úvodní kapitola této práce popisuje základní pojmy týkající se počítačové a internetové kriminality. Zahrnuje jednak vymezení pojmů počítačová kriminalita, kyberzločin, kyberprostor, ale i základních technických pojmů, jako je počítač, hardware či software. Přiblížení této terminologie je nezbytné pro pochopení dané problematiky. Další kapitola se již věnuje některým nezákonným jednáním v kyberprostoru, která jsou následně právně posouzena.

Třetí kapitola pak tvoří nejdůležitější část celé práce, neboť podrobně popisuje problém týkající se porušování autorského práva v souvislosti s počítači. Nejdříve se obecně věnuje nehmotným statkům a poté již čtenáře seznamuje s pirátstvím audio a audiovizuálních děl a posléze i s pirátstvím softwaru. Představuje nejdůležitější rozsudky, které se daných případů týkají, a to jak českých soudů, tak i Soudního dvora EU. V závěru kapitoly je představen možný výpočet výše způsobené škody v případech pirátství. Čtvrtá kapitola této diplomové práce představuje některé kauzy a to včetně rozsudků, které diskutovaný problém medializovaly.

Pátá kapitola se věnuje osobě pachatele, včetně jeho motivů nezákonného jednání. Poté čtenáři představí možné způsoby vyšetřování předmětné trestné činnosti a dále způsob případné mezinárodní spolupráce, bez které není možné delikty v kyberprostoru postihovat. Šestá kapitola je pak zaměřena na prostředky, které mohou přispět k zamezení nelegálních aktivit a případnou prevenci.

Sedmá kapitola práce pak představuje vlastní návrhy autora, včetně nových zákonných ustanovení, kterými by danou oblast řešil. V samém závěru následuje shrnutí uvedeného a možný předpokládaný vývoj kriminality v oboru ICT.

Internet and computer criminality

Summary

This thesis, as its name indicates, deals with the problems of our times associated with computers and the Internet, which make it possible to commit all sorts of crimes. Computers are part of our daily life and the sphere of information and communication technologies are constantly and rapidly developing, which gives space to potential perpetrators to find new approaches. The thesis is composed of eight chapters.

The opening chapter of this thesis describes the basic concepts related to computer and Internet criminality. It includes the definitions of computer criminality, cybercrime, cyberspace, as well as basic technical concepts such as computer, hardware or software. Approximation of this terminology is essential to understanding the issue. Next chapter is devoted to some illegal activities in cyberspace, which are then legally assessed.

The third chapter forms the most important part of the whole thesis because it describes in details the issue of copyright violations in connection with computers. At first it generally talks about intangible goods, and after that it acquaints to readers with piracy of audio and audiovisual works and later with software piracy. It shows the most important judgments that are connected to the discussed topic and were judged at the Czech courts and at the European Court of Justice. At the end of the chapter is introduced the calculating system of the possible damage in cases of piracy. The fourth chapter of this thesis presents some cases, including judgments that have been debated in media.

The fifth chapter is dedicated to the offender, including his motives of illegal conduct. After that the possible ways of investigation of the offense and the possible way of international cooperation without that it is impossible to punish offenses in cyberspace will be presented to the reader. The sixth chapter is focused on resources that can help to prevent illegal activities and possible prevention.

The seventh chapter of the thesis represents the author's own ideas, including the new statutory provisions that could solve the problem of the cyber criminality. At the very end is the summary of all possible anticipated development of criminality in the field of ICT.

Klíčová slova

Kybernalita / Porušování autorských práv na internetu / Pirátství / Prevence

Key words

Cybercrime / Copyright infringement on the Internet / Piracy / Prevention