Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra práva

Diplomová práce

Počítačová kriminalita v ČR se zaměřením na registrované a objasněné kybernetické komerční trestné činy páchané proti dětem

Bc. Martin Martínek

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Martin Martínek

Hospodářská politika a správa
Veřejná správa a regionální rozvoj

Název práce

Počítačová kriminalita v ČR se zaměřením na registrované a objasněné kybernetické komerční trestné činy páchané proti dětem

Název anglicky

Cyber Crime in the Czech Republic Focused on Registered and Explained Cybercrime Commercial Crimes Against Children

---

Cíle práce

- Objasnění tendencí vývoje a forem počítačové kriminality a její právní regulace mezinárodní, v EU a ČR
- Analýza problémů a překážek odhalování a dokazování kybernetických komerčních trestných činů páchaných proti dětem z hlediska platného práva v ČR
- Analýza registrovaných a objasněných komerčních trestných činů páchaných proti dětem, vyhodnocení příčin neobjasněnosti těchto trestných činů a posouzení vlivu sociálního prostředí
- Vyhodnocení možnosti prevence

Metodika

Práce bude rozdělena na teoretickou a praktickou část.

V teoretické části bude shromážděno maximum informací z literatury, informačních médií a statistik Policie České republiky v průběhu delšího časového období s návazností na technický vývoj. Bude použita metoda literární rešerše, výkladu práva, analýzy právní úpravy a komparativní metoda.

V praktické části bude použita metoda statistické analýzy pro objasnění tendencí vývoje a forem počítačové kriminality a její právní regulace mezinárodní, v EU a ČR. S využitím případových studií bude provedena analýza problémů a překážek odhalování a dokazování kybernetických komerčních trestných činů páchaných proti dětem z hlediska platného práva v ČR. Dále bude použita analýza registrovaných a objasněných komerčních trestných činů páchaných proti dětem, vyhodnocení příčin neobjasněnosti těchto trestných činů a posouzení vlivu sociálního prostředí. Za použití kvantitativní metody dotazníkového šetření budou formulovány současné možnosti prevence a obrany proti těmto trestným činům.

Doporučený rozsah práce

60-80 stran

Klíčová slova

Počítačová kriminalita, kybernetický trestný čin, osobní údaje, sdílená data, datové úložiště, oběti a pachatelé, skrytá identita, sociální prostředí

Doporučené zdroje informací

- GŘIVNA, Tomáš a POLČÁK, Radim, Kyberkriminalita a právo, vyd. Praha: Auditorium 2008, 220 s., ISBN 978-809-0378-674
- JIRÁSEK Petr, NOVÁK Luděk, POŽÁR Josef, Výkladový slovník kybernetické bezpečnosti, vyd. Policejní akademie 2015, 242 s., ISBN 978-80-7251-436-6
- JIROVSKÝ Václav, Kybernetická kriminalita – nejen o hackingu, crackingu, virech a trojských koních bez tajemství, vyd. Praha 2007, 284 s., ISBN: 978-80247-1561-2
- KALVODOVÁ Věra, HRUŠÁKVÁ Milana a kolektiv, Dokazování v trestním řízení – právní, kriminologické a kriminalistické aspekty, vyd.: Brno: Masarykova univerzita, 2015, 503s. ISBN978-80-210-8072-0
- KOLOUCH, Jan. Cybercrime. vyd. CZ.NIC, z.s.p.o., 2016, 528 s., ISBN 978-80-88168-18-8, dostupné z
- KOLOUCH J. VOLOVECKÝ P., Trestně právní ochrana před kybernetickou kriminalitou, vyd. Policejní akademie 2013, 117 s., ISBN: 978-80-7251402-1
- MATĚJKA, Michal, Počítačová Kriminalita, vyd. Praha: Computer Press, 2002, 106s. ISBN 80-7226-419-2
- SMEJKAL Vladimír, Internet @ §§§, vyd. Grada 1999, 168 s., ISBN: 807169-765-6
- Zároveň další literatura podle pokynů vedoucí DP
- ZOUBKOVÁ I., FIRSTOVÁ J. a kol., Kriminologie – aktuální problémy, vyd. Praha: Policejní akademie 2013, 270 s., ISBN 978-80-7251-395-6

Předběžný termín obhajoby

2019/20 LS – PEF

Vedoucí práce

JUDr. Jitka Mráčková, CSc.

Garantující pracoviště

Katedra práva

Elektronicky schváleno dne 18. 9. 2019

JUDr. Jana Borská, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 14. 10. 2019

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 21. 02. 2020

Čestné prohlášení

Prohlašuji, že svou diplomovou práci " Počítačová kriminalita v ČR se zaměřením na registrované a objasněné kybernetické komerční trestné činy páchané proti dětem " jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 4. dubna 2020 _____

Poděkování

Rád bych touto cestou poděkoval JUDr. Jitce Mráčkové CSc., za cenné připomínky, rady, ochotu a skvělé odborné vedení, které mi věnovala po celou dobu zpracovávání diplomové práce. Také chci poděkovat mojí rodině, která mě v průběhu celého studia podporovala a vytvářela mi tak potřebné harmonické zázemí.

Počítačová kriminalita v ČR se zaměřením na registrované a objasněné kybernetické komerční trestné činy páchané proti dětem

Abstrakt

Diplomová práce „Počítačová kriminalita v České republice se zaměřením na registrované a objasněné kybernetické komerční trestné činy páchané proti dětem„ se zabývá oblastí trestné činnosti, kde jsou děti zneužívány k výrobě dětské pornografie z důvodu dalšího komerčního využití těchto produktů. Analyzuje postupný právní vývoj v mezinárodní, evropské a zejména národní právní úpravě v České republice, kdy právní úprava se postupně musela adaptovat směrem k možnostem postihování tohoto nezákonného jednání. Materiály s tématikou dětské pornografie se začaly díky používání nových komunikačních technologií v lidské společnosti nezadržitelně šířit. Práce analyzuje problémy neobjasněnosti v této oblasti kyberkriminality a zaměřuje se i na jejich příčiny. Zkoumá i souvislost těchto činů se sociálním prostředím. Vyhodnotí tuto trestnou činnost i v návaznosti na celé území ČR se zpracováním statistické analýzy v rámci krajů. Zároveň jsou v práci zahrnuty i možnosti prevence před tímto druhem kyberkriminality a to z pohledu technického, právního a ekonomického.

Klíčová slova: Počítačová kriminalita, kybernetický trestný čin, kryptoměna, osobní údaje, sdílená data, datové úložiště, oběti a pachatelé, skrytá identita, sociální prostředí, kyberprostor, počítač, internet.

Cyber Crime in the Czech Republic Focused on Registered and Explained Cybercrime Commercial Crimes Against Children

Abstract

The diploma thesis „Computer Crime in The Czech Republic focused to Commercial Cyber Crime perpetrated on children which has been registered and clarified". Thesis deals with children who are abused for the production of child pornography for further commercial use of these materials. The thesis analyzes the gradual legal development in International, European area and especially legislation in the Czech Republic. The legislation had to gradually adapt itself and developed its possibilities of sanctions this unlawful conduct. Child pornography materials has started to spread unstoppably due to the huge development of ICT in a society. The thesis analyzes problems of unclearness in this area of cybercrime and focus on their causes. It also examines the link among these acts and the social environments. It will evaluate this crime also in relation to the whole territory of the Czech Republic with the processing of statistical analysis within the regions. At the same time, the thesis also includes the possibilities of prevention of theese cybercrime from the technical, legal and economic point of view.

Keywords: Cybercrime, cryptocurrency, personal data, shared data, data storage, victims and perpetrators, hidden identity, social environment, cyberspace, computer, internet.

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

ČR	Česká republika
USA	Spojené státy americké
EU	Evropská unie
ES	Evropská společenství
OSN	Organizace spojených národů
PČR	Policie České republiky
NCOZ	Národní centrála organizovaného zločinu
ETŘ	Evidence trestního řízení
ICT	Information and Communication Technologies
Web	World Wide Web
IP	IP address
atd.	a tak dále
tzv.	tak zvaně
sms	textová zpráva
mms	obrazová zpráva
NBÚ	Národní bezpečnostní úřad
TSK	takticko-statistické klasifikace

1 Úvod

„Všichni se pohybujeme prostorem a časem. Jde jen o to JAK, KAM a CO tady po sobě zanecháme. “

MM autor práce

Počítačová kriminalita je v současnosti a zároveň i do budoucna velice vyhledávaným druhem páchané trestné činnosti. Velká možnost anonymity pachatelů je jedním z hlavních důvodů, proč dochází k nárůstu takto páchané trestné činnosti a má jednoznačně zvyšující se tendenci. Proniknete-li hlouběji a nahlédnete-li alespoň částečně za horizont, zjistíte souvislosti, které nejsou na první pohled vidět, kdy právě tyto souvislosti byly, jsou a budou velice důležité, jak při samotném páchání trestné činnosti, tak při jejím odhalování a následném dokazování.

Úkolem diplomové práce je zanalyzovat právní úpravu kybernetických trestných činů se zaměřením na dětskou pornografii a to dle mezinárodního práva, práva EU a rovněž právní úpravy v České republice. Práce se zaměří na počet evidovaných a následně objasněných trestných činů v návaznosti na důvody a vlivy, které vedly k neobjasnění této kyberkriminality. Zároveň práce ukáže bariéry, které znemožňují odhalování a dokazování této trestné činnosti. V závěru budou navrhnuty možnosti prevence proti této trestné činnosti a to jak z pozice právní, tak i z pozice možných technických řešení.

Tato diplomová práce se ve své teoretické části nebude zabývat pouze různými formami počítačové kriminality, ale také její právní úpravou. I když byly celosvětově provedené změny vedoucí ke sjednocení legislativy a postupů, není vše tak úplně jednotné a právě některé nedostatky mohou zapříčinit i složitější možnost průchodu spravedlnosti.

Teoretická část se zaměří právě na kybernetické trestné činy páchané proti dětem v českém prostředí a zároveň ukáže různé druhy bariér, které ztěžují již samotné odhalování, tak i následné dokazování této závažné trestné činnosti. Jde o bariéry, které i při pročítání trestních spisů nejsou na první pohled vůbec viditelné a člověk, který není s touto problematikou blíže seznámen ani neví, co někdy pouhá formulace, nebo nedostatečný právní výklad v zákoně zapříčiní.

Praktická část bude zaměřena na analýzu této oblasti trestné činnosti a to, jak statistickou za určité období, tak na hlavní příčiny, kvůli kterým se některé trestné činy nepodařilo objasnit. V jedné části se bude práce věnovat i důležitému vlivu sociálního prostředí, které značnou

měrou působí jak na pachatele, tak i na jejich oběti. Tento vliv bude zřetelně patrný na četnosti činů v různých regionech naší republiky.

Součástí práce je i případová studie, na které je možné sledovat různé vlivy, které se právě v této trestné činnosti objevují a které jí ovlivňují.

Práce se také věnuje vyhodnocení možností prevence v boji proti této trestné činnosti a to jak po technické stránce řešení, tak po stránce zahrnující právní a ekonomické důsledky. Očekávanými výstupy této práce je globálnější pochopení rizik počítačové kriminality, kdy právě část, která se dotýká dětí, je velmi citlivá. Uvědomění si problému jako celku i s jeho skrytými stránkami je velice důležité a to jak při přístupu v boji proti této formě trestné činnosti, tak i při přístupu k prevenci a razantní eliminaci.

2 Cíl práce a metodika

2.1 Cíl práce

Tato práce si klade za cíl objasnění tendencí vývoje a forem počítačové kriminality a to včetně dostupných technických možností internetu. Uvede různé právní regulace v oblasti mezinárodního práva, práva EU a práva v rámci České republiky. Porovná tato nařízení i zákony a ukáže benevolenci stěžejních nařízení, které již v samotném počátku dávají pro jejich realizaci manévrovatelný prostor, dle uvážení konkrétního státu, v jejich uvedení do platných právních norem.

Zanalyzuje hlavní problémy a překážky při odhalování a dokazování kybernetických komerčních trestných činů páchaných proti dětem z hlediska platného práva v České republice.

Cílem praktické části je i statistické vyjádření v určeném časovém období, změny v počtu těchto činů, což ukáže přímou souvislost s technickým vývojem kybernetického vzestupu. Práce se pokusí zanalyzovat, jak velký vliv představuje sociální prostředí, ve kterém se oběti i pachatelé pohybují. Tato zjištění budou doplňkově vyjadřovat fakta z případové studie, ze které budou vyplývat důležité výstupy, které je nutné do budoucna učinit pro další eliminaci zasahujících faktorů.

2.2 Metodika

Práce je rozdělena na teoretickou a praktickou část. V teoretické části je provedena analýza platných právních úprav, podle kterých je k těmto trestným činům přistupováno ve světě a v ČR. Komparativní metoda tyto rozdíly vyhodnotí a srovná dostupné právní úpravy. Analytická metoda je použita hlavně pro srovnání obsahu právního výkladu a jeho uplatnění v praxi. Pro lepší pochopení problematiky počítačové kriminality bude použita historická metoda vývoje a vzestupu kyberkriminality, co by globální hrozby. Použita bude také metoda výkladu práva, která je podložena texty z těchto výkladů a odbornou literaturou. Bude použita i metoda literární rešerše, která ukáže rozdíly při nahlížení na tuto problematiku kyberkrimunality. Syntézou analýz registrovaných a objasněných komerčních trestných činů páchaných proti dětem bude vyhodnocena příčina neobjasněnosti těchto trestných činů.

V praktické části za použití metody statistické analýzy se práce pokusí zanalyzovat vliv sociálního prostředí na páchání této trestné činnosti v jednotlivých krajích ČR. Provedena je i analýza registrovaných a objasněných komerčních trestných činů páchaných proti dětem.

S využitím případové studie je provedena analýza problémů a překážek odhalování a dokazování kybernetických komerčních trestných činů páchaných proti dětem z hlediska platného práva v České republice. Jako další cíl praktické části je zhodnocení technických, právních a ekonomických možností prevence a jejich reálnost zavedení do praxe s přihlédnutím na složitost realizace. Cíle bude dosaženo pomocí návrhu řešení v jednotlivých oblastech zkoumání.

Analýza technických možností ukáže, jakým směrem by se kybernetická prevence mohla ubírat. Celková analýza ukáže, jak „moc, a nebo málo," jsme v globálním hledisku chráněni před touto formou kriminality. K získání dat byly mnohdy použity internetové zdroje a zdroje Policie České republiky, protože problematika kybernetických činů se specializací na komerční trestné činy zaměřené proti dětem není v dostupné odborné literatuře příliš zastoupena a publikována.

3 Teoretická část

3.1 Počítačová kriminalita, jako nová forma kriminality

3.1.1 Úvod do problematiky

Počítačová kriminalita začala být více vnímána až v posledních desetiletích. Nejdůležitější pro počítačovou kriminalitu je právě vzájemné propojení počítačů systémem. Prvotní propojení počítačů včetně komunikačních uzlů se uskutečnilo v USA. Tam byly v roce 1969 propojeny tři univerzity. Dvě z nich se nacházely v Kalifornii[1] a třetí byla až v Utahu[2]. První počítačová síť byla nazvána ARPANET[3]. Název byl odvozený od zkratky amerického oddělení obrany ARPA[4], které také celý projekt financovalo. V roce 1972 bylo sítí Arpanet propojeno celkem 23 počítačů po celém území USA. První globální[5] síť vznikla již koncem 80. let, kdy se začala prvotně sdílet data a propojovat systémy a to právě díky Internetu. Internet je *„globální systém propojených počítačových sítí, které používají standardní internetový protokol (TCP/IP). Internet slouží miliardám uživatelů po celém světě. Je to síť sítí, která se skládá z milionů soukromých, veřejných, akademických, obchodních a vládních sítí, s místním až globálním rozsahem, které jsou propojeny širokou škálu elektronických, bezdrátových a optických síťových technologií.“*[6]

V té době se také na internetu začínají objevovat prvotní náznaky počítačové kriminality[7] páchané prostřednictvím této globální sítě. V samotných začátcích se počítačová kriminalita v této oblasti týkala převážně napadání systému zvenčí za účelem ochromení funkčnosti, nebo jeho alespoň dočasné eliminace. Jeden z prvních útoků[8] byl veden proti vládním zpravodajským serverům Ukrajiny, Estonska a Jižní Osetie, kdy v důsledku tohoto útoku byl

[1] Kalifornie je státem USA a nachází se na západním pobřeží USA
[2] Utah je státem USA a nachází se v západním hornaté části USA
[3] ARPANET – složení dvou slov ARPA (kapitola 2.1.1) + NET –network anglicky v překladu SÍŤ
[4] ARPA - Advanced Research Projects Agency- Grantová agentura ministerstva obrany USA [online] [citace20.2.2020]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=40844
[5] Globální síť - Za globální síť se považuje taková síť, která je využívána celosvětově. Nejtypičtějším sítě tohoto druhu je Internet, který dnes pokrývá celý svět. [online] [citace20.2.2020]. Dostupné z http://protiproud.wz.cz/_informatika/GAN.htm
[6] Jirásek Petr, Novák Luděk, Požár Josef – Výkladový slovník kybernetické bezpečnosti, Policejní akademie ČR 2015, ISBN 978-80-7251-397-0 , str. 49
[7] Policie České republiky –Počítačová kriminalita „*Počítačová kriminalita je novodobý fenomén. Jde o podvodné jednání osob, využívajících veřejné sítě jako nástroje k páchání běžných podvodů. Internet slouží zejména k možnosti širšího oslovení potencionálních obětí a současně pak jako anonymizační prvek v rámci provedeného podvodu*“ [online] [citace 20.2.2020]. dostupné z: https://www.policie.cz/clanek/pomoc-obetem-tc-pocitacova-kriminalita.aspx
[8] NATOAKTUAL [online] [citace20.2.2020] dostupné z :https://www.natoaktual.cz/rusko-gruzinska-valka-deset-lekci-pro-estonsko-frv-/na_analyzy.aspx?c=A130820_112918_na_analyzy_m02

serverům zablokován dálkový přístup na webové stránky[9], ze kterých byla vládními servery čerpána důležitá data. Útoků mezi roky 2007 až 2009 bylo několik a byly provedeny vždy z vnějšího prostředí po síti[10]. V těchto případech bylo za hlavní cíl útoku vybráno ochromení funkčnosti komunikace v rámci státní správy a ukázka možnosti ochromení obranných složek států. Další závažný počítačový kybernetický útok byl uskutečněn ze strany čínské vlády proti Vietnamské republice v roce 2011. Tam byly použity blokace hypertextových odkazů[11].

Počítačová kriminalita začala postupně pronikat do různých částí kriminality. Jako první se v České republice začala rozvíjet majetková kriminalita ve spojení s počítači, až v době po roce 2005. V USA již bylo možné v roce 1992 zakoupení zboží prostřednictvím internetu, ale tento trend do Evropy a především k nám do České republiky dorazil se zpožděním v roce 2005. Mezi prvními trestnými činy v této oblasti byly majetkové podvody formou záloh zaslaných předem za objednané a nedoručené zboží spojené postupem času s inzercí neexistujícího zboží, služeb a podobně. Policie České republiky[12] začala kybernetickou kriminalitu[13] evidovat až od roku 2011[14] v rámci ETŘ[15]. Evidenčnímu systému v rámci PČR předcházel evidenční systém pod názvem ZIS 2000[16], který neumožňoval kybernetické trestné činy do systému vůbec vložit a to z toho důvodu, že nebyly do systému vůbec zaneseny. ETŘ se na

[9] WWW -World Wide Web hypertextový prohlížeč, který umožňuje prostřednictvím internetu zobrazovat obrázky, text, videa atd. zdroj - Pavel Satrapa - Internetový protokol IPV6 čtvrté vydání – Praha 2019 ISBN 978-80-88168-46-1 str. 22

[10] CESES - Kyberhrozby a kyberterorismus – kybernetické války [online] [citace20.2.2020]. Dostupné z: https://ceses.cuni.cz/CESES-70-version1-Kyber.pdf

[11] Hypertextový odkaz – může být obrázek, text, nebo nějaké místo na stránce, které je spojené s jinou stránkou a to buď na stejném serveru, nebo kdekoliv v internetové síti , [online] [citace20.2.2020].Dostupné z: http://www.ped.muni.cz/wtech/03_studium/cvt5/cvt5-07.pdf

[12] PČR – Policie České republiky *„Policie České republiky je jednotný ozbrojený bezpečnostní sbor zřízený zákonem České národní rady ze dne 21. června 1991. Slouží veřejnosti. Jejím úkolem je chránit bezpečnost osob a majetku, chránit veřejný pořádek a předcházet trestné činnosti. Plní rovněž úkoly podle trestního řádu a další úkoly na úseku vnitřního pořádku a bezpečnosti svěřené jí zákony, předpisy Evropských společenství a mezinárodními smlouvami, které jsou součástí právního řádu České republiky.“* [online] [citace20.2.2020]. Dostupné z: https://www.policie.cz/clanek/o-nas-policie-ceske-republiky-policie-ceske-republiky.aspx

[13] Jirásek Petr, Novák Luděk, Požár Josef – Výkladový slovník kybernetické bezpečnosti, Policejní akademie ČR 2015, ISBN 978-80-7251-397-0, str. 57

[14] Policie České republiky – Statistika kyberkriminality [online] [citace20.2.2020]. *Statistické vykazování trestné činnosti páchané prostřednictvím internetu a dalších sociálních sítí je vedeno od roku 2011, relevantní data za léta 2005 – 2010 tedy nejsou k dispozici. Data za celou Policii České republiky jsou obsahem přiložené tabulky. Dále povinný subjekt upozornil, že „kyberkriminalita“ je sledována až od roku 2011. Kyberkriminalitu rozlišuje Policie České republiky na kategorie:* spácháno internetem a spácháno ostatními sítěmi. *Konkrétní data naleznete v přiložené tabulce. Statistika Policie České republiky eviduje spáchané trestné činy (včetně příprav a pokusů), v současné době neexistují oficiální odhady míry latentní kriminality. Rovněž neexistuje metodika, jak provádět výpočty nebo spíše odhady množství a výše škod v souvislosti s latentní kriminalitou.* Dostupné z: https://www.policie.cz/clanek/statistika-kyberkriminality.aspx

[15] ETŘ – Evidence trestního řízení zpracovávané v rámci interního systému Policie České republiky

[16] ZIS 2000 – základní informační systém Policie České republiky, zaváděný na útvary od roku 2000 do roku 2004

útvary policie začalo postupně zavádět až od roku 2004. Rafinovanost pachatelů a propracovanost páchání se postupem času zvětšovala a počet podvedených, zneužitých lidí prostřednictvím internetu nezadržitelně stoupal. Počítačová kriminalita se časově vyvíjela a začala pronikat do všech možných směrů působnosti lidské existence.

3.1.2 Pojem počítačová kriminalita a její formy

Na začátku této části práce je nutné pro pochopení problematiky počítačové kriminality definovat některé základní pojmy. Tyto pojmy se přímo vztahují k počítačové kriminalitě a nebo s ní po technické stránce úzce souvisí. Po seznámení se s těmito základními pojmy bude počítačová kriminalita blíže definována.

Kybernetický prostor – tento pojem byl odvozen z beletristické literatury

„*Digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, službami a sítěmi elektronických komunikací.“*[17]

Informace – „*Každý znakový projev, který má smysl pro komunikátora i příjemce.“*[18]

Informaci můžeme vyjádřit i takto – jedná se o sdělení o objektech, událostech, myšlenkách. Jde o jistou formu sdělení, která má svůj specifický význam. Jako měřitelná jednotka ve světě výpočetní techniky je brán jeden bit (1 bt.). Jde o měřitelnou jednotku, podle které můžeme rozlišit velikost toku informace, nebo celkový obsah zprávy, který je odeslán, nebo uložen. Dle velikosti informace se bit navyšuje na kilobit, megabit, terabit.

Internet – (viz kapitola 3.1.1) v současné době je internet považován za informační veřejný prostředek k šíření informací. Jedná se o přenosové médium. Pro pohyb v této síti je využíván internetový protokol (viz. níže). Na základě připojení z jakéhokoliv místa na světě k této síti se ke konkrétnímu zařízení přiřadí jeho IP adresa (viz. níže), která by měla být jedinečná. Po zadání této adresy se pak můžeme připojit k zařízení odkudkoliv prostřednictvím internetu.

IP adresa - „ *Číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti, která používá IP (internetový protokol) slouží k rozlišení síťových rozhraní připojených k*

[17] Jirásek Petr, Novák Luděk, Požár Josef – Výkladový slovník kybernetické bezpečnosti, Policejní akademie ČR 2015, ISBN 978-80-7251-397-0 , str. 59
[18] Jirásek Petr, Novák Luděk, Požár Josef – Výkladový slovník kybernetické bezpečnosti, Policejní akademie ČR 2015, ISBN 978-80-7251-397-0 str. 45

počítačové síti. V současné době nejrozšířenější verze IPv4 používá 32b číslo zapsané dekadicky po osmicích bitech (např. 123.234.111.222).“ [19]

Definovat IP adresu jde i takto - je to adresa, která obsahuje číslice oddělené tečkami a jednoznačně identifikuje konkrétní síťové zařízení s využitím IP protokolu. Anglicky IP address - je v informatice číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti, která používá IP protokol.

IP protokol – „*Protokol, pomocí kterého spolu komunikují všechna zařízení na Internetu. Dnes nejčastěji používaná je jeho čtvrtá revize (IPv4), postupně se však bude přecházet na novější verzi (IPv6).“*[20]

Z důvodu nedostatku adres je IPv4[21] postupně nahrazován protokolem IPv6,[22] který používá 128bitové IP adresy zapsané hexadecimálně, například 2001:db8:0:1234:0:567:8:

Přechod z protokolu IPV4 byl rychlý. S rostoucím počtem výrobků připojených k internetu rostl i počet dostupných IP adres. Protokol IPV4 zahrnoval celkový počet 2^{32} adres (cca 4×10^9 = 4 miliardy adres). Z důvodu zaplnění tohoto počtu adres dne 3. února 2011 bylo přistoupeno k protokolu IPV6, který již umožňuje přirazení 2^{32} adres (cca 4×10^9 = 4 miliardy adres). V současné době je již vyčerpáno z protokolu zhruba 1.500.000 internetových adres.

Počítač – „*V souladu se zněním CSN 36 9001 se jedná o „stroj na zpracování dat provádějící samočinné posloupnosti různých aritmetických a logických operací“. Jinými slovy: stroj charakterizovaný prací s daty, která probíhá podle předem vytvořeného programu uloženého v jeho paměti.“*[23]

Počítač jde definovat také jako zařízení, které ve výpočetní a informační technice zpracovává data na základě vytvořeného programu. Jedná se o hardware, který představuje hmotnou část počítače, jako je klávesnice, monitor, operační základová deska, zdroj atd.. Pak je součástí

[19] Jirásek Petr, Novák Luděk, Požár Josef – Výkladový slovník kybernetické bezpečnosti, Policejní akademie ČR 2015, ISBN 978-80-7251-397-0 str. 51
[20] Jirásek Petr, Novák Luděk, Požár Josef – Výkladový slovník kybernetické bezpečnosti, Policejní akademie ČR 2015, ISBN 978-80-7251-397-0 str. 50
[21] Pavel Satrapa - Internetový protokol IPV6 čtvrté vydání – Praha 2019 ISBN 978-80-88168-46-1 str. 24
[22] Pavel Satrapa - Internetový protokol IPV6 čtvrté vydání – Praha 2019 ISBN 978-80-88168-46-1 str. 25
[23] Jirásek Petr, Novák Luděk, Požár Josef – Výkladový slovník kybernetické bezpečnosti, Policejní akademie ČR 2015, ISBN 978-80-7251-397-0 str. 68

počítače jeho software – neboli programové vybavení do kterého patří programy a především páteří je operační systém (Windows 7 – 10, Windows XP, Windows Vista, Linux a další).

Data – *„Z pohledu ICT reprezentace informací formalizovaným způsobem vhodným pro komunikaci, výklad a zpracování.“*[24]

Data lze definovat v informační technice, jako data zaznamenána v digitální číselné podobě. Tato data jsou dále zpracována. Obraz, zvuk, číslice jsou převedeny do binární soustavy a ve výsledném rozložení jde pouze o sérii jedniček a nul v číselné řadě.

Sdílená data – **sdílení – „***Možnost společně a současně se dělit o jeden nebo více zdrojů informací, paměti nebo zařízení.“*[25]

Právě internet umožňuje sdílení dat na neomezenou vzdálenost. V síti internet je možné sdílet datové soubory více způsoby. Buď sdílíme soubor z jediného serveru, jako jeho základní kopii, nebo můžeme využít spolupráce ostatních klientů, jako jsme my a sdílet soubory prostřednictvím peer-to-peer P2P (viz. níže). V tomto případě se na procesu stahování souboru podílejí všichni připojení klienti.

P2P – per-to-per -z anglického překladu rovný s rovným *„Aplikační síťový protokol pro přenos dat mezi dvěma počítači v síti a komunikaci uživatelů v uzavřené síti.“*[26]

Kryptoměna – „ *..."virtuální měny" znamenají digitální reprezentaci hodnoty, která není vydávána nebo zaručena centrální bankou nebo veřejným orgánem, nemusí být nutně připojena k legálně vytvořené měně a nemá právní postavení měny nebo peněz, ale je akceptována fyzickými nebo právnickými osobami jako prostředek směny a které lze elektronicky převádět, skladovat a obchodovat*“[27] Kryptoměny[28] jsou využívány v internetové platební síti.

[24] Jirásek Petr, Novák Luděk, Požár Josef – Výkladový slovník kybernetické bezpečnosti, Policejní akademie ČR 2015, ISBN 978-80-7251-397-0 str. 103
[25] Jirásek Petr, Novák Luděk, Požár Josef - Výkladový slovník kybernetické bezpečnosti, Policejní akademie ČR 2015, ISBN 978-80-7251-397-0 str. 87
[26] Završil Aleš - Kyberkriminalita – Právní monografie, ČR 2017, ISBN 978-80-7552-758-2 –kapitola Základní pojmy str. 37
[27] Matusziński Dariusz, 2018 - Co je kryptoměna a jak funguje. In: Český magazín o kryptoměnách - Kryptomagazin.cz [online]. [cit. 20.2.2020]. Dostupné z: https://kryptomagazin.cz/co-je-kryptomena/.
[28] Završil Aleš - Kyberkriminalita – Právní monografie, ČR 2017, ISBN 978-80-7552-758-2 – kapitola Kryptoměny str. 45

Počítačová kriminalita je různá a nelze všechny její formy označovat shodně. Celkem přehledně rozčlenil formy počítačové kriminality Smejkal již v jejich začátcích. Základní členění počítačové kriminality rozdělil do tří oblastí ve vztahu k počítači, jeho vybavení a obsahu na nosičích dat.

„1. Trestné činy ve vztahu k počítači, jeho příslušenství a jiným nosičům informací jako věcem movitým – majetková kriminalita v klasickém významu.

2. Trestné činy ve vztahu k software, k datům, resp. uloženým informacím – neboli informační kriminalita. Řadíme sem trestné činy ve vztahu k programu jako autorskému dílu, neboli útoky na nehmotný majetek.

3. Trestné činy, při nichž je počítač prostředkem k jejich páchání – hospodářská kriminalita. Počítač zde slouží jako hmotný substrát, nástroj zločince, hmotná schránka, ani její obsah nejsou cílem útoku, což ovšem zcela nevylučuje souběh sjednáními podle bodu 2.“[29]

Pojem počítačová kriminalita, může být shodně označen více názvy, jako je kyberkriminalita, internetová kriminalita nebo kybernalita. Podstatou této kriminality je páchání trestných činů prostřednictvím techniky, tedy za využití počítače a také trestné činy směřující proti počítačům. Pachatelé prostřednictvím své techniky získají a zneužijí obsah cizího počítače - média, nebo pouze pozmění určitou elektronickou stopu[30] tak, že následně dojde k její záměně a zneužití. Čím více se počítačová technika, kterou používáme v běžném životě, rozvíjí, tím více se pachatelé zaměřují na zdokonalení svého jednání. Velkou měrou k rozšíření trendu počítačové kriminality přispěl nepochybně Internet, který celý svět počítačově propojil. Současná doba umožňuje připojení prostřednictvím internetové sítě na jakékoli jiné zařízení, které je k síti připojené. A to je ono „kouzlo“ počítačové kriminality. Trestný čin tak můžete spáchat prostřednictvím internetové sítě třeba například v Japonsku a přitom sedět ve svém pokoji doma v České republice. Pachatelé ale nemusí vždy využívat k této trestné činnosti pouze počítače. Rozmanitost těchto trestných činů narůstá. Právě mobilita připojení k internetu je pak problém při odhalování konkrétního pachatele. Pachatel může pro připojení

[29] Smejkal Václav, Počítačová kriminalita: Hrozba budoucnosti, nebo realita dneška? Právní rádce č. 12/1999
[30] Elektronická stopa –„ *Jedná se o informaci, kterou uživatel internetu v tomto virtuálním prostředí po sobě zanechává“* Završil Aleš – Kyberkriminalita – Právní monografie, ČR 2017, ISBN 978-80-7552-758-2 –kapitola Základní pojmy str. 38

na síť využít jakékoli modernější zařízení s datovým modemem[31]. Moderně se tyto technologie označují pod zkratkou ICT[32] (Information and Communication Technologies).

Počítačovou kriminalitu již definovalo několik českých autorů, kteří se touto problematikou zabývali. Mezi prvními byli v roce 1997 autoři Porada Viktor a Konrád Zdeněk s tímto popisem *„počítačovou kriminalitu z kriminalistického hlediska rozumíme skupinu trestných činů páchaných prostředky výpočetní techniky v podmínkách komunikačních sítí, systémů, programového vybavení a databází výpočetní techniky.“*[33]

Z časovým odstupem několika let a také pokročilosti této kriminality je již definice v publikaci pod názvem Výkladový slovník kybernetické bezpečnosti od českých autorů Jirásek Petr, Novák Luděk, Požár Josef obsáhlejší a zní *„Trestná činnost v níž figuruje určitým způsobem počítač, jako souhrn technického a programového vybavení (včetně dat), nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět zájmu této trestné činnosti (s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité) nebo jako prostředí (objekt) nebo jako nástroj trestné činnosti (Více také Počítačová kriminalita).“*[34]

Počítačovou kriminalitu definoval ve své knize v roce 2007 i další odborník v této oblasti a to pan Václav Jírovský *„… kriminalitu, která může být namířena proti počítačům, jejich hardwaru, softwaru, datům, sítím apod.; nebo v ní vystupuje počítač pouze jako nástroj pro páchání trestného činu; případně počítačová síť a k ní připojená zařízení jsou prostředím, v němž se taková činnost odehrává.“*[35]

Úřední výklad pojmu počítačová kriminalita zveřejnilo i Ministerstvo vnitra ČR, které pojem definuje takto *„pod pojmem počítačová kriminalita je třeba chápat páchání trestné činnosti, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení*

[31] Datový modem –„*Zařízení pro převod digitální informace“*
Završil Aleš – Kyberkriminalita – Právní monografie, ČR 2017, ISBN 978-80-7552-758-2 –kapitola Základní pojmy str. 38

[32] ICT – „ *Je zkratka pro Informační a komunikační technologie. S větším nástupem komunikačních technologií ještě přidalo písmenko C (Communication) do původní zkratky IT aby byly zdůrazněny komunikačnítechnologie pro přenos informací, dat či hlasu.“* MANAGEMENT MANIA [online] [citace 20.2.2020]. Dostupné z: https://managementmania.com/cs/informacni-a-komunikacni-technologie

[33] Porada Viktor, Konrád Zdeněk - Metodika vyšetřování počítačové kriminality. 1. vydání. Praha 1997: Vydavatelství PA ČR, str. 7

[34] Jirásek Petr, Novák Luděk, Požár Josef - Výkladový slovník kybernetické bezpečnosti, Policejní akademie ČR 2015, ISBN 978-80-7251-397-0, str. 57

[35] Jírovský Václav - Kybernetická kriminalita, Praha 2007, ISBN 978-80-247-1561-2, str. 19

včetně dat, nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět této trestné činnosti, ovšem s výjimkou majetkové trestné činnosti, nebo jako nástroj trestné činnosti.“[36]

V mezinárodním měřítku definovala v roce 2000 Rada Evropy vymezení počítačové kriminality s tímto výkladem *„Trestný čin namířený proti integritě, dostupnosti nebo utajení počítačových systémů nebo trestný čin v tradičním smyslu, při kterém je užito moderních informačních a komunikačních technologií.“*[37] Dále v roce 2007 Rada upřesnila kategorie k této kriminalitě *„V praxi se pojem počítačová kriminalita vztahuje na tři kategorie trestné činnosti. Do první patří tradiční formy kriminality, jako například podvod či padělání, ačkoliv v souvislosti s počítačovou kriminalitou se toto týká konkrétně činů spáchaných prostřednictvím elektronických komunikačních sítí a informačních systémů (dále jen elektronické sítě). Do druhé kategorie patří zveřejňování nezákonného obsahu prostřednictvím elektronických médií (mj. materiály týkající se pohlavního zneužívání dětí či materiály podněcující k rasové nenávisti). Třetí kategorie zahrnuje trestné činy postihující výlučně elektronické sítě, tj. napadení informačních systémů, útoků typu „denial of service“ a hacking.“*[38]

Rada Evropy v této Úmluvě vedené pod číslem 185 z roku 2001 jasně formuluje základní pojmy kybernetické kriminality. Rada zde uvádí modelaci skutkových podstat kybernetických trestných činů. Jde o trestné činy, které spojuje stejné specifické prostředí. Od tohoto roku se i mezinárodně začala tato počítačová kriminalita označovat jako „*Cyber Crime*“ neboli „*Kybernetický Zločin*“ (viz kapitola 3.1.2). Práce se těmto právním úpravám a specifikacím bude věnovat v další navazující části.

3.1.3 Závěr

V samotném úvodu do problematiky bylo potřebné objasnit, jak vlastně Internet, jako globální síť vznikl (kapitola 3.1.1). Nikdo v počátcích nečekal, že z pouhého amerického univerzitního projektu financovaného samotnou vládou USA se zrodí ARPANET, ze kterého se časem

[36] Ministerstvo vnitra ČR - Analýza současného stavu a trendů vývoje trestné činnosti na úseku informačních technologií a Internetu včetně návrhu řešení, [online] [citace 20.2.2020]. Dostupné z: http://www.mvcr.cz/soubor/informacni-pdf.aspx.
[37] Matějka Michal, Počítačová kriminalita, Praha 2002, Computer Press, str. 5, původní pramen ÚMLUVA O POČÍTAČOVÉ KRIMINALITĚ Budapešť 23. listopadu 2001
[38] EUR-LEX 52007DC02-67 -KOMISE EVROPSKÝCH SPOLEČENSTVÍ - [online] [citace 20.2.2020]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52007DC0267&from=EN

vyvine něco tak převratného, jako Internet bezesporu je. Počátek je tedy v propojení tří univerzit USA v roce 1969, kde si v rámci této sítě studenti posílali jen vzájemné vzkazy. Ze tří univerzit bylo propojeno Arpanetem v roce 1972 celkem 23 univerzit a toto propojení se stalo globální sítí v polovině osmdesátých let pod názvem Internet. S pronikáním Internetu do celého světa se v rámci jeho fungování začala objevovat i kriminalita páchaná prostřednictvím této sítě sítí. Ze začátku šlo hlavně o ukázku moci prostřednictvím ochromení určité části sítě internetu. Ochromení těchto částí internetu využívaly někdy i vlády zemí navzájem a ochromení bylo vždy cílené bez zjevného finančního prospěchu pachatelů. Pak se pachatelé začali zaměřovat na využití Internetu z finanční stránky. Tak začala majetková kriminalita Internetu. Tento trend objednání zboží prostřednictvím Internetu a jeho zaplacením, ještě před doručením s úmyslem pachatele zboží nikdy nedodat dorazil ze zahraničí do České republiky až po roce 2005. Policie České republiky se musela tomuto trendu kriminality přizpůsobit a tak byla nucena změnit i interní systém, v rámci kterého trestnou činnost na území státu zaznamenává. Evidovat kybernetické trestné činy začala Policie České republiky s velkým zpožděním a to až od roku 2011. Celá společnost se vlastně učila poznávat svět internetu, ale také byla nucena pochopit základní pojmy, které jsou součástí sítě a bez těchto znalostí, se nemůžete v internetu vůbec orientovat.

3.2 Právní úprava v oblasti počítačové kriminality

3.2.1 Úvod

Se začátkem kyberkriminality byla celosvětově jakákoliv právní úprava o několik kroků pozadu. Tyto činy bylo možné pouze přiřadit již ke stávajícím právním postihům, které však nebyly schopny zcela zahrnout skutkovou podstatu těchto činů. Z toho důvodu byla potřebná kompletní legislativní změna na celosvětové úrovni, kde by tato část problematiky zločinu byla globálně chápána a postihována. Podstatou bylo se na tento druh kriminality podívat z úplně jiného úhlu a uvědomit si možné celosvětové důsledky a dopady. Od začátku páchání kyberkriminality jsme až do dnešní doby na úrovni vnitrostátní i mezinárodní úrovně, učinili velký pokrok (viz. následující části práce). Musíme si uvědomit, že technika jde stále dopředu a v tomto oboru to platí obzvlášť. S nárůstem obrany proti kyberkriminalitě, se bude současně navyšovat rafinovanost pachatelů. Dopadení a následné usvědčení v tomto směru kriminality bude těžší a těžší.

Jako důležitý základ pro možné zjištění, dokazování a následné trestní stíhání kybernetické trestné činnosti je mezinárodní spolupráce. Tato spolupráce však musí být opřena o pevný právní základ. Tento základ by měl být ve spolupracujících zemích v nejlepším případě jednotný, nebo alespoň podobný. Kyberkriminalita současného světa v rámci sítě Internet je ve své podstatě neomezená. Nikde není vytvořena žádná technická bariéra, která by znemožňovala spáchat kyberzločin odkudkoliv na světě.

3.2.2 Mezinárodní dokumenty k počítačové kriminalitě

Jako jeden z prvních dokumentů týkajících se mezinárodní úpravy kybernetických trestných činů lze považovat Manuál Organizace spojených národů z roku 1990 o prevenci a kontrole trestných činů spojených s počítači.[39] OSN se v tomto dokumentu zaměřuje na prioritní postavení této hrozby a nastínila globální nepřipravenost států na hrozby související s internetem. Z tohoto důvodu se následně celkem 53 členských zemí, které jsou součástí Rady Evropy[40], v roce 2000 sjednotilo a vydalo přelomový dokument pod názvem Úmluva Rady Evropy č. 185 o počítačové kriminalitě.[41] Tento dokument byl přijat dne 23. listopadu 2001. Česká republika ratifikovala Úmluvu č. 185 o počítačové kriminalitě v roce 2013. Úmluva je základem pro řešení vzájemné spolupráce v oblasti kyberkriminality mezi členskými státy, ale především má sloužit, jako návod pro vytvoření funkční legislativy členských států v této oblasti.

Dokument rozděluje trestné činy na dva Seznamy. Jeden seznam je označen jako Minimální a druhý jako Volitelný. Minimální seznam je tvořen tak, aby skutky v něm uvedené byly zapracovány do skutkových podstat trestných činů v právních řádech jednotlivých zemí. To je základem pro budoucí jednotnost v mezinárodním boji proti této trestné činnosti, jakou počítačová kriminalita jednoznačně je. Volitelný seznam je tvořen tak, aby zahrnoval specifická jednání, která by bylo možné označit za trestné činy, ale není to nezbytné.

---

[39] Manuál OSN pro prevenci a kontrolu počítačového zločinu. [online] OSN © 2001 [cit. 20.2.2020] Dostupné z: http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Guide.pdf

[40] Rada Evropy je mezinárodní celoevropská organizace, která zajišťuje spolupráci členských států zejména v oblasti podpory demokracie a ochrany lidských i sociálních práv a svobod. Datum založení Rady Evropy je 5. května 1949 podpisem zakládací listiny, tzv. Londýnské dohody. Sídlo má ve francouzském Štrasburku. Radu tvoří 47 členských států a několik zemí se speciálním statusem. Česká republika se k Radě Evropy připojila 30. června 1993. Misí a cílem Rady Evropy je vytvoření společného demokratického a právního prostoru, který zaručuje dodržování lidských práv, demokracii a respektování zákonů. [online] [cit.20.2.2020]. Dostupné z: http://www.radaevropy.cz

[41] Úmluva o počítačové kriminalitě, In: COE [právní informační systém]. Council of Europe Treaty office[online] [cit.20.2.2020]. Dostupné z: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

Minimální seznam zahrnuje tyto trestné činy

- neoprávněné kopírování autorsky chráněného programu
- poškozování počítačových dat a programů
- neoprávněné kopírování fotografie
- neoprávněný přístup
- neoprávněný průnik
- počítačové falzifikace
- počítačová sabotáž
- počítačové podvody

Volitelný seznam zahrnuje tyto trestné činy

- neoprávněné užívání autorsky chráněného programu
- změna v datech nebo počítačových programech
- neoprávněné užívání počítače
- počítačová špionáž [42]

Úmluva Rady Evropy č. 185 o počítačové kriminalitě je celkem rozdělena na čtyři oblasti trestné činnosti.

1. Trestné činy proti důvěřivosti, integritě a dostupnosti počítačových dat a systémů

- protiprávní přístup
- protiprávní zachycení informací (odposlech dat)
- narušování dat - narušování systémů - zneužívání zařízení

2. Trestné činy související s počítači - počítačové padělání

-počítačový podvod

3. Trestné činy související s obsahem počítače

- dětská pornografie

4. Trestné činy související s porušováním autorského práva a práv příbuzných autorskému právu [43]

[42] Látal I., Počítačová (informační) kriminalita a úloha policisty při jejím řešení -materiál z přílohy časopisu POLICISTA č. 3/1998, [online] Dostupné z: http://www.scritube.com/limba/ceha-slovaca/Potaov-informan-kriminalita-a-1513463.php

[43] Gřivna, T., Polčák, R., Kyberkriminalita a právo, první vydání, nakladatelství Auditorium, Praha 2008, Úmluva o počítačové kriminalitě - Budapešť 23. listopadu 2001 česká verze

V roce 2003 byla tato Úmluva ještě doplněna o Dodatkový protokol,[44] který rozšířil trestní postih i na činy rasově a xenofobně zaměřené, které budou spáchány prostřednictvím počítačových systémů. Prioritním důvodem vydání této Úmluvy byla možnost stíhání pachatelů těchto činů ve všech členských zemích. Nemělo se tedy stát, aby nějaký z činů nebyl v jiné členské zemi postižitelný. Součástí Úmluvy je i metodický postup vzájemné spolupráce států při vydávání pachatelů, zajišťování a získávání důkazních materiálů v rámci vyšetřování. Za podstatné lze považovat i skutečnost, že USA tuto Úmluvu podepsalo v roce 2011.[45] Do dnešního dne podepsalo a ratifikovalo Úmluvu celkem 62 zemí. Pro upřesnění je nutné doplnit, že Dodatkový protokol (viz. výše v této kapitole 3.2.2), který vstoupil v platnost dne 1. března 2005 neobsahuje a není v něm nijak upravena procesní stránka, tak jak je uváděna v Úmluvě číslo 185. Rada Evropy postupně vydává i druhý Dodatkový protokol vedený pod číslem 189.[46] V současné době probíhá proces schvalování tohoto druhého Dodatkového protokolu k Úmluvě Rady Evropy o kyberkriminalitě (CETS č. 185). Ten byl předložen Evropské komisi na jednání v Bruselu dne 5. února 2019. Vládě ČR ji Evropská komise po jejím jednání doručila pod názvem - ROZHODNUTÍ RADY o zmocnění k účasti na jednání o druhém dodatkovém protokolu k Úmluvě Rady Evropy o kyberkriminalitě (CETS č. 185).[47]

Pro ucelenost, je důležité uvést další důležité Úmluvy a nařízení, která se týkají této problematiky, jako je Radou Evropy dne 25. října 2007 vydaná Úmluva o ochraně dětí před sexuálním vykořisťováním a zneužíváním.[48] V článku 20 této Úmluvy pod názvem Trestné činy tykající se dětské pornografie je v prvním odstavci uvedeno: „*Každá strana přijme legislativní, nebo jiná nezbytná opatření s cílem učinit trestnými následující úmyslná jednání,*

[44] Dodatkový protokol k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů [online] [cit.20.2.2020]. Dostupné z: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804931

[45] Polčák, Radim. Internet a proměny práva. Praha: Auditorium, 2012, Téma (Auditorium). ISBN 978-80-87284-22-3, str. 388

[46] Dodatkový protokol k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů. In: COE [právní informační systém]. Council of Europe Treaty office [online] [cit. 20.02.2020]. Dostupné z: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008160f

[47] Evropská komise 2019[online] [cit. 20.02.2020] Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52019PC0071&from=NL

[48] Úmluva Rady Evropy 2007 , [online] 2019 Úmluva Rady Evropy o ochraně dětí proti sexuálnímu vykořisťování a pohlavnímu zneužívání, [online] Dostupné z: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168046e1

pokud jsou činěna v rozporu s právem“.[49] Pod písmenem f je dále uvedeno: *„vědomé získávání přístupu k dětské pornografii prostřednictvím komunikačních a informačních technologií*“. Bod 4 tohoto článku uvádí: „*Každá strana si může vyhradit právo neuplatnit plně nebo z části ustanovení odstavce 1 písmene f*“[50].

V tomto ustanovení je patrná jistá nerozhodnost v nařízení Rady Evropy. Jasná jednotnost postihu jednání budoucích pachatelů této trestné činnosti by měla být v každé zemi stejná. Je zjevně chybné dávat možnost každému jednotlivému státu nezanést postižitelnost tohoto jednání. Úmluva by měla stanovit jasná a stejná pravidla pro všechny a vůbec by neměla nastat situace, kdy v jedné zemi by byl tento postih možný a v další zemi nikoliv. Vždyť už jen formulace slov – „*pachatel vědomě získá“* - je jasné naplnění skutkové podstaty trestného činu. Není možné jasně vymezit jakým prostřednictvím a z čeho pachatel dětskou pornografii získá a pak dát prostor k možnosti neuplatnit, nebo si vyhradit právo tuto formulaci nemít v zemi legislativně zakotvenou. V rámci mezinárodní spolupráce při odhalování a dokazování této trestné činnosti pak bude postižitelnost velice složitá a pachatelé by se hypoteticky mohli přemístit do země, kde nebude tento postih upraven legislativou.

3.2.3 Dokumenty a přístupy EU k počítačové kriminalitě

V rámci Evropské unie byla postupně vydána také důležitá rozhodnutí, jako byla například dne 31. března 1992 Rozhodnutí rady Evropské unie 92/242/EHS[51] o bezpečnosti informačních systémů, dne 29. května 2000 Rámcové rozhodnutí Rady o boji proti dětské pornografii na internetu 2000/375/JHA[52], dne 22. prosince 2003 Rámcové rozhodnutí Rady Evropské unie 2004/68/SVV[53] o boji proti pohlavnímu vykořisťování dětí a dětské pornografii. Dne 24. května 2005 bylo vydáno Rámcové rozhodnutí Rady 2005/222/SVV[54] o útocích proti informačním systémům. Rámcové rozhodnutí Rady Evropské unie

[49] Úmluva Rady Evropy 2007, článek 20 -Trestné činy tykající se dětské pornografie str. 8 [online]. 2019 Dostupné z: www.psp.cz › sqw › text › orig2

[50] Úmluva Rady Evropy 2007, článek 20 bod 4 -Trestné činy tykající se dětské pornografie str. 8 [online]. 2019 Dostupné z: www.psp.cz › sqw › text ›orig2

[51] EUR LEX - Rada Evropské unie, [online] Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:31992D0242

[52] EUR LEX - Rada Evropské unie, [online] Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32014D0836

[53] EUR LEX - Rada Evropské unie, [online] Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A32004F0068

[54] EUR LEX - Rada Evropské unie, [online] Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A32005F0222

2005/222/SVV bylo dne 12. srpna 2013 nahrazeno Směrnicí Evropského parlamentu a Rady 2013/40/EU [55] o útocích na informační systém.

3.2.4 Právní úprava počítačové kriminality v ČR

Český právní řád se v době začátku kyberkriminality v ČR opíral pouze o trestní zákoník č. 140/1961 Sb. Ten by účinný do 31. 12. 2009. Ještě před tím, než bude proveden postupný historický rozbor vývoje Trestního zákoníku, budou uvedeny typové znaky trestného činu, ale také bude především uvedena samotná definice trestného činu.

Trestný čin podle § 13 odst. 1 zákona č. 40 /2009 Sb.“ - (*1) Trestným činem je protiprávní čin, který trestní zákon označuje za trestný a který vykazuje znaky uvedené v takovém zákoně.*

-(2) K trestní odpovědnosti za trestný čin je třeba úmyslného zavinění, nestanoví-li trestní zákon výslovně, že postačí zavinění z nedbalosti.*“*[56]

Typové znaky trestného činu - *„Souhrn typových znaků trestného činu určitého druhu, typických pro nebezpečnost činu tohoto druhu pro společnost, se v nauce označuje jako skutková podstata trestného činu. Pojem skutkové podstaty trestného činu lze tedy definovat jako souhrn typových znaků, kterými se od sebe odlišují různé typy trestných činů. Někdy bývá skutková podstata definována jako souhrn objektivních a subjektivních znaků, které určují jednotlivé druhy trestných činů a odlišují je navzájem.“*[57]

Skutková podstata trestného činu zahrnuje typové znaky.

Objekt – „*Objektem trestného činu jsou zájmy společnosti, které mají být chráněny a proti kterým trestný čin směřuje. Znaky objektu nejsou zpravidla ve skutkové podstatě vyjádřeny, ale dají se z ní vždy i odvodit.*“[58]

Objektivní stránka – „*Znaky objektivní stránky trestného činu jsou jednání, následek a příčinný vztah mezi nimi. Dalšími znaky jsou například místo a čas spáchání trestného činu., subjekt, subjektivní stránka.“*[59]

[55] EUR LEX - Rada Evropské unie, [online] Dostupné z https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A32013L0040
[56] § 13 trestního zákoníku (zákon č.40/2009 Sb.)
[57] Novotný Oto, Dolenský Adolf, Jelínek Jiří aj. -Trestní právo hmotné, obecná část, 4. přepracované vydání, Praha, ASPI Publishing, s.r.o., 2003, str. 9
[58] § 3 trestního zákoníku (zákon č.40/2009 Sb.)
[59] § 3 trestního zákoníku (zákon č.40/2009 Sb.)

Subjekt – „*Subjektem trestného činu je jeho pachatel, proto znaky charakterizují pachatele. Jde především o věk a příčetnost (ten, kdo v době spáchání trestného činu nedovršil patnáctý rok svého věku není trestně odpovědný, dále ten kdo pro duševní poruchu v době spáchání činu nemohl rozpoznat jeho nebezpečnost pro společnost nebo ovládat své jednání, není za tento čin trestně odpovědný), případně jde o jinou způsobilost nebo postavení pachatele trestného činu*."[60]

Subjektivní stránka – „*Subjektivní stránkou trestného činu je zavinění, které může být buď nedbalostní nebo úmyslné, přičemž je stanoveno, že k trestnosti činu je třeba úmyslného zavinění, pokud trestní zákon nestanoví výslovně, že postačí i zavinění z nedbalosti. Dalšími znaky subjektivní stránky jsou například motiv a záměr pachatele*."[61]

Historicky až v roce 1991 nově formuloval trestní zákoník č. 140/1961 Sb.,[62] skutkovou podstatu nového trestného činu, jakým bylo podle §257a[63] poškození a zneužití záznamu na nosiči informací. Do tehdy platného trestního zákoníku č. 140/1961 Sb., byl vložen novelou č. 557/1991 Sb.,[64] která nabyla účinnosti dnem 1. ledna 1992. Objektem tohoto trestného činu byla ochrana dat uložených na nosiči informací proti neoprávněným změnám a proti jejich neoprávněnému použití. Předmětem ochrany byl nosič informací, jeho obsah a technické a programové vybavení počítače.[65] Další novela tohoto zákoníku byla vydána v roce 2002 jako zákon č. 134/2002 Sb.[66]. Tato novela z roku 2002 byla vydána především z důvodu upřesnění jednání pachatele - skutkové podstaty způsobit škodu, nebo získání prospěchu v době, kdy

[60] § 3 trestního zákoníku (zákon č.40/2009 Sb.)
[61] § 3 trestního zákoníku (zákon č.40/2009 Sb.)
[62] Zákon č.140/1961 Sb.
[63] Zákon č. 140/1961 Sb., trestní zákon, účinnost ke dni 31.12.2009:
„ § *257a Poškození a zneužití záznamu na nosiči informací*
(1) Kdo získá přístup k nosiči informací a v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch
a) takových informací neoprávněně užije,
b) informace zničí, poškodí, změní nebo učiní neupotřebitelnými, nebo
c) učiní zásah do technického nebo programového vybavení počítače nebo jiného telekomunikačního zařízení, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti nebo peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty.
(2) Odnětím svobody na šest měsíců až tři léta bude pachatel potrestán,
a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny, nebo
b) způsobí-li takovým činem značnou škodu nebo získá-li sobě nebo jinému značný prospěch.
(3) Odnětím svobody na jeden rok až pět let bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu nebo získá-li sobě nebo jinému prospěch velkého rozsahu. „
[64] Novela TZ č. 557/1991 Sb. znění účinné od 1. 1. 1992 do 31. 12. 2009
[65] Šámal Pavel a Stanislav Rizman. Trestní zákon: Komentář. 1. vyd. Praha: SEVT, 1994, XI, 1036 s. Komentované zákony (SEVT). ISBN 80-704-9097-7
[66] Novela TZ č. 134/2002 Sb. znění účinné od 1. 7. 2002 do 31. 12. 2009

měl k počítači přístup. V praxi to znamenalo, že bylo možné postihnout jednání pachatele, který se k informacím z počítačového média dostal naprosto legálně, například, jako zaměstnanec firmy. Tyto informace, nebo údaje pak následně zneužil, upravil, smazal, nebo prodal. Skutková podstata tak byla jasně stanovena a nebylo již nutné dokazovat úmysl pachateli, který informace z počítačového média zneužil a to i v případech, když je získal již před několika lety. K paragrafu 257a bylo možné přiřadit i jednočinný souběh s dalšími trestnými činy.

Jednalo se například o souběh s paragrafy

- § 106 a § 107 tr. zák. - ohrožení utajované informace
- § 128 tr. zák. odst. 1 nebo 2 - zneužití informací v obchodním styku
- § 149 tr. zák. - nekalé soutěže
- § 152 tr. zák. - porušování autorských práv
- § 239 a § 240 tr. zák. - porušování tajemství dopravovaných zpráv

Dalším kybernetickým trestným činem vloženým do trestního zákoníku č.140/1961 Sb., byl trestný čin porušování autorského práva podle § 152. Tento paragraf došel několika změn, až do právní podoby ve formě trestního zákoníku č. 40/2009 Sb.,[67] s účinností od 1. 1. 2010. Právě § 257a trestního zákoníku nahrazují v trestním zákoníku č. 40/2009 Sb., tyto paragrafy

- § 230 Neoprávněný přístup k počítačovému systému a nosiči informací
- § 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat
- § 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

Jen pro upřesnění, trestní zákoník č. 40/2009 Sb., byl novelizován zákonem č. 306/2009 Sb.[68]. Trestní zákoník byl v ustanoveních týkajících se kybernetických trestných činů podle § 192 a § 311 dále novelizován trestním zákonem č. 330/2011 Sb.[69]. Tento zákon vstoupil v účinnost dnem 1. prosince 2011. Nutno doplnit, že Česká republika Úmluvu Rady Evropy

[67] Zákon č. 40/2009 Sb. ze dne 8. ledna 2009
[68] Novela TZ zákonem č. 306/2009 Sb. ze dne 7. srpna 2009
[69] Novela TZ zákonem č. 330/2011 Sb. ze dne 7. října 2011

č. 185 o počítačové kriminalitě dne 1. prosince 2013 ratifikovala. Poté následovala v České republice novela trestního zákoníku zákonem č. 141/2014 Sb.[70]. Touto novelou byly postupně splněny články Úmluvy, které český trestní zákoník dodatečně doplňoval o nové paragrafy související s touto trestnou činností. Trestní zákoník byl novelizován v roce 2018 zákonem č. 287/2018 Sb.[71]. Tato novelizace nabyla účinnosti od 1. února roku 2019. Naposledy byl trestní zákoník novelizován zákonem č. 315/2019 Sb.,[72] kdy jeho znění je účinné od 1. prosince roku 2019.

Na jednu stranu je znatelný jasný posun a snaha postupně upravovat a vkládat znění jednotlivých paragrafů, ale konkrétně u paragrafů 230 a 231 trestního zákoníku se musím ztotožnit s kritickým hodnocením týkajících se právě paragrafového znění. Zastávám shodný názor jako Jelínek[73], protože v paragrafech je úprava této problematiky vyjádřena moc kauzuisticky a vůbec nebere v úvahu obecné vyjadřování v ostatních hlavách trestního zákoníku.

Rovněž se shoduji se Smejkalem, který například u těchto paragrafů kritizuje formulaci pojmů *„…"jakýkoliv jiný prostředek" a „jakýkoliv jiný obdobný prostředek" v paragrafu 231, které smazává rozdíl mezi nástroji uvedenými v odstavci 1, písmeni a) a přístupovými údaji uvedenými pod písmenem b) tohoto odstavce*."[74]

[70] Novela TZ zákonem č. 141/2014 Sb. ze dne 19. června 2014
[71] Novela TZ zákonem č. 287/2018 Sb. ze dne 15. listopadu 2018
[72] Novela TZ zákonem č. 315/2019 Sb. ze dne 30. října 2019
[73] Jelínek, Jiří a kol., Trestní právo hmotné, 2016, ISBN 978-80-7502-120-5, str. 685
[74] Smejkal, Vladimír- Kybernetická kriminalita., Plzeň 2015- ISBN 978-80-7380-501-2, str. 413

Tabulka č.1 Změny trestního zákonodárství v reakci na postupný vývoj kyberkriminality v časovém období let (1991-2019)

Rok	Účinnost od data	Zákon	Nový § / změna § N / Z
Zákon č. 140 /1961 Sb.			
1991	1. ledna 1992	č. 557/1991 Sb.	**N** §257a , §152
2002	1. července 2002	č. 134/2002 Sb.	**Z** upřesnění skutkových podstat
2007	1. prosince 2007	271/2007 Sb.	**N** §205b
Zákon č. 40 / 2009 Sb.			
2009	8. ledna 2009	č. 40/2009 Sb.	**N**§182,§187,§183,§191,§192,§193,§230 ,§231,§232,§353,§354,§355,§357,§311 **Z** §205
2009	1. ledna 2010	č. 306/2009 Sb.	**Z** §354
2011	1. prosince 2011	č. 330/2011 Sb.	**Z** §192, §311
2014	1. srpna 2014	č. 141/2014 Sb.	**N** §193a, 193b
2018	1. února 2019	č. 287/2018 Sb.	**Z** §193a, §193b
Zákon č. 315 / 2019 Sb.			

Zdroj: vlastní zpracování

§ 152 Porušování autorských práv
§ 182 Porušení tajemství dopravovaných zpráv
§ 183 Porušení tajemství listin a jiných dokumentů
§ 187 Pohlavní zneužití
§ 191 Šíření pornografie
§ 192 Výroba a jiné nakládání s dětskou pornografií
§ 193 Zneužití dítěte k výrobě pornografie
§ 193a Účast na pornografickém představení
§ 193b Navazování nedovolených kontaktů s dítětem
§ 205 Nový název od 2007 z Ohrožování mravnosti na Šíření pornografie
§ 205b Zneužití dítěte k výrobě pornografie
§ 257a Poškození a zneužití záznamu na nosiči informací
§ 311 Teroristický útok

§ 353 Nebezpečné vyhrožování

§ 354 Změna názvu z Nebezpečné pronásledování na Stalking

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

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

§ 357 Šíření poplašné zprávy

Z tabulky jasně vyplývá, že největší změny v legislativě se odehrály v roce 2009, kdy vstoupil v platnost zákon č. 40/2009 Sb. Tento zákon již obsahoval znění několika nových paragrafů, podle kterých bylo možné stíhání pachatelů nových forem kyberkriminality. V období od roku 1991 do současnosti prošlo trestní zákonodárství v ČR celkovým počtem 98 změn. Například živnostenský zákon v současném znění č. 455/1991 Sb. prošel v období od roku 1991 sto šedesáti čtyřmi změnami. Otázkou je, zda máme v této oblasti trestního práva málo kvalifikovaných odborníků potřebných k novelizacím trestního zákoníku, nebo je to signál menšího politického zájmu. Jak se kyberkriminalita vyvíjela, s tím, že jedna forma této kriminality navazovala na druhou, nebo s ní úzce souvisela, tak již v současné době obsahuje český trestní zákoník podrobnější formulace o postihu kyberzločinu. Přesto i po uzákonění některých skutkových podstat je rozmezí výše trestu za tyto činy, dle mého názoru, velice nízké. Celkově by se výše trestů měla navýšit a to především v případech, kdy je ohrožen a narušen další psychický vývoj dětí, nebo mladistvých.

Dle mého názoru by se mělo jednat minimálně o dvojnásobné navýšení trestů. To by znamenalo až desetileté vězení pro pachatele, který by zneužil, nebo zlákal dítě k pornografickým aktivitám, za předpokladu, vzniku pornografického díla z těchto aktivit. Trest za nabízení a výrobu pornografie s dětskou tématikou by byl stanoven na horní hranici šesti let a za přechovávání dětské pornografie by pachateli hrozil trest v odnětí svobody čtyři roky. Možnost udělování podmíněných trestů při páchání této trestné činnosti by zákon striktně vůbec neumožňoval.

3.2.5 Dělení druhů kyberkriminality podle Policie České republiky

Policie České republiky definuje jednotlivé druhy kyberkriminality v současné době takto.

Podvodná jednání- „*Nejčastějším dokladovaným jednáním je přečin Podvod dle ust. § 209 trestního zákoníku, kdy není neobvyklý ani souběh s Neoprávněným přístupem k počítačovému systému a nosiči informací dle ust. § 230 trestního zákoníku. Mezi tyto skutky lze zařadit*

podvodné e-shopy, které vznikají pod záminkou vylákání finančních prostředků a po krátké existenci takový e-shop zaniká. Současně jsou finanční prostředky zpravidla vyvedeny mimo území našeho státu za účelem anonymizace finančních toků, případně jsou využívány virtuální měny. Obdobný je postup v rámci podvodných inzerátů (prodej automobilů, elektroniky, živých zvířat nebo třeba i pronájmy bytů), sbírek a v neposlední řadě také jednání známé jako tzv. nigerijské podvody. Do daného jednání lze zahrnovat také podvody prostřednictvím podvržených emailů nebo krádeže peněz z bankovních účtů za pomoci phishingu.“[75]

Hacking[76] – jde vlastně o překonání zabezpečení systému a získání neoprávněných informací. Pachatel pak svojí oběť vydírá, nebo citlivé informace rovnou zneužije (přístup k bankovním účtům, účtům na sociálních sítích atd.). V trestním zákoníku vedeno pod paragrafy § 230 Neoprávněný přístup k počítačovému systému a nosiči informací, nebo § 182 Porušení tajemství dopravovaných zpráv.

Blagging[77] – jde o kontaktování osob, nebo společností prostřednictvím internetu, kdy se pachatel vydává za někoho, koho by kontaktovaný měl znát a důvěřovat mu. Následně pak je touto formou požadována například úhrada nějaké faktury, nebo uzavření smlouvy, ze které pak pachatel profituje.

Podvodné e-shopy[78] - jde o internetové nabízení zboží, které pachatel nikdy fyzicky nevlastnil, pouze prostřednictvím internetu toto zboží zainzeroval a prodal. Drtivá většina těchto pachatelů vyžaduje za zboží platbu předem, kdy platba na účet je uskutečněna převodem do jiného státu, kde je účet pachatele u nějaké banky registrován. V souvislosti s těmito podvody se v poslední době začal objevovat trend pachatelů, kteří využijí účty jiných osob. Následně na tyto účty je za zboží převedena platba a majitelé legálních účtů předávají určitou finanční částku pachatelům. Tím se ale dopouštějí spáchání buď trestného činu dle § 216 – Legalizace výnosů z trestné činnosti, nedbalostního trestného činu dle § 217 Legalizace výnosů z trestné činnosti. Dříve vedeno pod označením názvu jako Podílnictví.

[75] Policie České republiky – Jednotlivé druhy kyberkriminality- [online] [citace 24.2.2020] Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx
[76] Policie České republiky – Jednotlivé druhy kyberkriminality- Hacking [online] [zdroj článek 2019] Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx
[77] Policie České republiky – Jednotlivé druhy kyberkriminality- Blagging [online] [zdroj článek 2019] Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx
[78] Policie České republiky – Jednotlivé druhy kyberkriminality- Podvodná inzerce a e-shopy [online] [zdroj článek 2019] Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx

Násilné projevy a hate crime – „*Do této kategorie spadají trestné činy jako např. Vydírání dle ust. § 175 trestního zákoníku, Nebezpečné vyhrožování dle ust. § 353 trestního zákoníku, Nebezpečné pronásledování (známé také pod pojmem stalking) dle ust. § 354 trestního zákoníku nebo také Šíření poplašné zprávy dle ust. § 357 trestního zákoníku, kdy všechny tyto skutky při využití informačních technologií nabývají vyšší míry anonymity. Za tímto účelem jsou využívány anonymizační servery nebo služby, např. proxy servery, tor síť, VPN atp. Sem patří i extremistické projevy mající povahu trestného činu Hanobení národa, rasy, etnické nebo jiné skupiny osob dle ust. § 355 trestního zákoníku, Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod dle ust. § 356 trestního zákoníku a další. Na zahraničních serverech jsou vytvářeny webové stránky s extrémně pravicovou či levicovou tématikou, které podněcují k nenávisti, diskriminaci nebo i vyzývají k násilí vůči menšinovým skupinám obyvatel či politickým uskupením. Dalším projevem jsou pak i smyšlené profily na sociálních sítích a diskuse k různým článkům v médiích.*“[79]

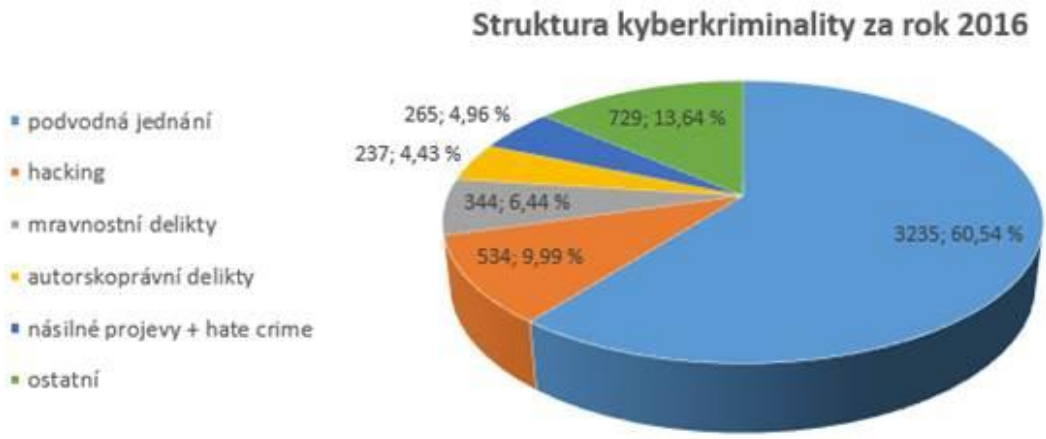
Trestné činy proti autorskému právu – „*Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle ust. § 270 trestního zákoníku spočívá zejména ve sdílení hudebních skladeb, filmů a softwaru v rozporu s autorským právem šířeným v rámci webových velkokapacitních úložišť nebo P2P sítí.*“[80]

Mravnostní trestné činy – „*Ohrožování výchovy dítěte dle ust. § 201 trestního zákoníku, Šíření pornografie dle ust. § 191 trestního zákoníku, Výroba a jiné nakládání s dětskou pornografií dle ust. § 192 trestního zákoníku, Zneužití dítěte k výrobě pornografie dle ust. § 193 trestního zákoníku, Účast na pornografickém představení dle ust. § 193a trestního zákoníku a v neposlední řadě Navazování nedovolených kontaktů s dítětem dle ust. § 193b trestního zákoníku.*“[81]

[79] Policie České republiky – Jednotlivé druhy kyberkriminality- [online] [citace 24.2.2020] Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx
[80] Policie České republiky – Jednotlivé druhy kyberkriminality- [online] [citace 24.2.2020] Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx
[81] Policie České republiky – Jednotlivé druhy kyberkriminality- [online] [citace 24.2.2020] Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx

Podle tohoto členění zveřejnila policie v roce 2017 strukturu kyberkriminality za rok 2016.

Obrázek č. 1 Struktura kyberkriminality za rok 2016



Zdroj: Policie České republiky

Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx

Některé trestné činy, které zahrnují kybernetické komerční trestné činy páchané proti dětem, budou blíže rozebrány v kapitole 3.3 této práce.

3.2.6 Závěr

Hrozba kyberkriminality začala být vnímána celosvětově již v devadesátých letech. Jako jeden z prvních dokumentů, který se kyberkriminalitou začal zabývat a rozpracovával jí, byl v roce 1990 vydaný Manuál Organizace spojených národů o prevenci a kontrole trestných činů spojených s počítači (viz. kapitola 3.1.2). Manuál poukázal na globální nepřipravenost států související s používáním sítě Internet. Na tuto začínající hrozbu zareagovala Rada Evropy, která v roce 2000 vydala přelomový dokument pod názvem Úmluva Rady Evropy č. 185 o počítačové kriminalitě (viz. kapitola 3.2.2). Úmluvu postupně doplnily dva Dodatkové protokoly. První byl vydán v roce 2003 (viz. kapitola 3.2.2) a schvalování Druhého dodatkového protokolu probíhá v současnosti. V roce 2007 vydává Rada Evropy dokument pod názvem Úmluva o ochraně dětí před sexuálním vykořisťováním a zneužíváním (viz. kapitola 3.2.2). Současně s Radou Evropy vydávala i svá rozhodnutí k problematice kyberkriminality také Evropská unie. V roce 1992 se jednalo o Rozhodnutí rady Evropské unie vedené pod č. 92/242/EHS o bezpečnosti informačních systémů (viz. kapitola 3.2.3). Následovalo Rámcové rozhodnutí Rady Evropské unie o boji proti dětské pornografii na

internetu z roku 2000 vedené pod č. 2000/375/JHA (viz. kapitola 3.2.3). V roce 2003 bylo vydáno Rámcové rozhodnutí Rady Evropské unie 2004/68/SVV o boji proti pohlavnímu vykořisťování dětí a dětské pornografii (viz. kapitola 3.2.3). Na toto rozhodnutí navazovalo v roce 2005 Rámcové rozhodnutí Rady Evropské unie vedené pod č. 2005/222/SVV o útocích proti informačním systémům (viz. kapitola 3.2.3). To bylo doplněno v roce 2013 Směrnicí Evropského parlamentu a Rady 2013/40/EU o útocích na informační systém (viz. kapitola 3.2.3).

V České republice se právní úprava v návaznosti na kybernetické trestné činy opírala o zákon č. 140/1961 Sb. Zákon byl od roku 1991 postupně novelizován a byly do něj vkládány další paragrafy umožňující postihovat tuto trestnou činnost. Největší změna a také největší počet nových paragrafů k této problematice nastal v roce 2009 s účinností zákona č. 40/2009 (nový trestní zákoník), který trestní zákoník č. 140/1961 Sb., zrušil. Zákon č. 40 / 2009 Sb. byl také postupem let několikrát novelizován. Poslední změnou je Zákon č. 315/2019 Sb., s účinností od 1. prosince 2019. Viz tabulka č. 1 (kapitola 3.2.4).

Tak, jak se celosvětově kyberzločin vyvíjel, byly i zákony v jiných zemích postupně měněny, nebo novelizovány a byly do nich zaneseny skutkové podstaty trestných činů kybernetické trestné činnosti v návaznosti na jejich vývoj. V tomto smyslu je ale z mého pohledu spatřováno největší pochybení mezinárodních orgánů, jakým Rada Evropy je, kdy dává možnost každému jednotlivému státu nemít legislativně zakotvenou stejnou postižitelnost protiprávního jednání, které se ke kyberkriminalitě váže (viz. kapitola 3.2.2). Paradoxně na začátku Rada ukládá zemím, aby přijmuly legislativní, nebo jiná nezbytná opatření s cílem učinit trestnými úmyslná jednání, pokud jsou činěna v rozporu s právem. Pak není nutné ani vydávání metodiky pro mezinárodní spolupráci v boji s kyberkriminalitou, když každá země si může udělat úpravu dle svého uvážení. V jednotě je síla a pokud budou existovat země s menšími právními postihy kyberkriminality, bude kyberzločinu tímto způsobem vytvořeno útočiště.

3.3 Kybernetické komerční trestné činy páchané proti dětem

3.3.1 Vymezení kybernetických komerčních trestných činů páchaných proti dětem

Než vůbec vstoupíme do této problematiky, je nutné si uvědomit, jak je vlastně definována osoba dítěte v trestním zákoníku České republiky. Trestní zákoník č. 40/2009 Sb., zde

vymezuje pojem dítě pod ustanovením § 126 a to jako *„osobu mladší osmnácti let, pokud trestní zákon nestanoví jinak.“*[82]

To je upřesněno v § 187, kdy pro účely trestného činu pohlavního zneužití je objektem dítě mladší patnácti let. Trestní zákoník hovoří o dítěti, bez stanovení jeho pohlaví. Za zmínku stojí i to, že v § 192 odst. 1 je rozšířen jako objekt skutkové podstaty trestného činu také na *„osobu, jež se jeví být dítětem.“*[83] V tomto případě je brána v potaz i stránka dokazování, kdy není možné pachateli prokázat skutečný věk dítěte z dětské pornografie na zajištěných materiálech.

V dnešní době je velice těžké odhadnout věkový stav osoby – dítěte. Ještě složitější je, dle mého názoru, znění dikce TZ *„osobu, jež se jeví být dítětem.“* Tato formulace je těžko uchopitelná a jen závislá na subjektivním pohledu každého z nás.

„…osobě, jež se jeví být dítětem“– tu lze opět rozlišovat situace podle toho, o jaký typ pornografie se jedná. V případě fotografického či filmového zachycení skutečných osob fakticky starších 18 let v nauce převládá názor. Že by tyto osoby měly vykazovat jednoznačnou podobnost s dítětem—tzn., že vzhled dané osoby (posuzován v kontextu celého díla) by většinu pozorovatelů skutečně zmátl, tak že by tuto osobu omylem považovali za dítě.“[84]

V tomto se jednoznačně shoduji s vyjádřením Jelínka, který chybnost formulace vyjádřil absolutně správně i s uvedením příkladu tvrzení.

„Považuji v těchto případech předstíraného dětského objektu za problematické, má-li se podobností s dítětem rozumět každé věrohodné předstírání, že osoba je mladší 18let (např. nepravdivé tvrzení ženy starší 18let, že je jí teprve 17let.“[85]

Z dalších důležitých aspektů je nutné ozřejmit, zda a jak je v trestním zákoníku uveden samotný pojem Pornografie a Dětská pornografie. Náš trestní zákoník jako takovou Pornografii vůbec nedefinuje. Není brán zřetel ani na skutečnou a virtuální pornografii. Z toho důvodu je přistupováno k odborné literatuře a různým judikátům. V Právnickém slovníku ČR je pornografie popsána takto: *„Pornografie může mít podobu díla písemného, fotografického, filmového, počítačového, elektronického nebo jiného (např. plastický model, soška).*

[82] § 126 trestního zákoníku (zákon č. 40/2009 Sb.) znění účinné od 1. 12. 2019
[83] § 192 trestního zákoníku (zákon č. 40/2009 Sb.) znění účinné od 1. 12. 2019
[84] Jelínek Jiří a kol., Trestní právo hmotné, 2016, ISBN 978-80-7502-120-5, str. 620
[85] Jelínek Jiří, Praha 2016, Vyjádření k žádosti Národního ústavu duševního zdraví - posouzení problematiky výroby stimulů pro základní výzkum pedofilních preferencí [online] [citace 24.2.2020] Dostupné z:https://www.sexuologickaspolecnost.cz/dokumenty/jelinek_vyjadreni_NUDZ2016.pdf

Pornografii lze charakterizovat tím, že vtíravým způsobem podněcuje sexuální pud, překračuje podle převládajících názorů ve společnosti uznávané hranice sexuální slušnosti, uráží neakceptovatelným způsobem cit pro sexuální slušnost. Test pornografické povahy díla spočívá tedy na posouzení, jednak zdali celkový dojem díla způsobuje morální pohoršení osobě s běžným cítěním, jednak zdali podněcuje sexuální pud. Samo zobrazení nahého lidského těla v přiměřené situaci (při koupání, pro účely reklamy) není pornografickým dílem, i když by mohlo vzbuzovat sexuální vzrušení. "[86]

Náš nejvyšší soud se touto otázkou také zabýval a dospěl k výroku, že *„Co lze považovat za pornografické dílo, není zákonem vymezeno. Právní teorie, jakož i judikatura soudů za takové pokládá dílo, které zvláště intenzivním a vtíravým způsobem zasahuje a podněcuje sexuální pud, překračuje podle převládajících názorů ve společnosti uznávané hranice sexuální slušnosti, uráží neakceptovatelným způsobem cit pro sexuální slušnost, vyvolává pocit studu.* "[87]

Otázkou stanovení pojmu pornografické dílo se zabýval Nejvyšší soud v roce 2005 *„za pornografické dílo lze pokládat snímky obnažených dětí, zachycující polohy skutečného či předstíraného sexuálního styku a jiné sexuálně dráždivé snímky*. "[88]

Je složité rozlišovat pornografická díla. Někdo může namítat, že je možné sexuální vzrušení třeba i z historických sošek, jako je například Věstonická Venuše, nebo některá malířská díla zobrazující nahé ženské tělo. O tomto se zmiňuje a problematiku upravuje Důvodová zpráva[89] k návrhu trestního zákoníku č. 40/2009 Sb., tak, aby tato umělecká díla byla vyňata.

V souhrnu lze vyjádřit, že problematika komerčních trestných činů se týká paragrafů trestního zákoníku, kterými jsou § 187 Pohlavní zneužití, § 191 Šíření pornografie, § 192 Výroba a jiné nakládání s dětskou pornografií, § 193 Zneužití dítěte k výrobě pornografie, § 193a Účast na pornografickém představení, § 193b Navazování nedovolených kontaktů s dítětem, § 201 Ohrožování výchovy dítěte.

[86] Hendrych a kolektiv, Praha 209, C.H. BECK, ISBN 978-80-7400-059-1 str. 481
[87] usnesení Nejvyššího soudu ČR, sp. zn. 8 T do 1002/2012
[88] Nejvyšší soud ČR, 2005 Rozsudek - R 35/2005
[89] Důvodná zpráva k zákoníku č. 40/2009 Sb. [online] [zdroj 24.2.2020] Dostupné z: https://www.vlada.cz/assets/ppov/lrv/ria/databaze/Revize-Zaverecne-zpravy-RIA-k-navrhu-zakona--kterym-se-meni-zakon-o-trestnim-rizeni-soudnim-_trestni-rad_.pdf

Pohlavní zneužití § 187 trestního zákoníku – Právě skutková podstat tohoto trestného činu spočívá v jakékoliv narušení dětské pohlavní sféry, kdy se jedná o dítě mladší 15 let.

„(1) Kdo vykoná soulož s dítětem mladším patnácti let nebo kdo je jiným způsobem pohlavně zneužije, bude potrestán odnětím svobody na jeden rok až osm let.

(2) Odnětím svobody na dvě léta až deset let bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 na dítěti mladším patnácti let svěřeném jeho dozoru, zneužívaje jeho závislosti nebo svého postavení a z něho vyplývající důvěryhodnosti nebo vlivu.

(3) Odnětím svobody na pět až dvanáct let bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 těžkou újmu na zdraví.

(4) Odnětím svobody na deset až osmnáct let bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 smrt.

(5) Příprava je trestná.“[90]

Toto ustanovení zákoníku chrání dítě v globálním smyslu jeho sexuální integrity. Ustanovení zahrnuje zásah do vývoje dítěte jak mravní, tak i tělesný. Ustanovení i dobře formuluje skutkovou podstatu spáchání činu v případě, kdy by oběť pachatele byla sama aktivní v sexuálním konání. Právě z toho důvodu je důležitá formulace –„ *..nebo kdo je jiným způsobem pohlavně zneužije.“*(viz. § 187 výše). Jiným způsobem je myšleno například osahávání na prsou, nebo genitálech, orální sex a další aktivity spojené s intimní sexualitou.

Za podstatnou a dle mého názoru stěžejní je věková hranice, kterou stanovuje TZ na 15 let, kdy je osoba brána jako dítě. Tato hranice se nejen v Evropě značně odlišuje a tak by její mezinárodní sjednocení bylo vhodné. Otázka věkové hranice dítěte bude podrobněji v této práci zkoumána a to na konci této kapitoly.

Šíření pornografie § 191 trestního zákoníku – Právě tento trestný čin zahrnuje postižení šíření dětské pornografie internetem a jinými komunikačními médii.

„(1). Kdo vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, v němž se projevuje násilí či neúcta k člověku, nebo

[90] § 187 trestního zákoníku (zákon č. 40/2009 Sb.) znění účinné od 1. 12. 2019

které popisuje, zobrazuje nebo jinak znázorňuje pohlavní styk se zvířetem, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci

(2) Kdo písemné, fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo

a) nabízí, přenechává nebo zpřístupňuje dítěti, nebo
b) na místě, které je dětem přístupné, vystavuje nebo jinak zpřístupňuje, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.
(3) Odnětím svobody na šest měsíců až tři léta bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 nebo 2

a) jako člen organizované skupiny,

b) tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem, nebo

c) v úmyslu získat pro sebe nebo pro jiného značný prospěch.

(4) Odnětím svobody na jeden rok až pět let bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 nebo 2

a) jako člen organizované skupiny působící ve více státech, nebo

b) v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu.“[91]

Ustanovení tohoto paragrafu s formulací skutkové podstat „*veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem“*, není úplně přesně formulováno. Právě počítačové sítě, jako je internet, jsou nejčastějším komunikačním kanálem pro šíření pornografie. Způsob šíření pornografie bude blíže specifikován ke konci této části práce.

Osobu pachatele této trestné činnosti dobře kvalifikuje například Průvodce trestněprávními předpisy a judikaturou.

„Pachatelem může být kdokoliv, kdo koná s úmyslem. Zákon nevyžaduje, aby měl pachatel specifické vlastnosti nebo schopnosti. V trestním zákoně najdeme tři kvalifikované skutkové podstaty, přitěžující okolnosti spočívají ve způsobu použitém pro šíření pornografie (filmem, tiskem), členství v organizované skupině a velikosti případného prospěchu.“[92]

[91] § 191 trestního zákoníku (zákon č. 40/2009 Sb.) znění účinné od 1. 12. 2019
[92] Fenyk Jaroslav, Trestní zákoník a trestní řád, Linde Praha 2010, ISBN 978-80-7201-802-4 str. 731

Výroba a jiné nakládání s dětskou pornografií § 192 trestního zákoníku – Skutková podstat tohoto trestného činu je obsahovou implementací směrnice Evropské rady a Parlamentu č. 93/2011, která nařizuje „*..členským státům přijmout opatření proti nakládání s dětskou pornografií, včetně jejího držení.* “[93]

„(1) Kdo přechovává fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě nebo osobu, jež se jeví být dítětem, bude potrestán odnětím svobody až na dva roky.

(2) Stejně bude potrestán ten, kdo prostřednictvím informační nebo komunikační technologie získá přístup k dětské pornografii.

(3) Kdo vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě nebo osobu, jež se jeví být dítětem, anebo kdo kořistí z takového pornografického díla, bude *potrestán odnětím svobody na šest měsíců až tři léta, zákazem činnosti nebo propadnutím věci.*

(4) Odnětím svobody na dvě léta až šest let nebo propadnutím majetku bude pachatel potrestán, spáchá-li čin uvedený v odstavci 3

a) jako člen organizované skupiny,

b) tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem, nebo

c) v úmyslu získat pro sebe nebo pro jiného značný prospěch.

(5) Odnětím svobody na tři léta až osm let nebo propadnutím majetku bude pachatel potrestán, spáchá-li čin uvedený v odstavci 3

a) jako člen organizované skupiny působící ve více státech, nebo

b) v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu “[94]

[93] Jelínek Jiří -Trestní právo hmotné: obecná část- Praha: LEGES 2016, ISBN 978-80-7502-120-5 str. 620
[94] § 192 trestního zákoníku (zákon č. 40/2009 Sb.) znění účinné od 1. 12. 2019

V ustanovení paragrafu je dobře zahrnuté konání pachatele, které je ustanoveno jako "*anebo kdo kořistí z takového pornografického díla"*. Kořistěním z díla tak umožňuje postihnout i případy, kdy pachatel získá z díla majetkový prospěch například zhotovením obalu nosiče, nebo se obohatí na samotné distribuci.

„Z hlediska českého trestního práva je otázka šíření pornografie řešena v § 191 až § 193 TZ. Jedná se o trestné činy šíření pornografie, výroba a jiné nakládání s dětskou pornografií a zneužití dítěte k výrobě pornografie. V § 191 T Z uvádí trestní zákoník jednotlivé formy nabízení závadné pornografie a stanoví podmínky pro to, aby se toto šíření stalo trestným dle českého trestního práva. Dle § 192 týkajícího se dětské pornografie se považuje za trestné kromě různých forem šíření dětské pornografie také její přechovávání."[95]

„Důvodem pro kriminalizaci přechovávání dětské pornografie je její větší závažnost oproti jiným formám pornografie. Její prohlížení patrně trestné nebude, pokud si jej osoba neukládá na nosič informací."[96]

Zneužití dítěte k výrobě pornografie § 193 trestního zákoníku –

„1) Kdo přiměje, zjedná, najme, zláká, svede nebo zneužije dítě k výrobě pornografického díla nebo kořistí z účasti dítěte na takovém pornografickém díle, bude potrestán odnětím svobody na jeden rok až pět let.

(2) Odnětím svobody na dvě léta až šest let bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1

a) jako člen organizované skupiny, nebo

b) v úmyslu získat pro sebe nebo pro jiného značný prospěch.

(3) Odnětím svobody na tři léta až osm let bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1

a) jako člen organizované skupiny působící ve více státech, nebo

b) v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu "[97]

[95] Jelínek Jiří a kol. -Trestní právo hmotné. 1. vydání. Praha: Leges, 2009. str. 560,
[96] Jelínek Jiří a kol.- O novém trestním zákoníku : Sborník příspěvků z mezinárodní konference Olomoucké právnické dny, květen 2009. 1. vydání. Olomouc: Leges, 2009.str .91-93

V tomto případě, jde-li o kořistění, zahrnuje tato skutková podstata například vědomé jednání osoby, která se jakkoliv účastí na zneužívání dítěte podílela. Jednání zahrnuje i pouhý převoz na místo, kde ke vzniku díla došlo. Právě takové jednání osob bude v části práce 4.2 Případová studie analyzováno.

Účast na pornografickém představení § 193a trestního zákoníku –

„Kdo se účastní pornografického představení nebo jiného obdobného vystoupení, ve kterém účinkuje dítě, bude potrestán odnětím svobody až na dvě léta.“[98]

Navazování nedovolených kontaktů s dítětem § 193b trestního zákoníku –

„Kdo navrhne setkání dítěti mladšímu patnácti let v úmyslu spáchat trestný čin podle § 187

odst. 1, § 192, 193, § 202 odst. 2 nebo jiný sexuálně motivovaný trestný čin, bude potrestán odnětím svobody až na dvě léta.“[99]

„Trestný čin navazování nedovolených kontaktů s dítětem, postihuje nedovolené navazování kontaktů s dítětem obecně ne jen prostřednictvím informačních a komunikačních technologií. Tato skutečnost je plněním směrnice nad rámec, směrnice předpokládá jen technologie, jako například webové kamery. Nově, se díky této skutkové podstatě trestá už samotné navrhnutí setkání za účelem jakékoliv trestné činnosti související se sexuální tématikou.“[100]

Legislativní vložení obou posledně uvedených paragrafů v roce 2014 do trestního zákoníku bylo skutečně nutné a umožnilo postihovat i další jednání související s dětskou pornografií.

Pachatelé této trestné činnosti, která je zaměřena proti dětem, v prvopočátcích většinou využijí naivity a důvěřivosti svých budoucích obětí. Prostřednictvím nejrůznějších sociálních sítí se prezentují jako jejich vrstevníci a snaží se v průběhu vzájemné komunikace získat nějaké intimní materiály, jakými jsou fotografie, nebo videa obnažených dětských těl. Po získání takových materiálů své oběti často vydírají, nebo se je snaží přimět k další spolupráci. Při spolupráci bývá oběti přislíben finanční obnos, který je tak lákavý, že oběti pod vidinou velké finanční hotovosti (pro dítě relativní) svolí a podlehnou nátlaku. Pachatel, tak vědomě

[97] § 193 trestního zákoníku (zákon č. 40/2009 Sb.) znění účinné od 1. 12. 2019
[98] § 193a trestního zákoníku (zákon č. 40/2009 Sb.) znění účinné od 1. 12. 2019
[99] § 193b trestního zákoníku (zákon č. 40/2009 Sb.) znění účinné od 1. 12. 2019
[100] Jelínek Jiří. Trestní právo hmotné: obecná část, zvláštní část. 5. aktualizované a doplněné vydání. Praha: Leges, 2016 - ISBN978-80-7502-120-5 str. 623-624

zmate dětskou mysl. Oběť se pak mylně domnívá, že bude focena profesionálním fotografem, nebo se může stát dokonce filmovou hvězdou. Pachatelé při svém protiprávním jednání vědí, jak oklamat dětskou mysl. Pachatel nemusí vždy nabízet jen finanční hotovost, někdy stačí dítěti nastínit určité výhody, které mu pak z jeho konání vyplynou. Ostatně toto bude uvedeno i v kapitole 4.2 Případová studie, která je součástí praktické části této práce. Je ale nutné upřesnit, že ne všechny takto zneužité děti musí pocházet z prostředí disfunkčních rodin, bez dobrého sociálního zázemí a pevného pouta rodičovské lásky. Pachatelé využívají skryté identity a v kontaktu přes sociální síť obvykle komunikují s dítětem například jako jejich vrstevníci, jak již bylo uvedeno. Skrývání identity pachatele je zpracováno v praktické části této práce 4.3.1 .

3.3.2 Problémy při objasňování kybernetických trestných činů páchaných proti dětem

Postup objasňování a dokazování kybernetických trestných činů má společný základ. Obdobné postupy jsou umožněny a vycházejí vždy z toho, že pachatel za sebou v kyberprostoru zanechává stopu. V tomto prostředí jde o informace obsažené v IP adrese, digitálním záznamu dat, nebo třeba v platební transakci uskutečněné prostřednictvím internetu. Taková stopa je označována jako Digitální stopa *„ …digitální stopou pak rozumíme jakoukoliv informaci s vypovídající hodnotou, uloženou nebo přenášenou v digitální podobě. "*[101]

Zajišťování digitálních stop je velice složité a v České republice ho provádějí orgány činné v trestním řízení. V případě užití digitální stopy jako důkazu, musí být její zajištění v souladu se zákonem. Při zajišťování je často nutný vstup do objektů - obydlí pachatelů, ve kterém se konkrétní důkazové médium nachází. Orgány činné v trestním řízení mohou úkony provádět až po vydání řádného souhlasu soudce s tímto zásahem do lidských práv. Stěžejní je především to, aby vytvořená elektronická kopie digitální stopy byla shodná s originálem a mohla být použita, jako nezpochybnitelný důkaz. V případě následného dokazování se musí obě formy kopie a také originálu shodovat obsahově. K zajišťování elektronických důkazů se vyjádřil i Ústavní soud v roce 2014. „ *Internet je zdrojem mnoha veřejně dostupných informací, které jsou tak přímo dostupné i orgánům činným v trestním řízení, ale stejně tak obsahuje množství informací soukromé povahy. Postupy aplikované příslušnými orgány při zjišťování těchto informací proto musí dodržovat rámec stanovený právními předpisy a musí*

[101] Porada Viktor, Roman Rak. -Teorie digitálních stop a její aplikace v kriminalistice a forenzních vědách. - Karlovarská právní revue 2006, č. 4

respektovat obecné principy, na nichž je založena činnost státních orgánů, zejména v maximální možné míře šetřit ústavně zaručená práva a svobody dotčených osob.“[102]

Právě tento nález Ústavního soudu řešil předložený důkaz Policií České republiky v podobě otisku obrazovky počítačového média – Print screen[103]. Tento otisk měl dokázat vzájemnou komunikaci účastníků prostřednictvím soukromého rozhraní komunikace na této síti. Komunikace byla uskutečněna prostřednictvím sociální sítě. Na takový důkazní materiál nebyl soudcem vydán příkaz podle § 88a odst. 1 trestního řádu[104] a nebyl ani dán souhlas k poskytnutí údajů samotným uživatelem telekomunikačního zařízení obrazovky, v tomto případě pachatele. Policejnímu orgánu tak byla uložena v rámci tohoto řízení pořádková pokuta. Složitost v zajišťování důkazů ze strany Policie České republiky v této oblasti kyberkriminality byla dobře specifikována již v roce *2005 „…bez skutečně špičkové průpravy v oblasti výpočetní techniky nemá policista šanci pachatele složitějších případů počítačové kriminality vůbec zjistit.“*[105]

K vydání první metodiky v ČR pro odhalování kybernetické trestné činnosti došlo v roce 1998.[106] Je nutné si uvědomit, že s globálním vývojem světa kybernetiky, se samozřejmě zlepšují a zdokonalují i elektronické prostředky, včetně rychlosti přenosu dat a jejich ochrana. Z tohoto důvodu je zjišťování a zajišťování digitálních stop z paměťových médií, nebo kyberprostoru, velice náročné. Trestná činnost pachatelů komerčních kybernetických trestných činů páchaných proti dětem se vztahuje zpravidla k delšímu časovému období a to především z důvodu větší ziskovosti a výhodnosti pro pachatele této trestné činnosti. Pachatelé se snaží za sebou nezanechat v kyberprostoru žádné, nebo pouze absolutně minimální stopy. V případě i minimálního podezření ze strany pachatele dochází k úplnému zničení těchto záznamů na paměťových médiích nebo v kyberprostoru. Právě pachatelé komerčních trestných činů páchají trestnou činnost, většinou jako organizovaná skupina.[107] Tato trestná činnost je i ze strany Policie České republiky odhalována pomocí speciálních týmů složených z odborníků v oblastech počítačové kriminality s dlouholetou praxí

[102] Nález Ústavního soudu, sp. zn. III. ÚS 3844/13, ze dne 30. 10. 2014.
[103] NET Servis, Zdroj 2020 [online] dostupné z http://www.otazky-a-odpovedi.cz/Jak-vytvorim-otisk-nebo-printscreen-obrazovky-toho-co-prave-na-monitoru-vidim/
[104]Zákon o trestním řízení soudním (trestní řád) č. 141/1961 Sb. - § 88 – [online] [citace 26.2.2020] Dostupné z: https://www.beck-online.cz/bo/chapterview-document.seam?documentId=onrf6mjzgyyv6mjugexhazryhawtsnq
[105] Smejkal Vladimír; Sokol Tomáš; Vlček Martin - Počítačové právo. 1. vyd. Praha: C.H. Beck 1995, str. 136
[106] Porada Viktor; Konrád Zdeněk - Metodika vyšetřování počítačové kriminality - 1. vyd.Praha1998 , Policejní akademie České republiky
[107] Porada Viktor; Straus Jiří - Kriminalistika: výzkum, pokroky, perspektivy- Plzeň 2013 - Vydavatelství Čeněk, str. 536.

zařazených u Služby kriminální policie a vyšetřování v jednotlivých krajích ČR.[108] Takové týmy provádějí nejprve rozbor dostupných důkazních materiálů a následně provádí operativně pátrací činnosti. Na základě výsledků těchto činností je pak ze strany Policie České republiky přistoupeno k Zahájení úkonů v TŘ.[109]

Pachatelé této specifické trestné činnosti ve většině případů využívají pro šíření závadových materiálů s dětskou pornografií právě internet. Komunikace zde bývá úmyslně skryta a snaha pachatelů o zahlazení stop je na vysoké úrovni. Z uvedeného důvodu v oblasti IT využívá Policie České republiky součinnost se speciálním celorepublikovým útvarem ÚZČ – Útvar zvláštních činností.[110] Právě pro zvýšení efektivity v trestním řízení, které je vedeno proti pachatelům kybernetické trestné činnosti, doporučuje Smejkal zřídit aplikaci nástrojů v podobě expertních systémů se statistickým hodnocením.[111] V průběhu vyšetřování jsou Policie České republiky zajišťovány důkazy, které, jak uvádí Porada a Straus, jsou následně podrobeny zkoumání znalců v oboru výpočetní techniky. Znalci zkoumají, jak uložená digitální data, tak elektronické stopy.[112] V rámci elektronické stopy se pak zkoumají ve virtuálních počítačových sítích pod názvem VPN[113] jednotlivé IP adresy. Tuto metodu popsal přehledně Maisner, který objasňuje, jak VPN ukrývá IP adresy. Na jednu IP adresu je v síti VPN napojeno několik počítačů. Servery v těchto sítích pak mění v časově krátkém období záznamy v DNS[114] o IP adresách. Za takto ukrytými IP adresami se následně skrývá konkrétní server, kde je ilegální obsah pachatelem ukryt. Oficiální provozovatelé takto napadených serverů vůbec nemusí tušit, že právě jejich server byl zneužit pro kyberkriminalitu a to ani po obsahové stránce.[115] Technicky a procesně je tato důkazní stránka orgánů činných v trestním

[108] Policie České republiky – Služba kriminální policie a vyšetřování, [online] [citace 28.2.2020] Dostupné z: https://www.policie.cz/clanek/o-nas-clanky-sluzba-kriminalni-policie-a-vysetrovani.aspx

[109] Policie České republiky – Zahájení trestního řízení , [online] [citace 26.2.2020]Dostupné z: https://www.policie.cz/clanek/trestni-rizeni.aspx

[110] Policie České republiky – Útvar zvláštních činností kriminální policie, [online] [citace 26.2.2020]. Dostupné z: https://www.policie.cz/clanek/utvar-zvlastnich-cinnosti-sluzby-kriminalni-policie-a-vysetrovani-716842.aspx

[111] Smejkal Vladimír -Kybernetická kriminalita - Plzeň 2015- Vydavatelství Čeněk, str. 499

[112] Porada Viktor, Straus Jiří -Kriminalistika: (výzkum, pokroky, perspektivy), Plzeň 2013: Vydavatelství Čeněk, 2013, str. 542.

[113] Virtuální privátní síť VPN - „*Jedná se o privátní počítačovou síť, která dovolí připojit vzdálené uživatele do cílené LAN přes Internet. Bezpečnost se řeší pomocí šifrovaného tunelu mezi dvěma body (nebo jedním a několika). Při navazování spojení je totožnost obou stran ověřována pomocí digitálních certifikátů.*“ Jirásek Petr, Novák Luděk, Požár Josef – Výkladový slovník kybernetické bezpečnosti, Policejní akademie ČR 2015, ISBN 978-80-7251-397-0, str. 184

[114] DNS server – „ *Distribuovaný hierarchický jmenný systém používaný v síti Internet. Překládá názvy domén na číselné IP adresy a zpět, obsahuje informace o tom, které stroje poskytují příslušnou službu (např. přijímají elektronickou poštu či zobrazují obsah webových prezentací) atd.*“ Jirásek Petr, Novák Luděk, Požár Josef – Výkladový slovník kybernetické bezpečnosti, Policejní akademie ČR 2015, ISBN 978-80-7251-397-0, str. 33

[115] Maisner Martin, Základy softwarového práva. 1. vyd. Praha: Wolters Kluwer ČR, 2011, str. 276 a násl.

řízení velice obtížná. Je třeba si ale uvědomit, že technická stránka dokazování je jedna věc, ale celkově se při objasňování a dokazování projevují bezesporu i ostatní vlivy, které nemalou měrou brzdí celkový průběh vyšetřování. Pohled na vlivy a příčiny neobjasněných trestných činů při dokazování a objasňování této trestné činnosti bude řešen v kapitole 4.1.2 praktické části práce.

3.4 Závěry teoretické části

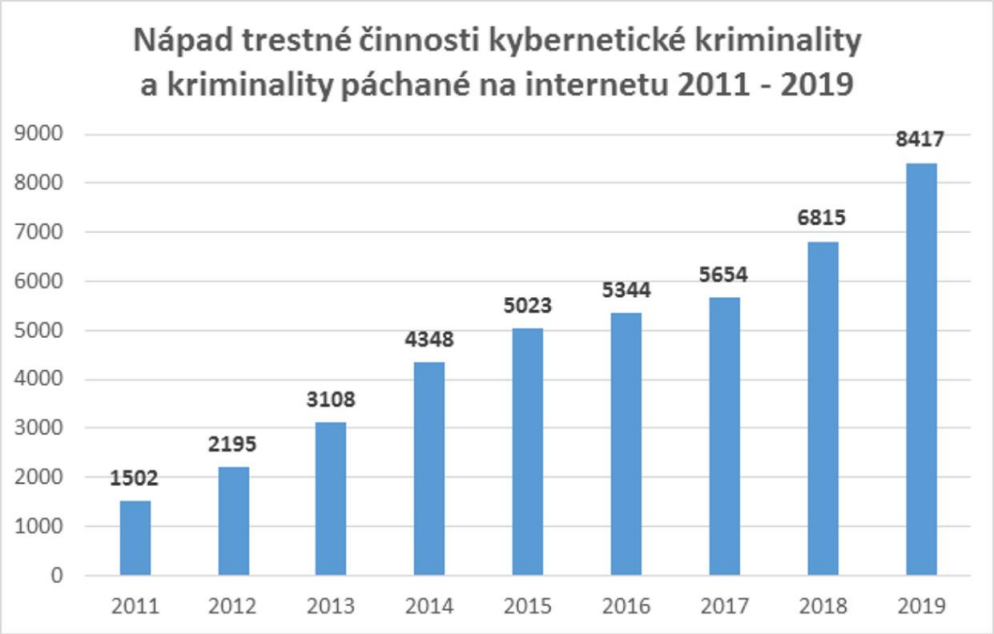
Samotný vznik Internetu, jako globální sítě s postupným vývojem a prvními projevy kyberkriminality byl podrobně zpracován v kapitole 3.1.1. Skutečnost, že se právě globální síť stane prostředkem pro páchání trestné činnosti, se dala očekávat. Celkově bylo nutné tuto činnost správně definovat a začít rozpoznávat hrozby, které s sebou přinášela. Jednání pachatelů a jejich sledovaný účel útoků byl postupně pojmenováván a vznikaly tak nové názvy a charakteristiky, pod kterými jsou označovány a rozlišovány dodnes. Počítačová kriminalita, stejně, jako Internet se ze země jejího vzniku USA rozšířila do celého světa postupem několika málo let. Rychlost závisela na technické a komunikační infrastruktuře dané země. První projevy kyberkriminality se v ČR začaly objevovat až po roce 2005. Ještě před tím si ale tuto globální hrozbu uvědomily nadnárodní orgány, jako je OSN a začaly se touto problematikou zabývat. V rámcovém řešení tak vznikl v roce 1990 jeden z prvních dokumentů v této oblasti pod názvem Manuál Organizace spojených národů o prevenci a kontrole trestných činů spojených s počítači. Postupně začala stejnou problematiku řešit i Rada Evropy a Evropská unie. Obě jmenované v průběhu času vydaly postupně několik dokumentů, které měly v rámci jednotlivých zemí upravit legislativu pro účinný boj s kyberkriminalitou. V rámci rychlého technického vývoje v oblasti kyberkriminality, byly některé dokumenty ještě podrobněji upraveny, případně byly postupně doplňovány o další související dokumenty. Tento postupný legislativní vývoj probíhal i v rámci ČR, kdy se v návaznosti na několik paragrafů vztahujících se k této části problematiky, přidávaly další a specifičtější. V těchto paragrafech byla již podrobně formulována příslušná skutková podstata konkrétních trestných činů. V návaznosti na změny trestního zákonodárství, byly od předních českých odborníků na tuto problematiku publikovány metodické příručky a právní výklady pojmů, ze kterých je možné čerpat i dnes. Podrobněji je tento vývoj zpracován v části práce kapitola 3.2. V rámci právního vývoje v oblasti dětské pornografie byly v ČR do trestního zákoníku legislativně vloženy v roce 2014 paragrafy 193a - Účast na pornografickém představení a paragraf 193b - Navazování nedovolených kontaktů s dítětem. Změna byla

provedena i v přístupu ohledně zajišťování důkazních prostředků, kdy orgány činné v trestním řízení musejí dle trestního řádu dodržovat jasně stanovené postupy a kroky, aby byl jejich důkazní materiál vůbec použitelný před soudem proti pachateli trestné činnosti. V souvislosti s důkazním materiálem byl ke konci teoretické části uveden i výrok Ústavního soudu při uplatňování zajištěných důkazů před soudem.

Závěrem této části práce lze konstatovat, že v budoucnu bude nutné učinit další změny, které by měly pružně a včas reagovat na vývoj problematiky kyberkriminality. Změna by se měla například týkat zohlednění větší společenské nebezpečnosti. Dítě, které se stalo obětí této závažné trestné činnosti, si tuto zkušenost odnáší do další části svého života a právě taková, i když po čase už jen vzpomínka, může ovlivnit jeho celý budoucí život. Tím se společenská nebezpečnost těchto trestných činů řadí do oblasti s nejvyšší prioritou.

Policie České republiky zveřejnila přehled kyberkriminality od roku 2011 do roku 2019. Čísla jasně vypovídají o tom, že kyberkriminalita je současným trendem zločinu. V roce 2011 evidovala Policie České republiky 1502 kybernetických trestných činů, zato v roce 2019 se toto číslo vyšplhalo k hranici 8417 evidovaných trestných činů.[116]

Obrázek č. 2 Nápad trestné činnosti prostřednictvím internetu, Policie České republiky 2011-2019



Zdroj: Policie České republiky Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

[116] Nápad trestné činnosti, Policie České republiky 201-2019, Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

V praktické části bude provedena analýza registrovaných a objasněných komerčních trestných činů páchaných proti dětem a to v časovém období po sobě jdoucích 4 let. V tabulkách budou označeny trestné činy vztahují se k dětské pornografii, kdy je Policie České republiky eviduje pod názvy - Komerční forma sexuálního zneužívání v závislosti (§ 187/2), Komerční forma sexuálního zneužívání v závislosti (§ 187/1,3,4), Ostatní mravnostní TČ (§ 190, § 192-§ 193). Také bude provedena procentuální analýza nárůstu této trestné činnosti v letech 2016 až 2019. V rámci krajů ČR bude statisticky zanalyzováno i šíření pornografie s jeho procentuálním nárůstem ve stejném období čtyř let. Uvedeny budou konkrétně i některé příčiny neobjasněnosti těchto trestných činů a práce se pokusí odhalit vliv sociálního prostředí na páchání této trestné činnosti v jednotlivých krajích ČR. Jako metoda bude použita i případová studie, ze které budou vyvozeny specifické závěry. Také budou zpracovány technické, právní a ekonomické možnosti prevence v této oblasti kyberkriminality.

4 Praktická část

4.1 Analýza registrovaných a objasněných komerčních trestných činů páchaných proti dětem

V této části práce bude provedena analýza registrovaných a objasněných komerčních trestných činů páchaných proti dětem. Je nutné si uvědomit, že tato samotná specifická problematika dětské pornografie je v oblasti normálního sexuálního vývoje, tedy jasně stanovených hranic normality jedince, za hranou sexuality, kterou by dospělý jedinec neměl, nejen z morálního hlediska, nikdy překročit. Do této skupiny musejí být zahrnuti, jak samotní pachatelé této závažné trestné činnosti, kteří hrubým způsobem mohou narušit sexuální vývoj dítěte, tak do této skupiny musíme zahrnout i samotné konzumenty výsledků jejich práce. Psychicky zdravý jedinec, posuzováno v oblasti sexuality, tedy netrpící sexuální deviací, nevyhledává dětskou pornografii. Z tohoto důvodu je skupina pachatelů ve vztahu k psychologii velice specifická. Z pohledu pachatele může jít pouze a zcela jen o finanční stránku věci, ve smyslu vlastního obohacení, ale i tak je morální vyspělost takovéhoto pachatele na velice nízké úrovni. Samotní odběratelé dětské pornografie jsou postiženi deviací spočívající v odlišné struktuře sexuální motivace, jež utváří tuto podobu sexuální poruchy a vede k vnějším projevům deviantního chování. Mají jiné osobní vnímání sexuality, než většinová společnost. Svojí odlišností a specifickou potřebou ve své podstatě vytvářejí prostředí trhu pro pachatele této činnosti, kteří jejich odlišnosti využívají. V tomto je spatřován rozdíl mezi sexuální deviací jako poruchou duševního zdraví a sexuální delikvencí, která značí porušení sociálních a právních norem.[117]

4.1.1 Statistická analýza (za období 2016-2019)

Tato podkapitola se věnuje analýze komerčních trestných činů, jak je evidovala Policie České republiky od roku 2016 do roku 2019. Tyto údaje byly čerpány z Odboru věcných gescí a statistik,[118] který statistická data tematizovaných problematik zpracovává. Údaje je možné zobrazit v interní síti Policie České republiky, která je označována jako INTRANET.[119] Dle jednotlivých žádostí je tento odbor schopný vytvořit specifickou analýzu dle zadání

[117] Weiss Petr, Sexuální deviace, Portál, s. r. o., Praha 2002, ISBN 978-80-7367-419-9
[118] Odbor věcných gescí a statistik je organizační článek Policejního prezidia České republiky
[119] Policie České republiky – Nahlížení do systémů *„ pro potřeby nahlížení do systému OSM je k dispozici síť Intranet“* [online] [cit. 29.02.2020] Dostupné z: https://www.policie.cz/clanek/nahlizeni-do-systemu.aspx

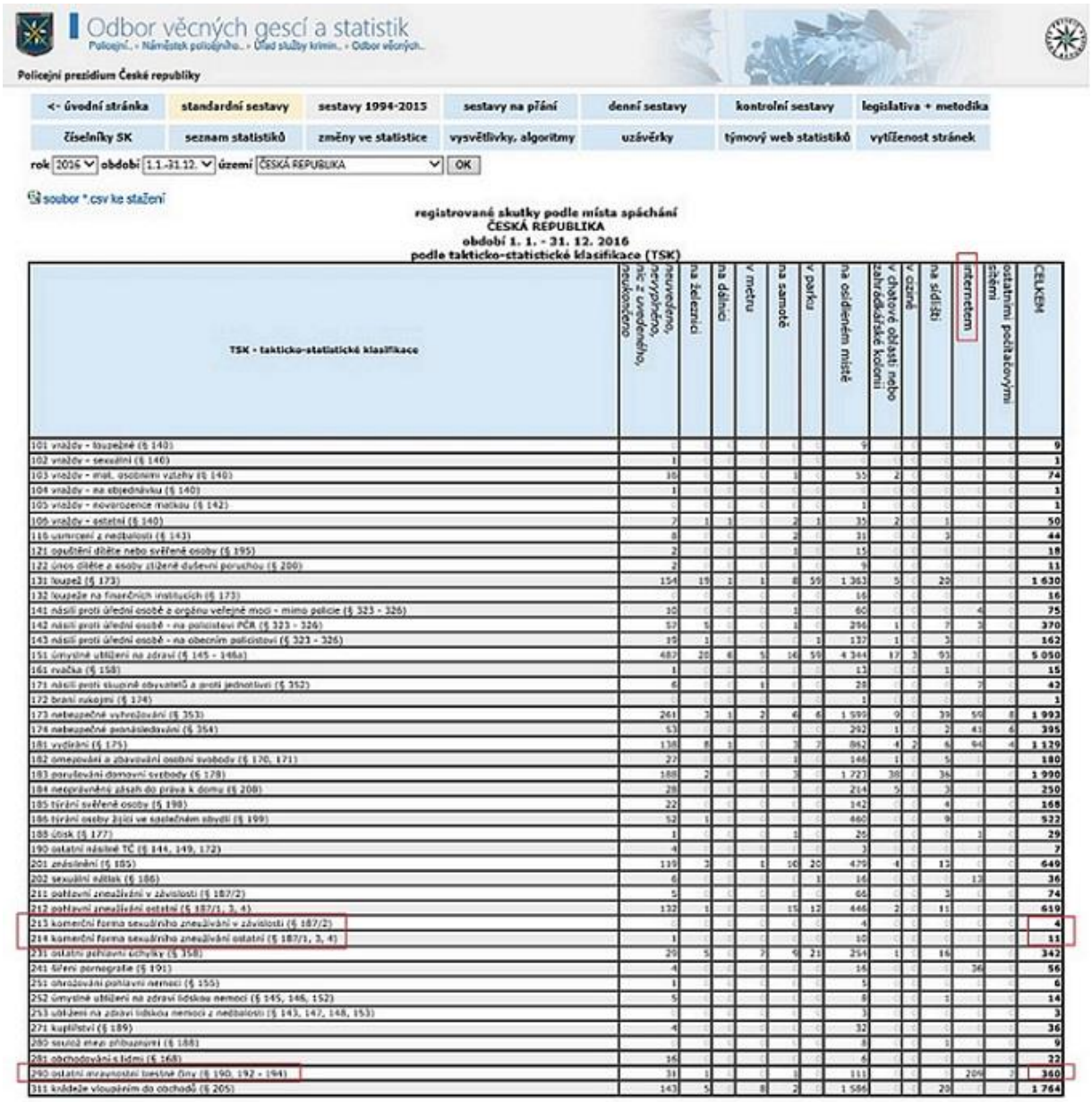
jednotlivých složek Policie České republiky, ale i soukromých subjektů. V případě soukromých subjektů je zde stanoveno pouze jediné pravidlo, aby informace nepodléhaly některému ze stupňů utajení[120] podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. V tom případě musí žadatel prokázat, že je držitelem tohoto osvědčení vydaného NBÚ.[121] Odbor statistik a gescí vede trestné činy pod zkratkou TSK,[122] kde jsou označeny pod čísly 213, 214, 290.

213 Komerční forma sexuálního zneužívání v závislosti (§ 187/2)
214 Komerční forma sexuálního zneužívání v závislosti (§ 187/1,3,4)
290 Ostatní mravnostní TČ (§ 190, § 192 - § 193)

V tabulkách, které jsou uvedeny v následující části této práce jsou od roku 2016 do roku 2019 vyznačeny uvedené trestné činy a v horní části tabulky je označen způsob páchání těchto skutků s uvedením - spácháno prostřednictvím internetu.

[120] Stupně utajení: § 4 zákona č. 412/2005 Sb., „*Utajovaná informace se klasifikuje stupněm utajení: a) Přísně tajné, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit mimořádně vážnou újmu zájmům České republiky, b) Tajné, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit vážnou újmu zájmům České republiky, c) Důvěrné, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit prostou újmu zájmům České republiky, d) Vyhrazené, jestliže její vyzrazení neoprávněné osobě nebo zneužití může být nevýhodné pro zájmy České republiky*". [online] [cit. 29.02.2020], Dostupné z: https://www.nbu.cz/cs/pravni-predpisy/zakon-c-412-2005/1122-uplne-zneni-zakona-c-412-2005/
[121] NBÚ – Národní bezpečnostní úřad - informace, Dostupné z: https://www.nbu.cz
[122] TSK – Takticko- statistické klasifikace

Obrázek č. 3 TSK Registrované skutky podle místa spáchání (internetem) za rok **2016**



Odbor věcných gescí a statistik

Policejní prezidium České republiky

<- úvodní stránka | standardní sestavy | sestavy 1994-2015 | sestavy na přání | denní sestavy | kontrolní sestavy | legislativa + metodika

číselníky SK | seznam statistik | změny ve statistice | vysvětlivky, algoritmy | uzávěrky | týmový web statistik | vytíženost stránek

rok 2016 období 1.1.-31.12. území ČESKÁ REPUBLIKA OK

soubor *.csv ke stažení

registrované skutky podle místa spáchání
ČESKÁ REPUBLIKA
období 1. 1. - 31. 12. 2016
podle takticko-statistické klasifikace (TSK)

TSK - taktico-statistická klasifikace	neuvedeno, nezjištěno, nic z uvedeného, neukončeno	na železnici	na dálnici	v metru	na samoté	v parku	na odlehlém místě	v chatové oblasti nebo zahrádkářské kolonii	v cizině	na sídlišti	internetem	ostatními počítačovými sítěmi	CELKEM
101 vražda - loupežné (§ 140)							9						9
102 vražda - sexuální (§ 140)	1												1
103 vražda - mat. osobními výhody (§ 140)	10				1		55	2					74
104 vražda - na objednávku (§ 140)	1												1
105 vražda - novorozence matkou (§ 142)							1						1
106 vražda - ostatní (§ 140)	7	1	1		2	1	35	2		1			50
110 usmrcení z nedbalosti (§ 143)	8				2		33			3			44
121 opuštění dítěte nebo svěřené osoby (§ 195)	2				1		15						18
122 únos dítěte a osoby ztížené duševní poruchou (§ 200)	2						9						11
131 loupež (§ 173)	154	19	2	1	8	59	1 363	5		20			1 630
132 loupeže na finančních institucích (§ 173)							16						16
141 násilí proti úřední osobě z orgánu veřejné moci - mimo policie (§ 323 - 326)	10				1		60				4		75
142 násilí proti úřední osobě - na policistovi PČR (§ 323 - 326)	52	5			1		296	1		7	3		370
143 násilí proti úřední osobě - na obecním policistovi (§ 323 - 326)	15	1				1	137	1		5			162
151 úmyslné ublížení na zdraví (§ 145 - 146a)	487	20	6	5	14	59	4 344	17	3	93			5 050
161 rvačka (§ 158)	1						13			1			15
171 násilí proti skupině obyvatelů a proti jednotlivci (§ 352)	6			1			28				2		42
172 braní rukojmí (§ 174)							1						1
173 nebezpečné vyhrožování (§ 353)	261	3	1	2	4	6	1 599	9		33	59	8	1 993
174 nebezpečné pronásledování (§ 354)	53						292	1		2	43	6	395
181 vydírání (§ 175)	136	8	1		7	7	862	4	2	6	94	4	1 129
182 omezování a zbavování osobní svobody (§ 170, 171)	27				1		146	1		5			180
183 porušování domovní svobody (§ 178)	188	2			3		1 727	38		36			1 990
184 neoprávněný zásah do práva k domu (§ 208)	28						214	5		3			250
185 týrání svěřené osoby (§ 198)	22						142			4			168
186 týrání osoby žijící ve společném obydlí (§ 199)	12	1					460			9			522
188 únos (§ 177)	1				1		26				1		29
190 ostatní násilné TČ (§ 144, 149, 172)	4						3						7
201 znásilnění (§ 185)	119	3		1	10	20	479	4		13			649
202 sexuální nátlak (§ 186)	6					1	16				13		36
211 pohlavní zneužívání v závislosti (§ 187/2)	5						64			3			74
212 pohlavní zneužívání ostatní (§ 187/1, 3, 4)	132	1			15	12	446	2		11			619
213 komerční forma sexuálního zneužívání v závislosti (§ 187/2)							4						4
214 komerční forma sexuálního zneužívání ostatní (§ 187/1, 3, 4)	1						10						11
231 ostatní pohlavní ochyby (§ 358)	20	5		2	9	21	254	1		16			342
241 šíření pornografie (§ 191)	4						14				36		56
251 ohrožování pohlavní nemocí (§ 155)	1						5						6
252 úmyslné ublížení na zdraví šířkou nemocí (§ 145, 146, 152)	5						8			1			14
253 ublížení na zdraví šířkou nemocí z nedbalosti (§ 143, 147, 148, 153)							3						3
271 kuplířství (§ 189)	4						32						36
280 soužití mezi příbuznými (§ 188)							8			1			9
281 obchodování s lidmi (§ 168)	16						6						22
290 ostatní mravnostní trestné činy (§ 190, 192 - 194)	31	1			1		113				204	3	360
311 krádež vloupáním do obchodů (§ 205)	143	5		8	2		1 586			20			1 764

Zdroj: Odbor gescí a statistik PP Policie České republiky

Z tabulky vyplývá, že Policie České republiky v roce 2016 registrovala počet činů spáchaných prostřednictvím internetu pod TSK 213, 214, 290.

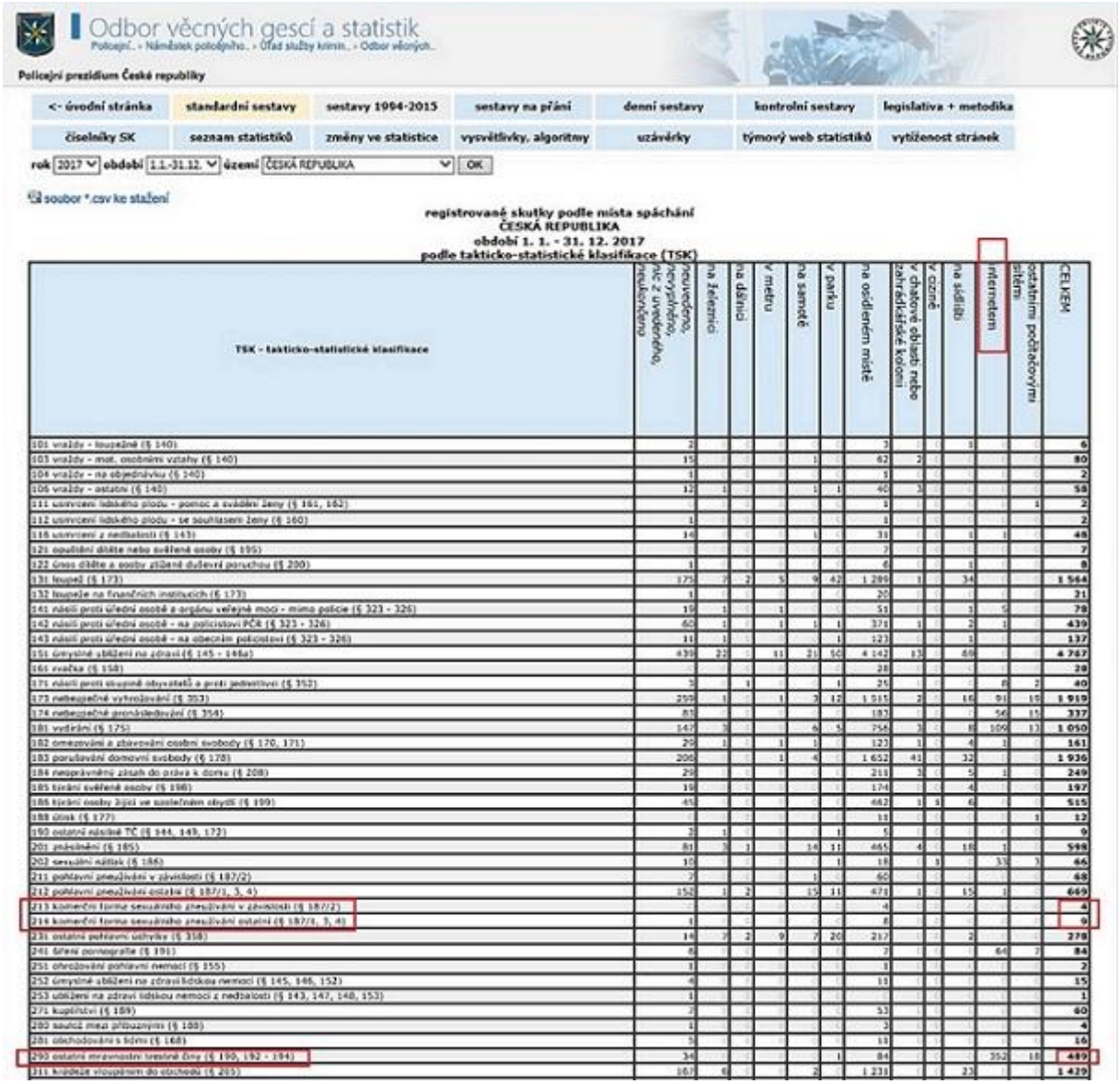
213 Komerční forma sexuálního zneužívání v závislosti (§187/2) 4

214 Komerční forma sexuálního zneužívání v závislosti (§187/1,3,4) 11

290 Ostatní mravnostní TČ (§190, 192-193) 360

Celkem **375** činů, z toho je evidováno **15** komerčních dle všech ustanovení § 187 TZ.

Obrázek č. 4 TSK Registrované skutky podle místa spáchání (internetem) za rok **2017**



Odbor věcných gescí a statistik

Policejní prezidium České republiky

<- úvodní stránka | standardní sestavy | sestavy 1994-2015 | sestavy na přání | denní sestavy | kontrolní sestavy | legislativa + metodika

číselníky SK | seznam statistik | změny ve statistice | vysvětlivky, algoritmy | uzávěrky | týmový web statistik | vytíženost stránek

rok 2017 období 1.1.-31.12. území ČESKÁ REPUBLIKA OK

soubor *.csv ke stažení

registrované skutky podle místa spáchání
ČESKÁ REPUBLIKA
období 1. 1. - 31. 12. 2017
podle taktico-statistické klasifikace (TSK)

TSK - taktico-statistické klasifikace	neuvedeno, nevyplněno, nic z uvedeného, neuloženo	na železnici	na dálnici	v metru	na samoobsluze	v parku	na ostatním místě	v chatové oblasti nebo zahrádkářské kolonii	v cizině	na sídlišti	internetem	ostatními počítačovými sítěmi	CELKEM
101 vraždy - loupežné (§ 140)	2						3			1			6
103 vraždy - mot. osobními vztahy (§ 140)	15				1		62	2					80
104 vraždy - na objednávku (§ 140)	1						1						2
106 vraždy - ostatní (§ 140)	12	1			1	1	40	3					58
111 usmrcení lidského plodu - pomoc a svádění ženy (§ 161, 162)							1					1	2
112 usmrcení lidského plodu - se souhlasem ženy (§ 160)	1						1						2
116 usmrcení z nedbalosti (§ 143)	14				1		31			1	1		48
121 opuštění dítěte nebo svěřené osoby (§ 195)							2						7
122 činu dítěte a osoby svěřené duševní poruchou (§ 200)	1						6			1			8
131 loupež (§ 173)	173	7	2	5	9	42	1 289	1		34			1 564
132 loupeže na finančních institucích (§ 173)	1						20						21
141 násilí proti úřední osobě a orgánu veřejné moci - mimo policie (§ 323 - 326)	19	1		1			51			3	3		78
142 násilí proti úřední osobě - na policistovi PČR (§ 323 - 326)	60	1		1	1	1	371	1		2	1		439
143 násilí proti úřední osobě - na obecním policistovi (§ 323 - 326)	11	1				1	123			1			137
151 úmyslné ublížení na zdraví (§ 145 - 146a)	439	22		11	21	50	4 142	13		66			4 767
161 svatba (§ 158)							28						28
171 násilí proti skupině obyvatel a proti jednotlivci (§ 352)	3		1			1	25				8	2	40
173 nebezpečné vyhrožování (§ 353)	299	1		1	2	12	1 515	2		16	91	10	1 919
174 nebezpečné pronásledování (§ 354)	83						182				56	11	337
181 vydírání (§ 175)	147	3			6	5	756	3		8	109	13	1 050
182 omezování a zbavování osobní svobody (§ 170, 171)	29	1		1	1		123	1		4	1		161
183 porušování domovní svobody (§ 178)	206			1	4		1 652	41		32			1 936
184 neoprávněný zásah do práva k domu (§ 208)	29						211	3		5	1		249
185 loupež svěřené osoby (§ 198)	19						174			4			197
186 loupež osoby žijící ve společném obydlí (§ 199)	45						462	1	1	6			515
188 únos (§ 177)							11					1	12
190 ostatní násilné TČ (§ 144, 149, 172)	3	1				1	5						9
201 znásilnění (§ 185)	81	3	1		14	11	465	4		18	1		598
202 sexuální nátlak (§ 186)	10					1	18		1		33	1	66
211 pohlavní zneužívání v závislosti (§ 187/2)	7				1		60						68
212 pohlavní zneužívání ostatní (§ 187/1, 3, 4)	152	1	2		15	11	471	1		15	1		669
213 komerční forma sexuálního zneužívání v závislosti (§ 187/2)							4						4
214 komerční forma sexuálního zneužívání ostatní (§ 187/1, 3, 4)	1						8						9
231 ostatní pohlavní ústrky (§ 198)	14	3	2	9	7	20	217			2			278
241 šíření pornografie (§ 191)	8						2				64	2	84
251 ohrožování pohlavní nemocí (§ 155)	1						1						2
252 úmyslné ublížení na zdraví lidskou nemocí (§ 145, 146, 152)	4						11						15
253 ublížení na zdraví lidskou nemocí z nedbalosti (§ 143, 147, 148, 153)	1												1
271 kuplířství (§ 189)	7						53						60
280 soužití mezi příbuznými (§ 188)	1						3						4
281 obchodování s lidmi (§ 168)	5						11			1			16
290 ostatní mravnostní trestné činy (§ 190, 192 - 194)	34					1	84				352	18	489
311 krádeže vloupáním do obchodu (§ 205)	167	6			2		1 231			23			1 429

Zdroj: Odbor gescí a statistik PP Policie České republiky

Z tabulky vyplývá, že Policie České republiky v roce 2017 registrovala počet činů spáchaných prostřednictvím internetu pod TSK 213, 214, 290.

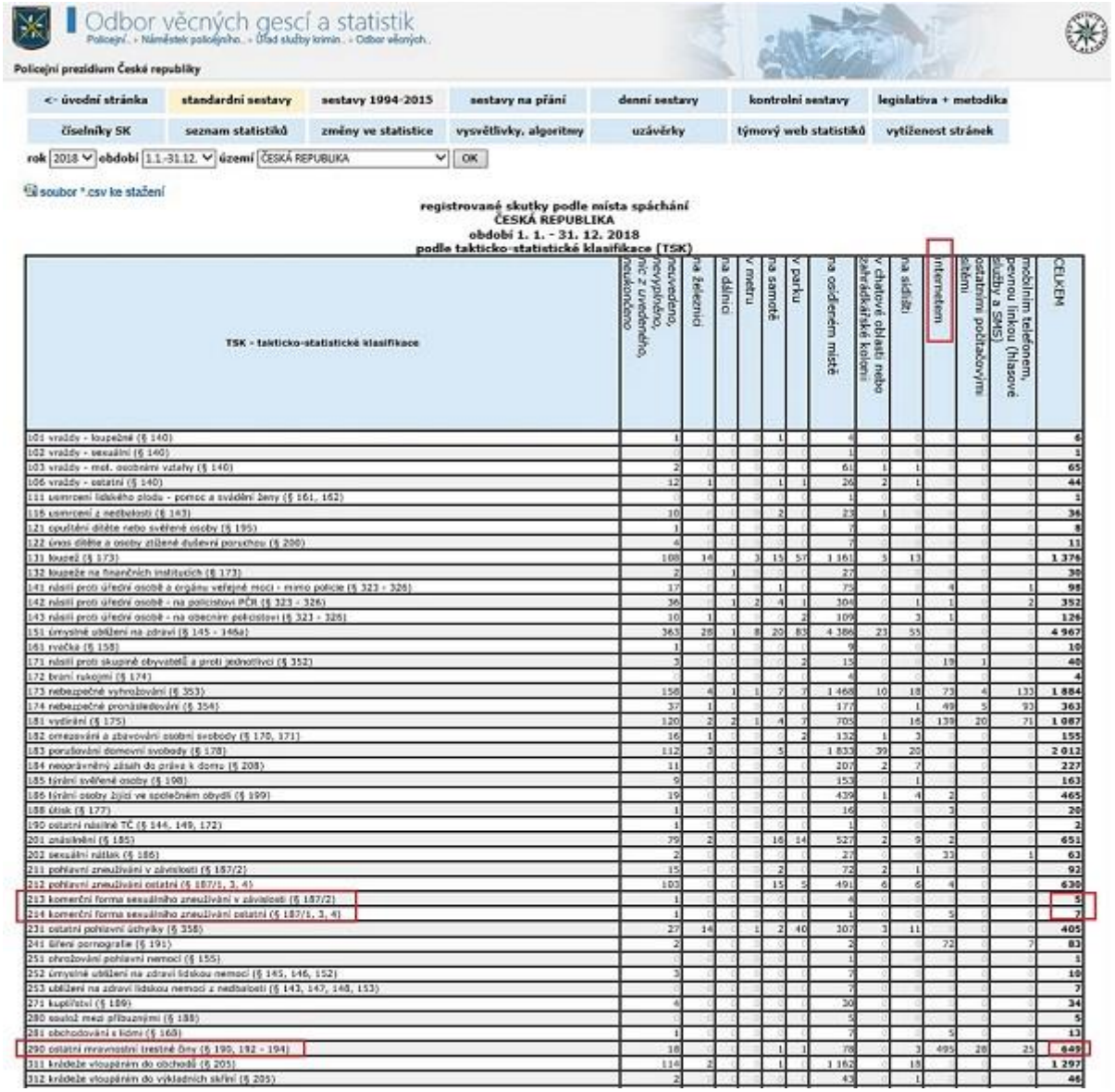
213 Komerční forma sexuálního zneužívání v závislosti (§187/2) 4

214 Komerční forma sexuálního zneužívání v závislosti (§187/1,3,4) 9

290 Ostatní mravnostní TČ (§190, 192-193) 489

Celkem **502** činů, z toho je evidováno **13** komerčních dle všech ustanovení § 187 TZ.

Obrázek č. 5 TSK Registrované skutky podle místa spáchání (internetem) za rok **2018**



Odbor věcných gescí a statistik

Policejní prezidium České republiky

<- úvodní stránka | standardní sestavy | sestavy 1994-2015 | sestavy na přání | denní sestavy | kontrolní sestavy | legislativa + metodika

číselníky SK | seznam statistik | změny ve statistice | vysvětlivky, algoritmy | uzávěrky | týmový web statistik | vytíženost stránek

rok 2018 období 1.1.-31.12. území ČESKÁ REPUBLIKA OK

soubor *.csv ke stažení

registrované skutky podle místa spáchání
ČESKÁ REPUBLIKA
období 1. 1. - 31. 12. 2018
podle takticko-statistické klasifikace (TSK)

TSK - takticko-statistické klasifikace	nezjištěno, nevyplněno, nic z uvedeného, neukončeno	na železnici	na dálnici	v metru	na samotě	v parku	na ostatním místě	v chatové oblasti nebo zahrádkářské kolonii	na sídlišti	internetem	ostatními počítačovými sítěmi	mobilním telefonem, pevnou linkou (hlasové služby a SMS)	CELKEM
101 vraždy - loupežné (§ 140)	1				1		4						6
102 vraždy - sexuální (§ 140)							1						1
103 vraždy - mot. osobními vztahy (§ 140)	2						61	1	1				65
106 vraždy - ostatní (§ 140)	12	1			1	1	26	2	1				44
111 usmrcení lidského plodu - pomoc a svádění ženy (§ 161, 162)							1						1
115 usmrcení z nedbalosti (§ 143)	10				2		23	1					36
121 opuštění dítěte nebo svěřené osoby (§ 195)	1						7						8
122 únos dítěte a osoby ztížené duševní poruchou (§ 200)	4						7						11
133 loupež (§ 173)	108	14		3	15	57	1 161	3	13				1 376
132 loupeže na finančních institucích (§ 173)	2		1				27						30
141 násilí proti úřední osobě a orgánu veřejné moci - mimo policie (§ 323 - 326)	17				1		75			4		1	98
142 násilí proti úřední osobě - na policistovi PČR (§ 323 - 326)	36		1	2	4	1	304		1	1		2	352
143 násilí proti úřední osobě - na obecním policistovi (§ 323 - 326)	10	1				2	109		3	1			126
151 úmyslné ublížení na zdraví (§ 145 - 146a)	363	28	1	8	20	83	4 386	23	55				4 967
161 rvačka (§ 158)	1						9						10
171 násilí proti skupině obyvatelů a proti jednotlivci (§ 352)	3					2	15			19	1		40
172 braní rukojmí (§ 174)							4						4
173 nebezpečné vyhrožování (§ 353)	158	4	1	1	7	7	1 468	10	18	73	4	133	1 884
174 nebezpečné pronásledování (§ 354)	37	1					177		1	49	5	93	363
181 vydírání (§ 175)	120	2	2	1	4	7	705		16	139	20	71	1 087
182 omezování a zbavování osobní svobody (§ 170, 171)	16	1				2	132	1	3				155
183 porušování domovní svobody (§ 178)	112	5			5		1 833	39	20				2 012
184 neoprávněný zásah do práva k domu (§ 208)	11						207	2	7				227
185 týrání svěřené osoby (§ 198)	9						153		1				163
186 týrání osoby žijící ve společném obydlí (§ 199)	19						439	1	4	2			465
188 útisk (§ 177)	1						16			3			20
190 ostatní násilné TČ (§ 144, 149, 172)	1						1						2
201 znásilnění (§ 185)	79	2			16	14	527	2	9	2			651
202 sexuální nátlak (§ 186)	2						27			33		1	63
211 pohlavní zneužívání v závislosti (§ 187/2)	15				2		72	2	1				92
212 pohlavní zneužívání ostatní (§ 187/1, 3, 4)	103				15	5	491	6	6	4			630
213 komerční forma sexuálního zneužívání v závislosti (§ 187/2)	1						4						5
214 komerční forma sexuálního zneužívání ostatní (§ 187/1, 3, 4)	1						1			5			7
231 ostatní pohlavní úchylky (§ 358)	27	14		1	2	40	307	3	11				405
241 šíření pornografie (§ 191)	2						2			72		7	83
251 ohrožování pohlavní nemocí (§ 155)							1						1
252 úmyslné ublížení na zdraví lidskou nemocí (§ 145, 146, 152)	3						7						10
253 ublížení na zdraví lidskou nemocí z nedbalosti (§ 143, 147, 148, 153)							7						7
275 kuplířství (§ 189)	4						30						34
280 soužití mezi příbuznými (§ 188)							5						5
281 obchodování s lidmi (§ 168)	1						7			5			13
290 ostatní mravnostní trestné činy (§ 190, 192 - 194)	18				1	1	78		3	495	28	25	649
311 krádeže vloupáním do obchodů (§ 205)	114	2			1		1 162		18				1 297
312 krádeže vloupáním do výkladních skříní (§ 205)	2						43		1				46

Zdroj: Odbor gescí a statistik PP Policie České republiky

Z tabulky vyplývá, že Policie České republiky v roce 2018 registrovala počet činů spáchaných prostřednictvím internetu pod TSK 213, 214, 290.

213 Komerční forma sexuálního zneužívání v závislosti (§187/2) 4

214 Komerční forma sexuálního zneužívání v závislosti (§187/1,3,4) 9

290 Ostatní mravnostní TČ (§190, 192-193) 489

Celkem **661** činů, z toho je evidováno **13** komerčních dle všech ustanovení § 187 TZ.

Obrázek č. 6 TSK Registrované skuty podle místa spáchání (internetem) za rok **2019**

registrované skutky podle místa spáchání
ČESKÁ REPUBLIKA
období 1. 1. - 31. 12. 2019
podle taktícko-statistické klasifikace (TSK)

TSK - taktícko-statistická klasifikace	neuvedeno, nevyplněno, nic z uvedeného, neukončeno	na železnici	na dálnici	v metru	na zastávce	v parku	na ostatním veřejném místě	v chatové oblasti nebo zahrádkářské kolonii	na sídlišti	internetem	sběrnými	ostatními počítačovými	pevnou linkou (hlasové služby a SMS)	mobilním telefonem,	hřbitovy vč. přilehlých parkovišť	koupaliště vč. přilehlých parkovišť	obchodní centra vč. přilehlých parkovišť	sportovní areály (mimo lyžařských) vč. přilehlých parkovišť	lyžařské areály vč. přilehlých parkovišť	festivaly a koncerty vč. přilehlých parkovišť	letiště vč. přilehlých parkovišť	kempy	CELKEM
0 právní kvalifikace nestanovena	2	3			4		62			2			1										73
101 vraždy - loupežné (§ 140)					1		11						1										12
103 vraždy - mot. osobními vztahy (§ 140)	3	1					68	1					1			1							74
104 vraždy - na objednávku (§ 140)	1						3						1										4
106 vraždy - ostatní (§ 140)	2						43	1	5				1			2							53
111 usmrcení lidského plodu - pomoc a svádění ženy (§ 161, 162)							1																1
112 usmrcení lidského plodu - se souhlasem ženy (§ 160)							1																1
116 usmrcení z nedbalosti (§ 143)	3	1		1	2	1	53	1															62
121 opuštění dítěte nebo svěřené osoby (§ 195)						2	8																10
122 činos dítěte a osoby ztížené duševní poruchou (§ 200)	1						7																8
131 loupež (§ 173)	20	23	3	3	14	75	1 233	2	36				1			15				2			1 427
132 loupeže na finančních institucích (§ 173)							12																12
141 násilí proti úřední osobě a orgánu veřejné moci - mimo kvalifikace (§ 323 - 326)	3	3					90			7	1	5											107
142 násilí proti úřední osobě - na policistovi PČR (§ 323 - 326)	6	2	1	1	3	1	331	2	4			3		1	2	3		2					362
143 násilí proti úřední osobě - na obecním policistovi (§ 323 - 326)	2	1					138	1	1	1		1			2								147
151 úmyslné ublížení na zdraví (§ 145 - 146a)	65	35	4	8	23	94	4 263	31	60			1	1	3	20	25	1	24	2	3			4 684
161 rvačka (§ 158)						1	7																8
171 násilí proti skupině obyvatelů a proti jednotlivci (§ 352)							29			19			1			1							50
172 braní rukojmí (§ 174)							1																1
173 nebezpečné vyhrožování (§ 353)	31	7	2		2	9	1 513	9	33	72	8	183	1		13	2						1	1 891
174 nebezpečné pronásledování (§ 354)	4						147		1	49	2	155											358
181 vydírání (§ 175)	24	7	1		14	13	784	3	17	169	13	102			12								1 159
182 omezování a zbavování osobní svobody (§ 170, 171)	3				3	1	148	2	5						1								163
183 porušování domovní svobody (§ 178)	15				3	1	1 893	73	37							1				2		1	2 026
184 neoprávněný zásah do práva k domu (§ 208)	1				3		199	5	1														208
185 týrání svěřené osoby (§ 198)	4						218	2	2														226
186 týrání osoby žijící ve společném obydlí (§ 199)	5						522		8														535
188 útisk (§ 177)							13			3			1										13
190 ostatní násilné TČ (§ 144, 149, 172)	1						1																4
201 znásilnění (§ 185)	14	2		1	37	24	580	6	13						3	1	1			1			683
202 sexuální nátlak (§ 186)	2	1			1		17			84													105
211 pohlavní zneužívání v závislosti (§ 187/2)	4					1	83																88
212 pohlavní zneužívání ostatní (§ 187/1, 3, 4)	28	8			23	16	570	6	10				1		2	1	3					2	672
213 komerční forma sexuálního zneužívání v závislosti (§ 187/2)							4																4
214 komerční forma sexuálního zneužívání ostatní (§ 187/1, 3, 4)	1						7																8
231 ostatní pohlavní úchylky (§ 358)	1	6	1	5	5	31	207		8						2	5	1						272
241 šíření pornografie (§ 191)							10			77	2	10											99
251 ohrožování pohlavní nemocí (§ 155)							1																1
252 úmyslné ublížení na zdraví lidskou nemocí (§ 145, 146, 152)					1		8																9
253 ublížení na zdraví lidskou nemocí z nedbalosti (§ 143, 147, 148, 153)							1																1
271 kuplířství (§ 189)	2						31			3						1							37
280 soužití mezi příbuznými (§ 188)							6																6
281 obchodování s lidmi (§ 168)	2						18																20
290 ostatní mravnostní trestné činy (§ 190, 192 - 194)	4	1			1		75		1	597	14	35											728

Zdroj: Odbor gescí a statistik PP Policie České republiky

Z tabulky vyplývá, že Policie České republiky v roce 2019 registrovala počet činů spáchaných prostřednictvím internetu pod TSK 213, 214, 290.

213 Komerční forma sexuálního zneužívání v závislosti (§187/2) 4

214 Komerční forma sexuálního zneužívání v závislosti (§187/1,3,4) 9

290 Ostatní mravnostní TČ (§190, 192-193) 489

Celkem **728** činů, z toho je evidováno **12** komerčních dle všech ustanovení § 187 TZ.

Tabulka č. 2 Vyhodnocení sledovaného období **2016 – 2019**

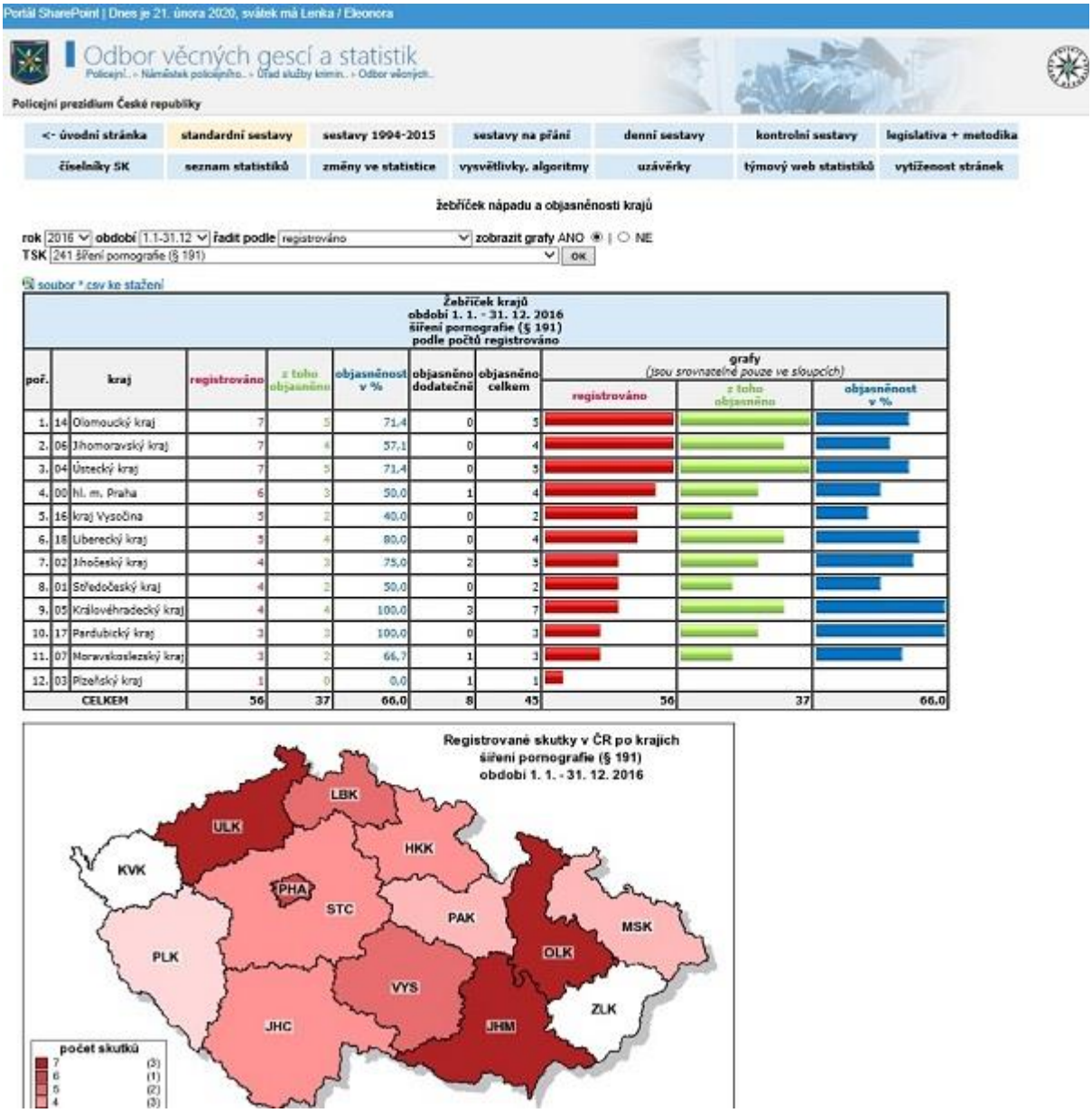
R O K	KOMERČNÍ TČ §187/1,2,3,4	CELKEM TČ §187/1,2,3,4 + §190,§192-§193	SPÁCHÁNO INTERNETEM
2016	15 činů	375 činů	209 činů
2017	13 činů	502 činů	352 činů
2018	13 činů	661 činů	500 činů
2019	12 činů	728 činů	597 činů
CELKEM TČ	**53 činů**	**2266 činů**	**1658 činů**

Zdroj: vlastní zpracování

Z provedené analýzy jasně vyplývá, že počet komerčních trestných činů, jak je ve sledovaném období registrovala Policie České republiky, se významně nelišil a jeho průměr za období čtyř let je 13,25 činů. Celkový nárůst počtu trestných činů v TSK 213, 214 a 290 za sledované období stoupl z 375 registrovaných trestných činů na neuvěřitelných 728 činů ročně. To je ve čtyřletém období nárůst o 94 % a tento nárůst je opravdu alarmující. Nejvíce je ale patrný nárůst v počtu těchto spáchaných skutků prostřednictvím internetu. Zde je z 209 činů ve čtyřletém období nárůst o 185 % na hranici 597 registrovaných činů. Tento nárůst je zapříčiněn tím, že internet umožňuje anonymitu.

Do této části práce je rovněž zahrnuta statistika z období let 2016 až 2019 ze stejného portálu, kde je zpracován počet trestných činů v krajích ČR, vedených pod TSK 241 šíření pornografie dle § 191 TZ. Na začátku bude uveden obrázek s počtem případů ve zpracování TSK č. 241 za rok 2016 a ostatní roky do období 2019 budou obsaženy v části práce 8 – Přílohy.

Obrázek č. 7 TSK 241 šíření pornografie - za rok **2016**



Žebříček krajů
období 1. 1. - 31. 12. 2016
šíření pornografie (§ 191)
podle počtů registrováno

poř.		kraj	registrováno	z toho objasněno	objasněnost v %	objasněno dodatečně	objasněno celkem
1.	14	Olomoucký kraj	7	5	71,4	0	5
2.	06	Jihomoravský kraj	7	4	57,1	0	4
3.	04	Ústecký kraj	7	5	71,4	0	5
4.	00	hl. m. Praha	6	3	50,0	1	4
5.	16	kraj Vysočina	5	2	40,0	0	2
6.	18	Liberecký kraj	5	4	80,0	0	4
7.	02	Jihočeský kraj	4	3	75,0	2	5
8.	01	Středočeský kraj	4	2	50,0	0	2
9.	05	Královéhradecký kraj	4	4	100,0	3	7
10.	17	Pardubický kraj	3	3	100,0	0	3
11.	07	Moravskoslezský kraj	3	2	66,7	1	3
12.	03	Plzeňský kraj	1	0	0,0	1	1
CELKEM			56	37	66,0	8	45

grafy (jsou srovnatelné pouze ve sloupcích)

registrováno	z toho objasněno	objasněnost v %
56	37	66,0

Zdroj: Odbor gescí a statistik PP Policie České republiky

V šíření pornografie je jasně viditelný nárůst skutků od roku 2016 z pouhých 56 skutků na 99 skutků v roce 2019. Při součtu všech skutků za období čtyř let ve všech krajích ČR podle evidence je pořadí ve sledovaných dvanácti zobrazovaných krajích, dle analýzy Policie České republiky, od nejvyššího evidováno celkově takto: Počet skutků za 4 roky – viz následující tabulka.

Tabulka č. 3 TSK Šíření pornografie vyhodnocení dle počtu registrovaných skutků dle krajů ČR za období **2016 - 2019**

1. Ústecký kraj **36**	5. Liberecký kraj **26**	9. Středočeský kraj **18**
2. Královohradecký kraj **35**	6. Moravskoslezský kraj **25**	10. kraj Vysočina **17**
3. hl. m. Praha **31**	7. Jihomoravský kraj **23**	11. Zlínský kraj **16**
4. Olomoucký kraj **27**	8. Jihočeský kraj **22**	12. Pardubický kraj **14**

Zdroj: vlastní zpracování

Z tabulky jednoznačně vyplývá, že šíření pornografie se děje na celém území ČR, avšak Ústecký kraj dominuje. V období čtyř let zde bylo evidováno o více než jedenkrát skutků více, než v kraji Pardubickém, který je veden až ke konci evidence. Další analýzy budou provedeny v části práce 4.1.3.

4.1.2 Příčiny neobjasněných trestných činů

Jak již bylo v této práci uvedeno, činnost pachatelů je prováděna obzvlášť skrytým a rafinovaným způsobem. Nikdo z pachatelů i jejich spolupachatelů z pochopitelných objektivních i subjektivních důvodů nechce, aby se vůbec někdy informace o tom, že se na tomto druhu trestné činnosti jakoukoli měrou podíleli, dostala na veřejnost. Velkou roli zde hraje čas a to je především překážkou pro vyšetřovatele. Právě shromažďování důkazů je problém, se kterým se Policie České republiky potýká nejvíce. Někdy je totiž uběhlá doba od spáchání k oznámení jednání majícího znaky této trestné činnosti příliš dlouhá. V případě, že si oběť neuchovává komunikaci s pachatelem, těžko můžeme předpokládat, že pachatel bude vědomě sám na sebe shromažďovat důkazy ve formě komunikace s obětí.

V České republice mají operátoři mobilních sítí dle zákona č. 273/2012 Sb.[123] povinnost uchovávat data o komunikaci půl roku.[124] Podstatou zálohování operátorů je sice komunikace,

[123] Zákon č. 273/2012 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), [online] [citace 26.2.2020]. Dostupné z: https://www.beck-online.cz/bo/chapterview-document.seam?documentId=onrf6mrqgezf6mrxgmwta

[124] V roce 2011 došlo ale ke zrušení povinnosti českých operátorů tyto data o komunikaci uchovávat. Tato situace nastala po návrhu pana poslance Bendy a dalších padesáti poslanců. Návrh poslanců byl odůvodněn tak, že časové rozmezí půl roku na uchovávání dat je zbytečně dlouhá doba. Ústavní soud návrhu překvapivě vyhověl dne 31. března 2011 a jako Nález Ústavního soudu č. 94/2011 Sb., neukládal za povinnost operátorům shromažďovat komunikační data. V tu chvíli nastala paradoxní situace, kterou zřejmě poslanci s panem Bendou úplně tak nedomysleli. Bez těchto dat od operátorů, neměla Policie České republiky vůbec možnost při vyhlášení

kterou ze zákona dodatečně poskytují, ale drtivá většina osob neví, že operátoři již neposkytují obsahy hovorů, zpráv nebo e-mailů. Vyžádané výpisy dle zákona č. 273/2012 Sb. obsahují jen informace, jakými jsou účastnická čísla, kdy, kde a jak dlouho spolu tato čísla komunikovala, nebo je pouze operátorem sdělena informace, z jaké emailové adresy byla zpráva odeslána na jinou adresu. Právě tato obsahová část komunikace, která není zálohována, by mohla být velice důležitá při dokazování trestné činnosti. Je ale pochopitelné, že si oběti od začátku komunikace s pachatelem nezálohují veškerou virtuální komunikaci v kyberprostoru. Při dokazování této trestné činnosti je pak ale takový důkaz, jakým je například Print Screen[125] obrazovky monitoru při komunikaci s pachatelem, stěžejní. V důkazním řízení nestačí pouhé tvrzení, že v komunikaci s pachatelem byl takový a takový obsah. Je tedy právně nutné, tento obsah komunikace něčím doložit. Variant komunikace v kyberprostoru je v současné době mnoho. Nejčastější jsou uživatelem voleny mobilní operátoři k odesílání sms, mms a uskutečňování hovorů. Mezi novodobé komunikační kanály dále patří Facebook[126], Skype[127], WatsApp[128], Messenger[129], Instagram[130], Twitter[131] a další. V případě zahraničních poskytovatelů je situace se zálohováním dat různorodá. SKYPE patří pod společnost Microsoft,[132] která má sídlo ve Spojených státech. Svojí pobočku má ale SKYPE v Lucembursku, kde byl v roce 2003 založen. Dle platných zákonů USA nic neukládá této společnosti za povinnost data uchovávat. Jde o výsostní postavení této společnosti, která, ale v rámci mezinárodní spolupráce při odhalování trestných činů vychází všeobecně státním bezpečnostním složkám vstříc. Požadované údaje od této společnosti má Policie České republiky po jejich vyžádání ještě tentýž den, nebo den následující. Horizont ukládání dat, je

---

mimořádné situace lokalizovat mobilní telefony, které u sebe mohou mít například ztracené díti, nebo senioři. Tento zákaz byl bezesporu jen bonusem pro kriminalitu. To se změnilo až 1. října 2012 z důvodu vydání zákona č. 273/2012 Sb. Nejdůležitější zněna byla zakotvena v § 97 odstavec 3, kde je opět stanovena povinnost poskytovatelů služeb elektronických komunikací uchovávat provozní a lokalizační údaje po dobu 6 měsíců. Mobilní operátoři opět museli shromažďovat mobilní data a tak bylo možné zpětně zjišťovat důležité lokace mobilních telefonů zájmových osob. Celou kauzou se následně ještě zabýval Ústavní soud, který dne 22. května 2019 vše potvrdil a tím stanovil jasná pravidla v ČR pro uchovávání dat mobilních operátorů.

[125] V překladu otisk obrazovky – Zdroj NET Servis, [online] [citace 24.2.2020] Dostupné z : http://www.otazky-a-odpovedi.cz/Jak-vytvorim-otisk-nebo-printscreen-obrazovky-toho-co-prave-na-monitoru-vidim/

[126] Webový systém sloužící ke komunikaci mezi lidmi – zasílání textových a obrazových zpráv atd.

[127] Dceřiná společnost firmy Microsoft – umožňuje v síti PTP uskutečňovat telefonní hovory

[128] Dceřiná společnost firmy Facebook - zasílání textových a obrazových zpráv s možností uskutečnit i videohovor prostřednictvím PC, telefonu, tabletu atd.

[129] Webový klient od společnosti Facebook umožňující zasílání textových a obrazových souborů s možností chatování

[130] Aplikace pro mobilní systémy umožňující zasílání textových a obrazových souborů s možností chatování

[131] Sociální internetová síť umožňující jejím uživatelům sdílet a komentovat textové příspěvky ostatních uživatelů

[132] Americká společnost vyrábějící PC, programy a ostatní počítačové hardwarové a softwarové vybavení

ale zřejmě podobný, jako u českých operátorů. V případě Instagramu a WhatsApp které patří pod společnost Facebook je situace o něco složitější. Pro získání základních komunikačních údajů je možné žádost směřovat na evropskou pobočku, ale v případě zjištění úplného obsahu komunikace je nutné, aby tuto žádost podalo Nejvyšší státní zastupitelství ČR. Žádost je pak odeslána do Spojených států amerických, kde společnost Facebook sídlí. Délka doby ukládání opět v časovém horizontu odpovídá ukládání záznamů u nás. Oficiální stanovisko ze strany Facebooku a ostatních dříve jmenovaných společností, ohledně zálohování dat pocházejících rámcově z jejich sítí, nebylo nikdy vydáno. Skutečností je, že třeba sousední Slovensko, nebo Německo vůbec virtuální data nezálohují. Společnost Google se sídlem také ve Spojených státech amerických podává pouze základní informace o komunikaci v kyberprostoru bez vyžádání státního zástupce České republiky.

Celkové zhodnocení počítačové kriminality v počtu registrovaných a objasněných komerčních trestných činů páchaných proti dětem nebude nikdy úplně objektivní. Čísla statistik, která uvádí Policie České republiky jako evidované a následně objasněné skutky jsou jen špičkou pomyslného ledovce. Většina této trestné činnosti se přesunula do částí internetu, která je normálnímu uživateli skryta. Kyberkriminalita a internet jsou dvě od sebe neoddělitelné části. Je ale nutné si uvědomit, že to není jen viditelný internet, kde dochází k páchání trestné činnosti, ale především je to jeho skrytá část. Právě tam se kyberzločin a obzvlášť obchod s dětskou pornografií přesunul. Je to jedna z dalších příčin, proč se nedaří tuto trestnou činnost v plné míře odhalovat. Pro pochopení příčin neobjasněnosti těchto trestných činů je v této části práce pojem skrytý internet osvětlen.

Hloubkový internet, se dělí na dvě části a za normálních okolností není počítačovým prohlížečům viditelný. Tento internet je dle své hloubky utajení nazýván Deep Web (Hluboký, nebo neviditelný web) a Dark Web (Temný web). Odhady odborníků z oblasti IT[133] za poslední roky jsou takové, že tzv. normální povrchový internet, který používají běžní uživatelé na celém světě ke komunikaci, tvoří pouze 4 procenta celkového internetu. Zbylých 96 procent je tvořeno právě Hlubokým a Temným internetem. Temný web se začal používat v roce 2009. Komunikace zde probíhá prostřednictvím šifrovaných anonymních sítí, které fungují uvnitř internetu. Na tomto webu dochází k největšímu obchodování s dětskou pornografií, nelegálními léky a prodávají a nakupují se zde také zbraně i drogy. Za toto zboží

[133] IT – informační technologie

se zde nejčastěji platí kryptoměnou. Kryptoměny[134] se skvěle hodí k utajení a anonymitě nejen prodejců, ale také odběratelů.

Další překážkou při objasňování kyberkriminality v oblasti kybernetických trestných činů páchaných proti dětem je strach a stud z odhalení a to i v případě poškozených osob. Do této skupiny by se daly zahrnout, jak oběti, těchto trestných činů, tak i jejich blízcí. Většina z nich o tom, co se událo, nebo co se stále děje, mluvit nechce, nebo páchání trestné činnosti úmyslně přehlíží a vědomě ji vnitřně popírá. Policie České republiky se ale často již při prvotních úkonech ověřování informace o páchání v oblasti této trestné činnosti setkává se skutečností, že získání kvalitních informací z dané lokality, kde k páchání trestné činnosti dochází, je velice složité. Na vině jsou místní občanské poměry, ale také mezilidské vztahy. Běžnou praxí je i situace, kdy s Policií nechtějí spolupracovat ani samotní oznamovatelé z důvodu odhalení jejich identity při vyšetřování případu.

4.1.3 Vliv sociálního prostředí na páchání komerčních trestných činů zaměřených proti dětem v krajích ČR

V každém jedinci se sociální prostředí, ve kterém vyrůstá a ve kterém se pohybuje, jasně odráží a v průběhu života ho celou dobu ovlivňuje. Kriminální jednání pachatelů je odrazem vnějších vlivů, které na ně působí. Abychom byli schopni pachatele sociálně zařadit, musíme znát jeho hodnotové orientace, sociální začlenění a další vlivy s tím spojené. Sociální prostředí působí stejně na pachatele, jako na jejich oběti.

U komerčních trestných činů zaměřených proti dětem, jak je eviduje Policie České republiky vycházela statistická analýza v krajích ČR takto - viz. následující tabulka a jednotlivé analýzy Policie České republiky pro roky 2016 až 2019 jsou uvedeny v části práce 8 – Přílohy, obrázek č. 8 - č. 19.

[134] Specifikace kryptoměn - Kryptoměnu, třeba jako je Bitcoin nelze nijak ovlivňovat a je ve své podstatě decentralizovaná od všech světových vlád. Nikdo nemůže způsobit její inflaci, měnu padělat, řídit finanční toky, ale hlavně jí nikdo nemůže zabavit, jako finanční hotovost na běžném účtu. To se týká i zmrazení účtu. Nikdo kromě majitele nemusí znát soukromý kryptovací klíč. Tento klíč slouží k přístupu k účtu, kde je virtuální měna uložena. Do dnešního dne se nikomu nepodařilo kryptování, tedy šifrování, v síti kryptoměn rozluštit a proniknout do ní. Nejznámější kryptoměny jsou často útokem hackerů, ale zatím bez závažné hrozby a penetrace zvenčí. Jedinou nevýhodou této virtuální měny je možnost ztracení kryptovacího klíče od schránky, kde je kryptoměna datově uložena. Platby prostřednictvím kryptoměn probíhají zcela hladce, ale pachatelům hlavně nahrává skutečnost, že probíhají anonymně. V současné době je například hodnota jednoho Bitcoinu v přepočtu 189.193,- Kč. Internetový obchod ALZA začal platbu touto anonymní měnou akceptovat a přijímat již v roce 2017. V České republice se také uskutečnila koupě prvního bytu při použití virtuální měny a to v Praze roku 2017. Využitelnost kryptoměn a hlavně jejich anonymita a snadná obchodovatelnost pachatelům v této oblasti jejich anonymitu jen usnadňuje. Počet kryptoměn se v březnu roku 2018 pohyboval okolo hranice 1658 různých druhů.

Tabulka č. 4 Komerční trestné činy zaměřené proti dětem **2016 – 2019** dle TSK Policie České republiky

R O K	REGISTROVÁNO /OBJASNĚNO §187/2	REGISTROVÁNO /OBJASNĚNO §187/1,3,4	KRAJE /POČET /EVIDOVÁNO
2016	4 / 2 činů	4 / 2 činů	Liberecký 6 Olomoucký 2
2017	4 / 3 činů	9 / 8 činů	Středočeský 6, Královohradecký 2, Pardubický 1, Karlovarský 1, Liberecký 1, Zlínský 1, Olomoucký 1
2018	5 / 5 činů	7 / 3 činů	Středočeský 7, Královohradecký 2, Jihočeský 1, Liberecký 1, Ústecký 1
2019	4 / 2 činů	8 / 6 činů	Jihomoravský 4, Liberecký 3, Středočeský 2, Karlovarský 1, Moravskoslezský 1, Jihomoravský 1
Celkem	**17 / 12 činů**	**28 / 19 činů**	**Celkem 45 /objasněnost 66,45%**

Zdroj: vlastní zpracování – čerpáno z: Odbor gescí a statistik PP – vedeno v práci sekce 8 Přílohy

Tabulka č. 5 Ostatní mravnostní trestné činy **2016 – 2019** dle TSK Policie České republiky

R O K	REGISTROVÁNO /OBJASNĚNO §190 - §194	KRAJE /POČET /EVIDOVÁNO
2016	360 / 240 činů	Praha 56, Jihomoravský 52, Moravskoslezský 35, Středočeský 30, Plzeňský 27, Královohradecký 26, Zlínský 25, Ústecký 22, Liberecký 22, kraj Vysočina 21, Olomoucký 14, Jihočeský 12, Pardubický 12, Karlovarský 6
2017	489 / 309 činů	Praha 78, Moravskoslezský 63, Jihočeský 45, Středočeský 43, Královohradecký 39, Olomoucký 35, Ústecký 34, Jihomoravský 32, Zlínský 31, Liberecký 24, kraj Vysočina 23, Pardubický 18, Plzeňský 14, Karlovarský 10
2018	649 / 427 činů	Praha 92, Moravskoslezský 80, Jihomoravský 79, Královohradecký 60, Středočeský 52, Jihočeský 46, Plzeňský 42, Ústecký 40, kraj Vysočina 37, Liberecký 32, Zlínský 31, Pardubický 24, Olomoucký 22, Karlovarský 12
2019	728 / 508 činů	Jihomoravský 117, Praha 102, Moravskoslezský 66, Středočeský 64, Ústecký 56, Královohradecký 55, Jihočeský 54, Zlínský 44, kraj Vysočina 42, Olomoucký 31, Pardubický 30, Plzeňský 25, Liberecký 23, Středočeský 2, Karlovarský 19
Celkem	**2217 / 1484 činů**	**2217 činů /celková objasněnost 66,75%**

Zdroj: vlastní zpracování – čerpáno z: Odbor gescí a statistik PP – vedeno v práci sekce 8 Přílohy

Zajímavá je stejná dvoutřetinová objasněnost trestných činů.

Pořadí dle krajů ve statistice komerčních trestných činů v období let **2016 – 2019** dle TSK Policie České republiky.

1. Středočeský 15 činů, 2. Liberecký 9 činů, 3. Jihomoravský a Královohradecký 4 činy, Olomoucký a Moravskoslezský 3 činy, ostatní uvedené kraje po jednom činu.

Statistická analýza komerčních trestných činů vyhodnotila v období mezi lety 2016 - 2019, jako kraj s největším počtem těchto trestných činů kraj Středočeský a Liberecký.

Celková objasněnost těchto činů v tomto období byla 66,45%.

Pořadí dle krajů ve statistice ostatních mravnostních trestných činů dle § 190 - 194 v období let 2016 – 2019 .

1. Praha 328 činů, 2. Jihomoravský kraj 280 činů, 3. Moravskoslezský kraj 244 činů.

Statistická analýza ostatních mravnostních trestných činů vyhodnotila v období mezi lety 2016 - 2019, jako kraj s největším počtem těchto trestných činů Prahu a Jihomoravský kraj.

Celková objasněnost těchto skutků v tomto období byla 66,75 %.

Z hlediska poměru sociálního prostředí k páchání této trestné činnosti se tyto dvě analýzy v krajích odlišují. Z pohledu komerčních trestných činů proti dětem se v případě první analýzy jednalo o nejvážnější situaci ve Středočeském kraji. Tento kraj se ale mezi sociálně slabé kraje zařadit nedá. Z toho je patrný závěr, že policejní statistiky pouze evidují místo spáchání skutku dle místní krajové příslušnosti, ale již neevidují, z jakého kraje pocházely oběti této trestné činnosti. Po prostudování několika policejních spisů v uvedeném období, které jsou zde statisticky uváděné, bylo zjištěno, že ani statistická analýza místa trvalého bydliště oběti by tento vliv sociálního prostředí neukázala. Důvod je v rozdílném údaji o místě trvalého bydliště oběti dle registru obyvatel ČR a místem jejího skutečného bydliště. Právě slabší sociální vrstva obyvatel, která byla touto trestnou činností zasažena, má jako údaj o trvalém bydlišti uvedenu adresu místního úřadu. Zpracováním případové studie v následující kapitole této práce, bude tento vliv sociálního prostředí na oběti a jejich okolí znatelnější. Vliv sociálního prostředí na komerční trestnou činnost páchanou proti dětem v internetovém prostředí nelze z policejních statistik jednoznačně určit. V policejní databázi ETŘ, ani v žádných ostatních databázích, které Policie České republiky používá, není sociální prostředí osob nijak evidováno. Policejní orgán není ani oprávněn takové informace od osob vyžadovat. V navazující části práce jsou v případové studii zachyceny dva případy této problematiky. Bližším zkoumáním obou skutků je patrné, že sociální prostředí více ovlivňuje oběti, než

pachatele. Trestná činnost s tímto zaměřením, konkrétně jen ve vztahu k pachateli je schopna pohltit všechny části lidské společnosti, bez ohledu na věk, vzdělání a také finanční situaci. Tato činnost je páchána v průběhu delšího časového období ve všech regionech a pachatelé své oběti vyhledávají na celém území ČR. To platí ale i obráceně, jelikož oběti (s nimi například jejich rodiče) jsou schopni pod vidinou zisku k pachateli přijet až domů, bez ohledu na vzdálenost.

4.2 Případová studie

Pro případovou studii byly vybrány dva již ukončené případy dětské pornografie. Tyto případy spadají do statistiky Policie České republiky. Případové studie byly prováděny na základě zjištěných skutečností z policejních spisů k jednotlivým případům s přihlédnutím na velké množství materiálu ve spisech uložených. Byly stanoveny tři oblasti z případové studie dvou činů, na které se výzkum zaměřil a vzájemně je porovnal.

Oblast:
1. Důvod odhalení této trestné činnosti
2. Motivy pachatelů / účastníků / obětí při páchání této trestné činnosti
3. Konečný dopad na pachatele / účastníky / oběti

První případ, který byl také medializován, se odehrál na Náchodsku. Právě tam měl v bývalém textilním učilišti zřízený fotoateliér hlavní organizátor pan R. Jeho známá paní Y z Ukrajiny, která se dvěma dětmi dlouhodobě žila v České republice, byla v začátcích opětovným startovacím impulsem pro tuto trestnou činnost, kterou pan R pak léta páchal. Je důležité uvést, že obdobnou trestnou činnost páchal pan R i v minulosti a byl za ní odsouzen. Dalším spolupachatelem byl jeho známý pan H se stejnou trestní minulostí. Panu H měl pan R vypomáhat při tomto focení, kdy pan R focení časově nezvládal, protože sháněl po celé České republice nové, zajímavé objekty k fotografování. Rodiče dětí oslovoval prostřednictvím letáků, kde nabízel za sto fotografií finanční částku až čtyřicet tisíc korun. Pan R s panem H a paní Y se zaměřili na dětskou klientelu. Než začal pan R shánět své dětské oběti po celé ČR, tak v ateliéru za účasti paní Y fotili a natáčeli na video obě děti paní Y a to v různých erotických pozicích. Za sérii fotografií, kterou do zahraničí odesílala paní Y, inkasovali částky okolo 100 tisíc korun. Zásilky směřovaly do Švédska a Španělska, kde měl pan R kontakty již z minulosti. Pak začal pan R fotografovat i jiné děti, které v doprovodu svých rodičů začaly ateliér navštěvovat. Fotografie bez vědomí rodičů končily přes prostředníky v zahraničí na

placených internetových stránkách. Do ateliéru pana R průběžně přicházely děti v doprovodu svých rodičů a pan R rodiče ujišťoval, že se jedná o umělecké focení, nikoli pornografii. Jednalo se o rodiče s dětmi ze slabších sociálních skupin, kteří tak kompenzovali svojí finanční situaci. Rodiny pan R průběžně kontaktoval s přesvědčivou legendou účasti jejich dětí na uměleckém focení. Když rodiče souhlasili, tak do ateliéru pana R dorazili a to někdy i včetně proplacení cestovních nákladů. Samotnému focení byli rodiče přítomni někdy jen na začátku, kdy ještě nedocházelo k focení se sexuálním podtextem. Jednalo se o focení dětí v různých kostýmech a následně se pomalu přecházelo u děvčat na focení v krajkovém prádle včetně silonových punčošek, vysokých bot a sexy pohledů do objektivu.

Z informací vyšetřovacího spisu vyplývá, že takto organizovaná skupina nafotila přibližně sedmdesát dětí. Pan R ale u soudu tvrdil, že nafotil jen něco okolo dvaceti sérií fotografií s dětmi. Celá skupina měla i svého odborníka, který fotografie graficky upravoval do konečné umělecké podoby. Tuto službu pro skupinu obstarával známý pana R, pan M. Rodičům dětí pod vidinou finanční částky, která se pohybovala okolo 10 tisíce korun za jedno focení, asi ani nedocházelo, čeho jsou součástí.

Policie tento případ vyšetřovala od roku 2013. Necelé dva roky policisté shromažďovali důkazy sběrem dat ze zahraničních internetových portálů a monitorovali pohyb okolo ateliéru. Celý vyšetřovací spis má okolo 25 tisíc stran textu a důkazního materiálu. Pan R u soudu doznal, že jde z jeho strany o osobní selhání, ale dle jeho názoru se o pornografii nikdy nejednalo. Fotografie podle něj měly pouze sexuální charakter. Celá skupina si takto během prodeje dětské pornografie měla vydělat přibližně 5 miliónů korun. Součástí spisu jsou ale zjištěné finanční transakce, které při součtu dosahují hranice 15 miliónů korun. Při zatýkání této skupiny v roce 2014 došlo v rámci mezinárodní spolupráce k zatčení jejich dalších spolupachatelů ve státech Švédsko, Španělsko, Francie a Kanada.

Hlavního organizátora pana R odsoudil již potřetí Krajský soud na tři roky do vězení a uložil mu peněžitý trest. Rozsudek není pravomocný a je možné, že se pan R, jako již dvakrát předtím odvolá. Další členy skupiny soud odsoudil a to paní Y na tři roky ve vězení s dozorem, pana H na dva roky ve vězení s ostrahou a panu M uložil soud podmíněný trest dva roky s tříletou podmínkou.

Druhý případ ukazuje, jak vlastní matka může opět pro peníze zneužít k dětské pornografii své vlastní děti. Jedná se o nedávno ukončený případ a tak nebudou uváděna ani písmena označující jména zúčastněných. Pro upřesnění lze pouze uvést, že se tento případ odehrál v severní části naší republiky a oběti pocházejí ze slabšího sociálního prostředí.

Z výpovědi matky vyplynulo, jak se celá situace vyvíjela od samého počátku, kdy nejprve přišla k dcerám do pokoje a sdělila jim, že si udělá jen pár jejich fotografií. Dcery nic nenamítaly a tak jejich matka nafotila několik snímků děvčátek. Po předešlé domluvě fotografie odeslala zcela prostě prostřednictvím svého emailu na email, který jí byl předtím v elektronické komunikaci sdělen. Jednala s příslibem, že když se příjemci fotky budou líbit, pošle matce finanční částku. Fotografie se líbily a tak pan X zaslal běžným bankovním převodem finanční hotovost na účet matky. V doplňujícím emailu zaslaném matce následně uvedl, že by zaslal i větší částku, kdyby byla děvčátka oblečena třeba do šatiček, punčošek a tímto způsobem doplňuje své požadavky. Matka s tímto nadále neměla větší mentální problém a tak své dcery nastrojila dle požadavku a opět pořídila sérii fotografií. Popsaný postup se několikrát opakuje. Peníze za pořízené fotografie jsou pro matku, jak následně uvedla, příjemné, s ospravedlněním, že přeci je samoživitelka v chudém regionu. Jak se ale pozvolna navyšovala finanční částka za zaslané fotografie, zvyšovaly se i nároky platícího. Od sukýnek a punčošek se postupně upustilo a matka fotografovala děvčátka úplně nahá. Sice při výpovědi uvedla, že v duchu jí to přišlo divné a v hloubi duše si již říkala, že je to asi nějaký divný člověk, ale převážilo vědomí, že peníze se hodí a zase tolik se nestalo. Jen nafotila své holky spolu. Pak došlo ke změně, kdy kupující již nadále nebyl spokojen s fotografiemi, které obdržel a matce odepsal, že žádnou finanční hotovost nepošle. Matka si již na snadný finanční přivýdělek za fotografie navykla. Své dcery opět nafotila nahé, ale reakce dosud štědrého sběratele fotografií byly obdobně odmítající. Finanční situace matky se měla údajně kriticky zhoršit. Z tohoto důvodu přišel i zlom v přístupu matky, respektive, co všechno je matka ochotna s dcerami nadále nafotit. Instrukce v emailu jsou striktní a jasné. Úplná nahota děvčátek je již samozřejmostí, přibyly navíc konkrétní podrobné instrukce. Jednalo se o upřesnění polohy obou dětských těl, kde má být hlava, kde ruka a podobně. Matka se vnitřně ospravedlňuje sama před sebou v duchu svých slov: „a co, jindy po sobě sestry také lezou“. Za focení slibovala dcerám různé dárečky. Příjemce byl spokojen, což trvalo pouze po nějakou dobu. Následoval další útlum finančních prostředků za fotografie a požadavky na vše okolo dívek se stále zvyšovaly. Matka fotografovala a odesílala fotografie dle požadavků, ale opakovala se situace, kdy nebylo vše v pořádku. Následoval návrh

kupujícího, že si dívky přijede vlastnoručně zrežírovat a nafotit sám. Až v tomto okamžiku se něco v matce pohnulo a s návštěvou u nich doma nesouhlasila. Pan X se jeví fotografiemi již tak posedlý, že se jeho tlak na matku stupňoval. Matka se nakonec pod velkým psychickým nátlakem pana X raději, z důvodu obavy, dobrovolně přiznala na policii. Při následném vyšetřování vyšlo najevo, že i pan X fotografie šířil na placené weby v zahraničí a touto činností si měl vydělat přibližně jeden milion korun. Při domovní prohlídce bytu pana X bylo nalezeno dostatečné množství usvědčujícího materiálu s velkým časovým rozestupem. Tento dřívější, především fotografický materiál, měl dle svých slov v průběhu výslechu pan X jen pro vlastní potřebu. Některé nalezené fotografie nahých dětí z prostředí koupališť a od moře byly i několik desítek let staré.

Vyhodnocení případové studie

1. Oblast - Důvod odhalení této trestné činnosti

V prvním z uvedených případů nevedlo k odhalení, i přes značnou rozsáhlost, oznámení kohokoliv, kdo byl s případem jakýmkoli způsobem spjatý. Oznámení neučinil ani nikdo z rodičů dětí, kteří za fotografie svých dětí inkasovali nemalé finanční částky. Možná právě proto přehlíželi jasné signály k tomu, že se děje něco nezákonného. Pokud by se kdokoliv z nich alespoň zajímal o to, jak focení probíhalo a co měly jejich děti při focení na sobě, bylo by zneužívání zřejmě odhaleno dříve. Skupinu se podařilo Policii České republiky odhalit právě pečlivým monitoringem závadových stránek s dětskou pornografií. V celkovém součtu uvedených případů se jednalo o počet sedmdesáti zneužitých dětí v prvním případě a o dvě děti v případě druhém. Při úvaze, i kdyby mělo každé ze zneužitých dětí z prvního případu pouze jednoho rodiče, jedná se o více než sedm desítek dospělých, kteří mohli zasáhnout a neučinili tak. Je až nepochopitelné, že informace o tom v jakých oděvech, nebo i bez nich k focení docházelo, nebyla zřejmě žádnou z dětských obětí sdělena nějakému kamarádovi, nebo kamarádce ze školy či blízkého okolí obětí. V takovém případě by se dalo předpokládat, že ti by informaci předali například svým rodičům, kteří by tak mohli na případ upozornit. Je to zarážející skutečnost. Druhý případ je jiný v tom, že oznámení učinila matka sama na sebe, protože začínala pociťovat strach hlavně o svojí osobu. Důvody odhalení u těchto dvou nastíněných případů jsou tedy odlišné.

2. Oblast - Motivy pachatelů / účastníků / obětí při páchání této trestné činnosti

Motiv pachatelů byl v obou případech obdobný, ale ne úplně totožný. V prvním případě šlo o organizovanou skupinu, která od začátku chtěla dětskou pornografii využít za účelem zisku, tedy pouze majetkového obohacení. V druhém případě šlo o postupné prohloubení deviace pedofilie, kde finanční prospěch byl až vedlejším produktem. Vývoj osobnosti pachatele zde postupovala od shromažďování fotografií v minulosti, až ke snímkům s přesným určením rozložení dětských těl na nich zachycených. V tomto případě šlo ze začátku o shromažďování pro vlastní potřebu pachatele. Následoval ale prodej získaných pornografických materiálů, kdy pachatel využil situace poptávky na trhu a začal prodávat tento materiál dalším zájemcům. Motiv účastníků je jednoznačný a shodný na obou stranách a to zlepšení finanční situace. Motivy dětských obětí se nedají jednoznačně určit, ze závěrů provedených psychologických šetření vyplynulo, že v převážné většině šlo o absolutní důvěru v dospělé autority s ujištěním, že je vše v pořádku, je to přeci jen fotografování.

3. Oblast - Konečný dopad na pachatele / účastníky / oběti

Konečný dopad na pachatele prvního případu je na hlavní účastníky minimální. Při skutečnosti, že dva z pachatelů byli již za obdobný čin potrestáni v minulosti, jde o recidivu bez poučení z předchozího uloženého trestu za obdobnou činnost. Hlavní aktér pan R vše stále považuje za umělecké fotografování a snaží se obvinit soudy z prosazování zákonů, které jsou uplatňovány, dle jeho tvrzení, za oceánem. Ve druhém případě hlavní pachatel po odhalení spatřoval svojí chybu pouze v tom, že na matku dětí moc tlačil. Kdyby nechtěl fotografie dětí pořídit sám, nemuselo se vlastně nic stát. Dopad na účastníky, myšleno rodiče dětí obou případů, je také minimální. Nikdo z rodičů nebyl soudem vůbec potrestán, i když na jejich spoluvinu v prvním případě několikrát upozorňoval hlavní organizátor pan R. Dopad na samotné dětské oběti je velmi individuální. V uvedených případech se jednalo o poškozené v rozpětí věkové hranice od sedmi až do sedmnácti let. Některé oběti byly následně v péči psychologů, ale úplný dopad na následný vývoj dětské psychiky u obětí zjistit nelze.

4.3 Vyhodnocení možností prevence

Ještě před tím, než budou zhodnoceny možnosti prevence a to jak z technické, právní i ekonomické stránky, je důležité si uvědomit, co je hlavní podstatou toho, že se děti stávají terčem útoků prostřednictvím internetu. Jedna stránka problému je ta, že děti jsou důvěřivé a snadno zranitelné. Podstatná chyba je ale spatřována především v komunikaci. Tím je

myšlena komunikace s jejich nejbližšími a to s rodiči, nebo s těmi, kdo děti vychovává a s kým žijí. Kdyby totiž dospělí měli přehled, jaké stránky děti na internetu navštěvují, nebyla by selekce závadových stránek, ani jejich obsah takový problém. Už jen to, kdy dospělý má přehled s kým je dítě na internetu v kontaktu, je velkým bonusem. Jde hlavně o vzájemnou důvěru mezi dítětem a rodičem, respektive vychovávajícím dospělým. To je možná 90 procent prevence před kyberkriminalitou páchanou na dětech v českém i světovém měřítku.

4.3.1 Technické možnosti prevence

Technické možnosti jsou dvojího druhu, jednou možností prevence je technické zabezpečení vstupu na internet a druhým je technický pohled na komunikaci, jako takovou. Právě v oblasti možností skrývání pachatelů nastal před několika lety zlom. Proto je velice důležité, aby tuto problematiku odhalovali a zkoumali lidé, kteří budou mít trpělivost a někdy se nad možností utajení identity pachatele zamýšleli právě, jako pachatel. Vzorovým příkladem je úvodní fotografie k jakémukoliv účtu s doplňujícím označením NICK[135]. To, že pachatelé jen prohazují písmena ve svém profilu je nejjednodušší možnost. Nějakou dobu ale trvalo, než specialisté na odhalování kybernetických trestných činů přišli na to, že pouhé zrcadlové otočení fotografie k účtu zmate internetové vyhledavače tak, že si zrcadlovou fotku nepřiřadí k její obrácené kopii. Pachatelé tak využívali možnosti stažení profilového obrázku neznámého člověka. Tento obrázek následně jen zrcadlově otočili. Jednoduché, ale technicky dobře provedené.

Z technických možností obrany před kyberkriminalitou je nutná změna způsobu přihlašování na internet. Jako jedna z možných variant by přicházela v úvahu obdoba již zavedeného propojení mobilní aplikace v telefonu s počítačovým připojením k síti. Některé státy v rámci bezpečnosti postupně ruší telefonní dobíjecí karty, které nejsou nikde a na nikoho registrovány. V rámci bezpečnostních opatření jde o dobrý záměr.

Snahu o zrušení anonymních dobíjecích telefonních karet měla Policie České republiky již v roce 2010 a dobře věděla proč. Evropská komise o tomto kroku jednala v roce 2016 v Bruselu. Bohužel, žádné konečné stanovisko ke zrušení anonymních SIM karet nebylo vydáno. Z toho důvodu se například Maďarsko rozhodlo samo a učinilo kroky ke zrušení těchto karet v rámci svého státu. V České republice ve stejném roce byla myšlenka

[135] Nick - zkrácená verze anglického slova "nickname", v překladu znamená "přezdívka". Tento pojem často označuje uživatelské jméno (neboli username), pod kterým uživatel vystupuje například na chatu či v diskusních fórech, Dostupné z : https://it-slovnik.cz/pojem/nick

prezentována stranou STAN[136], ale hnutí PIRÁTI[137] bylo razantně proti tomuto návrhu a tak se o zrušení anonymních SIM karet do mobilních telefonů ani dále na vládní úrovni nejednalo. Důvod, jakou hrozbu představuje anonymní mobilní číslo, si uvědomila vláda v Pákistánu a tak v roce 2015 přistoupila k razantním krokům. Každý občan, který chtěl používat služby místních mobilních operátorů, se musel ke svému operátorovi dostavit a k jeho telefonnímu číslu byl přiřazen i jeho odebraný otisk prstu. Tento důvod byl učiněn především kvůli terorismu, ale ve své podstatě by fungoval i na kyberkriminalitu, jako takovou, právě ve spojení přenosového média a identifikace osoby. V případě technické bezpečnosti, by každé přenosové zařízení bylo v systému spojené s konkrétní osobou, zabránilo by se tak odeslání mnoha anonymů a jiných hrozeb. Za předpokladu propojení a svázání zařízení s kyberprostorem, je velká šance eliminace anonymního sdílení obsahu v těchto, nebo ve vzdálených zařízeních. Před připojením k síti by byl uživatel vyzván, aby potvrdil zaslaný kód na jeho zařízení a pod tímto kódem by se pak k internetové síti připojil. Jako doplněk by bylo možné toto přihlášení doplnit fotografií osoby z web kamery (fotoaparátu), kterou je dnes vybavena většina komunikačních médií. Tyto technologie postupují stále kupředu a právě skenování obličeje je jedna z poměrně přesných možností identifikace osob. Od poloviny roku 2018 se například rozběhl systém obličejové identifikace na našem největším letišti Václava Havla.[138] Díky tomuto systému se podařilo odhalit již několik desítek mezinárodně hledaných osob. Čím více ochranných prvků bude zapotřebí k identifikaci osoby při připojení k internetu, tím bude eliminace pachatelů větší.

Další způsob, který by bylo možné použít, je například základní skenování sítnice oka[139] přes webkameru, nebo například čtečka otisků prstů. Tyto čtečky jsou v současné době také součástí většiny komunikačních médií střední třídy.

Nejefektivnější je ale vzájemná provázanost všech těchto možností. Shromáždit konkrétní mobilní telefon s číslem účastníka pro zpětné ověření vstupu k internetu, podrobit se skenu sítnice přes web kameru, nebo fotoaparát v mobilu, načíst správný otisk prstu a mít svůj jedinečný přihlašovací kód a zvolené přístupové jméno NICK, by už nebylo tak snadné zfalšovat, nebo zkopírovat.

[136] STAN - politická strana –Starostové a nezávislí, Dostupné z: https://www.starostove-nezavisli.cz/
[137] PIRÁTI - politická strana, Dostupné z: https://www.pirati.cz/
[138] Mezinárodní letiště v ČR, Dostupné z: https://www.prg.aero
[139] Biometrický identifikační systém pro snímání očních duhovek, Dostupné z: http://www.biometricke-ctecky.cz/produkty/skenery-oka/

4.3.2 Právní možnosti prevence

Právní stránka je v této problematice důležitá. Jak již bylo uvedeno, naše zákony neznají ani přesnou definici slova PORNOGRAFIE. Její výklad je složitější, protože pod tímto slovem si každý z nás představuje možná trochu něco jiného. Základem po právní stránce je spíše otázka – Proč se na tvorbě zákonů více nepodílejí lidé, kteří s nimi přicházejí denně do styku a musejí v rámci svého zaměstnání vycházet i z judikatury. Problém je v ČR především v tom, že chybí adekvátní veřejná diskuse k návrhům zákonů. Kyberkriminalita spojená s jakýmkoli zneužitím dítěte je prostě fatální zásah do dětské sféry. Dětem a dospívajícím bychom měli vytvořit pevné základy pro jejich budoucí život a ne je v jejich útlém věku zranit po psychické stránce tak, že se naruší jejich vnímání okolního světa s absolutní negací důvěry v dospělé. Z toho důvodu je jasná přítomnost odborníků z oboru při tvorbě a úpravě zákonů nezbytná. Zároveň by měl být lépe po právní stránce ošetřen postih těch, kteří úmyslně nebo z nedbalosti spáchali nebo umožnili spáchání trestných činů zaměřených proti dětem. Naše zákony se postupně vyvíjejí a reagují na nové formy zločinu, ale výše trestů za tyto spáchané činy neodpovídá společenské nebezpečnosti. Kdyby tresty v této oblasti byly vyšší, pachatelé by si možná rozmysleli, jestli jim stojí za to vůbec tyto aktivity uskutečňovat a rozvíjet. Při myšlence na trest odnětí svobody v trvání 15 let při spáchání trestných činů spojených s dětskou pornografií a zneužitím dítěte, by si možná osmdesát procent potencionálních pachatelů rozmyslelo svůj původní záměr začít páchat tuto trestnou činnost. V současné době hrozí dle platného právního řádu ČR pět let vězení pachateli, který zneužije, nebo zláká dítě k pornografickým aktivitám, ze kterých vznikne pornografické dílo. Za výrobu a nabízení pornografie s dětskou tématikou hrozí pachateli tři roky odnětí svobody a při přechovávání dětské pornografie hrozí pachateli trestní sazba dva roky. To jsou ale všechno horní hranice trestu a ne vždy soud přistoupí k udělení právě této nejvyšší možné sazby. Trestní zákoník by se měl změnit i v ohledu na promíjení části trestů odsouzeným. To, že se ve výkonu trestu chová odsouzený vzorně, je sice hezké, ale skutečnost, že svým hrubým jednáním narušil sexuální vývoj a psychiku oběti, by měla být nepřípustná možnost jeho podmínečného propuštění. Zákon by se měl změnit také v udělování trestů a to ne pouze posuzovat, který z výčtu zločinů pachatele byl nejtěžší a podle něj zvolit trestní sazbu. Trestní sazby za všechny spáchané skutky by se měly pachateli sečítat a trest by pak zahrnoval celkovou souhrnnou dobu, tak jak se například právo praktikuje jinde (např. v USA). Celkově jsou postihy pachatelů v ČR velice mírné a tak často dochází u pachatelů k recidivě.

4.3.3 Ekonomické možnosti prevence

Z ekonomického hlediska by prevence nebyla až tak nákladná, jak se může zdát. Při technických možnostech, které byly uvedeny v části práce 4.3.1 spojených se vstupem do kyberprostoru, až po identifikaci uživatele komunikačního média. Většina těchto médií již možnosti ověření svého uživatel umožňuje. Maximálně by se navýšil počet centrálních úložišť, kde by tato data byla ukládána. Změna v ukládání dat z komunikačních přenosových médií bude do budoucna ale stejně nutná. Brzo začneme globálně využívat mobilní sítě páté generace 5G.[140] Jen asijští operátoři chtějí v období let mezi roky 2018 až 2025 investovat do této nové mobilní sítě v přepočtu 8,3 bilionu Kč. Takže investice do úložišť je zanedbatelná a ve své podstatě už samotná síť bude kvůli mnohanásobnému zrychlení všech operací potřebovat navýšení. Ekonomické zatížení států, nebo normálního občana by nemělo být překážkou. Více než do technických možností prevence je potřebné investovat do prevence mediální. V současné době byl do kin v ČR uveden filmový dokument s názvem V SÍTI,[141] který pojednává právě o problematice trestné činnosti v kyberprostoru a rafinovanosti pachatelů. Právě tento snímek je pro laickou veřejnost skvěle zpracován a hrozby z kyberprostoru jasně definuje a konkretizuje. Už jen názor Vrchní státní zástupkyně paní Lenky Bradáčové po zhlédnutí snímku je odrazem kvality tohoto dokumentu. Bradáčová pro TV Seznam v přímém rozhovoru uvedla *„Policie by měla posílit oddělení kyberkriminality a aktivního vyhledávání této trestné činnosti v prostoru internetu.“* [142]Zastávám názor, že využití tohoto díla, v oblasti plošné prevence před kyberkriminalitou by byl velký přínos pro větší gramotnost v této oblasti chápání kyberprostoru pro běžné uživatele a širokou veřejnost.

4.4 Závěry praktické části

V úvodu této části práce byla vyhodnocena statistická analýza komerčních trestných činů- Komerční forma sexuálního zneužívání v závislosti (§ 187/2), Komerční forma sexuálního zneužívání v závislosti (§ 187/1,3,4), Ostatní mravnostní TČ (§ 190, § 192 - § 193), jak je v období mezi roky 2016 až 2019 zaznamenávala Policie České republiky, konkrétně Odbor gescí a statistik Policejního prezidia ČR. Statisticky (viz. kapitola 4.1.1) bylo zjištěno, že ve sledovaném období byl celkový průměr 13,25 skutků za rok na celém území ČR. V oblastech

[140] Nová mobilní síť páté generace – nástupce současné sítě 4G LTE
[141] Dokument - V síti, [online] [citace 4.3.2020]. Dostupné z: https://www.vsitifilm.cz/
[142] TV Seznam – Bradáčová o filmu V síti, [online] [citace 4.3.2020]. Dostupné z: https://www.seznamzpravy.cz/clanek/bradacova-o-filmu-v-siti-predatori-nesmi-zustat-bez-postihu-91324

trestné činnosti vedených pod označení PČR TSK čísla 213, 214 a 290 narostl celkový počet trestných činů z 375 na 728 činů. To je nárůst této trestné činnosti ve sledovaných oblastech o 94 %. Byla provedena i analýza těchto skutků spáchaných prostřednictvím internetu, jak je PČR evidovala a zde byl nárůst skutků z počtu 209 na 579 evidovaných skutků. To je nárůst o 185% ve sledovaném období čtyř let, který vypovídá o závažnosti a zejména stoupající tendenci v této oblasti kyberkriminality.

V návaznosti na tyto statistiky byla vyhodnocena i situace v jednotlivých krajích ČR se sledováním šíření pornografie v období mezi roky 2016 až 2019. Bylo zjištěno, že počet těchto evidovaných skutků v rámci Policie České republiky se ve sledovaném období zvýšil z 56 skutků na konečné číslo 99 skutků evidovaných v roce 2019. To je opět skoro 100% nárůst. Dále byly vyhodnoceny problémy při objasňování této trestné činnosti, kdy Policie České republiky využívá všechna dostupná data i ze zahraničních zdrojů v rámci komunikace v kyberprostoru a bylo analyzováno specifické prostředí internetu, ve kterém se pachatelé této trestné činnosti pohybují a to z důvodu možného odhalení. Vyhodnocen byl vliv sociálního prostředí na páchání této trestné činnosti, kdy byla provedena statistická analýza komerčních (Komerční forma sexuálního zneužívání v závislosti - § 187/2, Komerční forma sexuálního zneužívání v závislosti - § 187/1,3,4) a ostatních mravnostních trestných činů (Ostatní mravnostní TČ- § 190, § 192 - § 193), v rámci krajů ČR v porovnání registrovaných a následně objasněných skutků v této části problematiky. V rámci případové studie byly uvedeny dva případy komerčních trestných činů (Komerční forma sexuálního zneužívání v závislosti - § 187/2, Komerční forma sexuálního zneužívání v závislosti - § 187/1,3,4 a Ostatních mravnostních trestných činů - § 190, § 192 - § 193) s vyhodnocením tří oblastí příčin odhalení, motivu i dopadu na účastníky. V oblastech technické, právní a ekonomické byly na danou problematiku kyberkriminality navrženy i případné možnosti řešení prevence. V technické oblasti by měl být kladen větší důraz na zlepšení softwarové možnosti přihlašování do komunikačních médií a také do zajištění kvalitních vyšetřovacích týmů v rámci Policie České republiky. Měla by se celkově zlepšit jejich vybavenost a technická znalost. Z právního pohledu na prevenci kriminality páchané v kyberprostoru je důležitý monitoring vývoje a flexibilní tvorba práva s vyšším důrazem na postih zvlášť společensky nebezpečného jednání. Ekonomické hledisko by běžné uživatele přenosových médií nemělo nijak zásadně postihnout. Ve finanční náročnosti spojené se zaváděním nové mobilní sítě 5G, která bude s internetem propojena, je softwarové i hardwarové řešení identifikace uživatele jen zanedbatelným finančním zatížením celého projektu 5G.

5 Výsledky a diskuze

5.1 Výsledky teoretické části

V teoretické části byl pojem počítačová kriminalita blíže upřesněn (kapitola 3.1), kdy bylo postupováno od zmapování samotných základů, které daly vzniknout globální síti internet. V rámci internetové sítě byly v historické návaznosti popsány první kybernetické činy, které v prvopočátcích neměly za úkol finanční zisk, ale pouze ukázku moci ve spojení s ochromením této sítě, nebo alespoň jejích částí.

Se vznikem kyberprostoru a činností v něm byly uvedeny a blíže upřesněny nové pojmy, které tuto činnost charakterizují a definují toto specifické jednání. S rozvojem globální sítě a začátkem kyberkriminality, byla provedena postupná analýza právního vývoje (kapitola 3.2), jak na začátek kyberzločinu reagovala světová organizace OSN, Rada Evropy, Evropská unie a ČR.

Dále je zpracován i vývoj práva v ČR, který jasně odráží zásadnost této problematiky, jak byla celosvětově vnímána, jako jasná hrozba. Postupný vývoj v otázce trestního zákoníku ČR (kapitola 3.2.4) byl zpracován od prvních ustanovení, které bylo možné použít pro stíhání pachatelů v začátcích kyberkriminality, až po zavedení nových paragrafových znění a novelizací, které již zahrnovaly skutkovou podstatu trestných činů v návaznosti na vývoj kyberkriminality. Zpracování tohoto vývoje v oblasti práva bylo provedeno v časovém sledu, v jakém byly jednotlivé paragrafy do trestního zákoníku doplňovány a jak jednotlivé paragrafy podrobněji konkretizovaly skutkové podstaty trestných činů páchaných v kyberprostoru. Důsledkem členění kybernetických trestných činů byly do trestního zákoníku zaneseny i trestné činy spadající do oblasti mravnostních trestných činů, které umožňovaly stíhat pachatele těchto činů páchaných proti dětem včetně různých forem účastenství (viz. tabulka č.1 vývoj TZ v období let 1991-2019, kapitola 3.2.4). Přesto stále není v TZ uvedena jasná specifikace pojmů, jako je PORNOGRAFIE a DĚTSKÁ PORNOGRAFIE. Z toho důvodu by se mělo začít jejich jasnou formulací a změnou současného zákona (kapitola 3.3.1).

Pak by nedocházelo k situacím, kdy při soudních procesech nejsou ani odborníci přesně schopni definovat určité pojmy spojené s pornografií a komunikací v souvislosti s kyberprostorem (kapitola 3.3.2). Každý, kdo se pokoušel, alespoň částečně seznámit s formulací virtuální a nebo i samotné pornografie zjistil, že není v trestním zákoníku správně upravena. Vždyť i soudní znalci z oboru sexuologie na tento problém již delší dobu

poukazují. Nutnost změny nebude ale jen v této oblasti. Za změnu stojí i formulování hranice věku dítěte ve vztahu k dětské pornografii. Od patnácti let můžete vést sexuální život, ale ve chvíli, kdy se u této sexuální aktivity nafilmujete, nebo nafotíte, tak je to dětská pornografie. Vždyť to vůbec nedává smysl. Příklad by jsme si, jako země, mohli vzít od našich sousedů na západě ve Spolkové republice Německo. Naše zákony považují za dětskou pornografii jakýkoliv pornografický materiál s osobou mladší 18 let. Německé zákony za dětskou pornografii považují jakýkoliv pornografický materiál, na kterém je zachycena osoba mladší 14 let. Tato hranice je ve Spolkové republice stanovena proto, že sexuálním životem je zde možné žít již od věku 14 let. Zadokumentovaný styk na obrazový nebo jiný materiál dospělé osoby s osobou v rozmezí 14 až 18 let je zde úřady považován za pornografii s mladistvými. Přechovávání pornografie, kde jsou zachyceny osoby ve věku 14 až 18 let není například v této zemi vůbec trestné. Tím je ale myšleno, pouze za předpokladu, že se ho dopouštějí osoby, které jsou na materiálech zaznamenány.

Vymezením komerčních trestných činů páchaných proti dětem v kyberprotstoru a následnou analýzou problémů při jejich objasňování v rámci orgánů činných v trestním řízení byla zakončena teoretická část.

5.2 Výsledky praktické části

Praktická část práce se zabývala statistickou analýzou s využitím databáze Policie České republiky (kapitola 4.1). Odbor gescí a statistik vedený pod Policejním prezidiem byl největším zdrojem informací pro realizaci statistik v období let 2016 až 2019. Statistická analýza a závěry, které z ní vyplynuly, byly provedeny v oblasti komerčních trestných činů a činů mravnostních, jak je Policie České republiky eviduje a které jsou svojí problematikou dětské pornografie navzájem spojeny. Z této analýzy vyplynulo, že ve sledovaném období mezi roky 2016 až 2019 se počet takto spáchaných trestných činů prostřednictvím internetu zvýšil o 185% (kapitola 4.1.1). Statistika této trestné činnosti v kyberprostoru byla zpracována v daném období a to analýzou počtu jednotlivých skutků v krajích ČR. Byly vyhodnoceny počty registrovaných a objasněných trestných činů a vyhodnocena průměrná objasněnost těchto trestných činů. Tato objasněnost se ve stejném sledovaném období 2016 až 2019 pohybuje okolo 2/3 na hranici 65% z celkového počtu registrovaných skutků (kapitola 4.1.3). Zpracováním konkrétních údajů byly kraje ČR seřazeny podle jejich rizikovosti. Ze všech těchto hodnot byl vytvořen i procentuální nárůst činů v daném období roků 2016 až 2019 (kapitola 4.1.1).

Příčiny při objasňování kybernetických trestných činů zaměřených proti dětem byly vyhodnoceny a byl z nich stanoven závěr, kdy bylo zjištěno, že hlavním důvodem je přesun této kyberkriminality do oblasti Deep Web (Hluboký, nebo neviditelný web) a Dark Web (Temný web), kde jsou pachatelé díky anonymitě přístupu k těmto webům více chráněni před jejich odhalením (kapitola 4.1.2).

Práce zkoumala i vliv sociálního prostředí v počtu registrovaných trestných činů této problematiky (kapitola 4.1.3). Údaje pro zpracování byly čerpány opět z Odboru gescí a statistik Policejního prezidia. Při zpracování všech dostupných údajů bylo zjištěno, že není možné vliv sociálního prostředí jednoznačně vyhodnotit z důvodu nedostatku informací, které k případům Policie České republiky eviduje. Zásadní problém je v rozdílnosti informací, které poškození, ale i pachatelé uvádějí jako adresy místa trvalého bydliště a skutečným místem jejich pobytu v ČR.

Z případové studie byly vyhodnoceny tři oblasti, které se zaměřily na důvody odhalení této trestné činnosti, motivy pachatelů a zúčastněných osob včetně konečného dopadu na oběti i pachatele (kapitola 4.2).

Byla zpracována možnost prevence v boji proti kyberzločinu v této oblasti a to z pohledu ekonomického, právního a technického. Ze závěrů vyplývá, že v oblasti práva bude nutnost definování základních pojmů, jako je například PORNOGRAFIE, ale také bude potřebná včasná reakce na nové změny v oblasti páchání této závažné trestné činnosti v kyberprostoru. Ekonomická společně s technickou otázkou prevence v boji s kyberkriminalitou by měla být přirozenou součástí celosvětového vývoje v oblasti IT (kapitola 4.3).

Za zmínku při praktických řešeních obrany před touto kyberkriminalitou stojí aktivita skupiny ANONYMUS,[143] která v roce 2017 zablokovala na Dark Webu přes 2.000 skrytých stránek, kde byly uloženy videosoubory a nebo databáze s dětskou pornografií. Při tomto množství to bylo přibližně 20 procent stránek Dark Webu. Zásadní postoj k této možnosti skrytého internetu se rozhodli prosazovat Spojené arabské emiráty. Tam, když použijete službu VPN[144]- virtuální privátní síť a budete přistiženi, hrozí Vám finanční postih, který začíná částkou 3.000.000,-Kč (v přepočtu z místní měny DIRHAM).

Ze všech dostupných informací této práce je jasné, že obchodování s dětskou pornografií na internetu pokračuje a neustále se počet případů navyšuje. Změna by měla nastat především

[143] Jedna z nejznámějších hackerských skupin známá svým bojem proti dětské pornografii

[144] Virtuální privátní síť, která při komunikaci po připojení účastníků používá pro větší soukromí kódové šifrování

v lepší technické a personální připravenosti ze strany Policie České republiky. Když může nezisková skupina pod názvem Anonymus zablokovat 20 procent stránek na Dark Webu s dětskou pornografií, proč by toto nebylo možné uskutečňovat i nadále. Americká vláda umožnila přístup na temný net z důvodu anonymní komunikace. Když něco děláte, tak víte, jak to funguje a můžete hrozbu eliminovat. Problém je, ale v současné době v tom, že kdyby se tak stalo a začaly by se stránky s dětskou pornografií a jiným nelegálním zbožím a službami blokovat, byl by to signál o monitoringu těchto stránek po celou dobu a nečinném přihlížení za účelem skrýt se v davu. Jako v síti internet, vše je propojené se vším. Obrana ale vždy existuje. Celkové zhodnocení počítačové kriminality v počtu registrovaných a objasněných komerčních trestných činů páchaných proti dětem nebude úplně objektivní. Čísla statistik, jak je registruje a uvádí Policie České republiky jako evidované a následně objasněné jsou jen špičkou pomyslného ledovce. Většina této trestné činnosti se přesunula do částí internetu, o kterých tato práce také pojednává (kapitola 4.1.2). Právě tam se uskutečňují obchody s dětskou pornografií a je zde páchána další závažná trestná činnost. Pachatelé se z vlastních chyb poučili a pouze se přizpůsobili. Ve skryté části internetu je v současné době dle odhadů páchano 90 procent trestné činnosti, která je skryta. Není to jen problém naší policie. Je to problém celosvětový. Bude nutné v rámci monitoringu a odhalování trestné činnosti právě v této skryté části internetu přijmout a vyškolit mnohem více odborníků. Není to jednoduchý úkol, ale upřímně, všichni kdo v kyberprostoru bojují se zločinem, jsou minimálně o jeden krok pozadu za pachateli. Kyberzločin se přesunul do neprozkoumané části internetu a policie měla i tak dost práce s odhalováním kyberkriminality v běžné rovině webových prohlížečů internetu.

6 Závěr

Práce se na začátku zabývala samotným pojmem počítačová kriminalita a specifikovala její různé formy (kapitola 3.1). Zaměřila se a zmapovala právní vývoj v této oblasti, jak celosvětově, tak v Evropském měřítku a podrobněji zanalyzovala tento vývoj také v České republice (kapitola 3.2.2 až 3.2.4). Zpracovala dělení druhů kyberkriminality a blíže se věnovala kybernetickým komerčním trestným činům páchaných proti dětem, jak je v ČR zpracovává Policie České republiky (kapitola 3.3.1). Práce zároveň poukázala na problémy při objasňování těchto kybernetickým trestným činům. Byly zanalyzovány registrované a objasněné trestné činy páchané proti dětem v letech 2016 – 2019 a to vyhodnocením statistik ze zdrojů Policie České republiky. Z analýzy vyplynulo, že se ve sledovaném období zvýšil počet takto spáchaných trestných činů prostřednictvím internetu o 185% (kapitola 4.1.1). Současně bylo i zanalyzováno šíření pornografie na celém území ČR v rámci jednotlivých krajů. Zde bylo zjištěno, že nejhorší situace v této oblasti je v Ústeckém a Královohradeckém kraji, kdy hl. m. Praha za těmito kraji jen lehce zaostává. Byly zkoumány i příčiny neobjasněných komerčních trestných činů zaměřených proti dětem (kapitola 4.1.2). Z tohoto výzkumu je patrné, že se právě trestná činnost přesunula do oblasti Deep Web (Hluboký, nebo neviditelný web) a Dark Web (Temný web), kde díky anonymitě přístupu k webům zůstávají pachatelé dále skryti. Součástí zpracování byla i snaha o zjištění vlivu sociálního prostředí na páchání této trestné činnosti, kdy bylo zjištěno, že není možné tento vliv jednoznačně vyhodnotit z dostupných informací, jak je Policie České republiky eviduje (kapitola 4.1.3). Do práce je také začleněna Případová studie, ze které byly vyhodnoceny tři oblasti zkoumání těchto činů (kapitola 4.2). V oblasti prevence se práce zaměřila na vyhodnocení technických, právních a ekonomických možností spojených s touto problematikou (kapitola 4.3), kdy v právní oblasti bude nutnost definování základních pojmů, jako je PORNOGRAFIE a včasná reakce na změny v druhu páchání této závažné trestné činnosti. Technická a ekonomická otázka by měla být přirozenou součástí celosvětového vývoje v oblasti IT.

Na závěr si musíme uvědomit, že kyberkriminalita prorůstá celou společností. Vždy mezi námi budou lidé, kteří s určitým druhem omezení v návaznosti na bezpečnost před kyberkriminalitou nebudou souhlasit. Budou to považovat za omezení jejich osobní svobody. Každá mince má dvě strany a je jen na nás, na jakou stranu se budeme chtít přiklonit. Hrozba kyberkriminality je v celosvětovém hledisku obrovská. Můžeme srovnávat statistiky a tvořit a novelizovat paragrafová znění, ale jedno je jisté, čísla, která jsou zveřejňována, nejsou úplně

objektivní. Počet nahlášených případů se v drtivé většině neshoduje se skutečností. Většina z nás se již s nějakou formou kyberkriminality setkala, ale nenahlásila ji.

Čas ubíhá všem stejně a bude záležet jen na nás, jak ho v oblasti prevence a boje s kyberzločinem využijeme.

7 Seznam použitých zdrojů

7.1 Knižní zdroje

Jirásek Petr, Novák Luděk, Požár Josef – *Výkladový slovník kybernetické bezpečnosti*, Policejní akademie ČR 2015, ISBN 978-80-7251-397-0

Pavel Satrapa - *Internetový protokol IPV6 čtvrté vydání* – Praha 2019 ISBN 978-80-88168-46-1

Završil Aleš – *Kyberkriminalita – Právní monografie* ,ČR 2017, ISBN 978-80-7552-758-2

Porada Viktor, Konrád Zdeněk - *Metodika vyšetřování počítačové kriminality. 1. vydání*. Praha 1998: Vydavatelství PA ČR ISBN 80-85981-75-0

Jírovský Václav - *Kybernetická kriminalita*, Praha 2007, ISBN 978-80-247-1561-2

Matějka Michal, *Počítačová kriminalita*, Praha 2002: Computer Press, ISBN 807-22-6419-2

Kolouch Jan, *CyberCrime* ,Edice CZ.NIC 2016, ISBN 978-80-881-6815-7

Gřivna, T., Polčák, R., *Kyberkriminalita a právo*, první vydání, nakladatelství Auditorium, Praha 2008 ISBN 978-80-903786-74

Polčák, Radim. *Internet a proměny práva*. Praha: Auditorium, 2012, Téma (Auditorium). ISBN 978-80-87284-22-3

Látal, I., Počítačová (informační) *kriminalita a úloha policisty při jejím* řešení -materiál z přílohy časopisu POLICISTA č. 3/1998

Novotný Oto, Dolenský Adolf, Jelínek Jiří aj. -*Trestní právo hmotné, obecná část*, 4. přeprac. vyd., Praha 2003, ASPI Publishing, s.r.o., ISBN 80-86395-73-1

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

Smejkal Vladimír- *Kybernetická kriminalita*., Plzeň 2015, ISBN 978-80-7380-501-2

Jelínek Jiří a kol. , *Trestní právo hmotné*, 2016, ISBN 978-80-7502-120-5

Jelínek Jiří, Praha 2016, *Vyjádření k žádosti Národního ústavu duševního zdraví* - posouzení *problematiky výroby stimulů pro základní výzkum pedofilních preferencí*

Hendrych a kolektiv, *Právnický slovník*, Praha 209, C.H. BECK, ISBN 978-80-7400-059-1

Fenykl Jaroslav, *Trestní zákoník a trestní řád*, Linde Praha 2010, ISBN 978-80-7201-802-4

Jelínek Jiří a kol.- *O novém trestním zákoníku* : Sborník příspěvků z mezinárodní konference Olomoucké právnické dny, květen 2009. 1. vydání. Olomouc: Leges, 2009, ISBN 978-80-87212-21-9

Porada Viktor, Roman Rak -*Teorie digitálních stop a její aplikace v kriminalistice a forenzních vědách* -Karlovarská právní revue 2006, Dostupné z: http://mail.vskv.cz/download/KPR/archiv/2006/kpr4_2006.pdf

Smejkal Vladimír; Sokol Tomáš; Vlček Martin - *Počítačové právo*. 1. vyd. Praha: C.H. Beck 1995, ISBN 80-7179-009-5

Porada Viktor; Konrád Zdeněk - *Metodika vyšetřování počítačové kriminality* - 1. vyd.Praha1998 , Policejní akademie České republiky, ISBN 80-85981-75-0

Porada Viktor; Straus Jiří - *Kriminalistika: výzkum, pokroky, perspektivy*- Plzeň 2013 - Vydavatelství Čeněk, ISBN: 978-80-7380-547-0

Maisner Martin, *Základy softwarového práva*. 1. vyd. Praha: Wolters Kluwer ČR, 2011 ISBN 978-80-7357-638-7

7.2 Internetové zdroje

Policie České republiky –Počítačová kriminalita [online] [citace 20.2.2020]. dostupné z: https://www.policie.cz/clanek/pomoc-obetem-tc-pocitacova-kriminalita.aspx

NATOAKTUAL [online] [citace20.2.2020] dostupné z: https://www.natoaktual.cz/rusko-gruzinska-valka-deset-lekci-pro-estonsko-frv-/na_analyzy.aspx

CESES - Kyberhrozby a kyberterorismus – kybernetické války [online] [citace20.2.2020]. Dostupné z: https://ceses.cuni.cz/CESES-70-version1-Kyber.pdf

Policie České republiky – Statistika kyberkriminality [online] [citace20.2.2020]. Dostupné z: https://www.policie.cz/clanek/statistika-kyberkriminality.aspx

Policie České republiky [online] [citace20.2.2020]. Dostupné z: https://www.policie.cz/clanek/o-nas-policie-ceske-republiky-policie-ceske-republiky.aspx

Matusziński, Dariusz. 2018 - Co je kryptoměna a jak funguje. In: Český magazín o kryptoměnách - Kryptomagazin.cz [online]. [cit. 20.2.2020]. Dostupné z: https://kryptomagazin.cz/co-je-kryptomena

MANAGEMENT MANIA- ICT [online] [citace 20.2.2020]. Dostupné z: https://managementmania.com/cs/informacni-a-komunikacni-technologie

Ministerstvo vnitra ČR - Analýza současného stavu a trendů vývoje trestné činnosti na úseku informačních technologií a Internetu včetně návrhu řešení, [online] [citace 20.2.2020]. Dostupné z: http://www.mvcr.cz/soubor/informacni-pdf.aspx

Mezinárodní letiště v ČR, Dostupné z: https://www.prg.aero

NBÚ – Národní bezpečnostní úřad - informace, Dostupné z: https://www.nbu.cz

EUR-LEX 52007DC02-67 -KOMISE EVROPSKÝCH SPOLEČENSTVÍ,- [online] [citace 20.2.2020]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52007DC0267&from=EN

Manuál OSN pro prevenci a kontrolu počítačového zločinu. [online] OSN © 2001 [cit. 20.2.2020] Dostupné z: http://216.55.97.163/wpcontent/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Guide.pdf

Rada Evropy [cit.20.2.2020]. Dostupné z: http://www.radaevropy.cz

Úmluva o počítačové kriminalitě. In: COE [právní informační systém]. Council of Europe Treaty office [online] [cit.20.2.2020]. Dostupné z: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms1

Dodatkový protokol k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů [online] [cit.20.2.2020]. Dostupné z: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804931bf

Úmluva Rady Evropy o ochraně dětí proti sexuálnímu vykořisťování a pohlavnímu zneužívání, 2007 , [online] [cit.20.2.2020]. Dostupné z: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168046e1

Úmluva Rady Evropy 2007, článek 20 bod 4 -Trestné činy tykající se dětské pornografie str. 8 [online]. 2019 Dostupné z: www.psp.cz › sqw › text

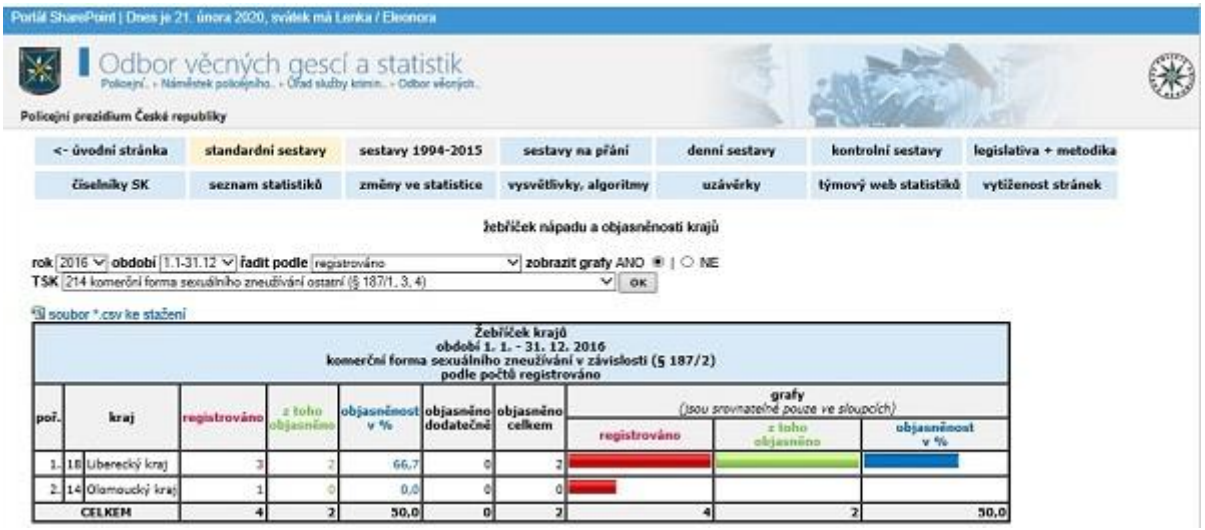
Policie České republiky – Jednotlivé druhy kyberkriminality- [online] [citace 24.2.2020] Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx

Nápad trestné činnosti, Policie České republiky 201-2019, Dostupné z: www.policie.cz/clanek/kyberkriminalita.aspx

Důvodná zpráva k zákoníku č. 40/2009 Sb. [online] [zdroj 24.2.2020] Dostupné z: https://www.vlada.cz/assets/ppov/lrv/ria/databaze/Revize-Zaverecne-zpravy-RIA-k-navrhu-zakona--kterym-se-meni-zakon-o-trestnim-rizeni-soudnim-_trestni-rad_.pdf

8 Přílohy

Obrázek č. 8 Komerční forma sexuálního zneužívání v závislosti (§187/1,3,4) **2016**



Portál SharePoint | Dnes je 21. února 2020, svátek má Lenka / Eleonora

Odbor věcných gescí a statistik

Policejní prezidium České republiky

<- úvodní stránka | standardní sestavy | sestavy 1994-2015 | sestavy na přání | denní sestavy | kontrolní sestavy | legislativa + metodika

číselníky SK | seznam statistik | změny ve statistice | vysvětlivky, algoritmy | uzávěrky | týmový web statistiků | vytíženost stránek

žebříček nápadu a objasněnosti krajů

rok 2016 období 1.1-31.12 řadit podle registrováno zobrazit grafy ANO | NE

TSK 214 komerční forma sexuálního zneužívání ostatní (§ 187/1, 3, 4) OK

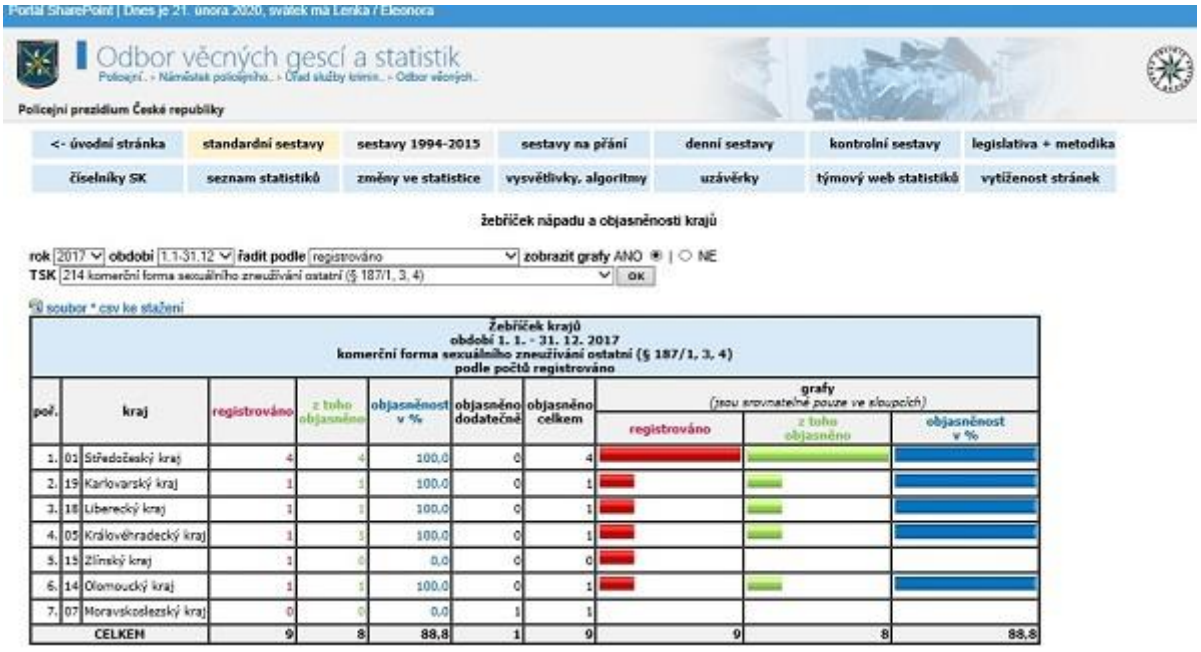
soubor *.csv ke stažení

Žebříček krajů
období 1. 1. - 31. 12. 2016
komerční forma sexuálního zneužívání v závislosti (§ 187/2)
podle počtů registrováno

poř.		kraj	registrováno	z toho objasněno	objasněnost v %	objasněno dodatečně	objasněno celkem	grafy (jsou srovnatelné pouze ve sloupcích) registrováno	z toho objasněno	objasněnost v %
1.	18	Liberecký kraj	3	2	66,7	0	2			
2.	14	Olomoucký kraj	1	0	0,0	0	0			
CELKEM			4	2	50,0	0	2	4	2	50,0

Zdroj: Odbor gescí a statistik PP Policie České republiky

Obrázek č. 9 Komerční forma sexuálního zneužívání v závislosti (§187/1,3,4) **2017**



Portál SharePoint | Dnes je 21. února 2020, svátek má Lenka / Eleonora

Odbor věcných gescí a statistik

Policejní prezidium České republiky

<- úvodní stránka | standardní sestavy | sestavy 1994-2015 | sestavy na přání | denní sestavy | kontrolní sestavy | legislativa + metodika

číselníky SK | seznam statistik | změny ve statistice | vysvětlivky, algoritmy | uzávěrky | týmový web statistiků | vytíženost stránek

žebříček nápadu a objasněnosti krajů

rok 2017 období 1.1-31.12 řadit podle registrováno zobrazit grafy ANO | NE

TSK 214 komerční forma sexuálního zneužívání ostatní (§ 187/1, 3, 4) OK

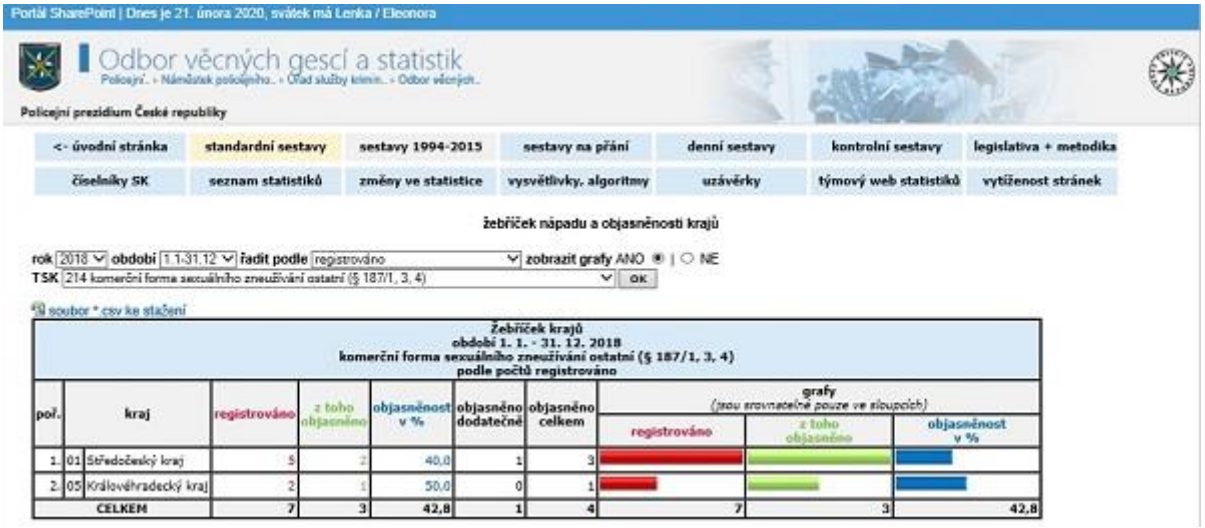
soubor *.csv ke stažení

Žebříček krajů
období 1. 1. - 31. 12. 2017
komerční forma sexuálního zneužívání ostatní (§ 187/1, 3, 4)
podle počtů registrováno

poř.		kraj	registrováno	z toho objasněno	objasněnost v %	objasněno dodatečně	objasněno celkem	grafy (jsou srovnatelné pouze ve sloupcích) registrováno	z toho objasněno	objasněnost v %
1.	01	Středočeský kraj	4	4	100,0	0	4			
2.	19	Karlovarský kraj	1	1	100,0	0	1			
3.	18	Liberecký kraj	1	1	100,0	0	1			
4.	05	Královéhradecký kraj	1	1	100,0	0	1			
5.	15	Zlínský kraj	1	0	0,0	0	0			
6.	14	Olomoucký kraj	1	1	100,0	0	1			
7.	07	Moravskoslezský kraj	0	0	0,0	1	1			
CELKEM			9	8	88,8	1	9	9	8	88,8

Zdroj: Odbor gescí a statistik PP Policie České republik

Obrázek č. 10 Komerční forma sexuálního zneužívání v závislosti (§187/1,3,4) **2018**

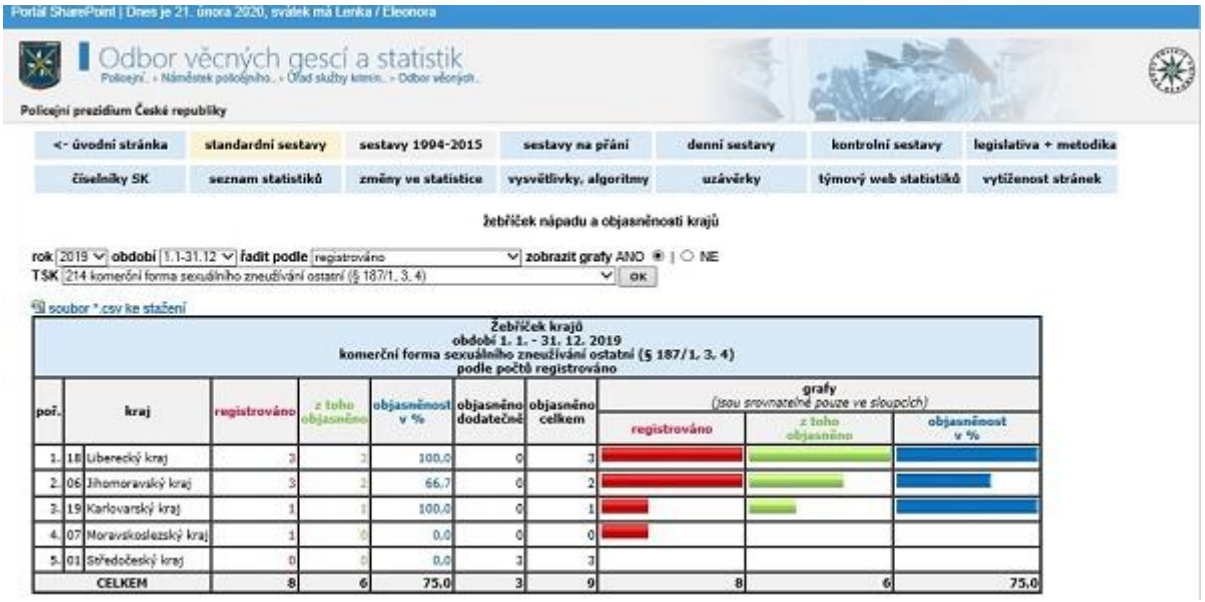


Žebříček krajů
období 1. 1. - 31. 12. 2018
komerční forma sexuálního zneužívání ostatní (§ 187/1, 3, 4)
podle počtů registrováno

poř.		kraj	registrováno	z toho objasněno	objasněnost v %	objasněno dodatečně	objasněno celkem	grafy (jsou srovnatelné pouze ve sloupcích) registrováno	z toho objasněno	objasněnost v %
1.	01	Středočeský kraj	5	2	40,0	1	3			
2.	05	Královéhradecký kraj	2	1	50,0	0	1			
CELKEM			7	3	42,8	1	4	7	3	42,8

Zdroj: Odbor gescí a statistik PP Policie České republiky

Obrázek č. 11 Komerční forma sexuálního zneužívání v závislosti (§187/1,3,4) **2019**

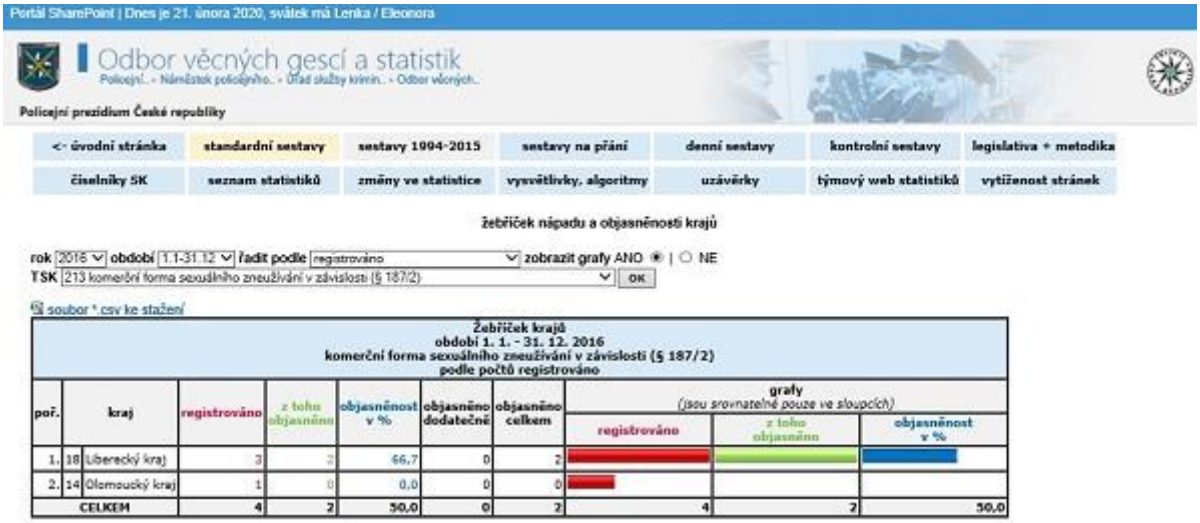


Žebříček krajů
období 1. 1. - 31. 12. 2019
komerční forma sexuálního zneužívání ostatní (§ 187/1, 3, 4)
podle počtů registrováno

poř.		kraj	registrováno	z toho objasněno	objasněnost v %	objasněno dodatečně	objasněno celkem	grafy (jsou srovnatelné pouze ve sloupcích) registrováno	z toho objasněno	objasněnost v %
1.	18	Liberecký kraj	3	3	100,0	0	3			
2.	06	Jihomoravský kraj	3	2	66,7	0	2			
3.	19	Karlovarský kraj	1	1	100,0	0	1			
4.	07	Moravskoslezský kraj	1	0	0,0	0	0			
5.	01	Středočeský kraj	0	0	0,0	3	3			
CELKEM			8	6	75,0	3	9	8	6	75,0

Zdroj: Odbor gescí a statistik PP Policie České republiky

Obrázek č. 12 Komerční forma sexuálního zneužívání v závislosti (§187/2) **2016**

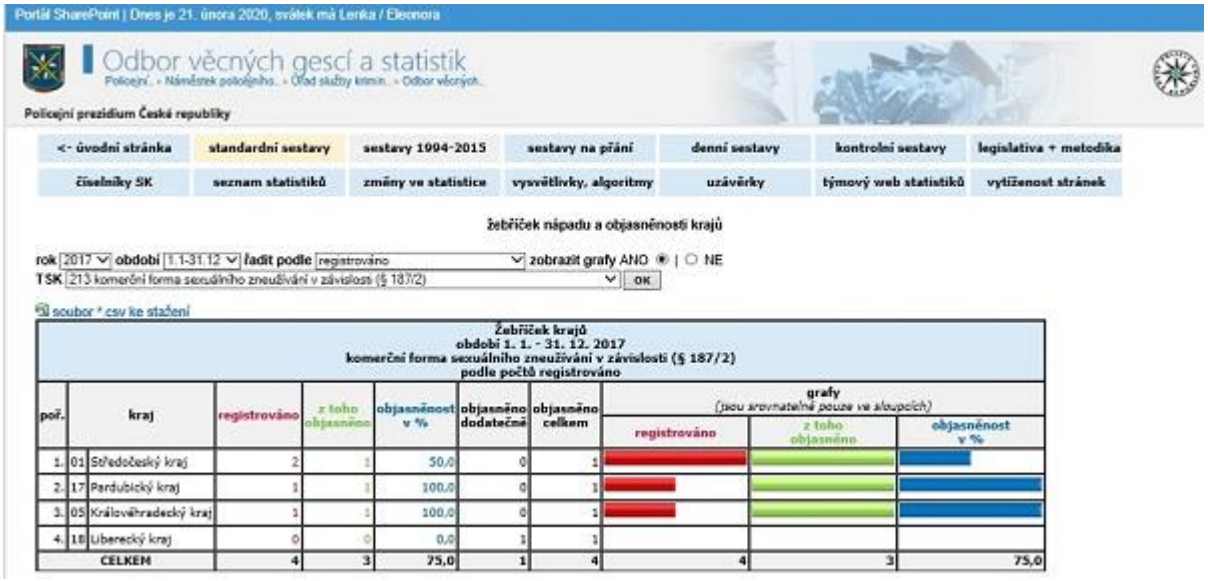


Žebříček krajů
období 1. 1. - 31. 12. 2016
komerční forma sexuálního zneužívání v závislosti (§ 187/2)
podle počtů registrováno

poř.		kraj	registrováno	z toho objasněno	objasněnost v %	objasněno dodatečně	objasněno celkem	grafy (jsou srovnatelné pouze ve sloupcích) registrováno	z toho objasněno	objasněnost v %
1.	18	Liberecký kraj	3	2	66,7	0	2			
2.	14	Olomoucký kraj	1	0	0,0	0	0			
CELKEM			4	2	50,0	0	2	4	2	50,0

Zdroj: Odbor gescí a statistik PP Policie České republiky

Obrázek č. 13 Komerční forma sexuálního zneužívání v závislosti (§187/2) **2017**

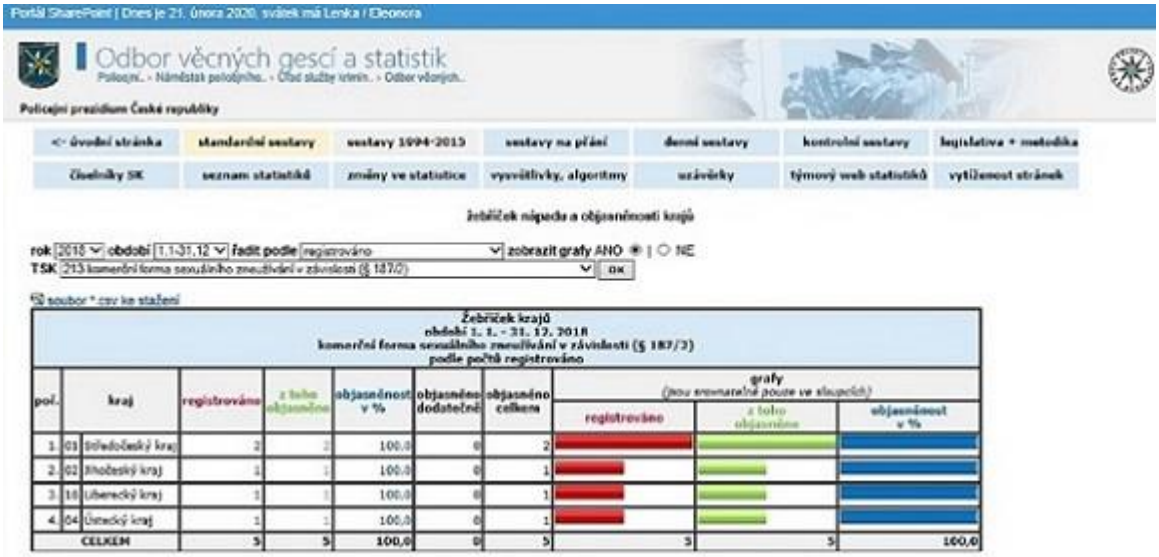


Žebříček krajů
období 1. 1. - 31. 12. 2017
komerční forma sexuálního zneužívání v závislosti (§ 187/2)
podle počtů registrováno

poř.		kraj	registrováno	z toho objasněno	objasněnost v %	objasněno dodatečně	objasněno celkem	grafy (jsou srovnatelné pouze ve sloupcích) registrováno	z toho objasněno	objasněnost v %
1.	01	Středočeský kraj	2	1	50,0	0	1			
2.	17	Pardubický kraj	1	1	100,0	0	1			
3.	05	Královéhradecký kraj	1	1	100,0	0	1			
4.	18	Liberecký kraj	0	0	0,0	1	1			
CELKEM			4	3	75,0	1	4	4	3	75,0

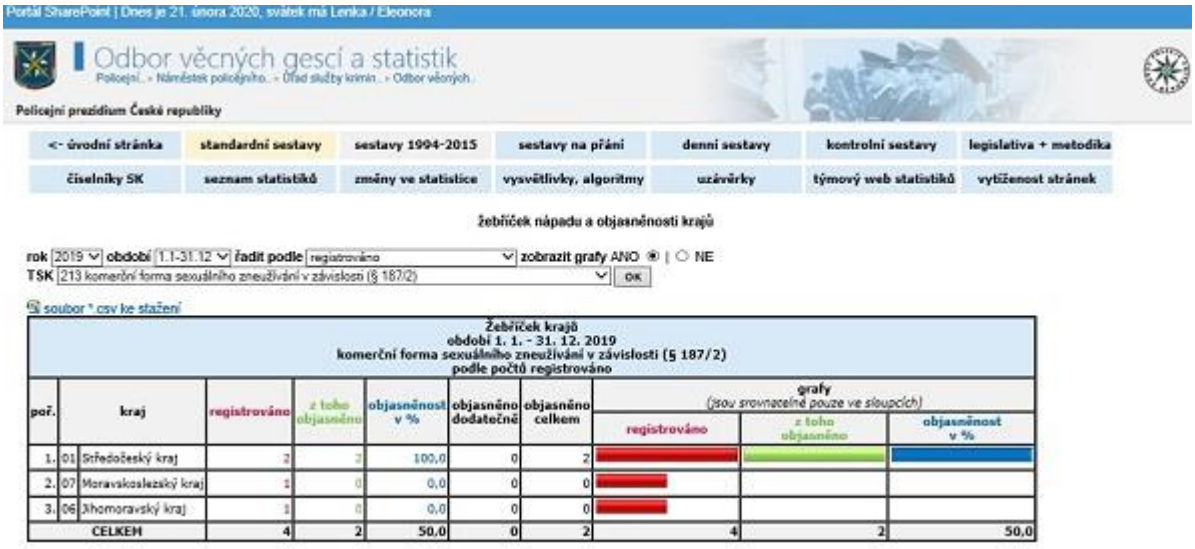
Zdroj: Odbor gescí a statistik PP Policie České republiky

Obrázek č. 14 Komerční forma sexuálního zneužívání v závislosti (§187/2) **2018**



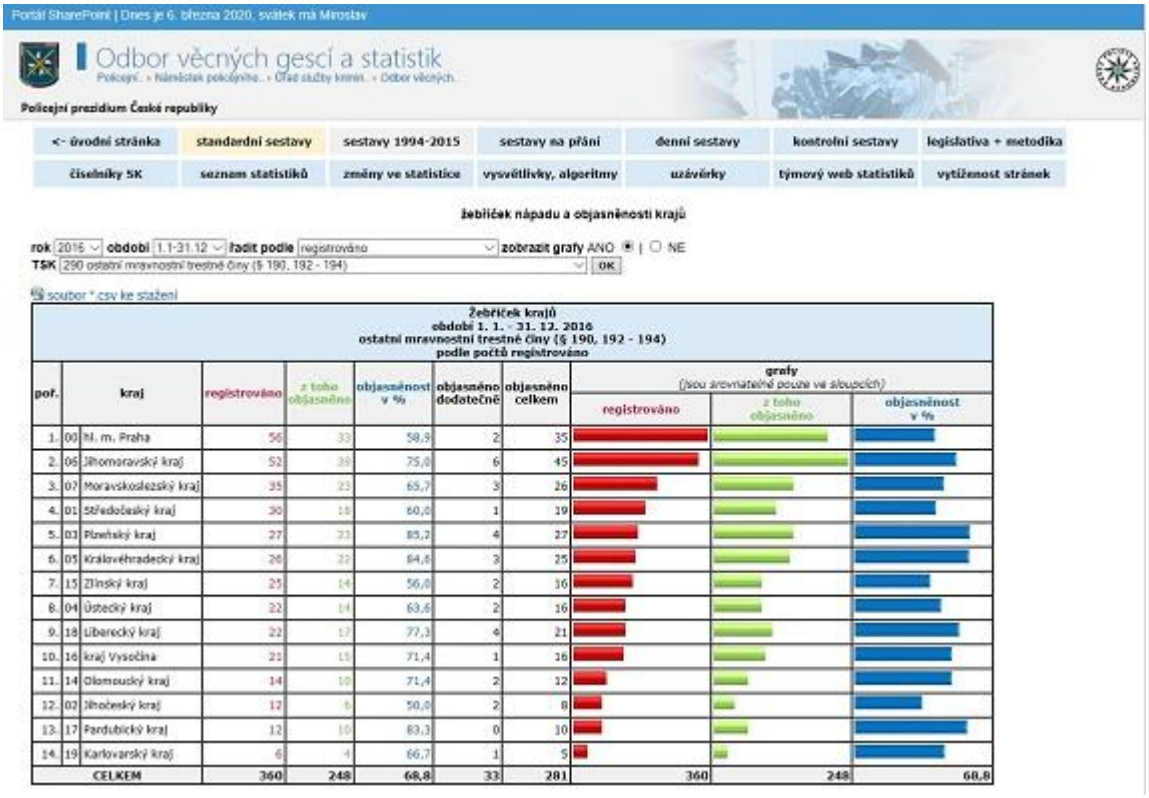
Zdroj: Odbor gescí a statistik PP Policie České republiky

Obrázek č. 15 Komerční forma sexuálního zneužívání v závislosti (§187/2) **2019**



Zdroj: Odbor gescí a statistik PP Policie České republiky

. **Obrázek č. 16** Ostatní mravnostní TČ (§190 - 194) **2016**



Portál SharePoint | Dnes je 6. března 2020, svátek má Miroslav

Odbor věcných gescí a statistik

Policejní prezidium České republiky

<- úvodní stránka | standardní sestavy | sestavy 1994-2015 | sestavy na přání | denní sestavy | kontrolní sestavy | legislativa + metodika

číselníky SK | seznam statistik | změny ve statistice | vysvětlivky, algoritmy | uzávěrky | týmový web statistik | vytíženost stránek

žebříček nápadu a objasněnosti krajů

rok 2016 období 1.1-31.12 řadit podle registrováno zobrazit grafy ANO | NE

TSK 290 ostatní mravnostní trestné činy (§ 190, 192 - 194) OK

soubor *.csv ke stažení

Žebříček krajů
období 1. 1. - 31. 12. 2016
ostatní mravnostní trestné činy (§ 190, 192 - 194)
podle počtů registrováno

poř.	kraj	registrováno	z toho objasněno	objasněnost v %	objasněno dodatečně	objasněno celkem	grafy (jsou srovnatelné pouze ve sloupcích) registrováno	z toho objasněno	objasněnost v %
1.	00 hl. m. Praha	56	33	58,9	2	35			
2.	06 Jihomoravský kraj	52	39	75,0	6	45			
3.	07 Moravskoslezský kraj	35	23	65,7	3	26			
4.	01 Středočeský kraj	30	18	60,0	1	19			
5.	03 Plzeňský kraj	27	23	85,2	4	27			
6.	05 Královéhradecký kraj	26	22	84,6	3	25			
7.	15 Zlínský kraj	25	14	56,0	2	16			
8.	04 Ústecký kraj	22	14	63,6	2	16			
9.	18 Liberecký kraj	22	17	77,3	4	21			
10.	16 kraj Vysočina	21	15	71,4	1	16			
11.	14 Olomoucký kraj	14	10	71,4	2	12			
12.	02 Jihočeský kraj	12	6	50,0	2	8			
13.	17 Pardubický kraj	12	10	83,3	0	10			
14.	19 Karlovarský kraj	6	4	66,7	1	5			
	CELKEM	360	248	68,8	33	281	360	248	68,8

Zdroj: Odbor gescí a statistik PP Policie České republiky

Obrázek č. 17 Ostatní mravnostní TČ (§190 - 194) **2017**

Portál SharePoint | Dnes je 6. března 2020, svátek má Miroslav

Odbor věcných gescí a statistik

Policejní prezidium České republiky

<- úvodní stránka | standardní sestavy | sestavy 1994-2015 | sestavy na přání | denní sestavy | kontrolní sestavy | legislativa + metodika

číselníky SK | seznam statistik | změny ve statistice | vysvětlivky, algoritmy | uzávěrky | týmový web statistik | vytíženost stránek

žebříček nápadu a objasněnosti krajů

rok 2017 období 1.1-31.12 řadit podle registrováno zobrazit grafy ANO | NE

TSK 290 ostatní mravnostní trestné činy (§ 190, 192 - 194) OK

soubor *.csv ke stažení

Žebříček krajů
období 1. 1. - 31. 12. 2017
ostatní mravnostní trestné činy (§ 190, 192 - 194)
podle počtů registrováno

poř.	kraj	registrováno	z toho objasněno	objasněnost v %	objasněno dodatečně	objasněno celkem	grafy (jsou srovnatelné pouze ve sloupcích) registrováno	z toho objasněno	objasněnost v %
1.	00 hl. m. Praha	78	39	50,0	5	44			
2.	07 Moravskoslezský kraj	69	42	66,7	4	46			
3.	02 Jihočeský kraj	45	27	60,0	1	28			
4.	01 Středočeský kraj	43	20	46,5	3	23			
5.	05 Královéhradecký kraj	39	29	74,4	3	32			
6.	14 Olomoucký kraj	35	29	82,9	1	30			
7.	04 Ústecký kraj	34	24	70,6	7	31			
8.	06 Jihomoravský kraj	32	23	71,9	10	33			
9.	15 Zlínský kraj	31	21	67,7	5	26			
10.	18 Liberecký kraj	24	18	75,0	6	24			
11.	16 kraj Vysočina	23	14	60,9	4	18			
12.	17 Pardubický kraj	18	13	72,2	0	13			
13.	03 Plzeňský kraj	14	4	28,6	1	5			
14.	19 Karlovarský kraj	10	6	60,0	0	6			
	CELKEM	489	309	63,1	50	359	489	309	63,1

Zdroj: Odbor gescí a statistik PP Policie České republiky

Obrázek č. 18 Ostatní mravnostní TČ (§190 - 194) **2018**

Portál SharePoint | Dnes je 6. března 2020, svátek má Miroslav

Odbor věcných gescí a statistik

Policejní prezidium České republiky

<- úvodní stránka | standardní sestavy | sestavy 1994-2015 | sestavy na přání | denní sestavy | kontrolní sestavy | legislativa + metodika

číselníky SK | seznam statistik | změny ve statistice | vysvětlivky, algoritmy | uzávěrky | týmový web statistik | vytíženost stránek

žebříček nápadu a objasněnosti krajů

rok 2018 | období 1.1-31.12 | řadit podle registrováno | zobrazit grafy ANO | NE

TSK 290 ostatní mravnostní trestné činy (§ 190, 192 - 194) | OK

soubor *.csv ke stažení

Žebříček krajů
období 1. 1. - 31. 12. 2018
ostatní mravnostní trestné činy (§ 190, 192 - 194)
podle počtů registrováno

poř.		kraj	registrováno	z toho objasněno	objasněnost v %	objasněno dodatečně	objasněno celkem	grafy (jsou srovnatelné pouze ve sloupcích) registrováno	z toho objasněno	objasněnost v %
1.	00	hl. m. Praha	92	53	57,6	8	61			
2.	07	Moravskoslezský kraj	80	54	67,5	11	65			
3.	06	Jihomoravský kraj	79	56	70,9	7	63			
4.	05	Královéhradecký kraj	60	52	86,7	6	58			
5.	01	Středočeský kraj	52	32	61,5	7	39			
6.	02	Jihočeský kraj	46	24	52,2	9	33			
7.	03	Plzeňský kraj	42	26	61,9	8	34			
8.	04	Ústecký kraj	40	28	70,0	7	35			
9.	16	kraj Vysočina	37	22	59,5	7	29			
10.	18	Liberecký kraj	32	17	53,1	4	21			
11.	15	Zlínský kraj	31	21	67,7	5	26			
12.	17	Pardubický kraj	24	19	79,2	2	21			
13.	14	Olomoucký kraj	22	13	59,1	4	17			
14.	19	Karlovarský kraj	12	8	66,7	1	9			
		CELKEM	649	425	65,4	86	511	649	425	65,4

Zdroj: Odbor gescí a statistik PP Policie České republiky

Obrázek č. 19 Ostatní mravnostní TČ (§190 - 194) **2019**

Portál SharePoint | Dnes je 6. března 2020, svátek má Miroslav

Odbor věcných gescí a statistik

Policejní prezidium České republiky

<- úvodní stránka | standardní sestavy | sestavy 1994-2015 | sestavy na přání | denní sestavy | kontrolní sestavy | legislativa + metodika

číselníky SK | seznam statistik | změny ve statistice | vysvětlivky, algoritmy | uzávěrky | týmový web statistik | vytíženost stránek

žebříček nápadu a objasněnosti krajů

rok 2019 | období 1.1-31.12 | řadit podle registrováno | zobrazit grafy ANO | NE

TSK 290 ostatní mravnostní trestné činy (§ 190, 192 - 194) | OK

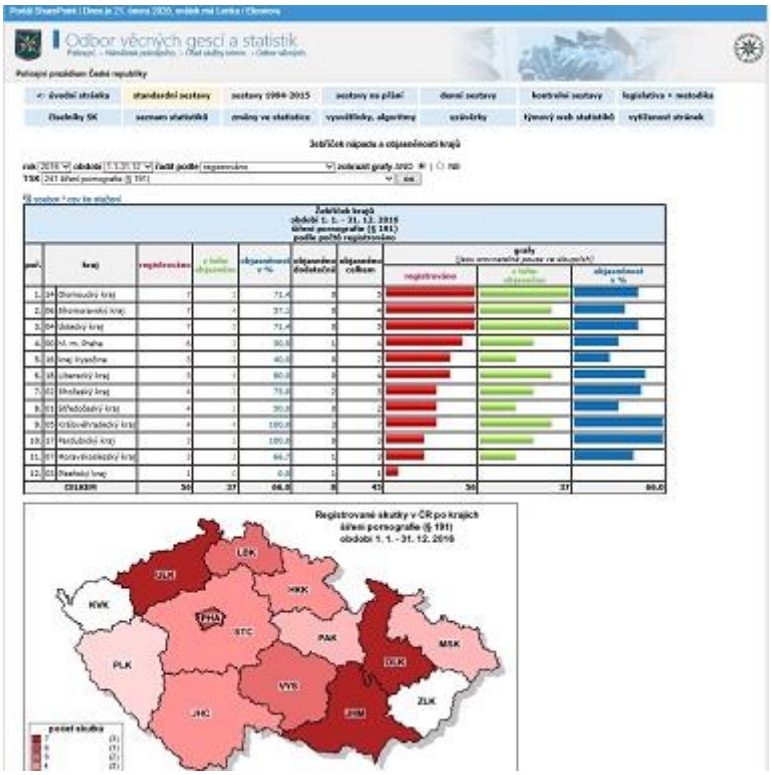
soubor *.csv ke stažení

Žebříček krajů
období 1. 1. - 31. 12. 2019
ostatní mravnostní trestné činy (§ 190, 192 - 194)
podle počtů registrováno

poř.		kraj	registrováno	z toho objasněno	objasněnost v %	objasněno dodatečně	objasněno celkem	grafy (jsou srovnatelné pouze ve sloupcích) registrováno	z toho objasněno	objasněnost v %
1.	06	Jihomoravský kraj	117	95	81,2	16	111			
2.	00	hl. m. Praha	102	55	53,9	17	72			
3.	07	Moravskoslezský kraj	66	48	72,7	15	63			
4.	01	Středočeský kraj	64	36	56,3	8	44			
5.	04	Ústecký kraj	56	41	73,2	8	49			
6.	05	Královéhradecký kraj	55	50	90,9	13	63			
7.	02	Jihočeský kraj	54	40	74,1	13	53			
8.	15	Zlínský kraj	44	40	90,9	10	50			
9.	16	kraj Vysočina	42	25	59,5	8	33			
10.	14	Olomoucký kraj	31	20	64,5	3	23			
11.	17	Pardubický kraj	30	20	66,7	4	24			
12.	03	Plzeňský kraj	25	9	32,0	8	16			
13.	18	Liberecký kraj	23	16	69,6	10	26			
14.	19	Karlovarský kraj	19	14	73,7	8	22			
		CELKEM	728	508	69,7	141	649	728	508	69,7

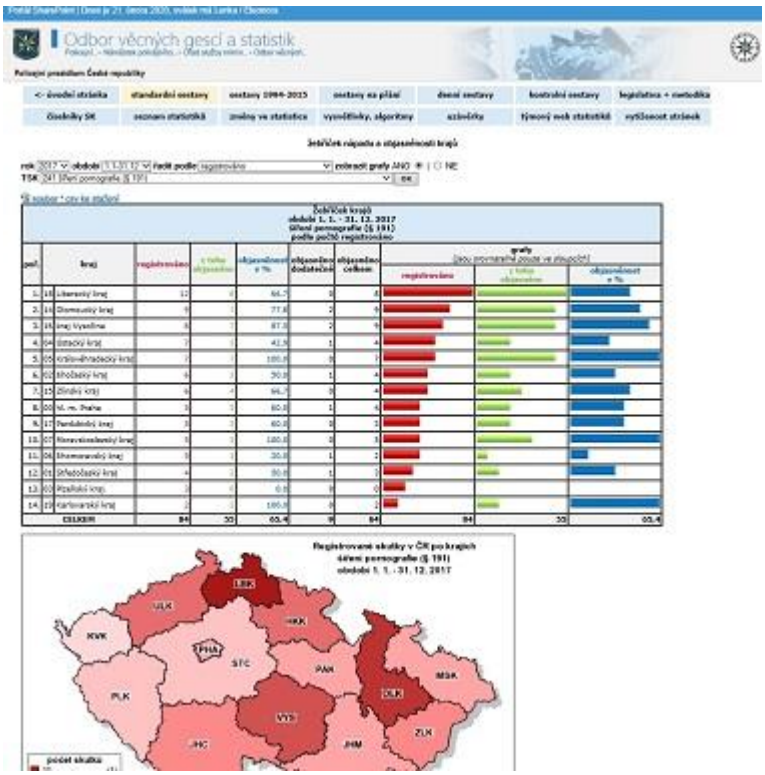
Zdroj: Odbor gescí a statistik PP Policie České republiky

Obrázek č. 20 Žebříček krajů – šíření pornografie 2016



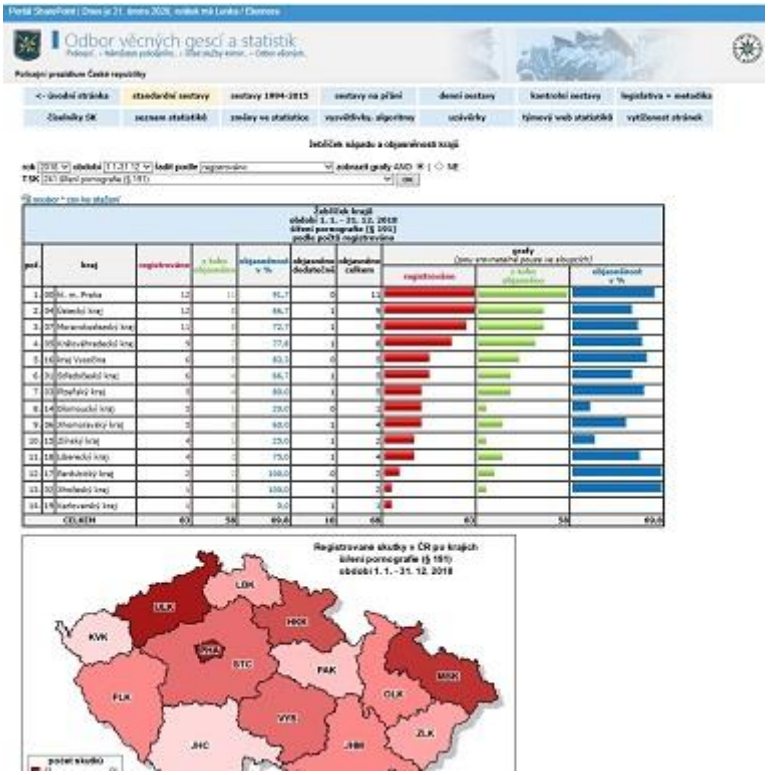
Zdroj: Odbor gescí a statistik PP Policie České republiky

Obrázek č. 21 Žebříček krajů – šíření pornografie 2017



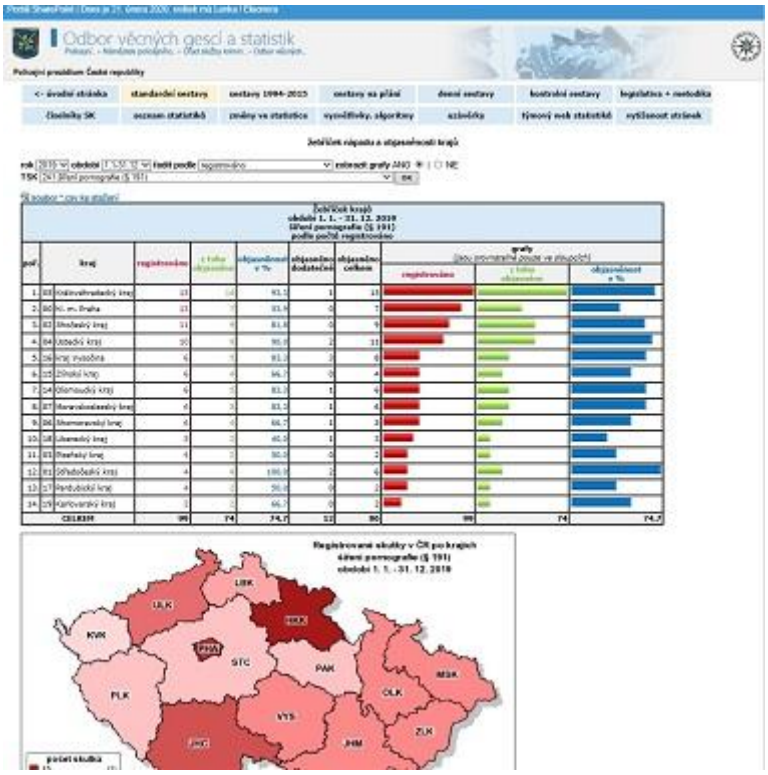
Zdroj: Odbor gescí a statistik PP Policie České republiky

Obrázek č. 22 Žebříček krajů – šíření pornografie 2018



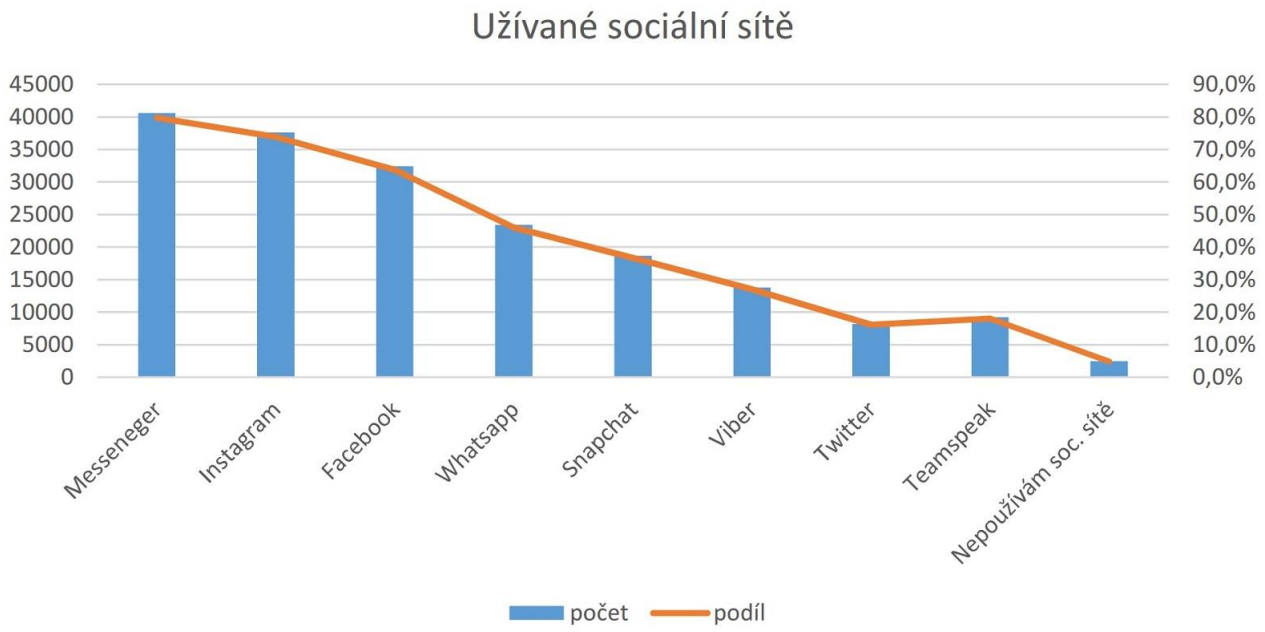
Zdroj: Odbor gescí a statistik PP Policie České republiky

Obrázek č. 23 Žebříček krajů – šíření pornografie 2018



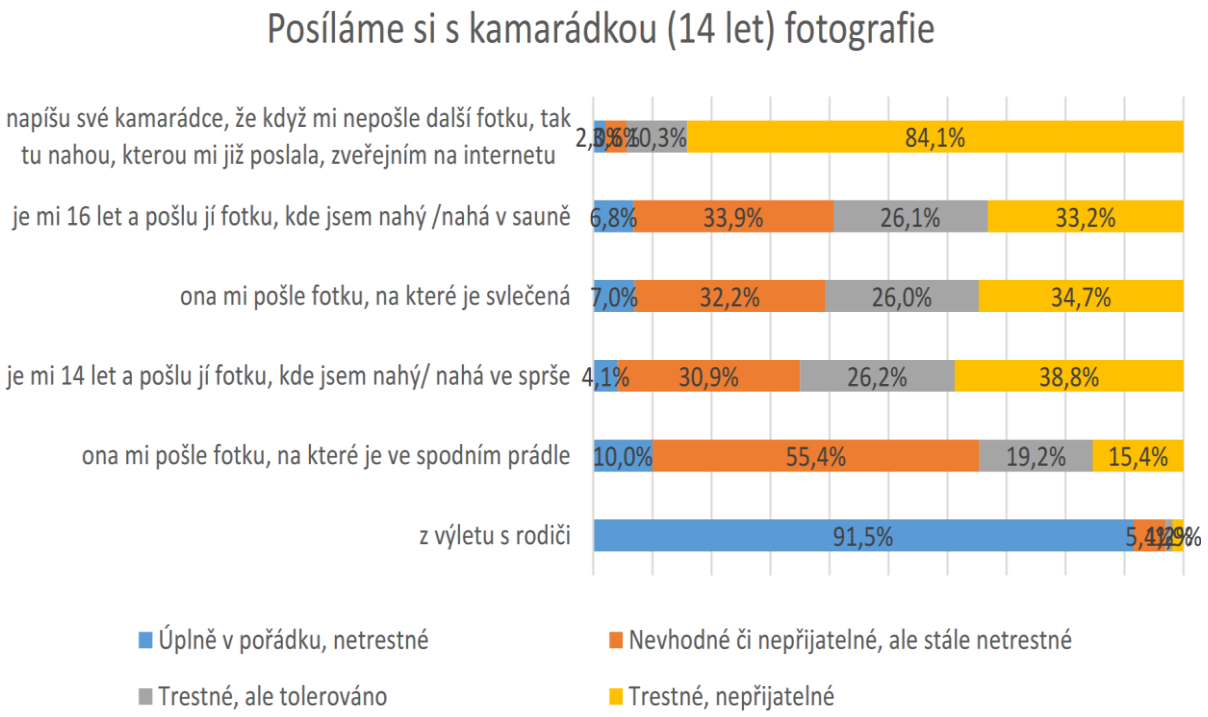
Zdroj: Odbor gescí a statistik PP Policie České republiky

Obrázek č. 24 Užívané sociální sítě



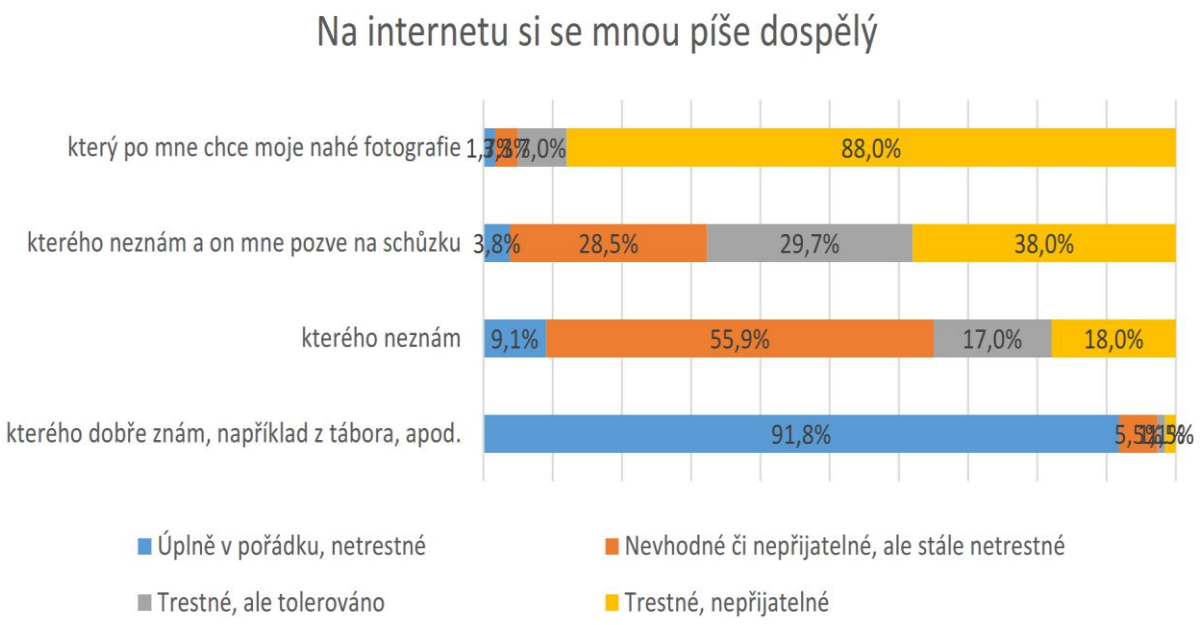
Dostupné z: https://www.policie.cz/clanek/vyzkum-vnimani-kyberkriminality-mezi-detmi-v-ramci-projektu-kpbi.aspx

Obrázek č. 25 Posílání fotografií s kamarádkou (14 let) - statistika



Dostupné z: https://www.policie.cz/clanek/vyzkum-vnimani-kyberkriminality-mezi-detmi-v-ramci-projektu-kpbi.aspx

Obrázek č. 26 Na internetu si se mnou píše dospělý



Dostupné z: https://www.policie.cz/clanek/vyzkum-vnimani-kyberkriminality-mezi-detmi-v-ramci-projektu-kpbi.aspx

Obrázek 27: ukázka tří kryptoměn – Bitcoin Litecoin, Etherneum

Zdroj: E15 Dostupné z: https://www.e15.cz/seznam-kryptomen