ZÁPADOČESKÁ UNIVERZITA V PLZNI

Fakulta právnická

Katedra trestního práva

DIPLOMOVÁ PRÁCE

Kyberkriminalita na sociálních sítích

Zpracovala: Adéla Heroutová

Vedoucí diplomové práce: doc. JUDr. Jan Chmelík, Ph.D.

Plzeň 2023

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta právnická
Akademický rok: 2022/2023

ZADÁNÍ DIPLOMOVÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Adéla HEROUTOVÁ**
Osobní číslo:	**R18M0106P**
Studijní program:	**M6805 Právo a právní věda**
Studijní obor:	**Právo**
Téma práce:	**Kyberkriminalita na sociálních sítích**
Zadávající katedra:	**Katedra trestního práva**

Zásady pro vypracování

1. Vymezení základních pojmů
2. Sociální sítě
3. Jednotlivé druhy kybernetické kriminality na sociálních sítích (kyberšikana, krádež virtuální identity, sexting, kybergrooming, kyberstalking)
4. Vyšetřování a odhalování kybernetické kriminality na sociálních sítích

Rozsah diplomové práce:
Rozsah grafických prací:
Forma zpracování diplomové práce: **tištěná**

Seznam doporučené literatury:

GŘIVNA, Tomáš a Radim POLČÁK, ed. Kyberkriminalita a právo. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4.
CHMELÍK, Jan a kol. Mravnost, pornografie a mravnostní kriminalita. 1. vyd. Praha: Portál, s.r.o., 2003. ISBN 80-7178-739-6.
Kolouch, Jan. *Cybercrime*, 1.vydání.; CZ.NIC, z. s. p. o.: Milešovská 5, 130 00 Praha 3, 2016. ISBN 978-80-88168-18-8
SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7.
ZAVRŠNIK, Aleš. Kyberkriminalita. Praha: Wolters Kluwer, 2017. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7552-758-5.

Vedoucí diplomové práce: **Doc. JUDr. Jan Chmelík, Ph.D.**
Katedra trestního práva

Datum zadání diplomové práce: **1. února 2022**
Termín odevzdání diplomové práce: **31. března 2023**

Západočeská univerzita v Plzni
L.S.
Fakulta právnická

JUDr. et PhDr. Stanislav Balík, Ph.D.
děkan

Doc. JUDr. František Vavera, Ph.D., LL.M.
vedoucí katedry

V Plzni dne 8. srpna 2022

Prohlášení

„Čestně prohlašuji, že jsem diplomovou práci na téma Kyberkriminalita na sociálních sítích vypracovala samostatně a že jsem vyznačila všechny prameny, ze kterých jsem při psaní této práce čerpala a vycházela.“

Plzeň, březen 2023

_____

Adéla Heroutová

Poděkování

Na tomto místě bych ráda poděkovala vedoucímu mé diplomové práce doc. JUDr. Janu Chmelíkovi, Ph.D. za jeho ochotu, užitečné připomínky a rady, které mi při psaní této práce velice pomohly. Velké poděkování patří rovněž Oddělení analytiky a kybernetické kriminality Městského ředitelství Policie České republiky v Plzni, jež mi umožnilo osobní konzultaci, která byla pro tuto práci značným přínosem. A nakonec bych ráda poděkovala rodině a svému partnerovi.

Obsah

Seznam zkratek

ČR	Česká republika
ICT	informační a komunikační technologie
NCOZ	Národní centrála proti organizovanému zločinu
OČTŘ	orgány činné v trestním řízení
OKTE	Odbor kriminalistické techniky a expertiz
TrŘ	zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád)
TrZ	zákon č. 40/2009 Sb., Trestní zákoník
Úmluva	Úmluva o počítačové kriminalitě
ÚS	Ústavní soud
ÚZČ	Útvar zvláštních činností služby kriminální policie a vyšetřování
ZoEK	zákon č. 127/2005 Sb., o elektronických komunikacích

Úvod

V dnešním světě zaujímají stále většího významu sociální sítě, na kterých jejich uživatelé tráví v některých případech i řadu hodin každý den. Sociální média mají pro naši společnost značný přínos, neboť díky nim mají jejich uživatelé snadný přístup k informacím, možnost komunikace s jinými uživateli, ať už se nacházejí kdekoliv na světě, prostor vyjadřovat své názory bez ostychu a celou škálu dalších jiných kladů. Lze dokonce říci, že pro některé osoby je život on-line jednodušší, nežli život off-line. Sociální média umožňují svým uživatelům nasazení pláště anonymity, pod kterým jsou leckdy odvážnější, a dovolí si činit i takové věci, které by se ve světě reálném neodvážili. Nicméně mají i svou stinnou stránku v podobě různých rizik, která tento prostor skýtá, a která jsou zároveň obsahem této práce. Diplomová práce je zaměřena na kyberšikanu, sexting, kybergrooming, kyberstalking a krádež virtuální identity, přičemž cílem této práce je objasnit tyto pojmy, poskytnout jejich trestněprávní kvalifikaci a tomu odpovídající judikaturu. Současně pak zjistit rozšíření těchto patologických jevů ve společnosti prostřednictvím dotazníkového šetření. Nakonec si práce klade za cíl nabídnout vhled do trestního práva procesního, a to konkrétně do postupu orgánů činných v trestním řízení při odhalování a vyšetřování trestné činnosti na sociálních sítích. Pro splnění těchto cílů bude využívána metoda deskriptivní, analytická a komparativní, která bude používána zejména ve vztahu k provedenému výzkumu.

Diplomová práce je složena ze tří částí, přičemž její první část tvoří kapitola první a kapitola druhá. V první kapitole jsou objasněny základní pojmy, kterým je nezbytné porozumět, neboť je s nimi pracováno v celém obsahu této práce. Kapitola druhá je zaměřena na samotné sociální sítě, a zejména pak zodpovídá otázku „kdo nese odpovědnost za sdílený protiprávní obsah na sociální síti? Daná sociální síť anebo uživatel této sítě?“

Druhou částí je kapitola třetí, která je meritem této práce. Tato kapitola je systematizována do celkem pěti podkapitol, kdy každá jednotlivá podkapitola objasňuje danou problematiku, a tedy kyberšikanu, sexting, kybergrooming, kyberstalking a krádež virtuální identity. V těchto podkapitolách jsou jednotlivé rizikové jevy sociálních sítí důkladně objasněny a to tak, aby bylo zřejmé, co je jejich obsahem, čím se vyznačují a jak se projevují. Pro lepší dokreslení a pochopení daného rizikového jevu obsahují podkapitoly reálné případy, které tak lépe demonstrují danou problematiku. Současně je poskytnut právní rámec těchto

rizik, neboť v některých případech se již jedná o natolik společensky škodlivá jednání, že vyžadují trestněprávní reakce. Skutkové podstaty jsou přitom důkladně rozebrány tak, aby bylo možné pochopit jejich aplikaci na projevy kyberšikany, sextingu, kybergroomingu, kyberstalkingu a krádeže identity. Dále je poskytnuta přiléhavá judikatura, která doplňuje jednotlivé podkapitoly a napomáhá lepšímu propojení mezi teoretickým popsáním těchto rizik a jejich sankcionováním. Jednotlivé podkapitoly obsahují provedený kvantitativní výzkum, pro který byl zvolen internetový dotazník s heterogenním souborem respondentů. Primárním cílem realizovaného výzkumu bylo zjistit, jaká je úroveň výskytu těchto patologických jevů ve společnosti.

Kapitola třetí obsahuje hmotněprávní kvalifikaci trestných činů páchaných v prostředí sociálních sítí. Část třetí, a tedy kapitola čtvrtá, objasňuje trestněprocesní postup při jejich odhalování a vyšetřování. Odhalování a vyšetřování trestné činnosti páchané v prostředí sociálních sítí je svým způsobem specifické, neboť jsou sociální sítě digitálním prostředím, které je svou povahou nestálé a proměnlivé, a proto je vyžadován kvalifikovaný postup orgánů činných v trestním řízení. Tato kapitola vznikla po odborné konzultaci s Oddělením analytiky a kybernetické kriminality Městského ředitelství Policie České republiky v Plzni, s jejichž pomocí bylo možné uvést, jak probíhá trestněprocesní postup orgánů činných v trestním řízení při odhalování a vyšetřování tohoto druhu trestné činnosti v praxi.

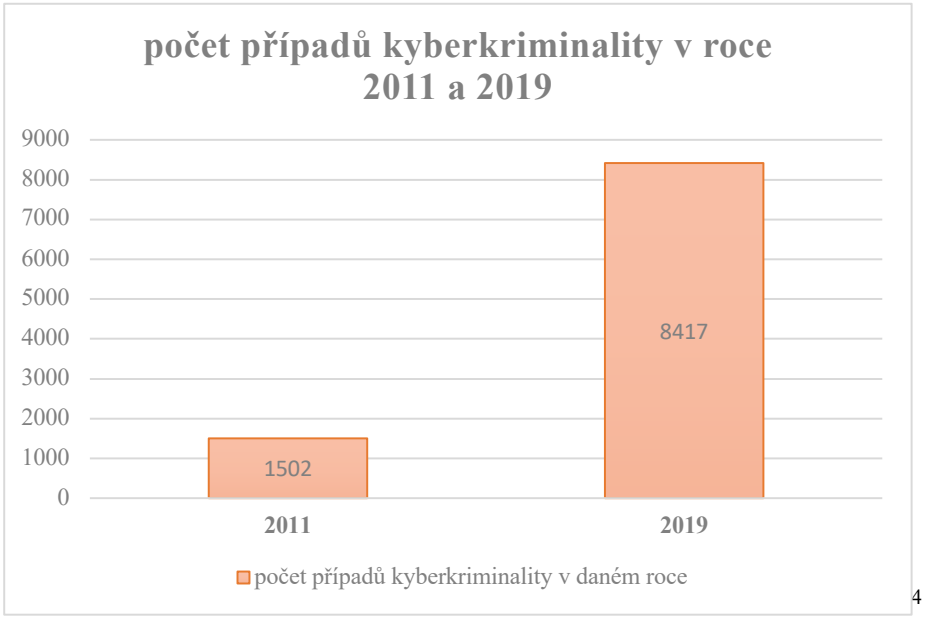
1 Vymezení základních pojmů

V této kapitole je objasněn pojem kyberkriminalita, stejně jako další pojmy, které jsou s touto problematikou a tématem diplomové práce neodmyslitelně spojeny.

1.1 Kybernetická kriminalita

Téměř v každém odvětví lidské činnosti jsou nějakým způsobem využívány informační či komunikační technologie (dále jen „ICT“). Dnešní doba, doba vědeckotechnického pokroku, s sebou přináší stále častější využívání těchto technologií.[1] Na základě analýz prováděných mezi roky 2012 a 2022 se počet uživatelů internetu více než zdvojnásobil, a to z 2,18 miliard uživatelů na 4,95 miliard uživatelů[2], avšak tento nárůst je také spojen se zneužíváním ICT k dopouštění se trestné činnosti.[3]

Na základě údajů zjištěných a vyhodnocených Policí ČR lze v tomto grafu vidět rozmach kyberkriminality v ČR od roku 2011 do roku 2019.



[4]

[1] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. s. 31.
[2] *Digital 2022: Another year of bumper growth.* [online]. We are social, [cit. 27.10.2022]. Dostupné z: https://wearesocial.com/uk/blog/2022/01/digital-2022-another-year-of-bumper-growth-2/
[3] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. s. 31.
[4] *Kyberkriminalita*. [online]. Policie České republiky, [cit. 27.10.2022]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

Kybernetická kriminalita je označována více pojmy, a to dle náhledu daného autora nebo právní úpravy. Lze se setkat s pojmy jako například elektronická kriminalita, kybernetická kriminalita, kyberkriminalita nebo počítačová kriminalita, avšak termín počítačová kriminalita byl již v dnešní době překonán, neboť díky technickému pokroku na sebe některá technická zařízení převzala funkci počítačů. Pojem počítač pak nahradil pojem ICT. Rozdílné pojmenování u autorů netkví pouze v rozdílném označení, nýbrž i v odlišném obsahovém chápání této problematiky.[5]

Neexistuje všeobecná definice, která by správně dokázala zahrnout veškeré aspekty kybernetické kriminality, jelikož dochází k neustálému zdokonalování ICT. Jsou rozvíjeny jejich funkce a možnosti, čímž však úměrně rostou i příležitosti pro jejich zneužívání k dopouštění se trestné činnosti. Právě z těchto důvodů nelze dostatečně reagovat všeobecnou definicí na tento rozvoj.[6] Kybernetická kriminalita je Policií ČR definována jako *„trestná činnost, která je páchána v prostředí informačních a komunikačních technologií včetně počítačových sítí.“* A trestný čin buďto směřuje přímo proti těmto technologiím, jež představují cíl útoku, anebo jsou nástrojem, pomocí kterého je protiprávní jednání pácháno. Místem, ve kterém k páchání kybernetické trestné činnosti dochází, je kybernetický prostor.[7]

Pouze taková jednání, na která lze aplikovat ustanovení platné trestněprávní úpravy, lze pod pojem kriminalita podřadit. V rámci ICT dochází k celé řadě jednání, jež mohou být pro společnost škodlivá, ale pokud nenaplňují znaky žádného trestného činu, nejedná se o trestné činy dle platné trestněprávní úpravy, a nejedná se tedy o kriminalitu jako takovou.[8]

V souvislosti se zdokonalováním ICT, tedy i sociálních sítí, je žádoucí, aby poskytovatelé sociálních sítí, a stejně tak i jejich uživatelé, byli na riziko možného kybernetického útoku připraveni. Za účelem prevence kybernetické

[5] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. s. 31-32.
[6] Tamtéž, s. 33.
[7] *Kyberkriminalita.* [online]. Policie České republiky, [cit. 27.10.2022]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspxu
[8] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. s. 34-35.

kriminality je nutné podchycovat tuto problematiku legislativou, která na tento rychlý rozvoj pružně reaguje.[9]

1.2 Kybernetický prostor

Zákon o kybernetické bezpečnosti, zákon č. 181/2014 Sb., definuje kyberprostor v ust. § 2 písm. a) jako *„digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.“*

Právě díky internetu, celosvětově distribuované počítačové síti, která je tvořena z dalších menších sítí, jež jsou vzájemně propojeny, je subjektům počítačové sítě umožněna vzájemná interakce, tedy komunikace, přenos dat a informací, nebo také poskytování služeb. Prostor, který díky internetu vznikl, a ve kterém se vše odehrává, je kybernetický prostor, který je virtuální, nemá žádné pomyslné hranice, skutečný začátek ani konec, a je neomezený. V tomto prostoru velmi důležitou pozici zastupují technologie a na ně napojené služby. Dalším podstatným aspektem kyberprostoru jsou informace, ale i dezinformace v něm obsažené, díky kterým má tato virtuální realita vliv na mínění uživatelů, a tudíž také dopad na svět reálný.[10]

1.3 Kybernetický útok

Kybernetický útok je škodlivé jednání útočníka, které je činěno v kybernetickém prostoru, a které je cíleno proti zájmům jiného subjektu. Avšak ne každý kybernetický útok, přestože vykazuje známky společenské škodlivosti, je trestný čin, jelikož se může stát, že absentuje ustanovení, pod které by bylo možné předmětný kybernetický útok subsumovat. Každé kybernetické protiprávní jednání je kybernetickým útokem, ale ne každý kybernetický útok je protiprávním z pohledu trestního práva, pakliže není takový čin zakotven v platné trestněprávní úpravě.[11]

---

[9] PORADA, Viktor a Karel RAIS. *Právní, kriminalistické a kybernetické aspekty kybernetické kriminality a bezpečnosti: pocta Vladimíru Smejkalovi*. Brno: Akademické nakladatelství CERM, 2021. ISBN 978-80-7623-065-1. s. 116-117.

[10] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. s. 42-46.

[11] Tamtéž, s. 55.

2 Sociální sítě

Sociální síť je typ služby poskytované poskytovatelem služeb informační společnosti ve virtuální realitě. Registrovaní uživatelé dané virtuální sociální sítě, fyzické či právnické osoby, na ní mají vytvořený svůj osobní nebo firemní profil, pod kterým vystupují, a to dle smluvních podmínek poskytovatele sociální sítě. Tito uživatelé si mohou díky této službě mezi sebou nejen vyměňovat či zveřejňovat informace, ale i sdílet například snímky, videa atp.[12]

Mezi nejpopulárnější sociální sítě dnešní doby lze řadit Facebook, Instagram, Snapchat, WhatsApp, Skype nebo YouTube a konkrétně v České republice, bylo dříve možné do tohoto demonstrativního výčtu zařadit i populární sociální síť Lidé.cz,[13] která však v roce 2020 zanikla. Jedním z důvodů pro ukončení jejího provozu byla i skutečnost, že se na ní vyskytovali sexuální predátoři.[14]

Na základě údajů zpracovaných Českým statistickým úřadem bylo zjištěno, že počet uživatelů sociálních sítí ve věku 16 let a více vzrostl od roku 2010 z 9,4 % na 53,8 %, a to k roku 2020.[15] Se stále zvyšující se popularitou sociálních sítí roste i trestná činnost, jež je v tomto prostředí páchána.[16] Tomu tak může být i z toho důvodu, že jsou sociální sítě pro možného útočníka místem, kde je mu značně usnadněn přístup k jeho potencionální oběti, protože tato oběť sama o sobě dobrovolně zveřejňuje osobní údaje na svém profilu.[17]

2.1 Odpovědnost za obsah na sociálních sítích

Internet je prostor, ve kterém existují subjekty, prostřednictvím nichž uživatelé sdílejí či na něm ukládají svůj obsah. Jedná se o subjekty, které zprostředkovávají tyto aktivity mezi internetem a uživateli, a právě tímto

[12] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. s. 151-152.
[13] Tamtéž, s. 153.
[14] KAPICIÁNOVÁ, Aneta. *Seznam.cz zavře v polovině prosince svou službu Lidé.cz*. [online]. Blog Seznam.cz, [cit. 22.10.2022]. Dostupné z: https://blog.seznam.cz/2020/11/seznam-cz-zavre-v-polovine-prosince-svou-sluzbu-lide-cz/
[15] *Česká republika – vývoj v čase. Tabulka 5.2: Osoby v ČR používající sociální sítě*. [online]. Český statistický úřad, [cit. 22.10.2022].
Dostupné z: https://www.czso.cz/documents/10180/122362692/0620042052.pdf/76f76896-4758-480a-8856-9d6658534cba?version=1.1
[16] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7. s. 226.
[17] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. s. 155.

subjektem jsou jinou osobou poskytované služby jako Facebook či YouTube. Tito zprostředkovatelé se nazývají *definiční autority*, a jsou zákonem označováni jako poskytovatelé služeb informační společnosti. Poskytování služeb informační společnosti je upraveno zákonem č. 480/2004 Sb., o některých službách informační společnosti (dále jen „zákon o některých službách informační společnosti“).[18] Dle tohoto zákona jsou sociální sítě řazeny pod poskytování služeb typu *hosting*, které je založeno na ukládání informací, jež jsou poskytnuty uživatelem takové služby.[19] Tento zákon byl do právního řádu České republiky implementován směrnicí 2000/31/ES, o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu na vnitřním trhu (dále jen „směrnice o elektronickém obchodu“), která byla přijata v reakci na praktickou nemožnost poskytovatele služeb informační společnosti monitorovat obsah sdílený uživateli, čímž zavedla vyloučení odpovědnosti poskytovatele za sdílený protiprávní obsah uživatelem, a to v případě splnění stanovených podmínek. Režim, ve kterém poskytovatel dodrží tyto podmínky stanovené směrnicí se nazývá *Safe Harbour*, též překládaný jako režim tzv. *bezpečných přístavů*, a umožňuje liberaci poskytovatele z odpovědnosti za protiprávní obsah.[20] Podmínky, které stanovují vyloučení odpovědnosti poskytovatele za protiprávní obsah, zakotvuje ust. § 5 zákona č. 480/2004 Sb., o některých službách informační společnosti, kdy:

„(1) Poskytovatel služby, jež spočívá v ukládání informací poskytnutých uživatelem, odpovídá za obsah informací uložených na žádost uživatele, jen

a) mohl-li vzhledem k předmětu své činnosti a okolnostem a povaze případu vědět, že obsah ukládaných informací nebo jednání uživatele jsou protiprávní, nebo

b) dozvěděl-li se prokazatelně o protiprávní povaze obsahu ukládaných informací nebo o protiprávním jednání uživatele a neprodleně neučinil veškeré kroky, které lze po něm požadovat, k odstranění nebo znepřístupnění takovýchto informací.

---

[18] PORADA, Viktor a Karel RAIS. *Právní, kriminalistické a kybernetické aspekty kybernetické kriminality a bezpečnosti: pocta Vladimíru Smejkalovi*. Brno: Akademické nakladatelství CERM, 2021. ISBN 978-80-7623-065-1. s. 104-105.

[19] DUFKOVA, Anna. *Režim Safe Harbour v rámci poskytování hostingových služeb.* [online]. Epravo.cz – Váš průvodce právem – Sbírka zákonů, judikatura, právo, [cit. 21.11.2022]. Dostupné z: https://www.epravo.cz/top/clanky/rezim-safe-harbour-v-ramci-poskytovani-hostingovych-sluzeb-108663.html

[20] PORADA, Viktor a Karel RAIS. *Právní, kriminalistické a kybernetické aspekty kybernetické kriminality a bezpečnosti: pocta Vladimíru Smejkalovi*. Brno: Akademické nakladatelství CERM, 2021. ISBN 978-80-7623-065-1. s. 105-106.

(2) Poskytovatel služby uvedený v odstavci 1 odpovídá vždy za obsah uložených informací v případě, že vykonává přímo nebo nepřímo rozhodující vliv na činnost uživatele.“

V případě, že jednání poskytovatele naplní znaky některého z výše uvedených jednání, „vypluje“ z onoho „bezpečného přístavu“ a může být právně odpovědný za protiprávní obsah zveřejněný uživatelem. V této věci je rovněž nezbytné zmínit judikaturu Soudního dvora Evropské Unie, konkrétně rozsudek ve věci C-324/09. Dle tohoto rozhodnutí nelze pod režim *Safe Harbour* řadit aktivní typ poskytovatelů, u kterých lze říci, že by obsah služby, jež poskytují, znali či měli o takovém obsahu přehled díky prováděnému monitoringu.[21]

Dále považuji za podstatné uvést, že dle ust. § 6 zákona o některých službách informační společnosti není po poskytovateli požadováno, aby prováděl dozor nad ukládaným či přenášeným obsahem a iniciativně zjišťoval možnost existence protiprávního obsahu.[22]

Již z výše uvedených skutečností je patrné, že primárně nesou odpovědnost za svou vlastní aktivitu na síti její uživatelé. V případě sdílení či ukládání nezákonného obsahu je uživatel za takové aktivity odpovědný. Až v případě „vyplutí z bezpečného přístavu“ může nést poskytovatel akcesorickou odpovědnost.[23]

2.1.1 Akt o digitálních službách (*Digital Services Act*)

Rychlý vývoj digitálních služeb má nepopiratelně masivní dopad na společnost, čímž je spojena i nutnost regulovat toto prostředí právem Evropské Unie. Od přijetí směrnice o elektronickém obchodu v roce 2000 se rozvoj těchto služeb natolik inovoval, že je nutné schválení takové právní úpravy v této oblasti, která bude na tento rychlý pokrok reagovat.[24]

[21] PORADA, Viktor a Karel RAIS. *Právní, kriminalistické a kybernetické aspekty kybernetické kriminality a bezpečnosti: pocta Vladimíru Smejkalovi*. Brno: Akademické nakladatelství CERM, 2021. ISBN 978-80-7623-065-1. s. 106.
[22] Tamtéž, s.108.
[23] Tamtéž, s. 104.
[24] Důvodová zpráva k návrhu nařízení Evropského parlamentu a Rady o jednotném trhu digitálních služeb (akt o digitálních službách) a o změně směrnice 2000/31/ES,
Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52020PC0825

Novým legislativním návrhem Evropské komise je nařízení Evropského parlamentu a Rady o jednotném digitálním trhu (akt o digitálních službách) a o změně směrnice 2000/31/ES (dále jen „akt“), který nabyl platnosti dne 16. 11. 2022. Avšak je nutné zavedení národních koordinátorů pro oblast digitálních služeb k datu 17. 2. 2024, kdy rovněž nastane jeho přímá aplikovatelnost na všechny aktem zavázané subjekty.[25]

Cílem nově přijaté právní úpravy je především zajištění základních práv a svobod v digitálním prostředí, zabezpečení ochrany uživatelů on-line, a to zejména restrikcí protizákonného obsahu[26] v podobě možnosti nahlášení nezákonného obsahu uživateli, zavedením ohlašovací povinnosti pro samotné platformy, které budou při podezření ze spáchání trestné činnosti proti životu či zdraví povinny oznámit závadný obsah příslušným orgánům činným v trestním řízení.[27] Zvýšená pozornost je kladena především na ty platformy, jejichž služby využívá přes 10 % spotřebitelů v rámci Evropské Unie. Ty budou podléhat dohledu, který bude vykonáván převážně na národní úrovni, ale i na unijní úrovni, a to konkrétně Evropskou komisí s podporou Evropského výboru pro digitální služby.[28] Jedná se pouze o výčet některých pravidel, které budou touto úpravou zavedeny.

[25] *Akt o digitálních službách: zajištění bezpečného online prostředí odpovědného vůči uživatelům.* [online]. Evropská komise, [cit. 21.11.2022].
Dostupné z: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_cs
[26] Tamtéž.
[27] *Evropský návrh regulace digitálních služeb – Centrum proti hybridním hrozbám.* [online]. Ministerstvo vnitra České republiky, [cit. 21.11.2022].
Dostupné z: https://www.mvcr.cz/chh/clanek/evropsky-navrh-regulace-digitalnich-sluzeb.aspx
[28] *Akt o digitálních službách: zajištění bezpečného online prostředí odpovědného vůči uživatelům.* [online]. Evropská komise, [cit. 21.11.2022].
Dostupné z: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_cs

3 Jednotlivé druhy kyberkriminality na sociálních sítích

V rámci této kapitoly je důkladně rozebírána kyberšikana, sexting, kybergrooming, kyberstalking a krádež virtuální identity. Dále jsou v příslušných podkapitolách uvedeny případy, pro lepší demonstraci dané problematiky, právní rámec trestné činnosti páchané v prostředí sociálních sítí a příslušná judikatura.

Součástí diplomové práce je rovněž kvantitativní výzkum, kterého se zúčastnilo 509 respondentů, konkrétně 367 osob ztotožňující se s ženským pohlavím (dále jen „ženy“), 134 s mužským pohlavím (dále jen „muži“) a 8 osob s jiným pohlavím. Pro tento výzkum byl zvolen internetový dotazník, okruh adresátů nebyl nikterak omezen, složení výzkumného vzorku je tedy heterogenní. Účast respondentů na výzkumu byla zcela dobrovolná a anonymní. V rámci dotazníkového šetření byli respondenti tázáni na otázky spojené s kyberšikanou, sextingem, kybergroomingem, kyberstalkingem a odcizením účtu na sociálních sítích. Cílem výzkumu bylo zjistit, jaké povědomí a zkušenosti mají respondenti s kyberkriminalitou na sociálních sítích, tedy obeznámenost s problematikou a její četnost. Dále byl realizovaný výzkum cílen převážně na oběti kyberkriminality na sociálních sítích, zejména zda jsou jimi častěji muži nebo ženy, a jaká věková kategorie je v tomto směru nejvíce ohrožena. Získaná data jsou prezentována vždy u tematicky příslušné podkapitoly společně s grafickým znázorněním.

Z důvodu nízkého zastoupení osob ztotožňujících se s jiným pohlavím, konkrétně v počtu 8 respondentů, nebude tento vzorek v následujících grafech dále zohledňován, neboť výsledky by nebyly pro takto nízký vzorek relevantní. Současně i s odkazem na to, že český právní řád vychází z dělení pohlaví na ženské a mužské.[29] Přesto však je nezbytné podotknout, že i těchto 8 respondentů neztotožňujících se s ženským ani mužským pohlavím, se s problematikou kyberkriminality na sociálních sítích rovněž potýkalo. Namísto 509 celkových respondentů bylo výchozím celkovým počtem v jednotlivých podkapitolách 501 respondentů.

[29] viz nález Ústavního soudu České republiky sp. zn. II.ÚS 2460/19 ze dne 7. 6. 2022.

3.1 Kyberšikana

Pro vymezení kyberšikany je nezbytné objasnění pojmu šikana. Šikana je úmyslné, dlouhodobější, agresivní jednání jedince či kolektivu namířené proti oběti, která sebe sama není schopná před takovým jednáním zdařile ochránit.[30] *„Šikana v reálném světě spočívá ve snaze útočníka ublížit, ponížit, zesměšnit, urazit jiného, ať fyzicky či psychicky.“*[31]

V případě kyberšikany probíhá takové jednání v kyberprostoru, a to prostřednictvím mobilního telefonu anebo internetu. Na rozdíl od „klasické“ šikany může útočník vystupovat v kyberprostoru anonymně a jeho jednání má dalekosáhlejší dopad co do publicity jeho jednání.[32] Dalším rozdílem je fakt, že útočník v případě kyberšikany může na svoji oběť útočit i v případě, je-li od své oběti polohou vzdálený, protože svou oběť šikanuje v kyberprostoru.[33]

Přes výše uvedené rozdíly je nutné podotknout, že ve vyšším počtu případů je šikana a kyberšikana vzájemně propojena, neboť příčinou kyberšikany mohou být již porušené sociální vtahy ze světa reálného, promítnuté do kyberprostoru.[34]

3.1.1 Znaky kyberšikany

Anonymita. Útočník může nabýt pocitu, že v případě anonymního vystupování na internetu jej nelze odhalit a zjistit jeho identitu.[35]

Časoprostor. Jelikož kyberšikana probíhá prostřednictvím ICT, může tak útočník činit v jakýkoliv čas, z jakéhokoliv místa, a jeho cílem může být kdokoliv. Prostor, ve kterém ke kyberšikaně dochází, je neomezený. Útočník tak může útočit opakovaně, například psaním urážlivých komentářů na sociálních sítích.[36]

---

[30] ZAVRŠNIK, Aleš. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7552-758-5. s. 27.
[31] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. s. 309.
[32] ZAVRŠNIK, Aleš. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7552-758-5. s. 27-28.
[33] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. s. 309.
[34] ČERNÁ, Alena. *Kyberšikana: průvodce novým fenoménem*. Praha: Grada, 2013. Psyché (Grada). ISBN 978-80-210-6374-7. s. 48-49.
[35] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. s. 310.
[36] Tamtéž, s. 310.

(Ne)zjistitelnost. V reálném životě může být „klasický“ typ šikany snáze zjistitelný, jelikož může mít viditelné zevní projevy, kterými jsou např. hematomy. Takové známky mohou být pro okolí oběti alarmující a pomohou k jejímu odhalení.[37]

Trvalost. Jednotlivé dílčí útoky kybernetické kriminality jsou v rámci kyberprostoru uchovány a stále trvají, a pro danou oběť nenabírá jednotlivý kybernetický útok konce, neboť jí může být neustále připomínán.[38]

Rysy útočníka. Rozdílem mezi „klasickým“ typem šikany a kyberšikany spočívá i v charakteristických atributech útočníka. V kyberprostoru může být útočníkem i takový jedinec, který není fyzicky zdatný nebo nemá příznivé sociální postavení v kolektivu atp. Obecně lze říci, že v kyberprostoru může být útočníkem kterýkoliv jedinec bez ohledu na jeho fyzické či sociální předpoklady.[39]

3.1.2 Projevy kyberšikany

Kyberšikana může být páchána několika způsoby, ale všechny tyto způsoby mají jeden společný cíl, a to buď své oběti ublížit, ponížit ji, zesměšnit ji nebo ji urazit. Mezi typické projevy kyberšikany se řadí:

1.) *„Pomlouvání, zastrašování, urážení, zesměšňování či jiné ztrapňování.*
2.) *Pořizování zvukových záznamů, videí či fotografií, jejich grafické či jiné upravování a následné zveřejňování s cílem poškodit (zesměšnit) vybranou osobu.*
3.) *Natáčení videí, při kterých je oběť napadána fyzicky či je jinak psychicky týrána a zesměšňována. Tato videa jsou následně zveřejněna online (jedná se o tzv. Happy Slapping).*
4.) *Vytváření sociálních účtů (úprava původních či vytváření nových profilů), diskusních portálů aj., které urážejí, pomlouvají nebo ponižují konkrétní osobu.*
5.) *Zneužívání cizího účtu-krádež identity.*
6.) *Provokování a napadání uživatelů v diskusních fórech.*
7.) *Odhalování cizích tajemství.*
8.) *Vydírání pomocí internetu.*

[37] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. s. 310.
[38] Tamtéž, s. 310.
[39] Tamtéž, s. 310.

9.) Obtěžování a pronásledování voláním, psaním zpráv nebo prozváněním.“[40]

Obecně lze formy kyberšikany rozčlenit do čtyř kategorií:

1.) kyberšikana slovní, a to prostřednictvím textových zpráv na sociální síti,
2.) kyberšikana obrazová, prostřednictvím fotografií anebo videí, jež agresor šíří či publikuje na sociální síti,
3.) kyberšikana vyčleňující, kdy hlavním cílem agresora je oběť vyčlenit, a to např. z určité sociální skupiny, sociální sítě atp.,
4.) kyberšikana podvodná, kdy agresor na sociálních sítích vystupuje podvodným způsobem, tím že se na sociální síti vydává za jinou osobu anebo po odcizení jejího účtu tento účet užívá.[41]

3.1.3 Případy kyberšikany

Případem kyberšikany je životní zkušenost 14leté studentky Anny Halman, která se obětí tohoto útoku stala dne 20. 10. v roce 2006 na polském gymnáziu ve městě Gdaňsk. Dívka byla obětí šikany a kyberšikany, když ve shora uvedeném roce byla ve třídě napadena svými čtyřmi spolužáky, přičemž jeden z útočníků byl jejím bratrancem. Napadení spočívalo v tom, že ji inkriminovaného dne proti její vůli útočníci vysvlékli, nevhodně se ji dotýkali a simulovali na dívce znásilnění a orální pohlavní styk. Jeden z útočníků pořídil videonahrávku útoku na své mobilní zařízení, a následně dívce společně vyhrožovali jejím zveřejněním na internetu, což útočníci posléze skutečně učinili. Přestože se Anna v důsledku nepoměru sil nebyla schopna útoku ubránit, a to ani se zastáním jiných spolužaček, podařilo se jí během útoku utéct do svého domova. O incidentu byla následně informována učitelka této třídy, která o tomto útoku zpravila dospělého bratra oběti, jenž na žádost své sestry rodičům o incidentu neřekl, a taktéž neučinila ani Anna. Ta následujícího dne spáchala sebevraždu oběšením. Případem se zabývala policie, díky které bylo zjištěno, že se nejednalo o ojedinělý útok těchto útočníků

[40] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. s. 310-311.
[41] ZAVRŠNIK, Aleš. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7552-758-5. s. 28.

proti Anně, ale že dívka čelila obdobným útokům již řadu týdnů, konkrétně od doby, kdy odmítla s jedním ze členů skupiny navázat partnerský vztah.[42]

Odborníci registrují případy kyberšikany, kdy útočníci jménem svých bývalých partnerek sdílí nabídky služeb sexuálního charakteru doložené o jejich osobní informace, např. telefonní číslo, a to bez jejich vědomí. Z těchto případů je patrné, že kyberšikana poškozuje oběť převážně psychicky, přičemž velký vliv na psychiku oběti má anonymita útočníka, jelikož oběť nezná jeho pravou identitu.[43]

Z šetření prováděného psychology bylo zjištěno, že oběť, která byla kyberšikanována, trpí psychickými následky v podobě hypersenzitivity, smutku, studu atp. U těchto osob se mohou z pohledu delšího časového období projevit i duševní onemocnění, např. deprese, ale i psychosomatické poruchy, jakými mohou být insomnie, bolesti hlavy atp. Nicméně následky se mohou u oběti vyskytovat i v rámci jejího běžného života, což se může projevit ku příkladu zhoršením školního prospěchu.[44]

3.1.4 Právní úprava kyberšikany

Zákon č. 40/2009 Sb., Trestní zákoník (dále jen „TrZ“) nezakotvuje skutkovou podstatu kyberšikany, a rovněž neupravuje ani šikanu „klasickou“. Jak je již výše uvedeno, kyberšikana může mít širokou škálu projevů, a tyto projevy lze subsumovat pod některé trestněprávní ustanovení. Avšak ne každé jednání, které je kyberšikanou, je trestným činem, a to z důvodu chybějícího ustanovení, pod které by bylo možné jednání útočníka podřadit. Takovým případem může být opakované zesměšňování jiného uživatele na sociální síti útočníkem, přičemž na takové jednání nelze aplikovat žádné trestněprávní ustanovení, nebo by byla taková aplikace velice komplikovaná.[45]

V případě páchání kyberšikany může pachatel svým jednáním naplnit skutkovou podstatu jednoho či více trestných činů zakotvených v TrZ, kdy

[42] Tým projektu E-bezpečí. *Anna Halman (Polsko, 2006).* [online]. E-bezpečí, [cit. 21.11.2022]. Dostupné z: https://www.e-bezpeci.cz/index.php/72-kazuistiky/1426-anna-halman-polsko-2006
[43] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7. s. 403.
[44] ZAVRŠNIK, Aleš. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7552-758-5. s. 29.
[45] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. s. 312.

se nejčastěji může jednat o vydírání podle ust. § 175 TrZ, pomluvu podle ust. § 184 TrZ, nebezpečné vyhrožování podle ust. § 353 TrZ, nebezpečné pronásledování podle ust. § 353 TrZ[46], přičemž nebezpečnému pronásledování se budu hlouběji věnovat v podkapitole zaměřené na kyberstalking.

a) Vydírání podle ust. § 175 TrZ

Vydírání je zakotveno v ust. § 175 odst. 1 TrZ *„Kdo jiného násilím, pohrůžkou násilí nebo pohrůžkou jiné těžké újmy nutí, aby něco konal, opominul nebo trpěl, bude potrestán odnětím svobody na šest měsíců až čtyři léta nebo peněžitým trestem.*“ V případě trestného činu vydírání je trestná i příprava, a to podle ust. § 175 odst. 5 TrZ.

TrZ v této skutkové podstatě chrání svobodné rozhodování jedince. Objektivní stránku představuje určitá podoba nátlaku vyvíjená pachatelem, pod kterým je jiná osoba nucena něco konat, opominout či trpět[47] a v případě, že by tak učinila, byla by zřetelně postihnuta po citové nebo majetkové stránce.[48] K naplnění objektivní stránky trestného činu vydírání dojde již v okamžiku, kdy pachatel užil násilí, pohrůžky násilí či jiné těžké újmy, v úmyslu donutit jinou osobu něco konat, opominout či trpět, a to proti její svobodné vůli. Jedná se tak o předčasný dokonaný trestný čin, kdy není podstatné, zda se osoba vyvíjenému nátlaku podřídila, a pachatel tak naplnil jím stanovený cíl. Pro naplnění subjektivní stránky trestného činu je vyžadováno úmyslné zavinění pachatele, kterým může být jak osoba fyzická, tak osoba právnická.[49]

Nátlak pachatele spočívající v pohrůžce násilím nebo pohrůžce jiné těžké újmy může být činěn i prostřednictvím sociální sítě, e-mailové schránky, mobilního telefonu atp., a osoba, vůči které tato výhrůžka směřuje, nemusí být takovému jednání fyzicky přítomna. Pohrůžka násilím může představovat jednak násilí okamžité, pakliže se osoba vůli pachatele nepodvolí v daný okamžik, anebo může znamenat násilí vykonané v budoucnu. A pachatel může hrozit i tím, že násilí vykoná na jiné osobě, např. rodinném příslušníku, věci či zvířeti. Pohrůžka jiné

[46] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7. s. 403.
[47] KALVODOVÁ, Věra, ŠČERBA, Filip. In: ŠČERBA, Filip a kol. Trestní zákoník. 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8 s. 1448.
[48] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7. s. 408.
[49] KALVODOVÁ, Věra, ŠČERBA, Filip. In: ŠČERBA, Filip a kol. Trestní zákoník. 1. vydání. Praha: C. H. Beck, 2020. s. 1448-1453.

těžké újmy pak představuje širokou škálu možných jednání pachatele. V souvislosti se sociálními sítěmi je příhodné uvést výhrůžku zveřejnění intimních fotografií, přeposlání fotografií tohoto charakteru rodinným příslušníkům, čímž může být poškozený postižen na své cti anebo dobré pověsti. Výhrůžka může rovněž spočívat ve zveřejnění intimních fotografií např. dítěte poškozeného. Pro naplnění této skutkové podstaty není rozhodné, zda skutečně pachatel těmito fotografiemi disponuje, a je tak způsobilý svou výhrůžku naplnit, neboť již tímto vyhrožováním byl chráněný objekt zasažen.[50]

b) Pomluva podle ust. § 184 TrZ

Podle ust. § 184 TrZ odst. 1 *„Kdo o jiném sdělí nepravdivý údaj, který je způsobilý značnou měrou ohrozit jeho vážnost u spoluobčanů, zejména poškodit jej v zaměstnání, narušit jeho rodinné vztahy nebo způsobit mu jinou vážnou újmu, bude potrestán odnětím svobody až na jeden rok.*

Podle odst. 2 *„Odnětím svobody až na dvě léta nebo zákazem činnosti bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem.“* Přičemž v případě sociálních sítí se na trestný čin pomluvy bude aplikovat ust. § 184 odst. 2 TrZ.[51]

Uvedená skutková podstata chrání čest, dobrou pověst a vážnost jedince. Objektivní stránka pak představuje takové jednání, které spočívá ve sdělení lživého údaje o jiné osobě, který je svou podstatou schopen zásadně ohrozit její seriózност u spoluobčanů. Následek spočívá v ohrožení vážnosti osoby poškozeného, dle demonstrativního výčtu zejména v jeho pracovních či rodinných vztazích, anebo je-li tento lživý údaj schopen způsobit mu jinou vážnou újmu. Pro dokonání tohoto trestného činu je podstatné posuzovat to, zda je taková lživá informace způsobilá jiné osobě způsobit újmu, nikoliv to, zda skutečně újmu způsobila. Tento lživý údaj přitom může být sdělen ústně, prostřednictví sociální sítě, zveřejněním na internetu atp. Avšak se musí jednat o takový údaj, u kterého je možné verifikovat jeho pravdivost, pakliže není možné jeho pravdivost objektivně ověřit, nejedná se o trestný čin pomluvy podle ust. § 184 TrZ. Z hlediska subjektivní stránky

[50] KALVODOVÁ, Věra, ŠČERBA, Filip. In: ŠČERBA, Filip a kol. Trestní zákoník. 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 1448-1450.
[51] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7. s. 383.

je u pachatele vyžadováno úmyslné zavinění v podobě úmyslu přímého anebo nepřímého. Pachatel jedná s nepřímým úmyslem např. tehdy, když šíří takový údaj, u kterého si neověří jeho správnost, přestože ví, že je taková informace způsobilá ohrozit vážnost jiné osoby u spoluobčanů. Pachatelem trestného činu pomluvy může být fyzická i právnická osoba.[52]

S nejvyšší pravděpodobností jsou právě sociální sítě nejčastějším místem, kde je tento trestný čin páchán. Na sociálních sítích je uživatelům umožněno sdělovat a zveřejňovat své názory a jiná sdělení, sdílet fotografie či videonahrávky, s čímž je však spjata určitá četnost negativních příspěvků, které mohou vykazovat zákonné znaky trestného činu pomluvy.[53]

c) Nebezpečné vyhrožování podle ust. § 353 TrZ

Dle ustanovení § 353 odst. 1 TrZ *„(1) Kdo jinému vyhrožuje usmrcením, těžkou újmou na zdraví nebo jinou těžkou újmou takovým způsobem, že to může vzbudit důvodnou obavu, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti.“* A rovněž nebezpečné vyhrožování, stejně jako pomluva dle ust. § 184, může být činěno dálkově, tedy i prostřednictvím sociálních sítí.[54]

V této skutkové podstatě TrZ chrání interpersonální soužití před závažnými výhrůžkami. Objektivní stránka představuje vyhrožování pachatelem jiné osobě, a to alternativně, usmrcením, těžkou újmou na zdraví nebo jinou těžkou újmou, takovým způsobem, který je schopný u této jiné osoby (u poškozeného) vyvolat důvodnou obavu. Tento trestný čin je řazen do skupiny ohrožovacích trestných činů, a pro naplnění objektivní stránky nemusí nastat následek ve formě poruchy, avšak rovněž ani to, aby se poškozený skutečně obával realizace učiněné výhrůžky.[55]

Učiněná výhrůžka musí být schopná vyvolat důvodnou obavu, kterou „se rozumí vyšší stupeň tísnivého pocitu ze zla, kterým je vyhrožováno.“ Přičemž nelze izolovat samotnou vyhrůžku, ale je nezbytné hodnotit celou situaci, ve které k takovému konání pachatele došlo, komplexně. Samotné prohlášení pachatele v sobě nemusí zahrnovat přímo vyhrůžku usmrcením, způsobením těžké

[52] KALVODOVÁ, Věra, ŠČERBA, Filip. In: ŠČERBA, Filip a kol. Trestní zákoník. 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 1509-1512.
[53] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7. s. 384.
[54] Tamtéž, s. 393.
[55] PROVAZNÍK, Jan. In: ŠČERBA, Filip a kol. Trestní zákoník. 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 2909.

újmy na zdraví či jiné těžké újmy, pakliže je vyhrůžka spolu s dalším jednáním pachatele schopna v poškozeném důvodnou obavu některého z těchto následků skutečně vyvolat. Na to, zda je vyhrůžka způsobilá vzbudit v jiném obavu, může mít vliv celá řada faktorů. Především se posuzuje samotný obsah vyhrůžky, osoba pachatele, jeho tělesné a osobností rysy, které je třeba konfrontovat s osobou poškozeného (zda je vyhrožováno dítěti, osobě vysokého věku). Důležitou roli pak může hrát ku příkladu i vzájemný sociální vztah mezi pachatelem a poškozeným.[56]

Z hlediska subjektivní stránky trestného činu je vyžadováno úmyslné zavinění ve formě úmyslu přímého i nepřímého. Pro naplnění znaku subjektivní stránky trestného činu nebezpečného vyhrožování není podstatné, zda pachatel v době, kdy jiné osobě vyhrožoval, měl v úmyslu v ní důvodnou obavu z realizace výhrůžky skutečně vyvolat. Podstatné je, že se jedná o takovou výhrůžku, která je svou povahou způsobilá v jiném skutečně důvodnou obavu vyvolat. Subjektem může být osoba fyzická i právnická.[57]

Vzhledem ke stále četnějšímu výskytu kyberšikany by mohlo být prospěšné její legální zakotvení, které by bylo možné na patologické projevy činěné v kyberprostoru aplikovat. Domnívám se, že legální definice by rovněž upřesnila, jaké jednání konkrétně by bylo považováno za protiprávní z pohledu trestního práva, a mohlo by dojít k budoucí prevenci kyberšikany nejen na sociálních sítích.

3.1.4.1 Právní úprava kyberšikany na Slovensku

Slovenská republika vzhledem ke stále častějšímu výskytu kyberšikany, i s ohlédnutím na přírůstek této problematiky v období koronavirové krize započaté v roce 2019, zakotvila trestný čin nebezpečného elektronického obtěžování ve svém trestním zákoně s účinností od 1. 7. 2021.[58] Skutková podstata nebezpečného elektronického obtěžování je definována v ust. § 360b Trestního zákona, z. č. 300/2005 Z. z., kdy je stanoveno:

[56] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7. s. 394-395.
[57] PROVAZNÍK, Jan. In: ŠČERBA, Filip a kol. Trestní zákoník. 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 2914.
[58] VANC, Martina. *Trestný čin nebezpečného elektronického obťažovania*. [online]. Právne Noviny – zrozumiteľné informácie pre všetkých, [cit. 28.11.2022].
Dostupné z: https://www.pravnenoviny.sk/trestny-cin-nebezpecneho-elektronickeho-obtazovania

„Kdo úmyslně prostřednictvím elektronické komunikační služby, počítačového systému nebo počítačové sítě podstatným způsobem zhorší kvalitu života jiného tím, že

a) jej dlouhodobě ponižuje, zastrašuje, neoprávněně jedná jeho jménem nebo dlouhodobě jinak obtěžuje, nebo

b) neoprávněně zveřejní nebo zpřístupní třetí osobě obrazový, zvukový nebo obrazově zvukový záznam jeho projevu osobní povahy získaný s jeho souhlasem, způsobilý značnou měrou ohrozit jeho vážnost nebo přivodit mu jinou vážnou újmu na právech,

bude potrestán odnětím svobody až na tři roky.“[59]

Slovenská trestněprávní úprava, stejně jako česká trestněprávní úprava, neměla do této novelizace trestního zákona žádné ustanovení, které by upravovalo samostatně kyberšikanu. Stejně jako je tomu v České republice, byly projevy kyberšikany subsumovány pod existující ustanovení trestního zákona např. trestného činu vydírání, nátlaku, a to v případě, bylo-li takové podřazení možné. Nicméně s ohledem na to, že určité projevy kyberšikany nebylo možné trestat v souladu s trestním zákonem, došlo k zakotvení trestného činu nebezpečného elektronického obtěžování. Díky zaplnění těchto mezer jsou nově pokryty projevy kyberšikany, kdy například podle písm. b) výše zmíněného ustanovení pachatel publikuje na internetu (tedy i sociálních sítích) záznam, který byl sice pořízen se souhlasem oběti, ale ne za účelem zveřejnění, a kdy se tímto zveřejněním změní k horšímu kvalita života poškozeného.[60]

Z pohledu systematiky byl tento trestný čin začleněn do IX. hlavy Trestního zákona, která upravuje trestné činy proti jiným právům a svobodám. Z hlediska obligatorních znaků skutkové podstaty je objektem trestného činu elektronického obtěžování ochrana soužití občanů před kyberšikanou. Objektivní stránka je vymezena alternativně, a spočívá ve značném zhoršení kvality života poškozeného tím, že jej pachatel buďto dlouhodobě ponižuje, zastrašuje, neoprávněně jedná jeho jménem či ho jinak po delší časové období obtěžuje. Anebo pachatel neoprávněně zveřejní či zpřístupní třetí osobě záznam osobního charakteru např. fotografii, videonahrávku, kterou pořídil se souhlasným stanoviskem poškozeného, ale jež

[59] ust. § 360b Trestního zákona, z. č. 300/2005 Z. z., překlad vlastní.

[60] VANC, Martina. *Trestný čin nebezpečného elektronického obťažovania*. [online]. Právne Noviny – zrozumiteľné informácie pre všetkých, [cit. 28.11.2022].
Dostupné z: https://www.pravnenoviny.sk/trestny-cin-nebezpecneho-elektronickeho-obtazovania

nebyla pořízena za účelem jejího šíření jiné osobě, a kdy je takovéto šíření schopné značným způsobem ohrozit serióznost poškozeného anebo mu přivodit jinou vážnou újmu na právech. Pro naplnění subjektivní stránky trestného činu je vyžadováno úmyslné zavinění, přičemž dostačujícím je i úmysl nepřímý. Pachatelem může být pouze osoba fyzická.[61]

Dle důvodové zprávy čerpal zákonodárce pro vymezení těchto obligatorních znaků trestného činu z platné trestněprávní úpravy. Jak je již výše zmíněno, určité projevy kyberšikany bylo možné postihnout již před novelizací slovenského Trestního zákona, a v tomto ohledu může být problematické zdvojení právní úpravy. V důvodové zprávě je uvedeno, že zakotvením trestného činu elektronického obtěžování nedochází k duplikaci právní úpravy, kterou je možné na projevy kyberšikany aplikovat, ale že je touto novelou platná trestní úprava doplňována. Zároveň zákonodárce uvádí odlišnosti od jiných trestných činů s obdobnými zákonnými znaky.[62]

Zákonná úprava elektronického obtěžování nicméně nepamatuje na hybridní trestnou činnost, kdy pachatel o konání trestného činu pořizuje videonahrávku, kterou následně publikuje v on-line prostoru (viz výše uvedený případ *Anna Halman*). Zveřejnění této nahrávky v kyberprostoru není trestným činem elektronického obtěžování postižitelné, jelikož podle první alternativy není činěno dlouhodobě, a v případě druhé alternativy absentuje souhlas poškozeného s pořízením videonahrávky.[63]

V neposlední řadě je nutné zmínit princip *ultima ratio,* kdy trestní právo představuje prostředek, který je možné užít až za situace, kdy nelze uplatnit prostředků jiného právního odvětví. Trestní právo je tedy až nejzazším prostředkem pro ochranu společnosti. Avšak ve slovenské právní úpravě absentuje přestupek, pod který by bylo možné kyberšikanu subsumovat, tedy praktická nemožnost postihnout společensky méně závažné jednání správním právem. V některých případech by byla možná aplikace skutkových podstat přestupků proti občanskému soužití nebo přestupků proti majetku, nicméně skutková podstata přestupku kyberšikany zakotvena není.[64]

[61] GŘIVNA, Tomáš, Martin RICHTER a Hana ŠIMÁNOVÁ, ed. *Vliv nových technologií na trestní právo*. Praha: Auditorium, 2022. ISBN 978-80-87284-95-7. s. 333-335.
[62] Tamtéž, s. 333.
[63] Tamtéž, s. 338.
[64] Tamtéž, s. 342-345.

3.1.5 Judikatura

Okresní soud v Liberci dne 9. 5. 2013 rozhodoval ve věci obžalované X a poškozené Y, kdy obžalovaná vytvořila e-mailovou adresu, která odpovídala e-mailové adrese, jež užívala poškozená. Z této e-mailové adresy zaslala na e-mailovou adresu poškozené odkaz s tím, že v případě jeho stvrzení by obžalované bylo umožněno zasílat e-mailové zprávy pod e-mailovou adresou poškozené, a současně tedy jejím jménem. Dále pak na sociální síti Facebook založila profil, kde jako jméno na tomto profilu uvedla jméno poškozené, a to bez jejího souhlasu. Tento profil byl aktivní od 22. 4. 2010 do 25. 3. 2011, kdy byl smazán. V mezidobí, kdy byl tento profil aktivní, na něm obžalovaná zveřejňovala bez souhlasu poškozené její fotografie, k nimž získala přístup z webových stránek poškozené, a které obžalovaná přetvořila za účelem ponížení poškozené. Dále na tomto facebookovém účtu obžalovaná zveřejňovala příspěvky, které byly v rozporu s politickým smýšlením poškozené, příslušnicí a funkcionářkou KSČM. Jejich čtenáři se mylně domnívali, že tyto názory vychází od poškozené, čímž byla poškozené způsobena újma v oblasti její politické kariéry. Poškozená rovněž uvedla, že v důsledku jednání obžalované utrpěla negativní zdravotní následky. Obžalovaná byla rozsudkem Okresního soudu v Liberci uznána vinou pro přečin poškození cizích práv podle ust. § 181 odst. 1 písm. a) TrZ, proti kterému podala obžalovaná odvolání pro nesprávnost tohoto rozsudku v celém jeho rozsahu. Přičemž uvedla, že již druhostupňový soud v této věci rozhodoval usnesením (čj.: 31 To 494/2012-334, ze dne 27. 2. 2013), ve kterém rozsudek prvostupňového soudu v odsuzující části zrušil a nařídil tomuto soudu věc znovu projednat a v této věci vydat rozhodnutí.[65]

Dne 26. 3. 2014 rozhodoval o podaném odvolání Krajský soud v Ústí nad Labem – pobočka v Liberci, kdy zrušil rozsudek Okresního soudu ze dne 9. 5. 2013 a vynesl zprošťující rozsudek v této věci. Z odůvodnění je zřejmé, že ve věci nebylo obžalované bez pochybností prokázáno, že se dopustila skutku, pro nějž byla obžaloba podána. Na základě výpovědi, jež byla doplněna ve veřejném zasedání soudu druhého stupně, bylo zjištěno, že nelze s jistotou říci, jaká osoba se k zájmové e-mailové adrese připojovala. Dle svědecké a znalecké výpovědi podané soudu prvního stupně nelze s dostatečnou jistotou zjistit, jaká

[65] Rozsudek Krajského soudu v Ústí nad Labem – pobočka v Liberci ze dne 26. 3. 2014, sp. zn. 31To247/2013.

osoba na sociální síti Facebook profil založila. Z podané svědecké výpovědi vyplývá, že ústředna provozovatele sociální sítě Facebook, jež má sídlo ve Spojených státech amerických, sice má technické možnosti pro vyhledání osoby, která konkrétní profil vytvořila, avšak dožádání ústředny této společnosti lze pouze cestou právní pomoci v případě spáchání závažných trestných činů, a tudíž není možné zvolit tento postup v tomto případě. Mimo jiné obžalovaná u soudu prvního stupně uvedla, že k danému počítači měla přístup jakákoliv osoba, která se v obydlí nacházela, což nebylo vyvráceno.[66]

Případem kyberšikany se také zabýval Okresní soud v Klatovech dne 28. 3. 2022. Obviněná dne 11. 1. 2022 prostřednictvím svého facebookového účtu odeslala zprávu poškozené, předsedkyni Poslanecké sněmovny Parlamentu České republiky, s obsahem ve znění: *„Ty svině. Za své názory patříš postavit ke zdi, vyhodit z okna, nebo si dát psychologické testy na psychiatrii. Zasloužíš si být znásilněna a mučena alespoň deseti imigranty.“* Okresní soud kvalifikoval jednání obviněné jako přečin nebezpečného vyhrožování podle ust. **§ 353 odst. 1 TrZ**, a v této věci vydal samosoudce trestní příkaz, kterým byla obviněná odsouzena k peněžitému trestu v celkové výši 12 000 Kč.[67]

3.1.6 Výzkum

a) Povědomí o kyberšikaně

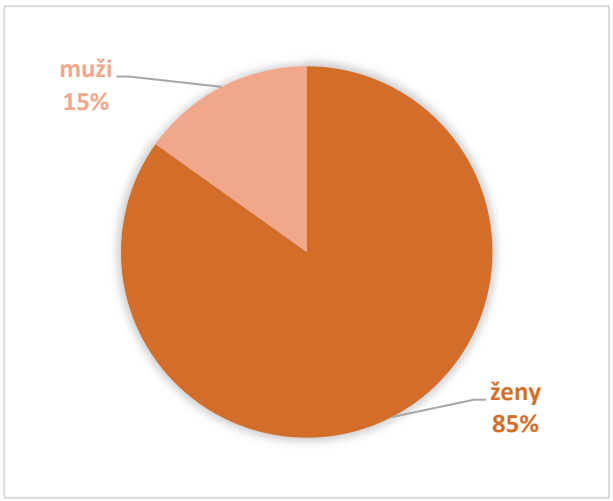
Z celkových 501 (100 %) respondentů jich **499 (99,6 %)** uvedlo, že zná pojem kyberšikana. Lze tak obecně říci, že společnost je s touto problematikou obeznámena.

b) Oběti kyberšikany

Z 501 (100 %) respondentů jich celkem **152 (30,3 %)** uvedlo, že byli během svého života obětí kyberšikany.

[66] Rozsudek Krajského soudu v Ústí nad Labem – pobočka v Liberci ze dne 26. 3. 2014, sp. zn. 31To247/2013.
[67] Trestní příkaz Okresního soudu v Klatovech ze dne 28. 3. 2022, sp. zn. 1 T 62/2022.

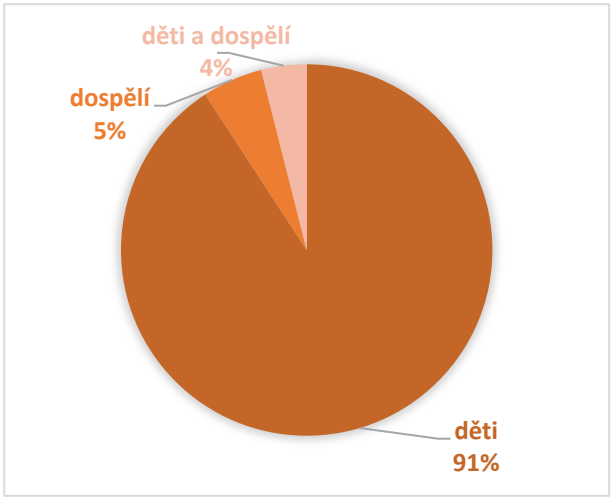
I. Oběti kyberšikany podle pohlaví



Z výsledků dotazníkového šetření vyplývá, že jsou častěji kyberšikanovány ženy. Nicméně vezeme-li v úvahu vyšší procentuální zastoupení žen v dotazníkovém šetření, jsou výsledky následující:

- z celkového počtu 367 (100 %) žen v dotazníkovém šetření 129 (35,1 %) uvedlo, že bylo obětí kyberšikany,
- v případě mužů pak z celkových 134 (100 %) totéž uvedlo 23 (17,2 %) respondentů. **Závěrem lze říci, že na základě výsledků z provedeného výzkumu jsou obětí kyberšikany častěji ženy.**

II. Oběti kyberšikany podle věku



V tomto případě je grafické znázornění koncipováno v souladu s ust. § 126 TrZ, dle kterého se dítětem rozumí osoba mladší 18 let. Graf je složen ze tří kategorií, a tedy děti, dospělí, a současně děti a dospělí, neboť někteří respondenti

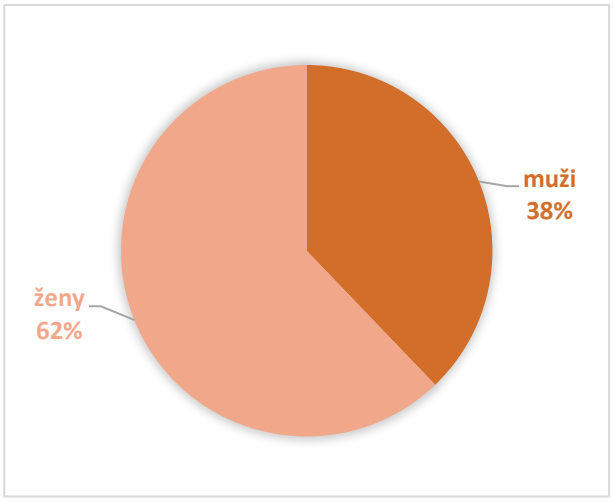
byli obětí kyberšikany během svého života vícekrát. **Z výsledků dotazníkového šetření lze říci, že jsou častěji kyberšikanovány děti.**

Výzkumem rizikového chování českých dětí v prostřední internetu realizovaným v roce 2014 bylo zjištěno, že se s některým z projevů kyberšikany střetlo 50,9 % dětí, a to z celkového počtu 28 232 respondentů ve věku 11-17 let.[68]

c) Agresoři kyberšikany

Z celkového počtu 501 (100 %) respondentů jich 37 (7,4 %) uvedlo, že kyberšikanovalo jinou osobu.

I. Agresoři podle pohlaví



Z výsledků realizovaného výzkumu vyplývá, že častěji kyberšikanují ženy nežli muži. Nicméně vezmeme-li v úvahu vyšší procentuální zastoupení respondentů ženského pohlaví v dotazníkovém šetření, jsou výsledky následovné:

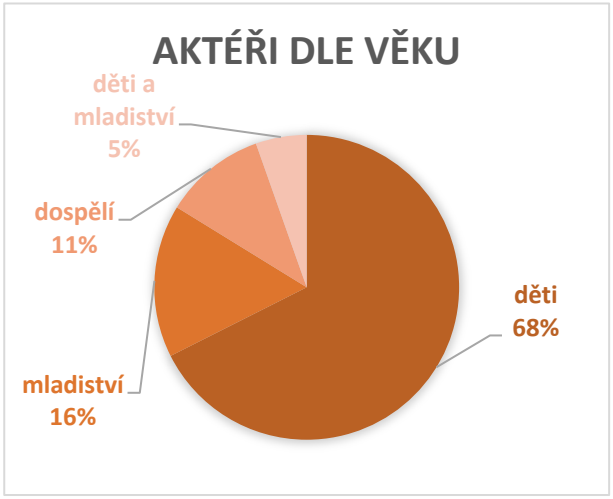
- z celkového počtu 367 (100 %) žen v dotazníkovém šetření jich 23 (6,3 %) uvedlo, že kyberšikanovalo jinou osobu,

[68] Kopecký, Kamil; Kožíšek, Martin. [online]. *Výzkum rizikového chování českých dětí v prostředí internetu 2014,* [cit. 19.3.2022]. Dostupné z: https://www.e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/61-vyzkum-rizikoveho-chovani-ceskych-deti-v-prostredi-internetu-2014-prezentace/file

- v případě mužů pak z celkových 134 (100 %) totéž uvedlo 14 (10,4 %) respondentů. **Na základě těchto výsledků lze říci, že naopak častěji kyberšikanují muži.**

Hanka Macháčková a Lenka Dědková uvádějí v publikaci *Kyberšikana: průvodce novým fenoménem*, že výsledky výzkumů, jež obsahovaly členění agresorů a obětí podle pohlaví nejsou vždy shodné. Častým důvodem pro rozdílnost získaných dat je definice kyberšikany uvedená v daném výzkumu a současně i to, na jaké formy kyberšikany je dotazník zaměřen. A to z důvodu, že osoby ženského a mužského pohlaví často navštěvují internet za odlišným účelem. Osoby mužského pohlaví spíše vyhledávají internetové hry, zatímco ženy se naopak častěji účastní veřejných diskuzí. Muži se tak spíše střetnout s přímou podobou kyberšikany, tedy přímo urážením, ženy naopak se zostuzováním a pomluvou, tedy nepřímou podobou kyberšikany.[69]

II. Agresoři podle věku



V případě dělení aktérů dle věku jsem postupovala v souladu se zákonem č. 218/3002 Sb., o odpovědnosti mládeže za protiprávní činy a soudnictví ve věcech mládeže (dále jen „zákon o soudnictví ve věcech mládeže“), kdy jsem agresory členila do kategorií na děti (osoby mladší 15 let), mladistvé (osoby, jež dovršily 15 let a nepřekročily 18 rok svého věku)[70] a dospělé osoby (osoby, jež překročily 18 rok svého věku). Tyto tři kategorie jsou rozšířeny o kategorii děti a mladiství,

[69] ČERNÁ, Alena. *Kyberšikana: průvodce novým fenoménem*. Praha: Grada, 2013. Psyché (Grada). ISBN 978-80-210-6374-7. s. 68.
[70] Podle ust. § 2 odst. 1 písm. b), c) zákona o soudnictví ve věcech mládeže.

a to z toho důvodu, že dva respondenty nelze s jistotou zařadit pouze do jedné z těchto kategorií, neboť v dotazníku uvedli delší časové období. Přičemž je nezbytné zdůraznit, že osoba, jež v době spáchání činu nedovršila 15 let, není podle ust. § 25 TrZ trestně odpovědná. **Z výsledků provedeného výzkumu vyplývá, že nejčastěji kyberšikanují děti.**

3.2 Sexting

Jedním z rizikových jevů v oblasti internetu, a zvláště pak na sociálních sítích, je sexting. Pojem sexting, v českém předkladu sextování, vznikl spojením slov „sex“ a „textování“.[71] Jedná se o formu elektronické komunikace, jejíž podstata spočívá v rozesílání sexuálně laděných zpráv, fotografií či videonahrávek sugestivní povahy, např. fotografie zachycující atraktivní výraz, erotické prádlo, anebo explicitní povahy, a to snímek obnaženého těla. Tento materiál rozesílá buďto osoba, která jej pořídila, tzv. *self-texting*, anebo jiný uživatel, který takového materiálu určitým způsobem nabyl, tzv. *peer-texting*. Avšak tyto základní typy se mohou navzájem prolnout v okamžiku, kdy autor dobrovolně zašle vlastní sexuálně laděný materiál jedné osobě, která jej bez jeho vědomí šíří mezi jiné uživatele, kterým původně tento materiál určen nebyl. A právě v tom tkví zmíněná rizikovost sextingu.[72]

Pokud je sexting provozován mezi osobami zletilými s jejich souhlasem, nejedná se z pohledu trestněprávního o protiprávní čin, na rozdíl od případů, kdy jsou obsahem této formy komunikace materiály zobrazující dítě.[73] Trestně postižitelným je tedy sexting mezi dítětem a dospělou osobou anebo mezi dětmi navzájem,[74] jsou-li tyto osoby trestně odpovědné.

3.2.1 Rizikovost sextingu

Obsah zasílaného materiálu je bezesporu citlivé povahy, který může osoba, jež takový materiál získá, jednoduše zneužít. Její motiv pak může být různorodý. Osoba, jenž disponuje materiálem sexuální povahy jiného jedince, ho pod pohrůžkou jeho rozšíření může vydírat k zaslání dalšího takové materiálu, k znovunavázání partnerského vztahu, zaslání peněžní částky, k pohlavnímu styku atp.[75]

---

[71] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. s. 314.
[72] SZOTKOWSKI, René. *Sexting u českých dětí*. Olomouc: Univerzita Palackého v Olomouci, 2020. ISBN 978-80-244-5793-2. s. 32-33.
[73] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. s. 315-317.
[74] SZOTKOWSKI, René. *Sexting u českých dětí*. Olomouc: Univerzita Palackého v Olomouci, 2020. ISBN 978-80-244-5793-2. s. 37.
[75] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. s. 315.

Sexting je tedy provozován buďto se souhlasem obou stran, konsensuálně, charakteristicky v partnerských a jiných milostných vztazích, nebo nekonsensuálně, bez souhlasu druhé strany. V případě nekonsensuálního sextingu je získání tohoto materiálu dosahováno nátlakem, vydíráním atp., a může se v tomto případě jednat o trestnou činnost.[76]

Získaný materiál může představovat prostředek k pomstě, často mezi bývalými partnery. Partner nejprve konsensuálně získá intimní materiál od druhého, a po rozpadu jejich milostného vztahu ho již bez jeho souhlasu zveřejní za účelem msty, poškození nebo zesměšnění. Šíření sexuálně laděného materiálu za účelem msty je také označováno jako *revenge porn*, v českém znění pornografie z pomsty,[77] a je jedním z projevů kyberšikany.[78]

Následky sextingu mohou u obětí, jejichž intimní materiály byly zneužity, vyvolat zdravotní komplikace, zejména častější výskyt psychopatologií. U osob, jejichž intimní fotografie anebo videa byla rozšířena po internetu, byl zaznamenán vyšší výskyt deprese, úzkosti či pocitu méněcennosti. Častěji pak tyto osoby užívají omamné a psychotropní látky.[79]

3.2.2 Sexting ve spojení s dalšími rizikovými jevy

Intimní materiál získaný prostřednictvím sextingu je možné využít i k jiným kybernetickým útokům, a to ke kyberšikaně, kybergroomingu a kyberstalkingu.[80]

3.2.2.1 Sexting jako specifická podoba kyberšikany

Intimní materiál může být v rámci kyberšikany zneužit útočníkem za účelem zostuzení, ztrapnění anebo vydírání oběti, a takový útok může mít až destruktivní dopad na její psychiku. Přičemž tento materiál útočník může získat přímo od osoby, která ho pořídila anebo jej nabude jiným způsobem, např. krádeží identity či od jiné osoby, které byl v minulosti poskytnut.[81]

---

[76] SZOTKOWSKI, René. *Sexting u českých dětí*. Olomouc: Univerzita Palackého v Olomouci, 2020. ISBN 978-80-244-5793-2. s. 37.
[77] Tamtéž, s. 40.
[78] Tým projektu E-bezpečí. *Co je to revenge porn.* [online]. E-bezpečí, [cit. 2.3.2023]. Dostupné z: https://www.e-bezpeci.cz/index.php/o-projektu/realizani-tym/71-trivium/2341-revenge-porn
[79] SZOTKOWSKI, René. *Sexting u českých dětí*. Olomouc: Univerzita Palackého v Olomouci, 2020. ISBN 978-80-244-5793-2. s. 44.
[80] Tamtéž, s. 77.
[81] Tamtéž, s. 77-78.

Jak je již výše uvedeno, typem útoku, kdy je útočníkem oběť kyberšikanována rozesíláním intimního materiálu, je pornografie z pomsty. Ta se v České republice objevila např. v souvislosti s případem tzv. *Roztahovaček*.[82] Jednalo se o řadu profilů založených na sociální síti Facebook, jež vznikly za účelem zveřejňování intimních fotografií žen, které byly autorům této stránky poskytnuty jejich bývalými partnery. Partneři jich přitom nabyli formou konsensuálního sextingu za doby trvání jejich partnerského vztahu. Na profilu zveřejněná fotografie byla doplněna o dehonestující popisek. Ze strany autorů těchto stránek došlo k naplnění znaků trestného činu pomluvy podle ust. § 184 TrZ.[83] Nicméně pokud by tyto příspěvky neobsahovaly popisek urážlivé povahy, je třeba se zamyslet nad jinou možnou právní kvalifikací. Podle názoru JUDr. A. Beranové, Ph.D. v díle „*Vliv nových technologií na trestní právo*" by v případě, kdy osoba dobrovolně zašle svůj intimní materiál druhému, který jej již bez souhlasu této osoby zveřejní, byla možná trestněprávní kvalifikace podle ust. § 181 TrZ.[84] Skutková podstata trestného činu poškození cizích práv podle tohoto ustanovení chrání nemajetková práva osob, a to jak osob fyzických, tak právnických, včetně státu. Objektivní stránka je naplněna, pokud pachatel podvodným jednáním buďto uvede jinou osobu v omyl, anebo využije jejího omylu, a způsobí tímto svým jednáním následek v podobě vážné újmy na právech jiné osoby. Osoba, která utrpěla újmu na svých právech může být odlišnou od té, jež byla uvedena v omyl nebo jejíhož omylu bylo pachatelem využito.[85] Z hlediska subjektivní stránky je vyžadováno úmyslné zavinění, přičemž dostačujícím je úmysl nepřímý. Pachatelem může být osoba fyzická, a rovněž i osoba právnická.[86] Přičemž zda byla v daném případě pachatelovým jednáním způsobena vážná újma na právech, a bude tak posuzováno jako trestný čin, anebo zda bude postihováno jiným než trestním právem, je třeba hodnotit vzhledem k okolnostem daného případu. Obzvláště pak na jakém právu byl poškozený zasažen, jaká byla míra způsobené újmy na tomto právu a jaký dopad mělo jednání pachatele

[82] Tým projektu E-bezpečí. *Co je to revenge porn.* [online]. E-bezpečí, [cit. 2.3.2023]. Dostupné z: https://www.e-bezpeci.cz/index.php/o-projektu/realizani-tym/71-trivium/2341-revenge-porn
[83] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. s. 315-316.
[84] GŘIVNA, Tomáš, Martin RICHTER a Hana ŠIMÁNOVÁ, ed. *Vliv nových technologií na trestní právo*. Praha: Auditorium, 2022. ISBN 978-80-87284-95-7. s. 254-255.
[85] Tamtéž, s. 252.
[86] KALVODOVÁ, Věra, ŠČERBA, Filip. In: ŠČERBA, Filip a kol. Trestní zákoník. 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 1486.

na poškozeného.[87] V případě pornografie z pomsty by tato právní kvalifikace připadala v úvahu, pokud pachatel vytvoří na sociální síti profil pod jménem poškozené, a na tomto profilu publikuje pornografický anebo jiný choulostivý materiál, jež mu sama v minulosti zaslala, čímž uvádí v omyl jiné uživatele vyskytující se na této síti, kteří tento materiál zhlédli a domnívali se, že jej sdílela sama poškozená. Za situace, kdy pachatel zveřejní choulostivý materiál získaný od poškozené na základě jejich intimního vztahu založeného na vzájemné důvěře, by byla rovněž možná kvalifikace podle ust. § 181 TrZ, neb ji tímto jednáním uvádí v omyl. Poškozená totiž v tomto případě předpokládá, že materiál zaslaný pachateli na základě jejich vzájemné intimity zůstane uchován pouze mezi nimi.[88]

Nicméně tento názor nesdílí část odborné veřejnosti, dle které by takové případy neměly být posuzovány podle ust. § 181 TrZ, ale podle ust. § 86 zákona č. 89/2012 Sb., občanského zákoníku, neb se jedná o občanskoprávní delikt. Tento názor je podložen tím, že pachatel v době nekonsensuálního zveřejnění intimním materiálem druhé osoby zaslaným mu dobrovolně plně disponuje, a tudíž poškozenou nemůže uvádět v omyl či jejího omylu využívat.[89]

3.2.2.2 Sexting jako nerozlučná součást kybergroomingu

Predátor v případě kybergroomingu navazuje kontakt s obětí, kterou je obvykle dítě ve věkovém rozmezí 11-17 let. Během jejich virtuální komunikace se snaží získat její obnažené fotografie, videa, kterými ji posléze může vydírat za účelem dosažení jejich osobní schůzky.[90]

3.2.2.3 Sexting v souvislosti s kyberstalkingem

Kyberstalking spočívá v záměrném, dlouhodobém, opakovaném pronásledování oběti v on-line prostředí, které oběti snižuje kvalitu jejího života, jelikož je jednáním útočníka omezována na svém soukromí a osobní svobodě. Spojitost se sextingem je dána tím, že útočník může pro manipulaci a vydírání oběti užít jejího intimního materiálu, kterým disponuje.[91]

---

[87] GŘIVNA, Tomáš, Martin RICHTER a Hana ŠIMÁNOVÁ, ed. *Vliv nových technologií na trestní právo*. Praha: Auditorium, 2022. ISBN 978-80-87284-95-7. s. 253.
[88] Tamtéž, s. 255.
[89] Tamtéž, s. 254-255.
[90] SZOTKOWSKI, René. *Sexting u českých dětí*. Olomouc: Univerzita Palackého v Olomouci, 2020. ISBN 978-80-244-5793-2. s. 8.
[91] Tamtéž, s. 82.

3.2.3 Sexting u dětí

Sexting je spojen s problematikou dětské pornografie, zejména má značný vliv na její šíření ve virtuálním světě.[92] Výroba a šíření dětské pornografie je problematika spojená s komerčním zneužíváním dětí, jež představovalo hlavní téma Stockholmského světového kongresu konaného v roce 1996. Dle tohoto kongresu se komerčním zneužitím dítěte rozumí výměna peněz, předmětů či jiné odměny v naturáliích za využití dítěte pro sexuální účely. Mezi tři hlavní formy komerčního zneužívání dětí patří obchodování s dětmi, dětská prostituce a dětská pornografie.[93]

Docent J. Chmelík v díle *Mravnost, pornografie a mravnostní kriminalita* popisuje dětskou pornografii jako jakýkoli materiál v textové, obrazové nebo zvukové formě, který používá děti v sexuálním smyslu. V případě obrazové pornografie je zachyceno dítě během skutečné či fingované sexuální činnosti nebo exponování jeho pohlavních orgánů za účelem uspokojení sexuálních potřeb uživatele, a současně taková činnost zahrnuje i výrobu, šíření nebo používání takového materiálu. Zvuková pornografie obsahuje předstíraný či skutečný záznam dětského hlasu za účelem ukojení sexuálních potřeb uživatele, a taktéž zahrnuje i výrobu, šíření nebo používání takového materiálu.[94]

Materiál používající děti v sexuálním kontextu se stále častěji vyskytuje na internetových stránkách, ke kterým má prakticky neomezený přístup jakýkoliv uživatel s připojením k internetu po celém světě.[95] Děti jsou pro predátory mnohdy snadným cílem, jelikož si neuvědomují, že prostředí sociálních sítí se od skutečného světa tolik neliší, a ani to, že jsou vzájemně propojeny. Následky zaslání takového materiálu se mohou projevit nejen v prostředí internetu, ze kterého není téměř možné již zaslaný materiál odstranit, a který je v něm často navždy uchován, ale i ve světě reálném.[96]

Na pomoc v boji proti dětské pornografii byla přijímána řada právních dokumentů na úrovni mezinárodní i unijní právní úpravy.[97] V rámci mezinárodní

[92] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. ISBN 978-80-7387-545-9. s. 62.
[93] CHMELÍK, Jan. *Mravnost, pornografie a mravnostní kriminalita*. Praha: Portál, 2003. ISBN 80-7178-739-6. s. 52.
[94] Tamtéž, s. 52.
[95] Tamtéž, s. 53.
[96] SZOTKOWSKI, René. *Sexting u českých dětí*. Olomouc: Univerzita Palackého v Olomouci, 2020. ISBN 978-80-244-5793-2. s. 59.
[97] ZAVRŠNIK, Aleš. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7552-758-5. s. 21.

právní úpravy byla dne 23. 11. 2001 v Budapešti přijata Úmluva o počítačové kriminalitě (dále jen „Úmluva“), kterou Česká republika ratifikovala 22. 8. 2013 s platností od 1. 12. 2013. Cílem Úmluvy je především harmonizace právních řádů smluvních stran Úmluvy na poli trestných činů páchaných v kyberprostoru.[98] Úmluva upravuje v hlavě 3 (Trestné činy související s obsahem) čl. 9 trestné činy související s dětskou pornografií. Strany Úmluvy se přitom zavazují do svých právních řádů přijmout legislativní opatření kriminalizující celou řadu jednání páchaných v kyberprostoru ve spojitosti s dětskou pornografií.[99] Dne 25. 10. 2007 s platností pro Českou republiku od 1. 9. 2016 byla přijata Lanzarotská úmluva Rady Evropy na ochranu dětí proti sexuálnímu vykořisťování a pohlavnímu zneužívání,[100] jež klade značný důraz na preventivní opatření a poskytuje vyšší úroveň ochrany obětem.[101] Jedním z důvodů přijetí Lanzarotské úmluvy je stálé rozrůstání této problematiky, a to zejména v důsledku zvyšujícího se počtu uživatelů ICT.[102] Na úrovni unijní úpravy byla přijata 13. 12. 2011 směrnice Evropského parlamentu a Rady 2011/93/EU o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV.

3.2.3.1 Právní úprava dětské pornografie v souvislosti s fenoménem sextingu

Pokud osoba vybídne dítě k pořízení a zaslání sexuálně laděného materiálu může spáchat trestný čin výroby a jiného nakládání s dětskou pornografií podle ust. § 192 TrZ, trestný čin zneužití dítěte k výrobě pornografie podle ust. § 193 TrZ, dále pak přichází v úvahu i ohrožování výchovy dítěte podle ust. § 201 TrZ[103] a další trestné činy v závislosti na okolnostech daného případu. V souvislosti s právní úpravou sextingu u dětí se budu hlouběji věnovat základním skutkovým podstatám trestných činů podle ust. § 192 TrZ a ust. § 193 TrZ.

---

[98] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. s. 332.
[99] GŘIVNA, Tomáš a Radim POLČÁK, ed. *Kyberkriminalita a právo*. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4. s. 170-171.
[100] Sdělení č. 59/2016 Sb. m. s., Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy Rady Evropy o ochraně dětí proti sexuálnímu vykořisťování a pohlavnímu zneužívání.
[101] ZAVRŠNIK, Aleš. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7552-758-5. s. 21.
[102] Preambule Úmluvy Rady Evropy o ochraně dětí proti sexuálnímu vykořisťování a pohlavnímu zneužívání.
[103] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. s. 317.

a) Výroba a jiné nakládání s dětskou pornografií podle ust. § 192 TrZ

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

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

(3) Kdo vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě nebo osobu, jež se jeví být dítětem, anebo

kdo kořistí z takového pornografického díla,

bude potrestán odnětím svobody na šest měsíců až tři léta, zákazem činnosti nebo propadnutím věci.

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

a) jako člen organizované skupiny,

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

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

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

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

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

Všechny tři základní skutkové podstaty, které tvoří trestný čin podle ust. § 192 TrZ, mají společný objekt. Avšak ohledně toho, co je pod primární ochranou tohoto ustanovení, vznikla v rámci odborné veřejnosti neshoda. Dle právního názoru docenta F. Ščerby v komentáři *Ščerba a kol.* chrání základní skutkové podstaty uvedené v odstavcích 1 až 3 primárně morální principy společnosti před dětskou pornografií, jejíž výroba a jiné nakládání s ní je nezákonné a společností neakceptovatelné z pohledu uznávaných mravních hodnot. Druhotně ve smyslu sekundárního objektu chrání děti před jejich zneužíváním k výrobě pornografického materiálu a s jeho nakládáním, jehož zasažení není pro dokonání tohoto trestného činu nezbytné. Zejména je oporou tohoto tvrzení skutečnost, že dětskou pornografií je rovněž materiál zobrazující nebo jinak využívající osobu,

jež se jeví být, nikoliv je, dítětem (viz níže). Nicméně v souvislosti s objektem trestného činu podle ust. § 192 TrZ se objevil názor obsažený v jiných komentářích a publikacích (srov. *Šámal a kol. 2012* s. 1891, *Draštík a kol. 2015* s. 1036), dle kterého ust. § 192 TrZ primárně chrání děti před jejich zneužíváním k pornografickým účelům.[104]

V důsledku toho, že primárním objektem trestného činu podle ust. § 192 TrZ je ochrana morálních hodnot[105], nikoliv ochrana dětí před jejich zneužíváním k pornografickým účelům, lze vyvodit dvě právní konsekvence. V první řadě není možné u osob mladších 18 let uplatnit zásadu, podle které nemůže být pachatelem osoba, kterou příslušné ustanovení chrání, a tudíž pachatelem může být i mladistvý. V druhé řadě není vyloučen jednočinný souběh trestných činů výroby a jiného nakládání s dětskou pornografií podle ust. § 192 odst. 3 TrZ a zneužití dítěte k výrobě pornografie podle ust. § 193 TrZ, jelikož objekty těchto trestných činů nejsou totožné. Zatímco objektem u trestného činu podle ust. § 193 TrZ je ochrana dítěte, v případě ust. § 192 TrZ to jsou již zmíněné morální principy společnosti odsuzující dětskou pornografii.[106]

Pro rozebrání základních skutkových podstat je nezbytné objasnění pojmů:

I. Dětská pornografie

Ust § 192 odst. 1 a 3 blíže specifikuje dětskou pornografii, když vymezuje její formu jako „*fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě nebo osobu, jež se jeví být dítětem.“* Přičemž vymezení pojmu „pornografické dílo“ v naší právní úpravě absentuje. Za pornografické dílo lze dle judikatury považovat „*jakýkoliv předmět, který je-li pozorován ať přímo nebo prostřednictvím technického zařízení, zvláště intenzivním a vtíravým způsobem zasahuje a podněcuje samotný sexuální pud. Současně takové dílo podle převládajících názorů většiny členů společnosti hrubě*

[104] ŠČERBA, Filip. In: ŠČERBA, Filip a kol. Trestní zákoník. 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 1561-1562.
[105] viz Usnesení Nejvyššího soudu ze dne 28. 4. 2021, sp. zn. 8 Tdo 271/2021, dle kterého se objekty trestných činů podle ust. § 192 odst. 3 TrZ a ust. § 193 TrZ neshodují, a taktéž ani jejich objektivní stránka (s výjimkou „kořistění“, kde má přednost přísnější ust. § 193 TrZ). Jednočinný souběh trestného činu podle ust. § 192 odst. 3 TrZ s trestným činem podle ust. § 193 odst. 1 TrZ je tedy vzhledem k uvedenému možný. Zároveň je nutné říci, že tato ustanovení nejsou v poměru speciality, ani subsidiarity a nebyl shledán ani žádný jiný důvod pro vyloučení jednočinného souběhu v tomto případě.
[106] ŠČERBA, Filip. In: ŠČERBA, Filip a kol. Trestní zákoník. 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 1562.

porušuje uznávané morální normy společnosti a vyvolává v nich pocit studu. Pro pornografický charakter je rozhodující obsah celého díla, nikoli jen jeho určitá část, výseč, kapitola nebo úryvek apod.“[107] Při výkladu dětské pornografie je nezbytné reflektovat definici dětské pornografie obsažené ve směrnici č. 2011/93/EU (dále jen „Směrnice“), neboť právní úprava obsažená v ust. § 192 TrZ je důsledkem její implementace.[108] Dle této Směrnice se za dítě považuje osoba mladší 18 let a dětskou pornografii definuje v čl. 2 písm. c) jako „*i) jakýkoliv materiál, který zobrazuje dítě, které se účastní skutečného nebo předstíraného jednoznačně sexuálního jednání, ii) jakékoli zobrazení pohlavních orgánů dítěte prvotně k sexuálním účelům, iii) jakýkoliv materiál, který zobrazuje osobu se vzhledem dítěte, která se účastní skutečného nebo předstíraného jednoznačně sexuálního jednání, nebo každé zobrazení pohlavních orgánů osoby se vzhledem dítěte k prvotně sexuálním účelům, nebo iv) realistické obrázky dítěte, které se účastní jednoznačně sexuálního jednání, nebo realistické obrázky pohlavních orgánů dítěte k prvotně sexuálním účelům.“*[109] Dle judikatury lze za dětskou pornografii „*pokládat např. snímky obnažených dětí v polohách vyzývavě předvádějících pohlavní orgány za účelem sexuálního uspokojení, dále pak snímky dětí zachycující polohy skutečného či předstíraného sexuálního styku s nimi, popř. i jiné obdobně sexuálně dráždivé snímky dětí. Nejde-li o takové snímky, pak závěr o pornografickém charakteru díla nelze bez dalšího dovozovat jen z toho, že jsou za účelem uspokojení osob trpících sexuální deviací (tj. osob, pro které jsou sexuálně atraktivní nedospělé osoby) zpřístupňovány takovými prostředky, které tyto osoby vyhledávají.“*[110] Jelikož legální definice dětské pornografie v TrZ absentuje, posouzení, zda se v konkrétním případě jedná o dětskou pornografii, náleží orgánům činným v trestním řízení a odborníkům z řad znalců.[111]

Za značně problematický je považován tzv. *sharenting*. Jedná se o případ, kdy dětskou pornografii pořizují a šíří přímo rodiče vlastního dítěte, např. pořídí fotografii obnaženého dítěte v bazénku a následně ji nahrají na svůj profil

[107] JELÍNEK, Jiří. *Trestní právo hmotné: obecná část, zvláštní část*. 7. aktualizované a doplněné vydání. Praha: Leges, 2019. Student (Leges). ISBN 978-80-7502-380-3. s. 619-620.
[108] ŠČERBA, Filip. In: ŠČERBA, Filip a kol. Trestní zákoník. 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 1563.
[109] čl. 2 písm. a), c) směrnice Evropského parlamentu a rady 2011/93/EU ze dne 13. 12. 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV.
[110] Usnesení Nejvyššího soudu ze dne 28. 12. 2004, sp. zn. 7 Tdo 1077/2004.
[111] SZOTKOWSKI, René. *Sexting u českých dětí*. Olomouc: Univerzita Palackého v Olomouci, 2020. ISBN 978-80-244-5793-2. s. 62.

na sociální síti. Přestože rodiče v tomto případě nepořídili snímek za účelem sexuálního uspokojení, může být v tomto smyslu zneužit predátory, kteří se v on-line prostředí vyskytují. Dle názoru docenta F. Ščerby vyjádřeného v komentáři *Ščerba a kol.* by bylo posouzení takového materiálu jako dětské pornografie nesprávné, neboť rodiče nepořizovali tuto fotografii za účelem sexuálního uspokojení, a rovněž nepředpokládali, že by v tomto kontextu mohla být fotografie jejich dítěte predátorem zneužita. Posouzení fotografie jako pornografického díla v důsledku toho, že byla zneužita k jinému účelu, než ke kterému byla vytvořena, by vykazovalo subjektivistický přístup, který by neměl být v trestním právu akceptován.[112]

II. Dítě

Podle ust. § 126 TrZ je osoba, která je mladší 18 let, považována za dítě. Posledním dnem, kterým je oběť považována za dítě, je podle ust. § 139 TrZ den před dosažením 18. roku jejího života. Přičemž nabytí plné svéprávnosti před dosažením 18 let není z pohledu trestního práva podstatné.[113] Směrnice ani TrZ neberou v úvahu pohlavní zletilost dítěte. V České republice je pohlavní styk legální od 15 let (viz ust. § 187 TrZ), a nastává tak tzv. *právní paradox*, kdy mladistvý sice může mít legálně pohlavní styk, avšak jakákoliv jeho dokumentace již legální není.[114]

III. Osoba, jež se jeví být dítětem

Dětskou pornografií se rozumí i takový materiál, který ve skutečnosti nezobrazuje či jinak nevyužívá dítě, ale osobu, která svou vizáží, chováním, ošacením anebo v kontextu celého díla jako dítě působí, což může v průměrném divákovi vyvolat přesvědčení, že se o dítě skutečně jedná. V případě, kdy by takový divák byl schopen rozpoznat anebo by se alespoň domníval, že vyobrazená osoba pouze předstírá, že je dítětem, nejednalo by se o dětskou pornografii.[115] Dle názoru sexuologů by naopak mohlo být používání dospělých osob, které se za děti pouze vydávají, spíše přínosné ve smyslu snížení případných rizik hrozících od osob

[112] ŠČERBA, Filip. In: ŠČERBA, Filip a kol. Trestní zákoník. 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 1564.
[113] Tamtéž, s. 1523.
[114] SZOTKOWSKI, René. *Sexting u českých dětí*. Olomouc: Univerzita Palackého v Olomouci, 2020. ISBN 978-80-244-5793-2. s. 112.
[115] ŠČERBA, Filip. In: ŠČERBA, Filip a kol. Trestní zákoník. 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 1564-1565.

se sexuální parafilií, předmětem jejichž zájmu vždy budou dívky anebo chlapci mladší 18 let, a to i pod hrozbou trestního postihu.[116]

Za dětskou pornografii je považován i takový materiál, který vskutku realisticky zobrazuje nebo jinak využívá osobu uměle vytvořenou, např. počítačem vytvořenou animaci, která se divákovi jeví jako skutečné dítě.[117] V některých publikacích se lze setkat s termínem „dětská kyberpornografie“[118] nebo tzv. „animovaná dětská pornografie“[119] Kriminalizaci animované dětské pornografie část odborné veřejnosti odmítá[120], dle J. Chromého by však její legalizace pouze podpořila mínění, že je dětská pornografie v souladu s morálními hodnotami naší společnosti.[121]

Objektivní stránkou základní skutkové podstaty v odstavci prvním je přechovávání dětské pornografie. Přechováváním je míněna držba takového materiálu a libovolná dispozice s ním. Není podstatné, zda má pachatel takový materiál fyzicky přímo k dispozici, zásadní je, že má takový materiál ve své moci. Přičemž jej může mít uschovaný na pevném disku počítače, v mobilním telefonu, v e-mailové schránce atp. Není podstatné, zda se ku příkladu počítač, který je v držbě pachatele, a jehož pevný disk obsahuje dětskou pornografii, nachází na pracovišti, v obydlí, rekreačním objektu či dalším jiném místě. Pro naplnění objektivní stránky této skutkové podstaty je stěžejní, že si je pachatel vědom toho, že dětskou pornografii přechovává, přičemž není podstatné, jakým způsobem se k ní dostal.[122]

Naproti tomu objektivní stránkou druhé základní skutkové podstaty obsažené v odstavci druhém je získání přístupu k dětské pornografii za využití ICT. Pachatel v tomto případě nemá dílo ve své moci, tudíž jej nepřechovává, ale ICT využívá za účelem vyhledání a seznámení se s dětskou pornografií, např. se stane

---

[116] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7. s. 286.
[117] ŠČERBA, Filip. In: ŠČERBA, Filip a kol. Trestní zákoník. 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 1565.
[118] ZAVRŠNIK, Aleš. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7552-758-5. s. 23.
[119] JELÍNEK, Jiří. *Trestní právo hmotné: obecná část, zvláštní část*. 7. aktualizované a doplněné vydání. Praha: Leges, 2019. Student (Leges). ISBN 978-80-7502-380-3. s. 621.
[120] Tamtéž, s. 621.
[121] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7. s. 286.
[122] ŠČERBA, Filip. In: ŠČERBA, Filip a kol. Trestní zákoník. 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 1565-1566.

členem skupiny na sociální síti, jejíž činnost je zaměřena na vzájemné sdílení dětské pornografie.[123] Tato skutková podstata by měla dopadat zejména na osoby, kvůli kterým se dětská pornografie v on-line prostředí vyskytuje, a kteří přístup k ní získávají obvykle po zaplacení stanovené finanční částky.[124]

Objektivní stránku základní skutkové podstaty v odstavci třetím pachatel naplní, když *„vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří“* dětskou pornografii (alinea první), anebo kořistí-li z ní (alinea druhá). Alinea první uvádí široké spektrum jednání, přičemž v souvislosti se sociálními sítěmi budou uvedeny dva možné příklady zaměřené na výrobu a veřejné zpřístupnění tohoto materiálu. Výrobou je jakékoliv zhotovení dětské pornografie, např. natočení videa obsahujícího dětskou pornografii, vyfocení pohlavních genitálií dítěte atp. Za výrobu lze tedy pokládat i případ, kdy si dva mladiství natočí jejich pohlavních styk pouze pro vlastní potřebu. Pokud pachatel činí dětskou pornografii veřejně přístupnou, tak ji v případě sociálních sítí umístí veřejně tak, aby se s jejím obsahem mohl seznámit neomezený okruh uživatelů dané platformy. Není přitom podstatné, zda se uživatelé s tímto obsahem seznámí všichni najednou, nebo postupně za sebou v průběhu času. Skutková podstata podle ust. § 193 odst. 3 TrZ alinea druhá postihuje kořistění z dětské pornografie, kdy se takovýmto jednáním rozumí dosažení jakéhokoliv majetkového prospěchu, potažmo jiné výhody plynoucí z její výroby, distribuce či zpřístupnění. Dále je důležité podotknout, že se všechny tři kvalifikované skutkové podstaty váží pouze k tomuto odstavci.[125]

Pro všechny tři základní skutkové podstaty je z hlediska naplnění subjektivní stránky požadováno úmyslné zavinění. Pachatel tedy musí vědět, že se jedná o dětskou pornografii. Pachatelem může být kterákoliv trestně odpovědná fyzická osoba, včetně mladistvého, a rovněž i osoba právnická.[126]

[123] ŠČERBA, Filip. In: ŠČERBA, Filip a kol. Trestní zákoník. 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 1566.
[124] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7. s. 288.
[125] ŠČERBA, Filip. In: ŠČERBA, Filip a kol. Trestní zákoník. 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 1556-1568.
[126] Tamtéž, s. 1567.

b) Zneužití dítěte k výrobě pornografie podle ust. § 193 TrZ

Trestného činu zneužití dítěte k výrobě pornografie se dopustí ten, kdo *„přiměje, zjedná, najme, zláká, svede nebo zneužije dítě k výrobě pornografického díla nebo kořistí z účasti dítěte na takovém pornografickém díle“,* za což mu může být uložen trest odnětí svobody v délce trvání jednoho roku až pěti let.

Objektem je zde zájem na ochraně dětí před sexuálním zneužíváním pro pornografické účely, a rovněž je předmětem ochrany jejich mravní rozvoj a edukace, zejména v oblasti zdravé sexuality. K naplnění objektivní stránky přitom může dojít širokou škálou možných jednání.[127]

Pod pojmem „přiměje“ se rozumí určitý nátlak, který je pachatelem na dítě vyvíjen, a který může mít podobu pobízení, prosby, návrhu atp., a to včetně násilného jednání či jiného způsobu donucení. Zejména se jedná o případy, kdy pachatel zneužívá blízkého vztahu, jež s dítětem má.[128]

„Zjednání“ znamená uzavření dohody, jejíž obsahem je účast dítěte na výrobě pornografického materiálu. S uzavřením této dohody musí obě strany, tedy dítě a pachatel, výslovně či konkludentně souhlasit.[129]

„Najmutí“ je specifickou podobou zjednání, neb je v tomto případě rovněž uzavírána dohoda. Nicméně podstatným znakem najmutí je úplata, v peněžité či jiné podobě.[130]

„Zlákáním“ je míněno přesvědčení dítěte k účasti na výrobě dětské pornografie, přičemž tak pachatel činí přislíbením různých benefitů a pozitiv plynoucích z takové účasti, např. vysoký finanční zisk, zajištění jeho anonymity atp.[131]

„Svedení“ znamená vyvolání rozhodnutí v dítěti účastnit se výroby pornografického materiálu, zejména tím, že o něm pachatel mluví pouze v superlativech, dané dítě přemlouvá anebo zdůrazňuje benefity, jež z účasti plynou atp. Oproti zlákání, které může směřovat i vůči neurčitému okruhu dětí ku příkladu učiněním nabídky na sociální síti, směřuje svedení vždy vůči jedné konkrétní osobě.[132]

---

[127] ŠČERBA, Filip. In: ŠČERBA, Filip a kol. Trestní zákoník. 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 1573.
[128] Tamtéž, s. 1546-1573.
[129] Tamtéž, s. 1546.
[130] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7. s. 314.
[131] ŠČERBA, Filip. In: ŠČERBA, Filip a kol. Trestní zákoník. 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 1546.
[132] Tamtéž, s. 1546-1547.

Pokud pachatel zapojí dítě do účasti na výrobě pornografického materiálu bez respektování jeho vůle, jedná se o případ zneužití dítěte. O zneužití dítěte lze hovořit v případě, kdy pachatel dítěti tvrdí, že zachycuje fotografie k jiným než pornografickým účelům, čímž ho uvede v omyl nebo jeho omylu tímto jednáním zneužije. Anebo pokud pachatel využije bezbrannosti dítěte, která je zapříčiněna užitím návykové či psychotropní látky, stavem spánku, nebo která je způsobena nízkým věkem, pro který není schopno pochopit smysl jednání pachatele.[133]

„Kořistění“ viz výklad k ust. § 192 odst. 3 s rozdílem, že v tomto případě pachatel získá takový prospěch již z účasti dítěte na pornografickém materiálu, ku příkladu když rodič obdrží finanční částku za dovezení jeho potomka na místo natáčení.[134]

Z hlediska subjektivní stránky se požaduje úmyslné zavinění a pachatelem může být fyzická i právnická osoba.[135]

3.2.3.2 Hypotetické situace v prostředí sociálních sítí a jejich právní kvalifikace

Docent F. Ščerba uvádí v komentáři *Ščerba a kol.* v současné době vyskytující se případy v on-line prostředí, zejména na sociálních sítích, společně s jejich právní kvalifikací.

1. V případě, kdy pachatel navázal komunikaci skrze určitou sociální síť s dítětem a požádal ho o zaslání nahých fotografií jeho těla, přičemž si byl vědom, že tyto fotografie mají povahu pornografie a rovněž, že se jedná o osobu mladší 18 let. A zároveň:

a) tak dítě učinilo poté, co jej pachatel k zaslání těchto fotografií přemluvil. Pokud se jednalo o dítě, které dovršilo 15 let, dopustil by se pachatel trestného činu podle ust. § 193 odst. 1 TrZ (neb dítě k zaslání těchto fotek svedl) v konkurenci s návodem podle ust. § 24 odst. 1 písm. b) TrZ k provinění podle ust. § 192 odst. 3 TrZ. Pokud se však jednalo o dítě, které nedovršilo 15 roku svého života, byla by právní kvalifikace odlišná. Pachatel by se v tomto případě dopustil trestného činu podle ust. § 193 odst. 1 TrZ a současně se jako nepřímý pachatel dopustil trestného

[133] ŠČERBA, Filip. In: ŠČERBA, Filip a kol. Trestní zákoník. 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 1574.
[134] Tamtéž, s. 1574.
[135] Tamtéž, s. 1574.

činu podle ust. § 192 odst. 3 TrZ, neb k jeho spáchání užil osobu, která není trestně odpovědná.

b) V případě, kdy by pachatel požádal dítě o obnaženou fotografii, kterou vyfotilo již v minulosti, dopustil by se trestného činu podle ust. § 192 odst. 1 TrZ, neboť by fotografii obdržel a volně by s ní disponoval, tedy ji přechovával.

c) Pakliže dítě v rámci komunikace na sociální síti pachateli na jeho prosbu zpřístupní obnaženou fotografii, kterou má uloženou v paměti svého počítače, jedná ze strany pachatele k naplnění znaků trestného činu podle ust. § 192 odst. 2 TrZ.

d) Pokud by pachatel komunikoval s dítětem prostřednictvím videohovoru (tedy živého přenosu on-line), a tato nezletilá osoba by na popud pachatele předvedla pornografické představení, došlo by ze strany pachatele k naplnění znaků trestného činu účasti na pornografickém představení podle ust. § 193a TrZ.[136]

3.2.4 Judikatura

Dne 19. 11. 2019 byl obžalovaný P.B. uznán rozsudkem Krajského soudu v Brně vinným ze spáchání následujících trestných činů:

I. zločinem sexuálního nátlaku podle ust. § 186 odst. 1 alinea první, alinea druhá, odst. 5 písm. a) TrZ, dílem spáchaným ve stádiu pokusu podle ust. § 21 odst. 1 TrZ, přečinem výroby a jiného nakládání s dětskou pornografií podle ust. **§ 192 odst. 2 a 3 TrZ**, přečinem zneužití dítěte k výrobě pornografie podle ust. **§ 193 odst. 1 TrZ**, přečinem ohrožování výchovy dítěte podle ust. § 201 odst. 1 písm. a) TrZ, když dne 16. 4. 2017 na sociální síti Facebook, kde se pod falešným profilem prezentoval jako dívka, a prostřednictvím kterého navázal kontakt s nezletilou E.K. Této nezletilé zaslal snímky dívky, za kterou se na této síti vydával, čímž nezletilou E.K. uvedl v omyl, jelikož skutečně uvěřila, že navázala komunikaci s touto dívkou. Během jejich komunikace obžalovaný nezletilou E.K. přesvědčil k zaslání pornografického materiálu, konkrétně se jednalo o fotografii pohlavních genitálií nezletilé a snímek, na kterém má

[136] ŠČERBA, Filip. In: ŠČERBA, Filip a kol. *Trestní zákoník: komentář.* 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 1568-1570.

ve svých ústech úd jejich psa. Posléze mu již E.K. odmítla zaslat další takový materiál. Obžalovaný však po ní zaslání dalšího takového materiálu požadoval, pod pohrůžkou zveřejnění jí již zaslaného materiálu a kontaktování jejího přítele D.K. s tím, že mu odešle zprávu, že je „*děvka*“. Dále pak snímek pohlavních genitálií nezletilé E.K. zaslal její sestře S.K., rovněž nezletilé, s návrhem, že pakliže mu ona poskytne materiál choulostivé až pornografické povahy, odstraní pornografický materiál její sestry E.K., přičemž S.K. na tento návrh nepřistoupila, a žádný materiál obžalovanému neposkytla. Obžalovaný si musel být vědom toho, že jsou obě dívky nezletilé, vzhledem k fotografiím, jež mají umístěné na svých facebookových profilech.

II. Přečinem výroby a jiného nakládání s dětskou pornografií podle ust. **§ 192 odst. 2 a 3 TrZ**, přečinem ohrožování výchovy dítěte podle ust. § 201 odst. 1 písm. a) TrZ, tím, že v době od 27. 2. 2016 minimálně do 23. 3. 2016 na sociální síti Facebook z profilu se jménem M.N. odeslal nezletilé A.P. a K.V. videonahrávku zachycující vsouvání mrkve do ženských pohlavních genitálií a další pornografický materiál, a to i přesto, že si byl vědom, že jsou tyto dívky mladší 18 let.

III. Přečinem zneužití dítěte k výrobě pornografie podle ust. § 193 odst. 1 TrZ, přečinem výroby a jiného nakládání s dětskou pornografií podle ust. **§ 192 odst. 2 a 3 TrZ**, přečinem ohrožování výchovy dítěte podle ust. § 201 odst. 1 písm. a) TrZ, když skrze sociální síť Facebook z profilu X navázal komunikaci s nezletilou P.T., která mu mimo jiné sdělila, že jí je 13 let. Této nezletilé poslal pornografický materiál, taktéž i dětskou pornografii, a zároveň ji lákal k tomu, aby mu ona sama odeslala její pornografický materiál, čemuž dívka dobrovolně a opakovaně vyhověla.

IV. Přečinem výroby a jiného nakládání s dětskou pornografií podle ust. **§ 192 odst. 1 TrZ,** tím, že do 11. 1. 2017 ve svém mobilu L a do 4. 11. 2017 ve svém mobilním telefonu V přechovával dětskou pornografii pro účely sexuálního ukájení.[137]

[137] Rozsudek Krajského soudu v Brně ze dne 19. 11. 2019, sp. zn. 48 T 4/2019.

Za tyto trestné činy a v souběhu spáchaným přečinem nedovolené výroby a jiného nakládání s omamnými a psychotropními látkami a s jedy podle ust. § 283 odst. 1 TrZ, kterým byl uznán vinným trestním příkazem ze dne 4. 6. 2018, a jež se stal pravomocným dne 19. 6. 2018, byl odsouzen k souhrnnému trestu odnětí svobody v délce trvání 36 měsíců s podmíněným odkladem na zkušební dobu v trvání 60 měsíců. Současně byl uložen trest propadnutí věci. Dále bylo obžalovanému uloženo ústavní ochranné léčení sexuologické.[138]

3.2.5 Výzkum

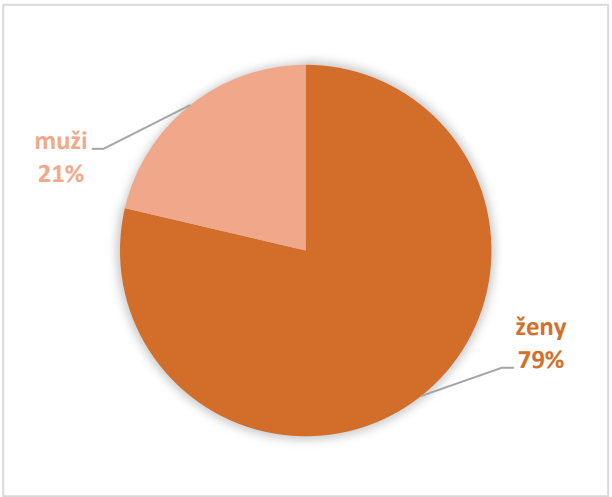
a) Povědomí o sextingu

Z celkových 501 (100 %) respondentů jich **449 (89,6 %)** uvedlo, že zná pojem sexting. Nicméně se domnívám, že i někteří z respondentů, jež uvedli, že tento pojem neznají, jsou s podstatou tohoto fenoménu obeznámeni, byť neznají přesný pojem, kterým je označován.

b) Osoby, jež zaslaly svůj intimní materiál jiné osobě

Celkem **314 (62,7 %)** respondentů zaslalo jiné osobě vlastní intimní materiál (např. sexuálně laděnou zprávu, fotografii, na níž byli částečně anebo úplně obnažení atp.).

III. Osoby, jež zaslaly svůj intimní materiál jiné osobě podle pohlaví

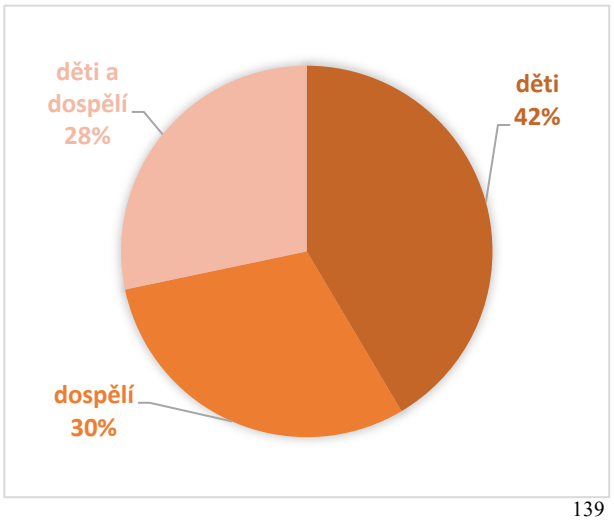


[138] Rozsudek Krajského soudu v Brně ze dne 19. 11. 2019, sp. zn. 48 T 4/2019.

Dle výsledků provedeného výzkumu lze říci, že častěji zasílají intimní materiál ženy nežli muži. Nicméně vezeme-li v úvahu vyšší procentuální zastoupení žen v dotazníkovém šetření, jsou výsledky následující:

- z celkového počtu 367 (100 %) žen v dotazníkovém šetření jich 247 (67,3 %) uvedlo, že jiné osobě zaslalo svůj intimní materiál,
- v případě mužů pak z celkových 134 (100 %) totéž uvedlo 67 (50 %) respondentů. **Závěrem lze říci, že dle provedeného výzkumu častěji zasílají vlastní intimní materiál ženy.**

I. Osoby, jež zaslaly svůj intimní materiál jiné osobě podle věku



[139]

V tomto případě je grafické znázornění koncipováno v souladu s ust. § 126 TrZ, dle kterého se dítětem rozumí osoba mladší 18 let. Graf je složen ze tří kategorií, a tedy děti, dospělí, a současně děti a dospělí, neboť někteří respondenti zaslali jiné osobě vlastní intimní materiál během svého života vícekrát. **Z výsledků provedeného výzkumu vyplývá, že nejčastěji zasílají intimní materiál děti, tedy osoby mladší 18 let.**

Výzkumem rizikového chování českých dětí v prostředí internetu uskutečněného v roce 2014 bylo zjištěno, že celkem 7,81 % respondentů mladších 18 let z celkových 28 232 dětí umístilo na internet sexuálně laděný snímek nebo videonahrávku anebo snímek či videonahrávku, na níž jsou částečně nebo úplně obnaženi. Z těchto 7,23 % bylo celkem 47 % chlapců a 53 % dívek.

[139] Jelikož celkem 3 respondenti neuvedli věk, kdy zaslali svůj intimní materiál, nejsou do uvedeného grafu započteni.

A 12,14 % respondentů takový materiál jiné osobě prostřednictvím mobilního telefonu anebo internetu zaslalo. Přičemž tak z celkových 12,14 % učinilo 60 % chlapců a 40 % dívek.[140]

c) Rizikovost sextingu

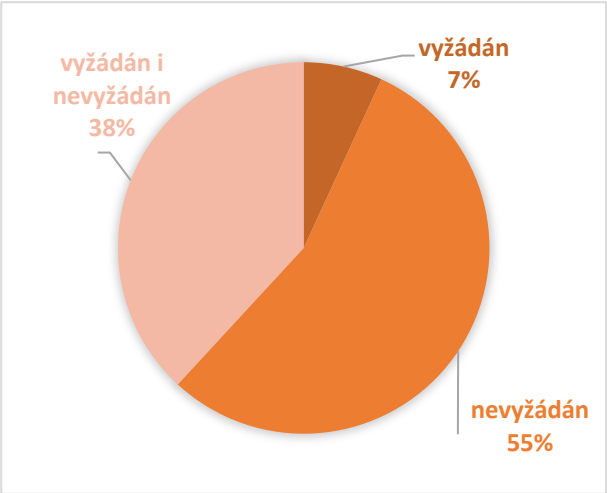
Tato část výzkumu byla zaměřena na rizika spojená se sextingem, a proto cílila pouze na respondenty, jež uvedli, že zaslali jiné osobě intimní materiál, tj. celkem **314 (62,7 %)** respondentů. Celkem **72 (22,9 %)** respondentů uvedlo, že byl jimi zaslaný intimní materiál **dále šířen** mezi jiné osoby, kterým nebyl určen. A **49 (15,6 %)** respondentů sdělilo, že jim bylo osobou, které zaslali vlastní intimní materiál, anebo osobou, jež k němu získala přístup, **vyhrožováno** anebo byli touto osobou **vydíráni.**

Již zmíněným Výzkumem rizikového chování českých dětí v prostředí internetu bylo zjištěno, že 9,86 % dětí zažilo situaci, kdy jiný uživatel internetu, se kterým se přátelili, zveřejnil v internetovém prostředí jejich sexuálně laděný snímek či videonahrávku anebo snímek či videonahrávku, kde jsou částečně nebo zcela obnaženi.[141]

Projektem upozorňujícím na rizika spojená s internetem byla animovaná *Sweetie*, dívka ve věku 10 let, jež byla stvořena v roce 2013 nizozemskou mezinárodní skupinou *Terre des Hommes Netherlands*. Během 10 týdnů byla uměle vytvořená dívka v on-line prostoru oslovena více než 20 tisícími osob mužského pohlaví ze 71 států, jež po dívce požadovalo, aby se obnažovala anebo se pohlavně ukájela. Celkem 1000 z těchto predátorů bylo ztotožněno a získané informace byly předány Interpolu.[142]

[140] KOPECKÝ, Kamil, KOŽÍŠEK, Martin. [online]. Výzkum rizikového chování českých dětí v prostředí internetu 2014, [cit. 19.3.2022]. Dostupné z: https://www.e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/61-vyzkum-rizikoveho-chovani-ceskych-deti-v-prostredi-internetu-2014-prezentace/file
[141] Tamtéž.
[142] SZOTKOWSKI, René. *Sexting u českých dětí*. Olomouc: Univerzita Palackého v Olomouci, 2020. ISBN 978-80-244-5793-2. s. 64.

d) Osoby, jež obdržely materiál intimní povahy



Výzkum byl v této části zaměřen na výskyt případů obdržení nevyžádané pornografie či intimního materiálu. Uvedený graf je koncipován do celkem tří kategorií, a to obdržení materiálu sexuální povahy po jejím předchozím vyžádání, získání tohoto materiálu bez jeho vyžádání, a třetí kategorie je složena z obou možností, neb řada respondentů během svého života obdržela jak materiál vyžádaný, tak nevyžádaný.

3.3 Kybergrooming

Kybergrooming je jedním z kyberzločinů páchaných v on-line prostředí. Predátor, který se na sociální síti vydává zpravidla za jinou osobu, naváže komunikaci se svou obětí, a to za účelem následného sexuálního zneužití ve světě reálném.[143] Přičemž oběti jsou typicky děti, nejčastěji ženy ve věku 13-17 let,[144] avšak mohou jimi být i dospělé osoby.[145] Útočník přitom na sociální síti navazuje kontakt klidně až s tisíci oběťmi současně, čímž na jednu stranu zvyšuje „úspěšnost" dosažení jeho cíle, a na straně druhé tímto nabývá nových zkušeností, které mu v budoucnu usnadňují věrohodnější komunikaci s novou obětí.[146]

Internet, a zejména sociální sítě, užívá značná část populace dennodenně. Prostřednictvím sociálních sítí uživatelé udržují kontakt se svými přáteli, zveřejňují na nich různorodé příspěvky, názory atp. Útočník si tak díky informacím zveřejněným na profilech uživatelů snadněji vytipuje svou oběť, a rovněž tyto údaje zneužívá pro sestavení vhodného falešného profilu a jednodušší komunikaci s ní. Je pro něho snadnější pochopit emoce oběti, její názory, a přizpůsobit tomu styl své komunikace. Vystupuje pak jako někdo, kdo s obětí souzní, čímž si získá její náklonost. Pro kybergrooming je tedy typická psychologická manipulace oběti, kdy predátor v rámci dlouhodobější komunikace s obětí získává její důvěru a navazuje s ní hlubší citový vztah. Své oběti se svěřuje se svými (smyšlenými) starostmi, anebo jí dává dárky, aby si ji získal. Postupně vzniká ze strany oběti emoční závislost na útočníkovi, se kterým má potřebu komunikovat na sociální síti co možná nejčastěji. Přitom se oběť obvykle uzavírá před svým okolím. Predátor čím dál tím více směřuje předmět komunikace k sexuální tématice a láká od oběti pornografický anebo jiný intimní materiál. Poté, co pachatel dosáhne osobního setkání, oběť zpravidla znásilní, pohlavně zneužije, anebo ji nutí k výrobě pornografického materiálu. K pohlavnímu styku či jinak sexuálně motivovanému jednání může útočník oběť donucovat i pod pohrůžkou zveřejnění citlivých materiálů, které od ní získal, anebo tím, že s ní ukončí jejich vztah, na kterém jí

[143] GŘIVNA, Tomáš, Martin RICHTER a Hana ŠIMÁNOVÁ, ed. *Vliv nových technologií na trestní právo*. Praha: Auditorium, 2022. ISBN 978-80-87284-95-7. s. 347-348.
[144] Některé zdroje uvádí, že je obětí nejčastěji dítě ve věku 11-17 let srov. SZOTKOWSKI, René. *Sexting u českých dětí*. Olomouc: Univerzita Palackého v Olomouci, 2020. ISBN 978-80-244-5793-2. s. 81.
[145] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. s. 313.
[146] SZOTKOWSKI, René. *Sexting u českých dětí*. Olomouc: Univerzita Palackého v Olomouci, 2020. ISBN 978-80-244-5793-2. s. 80.

v této fázi velice záleží.[147] Délka komunikace, po kterou je oběť útočníkem manipulována, než svolí k osobnímu setkání, se v jednotlivých případech různí. U některých obětí se může jednat o několik měsíců i let, než si kybergroomer získá jejich důvěru, jindy to může být pouze týden.[148]

Tyto popsané fáze tak lze členit na:

a) **Přípravu k oslovení oběti,** kdy si útočník vyhledá pro něho vhodnou oběť a založí si na sociální síti falešný profil, který je jí přizpůsoben.[149]
b) **Oslovení oběti a navazování hlubšího emočního vztahu**, kdy při kontaktování oběti útočník využívá informací uvedených na jejím profilu tak, aby bylo navázání komunikace úspěšné. Řeší stejné problémy a témata jako oběť, čímž dokazuje, že jí rozumí. Za účelem získání většího množství osobních informací a intimních materiálů oběť obdarovává.[150] Rovněž se jí snaží stranit od přátel a rodiny, např. větami jako „*neříkej o tom mamince, kdybys jí to řekl/a, nenáviděla by tě*.“[151]
c) **Příprava na osobní setkání**, kdy již oběť útočníkovi věří a může ji na schůzku vylákat. Útočník již v této fázi disponuje dostatečným množstvím jejích osobních dat a jiným citlivým materiálem, kterým ji může vydírat.[152]
d) **Osobní setkání s obětí**, kde útočník buď to svou oběť dále manipuluje, anebo na ni rovnou zaútočí.[153]

[147] GŘIVNA, Tomáš, Martin RICHTER a Hana ŠIMÁNOVÁ, ed. *Vliv nových technologií na trestní právo*. Praha: Auditorium, 2022. ISBN 978-80-87284-95-7. s. 347-349.
[148] SZOTKOWSKI, René. *Sexting u českých dětí*. Olomouc: Univerzita Palackého v Olomouci, 2020. ISBN 978-80-244-5793-2. s. 80.
[149] Tamtéž, s. 81.
[150] Tamtéž, 81.
[151] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. ISBN 978-80-7387-545-9. s. 53.
[152] SZOTKOWSKI, René. *Sexting u českých dětí*. Olomouc: Univerzita Palackého v Olomouci, 2020. ISBN 978-80-244-5793-2. s. 81.
[153] Tamtéž, s. 82.

3.3.1 Případ kybergroomingu

K jedním z nejznámějších případů kybergroomingu v České republice patří případ Pavla Hovorky, který v mezidobí od roku 2005 do roku 2007 sexuálně zneužil dvě desítky chlapců mladších 18 let.[154] První oběť vylákal na soutěž s názvem „*Dítě VIP*“, kdy jako výherce mohl chlapec z dětského domova strávit dva týdny v Praze. Dítě, jež jeho lsti uvěřilo, sexuálně zneužil. Dále vyhledával své oběti v on-line prostředí. Předmětem jeho zájmu byli nezletilí chlapci ze sociálně slabších rodin, s nimiž v internetovém prostředí komunikoval. S některými si telefonoval prostřednictvím mobilního telefonu, a od některých získal za úplatu jejich obnažené snímky. Své oběti lákal na osobní schůzku konanou v místě jeho pracoviště, kde je následně sexuálně zneužíval. Některé z obětí přitom k pohlavnímu styku přiměl pod pohrůžkou zveřejnění pornografického materiálu anebo jiné citlivé informace (např. jejich sexuální orientace), které získal prostřednictvím internetové komunikace.[155] Přičemž se měl dopustit trestných činů pohlavního zneužití, vydírání, svádění k pohlavnímu styku a ohrožování výchovy dítěte. Za tyto činy byl odsouzen odvolacím soudem k nepodmíněnému trestu odnětí svobody v délce trvání 6,5 roku.[156]

3.3.2 Právní úprava kybergroomingu

Kybergrooming je postihován ust. § 193b TrZ, který byl do naší právní úpravy přijat s účinností od 1. 8. 2014[157] jako výsledek implementace již výše[158] zmíněné směrnice 2011/93/EU ze dne 13. 12. 2011.[159]

---

[154] Tým projektu E-bezpečí. *Pavel Hovorka (Česká republika, 2008).* [online]. E-bezpečí, [cit. 16.3.2022]. Dostupné z: https://www.e-bezpeci.cz/index.php/72-kazuistiky/1446-pavel-hovorka-ceska-republika-2008

[155] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. ISBN 978-80-7387-545-9. s. 51.

[156] Tým projektu E-bezpečí. *Pavel Hovorka (Česká republika, 2008).* [online]. E-bezpečí, [cit. 16.3.2022]. Dostupné z: https://www.e-bezpeci.cz/index.php/72-kazuistiky/1446-pavel-hovorka-ceska-republika-2008

[157] GŘIVNA, Tomáš, Martin RICHTER a Hana ŠIMÁNOVÁ, ed. *Vliv nových technologií na trestní právo*. Praha: Auditorium, 2022. ISBN 978-80-87284-95-7. s. 356.

[158] viz kapitola 3.2.3.1 Právní úprava dětské pornografie v souvislosti s fenoménem sextingu

[159] JELÍNEK, Jiří. *Trestní zákoník a trestní řád: s poznámkami a judikaturou*. Praha: Leges, 2009, Glosátor. ISBN 978-80-7502-230-1. s. 296.

a) Navazování nedovolených kontaktů s dítětem podle ust. § 193b TrZ

„Kdo navrhne setkání dítěti mladšímu patnácti let v úmyslu spáchat trestný čin podle § 187 odst. 1, § 192, § 193, § 202 odst. 2 nebo jiný sexuálně motivovaný trestný čin, bude potrestán odnětím svobody až na dvě léta.“

TrZ touto skutkovou podstatou chrání osoby mladší 15 let před sexuálním zneužíváním, dále pak ochraňuje i jejich morální rozvoj, edukaci a zdravou sexualitu.[160]

Trestný čin podle ust. § 193b TrZ je předčasně dokonaným trestným činem, kterého se dopustí ten, kdo navrhne schůzku osobě mladší 15 let s úmyslem spáchat sexuálně motivovaný protiprávní čin. Tato skutková podstata je formou přípravy k trestným činům podle ust. § 187 odst. 1, § 192, § 193, § 202 odst. 2 TrZ anebo jiného trestného činu se sexuálním motivem. Zákonodárce zavedením předčasně dokonaných trestných činů do naší právní úpravy kriminalizuje přípravu k trestným činům, které nejsou zvlášť závažnými zločiny, a u nichž tedy není příprava trestná.[161] V případě, kdy by měl pachatel v úmyslu spáchat trestný čin podle ust. § 187 odst. 2 TrZ, který je zvlášť závažným zločinem, bylo by jednání pachatele postihováno jako příprava k tomuto zvlášť závažnému zločinu, a nikoliv jako trestný čin podle ust. § 193b TrZ.[162]

V případě, kdy by kybergroomer na sociální síti navázal kontakt s dítětem, kterému již bylo 15 let, a navrhl mu osobní schůzku s úmyslem spáchat sexuálně motivovaný trestný čin, byla by pro něho situace z trestněprávního hlediska příznivější. V některých případech tak kybergroomer raději vyčká do té doby, než dítě dovrší 15 let, a až poté mu navrhne osobní schůzku. Z právního hlediska tak lze děti od 15 do 18 let označit za více ohroženou skupinu, pokud predátor cílí právě na tuto věkovou kategorii.[163] V případě kybergroomingu navrhne pachatel oběti setkání skrze sociální síť anebo jinou komunikační technologii, nicméně touto skutkovou podstatou jsou stíhány i návrhy činěné jiným, klasičtějším způsobem, například dopisem, ústně atp.[164]

---

[160] ŠČERBA, Filip. In: ŠČERBA, Filip a kol. *Trestní zákoník: komentář*. 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 1581.
[161] JELÍNEK, Jiří. *Trestní zákoník a trestní řád: s poznámkami a judikaturou*. Praha: Leges, 2009, Glosátor. ISBN 978-80-7502-230-1. s. 296.
[162] ŠČERBA, Filip. In: ŠČERBA, Filip a kol. *Trestní zákoník: komentář*. 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 1581.
[163] SZOTKOWSKI, René. *Sexting u českých dětí*. Olomouc: Univerzita Palackého v Olomouci, 2020. ISBN 978-80-244-5793-2. s. 126-127.
[164] ŠČERBA, Filip. In: ŠČERBA, Filip a kol. *Trestní zákoník: komentář*. 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 1581-1582.

Z hlediska subjektivní stránky je vyžadováno úmyslné zavinění, a to pouze ve formě úmyslu přímého. Pro naplnění subjektivní stránky je nezbytné, aby si byl pachatel vědom věku dítěte. Tento znak by nebyl naplněn, pokud by se pachatel domníval, že již osoba dosáhla 15 roku svého života. Musí tedy vědět, že osoba, které činí návrh osobní schůzky, je osoba mladší 15 let, a zároveň jí tento návrh podat v úmyslu spáchat sexuálně motivovaný trestný čin. Pachatelem může být kdokoliv, jak osoba fyzická, tak právnická.[165]

Nezbytné je podotknout, že v prvé řadě je tato skutková podstata aplikovatelná až na konečnou fázi kybergroomingu, tedy fázi, kdy pachatel získal důvěru oběti a učinil jí návrh osobního setkání s úmyslem spáchat sexuálně motivovaný trestný čin. Nicméně tato fáze nemusí vždy nastat. A v druhé řadě by právní kvalifikace podle ust. § 193b TrZ nebyla možná za situace, kdy by osobní schůzku s útočníkem navrhla sama oběť.[166]

Před konečnou fází kybergroomingu je možná trestní represe podle ust. § 192 a ust. § 193 TrZ, pakliže kybergroomer od dítěte v rámci jejich on-line komunikace vyláká pornografický materiál. Dále pak přichází v úvahu i právní kvalifikace podle ust. § 186 TrZ, pokud donutil svou oběť k pohlavnímu sebeuspokojování či obnažování pod pohrůžkou jiné těžké újmy,[167] např. že o nepatřičném chování dítěte obeznámí jeho rodiče[168], anebo pokud zneužije její bezbrannosti, kterou může být např. stav psychické závislosti oběti na pachateli.[169]

3.3.3 Prevence kybergroomingu

Pro kybergrooming je stěžejní prevence, neboť osoby se sexuální parafilií vyhledávají své oběti (zejména děti) na internetu za účelem jejich následného sexuálního zneužití, a to i přesto, že lze takový čin postihnout trestním právem. Dnešní generace dětí se vyznačuje vysokou znalostí moderních technologií, avšak často si neuvědomuje rizika, která se v kyberprostoru vyskytují. Zejména

[165] ŠČERBA, Filip. In: ŠČERBA, Filip a kol. *Trestní zákoník: komentář*. 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 1582.
[166] GŘIVNA, Tomáš, Martin RICHTER a Hana ŠIMÁNOVÁ, ed. *Vliv nových technologií na trestní právo*. Praha: Auditorium, 2022. ISBN 978-80-87284-95-7. s. 356.
[167] Tamtéž, s. 356-357.
[168] ŠČERBA, Filip. In: ŠČERBA, Filip a kol. *Trestní zákoník: komentář*. 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 1518.
[169] GŘIVNA, Tomáš, Martin RICHTER a Hana ŠIMÁNOVÁ, ed. *Vliv nových technologií na trestní právo*. Praha: Auditorium, 2022. ISBN 978-80-87284-95-7. s. 357.

by z hlediska prevence byla vhodná výuka dětí ve školských zařízeních, zaměřená na rizika spojená s internetem. Nezbytná je však i informovanost rodičů, kteří by rovněž měli znát hrozby, které jim, ale zejména jejich dětem, na internetu hrozí. Rodič dítěte by jej měl varovat, jak na internetu vystupovat a seznámit ho s možnými rizikovými jevy tohoto prostředí. Zároveň by však rodiče měli jít svým dětem příkladem a být obezřetní, jaké údaje na svých profilech zveřejňují.[170]

Jedním z projektů, jež vznikl za účelem prevence kybernetické kriminality, je dokumentární film „V Síti“. Tento dokument vznikl za účelem otevření citlivého tématu sexuálního zneužívání dětí v prostředí internetu. Tři hlavní protagonistky dokumentu vystupují na sociálních sítích a jiných komunikačních technologiích jako nezletilé, 12leté dívky, a komunikují zde s potencionálními predátory. Dívky oslovilo během 10 dnů, po které se tento dokumentární film natáčel, celkem 2458 uživatelů internetu.[171] Tento dokumentární film napomohl odhalit trestnou činnost páchanou v kyberprostoru, přičemž jednomu z případů se budu hlouběji věnovat v následující kapitole *3.3.4 Judikatura.*

3.3.4 Judikatura

Obžalovaný M.K. byl rozsudkem Okresního soudu v Ústí nad Labem uznán vinným spácháním následujících trestných činů:

I. Pokusem přečinu ohrožování výchovy dítěte podle ust. § 21 odst. 1 TrZ, ust. § 201 odst. 1 písm. a), odst. 3 písm. a) TrZ, pokusem přečinu zneužití dítěte k výrobě pornografie podle ust. **§ 21 odst. 1, ust. § 193 odst. 1 TrZ**, pokusem přečinu navazování nedovolených kontaktů s dítětem podle ust. **§ 21 odst. 1, ust. § 193b TrZ**, pokusem přečinu šíření pornografie podle ust. § 21 odst. 1, § 191 odst. 2 písm. a) TrZ, když ode dne 12. 11. 2018 navazoval skrze sociální síť Lidé.cz, a poté prostřednictvím komunikační technologie Skype, kde vystupoval pod smyšlenými jmény, kontakt s hlavními představitelkami dokumentárního filmu „V síti“. Představitelky, které jsou ve skutečnosti dospělé, v rámci zmíněného dokumentu předstíraly, že jsou 12leté

[170] GŘIVNA, Tomáš, Martin RICHTER a Hana ŠIMÁNOVÁ, ed. *Vliv nových technologií na trestní právo*. Praha: Auditorium, 2022. ISBN 978-80-87284-95-7. s. 356-358.
[171] *O filmu.* [online]. V síti, [cit. 16.3.2022]. Dostupné z: https://vsitifilm.cz/o-filmu.html

dívky. Pachatel se dopustil výše uvedených trestných činů v domnění, že se jedná o nezletilé osoby, když konkrétně:

- během videohovoru s představitelkou vystupující pod profilem „Míša Soukupová“, která ho vícekrát uvědomila o tom, že je jí pouze 12 let, jí skládal komplimenty, požadoval po ní, aby se před kamerou obnažovala, což neučinila, tak žádal „alespoň“ snímek intimní povahy. Dále hovor směřoval k sexuální tématice, kdy se jí dotazoval, zda již políbila jinou osobu, má pubické ochlupení anebo či už masturbovala, načež jí zaslal snímek svého přirození. Obžalovaný jí poté, co mu poskytla přes opakující se prosby snímek obnažených prsou, sdělil, jaké sexuální touhy v něm její prsa vyvolávají. Posléze se jí dotazoval, zda zhlíží pornografii, když odvětila, že nikoliv, jí zaslal odkaz na pornografický materiál, jehož obsahem bylo video zobrazující ženu při sebeuspokojování. Dále pak dívce projevoval svou náklonnost tím, že jí sdělil, že ji miluje, a že by se s ní rád setkal za účelem sexuálních aktivit, jež blíže specifikoval. Na jimi domluvené setkání však nedorazil.
- Představitelku vystupující pod jménem „Niki Komárková“ během videohovoru opakovaně žádal k zaslání fotografie intimní až pornografické povahy, a rovněž jí slíbil, že jí sám poskytne svou intimní fotografii.
- Představitelku vystupující pod jménem „Kristýna Jůnová“ během videohovoru žádal, aby se obnažovala, což neučinila. Dále po ní požadoval, aby mu z koupelny zaslala fotografii bez horního dílu pyžama, a protože měla obavy, aby to nezjistila její „máma“, ji utvrzoval v tom, že fotografii okamžitě odstraní.
- Pod jinou přezdívkou znovu oslovil představitelku vystupující pod jménem „Míša Soukupová“, a přesto, že ho upozorňovala, že jí je 12 let, jí odeslal snímek svého přirození, žádal jí o zaslání pornografického materiálu, a stáčel konverzaci k sexuální tématice. Dívky se tázal, jak vypadá její přirození, zda má pubické ochlupení, zda se sebeuspokojuje, a dával jí přitom rady, jak tak nejlépe učinit. Dále jí sdělil, že by se s ní rád osobně sešel a měl s ní pohlavní styk, přičemž blíže specifikoval, jak by tento styk probíhal. Dívku však

upozornil, že o plánovaném osobním setkání nesmí nikomu říci. Poté však s dívkou ukončil veškerou komunikaci a již nereagoval.

II. Přečinem výroby a jiného nakládání s dětskou pornografií podle ust. § 192 odst. 1 TrZ, tím, že do 25. 2. 2020 v paměti svého počítače přechovával stovky snímků a videonahrávek obsahující dětský pornografický materiál.[172]

Za což mu byl soudem prvního stupně uložen úhrnný trest nepodmíněného odnětí svobody v délce trvání 2 let. Vedle nepodmíněného trestu odnětí svobody byl uložen rovněž trest propadnutí věci. Z odůvodnění rozsudku vyplývá, že ochranné léčení sexuologické nebylo možné v tomto případě uložit, neboť nebyla znaleckým posudkem u obžalovaného shledána žádná duševní porucha.[173]

Z odůvodnění je patrné, že trestné činy pod bodem I. nebyly kvalifikovány jako dokonané trestné činy, neboť v době spáchání těchto trestných činů byly hlavní představitelky dokumentárního filmu „V síti“ dospělé, a dokonání tedy nebylo objektivně možné vzhledem k nezpůsobilému předmětu útoku. Nicméně pachatel se těchto trestných činů dopustil formou pokusu podle ust. § 21 odst. 1 TrZ, když se domníval, že je dívkám skutečně 12 let, a tak věděl, anebo byl alespoň srozuměn s tím, že se dopouští činu postižitelného trestním právem. Dle subjektivní stránky trestného činu pachatel musel být minimálně srozuměn s tím, že svým jednáním poruší zájem chráněný TrZ. [174]

[172] Rozsudek Okresního soudu v Ústí nad Labem ze dne 1.4. 2021, sp. zn. 3 T 141/2020.
[173] Tamtéž.
[174] Tamtéž.

3.3.5 Výzkum

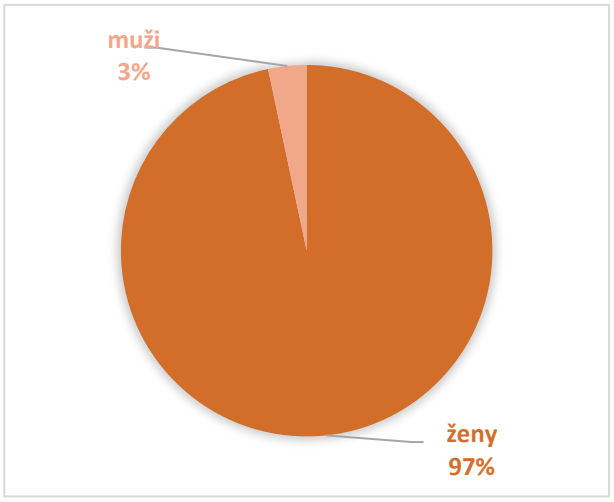
a) Povědomí o kybergroomingu

Z celkových 501 (100 %) pouze **117 (23,4 %)** respondentů uvedlo, že zná pojem kybergrooming. Ve srovnání s ostatními kybernetickými útoky je povědomí o fenoménu kybergroomingu nejnižší.

b) Oběti kybergroomingu

Z celkových 501 (100 %) respondentů jich **60 (12 %)** uvedlo, že se během svého života stalo obětí kybergroomingu. Přičemž je nutné podotknout, že ne vždy musí ke konečné fázi dojít.

I. Oběti kybergroomingu podle pohlaví

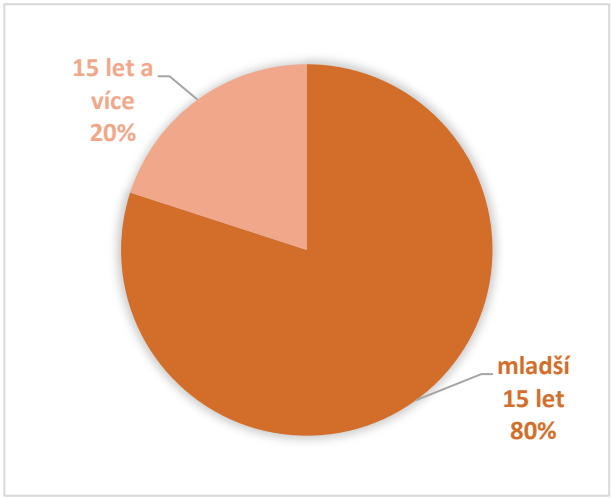


Dle výsledků provedeného výzkumu lze říci, že jsou obětí kybergroomingu častěji ženy. Nicméně vezeme-li v úvahu vyšší procentuální zastoupení žen v dotazníkovém šetření, jsou výsledky následující:

- z celkového počtu 367 (100 %) žen v dotazníkovém šetření jich 58 (15,8 %) uvedlo, že se během svého života stalo obětí kybergroomingu,
- v případě mužů pak z celkových 134 (100 %) totéž uvedli 2 (1,5 %) respondenti.

Závěrem lze říci, že provedeným výzkumem bylo zjištěno, že jsou oběti kybergroomingu častěji ženy.

II. Oběti kybergroomingu podle věku



Pro dělení obětí dle věku byla zohledněna věková hranice uvedená v ust. §193b TrZ *„Kdo navrhne setkání dítěti mladšímu patnácti let…“* Respondenti byli členěni do jednotlivých kategorií v závislosti na tom, kdy došlo k prvnímu kontaktu s kybergroomerem.[175] **Dle výsledků provedeného výzkumu kybergroomer nejčastěji oslovuje děti mladší 15 let a věkové rozpětí obětí kybergroomingu je 10 až 19 let (průměrný věk obětí byl přitom 13-14 let).** Celkem 58 (96,7 %) respondentů, v dotazníkovém šetření sdělilo, že bylo mladší 18 let. V případě, kdy by kybergroomer lákal po oběti materiály pornografické povahy, přicházela by v úvahu právní kvalifikace podle ust. § 192 a ust. § 193 TrZ.

Realizované dotazníkové šetření vykazuje obdobné závěry jako oficiální statistiky, dle kterých jsou nejčastěji oběti dívky ve věku 13 až 17 let.[176]

Výzkumem rizikového chování českých dětí v prostřední internetu realizovaným v roce 2014 bylo zjištěno, že 43,56 % dětí z celkových 28 232 respondentů ve věku 11-17 let, bylo pozváno přítelem či známým na osobní schůzku skrze internet. Na osobní setkání přišlo celkem 54,91 % dětí.[177]

[175] Část respondentů uváděla v dotazníkovém šetření delší časové období např. 14 až 16 let. Tito respondenti byli zařazení do kategorie „mladší 15 let“.
[176] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. s. 318 s. 313.
[177] Kopecký, Kamil; Kožíšek, Martin. [online]. *Výzkum rizikového chování českých dětí v prostředí internetu 2014,* [cit. 19.3.2022]. Dostupné z: https://www.e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/61-vyzkum-rizikoveho-chovani-ceskych-deti-v-prostredi-internetu-2014-prezentace/file

3.4 Kyberstalking

Pro vymezení kyberstalkingu je nezbytné vymezit pojem „stalking“, v českém překladu pronásledování. V minulosti se tento pojem užíval v kontextu s lovením zvěře, což vcelku příhodně vystihuje podstatu stalkingu, jak jej známe dnes. Namísto zvířete je však útočníkem pronásledován člověk, a následky mohou být pro oběť stalkera stejně tragické, jako by byly pro zvíře v případě zdařilého lovu.[178]

Pronásledováním se rozumí opětovná, trvající snaha stalkera kontaktovat svou oběť, a to i přes její nesouhlas. Jednání útočníka má mnohdy agresivní povahu, omezuje oběť na její osobní svobodě a soukromí, přičemž jí působí diskomfort anebo v ní dokonce vyvolává pocit strachu.[179] Opětovnou snahou lze rozumět více než 10 opakovaných pokusů o kontaktování oběti, a to v minimální délce trvání 4 týdnů. Pakliže stalking trvá delší dobu, je vysoké riziko stupňování útoků a násilí ze strany stalkera, které může skončit i usmrcením oběti.[180] Stalking přitom obsahuje širokou škálu možného jednání útočníka, a může k němu užívat jak prostředky zdánlivě zákonné, např. zasílá-li své oběti dary, textové zprávy, anebo užívá prostředků protiprávních, svou oběť vydírá, vyhrožují jí atp.[181]

Pokud je stalking činěn prostřednictvím ICT, jedná se o kyberstalking, který je zvláštní formou stalkingu. Pro kyberstalking je charakteristické zasílání textových zpráv, šíření nepravdivých údajů o oběti v prostředí internetu, zasílání spamů, odcizení dat uložených v počítačové technice oběti atp. Často útočník stalkuje oběť jak v reálném světě, tak kyberprostoru zároveň, což umocňuje negativní dopad na její psychiku.[182] Kyberstalking lze členit na přímý a nepřímý. V případě přímého kyberstalkingu útočník zasílá textové zprávy, e-maily, s nenávistným, nemorálním či výhrůžným obsahem přímo své oběti. O nepřímý kyberstalking se jedná, pokud útočník v prostředí internetu o oběti šíří nepravdivé informace nebo ve vztahu k ní přidává nenávistné či výhrůžné příspěvky.[183]

---

[178] ŠÁMAL, Pavel, ŠÁMALOVÁ, Milana. In: ŠÁMAL, Pavel a kol. *Trestní zákoník: komentář*. Praha: C.H. Beck, 2010. Velké komentáře. ISBN 978-80-7400-178-9. s. 3005.
[179] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. ISBN 978-80-7387-545-9. s. 69.
[180] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7. s. 396-397.
[181] ŠÁMAL, Pavel, ŠÁMALOVÁ, Milana. In: ŠÁMAL, Pavel a kol. *Trestní zákoník: komentář*. Praha: C.H. Beck, 2010. Velké komentáře. ISBN 978-80-7400-178-9. s. 3007.
[182] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7. s. 397.
[183] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. ISBN 978-80-7387-545-9. s. 70.

Stalking, ať již je činěn ve světě reálném anebo v kyberprostoru, lze právně kvalifikovat jako nebezpečné pronásledování podle ust. § 354 TrZ, v případě naplnění zákonných znaků tohoto trestného činu.[184] Tato skutková podstata byla do TrZ zavedena 1. 1. 2010 a umožnila tak komplexní reakci na výskyt tohoto nežádoucího jevu.[185]

3.4.1 Projevy stalkingu

a) Opětovné a déletrvající pokusy o kontakt s obětí zasíláním zpráv prostřednictvím mobilního telefonu, sociálních sítí atp., voláním, psaním dopisů. Přičemž tyto zprávy mají různou podobu, např. mohou být lichotivé, humorné, ale i vulgární či výhrůžné. V některých případech se nejprve může jednat o lichotivé a zdvořilé zprávy, kterými se uživatel snaží navázat komunikaci s obětí, posléze však přechází ke zprávám útočným.
b) Demonstrace moci a fyzické zdatnosti stalkera, zejména tím, že v oběti vyvolává strach, např. pohrůžkou usmrcení, těžkého ublížení na zdraví nebo jejím sledováním např. cestou domů. V případě kyberstalkingu oběti zasílá zprávy, obsahující informace o tom, co oběť aktuálně dělá či jaký oděv má zrovna na sobě.
c) Dalším projevem je záměrné poškození věci oběti, např. zničením jejího jízdního kola či poničením automobilu. Pro kyberstalking je typické neoprávněné získávání údajů o oběti prostřednictvím ICT nebo zasíláním malware za účelem poškození počítačové techniky oběti.
d) V některých případech může stalker předstírat, že je sám obětí stalkingu.
e) Šířením pomluv o oběti s cílem ohrozit její vážnost, vytvářením falešných profilů, na kterém jsou lživé údaje sdíleny atp.[186]

[184] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. s. 318.
[185] ŠÁMAL, Pavel, ŠÁMALOVÁ, Milana. In: ŠÁMAL, Pavel a kol. *Trestní zákoník: komentář*. Praha: C.H. Beck, 2010. Velké komentáře. ISBN 978-80-7400-178-9. s. 3004.
[186] Tým projektu E-bezpečí. *Co je to stalking a cyberstalking,* [online]. E-bezpečí, [cit. 17.3.2022]. Dostupné z: https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/kyberstalking/66-23

3.4.2 Případy kyberstalkingu

Garry Dellapenta se své oběti, kterou poprvé potkal v kostele, nejprve dvořil, avšak poté, co žena jeho opakované pokusy o bližší seznámení odmítala, zveřejnil v prostředí internetu její osobní údaje, své sexuální touhy ji znásilnit, a rovněž uvedl jakým způsobem je možné obejít bezpečnostní zabezpečení jejího domu. V reakci na zveřejnění jejích osobních údajů byla kontaktována desítkami mužů prostřednictvím telefonního hovoru. Šest z nich přitom vyhledalo tuto ženu osobně. V důsledku těchto událostí žena změnila své bydliště, byla propuštěna ze svého zaměstnání a žila ve strachu opouštět svůj nový domov.[187]

Dalším případem kyberstalkingu je případ paní Hany, která podala žádost o rozvod se svým manželem z důvodu jeho nepřiměřeně vysoké žárlivosti. Zjistila, že její manžel si je vědom toho, kde se konkrétně nacházela, aniž by ho o tom uvědomila, rovněž pak i s kým udržovala kontakt prostřednictvím svého mobilního telefonu. Poté, co se obrátila na Policii ČR, bylo zjištěno, že jí manžel do jejího mobilního telefonu nainstaloval aplikaci, jež mu umožňovala sledovat její aktivitu na tomto telefonu, a zároveň i její lokaci.[188]

3.4.3 Právní úprava kyberstalkingu

a) Nebezpečné pronásledování podle ust. § 354 TrZ

„(1) Kdo jiného dlouhodobě pronásleduje tím, že

a) vyhrožuje ublížením na zdraví nebo jinou újmou jemu nebo jeho osobám blízkým,

b) vyhledává jeho osobní blízkost nebo jej sleduje,

c) vytrvale jej prostřednictvím prostředků elektronických komunikací, písemně nebo jinak kontaktuje,

d) omezuje jej v jeho obvyklém způsobu života, nebo

e) zneužije jeho osobních údajů za účelem získání osobního nebo jiného kontaktu, a toto jednání je způsobilé vzbudit v něm důvodnou obavu o jeho

[187] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. ISBN 978-80-7387-545-9. s. 70-71.
[188] *Kybertsalking,* [online]. Internetem bezpečně, [cit. 17.3.2022]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kyberstalking/

život nebo zdraví nebo o život a zdraví osob jemu blízkých, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti.

(2) Odnětím svobody na šest měsíců až tři roky bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1

a) vůči dítěti nebo těhotné ženě,

b) se zbraní, nebo

c) nejméně se dvěma osobami.“

Objektem je zájem na ochraně nerušeného interpersonálního soužití před jednáním, které je dlouhodobé, svou povahou obtěžující a nevyžádané, a současně způsobilé vyvolat pocit strachu. Zároveň lze objektem rozumět též svobodu člověka, ochranu jeho soukromí před jeho neoprávněným narušením, tedy možnost každého jedince se svobodně rozhodovat, jaké osobě umožní přístup do svého soukromí.[189]

Objektivní stránka je pachatelem naplněna, pokud dlouhodobě pronásleduje poškozeného, přičemž tak činí taxativně vymezenými formami jednání pod písm. a) až e) tohoto ustanovení, které je způsobilé v něm vyvolat důvodnou obavu o vlastní život či zdraví anebo život a zdraví osob, které jsou jí blízké.[190] Trestný čin podle této skutkové podstaty spadá do kategorie ohrožovacích trestných činů, přičemž nebezpečí může oběti hrozit v krátkodobém nebo dlouhodobém časovém horizontu. Žádné jiné jednání, než které je uvedené v odst. 1 pod písm. a) až e), nemůže být za nebezpečné pronásledování podle ust. § 354 TrZ považováno. A to z důvodu, že by se jednalo o analogii v neprospěch pachatele, která je v trestním právu hmotném nepřípustná (zásada *nullum crimen sine lege stricta*). Takovým jednáním lze spatřovat např. nechtěné zasílání dárků oběti. Přesto, že se nejedná o formu jednání obsaženou v odst. 1 pod písm. a) až e) tohoto ustanovení, jedná se o projev charakteristický pro stalking, a může být důležitým operativním vodítkem pro prověření, zda útočník svým počínáním nenaplňuje i zákonné znaky tohoto trestného činu. Rovněž nelze pod tuto skutkovou podstatu podřadit případy,

[189] PROVAZNÍK, Jan. In: ŠČERBA, Filip a kol. *Trestní zákoník*: *komentář.* 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 2917.
[190] ŠÁMAL, Pavel, ŠÁMALOVÁ, Milana. In: ŠÁMAL, Pavel a kol. *Trestní zákoník: komentář.* Praha: C.H. Beck, 2010. Velké komentáře. ISBN 978-80-7400-178-9. s. 3006.

Kdy pronásledování není způsobilé vzbudit v poškozeném důvodnou obavu,[191] přestože jej pachatel pronásledoval jednáním uvedeným pod písm. a) až e).[192]

Zároveň musí jednání pachatele naplňovat kritérium dlouhodobosti, aby mohlo být ust. § 354 TrZ v daném v případě aplikováno. O nebezpečné pronásledování by se nejednalo v případě, pokud by se útočník dopustil pouze ojedinělého útoku. Požadavek dlouhodobosti je nutné hodnotit se zřetelem ke konkrétnímu případu, který je nezbytné posuzovat komplexně, a v úvahu je nutné vzít celou řadu faktorů, jako např. po jakou dobu byla oběť pronásledována, dále pak i dobu trvání dílčích útoků, jejich celkové množství, frekvenci, závažnost, heterogenitu, anebo i odezvu oběti na dané útoky, např. zda na zprávy útočníka odpovídala, zavdávala mu příčinu k dalšímu zasílání zpráv atp.[193] Ve většině případů se pak bude jednat o systematicky a ustavičně činěná jednání odporující běžným pravidlům chování, která mohou postupně nabývat na své intenzitě. Čím častěji jsou dílčí útoky prováděny, a čím větší je jejich heterogenita, tím nižší by měl být požadavek na délku trvání pro kvalifikaci jednání útočníka za nebezpečné pronásledování podle ust. § 354 TrZ. Pro zhodnocení jednání útočníka jako „nebezpečné pronásledování“ pomůže skutečnost, že by se dle klinického hlediska mělo jednat o minimálně 10 útoků v době trvání alespoň 4 týdnů.[194]

Formou nebezpečného pronásledování se rozumí podle písm.:

a) „Výhrůžka ublížením na zdraví nebo jinou újmou“

- Ve srovnání s trestným činem nebezpečného vyhrožování podle ust. § 353 TrZ lze v případě vyhrožování podle tohoto ustanovení uvést pouze některé zvláštnosti. Na rozdíl od ust. § 353 TrZ je v tomto případě vyžadována nižší míra intenzity výhrůžky, tedy vyhrožování ublížením na zdraví nebo jinou újmou. Intenzitu v tomto smyslu dorovnává dlouhodobost činěných výhrůžek.[195] V případě kyberstalkingu by se mohlo jednat např. o vyhrožování prostřednictvím sociálních sítí (za podmínky splnění požadavku dlouhodobosti).

[191] K pojmu důvodná obava viz kapitola 3.1.4 Právní úprava kyberšikany, písm. c) ust. § 353 TrZ.
[192] PROVAZNÍK, Jan. In: ŠČERBA, Filip a kol. *Trestní zákoník: komentář.* 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 2917-2919.
[193] Tamtéž, s. 2918.
[194] ŠÁMAL, Pavel, ŠÁMALOVÁ, Milana. In: ŠÁMAL, Pavel a kol. *Trestní zákoník: komentář*. Praha: C.H. Beck, 2010. Velké komentáře. ISBN 978-80-7400-178-9. s. 3008.
[195] PROVAZNÍK, Jan. In: ŠČERBA, Filip a kol. *Trestní zákoník: komentář.* 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 2919.

b) „Vyhledávání osobní blízkosti a sledování poškozeného“

- Sledováním se rozumí nabývání přímých poznatků o aktuální lokaci a činnosti poškozeného. V případě kyberstalkingu lze uvést příklad, kdy útočník nainstaluje do počítače poškozeného malware, díky kterému aktivuje jeho webkameru a skrze ni ho sleduje. Dále by pak za sledování mohlo být považováno i neoprávněné sledování polohy nebo elektronické komunikace poškozeného prostřednictvím informačních technologií, přestože se nejedná o přímé pozorování poškozeného vizuálním vnímáním útočníka.[196]

c) „Vytrvalé kontaktování“

- Elektronickou komunikací jsou i sociální sítě, na kterých si stalker v některých případech vytváří i více falešných profilů, ze kterých oběti zasílá nevyžádané zprávy. Typicky tak činí proto, že předstírá, že je jinou osobou, a snaží se tak oběť, která s ním komunikovat odmítá, obelstít. Zároveň se může jednat i o případy, kdy útočník získá k profilu poškozeného na sociální síti neoprávněný přístup, změní mu jeho přístupové heslo nebo zasílá skrze jeho profil zprávy jeho kontaktům na této síti. Zároveň musí být naplněn požadavek vytrvalosti, který je odlišný od požadavku dlouhodobosti. Vytrvalé kontaktování je takové jednání útočníka, kdy opakovaně zasílá zprávy poškozenému, který na ně nijak nereaguje anebo je považuje za obtěžující a nevyžádané. Vytrvalost přitom vyjadřuje neúnavné pokusy o kontaktování, např. zasíláním desítek nevyžádaných zpráv z profilu útočníka během jednoho týdne, anebo systematickou snahu o kontaktování oběti z řady útočníkem vytvořených falešných profilů.[197]

d) „Omezování v obvyklém způsobu života“

- Takovým omezením se rozumí určitý pokles kvality života poškozeného zapříčiněným pronásledováním útočníka. Přičemž snížení kvality se může týkat rodinné, pracovní, zájmové a jiné roviny života poškozeného. Příkladem může být změna bydliště v důsledku obav z pronásledovatele, nucená změna v oblasti pracovního života, ale i záměrné ničení věcí poškozeného atp. Rozhodujícím faktorem v určení, zda došlo k omezení běžného způsobu života

[196] PROVAZNÍK, Jan. In: ŠČERBA, Filip a kol. *Trestní zákoník: komentář.* 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 354.
[197] Tamtéž, s.2922.

je subjektivní hledisko poškozeného, a to spolu se subjektivní stránkou pronásledovatele, který musí být alespoň srozuměn s tím, že je v důsledku jeho jednání poškozený takto omezen.[198]

e) *„Zneužití osobních údajů za účelem získání osobního nebo jiného kontaktu s poškozeným“*

- Osobními údaji se podle čl. 4 odst. 1 nařízení 2016/679, známé jako GDPR, rozumí: „*veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.*“
- Vzhledem ke gramatickému výkladu slova „zneužije“ podle písm. e) tohoto ustanovení, kdy zákonodárce užil dokonaný vid, postačuje k naplnění této skutkové podstaty pouze jeden útok pachatele. Avšak samotné ust. § 354 TrZ klade důraz na splnění požadavku dlouhodobosti. V praxi je písm. e) aplikováno pouze v doplňkovém smyslu ke skutkovým podstatám uvedeným pod písm. a) až d) tohoto ustanovení. Tato doplňková funkce zvyšuje závažnost útočníkova jednání, rovněž i obavu poškozeného, a tím snižuje požadavek na dlouhodobost pachatelova protiprávního jednání. Hypoteticky si lze však představit, že by útočník svým jednáním naplnil pouze písm. e) tohoto ustanovení, a to za předpokladu, že by svým jednáním zneužil různé osobní údaje za účelem dosažení kontaktu s poškozeným. Útočník by např. „hacknul“ databázi, ze které by získal adresu poškozeného, z jiné databáze by pak získal telefonní číslo a z další databáze emailovou adresu, tyto údaje by následně použil k získání kontaktu s poškozeným. Důležitá je zde odlišnost, resp. mnohost databází, neboť pokud by opakovaně zneužíval pouze jednoho osobního údaje k opakovanému kontaktování poškozeného, byl by tento znak zaměnitelný se znakem uvedeným pod písm. c) tohoto ustanovení.[199]

[198] PROVAZNÍK, Jan. In: ŠČERBA, Filip a kol. *Trestní zákoník: komentář.* 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 2922-2923.
[199] Tamtéž, s. 2923-2924.

Z hlediska subjektivní stránky je vyžadováno úmyslné zavinění, a to ať formou úmyslu přímého, který v praxi převažuje, tak i úmyslu nepřímého, např. touží-li pachatel dosáhnout přízně poškozeného a navázat s ním partnerský vztah. Svým jednáním přitom směřuje k jinému cíli, avšak je srozuměn s tím, že v oběti svým počínáním může vzbudit důvodnou obavu o zdraví či život.[200]

Pachatelem může být pouze osoba fyzická. Není přitom podstatné, zda pachatel s poškozeným v minulosti setrvával ve vztahu či nikoliv. Obětí jeho počínání muže být i osoba jemu blíže neznámá, např. pokud je pachatel osoba trpící duševním onemocněním. Nicméně nejčastěji k nebezpečnému pronásledování dochází v reakci na rozpad manželství, partnerského či jiného vztahu, anebo v případě, kdy se pachateli s poškozeným tento vztah nepodařilo navázat, resp. byl poškozeným odmítnut a tento jeho závěr neakceptoval.[201]

V komparaci s rakouskou trestněprávní úpravou lze říci, že český TrZ klade přísnější požadavky pro naplnění skutkové podstaty tohoto trestného činu. Rakouský trestní zákoník (STGB15) namísto „důvodné obavy o život a zdraví" užívá „neúnosné narušení života oběti", které poměrně lépe vymezuje hranici toho, co je společensky škodlivé a vyžaduje trestněprávní reakce. Ve smyslu rakouského trestního zákoníku budou trestně postižitelné i méně závažné formy nebezpečného pronásledování, pakliže neúnosně narušují život oběti.[202]

3.4.4 Judikatura

Nejvyšší soud rozhodoval dne 30. 4. 2020 o podaném dovolání obviněného J. N., který byl rozsudkem obvodního soudu pro Prahu 6 ze dne 19. 9. 2019 uznán vinným přečinem nebezpečného pronásledování podle ust. **§ 354 odst. 1 písm. b), c), d) TrZ** a odsouzen k trestu odnětí svobody v trvání 4 měsíců s podmíněným odkladem na zkušební dobu v trvání 16 měsíců, a zároveň mu byla uložena povinnost zákazu styku s poškozenou po dobu trvání stanovené zkušební doby.

Obviněný po dobu minimálně od 31. 12. do 12. 2. 2019 kontaktoval svou bývalou přítelkyni (dále jen *„poškozenou"*) skrze aplikaci Messenger, přestože mu

[200] PROVAZNÍK, Jan. In: ŠČERBA, Filip a kol. *Trestní zákoník: komentář.* 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 2926.
[201] Tamtéž, s. 2927.
[202] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7. s. 402.

vícekrát zřetelně sdělila, že si kontakt z jeho strany nepřeje. Za tuto dobu jí zaslal celkem 992 zpráv, ve kterých ji žádal o znovunavázání jejich vztahu, nabízel jí osobní setkání, emočně ji vydíral, přičemž poškozená mu odpověděla celkem 136 zprávami. Dále ji prostřednictvím stejné aplikace kontaktoval od 6. 2. 2019 do 12. 2. 2019, a to opět přesto, že s ním komunikovat nechtěla. Současně se během ledna ve frekvenci 2x až 3x týdně pokoušel o osobní styk s poškozenou, konkrétně když na ni čekal před jejím obydlím nebo v jeho bezprostřední blízkosti. Poškozené přitom zasílal zprávy o její současné lokaci, přestože mu ji sama nesdělila, a zároveň se informoval o tom, s kým je v současné době v kontaktu. Počínání obviněného způsobilo podstatné zhoršení kvality života a psychiky poškozené, kdy trpěla nespavostí, měla obavy opouštět své obydlí, být ve svém obydlí, obavy z dalšího kontaktování ze strany obviněného, a to se zřetelem k jeho chování za doby trvání jejich intimního vztahu. Proti rozsudku Obvodního soudu pro Prahu 6 podal obviněný odvolání, které Městský soud v Praze usnesením zamítl.

Obviněný podal proti usnesení Městského soudu v Praze dovolání, kdy namítal nesprávné hmotněprávní posouzení skutku v tomto rozhodnutí. Konkrétně nenaplnění znaku dlouhodobosti, kdy nezbytná délka pro nebezpečné pronásledování je dle judikatury alespoň doba 4 týdnů, přičemž v jeho případě se dle jeho názoru jednalo pouze o 23 dní. A to vzhledem k tomu, že kontaktování poškozené v druhém období bylo podloženo nedůvěryhodnými důkazy, snímky obrazovky poškozené. Z hlediska naplnění znaku vyhledávání osobní blízkosti nebo sledování poškozené uvádí, že jeho jednání nevybočovalo z norem společensky uznávaného chování. Rozporuje splnění znaku vytrvalého kontaktování skrze prostředky elektronických komunikací, kdy uvádí, že počet jím zaslaných zpráv je v případě elektronické komunikace mezi partnery běžný. V souvislosti s naplněním znaku omezení v obvyklém způsobu života, a ve vztahu k tomu, že by jeho jednání bylo způsobilé v poškozené vyvolat důvodnou obavu namítá, že soud pouze přijal výpověď poškozené nikterak podloženou jiným důkazem.

Nejvyšší soud se vyjádřil k podanému dovolání, kdy odkázal na předchozí judikaturu, ve které vymezil pojem nebezpečné pronásledování, a sice jako jednání útočníka s cílem obtěžovat jinou osobu natolik intenzivním způsobem, že ohrožuje její psychickou, a mnohdy i fyzickou integritu. Přičemž v některých případech není hranice toho, co lze považovat za společensky přijatelné, a kdy se již jedná o jednání

vyžadující trestněprávní reakce, zcela zřetelná. Za překročení této meze je považován okamžik, kdy pronásledovatel zcela bezvýsledně projevuje snahu získat náklonnosti oběti, navzdory již jí projevené vůli nebýt jím nadále kontaktována. Ve vztahu ke znaku dlouhodobosti uvedl, že byl tento znak nepochybně naplněn, když jím byla poškozená pronásledována po dobu 6 týdnů, a to i vzhledem k různorodosti a frekvenci jednotlivých jednání. Jednání pachatele vybočovalo z pravidel společensky přijatelného chování, když poškozené zaslal celkem 992 nevyžádaných zpráv, získával si informace o jejím soukromém životě, a vyhledával s ní osobní kontakt, přestože opakovaně a zřetelně vyjadřovala, že si to nežádá a považuje takové jednání za obtěžující. K způsobilosti vyvolání důvodné obavy v poškozené Nejvyšší soud poukazuje na výklad tohoto pojmu, kdy není podstatné, zda se poškozená skutečně obává, ale že jednání pachatele je svou povahou způsobilé důvodnou obavu v ní skutečně vyvolat. Přičemž jednání obviněného takovouto způsobilost mělo, když poškozenou sledoval, zjišťoval si o ní informace, kontaktoval ji, a nepřijal fakt definitivního ukončení jejich partnerského vztahu. Ve vztahu k námitce vážící se k omezování v obvyklém způsobu života, došlo i k naplnění tohoto znaku, kdy z prováděného dokazování jednoznačně vyplývá zásah, který poškozená v důsledku jednání obviněného utrpěla na svém psychickém zdraví, neboť musela v tomto směru vyhledat i odbornou pomoc. Dle posouzení Nejvyššího soudu došlo ke splnění všech znaků pro kvalifikaci jednání obviněného jako nebezpečné pronásledování podle ust. § 354 odst. 1 písm. b), c), d), a dovolání obviněného odmítl.[203]

3.4.5 Výzkum

a) Povědomí o kyberstalkingu

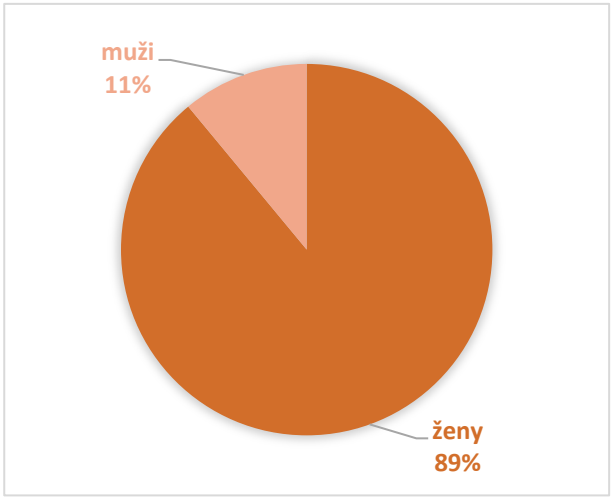
Z celkových 501 (100 %) respondentů jich celkem **435 (86,8 %)** uvedlo, že zná pojem kyberstalking. Na základně získaných dat lze říci, že obeznámenost s touto problematikou je ve společnosti relativně vysoká.

b) Oběti kyberstalkingu

Celkem **109 (21,8 %)** respondentů sdělilo, že se stalo obětí kyberstalkingu.

[203] Usnesení Nejvyššího soudu ze dne 30. 4. 2010, sp. zn. 4 Tdo 414/2020.

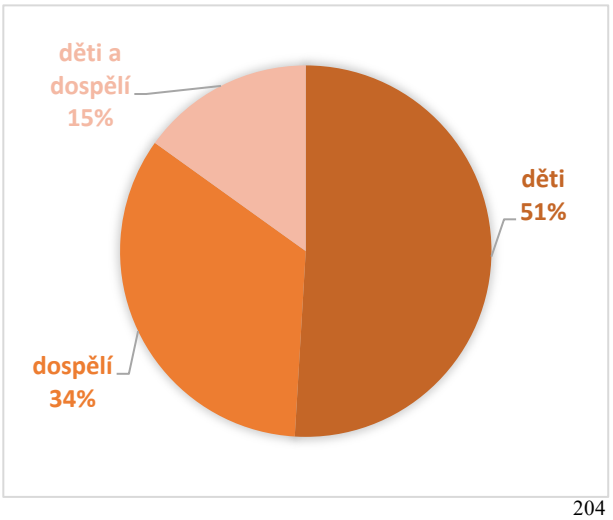
I. Oběti kyberstalkingu podle pohlaví



Dle výsledků provedeného výzkumu lze říci, že jsou obětí kyberstalkingu častěji ženy. Nicméně vezeme-li v úvahu vyšší procentuální zastoupení žen v dotazníkovém šetření, jsou výsledky následující:

- z celkového počtu 367 (100 %) žen v dotazníkovém šetření jich 97 (26,4 %) uvedlo, že se během svého života stalo obětí kyberstalkingu,
- v případě mužů pak z celkových 134 (100 %) totéž uvedlo 12 (9 %) respondentů. **Závěrem lze říci, že provedeným výzkumem bylo zjištěno, že jsou obětí kyberstalkingu častěji ženy.**

II. Oběti kyberstalkingu podle věku



[204]

[204] Celkem 3 respondenti neuvedli v dotazníkovém šetření věk, ve kterém se stali obětí kyberstalkingu. Z toho důvodu nejsou v uvedeném grafickém znázornění zohledněni.

V tomto případě je grafické znázornění koncipováno v souladu s ust. § 126 TrZ, dle kterého se dítětem rozumí osoba mladší 18 let. Graf je složen ze tří kategorií, a tedy děti, dospělí, a současně děti a dospělí, neboť někteří respondenti uvedli delší časové období, tj. období před dosažením i po dosažení 18 let. **Z výsledků provedeného výzkumu vyplývá, že jsou nejčastěji obětí kyberstalkingu děti, tedy osoby mladší 18 let.**

Z provedených studií na téma kyberstalkingu byly vyvozeny závěry, že jsou častěji prostřednictvím ICT pronásledovány ženy. Avšak ženy pronásledují muže skrze ICT častěji, nežli tomu činily dříve ve světě reálném. Dále lze říci, že převážnou část obětí tvoří osoby, které nejsou v partnerském vztahu. Děti jsou rizikovou skupinou v případě kyberstalkingu, kdy jim nebezpečí hrozí z řad jejich vrstevníků, nicméně v takovém případě se jedná o projev kyberšikany.[205]

[205] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. ISBN 978-80-7387-545-9. s. 80-81.

3.5 Krádež identity

Krádež virtuální identity, v anglickém překladu *identity theft*, je kybernetický útok, jež spočívá ve zmocnění se virtuální identity poškozeného pachatelem. Odcizení identity pak může být z hlediska časového trvalé či krátkodobé.[206] Motiv jednotlivých útočníků se může lišit, zpravidla má však tento útok finanční povahu, kdy důvodem pro krádež identity je získání přístupu k bankovnímu účtu poškozeného a možná manipulace s ním.[207]

Již výše jsem zmínila, že krádež identity je jedním z projevů kyberšikany, a krádež identity tak může mít i imateriální povahu.[208] Rozlišují se případy, kdy agresor založí na sociální sítí profil, tzv. falešný profil, pod kterým vystupuje, a vydává se jím za jiného. Na tomto profilu publikuje fotografie své oběti, údaje o ní, přičemž tento profil může vypadat věrohodně, a skutečně se tak ostatní uživatelé dané sociálně sítě mohou domnívat, že se jedná o oběť. Útočník tak činí za účelem poškození své oběti, například s cílem narušit její sociální vazby. Závažnější je krádež identity, kdy agresor získá přístupové údaje k účtu oběti, a vystupuje za ni přímo pod jejím profilem na sociální síti.[209] Krádež účtu na sociální síti je riziková především v tom, že se agresor seznámí s osobními daty poškozeného, jež může zneužít, a je způsobilý hodnověrným způsobem za něho na sociální síti vystupovat vůči ostatním uživatelům dané platformy.[210]

3.5.1 Právní úprava krádeže identity

Z trestněprávního pohledu se pachatel při krádeži identity obvykle dopouští více protizákonných jednání. V první řadě pachatel prolomí přihlašovací údaje poškozeného, a dostane se tak do jeho účtu na sociální síti. Pachatel může dosáhnout získání údajů poškozeného rovněž i instalací malware, tedy škodlivého kódu. Škodlivý kód funguje tím způsobem, že ze zařízení poškozeného soustřeďuje jeho citlivá data a přenáší je do zařízení útočníka, který tímto způsobem získá

[206] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. s. 318.
[207] ZAVRŠNIK, Aleš. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7552-758-5. s. 38.
[208] Tamtéž, s. 38.
[209] ČERNÁ, Alena. *Kyberšikana: průvodce novým fenoménem*. Praha: Grada, 2013. Psyché (Grada). ISBN 978-80-210-6374-7. s. 25.
[210] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7. s. 230.

přístupové údaje k virtuální identitě napadeného. Tímto jednáním se pachatel dopustí trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací podle ust. § 230 TrZ. Pokud pachatel překoná přihlašovací údaje, čímž se neoprávněně dostane k účtu oběti, naplní odst. 1 podle ust. § 230 TrZ, a pokud těchto údajů dosáhne instalací malware, naplní odst. 2 zmíněného ustanovení. Po napadení jeho účtu může dojít ke zneužití získaných údajů o této osobě, anebo může skrze účet poškozeného zaútočit na jiného uživatele.[211] Pachatel se tedy může svým jednáním dopustit i dalšího protiprávního jednání, kterým bude další trestný čin v souběhu, tzv. konkurenci, s trestným činem podle ust. § 230 TrZ. Těmito trestnými činy mohou být např. neoprávněné nakládání s osobními údaji podle ust. § 180 TrZ, porušení tajemství dopravovaných zpráv podle ust. § 182 TrZ, podvod podle ust. § 209 TrZ a další.[212]

a) Neoprávněný přístup k počítačovému systému a nosiči informací podle ust. § 230 TrZ

Tento trestný čin je obsažen v hlavě V. zvláštní části TrZ, a spadá do kategorie majetkových trestných činů páchaných v kyberprostoru společně s trestným činem opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat podle ust. § 231TrZ a poškození záznamu v počítačovém systému a na nosiči informací a zásahu do vybavení počítače z nedbalosti podle ust. § 232 TrZ. Zákonná úprava těchto trestných činů je především důsledkem Úmluvy a ust. § 230 TrZ je upraveno tak, aby s ní bylo v souladu. Rovněž pak podléhá harmonizaci se směrnicí 2013/40/EU, která taktéž cílí na problematiku kyberkriminality.[213]

Trestný čin podle ust. § 230 TrZ je složen ze dvou základních a tří kvalifikovaných skutkových podstat. Základní skutková podstata nevyžaduje způsobení škody poškozenému pachatelem. Tento znak je nezbytné naplnit až u kvalifikované skutkové podstaty.[214]

---

[211] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. s. 318-319.
[212] KANDOVÁ, Katarína, ČEP, David. In: ŠČERBA, Filip a kol. *Trestní zákoník: komentář*. 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8 s. 1890.
[213] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7. s. 556.
[214] KANDOVÁ, Katarína, ČEP, David. In: ŠČERBA, Filip a kol. *Trestní zákoník: komentář*. 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 1880-1881.

Podle ust. § 230 odst. 1 TrZ *„Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.“* Objektivní stránka této základní skutkové podstaty spočívá v překonání bezpečnostního opatření počítačového systému pachatelem, čímž neoprávněně nabyde přístupu k virtuální identitě napadeného. TrZ tedy neuvádí jako znak objektivní stránky tohoto trestného činu žádné další protiprávní jednání, a je tak naplněna již samotným prolomením bezpečnostních opatření a neoprávněným nabytím přístupu do počítačového systému.[215]

Podle § 230 odst. 2 TrZ *„Kdo získá přístup k počítačovému systému nebo k nosiči informací a*

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

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

Objektivní stránka druhé základní skutkové podstaty je naplněna, pokud pachatel nabude přístupu k počítačovému systému nebo k nosiči informací, je tedy způsobilý s nimi volně disponovat, a dopustí se některého z jednání uvedenými pod písm. a) až d), jež jsou vymezena alternativně. K naplnění této skutkové podstaty není podstatné, zda pachatel získal tento přístup neoprávněně.[216]

[215] KANDOVÁ, Katarína, ČEP, David. In: ŠČERBA, Filip a kol. *Trestní zákoník: komentář*. 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 1882.
[216] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7. s. 569.

V případě, že pachatel překonal bezpečnostní opatření, a neoprávněně tak nabyl přístupu k počítačovému systému nebo k jeho části, a zároveň se dopustil některého z jednání uvedených v ust. § 230 odst. 2 pod písm. a) až d) TrZ, není vyloučena konkurence těchto základních skutkových podstat. Pokud by takové jednání bylo posouzeno pouze podle jedné z nich, nebyla by dostatečně vyjádřena závažnost takového protiprávního jednání, neboť každá z těchto skutkových podstat chrání jiné společenské zájmy. Objektem základní skutkové podstaty podle prvního odstavce je důvěrnost počítačového systému a počítačových dat, jež jsou v nich uschována, a která mohou být zasažena neoprávněným přístupem k počítačovému systému, nebo k jeho části, po překonání bezpečnostních opatření. Skutková podstata vyjádřena v odstavci druhém naproti tomu chrání celistvost a dostupnost počítačových dat a systémů před neoprávněnými zásahy.[217] Z hlediska subjektivní stránky trestného činu je u obou základních skutkových podstat vyžadováno úmyslné zavinění, přičemž dostačujícím je i úmysl nepřímý. Pachatelem může být jakákoliv trestně odpovědná osoba, tedy osoba fyzická i právnická.[218]

Kvalifikované skutkové podstaty vymezené v odst. 3 až 5 se váží jak k první, tak k druhé základní skutkové podstatě. Přičemž ust. § 230 odst. 3 písm. a) TrZ řeší situaci, kdy pachatel získá přístup do počítačového systému,[219] a to oprávněně či neoprávněně,[220] a má zvláštní úmysl způsobit jinému škodu, jinou újmu anebo získat sobě nebo jinému neoprávněný prospěch. Pachatel tento svůj úmysl nemusí uskutečnit, nýbrž dostačujícím z hlediska naplnění této skutkové podstaty je, že tento úmysl má.[221] Pod pojmem škoda je míněna materiální újma, tedy škoda na majetku a ušlý zisk, zatímco jiná újma znamená penězi neocenitelnou, nemateriální újmu. Jako příklad jiné újmy lze uvést porušení občanské cti, narušení důvěry obchodního společníka, ztrátu hodnotných dat atp.[222] Neoprávněný prospěch je protiprávní prospěch nabytý pachatelem anebo jinou osobou, který může mít jak materiální, tak nemateriální podobu.[223]

---

[217] KANDOVÁ, Katarína, ČEP, David. In: ŠČERBA, Filip a kol. *Trestní zákoník: komentář.* 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 1881.
[218] Tamtéž, s. 1887.
[219] Tamtéž, s. 1887.
[220] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7. s. 572.
[221] KANDOVÁ, Katarína, ČEP, David. In: ŠČERBA, Filip a kol. *Trestní zákoník: komentář*. 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 1887.
[222] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7. s. 572.
[223] KANDOVÁ, Katarína, ČEP, David. In: ŠČERBA, Filip a kol. *Trestní zákoník: komentář.* 1. vydání. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8. s. 1887.

Pod ust. § 230 odst. 3 písm. b) TrZ je vyjádřen zvláštní úmysl pachatele, jenž spočívá v neoprávněném omezení funkčnosti počítačového systému nebo jiného nosiče informací. Ust. § 230 odst. 4 TrZ se vztahuje na případy, kdy činy uvedené v ust. § 230 odst. 1 nebo odst. 2 TrZ jsou podle písm. a) spáchány členem organizované skupiny, písm. b) je-li tímto činem způsobena značná škoda, písm. c) pokud je tímto činem přivozeno vážné poškození v činnosti orgánu státní správy, územní samosprávy, soudu nebo jiného orgánu veřejné moci, písm. d) tímto činem získá pachatel pro sebe či pro jiného značný prospěch, písm. e) je-li jím způsobeno vážné poškození v činnosti právnické osoby nebo fyzické osoby, jež je osobou podnikající. Ust. § 230 odst. 5 TrZ řeší situaci, kdy je činem uvedeným v základních skutkových podstatách způsobena podle písm. a) škoda velkého rozsahu, nebo je-li tímto činem podle písm. b) pro pachatele nebo jinou osobu získán prospěch velkého rozsahu.[224]

3.5.2 Judikatura

3.5.2.1 Usnesení Nejvyššího soudu sp. zn. 7 Tdo 1134/2020, ze dne 4. 11. 2020

Nejvyšší soud rozhodoval dne 4. 11. 2020 o podaném dovolání obviněného Š. H., který byl rozsudkem Okresního soudu v Českých Budějovicích dne 17. 12. 2019 uznán (mimo jiné) vinným přečinem neoprávněného přístupu k počítačovému systému a nosiči informací podle ust. **§ 230 odst. 1 TrZ**.

Obviněný užil přístupového hesla k e-mailové schránce poškozené (družka obviněného), které mu bylo z minulosti známo, neb ji tuto e-mailovou schránku pomáhal dříve založit, čímž neoprávněně získal k této e-mailové schránce přístup. Následně generací nového hesla bezpečnostní opatření změnil a k e-mailové schránce nastavil dvoufázové ověření na jím zadaném telefonním čísle. Dále obviněný za pomocí duplikátu SIM karty poškozené překonal bezpečnostní opatření k jejímu účtu na sociální síti Facebook, neboť své telefonní číslo užívala pro přihlášení se k tomuto profilu, čímž neoprávněně získal k tomuto jejímu profilu přístup. Rovněž pak heslo k účtu změnil. Tímto jednáním obviněný znemožnil své družce dále její e-mailovou schránku a profil na výše zmíněné platformě užívat. V této věci bylo podáno obviněným a v jeho neprospěch státní zástupkyní odvolání,

[224] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7. s. 574.

které bylo usnesením Krajského soudu v Českých Budějovicích pro nedůvodnost zamítnuto.

Obviněný podal v této věci dovolání k Nejvyššímu soudu, kde mimo jiné uvedl, že nedošlo k naplnění skutkové podstaty trestného činu podle ust. § 230 odst. 1 TrZ, jelikož nemusel bezpečnostní opatření překonávat, poněvadž mu bylo přístupové heslo z minulosti známo. Nejvyšší soud se ztotožnil s vyjádřením státní zástupkyně Nejvyššího státního zastupitelství, která ve svém vyjádření uvedla, že účet na sociální síti Facebook lze vnímat jako „obydlí". „Dveře" k tomuto obydlí tvoří nosič informací (počítačový systém či jiný nosič) a „klíčem" je ku příkladu heslo jakožto bezpečnostní opatření k příslušnému účtu, kterým lze tyto „dveře" odemknout. Není proto rozhodné, zda pachatel tento „klíč" zná z minulosti, a je tak schopen těmito „dveřmi" proniknout. Podstatné je, že pachatel ví, že těmito „dveřmi" proniká neoprávněně a narušuje tak soukromí poškozené, obdobně jako u porušování domovní svobody. Rovněž to, že obviněný pronikl do facebookového účtu poškozené pomocí duplikátní SIM karty, na kterou byl její soukromý účet na Facebooku vázán, a tím pak mohl získat nové heslo anebo se k účtu přímo přihlásit, lze vykládat za překonání bezpečnostního opatření ve smyslu ust. § 230 odst. 1 TrZ. Dovolání bylo Nejvyšším soudem jako zjevně neopodstatněné odmítnuto.[225]

3.5.2.2 Usnesení Nejvyššího soudu sp. zn. 7 Tdo 731/2015, ze dne 30. 9. 2015

Nejvyšší soud rozhodoval dne 30. 9. 2015 o podaném dovolání obviněného prap. Bc. J. S., který byl rozsudkem Okresního soudu v Příbrami dne 25. 11. 2014 uznán vinným přečinem neoprávněného přístupu k počítačovému systému a nosiči informací podle ust. **§ 230 odst. 2 písm. a), b) TrZ**, a byl odsouzen k trestu odnětí svobody v délce trvání 3 měsíců s podmíněným odkladem na zkušební dobu v trvání 12 měsíců. Obviněný se přečinu dopustil, když zkoušením náhodných kombinací uhodl přístupové heslo k elektronické poště a soukromému účtu na sociální síti Facebook své sestry, a neoprávněně na její facebookový účet vnikl. Následně na tomto profilu změnil její heslo, taktéž i profilovou fotografii, a zaslal jiným uživatelům této sociální sítě vybranou část soukromé elektronické pošty poškozené. Odvolání, které obviněný proti tomuto rozsudku podal, bylo Krajským soudem v Praze pro nedůvodnost zamítnuto.

[225] Usnesení Nejvyššího soudu sp. zn. 7 Tdo 1134/2020, ze dne 4. 11. 2020.

V podaném dovolání obviněný namítal, že byla v jeho věci porušena základní zásada trestního práva, zásady subsidiarity trestní represe podle ust. § 12 odst. 2 TrZ. A to z důvodu, že se jednalo o účet jeho sestry, která podala trestní oznámení v době, kdy si nebyla vědoma faktu, že osobou, jež se „nabourala" do jejího facebookového profilu, je její bratr. Dále pak uvedl, že v minulosti měl od své sestry souhlasné stanovisko se vstupem na tento její účet, avšak v současnosti jsou jejich rodinné vztahy nefunkční. Přesto však poškozená ve své výpovědi v hlavním líčení uvedla, že by jí ani v současné době vniknutí bratra na její facebookový profil nevadilo. Těmito skutečnostmi obviněný poukázal na značný stupeň snížení společenské škodlivosti v souvislosti se zásadou vyjádřenou v ust. § 12 odst. 2 TrZ, kdy dle jeho názoru je dostačující uplatnění norem jiného nežli trestního práva.

Dle vyjádření státního zástupce Nejvyššího státního zastupitelství se soudy již skutečnostmi uvedenými obviněným patřičně zabývaly. Upozornil na fakt, že z výpovědí poškozené vyplývá, že obviněnému nedala oprávnění ke vstupu na její soukromý účet, ani ke změně její profilové fotografie. Dále pak uvedl, že k trestnímu stíhání není zapotřebí souhlasu poškozené, jelikož se tento trestný čin neřadí mezi trestné činy podle ust. § 163 zákona č. 141/1961, o trestním řízení soudním (trestní řád a dále jen *„TrŘ"*), kdy je souhlasné stanovisko poškozeného s trestním stíháním nezbytné. K opomenutí základní zásady se vyjádřil v tom směru, že souhlasí s právním závěrem soudu prvního stupně, neb svým jednáním obviněný naplnil všechny znaky skutkové podstaty ust. § 230 odst. 2 písm. a), b) TrZ.

Dovolací soud neshledal námitky obviněného za důvodné, kdy ve svém vyjádření poukázal na to, že podle ust. § 230 odst. 2 TrZ může být vstup pachatele oprávněný i neoprávněný, narozdíl od ust. § 230 odst. 1 TrZ, avšak pachatel se neoprávněně, tedy bez souhlasu poškozené, dopustil jednání uvedeného pod písm. a), b) ust. § 230 odst. 2 TrZ. Přestože důvodem mohl být vtip, nepříznivé rodinné vztahy atp., podstatná je samotná neoprávněnost jednání obviněného, kterým se dopustil trestného činu podle ust. § 230 odst. 2 písm. a), b) TrZ, a tím byl zasažen zájem chráněný TrZ. Nejvyšší soud dovolání obviněného odmítl jako zjevně neopodstatněné.[226]

[226] Usnesení Nejvyššího soudu sp. zn. 7 Tdo 731/2015, ze dne 30. 9. 2015.

3.5.2.3 Současné případy řešené Policií ČR

Kriminalisté se během roku 2022 potýkali s novými způsoby útoků v kyberprostoru, jejichž následkem jsou škody v řádu jednotek milionů korun. Způsob provedení těchto útoků byl ve všech případech obdobný. Pachatel se neoprávněně zmocnil e-mailové schránky poškozeného, a skrze e-mailovou adresu prolomil bezpečnostní opatření na facebookovém profilu. Následně pak zaslal jiným uživatelům této sociální sítě, které měl poškozený na svém účtu v přátelích, zprávu obsahující odkaz. Po otevření tohoto odkazu se zobrazila stránka vizuálně připomínající stránku pro přihlášení se k této platformě. V okamžiku, kdy uživatelé zadali přihlašovací údaje ke svému účtu, byly současně získány i pachatelem. Pokud byl daný účet navázán na platební kartu poškozeného, pachatel pomocí finančních operací neoprávněně ve svůj prospěch získal finanční prostředky poškozeného. V konečné fázi pachatel sdílel na profilu poškozeného příspěvek zobrazující dětskou pornografii, na základě čehož byl poskytovatelem této sociální sítě účet odstraněn. Dle právní kvalifikace Policie ČR se jedná o trestný čin podle ust. § 230 TrZ.[227]

Dále Policie ČR zdůrazňuje, že vhodnou bezpečnostní ochranou pro zmenšení rizika potencionálního kybernetického útoku je dvoufázové ověření, tedy dvojí ověření identity uživatele v rámci přihlašovacího procesu, a současně i dostatečně silné přístupové heslo, které by se nemělo pro e-mailovou schránku a účet na sociální síti shodovat. Doporučena je rovněž i frekventovaná obměna stávajících hesel, nejméně jedenkrát za příslušný kalendářní rok.[228]

3.5.3 Výzkum

a) Povědomí o krádeži identity

Z výsledků provedeného výzkumu vyplývá, že z celkových 501 (100 %) respondentů jich 455 (90,8 %) zná pojem krádež virtuální identity. Lze tak předpokládat, že obeznámenost s touto problematikou je ve společnosti relativně vysoká.

---

[227] MORAVČÍK, Ondřej. *Nové praktiky podvodníků při krádežích facebookových identit.* Policie ČR. Policie České republiky, [cit. 27.10.2022].
Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx
[228] Tamtéž.

b) Uživatelé, kterým byl jejich účet na sociální síti odcizen

Celkem 179 (35,7 %) respondentům byl v minulosti účet na sociální síti odcizen. Přičemž 112 (62,6 %) uživatelů s odcizeným účtem využilo bezpečnostních opatření, jež daná platforma nabízí (zejména byl dotaz cílen na dvoufázové ověření). Celkem 105 (58,7 %) respondentům byl jejich odcizený účet navrácen. Sociální sítě, na kterých podle provedeného výzkumu nejčastěji dochází ke krádeži identity, jsou Instagram a Facebook.

Dle publikovaných dat byla v roce 2010 odcizena virtuální identita přibližně v 10 milionech případů pouze ve Spojených státech amerických. Avšak nejednalo se pouze o účty na sociálních sítích, ale i o zneužití údajů pro získání přístupu k jiným informačním systémům.[229]

[229] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7. s. 255.

4 Odhalování a vyšetřování kyberkriminality na sociálních sítích

Tato kapitola vznikla po odborné konzultaci s Oddělením analytiky a kybernetické kriminality Městského ředitelství Policie České republiky v Plzni a poskytuje alespoň krátký vhled do postupu orgánů činných v trestním řízení (dále jen „OČTŘ“) při odhalování a vyšetřování kyberkriminality na sociálních sítích v rámci trestního řízení. Zejména se však tato část diplomové práce soustředí na jednotlivé procesní instituty, které mohou OČTŘ při zajišťování dat ze sociálních sítí využít. Před tím, než bude věnována pozornost trestněprocesnímu postupu OČTŘ, je nezbytné vymezení pojmu digitální stopa a objasnění povahy sociálních sítí podle platné judikatury Ústavního soudu (dále jen „ÚS“).

4.1 Digitální stopa

Digitální stopa, je-li akceptovatelná OČTŘ, může sloužit jako důkazní materiál, a to nejen u trestných činů spáchaných v kyberprostoru.[230] V odborné literatuře se lze setkat s vícero definicemi digitální stopy, konkrétně pak dle docenta J. Koloucha lze digitální stopu chápat jako *„jakákoli data či informace přenesená, vytvořená, uložená či modifikovaná za použití počítačového systému.“*[231] Současně lze říci, že má digitální stopa mnohé specifické vlastnosti, a to právě proto, že se nachází v kyberprostoru. Vyznačuje se svou nehmotnou podobou, objemností co do velikosti dat, dynamickou povahou, nepříliš dlouhou životností[232] a relativně obtížnou lokalizací.[233] Pro zachování její průkazní hodnoty je nezbytný kvalifikovaný a zákonný procesní postup OČTŘ.[234] Z hlediska systematizace TrŘ je digitální důkaz podřazen současně pod věcné i listinné důkazy, v čemž lze

[230] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7. s. 697-698.
[231] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. s. 403.
[232] PORADA, Viktor a Karel RAIS. *Právní, kriminalistické a kybernetické aspekty kybernetické kriminality a bezpečnosti: pocta Vladimíru Smejkalovi*. Brno: Akademické nakladatelství CERM, 2021. ISBN 978-80-7623-065-1. s. 272.
[233] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. s. 403.
[234] PORADA, Viktor a Karel RAIS. *Právní, kriminalistické a kybernetické aspekty kybernetické kriminality a bezpečnosti: pocta Vladimíru Smejkalovi*. Brno: Akademické nakladatelství CERM, 2021. ISBN 978-80-7623-065-1. s. 273.

spatřovat jisté nedostatky, když se vyznačuje výše uvedenými specifickými vlastnostmi.[235]

4.2 Povaha sociálních sítí

Sociální sítě jsou využívány širokou masou uživatelů, avšak dle judikatury ÚS není jejich povaha ani čistě veřejná, ani čistě soukromá. Sociální síť má povahu veřejnou, pakliže uživatel na svůj profil přidává příspěvky pro nikterak omezený okruh uživatelů. Naopak soukromou povahu má v případě, když jsou uživatelem přidávány příspěvky pouze pro omezený okruh uživatelů, anebo pokud je prostřednictvím sociální sítě mezi uživateli vedena soukromá konverzace (v rámci tzv. *chatu*). Současně je nezbytné zdůraznit, že sám uživatel si nastavuje míru soukromí na svém profilu, tedy zda jsou jím přidané příspěvky na profilové stránce veřejně viditelné, anebo jsou-li přístupné pouze vymezenému okruhu uživatelů.[236]

Pokud se jedná o část veřejnou, mohou OČTŘ zajišťovat její obsah bez dalšího, tj. bez souhlasu státního zástupce anebo soudce,[237] a to právě pro její veřejnou přístupnost srovnatelnou v takovém případě s tiskem či televizí.[238] V případě, kdy by OČTŘ kontrolovaly a zaznamenávaly data z této veřejné části po delší časové období, bylo by nezbytné postupovat v souladu s ust. § 158d odst. 2 TrŘ, a tedy se souhlasem státního zástupce, jelikož by se v takovém případě již jednalo o sledování, při kterém jsou určitým způsoben zaznamenávána data, a tímto způsobem by již bylo zasahováno do soukromí uživatele. Lze totiž říci, že daný uživatel nepředpokládá, že by byl jím sdílený obsah dohledatelný po uplynutí delšího časového období.[239] Pokud je OČTŘ získáván obsah z části soukromé, je procesní postup obtížnější, přičemž je nezbytné, aby respektovaly zákonnou úpravu, postupovaly v souladu s trestním řádem a šetřily zaručených základních lidských práv a svobod.[240]

---

[235] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. s. 419.
[236] Nález Ústavního soudu České republiky, sp. zn. III.ÚS 3844/13 ze dne 30. 10. 2014.
[237] DOSTÁL, Otto. *Zajišťování důkazů u počítačové kriminality – uložiště, e-maily, telefony, sociální sítě a logy* (4 díl). Trestněprávní revue, 2019, č. 6. s. 123-127.
[238] SKALICKÁ, Veronika. *Není odposlech jako odposlech*. Trestněprávní revue, 2022, č. 1. s. 20-32.
[239] DOSTÁL, Otto. *Zajišťování důkazů u počítačové kriminality – uložiště, e-maily, telefony, sociální sítě a logy* (4 díl). Trestněprávní revue, 2019, č. 6. s. 123-127.
[240] Nález Ústavního soudu České republiky, sp. zn. III.ÚS 3844/13 ze dne 30. 10. 2014.

4.3 Trestněprocesní postup

OČTŘ se o spáchání trestné činnosti v prostředí sociálních sítí nejčastěji dozvídají prostřednictvím podaného trestního oznámení, k jehož přijímání má povinnost státní zástupce a policejní orgán podle ust. § 158 odst. 2 TrŘ. V praxi se tak může jednat např. o situaci, kdy podá trestní oznámení zákonný zástupce nezletilého, pokud byl tento nezletilý lákán predátorem k osobní schůzce, anebo byl-li jím vydírán, a to často poté, kdy od nezletilého v rámci komunikace na sociální síti získal pornografický anebo jiný intimní materiál. V takovém případě postupuje policejní orgán tak, že buďto sám zajistí snímek obrazovky (tzv. *screenshot*), jež opatří digitální pečetí (tzv. *hash*), anebo zajistí data prostřednictvím *screenshotu* nebo jejich nahráním na paměťovou kartu sám oznamovatel, a to pro účely jejich budoucího vydání podle ust. § 78 odst. 1 TrŘ. Současně jsou zajišťovány identifikační čísla profilových účtů a jiné, na předmětném účtu (či účtech), veřejně dohledatelné informace. Dalším častým způsobem, kterým se OČTŘ dozvídají o trestné činnosti spáchané na sociálních sítích, je mezinárodní cestou, konkrétně skrze neziskovou organizaci NCMEC (*National Center for Missing and Exploited Children*). Tato nezisková organizace v případě zachycení závadového obsahu na sociální síti uvědomí reportem Europol (pokud pochází závadová data z Evropy), a jestliže jsou tato data původem z České republiky, postoupí se případ do tuzemska, konkrétně Národní centrále proti organizovanému zločinu (dále jen „NCOZ“) společně s identifikačními údaji předmětného profilu. Pokud lze podezřelého podle daného profilu identifikovat, předá NCOZ případ věcně a místně příslušnému organizačnímu útvaru. V obou případech je následující postup totožný, a tedy podle ust. § 158 odst. 3 TrŘ sepíše policejní orgán neprodleně záznam o zahájení úkonů trestního řízení k objasnění a prověření skutečností důvodně nasvědčujících tomu, že byl spáchán trestný čin, a pokud hrozí nebezpečí z prodlení, sepíše tento záznam až po provedení neodkladných a neopakovatelných úkonů. Dále pak může policejní orgán činit další procesní postupy. Zejména v této fázi dochází k zajišťování dat ze sociálních sítí, přičemž se postup policejního orgánu může různit v závislosti na konkrétních okolnostech daného případu.[241]

[241] Osobní konzultace s Oddělením analytiky a kybernetické kriminality Městského ředitelství Policie České republiky v Plzni.

4.3.1 *Data freeze* podle ust. § 7b TrŘ

Policejní orgán může využít institutu *data freeze* podle ust. § 7b TrŘ, díky kterému jsou již existující data uchována v originální podobě, a to pro účely jejich možného budoucího zajištění dle jiného procesního nástroje, a to konkrétně podle ust. § 88a TrŘ.[242]

Ust. § 7b TrŘ, rozšiřující obecná ustanovení o poskytování součinnosti, bylo do naší právní úpravy přijato v důsledku povinnosti implementace čl. 16 a 29 Úmluvy. Podstatou tohoto ustanovení je, že policejní orgán může se souhlasem státního zástupce (i bez takového souhlasu nesnese-li věc odkladu a nelze-li souhlasu předem dosáhnout) vydat příkaz osobě, která drží data uložená v počítačovém systému nebo na nosiči informací (tedy komukoliv), aby je uchovala v nezměněné podobě pro účely trestního řízení po stanovenou dobu (nejdéle však po dobu 90 dnů), a současně učinila potřebná opatření pro uchování tajnosti jí takto uloženého příkazu. Předmětné ustanovení podléhá ze strany odborné veřejnosti kritice, neboť v takovém případě subjekty, které nejsou OČTŘ, zasahují do práv vlastníků těchto dat, když je bez jejich vědomí uchovávají a chrání, aby mohla být OČTŘ v budoucnu zajištěna pro důkazní účely v trestním řízení. Za problematické je přitom považováno to, že pro takový zásah ze strany subjektů odlišných od OČTŘ nebyl dán souhlas soudu.[243]

4.3.2 Dožádání podle ust. § 8 odst. 1 TrŘ

Pokud se sídlo provozovatele dané služby nachází v České republice, je možný postup pro OČTŘ příznivější, neboť mohou některé informace o uživateli získat prostřednictvím institutu dožádání podle ust. 8 § odst. 1 TrŘ.[244] Nicméně předmětné ustanovení zmocňuje OČTŘ pouze k získání takových informací, jež nepodléhají telekomunikačnímu tajemství, anebo na které se nevztahuje ochrana osobních a zprostředkovaných dat. Informace, jež může OČTŘ dožádat, lze souhrnně označit za údaje poskytovateli běžně známé z jeho činnosti. Docent

[242] Osobní konzultace s Oddělením analytiky a kybernetické kriminality Městského ředitelství Policie České republiky v Plzni.
[243] TLAPÁK NAVRÁTILOVÁ, Jana, GALOVCOVÁ, Ingrid. *Uchovávání dat uložených v počítačovém systému – poskytování součinnosti, nebo nahrazování činnosti orgánů činných v trestním řízení?.* Bulletin advokacie, 2019, č. 11, s. 36-39.
[244] Osobní konzultace s Oddělením analytiky a kybernetické kriminality Městského ředitelství Policie České republiky v Plzni.

J. Kolouch ve svém díle *CyberCrime* přibližuje tyto údaje, a sice, že OČTŘ jsou oprávněny zažádat např. o IP adresu uživatele, některé informace s IP adresou související, informace vztahující se k uživatelově e-mailové schránce, či o jiné základní identifikační a registrační údaje. Naproti tomu, pokud by OČTŘ vyžadovaly rozsáhlé penzum údajů, k jejichž zjištění by provozovatel musel analyzovat danou síť, nebyl by postup podle ust. § 8 odst. 1 TrŘ zákonný, neboť se by se již jednalo o zjišťování údajů z telekomunikačního provozu. Takové údaje by mohly být OČTŘ získány pouze na základě ust. § 88a TrŘ, tedy se souhlasem soudu, a při splnění zákonem stanovených podmínek.[245]

Za specifikum ust. § 8 odst. 1 TrŘ lze považovat jeho územní omezení, neboť OČTŘ mohou účinně využívat tohoto institutu pouze v České republice, tedy na poskytovatele jako je např. Seznam.cz, nebo Economia, a. s., která je provozovatelem Centrum.cz. Avšak je nezbytné si uvědomit, že v dnešním globalizovaném světě mají všechny velké společnosti poskytující sociální sítě svá sídla mimo Českou republiku, a tak je vyžadování dat ze strany OČTŘ značně ztížené, někdy až zcela nemožné. V takovém případě pak OČTŘ postupují podle ust. §88a TrŘ, avšak vyhovění tomuto příkazu ze strany zahraničních subjektů je čistě dobrovolné.[246] V některých případech však spolupráce na základě ust. § 88a TrŘ funguje dlouhodobě (např. se společností Meta Platforms, Google či Microsoft). Pro operativní účely a rychlost celého procesu pak OČTŘ využívají i výše zmíněného institutu dožádání podle ust. § 8 odst. 1 TrŘ, nicméně je pouze na těchto zahraničních subjektech, zda dané údaje dobrovolně poskytnou, či nikoliv. V případě odmítnutí poskytnutí takových údajů lze využít pouze Evropského vyšetřovacího příkazu (v rámci Evropské unie) anebo se lze jejich získání domoci cestou mezinárodní justiční spolupráce (mimo Evropskou unii), která je však značně časově náročná.[247]

[245] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. s. 414-415.
[246] Ust. §88a TrŘ je využíváno OČTŘ především na území České republiky za účelem vyžádání telekomunikačních údajů od subjektů zajišťujících veřejnou komunikační síť nebo poskytujících veřejnou službu elektronických komunikací (operátorů).
[247] Osobní konzultace s Oddělením analytiky a kybernetické kriminality Městského ředitelství Policie České republiky v Plzni.

4.3.3 Zjištění údajů o telekomunikačním provozu pode ust. § 88a TrŘ

Pokud jsou zjišťovány provozní, lokalizační či jiné obsahové údaje, především logy[248], anebo má-li společnost poskytující sociální síť sídlo mimo Českou republiku (v tomto případě se nejedná o jediný možný postup viz výše), postupují OČTŘ podle ust. § 88a TrŘ. Nicméně je tento postup možný pouze v případě, je-li trestní řízení vedeno pro úmyslný trestný čin s horní hranicí trestní sazby nejméně 3 roky, pro jiné v tomto ustanovení taxativně vyjmenované trestné činy nebo trestné činy k jejichž stíhání je Česká republika zavázána mezinárodní smlouvou (dle Úmluvy se jedná např. o trestné činy vztahující se k dětské pornografii[249]). A současně vydá v přípravném řízení soudce na návrh státního zástupce příkaz k vydání údajů, podléhajících telekomunikačnímu tajemství anebo ochraně osobních a zprostředkovaných dat, pouze pokud není možné sledovaného účelu dosáhnout jiným způsobem, nebo pokud by bylo dosažení tohoto účelu podstatně ztížené. Takto vydaný příkaz musí být písemný, řádně odůvodněný, a je-li vedeno trestní řízení pro trestný čin, k jehož stíhání je Česká republika zavázána mezinárodní smlouvou, musí obsahovat rovněž odkaz na danou mezinárodní smlouvu. V případě, vztahuje-li se příkaz ke konkrétnímu uživateli, jehož totožnost je známa, je nezbytné jej v něm identifikovat. Vydání informací komunikuje s danou sociální sítí Útvar zvláštních činností (dále jen „ÚZČ“). V momentu, kdy ÚZČ od společnosti poskytující sociální síť obdrží tyto údaje (typicky se bude jednat o registrační údaje, IP adresu, logy), předá je příslušnému OČTŘ k dalšímu postupu v trestním řízení. Prostřednictvím získané IP adresy je možné podezřelého snadněji identifikovat (anebo potvrdit jeho totožnost). V tomto směru je nezbytné rozlišovat IP adresu na statickou a dynamickou. Statická IP adresa může být přidělena ke konkrétnímu místu či uživateli, naopak dynamická IP adresa (tzv. NAT) je poskytována ve stejnou chvíli vícero uživatelům (a proto je v tomto případě nezbytné znát i přesný čas připojení do sítě či disponovat i jinými identifikačními údaji nežli pouhou IP adresou). Pro ztotožnění podezřelé osoby na základě získaných údajů postupují OČTŘ opět prostřednictvím ust. § 88a TrŘ, tzn. že je soudcem vydán příkaz k poskytnutí údajů o telekomunikačním provozu vážící se ke konkrétní IP adrese. Jelikož zákon č. 127/2005 Sb., o elektronických komunikacích (dále jen „ZoEK“) dopadá na v něm vymezené subjekty, tedy

[248] Záznam činností provedených v softwarovém systému.
[249] A naopak by tento postup nebyl možný např. u trestného činu pomluvy.

provozovatele komunikační sítě, může nastat i případ, kdy telekomunikační síť provozuje zapsaný spolek (např. PilsFree, z. s.), na který se tato zákonná úprava nevztahuje, a tyto společnosti nemají zákonnou povinnost uchovávat telekomunikační data, tudíž jimi nemusí disponovat. Zároveň je u těchto společností běžné, že poskytují dynamické IP adresy, které jsou přiděleny většímu okruhu uživatelů (tzv. NAT).[250]

Současně je nezbytné, v souvislosti s výše uvedeným, objasnit zákonnou úpravu ZoEK, kdy podle ust. § 97 odst. 3 mají subjekty zajišťující veřejnou komunikační síť nebo poskytující veřejnou službu elektronických komunikací (operátoři), v souvislosti s poskytováním jejich služeb, povinnost uchovávat provozní a lokalizační údaje po dobu 6 měsíců (tzv. *data retention*). Tyto údaje jsou povinny OČTŘ poskytnout na základě ust. §88a TrŘ, a to v případě splnění zákonem stanovených podmínek. Přičemž díky provozním a lokalizačním údajům OČTŘ zjistí detailní informace ohledně komunikace daného uživatele, např. v jakou hodinu se připojil k internetu.[251]

4.3.4 Sledování osob a věcí podle ust. § 158d (3) TrŘ

OČTŘ mohou získat přístup ke sledování obsahu komunikace podezřelého na základě povolení soudce podle ust. § 158d odst. 3 TrŘ. Povolení se vztahuje pouze na data již existující, nikoliv na data vzniklá v budoucnu. Na základě tohoto ustanovení tedy OČTŘ získají veškerý obsah již existující a uchované komunikace (resp. obsah té, o kterou si zažádají), a to k dané chvíli vyžádání dle časového rozsahu tohoto povolení.[252]

[250] Osobní konzultace s Oddělením analytiky a kybernetické kriminality Městského ředitelství Policie České republiky v Plzni.
[251] PŘÍKAZSKÁ, Lenka, MOHELSKÝ, Michal. *Současná právní úprava data retention je dle Ústavního soudu ústavně konformní a tedy přípustná.* [online]. Epravo.cz – Váš průvodce právem – Sbírka zákonů, judikatura, právo, [cit. 26.3.2023].
Dostupné z: https://www.epravo.cz/top/clanky/soucasna-pravni-uprava-data-retention-je-dle-ustavniho-soudu-ustavne-konformni-a-tedy-pripustna-110069.html?mail
[252] Osobní konzultace s Oddělením analytiky a kybernetické kriminality Městského ředitelství Policie České republiky v Plzni.

4.3.5 Odposlech a záznam telekomunikačního provozu podle ust. § 88 TrŘ

Pokud je vedeno trestní řízení pro zločin, na který zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně 8 let či jiné v tomto ustanovení taxativně vymezené trestné činy anebo trestné činy k jejichž stíhání je Česká republika zavázána na základě mezinárodní smlouvy, může být na návrh státního zástupce soudcem vydán příkaz k odposlechu a záznamu telekomunikačního provozu. Podle ust. § 88 odst. 5 TrŘ může OČTŘ nařídit záznam a odposlech telekomunikačního provozu i bez příkazu soudce, pakliže s tím uživatel odposlouchávané stanice souhlasí, avšak pouze v případě v tomto ustanovení taxativně vymezených trestných činů např. trestného činu vydírání podle ust. § 175 TrZ, nebezpečného vyhrožování podle ust. § 353 TrZ nebo nebezpečného pronásledování podle ust. § 354 TrZ.

OČTŘ v tomto případě získávají přístup k aktuálně probíhající komunikaci podezřelého uživatele. Avšak v souvislosti s kyberkriminalitou na sociálních sítích je využití tohoto institutu OČTŘ značně problematické, a to z rozličných důvodů, např. kvůli šifrované komunikaci, zahraničním subjektům atp. Policejní orgán dále nemohl uvádět bližší informace či konkrétní postupy z taktických důvodů.[253]

4.3.6 Domovní prohlídka podle ust. § 83 TrŘ

V některých případech může dojít k domovní prohlídce, nicméně se nejedná o pravidelný postup. Domovní prohlídka se provádí zejména u trestné činnosti související s dětskou pornografií a jinými vybranými trestnými činy. V takových případech totiž hrozí, že by mohly být digitální stopy v osobních zařízeních zničeny, smazány či modifikovány, pokud by nebyly včas zajištěny v rámci domovní prohlídky. OČTŘ tedy v těchto případech nemohou nařídit vydání těchto dat podle ust. § 78 odst. 1 TrŘ, neboť se tento postup jeví v takových případech jako neúčelný.

Pokud je tedy v takových případech podezřelá osoba ztotožněna, a značí-li zajištěná data, že v počítačovém systému nebo na nosiči informací, které se nacházejí v jejím bytě nebo jiném prostoru sloužícímu k bydlení či prostorám k nim náležejícím, uchovává důkazy důležité pro trestní řízení, provede policejní orgán

[253] Osobní konzultace s Oddělením analytiky a kybernetické kriminality Městského ředitelství Policie České republiky v Plzni.

domovní prohlídku, ke které vydává příkaz soudce na návrh státního zástupce. Při prováděné domovní prohlídce se zajišťují veškerá elektronická zařízení a příslušenství k nim náležející (USB flash disk, paměťové karty atp.). Při zajišťování elektroniky a jejího příslušenství je nezbytná přítomnost znalce, přičemž policejní orgány využívají primárně znalce z Odboru kriminalistické techniky a expertízy Policie České republiky (tzv. OKTE). Znalec předmětnou elektroniku a její příslušenství zajišťuje v souladu s předepsaným postupem tak, aby nedošlo k poškození dat, jejich modifikaci atp. Následně podrobí zajištěná zařízení znaleckému zkoumání.[254]

Zákonné nástroje pro zajišťování dat na sociální síti	
ust. § 7b TrŘ	Konzervace dat pro budoucí zajištění OČTŘ dle jiného právního nástroje
ust. § 8 odst. 1 TrŘ	Dožádání identifikačních a registračních údajů
ust. § 88a TrŘ	Zajištění údajů o telekomunikačním provozu
ust. § 158d odst. 3 TrŘ	Sledování již existujících záznamů na předmětném profilu
ust. § 88 TrŘ	Sledování do budoucna vzniklých záznamů na předmětném profilu
ust. § 83 TrŘ	Zajišťování důkazů v rámci domovní prohlídky

[254] Osobní konzultace s Oddělením analytiky a kybernetické kriminality Městského ředitelství Policie České republiky v Plzni.

Závěr

Pro celistvost této práce byla v první kapitole věnována pozornost základní terminologii, kterou si bylo pro lepší pochopení celého obsahu této práce nezbytné osvojit. Dále v kapitole druhé byla objasněna podstata sociálních sítí, přičemž lze s jistotou říci, že se jejich obliba každým rokem stupňuje, nicméně spolu s ní vzrůstá i trestná činnost, jež je v tomto prostředí páchána. Stále zvyšující se počet kybernetické trestné činnosti vnímám jako signál pro naléhavé řešení této problematiky. A současně lze očekávat, že bude množství případů spojených s kyberkriminalitou do budoucna stále jen stoupat, proto je nevyhnutelné, aby byla společnost na tento rozmach dostatečně připravena.

Kapitola třetí je nejobsáhlejší částí této práce, neboť je její samou podstatou. Jelikož naše trestněprávní úprava nepracuje s pojmy jako je kyberšikana, sexting, kybergrooming, kyberstalking nebo krádež virtuální identity, bylo cílem této diplomové práce objasnit tyto rizikové jevy, jež se v prostředí sociálních sítí hojně vyskytují, a nabídnout k nim možnou trestněprávní kvalifikaci podle pozitivní právní úpravy. Zároveň je každá podkapitola zabývající se těmito patologickými jevy doplněna i o přiléhavou judikaturu, která umožňuje lépe pochopit aplikaci jednotlivých ustanovení na konkrétní projevy kyberkriminality na sociálních sítích.

Nejprve byla rozebírána kyberšikana, byly vytyčeny její projevy a jejich možná právní kvalifikace. V tomto směru je nezbytné podotknout, že naše právní úprava kyberšikanu jako takovou neupravuje, a proto je nezbytné její jednotlivé projevy subsumovat pod existující ustanovení TrZ. Český zákonodárce by tak mohl přijmout např. po vzoru slovenské právní úpravy její legální zakotvení. Z mého pohledu by se tak dalo vyhnout situacím, kdy se některé z jejích projevů nedají postihnout trestním právem, a útočníci tak zůstávají nepotrestáni. Současně, a především, by její legální zakotvení mohlo eliminovat počet případů jejího výskytu. Podle mého názoru někteří uživatelé nedomýšlejí možné dopady jejich jednání v kyberprostoru na jiné osoby. Legální definice by pak mohla na straně jedné snížit výskyt kyberšikany, neboť by se řada uživatelů takovému jednání pod hrozbou trestní sankce vyvarovala, a současně by napomohla objasnit, jaké jednání je ve světe on-line přijatelné (resp. jaké jednání je protiprávní z pohledu trestního práva).

Následovně byl rozebírán sexting, který představuje zvlášť rizikovou komunikaci na sociálních sítích, a to z mnoha důvodů. Osoba, která zašle svůj intimní, choulostivý či pornografický materiál, může být prostřednictvím tohoto materiálu následně zneužívána, anebo vydírána např. za účelem poskytnutí dalšího takového materiálu. Stěžejním problémem sextingu je, že napomáhá ve vytváření a šíření dětské pornografie. V tomto směru spatřuji nezbytnou osvětu, co se rizik ohledně poskytování takového materiálu jiné osobě týče.

Sexting je zpravidla jednou z částí kybergroomingu, kterému byla taktéž věnována celá jedna podkapitola. Ve vztahu k právní úpravě kybergroomingu spatřuji určitou mezeru, a to že jsou ust. § 193b TrZ chráněny pouze osoby mladší 15 let. Přičemž v kapitole zaměřené na problematiku kybergroomingu lze nalézt, že dle oficiálních statistik jsou obětí kybergroomera nejčastěji děti ve věku od 13 do 17 let. Lze tak říci, že je věková kategorie dětí od 15 do 17 let nejvíce ohrožena, když lákání takto starého dítěte kybergroomerem k osobnímu setkání za účelem toto dítě např. znásilnit není trestným činem.

Dále byl rozebírán kybertstalking, který představuje nebezpečné pronásledování v kyberprostoru. V tomto ohledu byla rozbírána skutková podstata trestného činu nebezpečného pronásledování, kterou lze na tento rizikový jev aplikovat, pakliže jsou naplněny její zákonné znaky.

V neposlední řadě byla rozebírána krádež virtuální identity, a to zejména ve vztahu ke kyberšikaně, neboť je jedním z jejích charakteristických projevů. V tomto ohledu se lze ztotožnit s doporučením Policie České republiky uvedeným v rámci této podkapitoly a to, aby si uživatelé řádně chránili své účty v podobě všech možných bezpečnostních opatření, která jsou sociálními sítěmi poskytována (např. dvoufázové ověření v rámci přihlašovacího procesu).

V diplomové práci jsou obsažena data získaná z provedeného výzkumu, jež jsou detailně rozebrána v rámci jednotlivých podkapitol společně s grafickým znázorněním. Generálně pak lze ve vztahu k provedenému výzkumu říci, že kvantitativní metoda v podobě dotazníkového šetření samozřejmě nevykazuje 100% relevanci výsledků, nicméně získané výsledky jednoznačně ukazují, že se společnost, a v některých případech i relativně hojně, potýká s tímto druhem trestné činnosti.

Současně považuji za nezbytné uvést, že ve vztahu k těmto rizikovým jevům nepovažuji za stěžejní pouze legislativní rovinu, ale i rovinu psychologickou, kybernetickou, pedagogickou atp., neboť se jedná o mezioborovou problematiku.

Je nezbytné, aby byla přijímána právní úprava, která reaguje na růst a potažmo i různorodost tohoto druhu trestné činnosti, nicméně za stejně nezbytnou vnímám i edukaci, a to především dětí, jež jsou rizikovou skupinou především ve vztahu ke kyberšikaně, sextingu a kybergroomingu. Děti by měly být varovány, a to nejen svými pedagogy, ale i rodiči, na rizika spojená s komunikací ve virtuálním světě. V rámci školských zařízení by tak měla být začleněna i výuka ve vztahu k rizikovým jevům v on-line prostředí. Souhrnně řečeno, uživatelé sociálních sítí by se v tomto prostředí měli chovat tak, jako se chovají v prostředí světa reálného, což znamená s jistou míru obezřetnosti vůči neznámým osobám (tedy známým pouze z virtuálního prostředí). Nezbytné je mít na paměti, že pokud je uživatelem zaslán intimní, choulostivý, pornografický či jiný citlivý materiál, může být kýmkoliv zneužit, a to i v budoucnu, neboť data z tohoto prostředí pravděpodobně nikdy nezmizí a zůstanou v něm navždy uchována.

Nakonec pak byly uvedeny nejpodstatnější rysy odhalování a vyšetřování kyberkriminality na sociálních sítích, zejména ve vztahu k zajišťování digitálních důkazů. Kapitola čtvrtá obsahuje souhrn možných trestněprocesních postupů, kterých OČTŘ v rámci odhalování a vyšetřování trestné činnosti užívají. Procesní postup je přitom do značné míry komplikovaný, když se trestná činnost odehrává v kyberprostoru, který nemá hranice, a pachatel je osobou sedící za monitorem obrazovky, nacházejícím se kdekoliv na světě. Kapitola přitom přináší poznatky z praxe, a to díky Oddělení analytiky a kybernetické kriminality Městského ředitelství Policie České republiky v Plzni, jež mi umožnilo osobní konzultaci. Současně doufám, že tato kapitola napomůže k pochopení, jak OČTŘ v praxi postupují při odhalování a vyšetřování tohoto druhu trestné činnosti.

Resumé

The thesis deals with cybercrime on social networks. It discusses the risks that occur in the social networking environment, specifically cyberbullying, sexting, cybergrooming, cyberstalking and identity theft. In some cases, the manifestations of these negative phenomena may constitute the substance of one of the criminal offences enshrined in the Criminal Code of the Czech Republic.

The thesis is divided into three parts, the first part being devoted to the basic concepts that are essential to remember as they are inherently linked to this topic. At the same time, this part also explains the nature of social networks and in particular addresses the question of "who is responsible for the content disseminated on social networks".

The second part is the core of the whole thesis, as it deals with the various risk phenomena in a comprehensive way. It covers how they manifest themselves and what is at the heart of them, while providing real-life cases for a better understanding of the issue. It also discusses the various criminal offences that can be used to punish the behaviour in question. Finally, the relevant case law is presented. This section also contains the results of the research, which was carried out using a quantitative method in the form of a questionnaire survey. The aim of the research was primarily to determine the level of occurrence of these negative phenomena in society.

The third part explains the procedural approach of law enforcement agencies in detecting and investigating cybercrime on social networking sites. As this chapter was written in expert consultation with the Department of Analytics and Cybercrime of the Municipal Police Directorate of the Czech Republic in Pilsen, it allows for a better understanding of how law enforcement agencies proceed in practice. At the same time, it is necessary to point out that the investigation of this type of crime is greatly hampered by the fact that the place where the crime was committed is unrestricted cyberspace.

Cybercrime is a topical issue that needs to be addressed because, given the increasing popularity of digital technologies, crime in cyberspace will only continue to rise. This thesis has attempted to at least partially contribute to addressing this issue.

Klíčová slova

kyberkriminalita, kyberšikana, sexting, kybergrooming, kyberstalking, krádež identity

Keywords

cybercrime, cyberbullying, sexting, cybergrooming, cyberstalking, identity theft

Seznam použitých zdrojů a literatury

Knižní zdroje

ČERNÁ, Alena. *Kyberšikana: průvodce novým fenoménem*. Praha: Grada, 2013. Psyché (Grada). ISBN 978-80-210-6374-7.

GŘIVNA, Tomáš a Radim POLČÁK, ed. *Kyberkriminalita a právo*. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4.

GŘIVNA, Tomáš, Martin RICHTER a Hana ŠIMÁNOVÁ, ed. *Vliv nových technologií na trestní právo*. Praha: Auditorium, 2022. ISBN 978-80-87284-95-7.

HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. ISBN 978-80-7387-545-9.

CHMELÍK, Jan. *Mravnost, pornografie a mravnostní kriminalita*. Praha: Portál, 2003. ISBN 80-7178-739-6.

JELÍNEK, Jiří. *Trestní právo hmotné: obecná část, zvláštní část*. 7. aktualizované a doplněné vydání. Praha: Leges, 2019. Student (Leges). ISBN 978-80-7502-380-3.

KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.

PORADA, Viktor a Karel RAIS. *Právní, kriminalistické a kybernetické aspekty kybernetické kriminality a bezpečnosti: pocta Vladimíru Smejkalovi*. Brno: Akademické nakladatelství CERM, 2021. ISBN 978-80-7623-065-1.

SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7.

SZOTKOWSKI, René. *Sexting u českých dětí*. Olomouc: Univerzita Palackého v Olomouci, 2020. ISBN 978-80-244-5793-2.

ŠÁMAL, Pavel. *Trestní zákoník: komentář*. Praha: C.H. Beck, 2010. Velké komentáře. ISBN 978-80-7400-178-9. s. 3005.

ŠČERBA, Filip. *Trestní zákoník:* komentář. Praha: C.H. Beck, 2020. ISBN 978-80-7400-807-8.

ZAVRŠNIK, Aleš. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7552-758-5.

Elektronické zdroje

Akt o digitálních službách: zajištění bezpečného online prostředí odpovědného vůči uživatelům. [online]. Evropská komise.
Dostupné z: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_cs

Česká republika – vývoj v čase. Tabulka 5.2: Osoby v ČR používající sociální sítě. [online]. Český statistický úřad. Dostupné z: https://www.czso.cz/documents/10180/122362692/0620042052.pdf/76f76896-4758-480a-8856-9d6658534cba?version=1.1

Digital 2022: Another year of bumper growth. [online]. We are social. Dostupné z: https://wearesocial.com/uk/blog/2022/01/digital-2022-another-year-of-bumper-growth-2/

DUFKOVA, Anna. *Režim Safe Harbour v rámci poskytování hostingových služeb.* [online]. Epravo.cz – Váš průvodce právem – Sbírka zákonů, judikatura, právo. Dostupné z: https://www.epravo.cz/top/clanky/rezim-safe-harbour-v-ramci-poskytovani-hostingovych-sluzeb-108663.html

Evropský návrh regulace digitálních služeb – Centrum proti hybridním hrozbám. [online]. Ministerstvo vnitra České republiky. Dostupné z: https://www.mvcr.cz/chh/clanek/evropsky-navrh-regulace-digitalnich-sluzeb.aspx

KAPICIÁNOVÁ, Aneta. *Blog Seznam.cz zavře v polovině prosince svou službu Lidé.cz.* [online]. Blog Seznam.cz. Dostupné z: https://blog.seznam.cz/2020/11/seznam-cz-zavre-v-polovine-prosince-svou-sluzbu-lide-cz/

Kopecký, Kamil; Kožíšek, Martin. [online]. *Výzkum rizikového chování českých dětí v prostředí internetu 2014.* Dostupné z: https://www.e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/61-vyzkum-rizikoveho-chovani-ceskych-deti-v-prostredi-internetu-2014-prezentace/file

Kyberkriminalita. [online]. Policie České republiky. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx
Tým projektu E-bezpečí. *Anna Halman (Polsko, 2006).* [online]. E-bezpečí. Dostupné z: https://www.e-bezpeci.cz/index.php/72-kazuistiky/1426-anna-halman-polsko-2006

Kybertsalking. [online]. Internetem bezpečně. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kyberstalking/

MORAVČÍK, Ondřej. *Nové praktiky podvodníků při krádežích facebookových identit*. [online]. Policie ČR. Policie České republiky.
Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

O filmu. [online]. V síti. Dostupné z: https://vsitifilm.cz/o-filmu.html

PŘÍKAZSKÁ, Lenka, MOHELSKÝ, Michal. *Současná právní úprava data retention je dle Ústavního soudu ústavně konformní a tedy přípustná.* [online]. Epravo.cz – Váš průvodce právem – Sbírka zákonů, judikatura, právo. Dostupné z: https://www.epravo.cz/top/clanky/soucasna-pravni-uprava-data-retention-je-dle-ustavniho-soudu-ustavne-konformni-a-tedy-pripustna-110069.html?mail

Tým projektu E-bezpečí. *Co je to revenge porn.* [online]. E-bezpečí. Dostupné z: https://www.e-bezpeci.cz/index.php/o-projektu/realizani-tym/71-trivium/2341-revenge-porn

Tým projektu E-bezpečí. *Co je to stalking a cyberstalking,* [online]. E-bezpečí. Dostupné z: https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/kyberstalking/66-23

Tým projektu E-bezpečí. *Pavel Hovorka (Česká republika, 2008).* [online]. E-bezpečí. Dostupné z: https://www.e-bezpeci.cz/index.php/72-kazuistiky/1446-pavel-hovorka-ceska-republika-2008

VANC, Martina. *Trestný čin nebezpečného elektronického obťažovania*. [online]. Právne Noviny – zrozumiteľné informácie pre všetkých. Dostupné z: https://www.pravnenoviny.sk/trestny-cin-nebezpecneho-elektronickeho-obtazovania

Odborné články

DOSTÁL, Otto. *Zajišťování důkazů u počítačové kriminality – uložiště, e-maily, telefony, sociální sítě a logy* (4 díl). Trestněprávní revue, 2019, č. 6.

SKALICKÁ, Veronika. *Není odposlech jako odposlech*. Trestněprávní revue, 2022, č. 1.

TLAPÁK NAVRÁTILOVÁ, Jana, GALOVCOVÁ, Ingrid. *Uchovávání dat uložených v počítačovém systému – poskytování součinnosti, nebo nahrazování činnosti orgánů činných v trestním řízení?* Bulletin advokacie, 2019, č. 11.

Právní předpisy

Národní

Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů

Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů

Zákon č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů, ve znění pozdějších předpisů

Zákon č. 300/2005 Z. z., Trestný zákon

Zákon č. 40/2009 Sb., Trestní zákoník, ve znění pozdějších předpisů

Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů, ve znění pozdějších předpisů

Nadnárodní

Návrh Nařízení Evropského parlamentu a Rady o jednotném trhu digitálních služeb (akt o digitálních službách) a o změně směrnice 2000/31/ES

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

Směrnice Evropského parlamentu a Rady 2011/93/EU ze dne 13. 12. 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV

Úmluva Rady Evropy o ochraně dětí proti sexuálnímu vykořisťování a pohlavnímu zneužívání ze dne 25. 10. 2007 (Lanzarotská úmluva)

Úmluva Rady Evropy o počítačové kriminalitě dne 23. 11. 2001 (Budapešťská úmluva)

Judikatura

Nález Ústavního soudu České republiky sp. zn. II.ÚS 2460/19 ze dne 7. 6. 2022

Nález Ústavního soudu České republiky sp. zn. III.ÚS 3844/13 ze dne 30. 10. 2014

Rozsudek Krajského soudu v Brně ze dne 19. 11. 2019, sp. zn. 48 T 4/2019

Rozsudek Krajského soudu v Ústí nad Labem – pobočka v Liberci ze dne 26. 3. 2014, sp. zn. 31To247/2013

Rozsudek Okresního soudu v Ústí nad Labem ze dne 1.4. 2021, sp. zn. 3 T 141/2020

Rozsudek Soudního dvora Evropské unie ve věci C-324/09 ze dne 12. 7. 2011. *L'Oréal SA a další v. eBay International AG a další*.

Trestní příkaz Okresního soudu v Klatovech ze dne 28. 3. 2022, sp. zn. 1 T 62/2022

Usnesení Nejvyššího soudu sp. zn. 7 Tdo 1134/2020, ze dne 4.11. 2020

Usnesení Nejvyššího soudu sp. zn. 7 Tdo 731/2015, ze dne 30.9. 2015

Usnesení Nejvyššího soudu ze dne 28. 12. 2004, sp. zn. 7 Tdo 1077/2004

Usnesení Nejvyššího soudu ze dne 28. 4. 2021, sp. zn. 8 Tdo 271/2021

Usnesení Nejvyššího soudu ze dne 30. 4. 2010, sp. zn. 4 Tdo 414/2020

Důvodové zprávy a ostatní zdroje

Důvodová zpráva k návrhu nařízení Evropského parlamentu a Rady o jednotném trhu digitálních služeb (akt o digitálních službách) a o změně směrnice 2000/31/ES, Dostupné z:
https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52020PC0825

Sdělení č. 59/2016 Sb. m. s., Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy Rady Evropy o ochraně dětí proti sexuálnímu vykořisťování a pohlavnímu zneužívání