OBSAH

ZOZNAM POUŽITÝCH SKRATIEK 11

ÚVOD 13

I. ČASŤ ZÁKLADNÉ VÝCHODISKÁ

Kapitola 1 – Vymedzenie pojmu počítačová kriminalita 17

1.1 Počítačová kriminalita ako novodobý bezhraničný fenomén 17
1.2 Počítačová kriminalita ako európsky trestný čin v zmysle Zmluvy o fungovaní Európskej únie 20
1.3 Pojem počítačová kriminalita a absencia jeho definície 22
1.4 Skupiny počítačových trestných činov – alternatíva definície pojmu počítačová kriminalita 26
1.5 Spôsoby páchania počítačovej kriminality 29
1.5.1 Hacking 29
1.5.2 Cracking 31
1.5.3 Warez (a linking) 35
1.5.4 Porušovanie autorských práv prostredníctvom „torrent-ov“ 38
1.5.5 Malware 43
1.5.6 Phishing (a pharming) 46
1.5.7 Sniffing 51
1.5.8 Skimming 51
1.6 Páchatelia počítačovej kriminality 53
1.7 (Zdanlivá) anonymita počítačovej kriminality 53
1.8 Neprávna ochrana pred počítačovou kriminalitou 54
1.8.1 Zabezpečenie počítača a iných informačno-technických zariadení ochrannými prvkami 55
1.8.2 Inštalovanie najnovších aktualizácii operačného systému 56
1.8.3 Ochrana súborov 57
1.8.4 Používanie silných a zároveň odlišných hesiel 58
1.8.5 Obozretnosť pri sprístupnení údajov online 59
1.8.6 Zabezpečenie siete 60

Kapitola 2 – Právna úprava boja proti počítačovej kriminalite v Európskej únii (všeobecné východiská) 61
2.1 Primárne právo 61
2.2 Konkrétne sekundárne legislatívne opatrenia 62
2.3 Spoločné črty 65
2.3.1 Potláčanie počítačovej kriminality na spoločnom základe v podobe spoločných pravidiel 65
2.3.2 Predstavenie minimálnych pravidiel a potreba ich implementácie (zavedenia) v členských štátoch Európskej únie 66
2.3.3 Aproximácia a harmonizácia trestných činov a sankcií 67
2.3.4 Dôraz na trestnú zodpovednosť právnických osôb a ich sankcionovanie 68
2.4 Akceptácia opatrení Rady Európy 70

Kapitola 3 – Metodológia 72
3.1 Vymedzenie vedeckého problému 72
3.2 Literárna rešerš 75
3.3 Ciele monografie 80
3.4 Hypotéza 80
3.5 Vedecké metódy 81
3.6 Prípravné práce 81
3.7 Štruktúra 83
3.8 Rozsah 84
3.9 Príspevky autorov 84

II. ČASŤ FORMY POČÍTAČOVEJ KRIMINALITY V PRÁVNEJ ÚPRAVE EURÓPSKEJ ÚNIE A SLOVENSKEJ REPUBLIKY

Kapitola 4 – Podvody a falšovanie bezhotovostných platobných prostriedkov 87
4.1 Všeobecný kontext 87
4.2 Právny základ na úrovni Európskej únie a jeho analýza: Rámcové rozhodnutie 2001/413/SVV o boji proti podvodom a falšovaniu bezhotovostných platobných prostriedkov 88
4.2.1 Rámcové rozhodnutie a jeho ciele 88
4.2.2 Kľúčové pojmy 89

4.2.3 Vymedzenie trestných činov 90
4.2.4 Zodpovednosť právnických osôb a ich sankcionovanie 92
4.2.5 Právomoc viesť trestné stíhanie 94
4.2.6 Spolupráca štátov a výmena informácií 95
4.2.7 Implementácia požiadaviek Európskej únie v členských štátoch 96
4.3 Právna úprava v Slovenskej republike 100
4.3.1 Úvodná poznámka 100
4.3.2 Neoprávnené vyrobenie a používanie platobného prostriedku, elektronických peňazí alebo inej platobnej karty – § 219 Trestného zákona 100

Kapitola 5 – Útoky na informačné systémy 119

5.1 Všeobecný kontext 119
5.2 Právny základ na úrovni Európskej únie a jeho analýza: Smernica 2013/40/EÚ o útokoch na informačné systémy 120
5.2.1 Smernica a jej ciele 120
5.2.2 Nadväznosť na existujúcu právnu úpravu 121
5.2.3 Kľúčové pojmy 124
5.2.4 Vymedzenie trestných činov 124
5.2.5 Sankcie 129
5.2.6 Zodpovednosť právnických osôb a ich sankcionovanie 132
5.2.7 Súdna právomoc 134
5.2.8 Výmena informácií 135
5.2.9 Koordinácia trestného stíhania 136
5.3 Právna úprava v Slovenskej republike 137
5.3.1 Úvodná poznámka 137
5.3.2 Neoprávnené obohatenie – § 226 Trestného zákona 137
5.3.3 Neoprávnený prístup do počítačového systému – § 247 Trestného zákona 145
5.3.4 Neoprávnený zásah do počítačového systému – § 247a Trestného zákona 161
5.3.5 Neoprávnený zásah do počítačového údaja – § 247b Trestného zákona 173
5.3.6 Neoprávnené zachytávanie počítačových údajov – § 247c Trestného zákona 176

5.3.7 Výroba a držba prístupového zariadenia, hesla do počítačového systému alebo iných údajov – § 247d Trestného zákona 182

Kapitola 6 – Detská pornografia na internete a kontaktovanie detí na účely ich sexuálneho zneužitia 188

6.1 Všeobecný kontext 188
6.2 Boj proti detskej pornografii na internete na úrovni Európskej únie: Rozhodnutie 2000/375/SVV o boji proti detskej pornografii na internete 195
6.3 Vymedzenie konkrétnych opatrení: Smernica 2011/93/EÚ o sexuálnom zneužívaní a vykorisťovaní detí a detskej pornografii 198
6.3.1 Nadväznosť na existujúcu právnu úpravu 199
6.3.2 Základné pojmy 202
6.3.3 Vymedzenie trestných činov 206
6.3.4 Právomoc viesť trestné stíhanie a osobitné otázky vyšetrovania 212
6.3.5 Nestíhanie obete a neuplatňovanie trestov voči obeti..... 214
6.3.6 Zákaz vykonávania určitých aktivít z dôvodu odsúdenia 215
6.3.7 Zodpovednosť právnických osôb a ich sankcionovanie 216
6.3.8 Opatrenia na pomoc, podporu a ochranu detských obetí 218
6.3.9 Opatrenia proti online stránkam obsahujúcim alebo šíriacim detskú pornografiu..... 221
6.4 Právna úprava v Slovenskej republike 222
6.4.1 Úvodná poznámka..... 222
6.4.2 Výroba detskej pornografie – § 368 Trestného zákona 223
6.4.3 Rozširovanie detskej pornografie – § 369 Trestného zákona 252
6.4.4 Prechovávanie detskej pornografie a účasť na detskom pornografickom predstavení – § 370 Trestného zákona 264
6.4.5 Kontaktovanie detí prostredníctvom elektronickej komunikačnej služby na účely ich sexuálneho zneužitia – § 201a Trestného zákona..... 272

Kapitola 7 – Porušovanie právnej ochrany počítačových programov..... 289

7.1 Všeobecný kontext 289

7.2 Právny základ na úrovni Európskej únie a jeho analýza: Smernica 2009/24/ES o právnej ochrane počítačových programov 290
7.2.1 Ciele Smernice 290
7.2.2 Nadväznosť na existujúcu právnu úpravu 292
7.2.3 Kľúčové pojmy 293
7.2.4 Osobitné ochranné opatrenia a úkony podliehajúce obmedzeniam 294
7.2.5 Absencia trestnoprávnych sankcií 296
7.2.6 Obchodovanie s licenciami vzťahujúcimi sa na použité počítačové programy, ktoré boli stiahnuté z internetu: Rozsudok Súdneho dvora Európskej únie vo veci C-128/11, *UsedSoft proti Oracle* 297
7.2.7 Prebratie prvkov v užívateľskom manuáli počítačového programu do iného počítačového programu alebo užívateľského manuálu 307
7.3 Právna úprava v Slovenskej republike 309
7.3.1 Úvodná poznámka 309
7.3.2 Porušovanie autorského práva (softvérové pirátstvo) – § 283 Trestného zákona 309

III. ČASŤ JEDNOTKY EURÓPSKEJ ÚNIE POTLÁČAJÚCE POČÍTAČOVÚ KRIMINALITU

Kapitola 8 – Eurojust (Jednotka pre súdnu spoluprácu Európskej únie) ... 339
8.1 Všeobecné východiská 339
8.2 Úloha a činnosti Eurojustu v boji proti počítačovej kriminalite 340
8.3 Operácie štátov, ktoré podporil Eurojust 347
8.3.1 Podvod a zneužívanie detí na internete 347
8.3.2 Online podvody páchané prostredníctvom nelegálne získanej identity 347
8.3.3 Podvody na internetovej aukcii 348
8.3.4 Šírenie pirátskeho materiálu 348
8.3.5 Phishing 349
8.3.6 Podvod a falšovanie bezhotovostných platobných prostriedkov 350

8.3.7 Podvod a falšovanie bezhotovostných platobných prostriedkov II 351
8.3.8 Operácia BlackShades 351

Kapitola 9 – Europol (Európsky policajný úrad) 354
9.1 Všeobecné východiská 354
9.2 Úloha a činnosti Europolu v boji proti počítačovej kriminalite 355
9.3 Operácie štátov, ktoré podporil Europol 358
9.3.1 Benátsky karneval 358
9.3.2 Rescue 358
9.3.3 Crossbill 359
9.3.4 Mariposa II 359
9.3.5 Anonymous 360
9.3.6 Icarus 360
9.3.7 Night Clone 361
9.3.8 Iasi 361
9.4 Súčasť Europolu: Európske centrum boja proti počítačovej kriminalite 362

Kapitola 10 – Európske centrum boja proti počítačovej kriminalite 363
10.1 Všeobecné východiská 363
10.2 Európske centrum boja proti počítačovej kriminalite ako opatrenie Stratégie vnútornej bezpečnosti Európskej únie 365
10.3 Zriadenie a „právny základ“ 369
10.4 Spolupráca 371
10.5 Hodnotenie prvého roka činnosti 373

Kapitola 11 – Agentúra Európskej únie pre sieťovú a informačnú bezpečnosť 377
11.1 Všeobecné východiská 377
11.2 Právny základ: Nariadenie (EÚ) č. 526/2013 o Agentúre Európskej únie pre sieťovú a informačnú bezpečnosť 378
11.3 Ciele a úlohy Agentúry 379
11.4 Žiadosti Agentúre 382

POUŽITÉ PRAMENE 383
SUMÁR (ANGLICKY) 421

SUMÁR (NEMECKY) 423
OBSAH (ANGLICKY) 425
OBSAH (NEMECKY) 428

O AUTOROCH 432

VECNÝ REGISTER 436

trestnú činnosť špecifickú pre elektronické siete, t. j. útoky na informačné systémy, odmietnutie vstupu do systému a *hacking*. Tieto druhy útokov môžu byť tiež nasmerované proti najdôležitejším infraštruktúram v Európe a v mnohých oblastiach ovplyvniť existujúce systémy rýchleho varovania. Komisia dodáva, že spoločným prvkom pre všetky kategórie trestnej činnosti je, že ich možno páchať masovo.[44]

1.5 Spôsoby páchania počítačovej kriminality

Páchatelia počítačovej kriminality sú mimoriadne vynaliezaví, pokiaľ ide o spôsoby jej páchania. Niektoré sú zaužívané desiatky rokov, pričom boli neustále „vylepšované" a stali sa ich štandardným know-how. V mnohých konkrétnych prípadoch sú veľmi sofistikované, dokonca takmer neobjasniteľné.

Detailná analýza všetkých spôsobov páchania počítačovej kriminality by presahovala rámec tejto monografie. V nasledujúcom texte poukazujeme na tie najbežnejšie, ako aj najškodlivejšie.

1.5.1 Hacking

Hacking (hackerstvo) je najstarším spôsobom páchania počítačovej kriminality. Ide o neoprávnené preniknutie do cudzieho systému (napr. počítačového, informačného, riadiaceho) inou ako štandardnou cestou, a to prostredníctvom prelomenia alebo obídenia jeho bezpečnostnej ochrany. *Hacking* je neetickou činnosťou, ktorá je veľmi často na hrane zákona, často je protizákonná a v mnohých prípadoch dokonca vykazuje znaky trestného činu. Pre jeho páchateľov – *hackerov* – je často nič viac ako intelektuálnou výzvou. Obeťami *hackingu* boli napríklad Pentagon, NASA, Yahoo či Google. V Slovenskej republike bolo najznámejšou kauzou *hackingu* preniknutie do systému Národného bezpečnostného úradu Slovenskej republiky, teda ostro výsmešná kauza prelomenia hesla „nbusr123" (bližšie pozri Kapitolu 5, pozn. autorov).

[44] Komisia Európskych spoločenstiev (2007): Smerovanie k všeobecnej politike boja proti počítačovej trestnej činnosti. Oznámenie Komisie Európskemu parlamentu, Rade a Európskemu Výboru regiónov, KOM(2007) 267 v konečnom znení, s. 2.

Pôvod pojmov *hacker* a *hacking* nachádzame v 50. rokoch 20. storočia na Massachusettsskom technologickom inštitúte[45] v Spojených štátoch amerických, ktorý bol jednou z celosvetovo prvých inštitúcií poskytujúcich kurzy programovania a počítačových vied.[46] Pojem *hacker* v tých časoch označoval šikovných, vynaliezavých a technicky nadaných novátorov, ktorí realizáciou svojich nápadov podstatne prispievali k zlepšeniu funkčnosti vyvíjaného počítačového programu, a teda nemal pejoratívny a ani kriminálny nádych. *Hacking* (od angl. slova *hack* – rozseknúť) bol vnímaný kladne, a to ako požadovaný a schvaľovaný prístup k práci programátora v podobe elegantného a jednoduchého riešenia, ktorého výsledkom je rozseknutie programátorského problému. V 90. rokoch 20. storočia však začal byť *hacking* vnímaný negatívne za spoluúčastí médií, a to ako nelegálna aktivita zameraná na spôsobenie škody. Praobraz hackera v nedávnej minulosti pozostával v jeho vyobrazení ako vychudnutého, útleho pubertálneho chlapca, nosiaceho silné okuliare, žijúceho mimo spoločnosti a svojich rovesníkov, ktorý má slabú schopnosť interakcie so spoločnosťou, a teda svoje presadenie nachádza v imateriálnom prostredí svojho počítača. Z psychologického hľadiska hackeri boli prezentovaní ako asociálni introvertní okrajoví jedinci. Boli im prisudzované vlastnosti ako fanatickosť, arogancia, nadpriemerná inteligencia, namyslenosť a snaha o manifestáciu seba samého prostredníctvom počítača hraničiaca s narcizmom.[47] No v dnešných dňoch profil skutočného *hackera* uvedeným vlastnostiam nezodpovedá. Spravidla ide o osobu, ktorá sa navonok ničím zásadným neodlišuje od ostatných ľudí.

Hackeri pri dosahovaní svojich cieľov používajú sofistikované metódy, napríklad počítačové vírusy (pozri text nižšie, pozn. autorov), trojské kone

---

45 Massachusetts Institute of Technology (MIT). Bližšie pozri www.mit.edu.

46 MOORE, R. *Cybercrime*: *Investigating High-Technology Computer Crime*. 2nd edition. Oxon – New York : Routledge, 2011, ISBN 978-1-4377-5582-4, p. 18; RUSSELL, R. et al. *Hack Proofing Your Network*. 2nd edition. Rockland : Syngress Publishing, 2000, ISBN 1-928994-15-6, p. 2; takisto pozri: LEVY, S. *Hackers* : *Heroes of the Computer Revolution*. New York : Nerraw Manijaime/Doubleday, 1984, ISBN 0-385-19195-2; dielo bolo vydané aj v reprinte (Sebastopol : O'Reilly, 2010, ISBN 978-1-449-38839-3).

47 GREGUŠ, L. Páchatelia počítačovej kriminality (niektoré trestnoprávne a kriminologické aspekty páchateľov počítačovej kriminality). In ROMŽA, S. – FERENČÍKOVÁ, S. et MICHAĽOV, L. (eds.) *Počítačová kriminalita – juristické, kriminalistické a kriminologické aspekty.* Zborník príspevkov z medzinárodného vedeckého sympózia konaného dňa 28. marca 2014 na Katedre trestného práva Právnickej fakulty Univerzity Pavla Jozefa Šafárika v Košiciach. Košice : Univerzita Pavla Jozefa Šafárika v Košiciach, 2014, ISBN 978-80-8152-146-1, s. 225 a 228.

(pozri text nižšie, pozn. autorov), keyloggery[48], útok hrubou silou[49] či slovníkový útok[50]. V minulosti „hackerská etika" zakazovala na „nabúranom systéme" čokoľvek meniť či ukradnúť z neho informácie alebo údaje. V súčasnosti je situácia iná, keďže *hacking* je zdrojom nelegálne získaných informácií a údajov.

Na druhej strane, možno sa stretnúť aj s názormi, ktoré *hacking* považujú za umenie a schvaľujú ho. Jedným z argumentov je, že *hackeri* poukazujú na slabé miesta systémov a tým podporujú zvyšovanie ich bezpečnosti.[51]

1.5.2 Cracking

Cracking je konanie, ktorým dochádza k obchádzaniu alebo prelamovaniu ochranných prvkov, spravidla počítačových programov s úmyslom ich neoprávnene používať, resp. šíriť ich iným osobám, aby ich mohli neoprávnene používať. *Cracking* počítačových programov je ich modifikáciou s úmyslom odstrániť alebo obísť ich ochranné zabezpečenie pred nelegálnym používaním.[52]

---

48 *Keylogger* zaznamenáva stlačenia kláves na klávesnici počítača, a to bez vedomia jeho užívateľa. *Keylogger* v princípe neohrozuje počítač ani jeho riadny chod, keďže jeho cieľom je zisťovanie prihlasovacích hesiel užívateľa na jeho účtoch či kontách – napríklad e-mailový, pracovný či na internet bankingu. Navyše, „zaujímavé" informácie môže priniesť aj napríklad komunikácia na sociálnych sieťach. „Záznam" stlačených kláves je odoslaný jeho autorovi na pozadí činnosti operačného system, a teda užívateľ o tom nemá vedomosť (existujú aj *keyloggery*, ktoré dáta len ukladajú na hostiteľský počítač – napr. firemný, pričom je potrebné ich z neho fyzicky prevziať). Následne nie je problematické zo záznamu vyhľadať konkrétne poradie znakov, ktoré užívateľ počítača zadal ako údaj pri prihlásení na svoj účet či konto.

49 Útok hrubou silou (angl. *brute-force attack*) je používaný s cieľom uhádnutia kombinácie užívateľského mena + hesla. Tento útok spočíva v zadávaní všetkých možných kombinácii prihlasovacích mien, ako aj hesiel dovtedy, kým útočník natrafí na zhodu. Oveľa jednoduchšie je, ak útočník pozná prihlasovacie meno a snaží sa zistiť iba heslo. Útok má potenciál byť ešte úspešnejší v prípade slabých hesiel, ako napríklad „liborko" či „asdf".

50 Slovníkový útok (angl. *dictionary attack*) je používaný s cieľom uhádnutia užívateľského hesla. Útočník sa pokúša zadávať pravdepodobné heslá z pripraveného zoznamu slov, z pomedzi ktorých je predpoklad, že užívateľ si niektoré slovo alebo slová vybral ako heslo + číslo ako súčasť hesla alebo inú súčasť. Zdrojom slov pre použitý zoznam je napríklad slovník užívateľovho materinského jazyka. V porovnaní s útokom hrubou silou ide o potenciálne efektívnejší útok.

51 Naprílad: ERICKSON, J. *Hacking*: *The Art of Exploitation*. 2nd edition. San Francisco : No Starch Press, 2008, ISBN 978-1-59327-144-2, 488 strán; ANTO, Y. *The Art of Hacking*. Saarbrücken : Lambert Academic Publishing, 2012, ISBN 978-3-8484-2605-8, 268 strán.

52 DINGLE, A. *Software Essentials*: *Design and Construction*. Boca Raton : CRC Press, 2014, ISBN 978-1-4395-4120-4, s. 302.

Značná časť počítačových programov je licencovaná[53], t. j. ich legálne používanie vyžaduje zakúpenie platenej licencie, pričom ceny licencií sa pohybujú rádovo v desiatkach až stovkách eur. *Cracking* našiel živnú pôdu v oblasti softwarového pirátstva, keď dochádza k porušovaniu autorských práv k počítačovým programom. Logicky, *cracking* je nežiadúcim javom v prípade licencovaných počítačových programov, ku ktorým je potrebné zakúpiť licenciu k ich legálnemu používaniu. Príkladom sú operačné systémy počítača – napríklad *Windows* (XP, 7, 8 atď.), taktiež kancelárske programy – napríklad *Microsoft Office*, či grafické programy – napríklad *Photoshop*. Vymenovať úplný zoznam počítačových programov by bolo nad rámec a účely tejto monografie, ale opomenúť nemožno ani skutočnosť, že počítačovými programami sú aj hry – napríklad *HalfLife* a *Max Payne*.

Vývojári a výrobcovia licencovaných počítačových programov používajú rôzne ochranné prvky, ako napríklad sériové číslo, autentifikáciu na serveroch výrobcu pri spustení programu po jeho inštalácii, aktiváciu programu telefónom, nutnosť mať pri prvom spustení programu originálne inštalačné médium v CD/DVD mechanike. Často dochádza aj ku kombinácii ochranných prvkov. Kým v minulosti boli zabezpečovacie prvky veľmi jednoduché, v dnešných dňoch sú veľmi sofistikované.

Na druhej strane, páchateľ *crackingu* – *cracker* – svojou intelektuálnou činnosťou pomocou počítača prelamuje alebo obchádza ochranné prvky počítačových programov, a to takým spôsobom, aby bolo možné ich používať aj bez licencie. Vytvára tzv. *crack*, prostredníctvom ktorého je možné ochranu obísť.

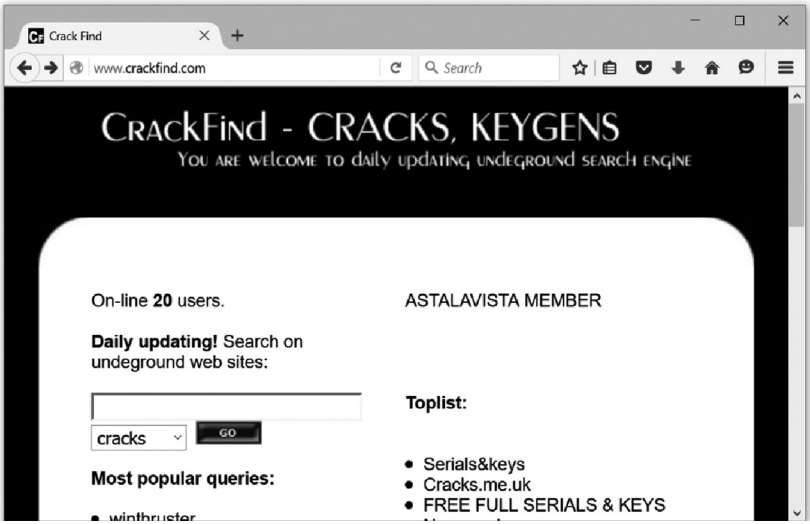
Cracky sú verejnosti prístupné väčšinou na internete, alebo si ich ľudia kopírujú navzájom. Príkladom *cracku* je balík súborov v zložke pomenovanej „Crack", ktoré je potrebné „už len" nakopírovať do zložky s nainštalovaným programom, ktorý nemá aktivovanú licenciu (a teda je úplne nepoužiteľný alebo použiteľný len v demo verzii[54]). Po nakopírovaní dôjde k nahradeniu vybraných pôvodných súborov novými súbormi, ktoré nebránia plnohodnotnému

[53] Bližšie pozri: ŠTĚDROŇ, B. *Ochrana a licencování počítačového programu*. Praha : Wolters Kluwer, 2010, ISBN 978-80-7357-555-7, 220 strán; pozri taktiež: MAISNER, M. et al. *Základy softwarového práva*. Praha : Wolters Kluwer, 2010, ISBN 978-80-7357-638-7, 340 strán.

[54] Demo verzia počítačového programu je taká alternatíva počítačového programu, ktorá je voľne šíriteľná, ale počítačový program nie je použiteľný úplne. V rámci demo verzie je program funkčný napríklad len počas 15 dní od jeho inštalácie alebo použiteľný na 10 spustení, alebo nie je možné využívať všetky prvky programu.

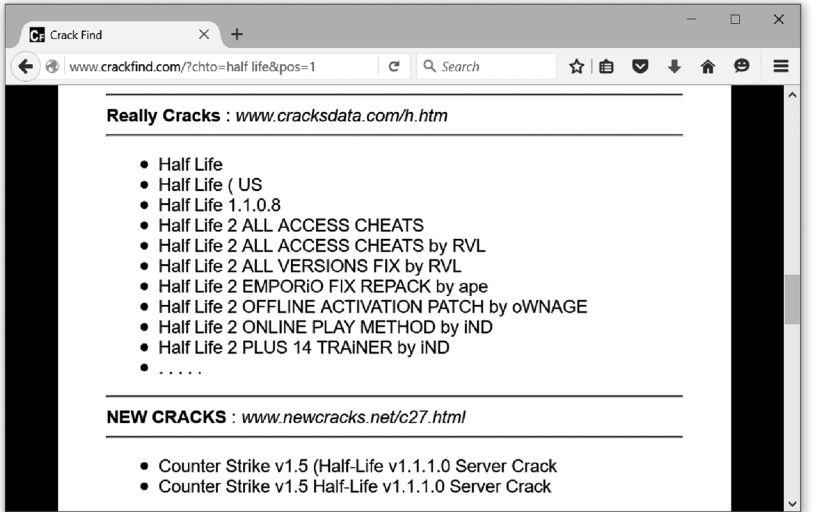
používaniu programu. Iným príkladom *cracku* je inštalačný súbor (*.exe), ktorý po jeho spustení automaticky prelomí zabezpečenie počítačového programu. Po jeho nainštalovaní počítačový program nevyžaduje licenciu, keďže došlo k jeho „odlicencovaniu".

Na internete je mnoho stránok, ktoré ponúkajú možnosť vyhľadať *cracky*. Príkladom je stránka <www.crackfind.com>, ktorej úvodné zobrazenie je nasledujúce:



obr. č. 1: internetová stránka CrackFind.com
zdroj: Libor Klimek – snímok vlastnej obrazovky (*screenshot*)

Do riadka s vyhľadávačom je potrebné napísať názov počítačového programu a kliknúť na tlačidlo „Go", ktorým je spustené vyhľadávanie. V našom prípade sme zadali názov hry *Half-Life* (počítačové hry sú takisto počítačové programy). Výsledok hľadania je veľmi rozsiahly, pričom poukazujeme len na časť výsledkov. Na nižšie uvedenom vyobrazení výsledkov je výpis nájdených *crackov*. Po stlačení na jednotlivé výsledky dôjde k presmerovaniu a následnému sťahovaniu konkrétneho *cracku*. Pravda, nie všetky *cracky* sú funkčné, a preto je potrebné skúsiť niekedy aj viac *crackov*.



obr. č. 2: internetová stránka CrackFind.com s výsledkami vyhľadávania crackov
zdroj: Libor Klimek – snímok vlastnej obrazovky (*screenshot*)

Často dochádza aj ku *crackingu* demo verzií počítačových programov. Demo verzie sú dostupné priamo na stránkach výrobcu programu. Častým dôvodom sprístupnenia počítačového programu v takejto verzii je záujem výrobcov na tom, aby záujemcovia o program si ho voľne stiahli, odskúšali a následne sa rozhodli, či si zakúpia k nemu licenciu. Na druhej strane, negatívom demo verzií mnohých počítačových programov je skutočnosť, že aj keď majú síce obmedzené použitie (napr. na dobu 15 dní), pri ich *cracknutí* sa stávajú plnohodnotnými programami. Mnoho ľudí vyhľadáva práve demo verzie programov na oficiálnych stránkach ich výrobcov a následne vyhľadávajú k nim *crack*. Je vhodné však poukázať, že takéto konanie je záležitosťou šikovnejších užívateľov internetu, keďže drvivá väčšina užívateľov počítačov a internetu nemá o tom vedomosť.

Cracking prešiel vývojom a stretávame sa takisto s jeho sofistikovanejšou podobou, ktorou je *preCracking*, keď počítačový program je pre-cracknutý (angl. *preCracked*). Ide o takú úpravu počítačového programu, ktorého zabezpečenie je odstránené. *Crackerom* je vytvorená úplne nová inštalačná verzia programu, ktorá počas inštalácie alebo po inštalácii nevyžaduje licenciu. *Cracker* nezasiahol do funkcionality programu, ale „iba" chýba jeho ochrana pred nelegálnym

používaním. Pre-cracknuté verzie sa od „tradičného" spôsobu *cracknutia* líšia tým, že cracknuté súbory sú skopírované už v rámci inštalácie programu, t. j. ide o modifikáciu inštalačného procesu. Takto upravené verzie počítačových programov sú veľmi obľúbené, keďže ich úspešné nainštalovanie do počítača vyžaduje „iba" opakované stláčanie tlačidla „Ďalej/Next" a na záver tlačidla „Ukončiť/Finish", pričom po úspešnom nainštalovaní sa objaví poďakovanie „*Thank you for your installation!*". Takto upravené programy sú dostupné spravidla na internete prostredníctvom serverov s úložiskami dát alebo prostredníctvom technológie *peer-to-peer* (P2P) – slangovo „cez torrenty", keď ich zdieľajú užívatelia internetu medzi sebou. Po ich stiahnutí nič nebráni tomu, aby boli jednoducho nainštalované a plnohodnotne používané, ale, samozrejme, nelegálne (viac pozri text nižšie – Porušovanie autorských práv prostredníctvom „.torrent-ov", pozn. autorov).

V neposlednom rade je vhodné poukázať na skutočnosť, že crack v podobe inštalačného súboru (*.exe), ktorý po jeho spustení automaticky prelomí zabezpečenie počítačového programu, alebo aj pre-cracknutý počítačový program, vôbec nemusí byť pre užívateľa „užitočný". Často ide o podvodné triky, pri ktorých dochádza k spusteniu škodlivého programu, ktorý nainštaluje do počítača škodlivý *malware* (pozri text nižšie, pozn. autorov).

1.5.3 Warez (a linking)

Pojmom *warez* sú označované autorským právom chránené diela, ktorých právna ochrana je porušená do takej miery, že sú sprístupnené na internete k voľnému stiahnutiu. Ide hlavne o počítačové programy, hudobné diela, audiovizuálne diela (filmy či seriály).[55] *Warez* sa stal celosvetovo závažným problémom, pričom môžeme pozorovať určitú koreláciu vo vzťahu k postupnému rozširovaniu a vývoju informačných a komunikačných technológií. Práve internet je miestom, kde sa veľmi výrazne prejavuje jeden z pojmových znakov všetkých predmetov duševného vlastníctva – možná všadeprítomnosť (potenciálna ubikvita).[56]

[55] SCHULTZ, M. Copynorms: Copyright and Social Norms. In YU, P. K. (ed.) *Intellectual Property and Information Wealth: Issues and Practices in the Digital Age. Volume 1*: *Copyright and Related Rights*. Westport : Praeger Publishers, 2007, ISBN 0-275-98883-X, p. 213; SCHWABACH, A. *Internet and the Law*: *Technology, Society and Compromises*. 2nd edition. Santa Barbara : ABC-Clio, 2014, ISBN 978-1-61069-350-9, p. 247 - 248.

[56] LAZÍKOVÁ, J. *Základy práva duševného vlastníctva*. Bratislava : Iura edition, 2012, ISBN 978-80-8078-476-8, s. 14.

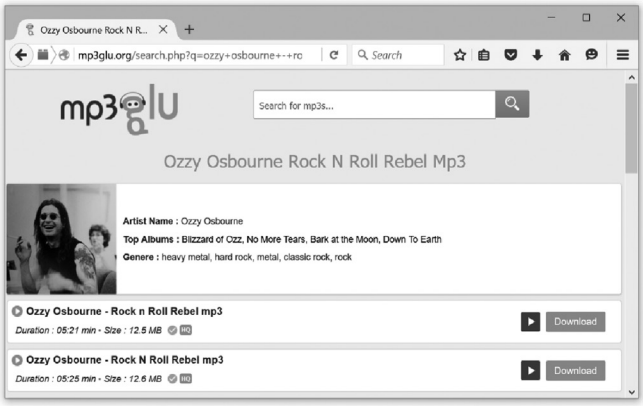
Pre svoju dostupnosť, vysokým prenosovým rýchlostiam, vysokému počtu používateľov a relatívne vysokej anonymite sa internet postupne stal veľmi atraktívnym spôsobom (miestom) porušovania autorských práv. Aj používateľ s priemernou počítačovou gramotnosťou sa veľmi rýchlo dokáže dostať k verejnosti sprístupneným autorským dielam a použiť ich bez toho, aby bol na takúto činnosť oprávnený licenčnou zmluvou, resp. zákonnou licenciou.[57]

Zdvojenou nádobou *warezu* je *linking,* t. j. linkovanie. Ide o neoprávnené zdieľanie súborov obsahujúcich autorským právom chránené diela, predovšetkým počítačové programy, hudobné diela a audiovizuálne diela (filmy či seriály). Páchatelia *linkingu* zneužívajú služby internetových stránok a serverov, ktoré umožňujú ukladanie súborov online (*File Hosting Services*). Linky, t. j. odkazy na takto uložené súbory, sprístupňujú napríklad na internetových stránkach venovaných *warezu*, na blogoch či diskusných fórach (tzv. *warez* fóra). Na jednej strane je takýmto spôsobom veľmi jednoduché stiahnuť z internetu nelegálnu rozmnoženinu ktoréhokoľvek diela. Podmienkou je, že dielo je „zašité na internete" a zároveň je prístupná *linka* (odkaz), ktorá presmeruje užívateľa internetu k sťahovaniu. Na druhej strane, životnosť takýchto liniek je problematická. Niektoré linky majú životnosť v týždňoch, iné v mesiacoch. Len v ojedinelých prípadoch *linka* je aktívna celé roky. To je zapríčinené tým, že správcovia serverov, na ktorých takéto súbory sú „zašité na internete", ich pri objavení premazávajú (mali by premazávať).

Príkladom *warezu* a zároveň *linkingu*, pokiaľ ide o hudobné diela, je internetová stránka <www.mp3glu.org>. Stránka obsahuje vyhľadávač, do ktorého je potrebné napísať názov hľadaného materiálu a spustiť vyhľadávanie. V našom prípade sme zadali spojenie „ozzy osbourne – rock n roll rebel" (*Rock ‚n' Roll Rebel* je pieseň *Ozzyho Osbourna na* albume *Bark at the Moon*[58]). Výsledok hľadania je rozsiahly, pričom poukazujeme len na časť výsledkov. Na nižšie uvedenom vyobrazení výsledkov je výpis s *linkami* na nájdené súbory.

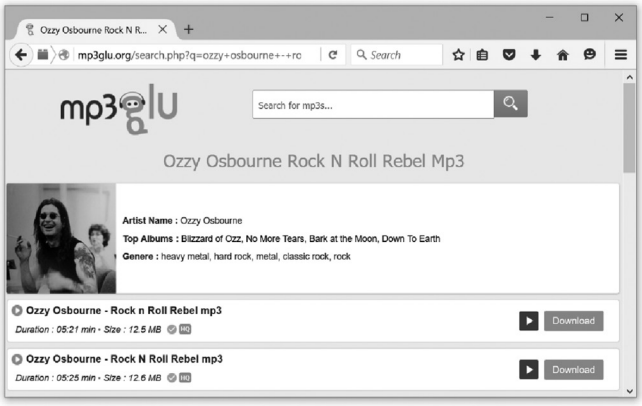
[57] SUCHAR, M. *Počítačová kriminalita ako európsky trestný čin.* Diplomová práca. Bratislava : Fakulta páva Paneurópskej vysokej školy, 2015, s. 26 (vedúci práce – Libor Klimek).

[58] Ozzy Osbourne *Rock 'n' Roll Rebel. LP Bark at the Moon*. London : CBS Records, 1983, pieseň A1.



obr. č. 3: internetová stránka mp3glu.com s výsledkami vyhľadávania a *linkingom*
zdroj: Libor Klimek – snímok vlastnej obrazovky (*screenshot*)

Po stlačení tlačidla „Download", ktoré je v tomto prípade *linkou*, dôjde k presmerovaniu a následnému sťahovaniu konkrétneho súboru. Aj keď sa stránka nazýva <www.mp3glu.org>, samotný súbor je umiestnený na stránke <http://cache.glujar.com>, ako to znázorňuje nasledujúci snímok.



obr. č. 4: internetová stránka mp3glu.com s presmerovaním sťahovania
zdroj: Libor Klimek – snímok vlastnej obrazovky (*screenshot*)

1.5.4 Porušovanie autorských práv prostredníctvom „.torrent-ov"

Porušovanie autorských práv prostredníctvom „.torrent-ov" (ďalej len „torrenty") je omnoho sofistikovanejšou formou porušovania autorských práv ako v podobe *warezu*. Možno veľmi zjednodušene konštatovať, že kým „amatéri" sťahujú prostredníctvom *warezu*, „profesionáli" sťahujú prostredníctvom *torrentov*. Za uplynulých 15 rokov sa *torrenty* stali dominantou súčasťou v oblasti porušovania autorských práv prostredníctvom internetu. Otázka *torrentov* je mimoriadne širokou polemikou, ktorá by si zaslúžila pozornosť v rozsahu samostatnej monografie, ktorá by záujemcu vtiahla do histórie *torrentov*, do detailného procesu ilegálneho zdieľania a sťahovania súborov, ochrany pred odhalením[59], výskumu spôsobených škôd a podobne. Autori sa však v nasledujúcom texte obmedzujú na základné poznatky predmetnej problematiky.

Právna ochrana autorských diel absolútne zlyháva v prípade nelegálneho sťahovania prostredníctvom tzv. *torrentov*. Takýto spôsob ich nadobudnutia otvára možnosti takmer neobmedzeného množstva nelegálne stiahnutého materiálu či súborov. Na jednej strane je prostredníctvom *torrentov* možné ilegálne stiahnuť takmer všetok autorským právom chránený materiál – počítačové programy vrátanie operačných systémov a hier, hudobné diela (nielen celé albumy, ale dokonca celé diskografie), televízne seriály či filmové diela vrátane pornografie, a v neposlednom rade aj knihy. Na druhej strane, *torrenty* sa takmer vôbec netýkajú voľne dostupného materiálu alebo súkromných dát (napr. osobné fotografie, videá a pod.).

Sťahovanie prostredníctvom *torrentov* využíva technológiu *peer-to-peer* (označovaná aj ako P2P).[60] Prvým krokom je inštalácia a spustenie programu, ktorý s nimi pracuje. Takého programy sú pomenované *torrent klienti* – napríklad *µTorrent*[61] alebo *BitTorrent*[62] – a sú voľne dostupné na internete. Je irelevantné, ktorý *torrent klient* je používaný konkrétnym užívateľom internetu,

[59] Pozri: BAILEY, M.: *Complete Guide to Anonymous Torrent Downloading & File Sharing*. Nerel Publications, 2013, ISBN 978-3950309317, 66 strán.

[60] Bližšie pozri napríklad: ORAM, A. (ed.) *Peer-to-Peer*: *Harnessing the Power of Disruptive Technologies*. Sebastopol : O'Reilly & Associates, 2001, ISBN 978-0-596-00110-0, 450 strán; BUFORD, J. – YU, H. et LUA, E. K. *P2P*: *Networking and Applications*. Burlington : Morgan Kaufmann Publishers, 2009, ISBN 978-0-12-374214-8, 408 strán; GIBLIN, R. *Code Wars*: *10 Years of P2P Software Litigation*. Cheltenham : Edward Elgar Publishing, 2011, ISBN 978-1-84980-621-3, 272 strán.

[61] Pozri <www.utorrent.com>.

[62] Pozri <www.bittorrent.com>.

keďže klienti navzájom spravidla spolupracujú. Tieto programy však sami osebe nesťahujú počítačové programy, hudbu, filmy, knihy a podobne, ale potrebujú prostredníka – súbor pomenovaný „torrent" (*.torrent). Takýto súbor obsahuje tzv. *tracker*, ktorý sprostredkúva komunikáciu medzi torrent klientami.

Zaujímavé je, že „cez torrenty" nedochádza k sťahovaniu z online stránok, ale z počítačov užívateľov internetu, ktorí sú pripojení k internetu v reálnom čase. Sťahovanie prebieha buď od jedného užívateľa, alebo od viacerých naraz. *Torrent klient* sťahuje „balíky" údajov od iných používateľov *torrent klientov*, ktoré na pevnom disku spája do celých súborov, až kým nedôjde k stiahnutiu celého materiálu. Nie je výnimočné, že v tom istom čase prebieha sťahovanie od desiatok užívateľov naraz, pričom rýchlosť sťahovania dosahuje vysoké hodnoty. Napríklad hudobný album vo formáte mp3 je možné stiahnuť za niekoľko minút alebo film v podobe DVD alebo HD súborov za necelú hodinu. Na druhej strane, *peer-to-peer* technológia neumožňuje „iba" sťahovanie dát, ale ide o dvojsmerný proces. Každý užívateľ popri sťahovaní musí zároveň odosielať dáta, keďže odosielanie je automatické.[63]

Užívateľ torrent klienta, ktorý zdieľa súbory dostupné na sťahovanie prostredníctvom *peer-to-peer* technológií, je pomenovaný *peer*. *Peerovia* sú rozdelení do dvoch skupín – *seederovia* a *leecheri*. *Seederovia* zdieľajú na svojich počítačoch kompletné súbory s nelegálnym materiálom – napríklad kompletné inštalačné súbory počítačového programu, kompletný hudobný album vo formáte .mp3 alebo plnú verziu filmu. *Leecheri* nemajú kompletné súbory, ale sú v procese ich získavania sťahovaním od iných *peerov*, pričom môžu šíriť už aj nekompletné dáta. *Peerovia* navzájom sťahujú súbory, pričom aspoň jeden z nich musel na začiatku mať kompletný materiál. Od toho je odvodené spojenie *peer-to-peer*.

[63] Na druhej strane, odosielanie dát je možné v mnohých klientoch zakázať, resp. limitovať, napríklad na rýchlosť 5 kB/s. Odosielanie dát je možné takisto zablokovať aj cez FireWall. No takýmito opatreniami môže dôjsť k podstatnému zníženiu rýchlosti sťahovania.