POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

BAKALÁŘSKÁ PRÁCE

2022 ROMAN MILOTÍNSKÝ

POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostního managementu

Katedra managementu a informatiky

Boj proti informační kriminalitě v ČR

Bakalářská práce

Fight against information crime in the Czech Republic

Bachelor thesis

VEDOUCÍ PRÁCE

RNDr. Václav Hník, CSc.

AUTOR PRÁCE

Roman Milotínský

PRAHA

2022

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpal, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Pohořelicích, dne 10. 2. 2022

…….....

Roman MILOTÍNSKÝ

Poděkování

Rád bych na tomto místě poděkoval svému vedoucímu práce RNDr. Václavu Hníkovi CSc. za cenné rady, věcné připomínky a vstřícnost při konzultacích a vypracování bakalářské práce. Dále bych také rád poděkoval kapitánovi Mgr. Romanu Mrákovi z Oddělení Kybernetické kriminality, který byl jako konzultant při vypracování této práce, za jeho ochotu a trpělivost.

ANOTACE

Práce se zabývá výhradně bojem proti informační kriminalitě v České republice. Je rozdělena do dvou částí, a to na teoretickou a praktickou. V teoretické části je zaměřena na informační kriminalitu, kde je popsána definice pojmu informační kriminalita, klasifikace a kybernetické hrozby. Dále pak na boj proti informační kriminalitě, kde jsou popsány orgány bojující proti této trestné činnosti v ČR. V praktické části je pak rozebrána případová studie konkrétního vyšetřovaného případu.

KLÍČOVÁ SLOVA

Boj proti informační kriminalitě, informační kriminalita, kybernetické hrozby, kyberkriminalita, mravnostní trestné činy, oběti.

ANNOTATION

This thesis deals with the fight against the cyber criminality in the Czech Republic. It is divided into two parts, theoretical and practical. It focuses on the cyber criminality in the theoretical part where you can find the definition of the term cyber criminality, its classification and cyber threats. What is more, you can also find the fight against the cyber criminality in the Czech Republic there. In the theoretical part there is the description of the government authorities that struggle with the cyber criminality. In the practical part there is the case study of the particular crime investigation.

KEYWORDS

Fight against information crime, cyber criminality, cyber threats, cybercrime, crimes of indecency, victims.

Obsah

Úvod

Současnou moderní a technologicky vyspělou společnost můžeme nazvat společností informační. Informační technologie se neustále vyvíjejí a naše společnost je na jejich existenci již takřka závislá. Moderní technologie jsou součástí našeho každodenního života a narážíme na ně téměř na každém kroku. To potvrzují i statistická data, která přináší poměrně znepokojující výsledky.

Podle výsledků těchto studií bylo roku 2014 na světové úrovni používáno kupříkladu zhruba 6,8 miliardy mobilních telefonů, zatímco světová populace dosahovala 7,1 miliardy lidí. Oproti tomu, 9 let předtím, v roce 2005, kdy světová populace dosahovala 6,5 miliardy lidí, bylo používáno zhruba 2,5 miliardy mobilních telefonů. Narůstající trend počtu uživatelů zažívají i sociální sítě Facebook, Google+, LinkedIn, Sina Weibo, Twitter, Tumblr a VKontakte)[1].

Podle výzkumu zabývajícího se sociálními sítěmi z roku 2018 využívalo v globálním měřítku sociální sítě 2,5 miliardy uživatelů neboli více než 1/3 světové populace, přičemž ani čeští uživatelé nestáli pozadu, *„roku 2018 používalo sociální sítě již 52 % Čechů starších 16 let. K nejdynamičtějšímu nárůstu uživatelů došlo přitom již mezi lety 2009 a 2012. Tehdy jejich podíl vzrostl z 5 na 31 %“*[2].

Moderní technologie a informační společnost s sebou přinášejí pro běžného občana mnoho pozitivních aspektů. Urychlují a usnadňují naše každodenní životy, umožňují nám získávat téměř okamžitě potřebné informace, sledovat v přímém přenosu události odehrávající se na druhé straně naší planety, komunikovat s přáteli či rodinou žijící na druhém konci zeměkoule či si můžeme z pohodlí domova objednat jakékoliv zboží.

Na druhé straně s sebou přináší i velké množství bezpečnostních rizik, se kterými se lidská společnost v historickém kontextu potýkat nikdy

[1] *FIRE M., GOLDSCHMIDT R., ELOVICI Y. 2014. Online social network*: Threats and Solutions. 2014. IEEE communication surveys. Volume 16, Issue 4, pp. 125-142.
[2] *ČSÚ. 2018. Více než polovina Čechů používá sociální sítě* [online]. Praha (Česká republika) Český statistický úřad, aktualizace 20. 11. 2018. [2021-11-5] URL: https://www.czso.cz/csu/czso/vice-nez-polovina-cechu-pouziva-socialni-site

nemusela. Jak se rozvíjejí informační technologie a navyšuje se jejich dosah, narůstá i spektrum, počet a frekvence trestných činů, ke kterým dochází v rámci kybernetického prostoru. V případě takových trestných činů hovoříme o tzv. informační kriminalitě. Tento pojem můžeme nahradit i dalšími ekvivalenty, kterými jsou kybernetická kriminalita, kyberkriminalita nebo počítačová kriminalita[3].

Tomu, že se skutečně v současné době jedná o globální problém dosahující markantních rozměrů, nasvědčuje i fakt, že roku 2009 musely být Bezpečnostní složky České republiky rozšířeny o celý bezpečnostní útvar nesoucí název Informační a kybernetické síly České republiky, které mají za úkol proti kybernetické kriminalitě na státní úrovni aktivně bojovat[4].

Informační kriminalita představuje hlavní objekt zájmu této bakalářské práce. Jejím hlavním cílem bude představit, jakými konkrétními mechanismy je v rámci České republiky bráněno počítačové kriminalitě. Téma bylo vybráno hned z několika důvodů. První důvod představuje můj vlastní zájem této bakalářské práce o toto téma a druhým důvodem je, že tato problematika je velice aktuální a kybernetické zločiny začínají být frekventovanější nežli útoky reálné. A jelikož se v kybernetickém prostoru pohybuje velké procento světové populace, měla by být tomuto tématu věnována velká pozornost.

V teoretické části této bakalářské práce se budu v rámci první kapitoly věnovat charakteristice informační kriminality a jejím obecným aspektům. Detailně popíši co je informační kriminalita, jaké státní orgány s touto hrozbou bojují, jaké rozeznáváme druhy počítačové kriminality a jaké konkrétní hrozby s sebou tento druh trestné činnosti přináší. V druhé kapitole teoretické části této práce se zaměřím na samotný boj s touto trestnou činností a zejména na konkrétní obranné mechanismy, které jsou využívány v současné době Českou republikou v boji proti počítačové kriminalitě. Jelikož je boj proti kybernetické kriminalitě obecně velmi rozsáhlý, zaměřil jsem se proto podrobně na útoky na integritu dětí, jakožto zvláště

[3] *Články: prevencekriminality.cz. Kyberkriminalita*. [online]. Praha (Česká republika) Ministerstvo vnitra, odbor prevence kriminality, 2014. [2021-11-5] URL: https://prevencekriminality.cz/prevence-kriminality/kyberkriminalita/

[4] *AČR. Velitelství informačních a kybernetických sil* [online]. Praha (Česká republika) Ministerstvo obrany, aktualizace 7. 10. 2021. [2021-11-5] URL: https://www.acr.army.cz/struktura/generalni/kyb/velitelstvi-kybernetickych-sil-a-informacnich-operaci-214169/

zranitelných obětí, konkrétně na mravnostní trestné činy, neboť bych byl velmi rád, aby i tato práce byla jistým preventivním prvkem.

V praktické části práce se budu zabývat případovou studií, založenou na reálném případu, který byl vyšetřován policií ČR, Krajským Ředitelstvím Policie Jihomoravského kraje, Oddělením kybernetické kriminality v Brně. Tento případ byl vyšetřován od roku 2013 do roku 2020.

V první části této případové studie si ukážeme, jak probíhalo vyšetřování Policie ČR, jaké byly provedeny úkony při šetření případu a odhalování pachatele. Dále se podíváme na postup soudního orgánu, kde od návrhu státního zástupce se dostaneme až k výroku soudu. Také zde podotknu, jakým způsobem je prováděno psychologické vyšetření a k jakému závěru bylo nakonec přihlédnuto. A na závěr si shrneme, jaká byla náprava pachatele. Zda byly postupy soudních orgánů a znalců v oboru zdravotnictví, odvětví psychologie dostatečné.

Metodologie

Teoretickou část předkládané bakalářské práce tvoří literární rešerše týkající se problematiky informační kriminality. K vypracování této části bylo využito dostupné škály primárních i sekundárních literárních zdrojů, vědeckých odborných článků i webových stránek organizací a spolků, které se problematikou informační kriminality zabývají. Z velké části se jedná o česky psanou odbornou literaturu, doplněnou anglicky psanými vědeckými články.

V analytické části této bakalářské práce je detailně popsána případová studie na případu, který byl vyšetřován Oddělením Kybernetické kriminality v Brně. Jedná se o případ mravnostní kriminality, konkrétně § 186 sexuální nátlak, § 201 ohrožování výchovy dítěte a § 191 šíření pornografie. Tato studie byla vypracována ze spisů, které mi byly zapůjčeny se svolením Oddělení kybernetické kriminality.

Výsledkem je předkládaná bakalářská práce, která disponuje dostatečným množstvím věrohodných a odborných informací týkajících se problematiky informační kriminality v České republice a především mechanismy, které jsou používány v boji proti tomuto druhu trestných činností. Čtenáři je tak poskytnut ucelený přehled nejnovějších poznatků ohledně problematiky počítačové kriminality.

1. Teoretická část

1.1. Informační kriminalita

Pojem *informační kriminalita* představuje v současné době již poněkud zastaralý odborný výraz, pro který se dnes používá spíše jeho ekvivalent „kybernetická kriminalita“ nebo jeho zkrácená forma „kyberkriminalita“. Tyto pojmy pak vycházejí z označení kybernetický prostor neboli kyberprostor, který představuje virtuální prostředí nemající žádného jasného počátku ani konce. Je to navíc prostředí, které nezná hranic, je globálního rozsahu a nelze s jistotou určit, jak rozsáhlé toto prostředí vlastně může být[5].

Pro označení trestných činů, ke kterým dochází v rámci virtuálního kybernetického prostředí lze použít i výraz *počítačová kriminalita*[6].

Konkrétně, Policie České republiky definuje kybernetickou kriminalitu jako „*trestná činnost, která je páchána v prostředí informačních a komunikačních technologií včetně počítačových sítí. Samotná oblast informačních a komunikačních technologií je buď předmětem útoku, nebo je páchána trestná činnost za výrazného využití informačních a komunikačních technologií jakožto významného prostředku k jejímu páchání*“[7].

V podobném duchu kybernetickou kriminalitu ve své knize definuje i Jirovský, který tento druh trestné činnosti nazývá „kybernalitou“. Kybernetické trestné činy pak vidí jako činy, které porušují zákon nebo jsou v přímém rozporu s morálními zásadami naší společnosti. Počítač v kybernetickém zločinu může vystupovat hned ve dvou polohách, a to jako objekt kybernetického útoku i jako nástroj, kterým jsou útoky páchány[8].

Více specifická je pak definice informační kriminality poskytnutá Ministerstvem vnitra České republiky, které uvádí, že „*pod pojmem počítačová*

[5]*Články: prevencekriminality.cz. Kyberkriminalita* [online]. Praha (Česká republika) Ministerstvo vnitra, odbor prevence kriminality, 2014. [2021-11-5] URL: https://prevencekriminality.cz/prevence-kriminality/kyberkriminalita/
[6]*Poznámka autora*.
[7]*PČR. Kyberkriminalita* [online]. Praha (Česká republika) Policie České republiky, 2021. [2021-11-5] URL: https://www.policie.cz/clanek/kyberkriminalita.aspx
[8]*JIROVSKÝ, V. Kybernetická kriminalita*: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. 1 vydání, Praha: Grada Publishing, 2007. ISBN: 978-80-247- 1561-2, s. 19.

kriminalita je třeba chápat páchání trestné činnosti, 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 této trestné činnosti, ovšem s výjimkou majetkové trestné činnosti, nebo jako nástroj trestné činnosti.[9]“

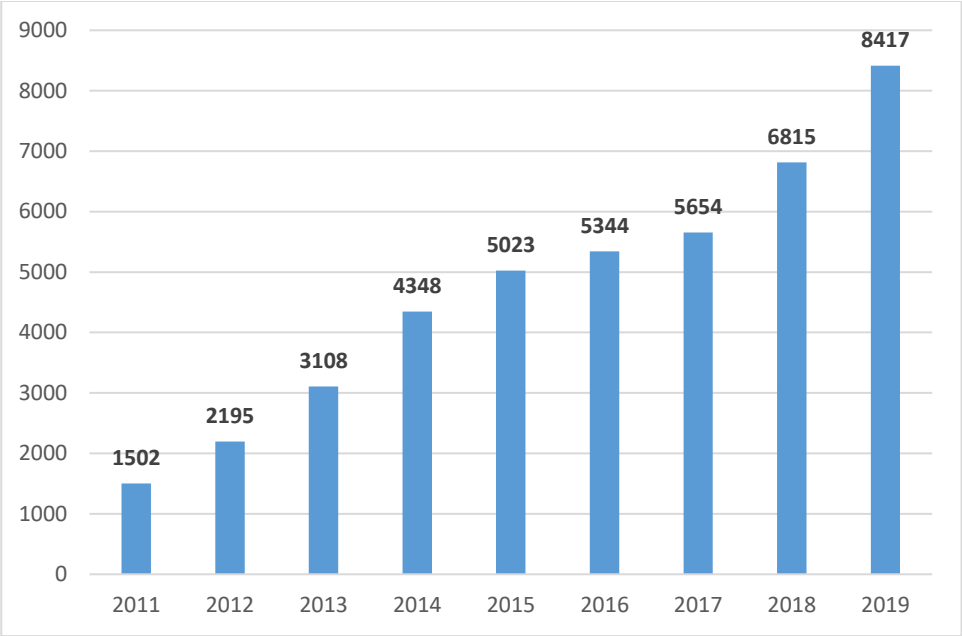
I široké veřejnosti musí byt jasné, že trestných činností, které spadají do kategorie kybernetické kriminality, je v současné době nepřeberné množství. Nejčastější trestnou činností páchanou v kyberprostoru je tzv. **podvodné jednání**, jehož charakteristiku nalezneme v právním ustanovení § 209 trestního zákoníku. Dalším činem často páchaným v prostředí virtuálního internetového prostředí je tzv. **hacking**, jehož definici opět nalezneme v právním ustanovení § 230 trestního zákoníku.

O jednotlivých druzích kybernetické kriminality si povíme detailněji v kapitole *1.2. Klasifikace*, ale je nutné si uvědomit, že spektrum kybernetických zločinů je velice pestré a potírat všechny jeho projevy je v současné době téměř nemožné.

Velmi vysoká je i samotná frekvence provádění kybernetické trestné činnosti. Jelikož se odhaduje, že v současné době využívají internet a kyberprostor zhruba ¾ lidské populace (zhruba 5,5 miliard lidí), lze kalkulovat, že každou sekundu dojde ke spáchání hned několika desítek informačních trestných činů různého charakteru. Během let dochází k citelnému narůstání počtu spáchaných kybernetických zločinů, a to jak na celosvětové úrovni, tak i na úrovni České republiky (viz. Graf).

---

[9] *MVČR. Kybernetická kriminalita v ČR z kriminologické perspektivy* [online]. Praha (Česká republika) Ministerstvo vnitra ČR, 2017. [2021-11-14] URL: https://www.google.com/url?client=internal-element-cse&cx=015489265366623571386:izzrwg3bmqm&q=https://www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx&sa=U&ved=2ahUKEwiw8JCCkq_2AhVBPewKHWMfCHQQFnoECAEQAQ&usg=AOvVaw0UDIlTmgISACQ4w75aLG6n



Graf: Počet spáchaných trestných činů v kyberprostoru v ČR v období 2011-2019.
Zdroj: pcr.cz

Kybernetická trestná činnost disponuje od ostatních druhů trestných činností mnoha specifiky. Vesměs jsou to specifické rysy, které umožňují kybernetické kriminalitě neustále se šířit, zvyšovat se v počtu a vyvíjet se. Zásadními specifiky informační kriminality jsou (a) všudypřítomná dostupnost, (b) nízké pořizovací náklady na její uskutečňování, (c) globální rozšíření kyberprostoru, v němž ke kriminalitě dochází, (d) vysoká míra anonymity pachatelů trestných činů a jejich složité vystopování a následné odhalení, (e) vysoká míra latence trestných činů, k odhalení jejichž viníků mnohdy dochází až s odstupem měsíců či let[10].

[10] *GŘIVNA, T; SCHEINOST, M; ZOUBKOVÁ, I. 2015. Kriminologie. 1 vydání, Praha*: Wolters Kluwer, a. s. ISBN: 978-80-7478-614-3, s. 336.

1.2. Klasifikace

Jak jsme si již zmínili v předcházející kapitole, trestných činů, které můžeme zahrnout do kategorie kybernetické kriminality, existuje v současné době velmi široké spektrum, přičemž se stále objevují nové a sofistikovanější druhy.

Aby odborníci v existujících i nově se objevujících trestných činnostech páchaných v rámci kyberprostoru udělali systém, zavedla se dvě základní hlediska, podle kterých můžeme zločiny snadněji klasifikovat. První hledisko rozděluje trestné činy podle toho, jakou úlohu v nich sehrává výpočetní technika, nejčastěji v podobě počítače, a druhé hledisko pak kategorizuje trestné činy podle jejich typu[11].

Postavení výpočetní techniky v rámci trestných činů

1) Trestné činy, v rámci kterých je počítač terčem útoku.

2) Trestné činy, které jsou spáchány využitím výpočetní techniky jako nástroje pro spáchání trestné činnosti.

Typ kybernetické trestné činnosti

1) Tradiční trestní činy - u této kategorie trestných činů může výpočetní technika sestávat v obou výše uvedených pozicích. Jedná se o klasické trestné činy, které byly prováděny lidmi i bez počítače. Konkrétně těmito činy mohou být krádeže, zpronevěry, podvody, padělání, šikana, mravnostní trestné činy, šíření extremismu, šíření dezinformací aj.

2) Trestné činy nové - tyto trestné činy jsou úzce spjaty s výpočetní technikou, bez které by k jejich vzniku ani nedošlo. V jiných aspektech lidských životů se tyto trestné činy neobjevují. Příkladem může být tzv. hacking, zneužití osobních údajů, sparing, pirátství aj.

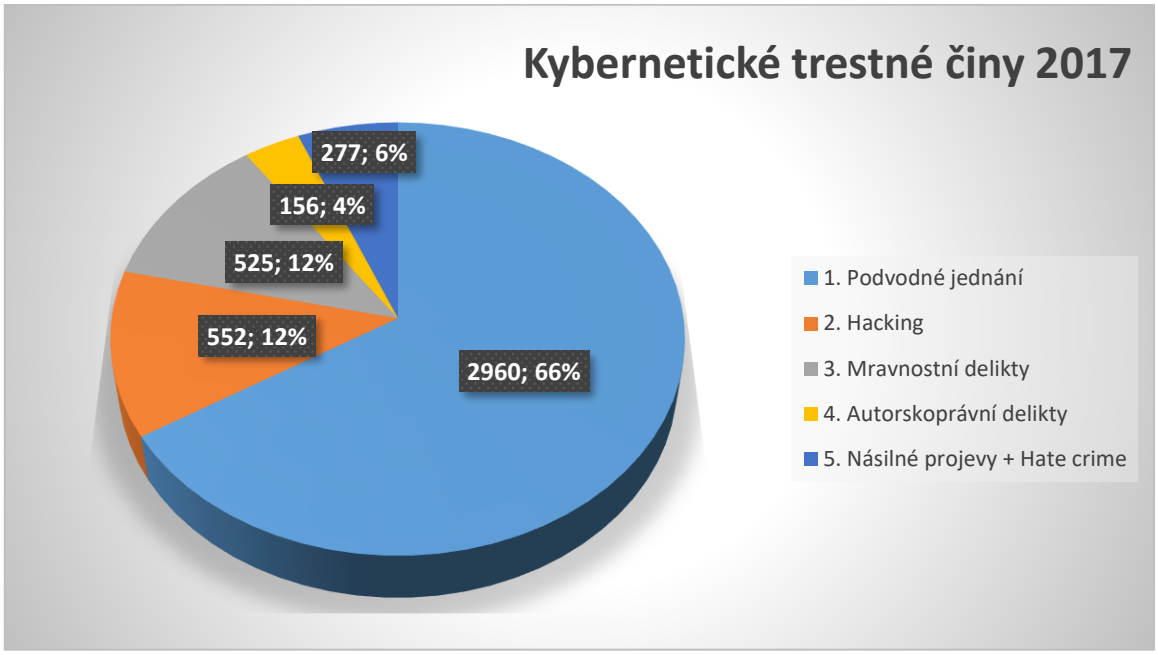
Policie České republiky v rámci svých oddělení, která bojují s kybernetickými zločiny, rozeznává několik hlavních kategorií informační

[11] *MATĚJKA, M. Počítačová kriminalita. 1 vydání, Praha*: Computer Press, 2002. ISBN: 80-7226-419-2, s. 25.

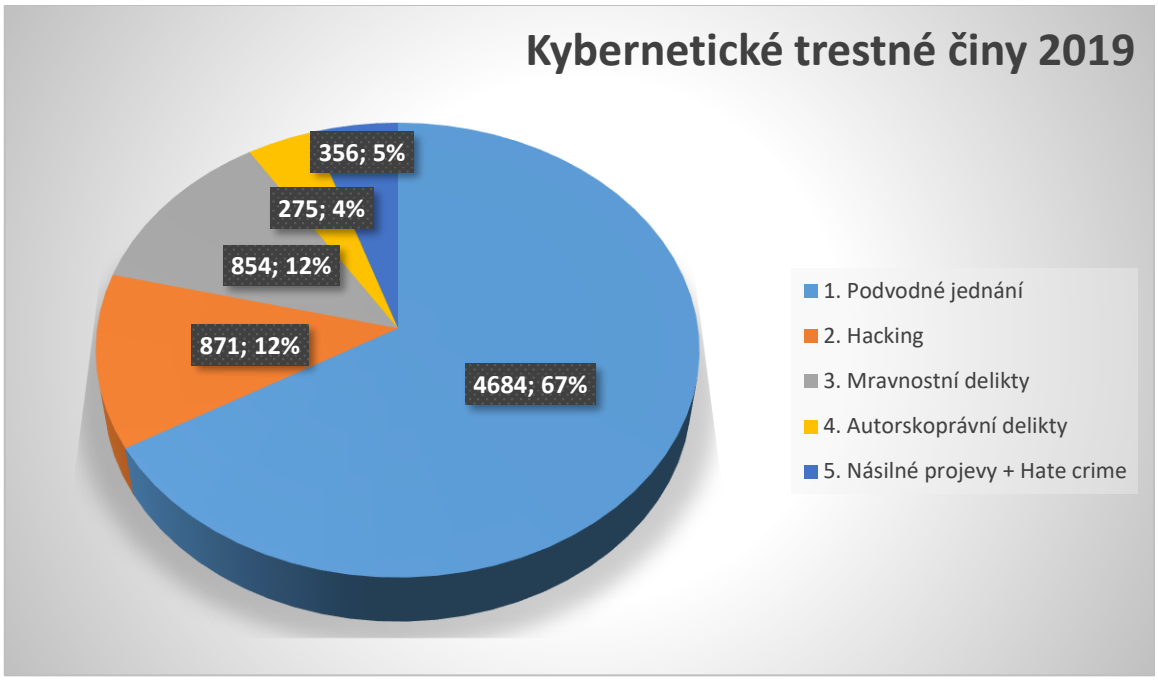
kriminality, se kterými se v rámci české internetové scény nejčastěji setkávají. Těmito jednotlivými kategoriemi pak konkrétně jsou[12]:

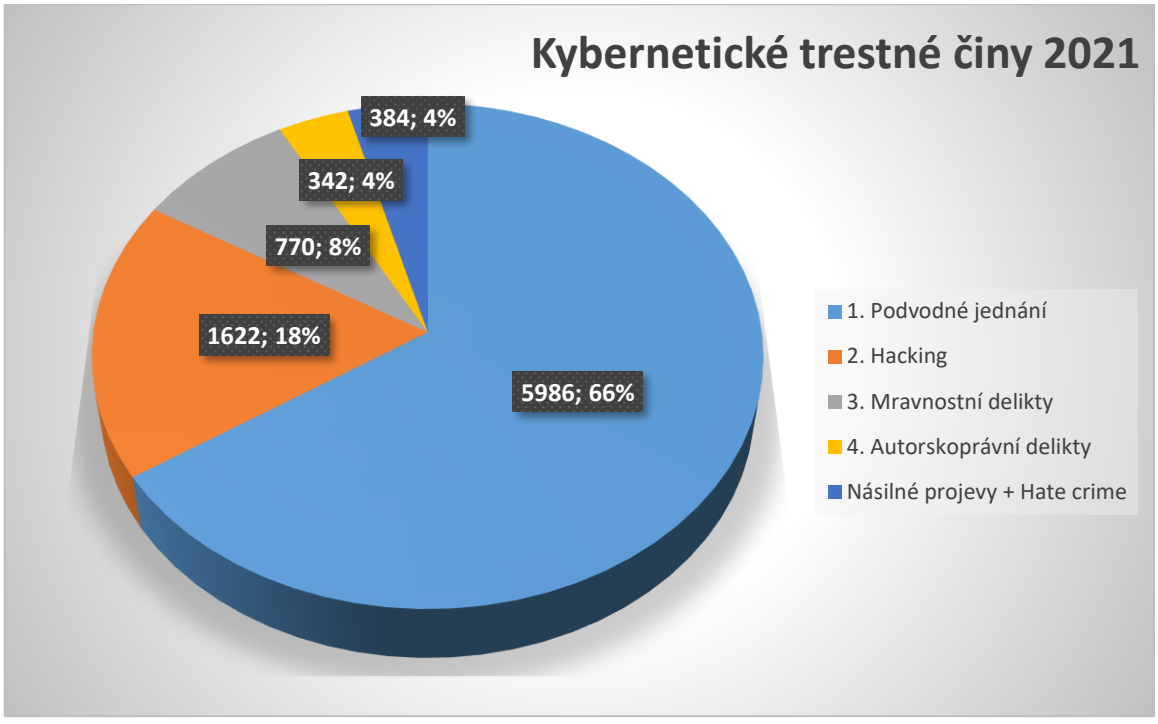
- Podvodná jednání
- Hacking
- Blagging
- Podvodné e-shopy
- Mravnostní delikty
- Trestné činy proti autorským právům
- Násilné projevy a tzv. hate crime

Nežli zahájíme charakteristiku všech výše uvedených kategorií kybernetických trestných činů, pro zajímavost si můžeme uvést názorný příklad toho, jaké konkrétní kybernetické trestné činy Policie ČR v rámci svých oddělení bojujících s kybernetickou kriminalitou musí nejčastěji vyšetřovat. Pro srovnání jsem vypracoval tři grafy, kde uvádím procentuální skladbu všech kybernetických trestných činů, které se udály na území České republiky ve srovnání s roky 2017, 2019, 2021 a které byly současně odhalené a aktivně řešené Policií ČR.



[12] *PČR. Jednotlivé druhy kyberkriminality* [online]. Praha (Česká republika) Policie České republiky, 2021. [2021-11-14] URL: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx





Grafy: Procentuální zastoupení jednotlivých kybernetických trestných činů v porovnání s roky 2017, 2019, 2021.
Zdroj: pcr.cz.

První kategorií kybernetických trestných činů, které jsou v bakalářské práci detailněji rozebrány, jsou **podvodná jednání**. V českých kruzích

se pak nejčastěji jedná o tzv. podvodné e-shopy, které vzniknou, mají ve své nabídce akční a výhodné zboží, a poté, co zákazníci za uvedené zboží zaplatí, e-shop zaniká. Typická je pro tyto e-shopy pouze krátká existence a také to, že finanční prostředky jsou po zrušení stránky přesunuty za hranice českého státu, aby tak došlo anonymizaci finančních toků. Na podobný způsob trestného jednání spoléhají i podvodné inzeráty, které se zejména v roce 2020 a 2021 hojně vyskytují na českém internetu. Dalšími trestnými činy, které jsou pachateli prováděny stejně, jsou i různé nadační sbírky nebo tzv. nigerijské podvody. Do této kategorie řadí Policie České republiky i podvodné e-maily a krádeže peněz prostřednictvím metody phishingu[13].

Další poměrně hojnou kategorii kybernetických trestných činů představuje činnost nazývaná hackerství neboli **hacking**. Hacking představuje v rámci kyberkriminality jeden z nejstarších typů trestné činnosti a můžeme si pod ním představit pronikání konkrétního jedince, který oplývá IT znalostmi, tzv. hackera, do konkrétního systému, sítě, osobního účtu nebo osobních dat jiných osob nebo organizací. Po proniknutí do „zaheslovaných“ a chráněných osobních kybernetických prostor může hacker libovolně využívat či zneužívat data, která jsou zde k dispozici (informace, dokumenty, citlivé fotografie či videa, finanční prostředky, osobní údaje, firemní údaje aj.)[14].

Blagging představuje podvodné kybernetické jednání, které využívá sociálního inženýrství a které se může týkat jak běžných uživatelů kyberprostoru, tak i velkých podniků či organizací. Jaký je princip tohoto poměrně rozšířeného podvodného jednání? Pachatelé osloví prostřednictvím e-mailu či jiné komunikační metody konkrétního jedince, vydávajíce se za jeho nadřízeného nebo za jinou osobu spřízněnou s konkrétní firmou s tím, že by potřebovali poskytnout nějaké soubory, informace, finanční prostředky atd. Pachatelé

[13]*PČR. Jednotlivé druhy kyberkriminality* [online]. Praha (Česká republika) Policie České republiky, 2021. [2021-11-14] URL: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx

[14]*McCARTHY, L, WELDON-SIVIY. D. Buď pánem svého prostoru*: jak chránit sebe a své věci, když jste online. 1 vydání, Praha: CZ. NIC, 2013. ISBN: 978-80-904248-6-9, s. 41.

povětšinou dobře znají fungování a vztahy v konkrétní firmě a z toho důvodu své oběti snadno manipulují, jelikož i zasílané zprávy mohou vypadat dosti reálně[15].

Velkou a opovrženíhodnou skupinu kybernetických trestných činů můžeme zahrnout do kategorie **mravnostních deliktů**. Činy proti mravnosti zahrnují všechny trestné činy, v rámci kterých dochází k oslovení dětí či mladistvých mladších 18 let věku, a to s cílem navázat s těmito osobami kontakt, spřátelit se a následně z nich vymámit citlivé fotografie nebo videa, nebo je dokonce přinutit k osobnímu setkání za účelem jejich sexuálního zneužití. Do této kategorie také řadíme vystavování citlivých fotografií nebo videí dětí či mladistvých, přeposílání těchto citlivých materiálů, umisťování těchto materiálů do kybernetického prostoru, distribuci jakýchkoli citlivých materiálů či dokonce jejich prodej[16].

V současné době jsou tímto způsobem získané materiály nejčastěji šířeny či směňovány v rámci uzavřených diskusních skupin, posílány v rámci osobních e-mailových zpráv nebo umisťovány na tzv. dark web. Do této skupiny trestných činů řadíme i další trestné činy, které jakýmkoli způsobem ohrožují a zneužívají osoby mladší 18 let věku (např. kuplířství, sexuální nátlak, obchodování s lidmi atd.)[17].

Další velmi rozmanitou a frekventovanou skupinu kybernetických trestných činů představují trestné činy mířené **vůči autorským právům**. Jedná se nejčastěji o sdílení hudebních skladeb, filmů a softwaru v rozporu s autorským právem šířeným v rámci webových velkokapacitních úložišť. Zjednodušeně a slangově jsou tyto trestné činy souhrnně nazývané jako „internetové pirátství“. Tato kategorie kybernetické kriminality je velice aktuální, vysoce frekventovaná a rozšířená v globálním měřítku. V České republice se porušením autorských práv

[15]*PČR. Jednotlivé druhy kyberkriminality* [online]. Praha (Česká republika) Policie České republiky, 2021. [2021-11-14] URL: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx
[16]*PČR. Jednotlivé druhy kyberkriminality* [online]. Praha (Česká republika) Policie České republiky, 2021. [2021-11-14] URL: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx
[17]*PČR. Jednotlivé druhy kyberkriminality* [online]. Praha (Česká republika) Policie České republiky, 2021. [2021-11-14] URL: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx

zaobírá *zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským*, který byl od svého vzniku již několikrát novelizován[18].

Poslední skupinu kybernetických trestných činů, o které se v této bakalářské práci zmíníme, můžeme nazvat „trestné činy prováděné **z nenávisti**“. Konkrétně však do této skupiny patří široké spektrum různých trestných činů, které mají jedno společné, a to již zmíněné šíření nenávisti, nabádání k nenávisti a šíření poplašných zpráv, které mají opětovně šířit mezi lidmi nenávist. Nenávist může být cílená vůči konkrétní rase nebo národnostní menšině, konkrétnímu náboženskému vyznání, konkrétní skupině lidí, politické skupině nebo konkrétní společnosti. Jedná se o šíření extremistických a radikálních myšlenek nebo šíření poplašných a nepravdivých informací, tzv. hoaxů[19].

1.3. Kybernetické hrozby

Výskyt a pohyb v kybernetickém prostoru s sebou přináší mnoho výhod, a to jak na úrovni jednotlivce, firmy nebo státu. Avšak přináší s sebou i mnoho různých bezpečnostních rizik a hrozeb, se kterými bychom měli dopředu počítat, chceme-li se v tomto prostoru pohybovat.

Při výčtu jednotlivých kategorií kybernetických trestných činů jsme si mohli povšimnout, že jednotlivé kybernetické hrozby a bezpečnostní rizika se týkají nejen běžných uživatelů všech věkových skupin, ale mohou se týkat i celých firem, nadnárodních podniků, států a dokonce mohou mít i globální dopad.

Jako běžný živitel kybernetického prostoru mohu své finanční prostředky snadno odeslat podvodným e-shopům s vidinou výhodného nákupu, mohu podlehnout výhodnému podvodnému inzerátu, můj bankovní účet může být napaden hackerem a svou firmu mohu přivést do problémů, nechám-li se zmanipulovat provozovatelem tzv. blaggingu.

I na úrovni státních útvarů nebo na mezinárodní úrovni je v současné době zapotřebí vysokého stupně ochrany proti kybernetickým útokům

[18]*Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským*.
[19]*PČR. Jednotlivé druhy kyberkriminality* [online]. Praha (Česká republika) Policie České republiky, 2021. [2021-11-14] URL: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx

a podvodům. Rozsáhlé útoky hackerů mohou nabourat státní síť, zneužít osobní údaje klientů bankovního sektoru či provádět špionážní machinace. Kybernetické útoky v současné době představují stále častější formu vedení konfliktů, která disponuje mnoha podstatnými výhodami, jsou nečekané a mohou být vedeny odkudkoliv.

I z toho důvodu disponují jednotlivé státy světa tzv. **kybernetickou obranou**, kterou rozumíme „*souhrn prostředků směřujících k zajištění ochrany kybernetického prostoru. Tyto prostředky mohou být různého charakteru – právní, organizační, vzdělávací, technické apod. Zjednodušeně řečeno, kybernetickou bezpečností se v tomto smyslu myslí zajištění důvěrnosti, integrity a dostupnosti informací a dat v kyberprostoru*.[20]“

[20]*VOJENSKÉ ZPRAVODAJSTVÍ. Kybernetická obrana* [online]. Praha (Česká republika) Ministerstvo obrany, 2016. [2021-11-21] URL: https://www.vzcr.cz/kyberneticka-obrana-46

2. Boj proti informační kriminalitě

V problematice boje proti kybernetické kriminalitě vystupuje v hlavní roli již zmíněný pojem „kybernetická bezpečnost“, která je definována jako „*souhrn organizačních, politických, právních, technických a vzdělávacích opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného a odolného kyberprostoru v České republice, a to jak pro subjekty veřejného a soukromého sektoru, tak pro širokou českou veřejnost.*[21]“

Jak lze vidět, v současné době existuje celá široká škála různých opatření a také velké množství různých orgánů, které se v rámci České republiky podílejí na boji proti kybernetické kriminalitě. Je důležité si také uvědomit, že tato opatření a orgány pracují jak na úrovni státní ochrany, na úrovni ochrany veřejných i soukromých subjektů, tak i na úrovni běžných uživatelů.

U zaměstnanců státního, veřejného sektoru i u běžných občanů jsou velmi důležitá různorodá preventivní opatření, která pomáhají eliminovat množství kybernetických trestných činů. Tyto programy jsou velmi často začleňovány do školních osnov a pomáhají lidem si již v útlém věku osvojit bezpečnostní prvky chování v rámci kyberprostoru.

Součástí zaměstnání lidí, kteří pracují s výpočetní technikou a moderními technologiemi, by měla být pravidelná školení o kybernetické bezpečnosti. Všeobecně jsou všechna preventivní opatření nejčastěji organizována Policií ČR a jejími experty zabývajícími se právě kyberkriminalitou nebo specializovanými organizacemi[22].

I přes četná preventivní opatření k výskytu kybernetických trestných činů dochází, a to stále častěji. Tyto trestné činy jsou evidovány na úrovni běžného uživatele kybernetického prostoru i na úrovni národní. A musíme si uvědomit, že při boji proti kybernetické kriminalitě stojí proti vyšetřujícím orgánům

[21]*PČR. Kyberkriminalita* [online]. Praha (Česká republika) Policie České republiky, 2019. [2021-11-18]. URL: https://www.policie.cz/clanek/kyberkriminalita.aspx
[22]*PČR. Prevence kyberkriminality* [online]. Praha (Česká republika) Policie České republiky, 2021. [2021-11-18] URL: https://www.policie.cz/clanek/prevence-kyberkriminality.aspx

mnoho podstatných aspektů zvýhodňujících právě pachatele kybernetické trestné činnosti[23]:

- Digitální stopy jsou mnohdy neviditelné, nestálé, značně rozsáhlé a dynamické, tedy proměnlivé v čase i místě spáchání skutku.
- Důkazní materiál kybernetických trestných činů mnohdy nelze zajistit.
- Oběti i pachatele informační kriminality nelze často vystopovat.
- Škody způsobené kybernetickou kriminalitou se obtížně zjišťují a vyčíslují.
- K zajištění, analýze a zkoumání digitálních stop jsou nutní vysoce kvalifikovaní policisté vybavení speciálním softwarem a hardwarem.
- Problémem jsou dlouhé prodlevy, které souvisí s rychlostí a relativní nepozorovatelností počítačového incidentu. Kvalita a včasnost zajištění digitálních stop přitom zásadně rozhodují o úspěchu vyšetřování.
- Legislativní rámec vyšetřování kybernetické kriminality je dosud nedokonalý, stále existují spíše fragmenty právních norem včetně trestního práva hmotného.
- Data se ukládají do struktur počítačových sítí. Data je proto třeba analyzovat přímo na místě činu.
- Používá se šifrování dat kvalitními algoritmy, které je velmi obtížné nebo dokonce nemožné prolomit.
- Rozšiřuje se využívání malé a mobilní digitální techniky, kde jsou data uložena v pamětech mikropočítačových systémů a je obtížné je podrobit analýze.

I přes velké množství aspektů, které hrají v neprospěch orgánů bojujících proti kyberkriminalitě, pomáhají právě orgány zajišťující kybernetickou bezpečnost identifikovat, analyzovat a řešit hrozby přicházející z kyberprostoru. Orgány v této problematice činné se dále snaží snižovat kybernetická rizika, eliminovat dopad kybernetických hrozeb na konkrétní uživatele a posilovat věrohodnost, bezpečnost a dostupnost dat informační infrastruktury. Hlavním

[23] *POŽÁR, J HNÍK, V. 2018. Specifické problémy boje s kybernetickou kriminalitou*. Policejní akademie ČR v Praze.

důvodem a cílem celé kybernetické bezpečnosti je ochrana kybernetického prostředí k realizaci informačních práv každého člověka[24].

2.1. Orgány bojující proti informační kriminalitě v rámci ČR

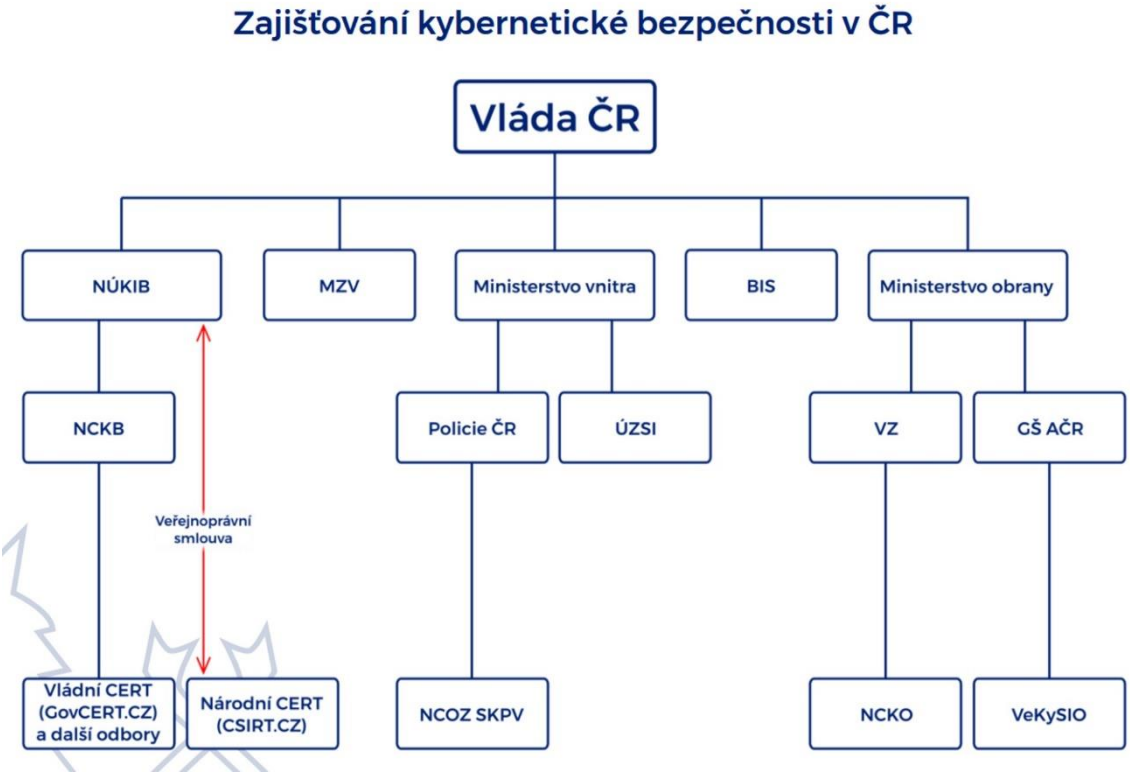
V rámci této kapitoly se budeme věnovat orgánům, které bojují proti kybernetické kriminalitě na území České republiky. Jelikož je naše země členskou zemí Evropské unie, vztahují se na ni i evropské regule a vyhlášky o kybernetické bezpečnosti.

Všechny členské státy Evropské unie přijaly roku 2020 novou podobu **Strategie kybernetické bezpečnosti EU**, jejíž primární cíl představuje zvýšení kybernetické odolnosti Evropy a zajištění toho, že každý občan Evropské unie bude moci bez potenciálního bezpečí využívat kybernetický prostor. V tomto dokumentu se nachází velké množství konkrétních návrhů na zavedení regulačních, investičních a politických nástrojů[25].

Jak můžeme vidět na Obr. 4, kybernetická bezpečnost České republiky je zajišťována i různými orgány samotné české vlády. Těchto orgánů je velké množství a každý se na boji proti kyberkriminalitě podílí z trochu jiného úhlu pohledu.

[24] *NÚKIB. Národní strategie kybernetické bezpečnosti ČR na období let 2015–2020* [online]. Praha (Česká republika) Národní ústav pro kybernetickou a informační bezpečnost, 2015. [2021-12-3] URL: https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/

[25] *RADA EU. Kybernetická bezpečnost: Jak EU řeší kybernetické hrozby* [online]. Praha (Česká republika) Rada Evropské unie, 2020. [2021-12-3] URL: https://www.consilium.europa.eu/cs/policies/cybersecurity/



Obr. 3: Kybernetická bezpečnost ČR.

Zdroj: itsec-nn-com

Nejvyšším postavením v boji proti kybernetické kriminalitě disponuje Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Ten pak řídí CERT (Cyber Emergency Response Team) a CSIRT bezpečnostní týmy. Dále pak Národní úřad pro kybernetickou a informační bezpečnost řídí Ministerstvo vnitra, pod jehož orgány patří Policie ČR a Ministerstvo obrany, a pod jeho správu patří Bezpečnostní složky ČR (i Informační a kybernetickou sílu). Své zásluhy na boji proti kybernetické kriminalitě má i BIS (Bezpečnostní informační služba) a MZV ČR (Ministerstvo zahraničních věcí ČR).

Mimo zmíněných nadnárodních strategických opatření je kybernetická bezpečnost ukotvena i v českých právních normách, tedy **v českých zákonech**. Konkrétních zákonů, které se zabývají různými formami kybernetických trestných činů, existuje hned několik (paragraf 230 a 231 trestního zákoníku (hacking, odposlechy, zásahy do dat), zákon č. 121/2000 Sb. (autorský zákon), zákon č. 127/2005 Sb. (o elektronické komunikaci), zákon č. 101/2000 Sb. (o ochraně osobních údajů), aj.).

Problémem právních systémů všech evropských i světových zemí je, že nejsou pravidelně a dostatečně rychle aktualizovány, a kybernetické trestné činy v nich nejsou řešeny komplexně. To pak ztěžuje postup **Policie ČR** a jejich odborně vzdělaným oddělením (kybernetickými oddíly) zaměřeným právě na boj proti kybernetickým zločinům[26].

Jelikož jsou jednotlivé státy mnohem častěji terčem kybernetických bojů nežli bojů pozemních, přibyla roku 2009 další složka Obranných sil České republiky, kterou nazýváme **Informační a kybernetické síly České republiky**. Úkoly této moderní a specifické bezpečnostní složky spočívají především v monitorování, plánování a vedení operací v rámci kybernetického prostoru a informačním prostředí na taktické úrovni. Dále je to podpora plánování a řízení strategické komunikace. Kybernetické síly dále disponují schopností podporovat vedení informačních operací v rámci operační a strategické úrovně a vést plné spektrum psychologických operací a civilně vojenské spolupráce[27].

Prvořadým důvodem pro vznik této specifické obranné složky je ochraňovat kybernetický prostor České republiky a všech jejích významných kybernetických objektů. Tato složka se také podílí na ochraně evropského kybernetického prostoru, čímž dodržuje předpisy Evropské unie. Obrana kybernetického prostoru souvisí i s pravidelným poskytováním informací a analýz o kybernetickém prostoru, jeho jednotlivých prvcích a aktérech, za vytvoření společného evropského operačního obrazu[28].

Nejvýznamnějším orgánem kybernetické bezpečnosti České republiky je **Národní úřad pro kybernetickou a informační bezpečnost**, který je znám pod zkratkou NÚKIB. NÚKIB představuje „*ústřední správní orgán pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany*“[29]. Tento státní

[26] *POŽÁR, J HNÍK, V. 2018. Specifické problémy boje s kybernetickou kriminalitou*. Policejní akademie ČR v Praze.
[27] *HAVLÍK, M. Příčiny vzniku a začlenění kybernetických sil a informačních operací do Armády České republiky* [online]. Brno (Česká republika) Vojenské rozhledy, 2020. [2021-12-3] UR: https://www.vojenskerozhledy.cz/kategorie-clanku/strategicke-rizeni/zacleneni-kybernetickych-sil
[28] *HAVLÍK, M. Příčiny vzniku a začlenění kybernetických sil a informačních operací do Armády České republiky* [online]. Brno (Česká republika) Vojenské rozhledy, 2020. [2021-12-3] UR: https://www.vojenskerozhledy.cz/kategorie-clanku/strategicke-rizeni/zacleneni-kybernetickych-sil
[29] *NÚKIB. Co je NÚKIB* [online]. Praha (Česká republika) Národní úřad pro kybernetickou a informační bezpečnost, 2017. [2021-12-5] URL: https://nukib.cz/cs/o-nukib/

úřad vznikl v roce 2017, a to na základě zákonu 205/2017 Sb., o kybernetické bezpečnosti[30].

Výše zmíněný státní úřad však nepředstavuje organizaci, která by se zaobírala jednotlivými kybernetickými útoky běžných uživatelů. Tento úřad jedná na národní a mezinárodní úrovni. Avšak pod jeho křídly se již nacházejí organizace, které se zaobírají i konkrétními počítačovými útoky směrovanými vůči běžným uživatelům. Těmito organizacemi jsou pak především bezpečnostní týmy typu CERT (Computer Emergency Response Team) a bezpečnostní týmy typu CSIRT (Computer Security Incident Response Team)[31].

Ačkoliv se výše uvedené bezpečnostní týmy ve svých primárních úkonech poněkud liší, můžeme je charakterizovat stejně, a to jako **„***tým, který je ve svém jasně definovaném poli působnosti zodpovědný za řešení bezpečnostních incidentů, z pohledu uživatelů nebo jiných týmů tedy místo, na které se mohou obrátit se zjištěným bezpečnostním incidentem nebo i jen podezřením*“[32].

[30]*PČR. Prevence kyberkriminality* [online]. Praha (Česká republika) Policie České republiky, 2021. [2021-12-5] URL: https://www.policie.cz/clanek/prevence-kyberkriminality.aspx
[31]*PČR. Prevence kyberkriminality* [online]. Praha (Česká republika) Policie České republiky, 2021. [2021-12-5] URL: https://www.policie.cz/clanek/prevence-kyberkriminality.aspx
[32]*PČR. Prevence kyberkriminality* [online]. Praha (Česká republika) Policie České republiky, 2021. [2021-12-5] URL: https://www.policie.cz/clanek/prevence-kyberkriminality.aspx

3. Sexuální a mravnostní trestné činy

V této části informační kriminality rozebereme konkrétní zločiny, jimiž jsou sexuální a mravnostní trestné činy. Mravnostní trestné činy nemůžeme vysvětlovat výhradně jako mravní otupělost, ani je nemůžeme chápat jako zvýšený pud na sexuální podněty při snížené ovládací a rozpoznávací schopnosti. Velký podíl na této kriminalitě mají osoby, které jsou z tohoto pohledu zcela „zdravé“, které nemají po psychiatrickém ani psychologickém vyšetření zjištěnou žádnou sexuální odchylku. Faktem však je, že podstatná část osob, u kterých je odhalena tato delikvence a u kterých je zjišťována sexuálně patologická motivace, zasahuje mimo vývojové vady i do špatné nebo nedostatečné mravní, sexuální, obecně pak do společenské výchovy. [33]

Mravnostní trestné činy zasahují čtyři základní roviny, a těmi jsou:

a) morální vztahy ve společnosti

b) život a zdraví člověka poškozených v důsledku protiprávního jednání ve sféře sexuálních vztahů

c) zdravý vývoj mládeže

d) dobré mravy v sexuálních vztazích mezi dospělými

3.1. Definice sexuální a mravnostní trestné činy

Jde o trestné činy vyjmenované zejména v třetí hlavě zvláštní části trestního zákoníku, kde se jedná o paragrafy § 185-193b trestního zákoníku. Tyto trestné činy zasahují důstojnost oběti v sexuální oblasti.[34]

Do této skupiny patří zejména trestné činy:

a) ohrožující svobodu rozhodování v oblasti pohlavního života – znásilnění a sexuální nátlak

[33] *Články: Otázky spojené s mravnostní trestnou činností* [online]. Praha (Česká republika) Právní prostor, 28. 5. 2014. [2021-12-15] URL: https://www.pravniprostor.cz/clanky/trestni-pravo/otazky-spojene-s-mravnostni-trestnou-cinnosti-ii-cast

[34] *Článek: PČR. Sexuální a mravnostní trestné činy* [online]. Praha (Česká republika) Policie České republiky, 2021. [2022-01-6] URL: https://www.policie.cz/clanek/sexualni-a-mravnostni-trestne-ciny.aspx

b) ohrožující zdravý mravní a tělesný vývoj dětí – například pohlavní zneužití nebo svádění dítěte k pohlavnímu styku a zneužití dítěte k výrobě pornografie
c) ohrožující některé mravní zásady – například výroba a jiné nakládání s dětskou pornografií, kuplířství[35]

3.2. Útoky pachatele v kyberprostoru

Pachatelé se dopouštějí útoků na své oběti nejčastěji ze svých domovů, z bezpečných míst, kde se připojují do sítě internet. Odtud skrze nejrůznější sociální sítě jako je Instagram, Facebook, Messenger, WhatsApp, Twitter, Snapchat, Telegram, Pinterest, Youtube, Tik-Tok, Google+ a mnoho dalších vystupují pod různými uživatelskými profily s falešnými přezdívkami a snaží se nalákat osoby (v tomto případě oběti), které vyhoví jejím požadavkům. Často se vydávají za osoby opačného pohlaví, aby tak lépe navázali kontakt s vyhledanou obětí. Na začátku navazují zcela jednoduchou komunikaci ve stylu „ahoj, jak se máš, co zrovna děláš, máš sourozence, kde pracují rodiče, jak často jsou doma“, čímž získávají přehled o tom, v jakém zázemí se dítě doma nachází. Většinou se jedná o děti z rodin, kde rodiče s dětmi netráví moc času. Pachatel se tak pasuje do role dobrého kamaráda či kamarádky, který je vyslechne a buduje si tak jejich důvěru. Jednou z možností, jak se může dítě dostat do jednoduché komunikace, jsou právě i síťové hry, jako například World of Tanks, Forge of Empires, Scarlet Fate, Big Farm, Taonga, Total Battle a mnoho dalších, kde děti navazují kontakt pomocí chatu ve hře. Následně si pak vymění své kontakty a začnou si psát na sociální síti WhatsApp, Skype nebo Messenger. Děti si zakládají své účty na Facebooku i v době, kdy jim ještě nebylo třináct let, přestože jim to společnost Facebook nedovoluje. Oni si však zadají při vytváření účtu jiné datum narození a mohou si tak účet bez problému vytvořit. Rodiče většinou ani netuší, že si jejich děti nějaký účet založily a vesele si chatují a sdílejí své fotografie a příběhy z rodinných dovolených nebo své „stories“ ze školy a podobně. V internetové síti je neomezené množství možností, můžeme se spojit s kýmkoliv přes cokoliv, jsme

[35] *Článek: PČR. Sexuální a mravnostní trestné činy* [online]. Praha (Česká republika) Policie České republiky, 2021. [2022-01-6] URL: https://www.policie.cz/clanek/sexualni-a-mravnostni-trestne-ciny.aspx

propojeni ve všech možných aplikacích, účtech, všude, kde se pohybujeme online, zanecháváme stopu. V dnešní době je tak pro pachatele velmi snadné zaútočit na kohokoliv, odkudkoliv a kdykoliv.

Tento typ kyberkriminality je páchán zejména na obětech od 6 do 15 let věku. Jedná se tedy o děti, které jsou zvlášť zranitelné a je třeba je chránit. Nemluvíme zde jen o dívkách, na kterých jsou páchány tyto kyberútoky, tato kriminalita je páchána i na chlapcích, a to v čím dál větším počtu. Pachatelé si je často vybírají kvůli jejich nevědomosti a ovlivnitelnosti, a tím tak snadněji dosáhnou svého cíle dostat z obětí citlivé fotografie či videa. Tyto si pak ukládají na své pevné disky, externí disky, zakládají si složky se jmény obětí. Pod výhružkou zveřejnění takového obsahu jejich blízkým pak nutí oběti k další spolupráci. Intence komunikace ze strany pachatele se neustále zvyšuje. Potřeba online spojení s obětí je tak silná, že jsou nuceny v jakémkoliv volném čase navázat video hovor či textovou komunikaci a plnit pachatelovu vůli. Touha pachatele po četné komunikaci se pak stává klíčem k jeho odhalení, kdy udivení rodiče, proč jejich dítěti pořád zvoní tablet, notebook nebo na rodinném stolním počítači neustále vyzvání Skype, nachází komunikaci a sdílený obsah s pachatelem a následně dochází k oznámení na policii.

3.3. Oběti

Kdo je zvlášť zranitelná oběť a co to znamená

Obětí sexuálního trestného činu se může stát kdokoli, muž i žena, bez ohledu na věk, vyspělost, způsob života, pověst, vzdělání, zkušenosti, zájmy atd. A také bez ohledu na to, zda jde o osobu pohlavně nedotčenou, či ne. Některé oběti trestných činů v sexuální oblasti jsou považovány dle zákona o obětech trestných činů za zvlášť zranitelné. Jde o děti, hendikepované osoby a další osoby, u kterých je zvýšené nebezpečí způsobení druhotné újmy, zejména s ohledem na jejich věk, pohlaví, rasu, národnost, sexuální orientaci, náboženské vyznání, zdravotní stav, rozumovou vyspělost, schopnost vyjadřovat se, životní situaci, v níž se nachází, nebo s ohledem na vztah k osobě podezřelé ze spáchání trestného činu nebo závislosti na ní. Za zvlášť zranitelné oběti jsou považovány také oběti trestného činu obchodování s lidmi. Zvlášť zranitelné oběti jsou takové oběti, u

kterých existuje vyšší nebezpečí způsobení tzv. druhotné újmy nebo zastrašování ze strany pachatele. Tyto oběti také mohou být zvláště náchylné k prohloubení prožívaného stresu a citového zranění v důsledku samotné účasti v trestním řízení, například při výslechu. Zákon proto stanoví speciální opatření pro zabránění prohlubování stresu oběti a snížení nebezpečí druhotné újmy, viktimizace.[36]

Jaké dopady může mít trestný čin na oběť

Prožívání újmy u obětí je velmi individuální. Záleží na mnoha faktorech, ke kterým patří mimo jiné charakter a okolnosti spáchaného trestného činu, či vztah oběti k pachateli, ale také vlastnosti oběti, její věk a jiné. Oběti trestných činů v sexuální oblasti často prožívají zejména psychickou a emocionální újmu. V reakci na prožitou traumatizující událost se u nich mohou objevovat nejrůznější pocity, jako je například vztek, šok, strach, pocit ponížení, stud, pocity bezmoci a bezradnosti. V důsledku této události mohou oběti trpět různými psychickými a fyziologickými obtížemi, ke kterým patří například výrazné změny nálad, návaly úzkosti, zvýšená podrážděnost, nesoustředěnost, ostražitost, stažení se ze sociálních kontaktů, ztráta chuti k jídlu, poruchy spánku, nespecifické bolesti zad, břicha a podobně. Příznaky mohou být velmi rozmanité a mohou se objevit bez ohledu na to, zda byla oběti trestným činem způsobena také újma fyzická. V některých případech mohou psychické příznaky přetrvávat dlouhodobě a rozvinout se v takzvanou posttraumatickou stresovou poruchu. Proto je důležité včas vyhledat odbornou pomoc.[37] Tu mohou hledat v registru poskytovatelů pomoci obětem trestných činů. Registr poskytovatelů pomoci obětem trestných činů obsahuje seznam organizací a dalších subjektů, které pomáhají obětem vyrovnat se s následky trestného činu. Jedná se o subjekty poskytující sociální služby, které poskytují psychologické a sociální poradenství, akreditované

[36] *Článek: PČR. Sexuální a mravnostní trestné činy* [online]. Praha (Česká republika) Policie České republiky, 2021. [2022-01-6] URL: https://www.policie.cz/clanek/sexualni-a-mravnostni-trestne-ciny.aspx

[37] *Článek: PČR. Sexuální a mravnostní trestné činy* [online]. Praha (Česká republika) Policie České republiky, 2021. [2022-01-6] URL: https://www.policie.cz/clanek/sexualni-a-mravnostni-trestne-ciny.aspx

subjekty poskytující právní informace a restorativní programy, advokáti, kteří poskytují právní pomoc a střediska probační a mediační služby, které poskytují právní informace, psychosociální podporu a restorativní programy.[38] Organizace poskytující pomoc jsou: Bílý kruh bezpečí, ROSA, Linka bezpečí, Dětské krizové centrum, Charita Česká republika, Policie ČR, probační a mediační služba.

[38] *Justice.cz – registr poskytovatelů pomoci obětem trestných činů* [online]. Praha (Česká republika) Ministerstvo spravedlnosti ČR, 2017. [2022-01-6] URL: https://www.justice.cz/web/msp/rozvoj-sluzeb-pro-obeti-trestne-cinnosti?clanek=registr-poskytovatelu-pomoci-obetem-trestnych-cinu

4. Praktická část

V praktické části této práce proberu případovou studii. Tato studie je založena na skutečném případu řešeném policií Jihomoravského kraje, oddělením kybernetické kriminality v letech 2013 až 2020. Jedná se o kybernetický útok kvalifikovaný jako trestný čin, konkrétně § 186 sexuální nátlak, § 201 ohrožování výchovy dítěte a § 192 výroba a jiné nakládání s dětskou pornografií. Za tyto skutky hrozí pachateli trest odnětí svobody až ve výši osmi let. Nastíním v této studii postup orgánů policie při odhalování a vyšetřování daného případu. Budou zde uvedeny úkony od zahájení trestního řízení, přes návrh státního zástupce na podání obžaloby až k samotnému řízení před soudem. Následně uvedu, jakým způsobem bylo provedeno vyšetření pachatele soudním znalcem ze sexuologického oddělení psychiatrické léčebny. Zda bylo toto vyšetření správně vyhodnoceno a zda byl udělen dostačující trest. V návaznosti na tento výrok se pak zaměřím na následnou nápravu pachatele. Z důvodů utajovaných informací vyplývajících ze spisu zde nebudou uvedena skutečná jména ani jména profilů a další citlivé informace. Některé věci budou vynechány nebo upraveny tak, aby nedošlo k porušení zákona o utajovaných informacích.

4.1. Případová studie

V našem případu, který zde rozebereme, se podíváme na pachatele, který na své oběti vyvíjel nátlak a vymáhal na svých obětech, aby se mu obnažovaly před webovou kamerou a sdílely s ním fotografie v sexuálních pózách. Tato osoba bude vystupovat v našem případu pod uživatelským profilem „AHA“ a oběť, nezletilá, která má uživatelský profil „xxxx“. Jedná se o případ, který byl řešen v letech 2013 až 2015 Oddělením Kybernetické kriminality v Brně a s jejich svolením a odborným dohledem si zde detailně popíšeme, jak celý incident probíhal. Od samého počátku, kdy začalo řešit tento případ Obvodní oddělení, které začalo s šetřením a následně vyhodnotilo, že se jedná o závažný trestný čin sexuálního nátlaku, předalo tento případ Krajskému Oddělení Kybernetické kriminality. Tímto správným a rychlým krokem tak umožnilo pokračování

vyšetřování případu oddělením, které má dobrou vybavenost, odbornost, dobře stanovené a pružné postupy k odhalování pachatelů této trestné činnosti. V tomto případě mohu říci, že vyhodnocení případu a postoupení věci z úrovně Obvodního oddělení na úroveň krajskou vedlo následně k odhalení a potrestání pachatele. Ve vyšetřování Krajským Oddělením Kybernetické kriminality byly zvoleny a učiněny velmi dobré a rychlé kroky. Žádosti o výpisy uskutečňovaných telekomunikačních provozů i žádosti k nařízení sdělení údajů ze strany společnosti Seznam.cz, tak i společnosti Nej TV a.s. proběhly v reálných časových intervalech. Ne vždy je totiž možné získat potřebná data včas. Čas je při získávání dat asi jediným záporným aspektem ve vyšetřování. Součinnost policie a postup Státního zástupce přivedl celý případ až k soudu, kde byl pachatel shledán vinným a odsouzen. Velmi dobře odvedená práce státních orgánů společnosti ulehčila od kriminálně závadové osoby. Přestože byl v případu dle mého názoru uveden ze strany znalce z odvětví psychiatrie špatný posudek o možnosti ambulantního léčení, který nevedl k nápravě pachatele, ale naopak k jeho recidivě, bylo spravedlnosti učiněno zadost a následným rozhodnutím soudu byl přeměněn na formu ústavního léčení. Veškerá jména a uživatelské profily, které zde budou uvedeny, jsou smyšlené a v případu skutečně nefigurují. Z důvodů utajovaných informací, které ze spisu vyplývají, a které však nemohou být uveřejněny, budou vynechány nebo pozměněny.

4.2. Vyšetřování policie

Dne 10. 06. 2013 byl na obvodním oddělení sepsán úřední záznam o podání vysvětlení, kdy oznamovatelkou byla matka poškozené osoby. Záznam o podání vysvětlení byl požadován z důvodu odhalení trestného činu nebo přestupku a jeho pachatele ve věci Kontaktování nezletilé prostřednictvím sociální sítě Skype. Po prvotním oznámení oznamovatelkou poškozené osoby učinila Policie České republiky následující úkony:

Úřední záznam o podání vysvětlení - v tomto záznamu uvedla matka, že v sobotu večer, když seděla u jejich notebooku, byl zapnutý Skype a na něj neustále volala nějaká osoba, která užívá na Skypu jméno „AHA“. Tato osoba byla velmi neodbytná a oznamovatelka několikrát její volání ukončila. Druhý den byla

matka zvědavá, kdo to byl ten den předtím tak neodbytný, otevřela notebook a podívala se do historie konverzace, kde zjistila, že její dcera komunikuje s osobou užívající profil „AHA“. V této konverzaci zjistila, že se tato osoba s její dcerou baví tak, že jí navádí, aby se hladila na různých místech těla, intimních místech, aby se svlékala, ukazovala se na kameru. Je tam napsané i to, že když si ho vymaže, tak rozešle fotky, které si udělal z toho, jak se ukazovala na kameru, všem přátelům na Facebooku. Poté si matka zavolala svoji dceru, aby jí vysvětlila, co to má znamenat. Na to jí odpověděla, že ví, o co jde, že na tuto osobu dostala kontakt od její spolužačky. Dále sdělila, že tam nějaké fotky dala, ale proč to udělala, nedokázala vysvětlit. Matka dále uvedla, že má podezření, že by tato osoba mohla ohrožovat jak její dceru, tak i jiné děti.[39]

Usnesení o zahájení trestního stíhání dle § 160/1 tr. ř.

Úřední záznam o vydání věci - a to notebooku poškozené, k získání potřebných dat, neboť šlo o důležitou věc pro řízení.

Protokol o výslechu svědka - v tomto případě osoby mladší patnácti let, který byl sepsán s poškozenou. Tato do protokolu uvedla následující: „Bydlím v rodinném domě, kde mám svůj pokoj a taky svůj počítač. Používám Facebook, Twitter, Ask.Fm, dále používám Skype, který máme v rodině všichni dohromady. Jen jednou jsem si psala přes Skype s někým, koho vůbec neznám. Moje kamarádka mi poslala jeden profil, o kterém jsme si mysleli, že je to profil našeho společného kamaráda, kterého známe z dřívějška. Měl kontakt pod jménem Thomas, o kterém jsme si mysleli, že je to on. On si nejdříve volal nebo psal s tou mojí kamarádkou a ona ten kontakt potom dala mně, protože si myslela, že je to on. Já jsem si s ním psala i volala přes Skype. Odhaduji, že to začalo někdy v prosinci, ale přesně to nevím. Zpočátku jsme si normálně psali. Pak jsme si volali přes Skype a on si asi vyfotil můj obličej. Já jsem měla web kameru, ale on asi ne, protože já jsem ho neviděla. Ale podle hlasu opravdu zněl jako ten můj kamarád, ale zřejmě si měnil hlas pomocí aplikace. Já jsem mu o sobě řekla jméno i příjmení, mám to uvedené i v profilu. Jiné údaje k mé osobě tam uvedené nemám. Kolik mi je let jsem mu neříkala ani nepsala. On se na to neptal. Na Facebooku mám uvedeno staré bydliště. Na Facebooku narození mám, ale ne svoje, protože

[39] *Trestní spis*. Číslo spisu Č. J. KRPB – 141793/TČ-2013-060079

Facebook je až od třinácti let, a když jsem si ho zakládala, tak mi ještě třináct nebylo. Takže jsem tam musela dát jiné datum narození. Na Skype jsem se přihlašovala pod jménem „xxxx“. Ten kamarád, nebo alespoň jsem si myslela, že je to kamarád, se přihlašoval pod jménem „AHA“. Při naší komunikaci jsem měla zapnutou webku. Žádné fotky jsem mu ale neposlala. My jsme si volali přes webkameru a on viděl můj obličej, a pak mi napsal, že si ten obličej vyfotil a že si ho nějak upraví a dá ho na internet upravený. Já jsem mu napsala, že nechci, aby ho někam dával. On mi napsal, že ho nikam nedá, pokud si s ním budu volat častěji. A to jsem poznala, že to není ten můj kamarád, protože ten by to nenapsal. Potom jsem si s ním často volala, aby ten můj obličej nikam neumístil. Volat jsem si s ním nechtěla, ale byla jsem dost často na počítači, a on jak se přihlásil, tak mi hned volal. Já jsem to vypínala, ale on hned začal s tou fotkou, tak jsem s ním musela telefonovat. Chtěl po mě, abych se svlékala, musela jsem si sundávat tričko, pak i kalhotky, pak chtěl, abych se svlékla celá. To mi psal hodněkrát. Párkrát jsem se opravdu svlékla, bála jsem se, aby někam neumístil tu fotku. Chtěl taky, abych na sebe na ta obnažená místa namířila i web kameru. Potom mi vyhrožoval, že mě vyfotil, jak jsem vyslečená, a takovou fotku umístí někde na sociálních sítí. To jsem samozřejmě nechtěla, tak jsem dělala, co po mě chtěl. O této komunikaci jsem nikomu neřekla, přišli na to až rodiče. Neřekla jsem to ani té své kamarádce. Jen jsem jí řekla, aby si ho smazala, že to není on, kdo si myslíme. Ona mi neříkala, že by s ní vedl takovou komunikaci jako se mnou. Jen říkala, že si s ní píše. Dřív mi psal i na Facebooku, potom psal jen na Skype. Jinak holkám ze třídy taky psal, chtěl, aby mu ukázaly nohy nebo tričko.“[40]

Protokol o zajištění dat – byl proveden technický úkon spočívající ve vyhotovení bitové kopie pevného disku.

Protokol o zpřístupnění dat – smazaná data bitové kopie zajištěného pevného disku byla obnovena na technologický pevný disk.

Žádost o poskytnutí informací dle § 8 odst. 1 trestního řádu – dožádání společnosti Seznam.cz o výpis uskutečněného telekomunikačního provozu emailové schránky

[40] *Trestní spis*. Číslo spisu Č. J. KRPB – 141793/TČ-2013-060079

Neznámý pachatel – návrh na vydání příkazu soudu ke zjištění údajů o telekomunikačním provozu

Příkaz ke sdělení údajů o uskutečněném telekomunikačním provozu okresním soudem

Úřední záznam – na základě telefonické žádosti byla pracovníky OOK provedena prověrka v místě bydliště možného podezřelého.

Příkaz k domovní prohlídce – Okresní soud nařídil na základě žádosti státního zástupce Okresního státního zastupitelství na vydání příkazu k domovní prohlídce domovní prohlídku bytu včetně prostor k bytu přináležejícím. Domovní prohlídka byla provedena jako neodkladný a neopakovatelný úkon s ohledem na charakter šetřené trestné činnosti a nutnosti zajistit důkazní prostředky před zahájením trestního stíhání.

Protokol o vydání věci – k vydání výpočetní techniky nacházející se v bytě podezřelého, kdy se jedná o jeden kus notebooku, jeden kus stolního počítače a externího USB HDD.

Protokol o zajištění dat – vyhotovení bitové kopie pevných disků, zajištěných u podezřelé osoby

Protokol o ohledání dat – zajištění všech používaných profilů podezřelé osoby a profilů kontaktovaných osob.

Usnesení – podle § 160 odstavce 1 trestního řádu se zahajuje trestní stíhání osoby vystupující pod profile „AHA“[41]

Protokol o výslechu obviněného – vyjádření obviněného k věci

„To, co je napsáno v usnesení, které jsem převzal poštou, je pravda. Je pravda, že jsem měl profil na Skypu pod jménem „AHA“ a měl jsem ho proto, abych se bavil s holkama o sexu. Moc si na to nevzpomínám, ale je pravda, že jsem se tam bavil s holkou, která měla profil „xxxx“. Bavila se tam se mnou o všem, i o sexu a ukazovala se mi nahá na webku. Jen jednou se stalo, že se mi nechtěla ukázat a tak jsem jí vyhrožoval, že jsem ji před tím vyfotil, jak se mi ukazovala a že ty fotky dám na internet. Ve skutečnosti jsem ji ale vůbec nevyfotil a ani jsem nijak nezaznamenával tu video komunikaci. Vůbec jsem neměl v úmyslu to na internet dát. Stalo se to skutečně jen jednou. Je pravda, že jsem se takto sexuálně

[41] *Trestní spis*. Číslo spisu Č. J. KRPB – 141793/TČ-2013-060079

bavil i s jinýma holkama, ale nic podobného jsem žádné další neudělal. Na otázku, proč jsem to dělal, bych řekl, že to bylo v době, kdy jsem se hodně hádal s přítelkyní a moc nám to neklapalo, tak jsem chodil na net, protože jsem nechtěl přítelkyni podvádět v reálu. Když jsem tam s někým navázal kontakt, tak to skutečně byly mladší holky. Vyloženě jsem nevyhledával malé holky, na to nejsem a necítím se jako nějaký pedofil. K tomu, že jsem původně řekl, když u mě byla v létě policie a vydával jsem ty počítače, že jsem už dlouho na profilu „AHA“ nebyl, tak to nebyla pravda. Ve skutečnosti jsem tam komunikoval ještě předtím. Uvědomil jsem si, že to, co jsem dělal, byla velká hloupost a lituji toho. Co nejdříve navštívím sexuologii a chci se léčit. Jsem si vědom a byl jsem upozorněn, že v případě, kdy bych v trestné činnosti jakkoli pokračoval, tak bych mohl být vzat do vazby.[42]

Protokol o výslechu svědka – výslech svědka otce obviněného

Protokol o výslechu svědka – výslech svědka matky poškozené

Poučení poškozeného – oběti trestného činu v trestním řízení

Poučení o poskytování informací o trestním řízení a osobách na něm zúčastněných

Protokol o výslechu svědka – výslech svědka otce poškozené

Opatření – podle § 105 odst. 1 trestního řádu s odkazem na ustanovení § 116 odst. 1 trestního řádu se přibírá znalec z oboru psychiatrie Sexuologického oddělení Psychiatrické léčebny.

Znalecký posudek – na duševní stav a sexualitu obviněného

Návrh na podání obžaloby – podle § 166 odst. 3 trestního řádu po skončení vyšetřování předkládán spis s návrhem na podání obžaloby proti obviněnému ze spáchání:

1) Zločinu sexuální nátlak dle § 186, odst. 1, odst. 5, písm. a) trestního zákoníku a přečinu ohrožování výchovy dítěte dle § 201, odst. 1, písm. a) trestního zákoníku 2) přečinu výroba a jiné nakládání s dětskou pornografií dle § 192, odst. 1) trestního zákoníku.[43]

[42] *Trestní spis*. Číslo spisu Č. J. KRPB – 141793/TČ-2013-060079
[43] *Trestní spis*. Číslo spisu Č. J. KRPB – 141793/TČ-2013-060079

4.3. Výrok soudu

ROZSUDEK JMÉNEM REPUBLIKY

Krajský soud v Brně rozhodl v hlavním líčení konaném dne 2. 9. 2015 v senátě složeném z předsedy a přísedících takto:

Obžalovaný **je vinen, že**

1. v době nejméně od 14. 2. 2013 do 8. 6. 2013 v místě svého trvalého bydliště, ze kterého se připojoval do sítě internet, kde za použití komunikačního nástroje Skype ze svého uživatelského profilu „AHA“ komunikoval s nezletilou, mající uživatelský profil „xxxx“, kterou při této komunikaci v místě jejího bydliště nutil k jejímu obnažování, hlazení na intimních místech a k pohlavnímu sebeukájení před webovou kamerou, přičemž vše sledoval na svém počítači a doplňoval písemnými pokyny, co a jak má nezletilá dělat, a když tato dále odmítala jeho pokyny plnit, vyhrožoval jí, že pokud nebude pokračovat, nebo bude jejich komunikaci jakýmkoli způsobem blokovat, zveřejní na sociální síti Facebook fotografie z předešlých video komunikací, které si měl bez jejího vědomí prostřednictvím Skypu pořídit, čímž byla nezletilá ve strachu ze zveřejnění těchto fotografií nucena v tomto jednání proti své vůli pokračovat, přičemž bezpečně věděl, že v době jejich komunikace nezletilá nedovršila patnáctý rok věku.[44]

2. v době nejméně od 21. 5. 2014 do 5. 8. 2014 v místě svého trvalého bydliště přechovával v celé adresářové struktuře externího pevného disku značky ADATA, o kapacitě 500 GB, celkem 9 složek, které obsahovaly 316 souborů s tématikou dětské pornografie, kdy z tohoto počtu bylo 315 obrazových souborů a 1 videosoubor, přičemž se jednalo o fotografie v datové podobě, znázorňující dívky ve věku mezi 15. a 18. rokem věku, případně osoby dětské vizáže, a to částečně či zcela nahé, v sexuálně vyzývavých polohách a v polohách při masturbaci s detaily intimních míst, a jeden filmový snímek v datové podobě s názvem „XXX Zoo-Porno“ v délce 18 minut 45 sekund, zobrazující zoofilní porno snímek s osobou, jež se jeví být dítětem a psem, kdy tato provádí felaci pohlavního orgánu psa a v různých polohách provádí se psem pohlavní styk,

tedy

[44] *Trestní spis*. Číslo spisu Č. J. KRPB – 141793/TČ-2013-060079

ad. 1

- jiného pohrůžkou jiné těžké újmy donutil k pohlavnímu sebeukájení a k obnažování, přičemž čin spáchal na dítěti mladším patnácti let,
- ohrozil mravní vývoj dítěte tím, že ho sváděl k nemravnému životu

ad. 2

- přechovával pornografické počítačové dílo, které zobrazuje dítě nebo osobu, jež se jeví být dítětem,

tím spáchal

ad. 1

- zločin sexuální nátlak podle § 186 odst. 1, odst. 5 písm. a) trestního zákoníku,

- přečin ohrožování výchovy dítěte podle § 201 odst. 1 písm. a) trestního zákoníku

ad. 2

- přečin výroba a jiné nakládání s dětskou pornografií podle § 192 odst. 1 trestního zákoníku,

a odsuzuje se za to

podle § 186 odst. 5 trestního zákoníku za použití § 43 odst. 1, § 40 odst. 2 a § 58 odst. 1 trestního zákoníku k úhrnnému trestu odnětí svobody v trvání

tří roků

podle § 84, § 81 odst. 1 a § 82 odst. 1 trestního zákoníku se výkon uloženého trestu podmíněně odkládá na zkušební dobu v trvání **pěti roků** a nad obžalovaným se zároveň vyslovuje **dohled.**

podle § 99 odst. 1, odst. 4 trestního zákoníku se obžalovanému ukládá **ústavní sexuologické ochranné léčení.**[45]

Takto byl vyhodnocen celý případ po prostudování policejního spisu soudem, a vynesen tento rozsudek. Pachatel odchází s podmíněným trestem odnětí svobody na zkušební dobu pěti roků a ukládá se mu ústavní sexuologické

[45] *Trestní spis*. Číslo spisu Č. J. KRPB – 141793/TČ-2013-060079

ochranné léčení. Dále si shrneme, z jakých informací soud vycházel a jaká byla rozhodující fakta pro vydání tohoto trestu.

Soud po provedeném dokazování zjistil skutkový děj uvedený ve výrokové části tohoto rozsudku. Bylo tedy prokázáno, že v období od února do června roku 2013 obžalovaný komunikoval zejména prostřednictvím Skypu s nezletilou, tehdy ve věku 13 roků, se kterou sdílel nejprve komunikaci vedoucí k jejímu obnažování a pohlavnímu sebeukájení před webovou kamerou a nezletilou instruoval, jak má při těchto praktikách postupovat. Pokud poškozená odmítla jeho pokyny splnit, vyhrožoval jí, a to tím způsobem, že zveřejní na Facebooku fotografie, které pořídil z předešlých video komunikací mezi oběma. Dále bylo prokázáno, že nejméně v období od května do srpna roku 2014 přechovával na pevném disku, který užíval, četné soubory obsahující dětskou pornografii, zejména se znázorněním dívek ve věku mezi 15. – 18. rokem věku, přičemž se jednalo o dívky obnažené, v sexuálně vyzývavých polohách a dále měl na disku uložen filmový snímek zobrazující zoofilní porno rovněž s osobou dětského vzezření ženského pohlaví. Uvedený skutkový děj byl zjištěn z plného doznání obžalovaného, dále z výpovědi poškozené a výpovědi jejích rodičů. Dokazování bylo zaměřeno též na znalecké zkoumání osoby obžalovaného, byly analyzovány údaje a data ve výpočetní technice užívané obžalovaným, přičemž byl proveden i přepis komunikace mezi obžalovaným a poškozenou nezletilou.[46]

Obžalovaný potvrdil, že přes Skype komunikoval pod profilem „AHA“, aby se mohl bavit s dívkami o sexu. Takto navázal kontakt s nezletilou, která se mu ukazovala nahá. Jednou se stalo, že nechtěla pokynům obžalovaného vyhovět, a proto jí vyhrožoval, že ji předtím fotil a tyto fotky že umístí na internet. Ve skutečnosti ji však vůbec nefotil ani nijak nezaznamenával video komunikaci mezi nimi. V přípravném řízení sice obžalovaný okrajově popřel, že by věděl o skutečném věku poškozené, nicméně u hlavního líčení před soudem již připustil, že tuto informaci měl, přičemž poškozené mělo být snad 14 roků. Obžalovaný se však necítí jako nějaký pedofil a dětskou pornografii si nestahoval. Nicméně doznává, že fotky a video na externím disku počítače jsou jeho a uložil je tam on.

[46] *Trestní spis*. Číslo spisu Č. J. KRPB – 141793/TČ-2013-060079

Obžalovaný potvrzuje i období, po které nejméně soubory byly na disku uloženy. Rozhodně se nezajímal o materiál, který by bylo možno označit jako dětskou pornografii, spíše mu šlo o dívky ve věku kolem 20 let.[47]

Poškozená nezletilá potvrdila skypovou komunikaci s obžalovaným s tím, že se původně domnívala, že jde o jednoho ze spolužáků. Sama komunikovala přes Skypový profil „xxxx“ a připustila, že měla i svůj Facebookový profil, ačkoliv jí dle příslušných propozic v době jeho založení ještě nebylo 13 roků. Při komunikaci s obžalovaným měla zapnutou web kameru, žádné fotografie mu neposílala. Poškozená dále popsala, že dle instrukcí obžalovaného se vysvlékala a sebeuspokojovala, to vše před funkční web kamerou. Obžalovaný se nikdy prostřednictvím web kamery poškozené neukázal. Dále poškozená potvrdila, že když požadavkům obžalovaného vyhovět nechtěla, vyhrožoval jí, že má k dispozici fotografie poškozené a umístí je na internet, přičemž má fotografii i jejího obličeje. Navzdory doznání obžalovaného i výpisům vzájemné komunikace s poškozenou tato tvrdí, že obžalovanému nenapsala svůj věk, pouze to, kde bydlí. O této komunikaci se poškozená nikomu nesvěřovala a přišli na to až její rodiče.[48]

Matka poškozené přišla na to, že na notebook, který jejich dcera používá, stále někdo volá na Skype. Šlo přitom o osobu vystupující pod pseudonymem „AHA“. Poté co prohlédla historii komunikace mezi její dcerou a tímto člověkem, zjistila, že šlo o komunikaci sexuální na výzvy dotyčného, přičemž v jedné pasáži její dceři vyhrožoval, že zveřejní vše, co proběhlo do současné doby a rozešle fotky a videa všem na Facebook. Přes tuto výhružku nadále nezletilá s dotyčným komunikovala. Její matka se tedy domnívá, že to na ní nezanechalo žádné trauma, ale hlavně si uvědomila, že udělala hloupost a má ponaučení do budoucna.[49]

V části spisu je založen přepis komunikace mezi skypovými profily obžalovaného „AHA“ a poškozené nezletilé „xxxx“. Z tohoto pak vyplývá, že v únoru 2013 oba komunikují mimo jiné na téma věku 14 roků, další komunikace probíhá zejména v únoru, dubnu a květnu 2013, přičemž po celou tuto dobu spolu

[47] *Trestní spis*. Číslo spisu Č. J. KRPB – 141793/TČ-2013-060079
[48] *Trestní spis*. Číslo spisu Č. J. KRPB – 141793/TČ-2013-060079
[49] *Trestní spis*. Číslo spisu Č. J. KRPB – 141793/TČ-2013-060079

obžalovaný s poškozenou intenzivně komunikují a je zjevné, že poškozená víceméně dobrovolně plní pokyny obžalovaného, svléká se před web kamerou a praktikuje nejrůznější sebeukájecí postupy. Stěžejní je informace z května 2013, kdy obžalovaný výslovně uvádí, že poškozenou fotil a jestli mu neukáže, co chce, tak veškeré fotky dá na Facebook, kde si jich určitě někdo všimne, avšak pokud poškozená ukáže, co bude chtít, tyto fotky smaže a už poškozenou nebude otravovat a dává jí minutu na rozmyšlenou.[50]

Předmětem ohledání a zajištění dat se stal jeden stolní počítač, jeden notebook a jeden externí USB HDD. Na pevném disku PC a na pevném disku notebooku byla zajištěna přítomnost Skype účtu „AHA“, jakož i dalších účtů, přičemž obžalovaný užíval tyto účty na Skypu k sexuální komunikaci zaměřené na video komunikaci, kde bylo osloveno řádově tisíc žen, dívek. Výskyt profilu „xxxx“ byl zjištěn na Skype účtu „AHA“ pouze v PC. Celkově ke komunikaci mezi účtem „AHA“ a „xxxx“ docházelo v období od února do června 2013. Ačkoliv součástí komunikace Skype mohou být i posílané fotografie či videosnímky, provozovatel Skype tyto neukládá. Pokud si je uživatel sám z příslušné komunikace nezkopíruje, dojde k jejich smazání. Prohlídkou všech vyselektovaných souborů pak nebyly zjištěny žádné soubory, které by mohly sloužit jako důkaz předmětné trestné činnosti ani soubory nebo videosoubory, kde by figurovala poškozená. Na externím HDD pak bylo u obžalovaného zajištěno celkem 316 souborů s tématikou dětské pornografie, z nichž 315 je obrazových a jeden videosoubor. V plném rozsahu je zachycen obsah tohoto externího HDD na DVD, které tvoří přílohu spisu. Dle údajů o telekomunikačním provozu byl činěn pokus ztotožnit příslušnou IP adresu, z níž bylo komunikováno s poškozenou, přičemž komunikační společnost sdělila, že tuto mimo jiné sdílel i klient (obžalovaný) na své trvalé adrese. Ovšem tato IP adresa byla sdílena mnoha dalšími klienty, kteří byli identifikováni. Dále bylo též specifikováno, že v předmětném případě komunikovala vnitřní IP adresa, kterou využívá právě klient (obžalovaný).[51]

Na základě shora popsaného dokazování s přihlédnutím na plné doznání samotného obžalovaného je možno uzavřít, že skutky, které mu byl kladeny již

[50] *Trestní spis*. Číslo spisu Č. J. KRPB – 141793/TČ-2013-060079
[51] *Trestní spis*. Číslo spisu Č. J. KRPB – 141793/TČ-2013-060079

obžalobou za vinu, byly skutečně obžalovaným spáchány a vykazují všechny znaky trestných činů.[52]

V případě bodu 1. výrokové části rozsudku bylo tedy prokázáno, že obžalovaný jiného pohrůžkou jiné těžké újmy donutil k pohlavnímu sebeukájení a k obnažování, přičemž čin spáchal na dítěti mladším 15 let. Za pohrůžku jiné těžké újmy je třeba považovat nátlakové jednání obžalovaného, pokud tento předstíral, že má k dispozici intimní snímky poškozené nezletilé, které měl údajně pořídit během předchozích videospojení, přičemž zveřejnění takových snímků na Facebook by nepochybně způsobilo poškozené závažnou újmu a dehonestaci, která zvláště u mladých lidí je psychicky velmi špatně snášena, často až s fatálními následky. Tímto tzv. sexuálním nátlakem pak nutil poškozenou, aby v přímém přenosu pokračovala v praktikách sebeukájení a obnažování, které jej vzrušovaly a které sledoval prostřednictvím web kamery. Zároveň, jak vyplývá ze vzájemné komunikace i doznání obžalovaného, věděl o tom, že poškozená je osobou mladší 15 let. Takovou osobu mravně ohrozil tím, že ji poměrně pravidelnou komunikací uvedeného charakteru sváděl k životu nikoliv mravnému. Za daných okolností tedy bylo třeba jednání obžalovaného pod bodem 1. výrokové části rozsudku kvalifikovat jako zločin sexuálního nátlaku dle § 186 odst. 1, odst. 5 písm. a) trestního zákoníku a současně jako přečin ohrožování výchovy dítěte dle § 201 odst. 1 písm. a) trestního zákoníku. Pod bodem 2. výrokové části bylo spolehlivě prokázáno, že obžalovaný přechovával pornografické dílo zobrazující dítě nebo osobu, jež se jeví být dítětem. Povaha těchto snímků a videosouborů je nejlépe patrná při jejich zobrazení a je zcela evidentní, že zachycuje dívky skutečně dětského vzezření. Proto v tomto případě bylo počínání obžalovaného kvalifikováno jako přečin výroby a jiného nakládání s dětskou pornografií dle § 192 odst. 1 trestního zákoníku. V případě všech tří právních kvalifikací si byl obžalovaný dobře vědom toho, k čemu dívku mladší 15 let nutí a pod jakou pohrůžkou, přičemž si musel být vědom i toho, že tímto způsobem osobu ve věku tzv. dítěte svádí k nemravnému životu. Stejně tak si byl vědom přechovávání závadných souborů s tzv. dětskou pornografií. Pokud se svého jednání přes uvedené vědomí dopustil, svědčí to o jeho vůli čin spáchat a trestná činnost tak

[52] *Trestní spis*. Číslo spisu Č. J. KRPB – 141793/TČ-2013-060079

byla v plném rozsahu spáchání v úmyslu přímém dle § 15 odst. 1 písm. a) trestního zákoníku. Dále soud akceptoval návrh znalkyně z oboru zdravotnictví – psychiatrie na uložení ochranného léčení sexuologického v ústavní formě.[53]

Proti tomuto rozsudku podal obžalovaný prostřednictvím svého obhájce odvolání, směřující pouze do výroku o uloženém ochranném léčení. Odvolatel namítl, že nesouhlasí s formou uloženého ochranného léčení, když je přesvědčen, že v daném případě by postačila ambulantní forma. Obžalovaný si svůj problém uvědomuje, má na svou poruchu náhled a chce se léčit. Během září a října 2015 vyhledal odbornou pomoc v sexuologické ambulanci Psychiatrické kliniky a absolvoval dvě sezení. Další sezení má domluveno. Sám by svou léčbu rád zintenzivnil. Vzhledem k tomu, že ústavní léčení je vždy spojeno s podstatným omezením osobní svobody léčeného a je radikálním zásahem do způsobu života, musí soud při ukládání této formy ochranného léčení pečlivě zvažovat jak povahu nemoci a léčebné možnosti, tak i povahu a závažnost trestné činnosti a povahu a závažnost nebezpečí, které do budoucna ze strany léčené osoby hrozí zájmu chráněnému trestním zákoníkem. Jelikož zahájil ambulantní léčbu, která mu lépe pomáhá pochopit jeho sexualitu a realizovat se v mezích zákona, je proto přesvědčen, že postačí ambulantní forma léčby. Navrhl proto, aby vrchní soud napadený rozsudek změnil a rozhodl, že ochranné léčení se vykoná ambulantně. Vrchní soud v Olomouci projednal ve veřejném zasedání odvolání obžalovaného proti rozsudku Krajského soudu v Brně a napadený rozsudek částečně zrušuje ve výroku o uloženém ochranném opatření a nařizuje sexuologické ochranné léčení ambulantní. Závěrem pak odvolací soud pro další chování obžalovaného na svobodě připomíná znění § 99 odst. 5 trestního zákoníku, podle kterého může být soudem změněno dodatečné ústavní léčení na ambulantní a naopak. Což v praxi znamená, že nebude-li se obžalovaný nadále dobrovolně podrobovat již započaté ochranné sexuologické léčbě ambulantní, bude tato příslušným okresním soudem změněna, a to i bez návrhu na ústavní.[54]

[53] *Trestní spis*. Číslo spisu Č. J. KRPB – 141793/TČ-2013-060079
[54] *Trestní spis*. Číslo spisu Č. J. KRPB – 141793/TČ-2013-060079

4.4. Znalecký posudek

Byl vypracován znalecký posudek z oboru zdravotnictví, odvětví psychiatrie.

Znalecký posudek vypracovala primářka Sexuologického oddělení Psychiatrické léčebny.

Ve znaleckém posudku je třeba posoudit a zodpovědět následující otázky:

1. Zda obviněný v době spáchání trestného činu trpěl, případně stále trpí duševní chorobou nebo poruchou či sexuální odchylkou, v kladném případě jakou a v jakém rozsahu.

Odpověď:

Obviněný v době spáchání trestného činu netrpěl žádnou duševní chorobou v pravém slova smyslu. Trpěl sexuální poruchou tzv. neúplnou sexualitou. To znamená, že neúplnou v tom smyslu, že jeho sexualita nemá vlohy pro úvodní stádia sexuality, kterými jsou motivační stavy atraktivity a proceptivity.

2. Měla případně zjištěná duševní choroba nebo porucha, závislost na návykových látkách nebo alkoholu či sexuální odchylka vliv na rozpoznávací a ovládací schopnosti obviněného v době spáchání trestného činu a jakou měrou.

Odpověď:

Neúplná sexualita neměla vliv na rozpoznávací schopnosti, ale měla vliv na ovládací schopnosti v době trestného činu a to tak, že způsobila podstatné snížení ovládacích schopností. Člověk s neúplnou sexualitou se ovládá daleko hůře, než člověk se standardní sexualitou, když vznikne zájem o sexuální interakci.

3. Zda je pobyt obviněného v případě zjištěné choroby, poruchy či odchylky na svobodě nebezpečný, z jakého důvodu a zda vyžaduje ochranné léčení a jsou dány podmínky pro uložení zabezpečovací detence.

Odpověď:

Pobyt obviněného na svobodě je nebezpečný v tom smyslu, že se bude i nadále zajímat o genitál nezletilých, které jsou daleko přístupnější, než dospělé, protože se zatím u nich ještě neprojevila cudnost. Pokud to nebude na internetu, protože ten by měl mít obviněný zakázaný, mohlo by se to stát v reálu, tedy s nějakou reálnou nezletilou, kterou buď bude znát, nebo jí někde náhodně potká. Proto znalkyně navrhuje léčení ochranné sexuologické ústavní formou. Cílem této

léčby by mělo být, aby obviněný pochopil, jak jeho sexualita funguje a pak jak tento typ sexuality realizovat v mezích zákona s dospělou svolnou partnerkou.[55]

Tento znalecký posudek byl vpracován dne 4. dubna 2015. Z posudku jasně vyplývá, že primářka psychiatrické a sexuologické léčebny nedoporučuje ambulantní léčbu z důvodů obavy z pokračování páchání trestné činnosti, kdy porucha obžalovaného je natolik závažná, že je nutná ústavní léčba. Jak již bylo výše zmíněno ve výroku soudu, kdy se obžalovaný prostřednictvím svého obhájce odvolal proti uložení ochranného ústavního léčení, který vydal Krajský soud v Brně, bylo v přezkumném řízení u Vrchního soudu v Olomouci zkoumáno přeměnění ústavního léčení na ambulantní. Zde z provedeného dokazování ve veřejném zasedání bylo z odborného vyjádření – lékařské zprávy ze dne 9. listopadu 2015 primářky psychiatrické a sexuologické léčebny zjištěno, že obžalovaný opakovaně navštěvuje sexuologickou ambulanci Psychiatrické nemocnice, kde se podrobuje náhledové terapii v souvislosti s poruchou jeho sexuální preference neúplné sexuality. Dle vyjádření lékařky je jmenovaný při terapii aktivní, spolupracuje a jeho informace o této problematice se rozrůstají. Uvědomuje si čím dál tím víc věcí o mechanismu své sexuality, a tím, že o sobě víc ví, stává se klidnějším. Za těchto okolností, když pacient začal řádně navštěvovat náhledovou terapii v psychiatrické nemocnici na sexuologickém oddělení, a tato terapie přináší pozitivní výsledky, postačuje, kdyby byla nařízena jen ambulantní forma ochranné sexuologické léčby. K tomuto vyjádření lékařky bylo přihlédnuto při rozhodování soudu ve věci přeměny ústavního léčení na ambulantní.

[55] *Trestní spis*. Číslo spisu Č. J. KRPB – 141793/TČ-2013-060079

4.5. Následná náprava pachatele

Obžalovaný docházel do sexuologické ambulance ode dne 12. 10. 2015, jelikož mu byla ochranná léčba sexuologická formou ambulantní nařízena dne 25. 11. 2015, je to bráno jako datum započetí výkonu ochranného léčení sexuologického formou ambulantní. Obžalovaný měl stanovený interval kontrol v sexuologické ambulanci 1x měsíčně, kdy se podrobil individuální kontrole v sexuologické ambulanci a též se v daný den účastnil i skupinové náhledové terapie. V té době nebyl obžalovaný nijak medikován. Na náhledových terapiích se aktivně zapojoval, měl dobré připomínky k probíraným tématům, projevoval náhled nad svou odchylkou a nic nenasvědčovalo pro recidivu jeho deviantní sexuality. Spolupracoval celkem dobře, párkrát se stalo, že nedodržel stanovený termín kontroly, o čemž byla informována jak Policie České republiky, tak i soud, nicméně tyto své prohřešky obžalovaný zdůvodnil. Na poslední kontrolu se obžalovaný dostavil dne 15. 6. 2018 a na další řádný termín, který byl stanoven na 27. 7. 2018 už se nedostavil. Svou nepřítomnost na tento řádný termín žádným způsobem neomluvil. Dne 20. 8. 2019 byl podán návrh na zrušení ochranné léčby ambulantní sexuologické, neboť byl obžalovaný vzat do vazby pro páchání obdobné trestné činnosti, pro kterou mu byla nařízena ochranná léčba.[56]

Dle šetření policie se obžalovaný nejméně v době od 24. února 2017 z místa svého trvalého bydliště připojoval do sítě internet na sociální síť Facebook pod novým profilem, přes komunikační nástroj Messenger, kde navázal kontakt s první nezletilou dívkou, které při komunikaci na sexuální téma sám zasílal dříve získané fotografie a videa s tématikou dětské pornografie a současně ji nabádal na vytváření a zasílání svých, tzv. nahých až pornograficky laděných fotografií, videí a uskutečňování online video komunikací se stejným obsahem, což nezletilá v několika případech zpočátku dobrovolně učinila, a poté, co toto začala odmítat, pod pohrůžkou zveřejnění dříve získaného materiálu ji nutil, aby si jej nezablokovala a nadále s ním komunikovala a posílala další osobní pornografická díla. A to přestože znal její věk z dřívější komunikace. Dále v době od 27. února 2017 rovněž stejnou praktikou, navázal komunikaci s druhou nezletilou dívkou,

[56] *Trestní spis*. Číslo spisu Č. J. KRPB – 141793/TČ-2013-060079

přes komunikační nástroj Messenger, kdy po poškozené vyžadoval stejné fotografie, videa, které byly pornograficky laděné a video komunikaci se stejným obsahem. I v tomto případě takto jednal přes skutečnost, že znal věk poškozené. Nejméně od začátku měsíce března do 26. března 2017 opět z místa trvalého bydliště v prostředí sítě internet na sociální síti Facebook pod novým profilem, přes komunikační nástroj Messenger, navázal kontakt s třetí nezletilou dívkou a ač znal její skutečný věk, zaslal jí celkem pět videí obsahujících pornografické dílo zobrazující dítě s osobou, jež se jeví být dítětem a požadoval po ní, aby mu poslala své osobní pornograficky laděné video, kdy mu nezletilá zaslala nejméně tři videosoubory. Poté co si tento profil poškozená zablokovala, neboť v tomto dále nechtěla pokračovat, vytvořil si obžalovaný nový profil, pod kterým s poškozenou opět navázal kontakt, kde jí sdělil, že je to on a vyhrožoval jí zveřejněním získaných souborů v případě, že s ním přestane nadále komunikovat. Tento čin znovu opakoval v době od 18. 4. 2017 do 16. 7. 2017 rovněž stejným způsobem přes komunikační nástroj Messenger na čtvrtou dívku, i když bezpečně znal její věk. Posledním zjištěným trestným činem, kterého se obžalovaný dopustil dne 6. září 2018 z přesně nezjistitelného místa, kdy za použití mobilního internetového připojení z telefonního čísla přistoupil do sítě internet a na sociální síti Facebook zaslal pod falešným uživatelským jménem na další Facebookové profily dva videosnímky v digitální podobě, na kterých se nacházely dívky zjevně mladší osmnácti let při orálním styku s mužem, přičemž se tato díla s tématikou dětské pornografie dostala k celkem 251 uživatelům Facebooku. Po prostudování celého policejního spisu obžalovaného Krajský soud v Brně v hlavním líčení konaném v červnu 2020 odsoudil, a to **k úhrnnému nepodmíněnému trestu odnětí svobody v trvání čtyřiceti osmi měsíců do věznice s ostrahou**.[57]

[57] *Trestní spis*. Číslo spisu Č. J. KRPB – 141793/TČ-2013-060079

Závěr

Jak jsme si řekli již v úvodu, současnou moderní a technologicky vyspělou společnost dnes můžeme nazvat společností informační. Moderní technologie se neustále vyvíjejí a provází nás na každém kroku. To nám přináší mnoho pozitivních aspektů, ale i velké množství bezpečnostních rizik. Na začátku jsme si uvedli co je to informační kriminalita, jak ji můžeme klasifikovat a jaké hrozby na nás v kybernetickém prostoru mohou číhat. Řekli jsme, jak probíhá boj proti informační kriminalitě v České republice a jaké konkrétní orgány proti této trestné činnosti bojují.

V obecné rovině můžeme říci, že v současné době jsou na vzestupu různá podvodná jednání, jejich nárůst je opravdu markantní, a to i přes častá varování v médiích. Můžeme jen doufat, že se bude jednat o dočasný trend, než se společnost zdokonalí ve využívání informačních technologií a nabude lepších zkušeností.

Rád bych zde zmínil, že přestože je ostatní kybernetická kriminalita také dosti závažná a cílí na veškeré obyvatelstvo, neměli bychom zapomínat na zvlášť zranitelné oběti, kterými jsou zejména děti. Proto jsem se podrobně zaměřil na část kybernetické kriminality a to na mravnostní trestné činy. Do této skupiny spadá hned několik trestných činů, jako jsou zejména sexuální nátlak dle § 186, šíření dětské pornografie § 191, ohrožování výchovy dítěte § 201, znásilnění § 185 a pohlavní zneužití § 187.

V praktické části této práce jsem se zaměřil na kazuistiku vyšetřovaného případu Oddělením kybernetické kriminality. Prostudoval jsem podrobně veškeré spisy, ve kterých je uveden celý postup při odhalování pachatele, který si vyhledával své oběti pomocí sítě internet. Konkrétně v převážné části využíval nástroj Skype přes který se svými oběťmi komunikoval. Příčin proč si děti zakládají účty na různých aplikacích už ve velmi raném věku je mnoho. Dávají tak bohužel velký prostor pro pachatele této trestné činnosti. A zde jsem narazil na velkou hrozbu. Hrozbu, která spočívá v nedostatečné informovanosti společnosti, zejména tedy rodičů, kteří podceňují rizika v prostředí internetu. Někteří o těchto hrozbách ani netuší. Tak často se dnes pohybujeme v kyberprostoru, že si ani

neuvědomujeme, jak do něj pouštíme i naše ratolesti bez nějakého upozornění, poučení, co by je zde mohlo potkat, nebo jaké by to mohlo mít následky. Děti jsou snadnými oběťmi, proto bychom je měli co nejvíce chránit a snažit se poukázat na nástrahy, které na ně v dnešním kyberprostoru mohou číhat. A kdo nejlépe by je měl upozornit, než samotní rodiče ve kterých mají největší důvěru. Nemohu zde opomenout zmínit, že se nejedná jen o dívky, na kterých jsou páchány trestné činy, ale tyto útoky jsou páchány ve velké míře i na chlapce.

Osobně se domnívám, že je zde potřeba v co největší možné míře zlepšit informovanost na straně koncových uživatelů, aby si uvědomili, jaká rizika se v kybernetickém prostoru skrývají. Aby rodiče více komunikovali se svými dětmi o skrytých hrozbách, které se v internetovém prostředí vyskytují, věnovali jim v tomto směru větší pozornost a prováděli častější kontroly o tom, kde se v rámci „sítě“ pohybují.

Závěrem můžeme konstatovat, že vývoj informačních technologií jde stále kupředu a boj s kyberkriminalitou je o to více složitější. Orgány bojující s touto trestnou činností jsou neustále o krok pozadu, pachatel má totiž mnoho výhodných aspektů na své straně. Svádí tak nelehký boj, ale i přes to všechno, z něj často vychází vítězně. Zde už můžeme jen doufat, že v rámci Strategie kybernetické bezpečnosti EU, jejímž primárním cílem je zvýšení kybernetické odolnosti Evropy, bude zajištěno pro každého občana Evropské unie, moci využívat bez potencionálního nebezpečí kybernetický prostor.

Seznam použité literatury

Bibliografické zdroje

[1] FIRE M., GOLDSCHMIDT R., ELOVICI Y. 2014. Online social network: Threats and Solutions. 2014. IEEE communication surveys. Volume 16, Issue 4, pp. 125-142.

[2] GŘIVNA, T; SCHEINOST, M; ZOUBKOVÁ, I. 2015. Kriminologie. 1 vydání, Praha: Wolters Kluwer, a. s. ISBN: 978-80-7478-614-3.

[3] JIROVSKÝ, V. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. 1 vydání, Praha: Grada Publishing, 2007. ISBN: 978-80-247- 1561-2.

[4] MATĚJKA, M. Počítačová kriminalita. 1 vydání, Praha: Computer Press, 2002. ISBN: 80-7226-419-2.

[5] McCARTHY, L, WELDON-SIVIY. D. Buď pánem svého prostoru: jak chránit sebe a své věci, když jste online. 1 vydání, Praha: CZ. NIC, 2013. ISBN: 978-80-904248-6-9.

[6] POŽÁR, J HNÍK, V. 2018. Specifické problémy boje s kybernetickou kriminalitou. Policejní akademie ČR v Praze.

[7] Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským.

[8] Trestní spis. Číslo spisu Č. J. KRPB – 141793/TČ-2013-060079

Elektronické zdroje

[9] AČR. Velitelství informačních a kybernetických sil [online]. Praha (Česká republika) Ministerstvo obrany, aktualizace 7. 10. 2021. [2021-11-5] URL: https://www.acr.army.cz/struktura/generalni/kyb/velitelstvi-kybernetickych-sil-a-informacnich-operaci-214169/

[10] Články: prevencekriminality.cz. Kyberkriminalita [online]. Praha (Česká republika) Ministerstvo vnitra, odbor prevence kriminality, 2014. [2021-11-5] URL: https://prevencekriminality.cz/prevence-kriminality/kyberkriminalita/

[11] ČSÚ. 2018. Více než polovina Čechů používá sociální sítě [online]. Praha (Česká republika) Český statistický úřad, aktualizace 20. 11. 2018. [2021-11-5] URL: https://www.czso.cz/csu/czso/vice-nez-polovina-cechu-pouziva-socialni-site

[12] HAVLÍK, M. Příčiny vzniku a začlenění kybernetických sil a informačních operací do Armády České republiky [online]. Brno (Česká republika) Vojenské rozhledy, 2020. [2021-12-3] UR: https://www.vojenskerozhledy.cz/kategorie-clanku/strategicke-rizeni/zacleneni-kybernetickych-sil

[13] MVČR. Kybernetická kriminalita v ČR z kriminologické perspektivy [online]. Praha (Česká republika) Ministerstvo vnitra ČR, 2017. [2021-11-14] URL: https://www.google.com/url?client=internal-element-cse&cx=015489265366623571386:izzrwg3bmqm&q=https://www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx&sa=U&ved=2ahUKEwiw8JCCkq_2AhVBPewKHWMfCHQQFnoECAEQAQ&usg=AOvVaw0UDlITmgISACQ4w75aLG6n

[14] NÚKIB. Co je NÚKIB [online]. Praha (Česká republika) Národní úřad pro kybernetickou a informační bezpečnost, 2017. [2021-12-5] URL: https://nukib.cz/cs/o-nukib/

[15] NÚKIB. Národní strategie kybernetické bezpečnosti ČR na období let 2015–2020 [online]. Praha (Česká republika) Národní ústav pro kybernetickou a informační bezpečnost, 2015. [2021-12-3] URL: https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/

[16] PČR. Jednotlivé druhy kyberkriminality [online]. Praha (Česká republika) Policie České republiky, 2021. [2021-11-14] URL: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx

]17] PČR. Kyberkriminalita [online]. Praha (Česká republika) Policie České republiky, 2021. [2021-11-5] URL: https://www.policie.cz/clanek/kyberkriminalita.aspx

[18] PČR. Prevence kyberkriminality [online]. Praha (Česká republika) Policie České republiky, 2021. [2021-11-18] URL: https://www.policie.cz/clanek/prevence-kyberkriminality.aspx

[19] RADA EU. Kybernetická bezpečnost: Jak EU řeší kybernetické hrozby [online]. Praha (Česká republika) Rada Evropské unie, 2020. [2021-12-3] URL: https://www.consilium.europa.eu/cs/policies/cybersecurity/

[20] VOJENSKÉ ZPRAVODAJSTVÍ. Kybernetická obrana [online]. Praha (Česká republika) Ministerstvo obrany, 2016. [2021-11-21] URL: https://www.vzcr.cz/kyberneticka-obrana-46

[21] Články: Otázky spojené s mravnostní trestnou činností [online]. Praha (Česká republika) Právní prostor, 28. 5. 2014. [2021-12-15] URL: https://www.pravniprostor.cz/clanky/trestni-pravo/otazky-spojene-s-mravnostni-trestnou-cinnosti-ii-cast

[22] Článek: PČR. Sexuální a mravnostní trestné činy [online]. Praha (Česká republika) Policie České republiky, 2021. [2022-01-6] URL: https://www.policie.cz/clanek/sexualni-a-mravnostni-trestne-ciny.aspx

[23] Justice.cz – registr poskytovatelů pomoci obětem trestných činů [online]. Praha (Česká republika) Ministerstvo spravedlnosti ČR, 2017. [2022-01-6] URL: https://www.justice.cz/web/msp/rozvoj-sluzeb-pro-obeti-trestne-cinnosti?clanek=registr-poskytovatelu-pomoci-obetem-trestnych-cinu

[24] *PČR. Prevence kyberkriminality* [online]. Praha (Česká republika) Policie České republiky, 2021. [2021-12-5] URL: https://www.policie.cz/clanek/prevence-kyberkriminality.aspx