**VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE**

# BAKALÁŘSKÁ PRÁCE

# KYBERNETICKÁ KRIMINALITA PÁCHANÁ NA DĚTECH V JIHOČESKÉM KRAJI

**Autor práce: Martin Valert, DiS.**

**Studijní program: Bezpečnostně právní činnost**

**Forma studia: Kombinovaná**

**Vedoucí práce: JUDr. Milan Kocík, MBA**

**Katedra: Katedra právních oborů a bezpečnostních studií**

**2023**

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 6, 370 01 České Budějovice

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Martin Valert, DiS.

Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Místo studia: Příbram

**Název bakalářské práce:** Kybernetická kriminalita páchaná na dětech v Jihočeském kraji

**Název bakalářské práce v anglickém jazyce:** Cybercrime Committed against Children in the South Bohemian Region

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce (jméno a příjmení, včetně titulů): JUDr. Milan Kocík, MBA

Datum zadání bakalářské práce (měsíc, rok): listopad 2022

Cíl bakalářské práce:

1/ Hlavním cílem bakalářské práce je zjistit, jak rodiče nezletilých dětí vnímají rizika online prostředí s explicitním zaměřením na konkrétní formy kyberkriminality, tedy zhodnocení vnímání kybernetické kriminality mezi rodiči.

2/ Vedlejším cílem bakalářské práce je blíže charakterizovat a specifikovat kyberkriminalitu páchanou na nezletilých dětech.

| | | |
|---|---|---|
| Student:<br>Martin Valert, DiS. | 26.10.2022<br>*datum* | M. Valert<br>*podpis* |
| Vedoucí práce:<br>JUDr. Milan Kocík, MBA | 26. 10. 2022<br>*datum* | <br>*podpis* |

Schvaluji zadání bakalářské práce:

| | | |
|---|---|---|
| Vedoucí katedry:<br>doc. JUDr. Roman Svatoš, Ph.D. | 13.12.2022<br>*datum* | <br>*podpis* |
| Prorektor pro studium a vnitřní záležitosti:<br>doc. PhDr. Miroslav Sapík, Ph.D. | 13.12.2022<br>*datum* | <br>*podpis* |
| Rektor:<br>doc. Ing. Jiří Dušek, Ph.D. | 9.1.2023<br>*datum* | <br>*podpis* |

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z.ú. -2- ČESKÉ BUDĚJOVICE

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucí(ho) a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucímu bakalářské práce JUDr. Milanovi Kocíkovi, MBA za cenné rady, připomínky a metodické vedení práce.

# ABSTRAKT

VALERT, M. *Kybernetická kriminalita páchaná na dětech v Jihočeském kraji.* České Budějovice: Vysoká škola evropských a regionálních studií, 2023. 76 s. Vedoucí bakalářské práce: JUDr. Milan Kocík, MBA.

**Klíčová slova:** kybernetická kriminalita, kyberprostor, internet, nezletilé dítě, kybergrooming, sexting, kyberšikana, kyberstalking.

Bakalářská práce (dále jen „práce“) pojednává o kybernetické trestné činnosti vztahující se k nezletilým obětem, dětem, v Jihočeském regionu. Pro účely této práce je za nezletilé dítě považováno každé dítě, které v době spáchání protiprávního jednání nedovršilo 15. rok života. Úvod teoretické části práce má snahu formou širšího teoreticko-praxeologického a empirického vhledu včetně „de lege lata“ reflexe účinné právní úpravy primárně objasnit základní pojmy a projevy kybernetické kriminality páchané na dětech, přičemž v rámci subkapitol jsou k vybraným formám za pomocí kazuistiky demonstrovány jednotlivé případy, jež ukazují, jaké nebezpečí předmětná kriminalita skýtá. Dále je čtenář seznámen se subjekty dané kriminality. Teoretickou část práce uzavírají možnosti prevence, které představují klíč ke kontrole tohoto negativního jevu. V praktické části práce se autor formou užité kvantitativní výzkumné techniky snaží zjistit, jak rodiče nezletilých dětí vnímají nebezpečí kybernetické kriminality a jaké realizují preventivní opatření, aby ochránili své děti.

# ABSTRACT

VALERT, M. *Cybercrime Committed against Children in the South Bohemian Region: Bachelor Thesis.* České Budějovice: The College of European and Regional Studies, 2023. 76 p. Supervisor: JUDr. Milan Kocík, MBA.

**Keywords:** cybercrime, cyberspace, internet, underage child, cyber grooming, sexting, cyberbullying, cyberstalking.

The Bachelor thesis (hereinafter referred to as the "thesis") focuses on cybercrime involving underage victims, children, in the South Bohemia region. Any child who has not reached the age of 15 years at the time of the offence is considered a minor in this thesis. The Introduction of the theoretical part of the thesis strives to clarify the fundamental concepts and manifestations of cybercrimes committed against children primarily through a broader theoretical, practical and empirical approach, including a "de lege lata" reflection on the applicable legislation. Its sub-chapters discuss particular cases demonstrating the dangers of cybercrimes committed against children. Furthermore, the reader gets acquainted with the subjects of the respective crime. The theoretical part of the thesis is concluded by the prevention options, which constitute the key to controlling this adverse phenomenon. The author applies a quantitative research method to determine how parents of underage children perceive the danger of cybercrime and what preventive measures they implement to protect their children. This part constitutes the practical part of the thesis.

# Obsah

# Úvod

Dnešní společnost si ve vztahu k užívání informačních a komunikačních technologií, internetu a sociálních sítí vytvořila tzv. procesuální závislost, kdy internet a sociální sítě je tak třeba vnímat jako nástroj, který může být využit jak pozitivně, tak negativně. Takřka pro všechny věkové skupiny se stal internet a sociální sítě nedílnou součástí života. Čím dál tím více lidí upřednostňuje komunikaci na dálku, což můžou mít za vinu vnější činitelé, především vliv společnosti, dostupnost a nekontrolovanost používání. Všichni uživatelé sociálních sítí využívají svého práva vyjadřovat své názory slovem, písmem, obrazem nebo jiným způsobem, jakož i svobodně vyhledávat, přijímat a rozšiřovat ideje a informace bez ohledu na hranice státu s tím, že cenzura je nepřípustná. Což nám vlastně zaručuje Listina základních práv a svobod, jejíž nedílnou součástí je svoboda projevu a právo na informace.[1] Avšak i svoboda slova má své meze.

Je potřeba si taktéž uvědomit, že rozmach informačních a komunikačních technologií, vč. počítačových sítí a systémů se neustále zlepšuje a zrychluje, kdy každá nově nastupující technologie představuje kromě užitku taktéž potencionální hrozbu pro společnost, ze které následně plynou bezpečnostní rizika.

S ohledem na skutečnost, že řada činností je uskutečňována ve virtuálním prostředí, trestná činnost v oblasti kybernetické kriminality tak proniká do všech kriminálních oblastí. Ze statistických výstupů vyplývá, že počet deliktů v této oblasti kriminality se téměř každým rokem zvyšuje. Jen pro zajímavost, např. v roce 2021 bylo evidováno 9518 trestných činů, což ve srovnání s rokem 2020 potvrzuje nárůst o 1 445 skutků ve virtuálním prostředí.[2]

Trestné činy související s kyberkriminalitou páchané na nezletilých dětech jsou negativním jevem, se kterým se setkáváme jak v ČR, tak i v ostatních zemích světa. Jedná se o společenský a bezpečnostní problém, při kterém dochází k porušování zájmů chráněných zákonem. Kybernetická kriminalita tak představuje velmi aktuální téma a je potřeba jí věnovat větší pozornost.

Volba tématu bakalářské práce byla zvolena z toho důvodu, že její autor je příslušníkem bezpečnostního sboru Policie České republiky, kdy jeho hlavní pracovní

[1] Čl. 17 odst. 1, odst. 2, odst. 3 ústavního zák. č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů.
[2] MORAVČÍK, O. Vývoj registrované kriminality v roce 2021. *Policie České republiky* [online]. 2021 [cit. 28.10.2022]. Dostupné z WWW: <https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2021.aspx>.

náplní bylo prověřování trestné činnosti týkající se zejména kybernetické kriminality a má tedy k dané problematice poměrně blízký vztah. V práci tak bude využit praxeologický vhled a teoretické poznatky doplněny a specifikovány praktickými zkušenostmi autora práce. Autor práce se o dané téma navíc zajímá i z pohledu rodiče, neboť jako odpovědná osoba v současné době řeší možnosti prevence, kdy laickým průzkumem mezi přáteli bylo zjištěno, že si rodiče neuvědomují a nepřipouští možná rizika hrozící jejich dětem používáním internetu a technologií. Rodiče jsou tedy významným subjektem ovlivňujícím chování a jednání dítěte, kdy neznalost potenciálních rizik v online prostředí může být kriminogenním faktorem s rizikovým potenciálem zvyšovat viktimnost dítěte.

# 1 Cíl a metodika bakalářské práce

Hlavním cílem práce je zjistit, jak rodiče nezletilých dětí vnímají rizika online prostředí s explicitním zaměřením na konkrétní formy kyberkriminality, tedy zhodnocení vnímání kybernetické kriminality mezi rodiči. Vedlejším cílem práce je blíže charakterizovat a specifikovat kyberkriminalitu páchanou na nezletilých dětech.

K dosažení hlavního cíle bude využita kvantitativní strategie za využití metody dotazníkového šetření mezi rodiči nezletilých dětí navštěvující základní školy v Jihočeském regionu, kdy vhodnou kombinací otázek bude identifikováno vnímaní kybernetické kriminality mezi rodiči, dále bude zjišťována existence a realizace preventivních opatření rodičů ve vztahu k definované kriminalitě a jaké si stanovili či stanoví opatření, aby ochránili své děti. Vedlejšího cíle bude dosaženo analýzou literárních a dalších zdrojů, analýzou a vyhodnocení statistických dat a kazuistikou, kdy teoreticko-popisným způsobem bude zpracován fenomenologický popis kybernetické kriminality s důrazem na její základní projevy cílené na zvlášť zranitelné oběti.

Jedná se o praktickou práci. Bakalářská práce je rozdělena do dvou částí. První část práce má 5 kapitol a je zaměřena teoreticky. Druhá část bakalářské práce je zaměřena prakticky a bude zpracována pomocí dotazníkového šetření u rodičů nezletilých dětí navštěvující základní školy v Jihočeském regionu.

Ve druhé kapitole budou pro lepší orientaci v dané problematice vysvětleny základní pojmy. Obzvlášť jde o kriminalitu, kyberkriminalitu, kyberprostor a internet.

Ve třetí kapitole budou představeny projevy kybernetické kriminality s explicitním zaměřením na konkrétní formy, jež se bezprostředně týkají nezletilých obětí. Dále bude provedena analýza statistických dat.

Ve čtvrté kapitole bude pozornost věnována subjektům kybernetické kriminality, kdy tato kapitola bude rozdělena do dvou skupin, a to pachatel a oběť.

Pátá kapitola pojednává o prevenci kybernetické kriminality, respektive o možnostech, jak se bránit proti tomuto negativnímu jevu.

V poslední, tedy v šesté kapitole, budou na základě dotazníkového šetření podrobně znázorněny výsledky šetření pomocí grafů.

V závěru bakalářské práce budou vyhodnoceny cíle bakalářské práce s možnými doporučeními.

# 2 Výklad základních pojmů

V této kapitole budou vymezeny a vysvětleny některé základní pojmy pro lepší orientaci v dané problematice.

## 2.1 Kriminalita

Kriminalita je negativní sociální jev, fenomén, který doprovází lidstvo od samého počátku. Z tohoto lze usoudit, že ji nelze zcela odstranit a je součástí našeho společenství. K tomuto pojmu existuje řada různých definic. Trestní zákon může být klíčem, podle něhož označíme určité jednání za kriminální a představuje pak vcelku jednoduše souhrn spáchaných trestných činů. Zmíněné pojetí je zpravidla chápáno jako legální definice.[3] Avšak z hlediska sociologie sem můžeme řadit i jednání, jež z pohledu zákona nejsou protiprávní, ale společensky patologická, kdy trestné činnosti předcházejí nebo jí výrazně podmiňují (např. extremismus, alkoholismus).[4]

Synonymem kriminality je zločinnost.[5] S pojmem úzce souvisí kriminologie, která se zabývá zkoumáním kriminality (zločinností), kdy předmětem pozornosti je tzv. kriminální fenomenologie, tedy jak se zločinnost projevuje, popisuje její strukturu, statiku a dynamiku. Kriminologie se dále zabývá příčinami a podmínkami kriminality, kdy v tomto případě hovoříme o tzv. kriminální etiologii.[6] Jedná se tedy o dva základní přístupy pro poznávání kriminality, kdy až poté lze přistoupit k její kontrole, jež se uskutečňuje prostřednictvím represivních nebo preventivních strategií, kdy snahou státu a společnosti je o její udržení v přijatelných mezích.[7] Spáchanou kriminalitu můžeme obecně dělit na registrovanou (viditelnou) část, kterou policejní orgány buď zjistí z vlastní činnosti, nebo na základě oznámení osob či institucí a latentní (skrytou) část, jež tvoří rozdíl mezi skutečnou a registrovanou kriminalitou.[8]

Kriminalita je dále předmětem zkoumání kriminalistiky, kriminální politiky a trestněprávní vědy, kdy každá z nich zkoumá kriminalitu z jiného pohledu, odlišnými metodami a s jinými úkoly.[9]

---

[3] TOMÁŠEK, J. *Úvod do kriminologie: Jak studovat zločin.* Praha, 2010. s. 11.
[4] CHROMÝ, J. *Kriminalita páchaná na mládeži: aktuální jevy a nová právní úprava v České republice.* Praha, 2010. s. 17.
[5] JELÍNEK, J., et al. *Kriminologie*. Praha, 2021. s. 22.
[6] Tamtéž. s. 23.
[7] GŘIVNA, T., SCHEINOST, M., ZOUBKOVÁ, I., et al. *Kriminologie.* 5. vydání. Praha, 2019. s 25–26.
[8] Tamtéž. s. 34.
[9] ZOUBKOVÁ, I., et al. *Kriminologický slovník.* Plzeň, 2011. s. 81.

*Obrázek 1 Vývoj registrované a objasněné kriminality v letech 2008–2021*[10]


Výše uvedený graf znázorňuje vývoj registrované a objasněné kriminality v období od roku 2008 do roku 2021. Z grafu je patrné, že registrovaná kriminalita klesá. Přestože kriminalita poklesla, tak byl zaznamenán nárůst škod způsobených trestnými činy, kdy se jedná o souhrnnou částku 21,3 mld. Kč.[11] Dle úsudku policie je kriminalita z dlouhodobého pohledu na historicky nejnižší úrovni z následujících důvodů:

- Snížení mobility osob a omezení veřejných či veřejnosti přístupných aktivit v souvislosti s opatřením proti pandemii (Covid-19).
- Optimalizace statistického vykazování následkem čehož došlo k pohybu v jednotlivých subkategoriích.
- V souvislosti s novelizací trestního zákoníku byla změněna hranice výše škody při kvalifikaci trestného činu na 10 000 Kč.
- Důraz na viditelný výkon služby, zacílení na využívání dostupných nástrojů pro odhalování kriminality a zefektivnění práce policistů a kriminalistů při objasňování trestné činnosti.[12]

[10] MORAVČÍK, O. Vývoj registrované kriminality v roce 2021. *Policie České republiky* [online]. 2021 [cit. 28.10.2022]. Dostupné z WWW: <https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2021.aspx>.
[11] Tamtéž.
[12] Tamtéž.

## 2.2 Kybernetická kriminalita

Pojem kybernetická kriminalita je pojem kriminologický nikoli právní. Trestní právo tento pojem neužívá a neuvádí kybernetické trestné činy jako ucelenou skupinu, najdeme je pod více hlavami trestního zákoníku, jako např. trestné činy proti životu, proti zdraví, proti majetku a další. Náhled na obsah a rozsah pojmu „kybernetická kriminalita není jednotný. Mnohdy je kybernetická kriminalita označována jako počítačová kriminalita či internetové kriminalita.

Budeme-li vycházet z legální definice kriminality, kybernetickou kriminalitu lze jednoduše charakterizovat jako protiprávní jednání, ke kterému dochází v kyberprostoru.[13] Jedná se tedy o souhrn spáchaných trestných činů v určitém prostředí. V současné době je převážná část kybernetické kriminality páchána prostřednictvím internetu.[14]

Jirkovský ve svém díle[15] ke kybernetické kriminalitě uvádí, že se jedná o jednání, které je v rozporu s morálními pravidly společnosti nebo jsou jím porušovány právní normy. Přičemž tato činnost je namířena proti počítačům a jejich dílčím prvkům, nebo v ní vystupuje počítač pouze jako nástroj využitý pro spáchání trestného činu, případně počítačová síť a k ní připojené prostředky jsou oblastí, v němž se takové jednání uskutečňuje.

Jan Kolouch ve své knize CyberCrime[16] uvádí, že pod označením kybernetická kriminalita bývají v odborných publikacích nejčastěji označena taková kriminální jednání, při kterých jsou prostředky informačních a komunikačních technologií užity jako nástroj pro spáchání trestného činu, nebo cílem útoku pachatele, přičemž tento útok je trestným činem.

Globalizace kyberprostoru, nízké náklady, nízké povědomí obětí a rostoucí závislost společnosti na internetu jsou významnými faktory velkého rozmachu ať už ve formách jednotlivých aktivit nebo v počtu jednání, který v posledních letech kybernetická kriminalita zažívá.[17]

[13] SMEJKAL, V. *Kybernetická kriminalita.* 3. vydání. Plzeň, 2022. s. 31.
[14] GŘIVNA, T., SCHEINOST, M., ZOUBKOVÁ, I., et al. *Kriminologie.* 5. vydání. Praha, 2019. s 390.
[15] JIRKOVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha, 2007. s. 19.
[16] KOLOUCH, J. *CyberCrime*. Praha, 2016. s. 35.
[17] JELÍNEK, J., et al. *Kriminologie*. Praha, 2021. s. 480–481.

### 2.2.1 Dělení kybernetické kriminality

S ohledem na skutečnost, že není jednotná definice kybernetické kriminality, tak není ani jednotné dělení této specifické společensky škodlivé činnosti. Nabízí se tak prostor pro několik třídění podle jiných aspektů.

Dle názoru autora bakalářské práce je nejpřehlednější třídění podle Statutu Komise expertů na kybernetickou kriminalitu z roku 2000, která klasifikuje předmětnou kriminalitu:

- Dle postavení počítače při páchání trestné činnosti:
  - terč útoku,
  - nástroj útoku.
- Podle typu činu:
  - protiprávní jednání nová,
  - protiprávní jednání tradiční.[18]

Počítačovou kriminalitu lze dělit taktéž do pěti základních kategorií:

- Neoprávněné zásahy do vstupních dat.
- Neoprávněné změny v uložených datech.
- Neoprávněné pokyny k počítačovým operacím.
- Neoprávněné pronikání do počítačů, počítačového systému a jeho databází.
- Napadení cizího počítače, programového vybavení a souborů a dat v databázích.[19]

Úmluva o kyberkriminalitě dělí kybernetické trestné činy na:

- Trestné činy proti utajování, integritě a dostupnosti počítačových dat a systémů.
- Trestné činy související s počítači.
- Trestné činy související s obsahem.
- Trestné činy související s porušováním autorských práv a práv souvisejících.[20]

[18] MATĚJKA, M. Počítačová kriminalita. In *Statut Komise expertů Rady Evropy pro zločin v kyberprostoru (Commitee of Experts on Crime in Cyberspace).* Rada Evropy, 2000.
[19] STRAUS, J., et al. *Kriminalistická metodika.* Plzeň, 2006. s. 272–274.
[20] KOLOUCH, J. *CyberCrime*. Praha, 2016. s. 38.

Jan Kolouch dále srovnáním několika definic třídí trestné činy související s kybernetickou kriminalitu do třech skupin:

- *„trestné činy, jejichž individuálním objektem charakterizujícím skutkovou podstatu je přímo ochrana počítačového systému, jeho vybavení a součástí před specifickými druhy útoku, resp. oprávněné zájmy osob na nerušené užívání těchto technických prostředků,*
- *trestné činy, kde je způsob spáchání prostřednictvím informační a komunikační techniky jedním ze znaků skutkové podstaty,*
- *ostatní v úvahu připadající trestné činy, které nespadají do první ani druhé kategorie, avšak které mohou být v konkrétním případě též spáchány prostřednictvím informačních technologií a které odpovídají výše uvedené definici, neboť v rámci jejich odhalování a objasňování se mohou uplatnit obdobné postupy jako při vyšetřování trestných činů z 1. a 2. kategorie (např. obdobně zaměřené znalecké posudky)*.“[21]

### 2.2.2 Trestně právní ochrana

Trestně právní ochrana v dané problematice spočívá především v tom, že zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů (dále jen trestní zákoník) jakožto základní právní norma trestního práva hmotného označuje jednání, kterými dojde k porušení či ohrožení zájmů, hodnot a vztahů chráněných zákonem za trestné činy a umožňuje za ně uložit trestní sankce. Tato právní norma obsahuje mimo jiné z pohledu kybernetické trestné činnosti taktéž speciální skutkové podstaty, které jsou zaměřeny právě na dotčenou kriminalitu.

„Kybernetické trestné činy“, respektive protiprávní jednání související s předmětnou kriminalitou, jež jsou uvedeny ve zvláštní části trestního zákoníku, lze třídit obdobně jako kybernetickou kriminalitu, tedy na trestné činy, které jsou terčem kybernetického útoku, při jejichž páchání představují prostředky informačních a komunikačních technologií předmět ochrany a na trestné činy při jejichž páchání jsou prostředky informačních a komunikačních technologií užity ke spáchání trestného činu. Existují desítky trestných činů, které jsou v kontextu s kybernetickou kriminalitou. V důsledku nestejnorodosti jednotlivých typů kybernetických útoků se trestněprávní regulace rozpadá do mnoha skutkových podstat trestných činů z různých hlav trestního

[21] KOLOUCH, J. *CyberCrime*. Praha, 2016. s. 37.

zákoníku. Jedná se zejména o trestné činy proti životu a zdraví (hlava I), trestné činy proti svobodě a právům na ochranu osobnosti, soukromí a listovního tajemství (hlava II), trestné činy proti lidské důstojnosti v sexuální oblasti (hlava III), trestné činy proti rodině a dětem (hlava IV), trestné činy proti majetku (hlava V) a trestné činy proti pořádku ve věcech veřejných (hlava X).

Nejedná se ovšem jen o trestní zákoník, ale i o jiné právní normy, které se dotýkají kybernetické kriminality, a to jak v ČR, tak v zahraničí.

Právní normy České republiky související s kybernetickou trestnou činností:

- Ústavní zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpisů
- Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů
- Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky
- Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim
- Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád)
- Zákon č. 218/2003 Sb., zákon o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů (zákon o soudnictví ve věcech mládeže)
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
- Zákon č. 273/2008 Sb., o Policii České republiky
- Zákon č. 106/1999 Sb., o svobodném přístupu k informacím
- Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon)
- Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)
- Zákon č. 89/2012 Sb., občanský zákoník
- Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů[22]

[22] Uvedeno příkladem, nejedná se o celkový výčet dokumentů, jež souvisejí s kybernetickou kriminalitou.

Nejvýznamnějším mezinárodním právním dokumentem je Úmluva Rady Evropy č. 185 o kyberkriminalitě, která v České republice vstoupila v platnost dne 01.12.2013, a její dodatkový protokol Rady Evropy č. 189. Výše uvedená úmluva sjednotila národní právní úpravu v oblasti kybernetické kriminality, stanovuje povinnost realizovat do právních řádů takové nástroje, pomocí kterých bude umožněn a zajištěn postih stanovených kybernetických trestných činů. Dodatek dále stanovuje oblast trestných činů, které nejsou v úmluvě o kyberkriminalitě obsaženy.[23]

Dále existuje řada dalších dokumentů sloužících ke sladění právních úprav při potírání kybernetické trestné činnosti. Jedná se zejména o Směrnice Evropského parlamentu a Rady.

### 2.2.3 Kriminalistické stopy u kybernetické kriminality

Kriminalistické stopy lze vyjádřit jako *„změnu v materiálním prostředí nebo ve vědomí člověka, která souvisí příčinně, místně nebo časově s kriminalisticky relevantní událostí, je zjistitelná, zajistitelná a využitelná současnými metodami, prostředky a postupy.“*[24] V případě kybernetické kriminality se bude jednat zejména o digitální (počítačové) stopy a paměťové stopy, přičemž každá z těchto stop má svůj význam. Obecně význam kriminalistických stop spočívá v udávání skutečného obrazu na místě činu, kdy jsou jedním ze stěžejních prostředků pro zjištění skutkového stavu věci. Z pohledu trestního práva procesního je zásada zjišťování skutkového stavu bez důvodných pochybností jednou ze základních zásad trestního řízení[25].

**Digitální stopy**

Casey ve svém díle[26] definuje digitální stopu jako: *„jakákoli data uložená nebo přenesená za použití počítače, která podporují nebo prolamují teorii o tom, jak se čin stal, či která pomáhají vysvětlit záměry pachatele, nebo jeho alibi.“*

Ačkoliv se virtuální prostředí zdá být anonymní, tak je nutno ovšem podoktnout, že prakticky každý uživatel internetu, počítačového systému či jiné informační technologie zanechává o své činnosti vědomě nebo nevědomky nějaké informace, přičemž soubor těchto vytvořených, upravených, uložených, odeslaných nebo přijatých

[23] KOLOUCH, J. *CyberCrime*. Praha, 2016. s. 332 a násl.
[24] PORADA, V., STRAUS, J. Kriminalistické stopy. Teorie, metodologie, praxe. In PORADA, V., et al. *Kriminalistika.* Brno: CERM, 2001. 746 s. ISBN 80-7204-194-0.
[25] Upravuje § 2 odst. 5 zák. č. 141/1961 Sb., o trestním řízení soudním (trestní řád).
[26] CASEY, E. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet.* 2. edition. London, 2004. s. 12 a násl.

dat či informací tvoří digitální stopu. Ve vztahu k možnosti ovlivnit uživatelem vznik digitálních stop, lze tyto stopy rozdělit na ovlivnitelné a neovlivnitelné.[27] Vznikají tedy působením člověka. Jinými slovy se aktivita uživatele odráží do materiálního prostředí konkrétní technologie, a to oběma směry.[28] Bude se jednat zejména o různé soubory, emailovou komunikaci, vyhledávané soubory, cookies, příspěvky na sociálních sítí, IP adresu, poskytovatele připojení apod. Přestože vnímáme data jako nehmotný statek, tak zajištěné digitální stopy jsou hmotného, materiálního charakteru, neboť při zajištění se ukládají na paměťové médium. Digitální stopy jsou velice objemné, vysoce latentní, nestálé, rozsáhlé a dynamické, respektive proměnlivé v čase i místě spáchání činu.[29] Přičemž k zajištění a následného zkoumání těchto stop je třeba kvalifikovaných odborníků na vysoké úrovni. Digitální stopa má největší význam především pro vyšetřování trestné činnosti. Digitální stopa je zařazena pod ustanovení § 112 odst. 1, odst. 2 tr. řádu, jedná se tedy o věcný či listinný důkaz.[30] Typickým věcným důkazem u kybernetické kriminality budou např. paměťová uložiště nebo počítačové systémy. V případě listinného důkazu se bude jednat o listinou dokumentaci obsahující data či informace.

**Paměťové stopy**

Paměťové stopy vznikají ve vědomí člověka prostřednictvím receptorů lidských smyslů. Nejčastěji se využívají smysly jako zrak a sluch, tedy skutečnost, co konkrétní osoba viděla a slyšela, méně pak ostatní smysly jako hmat, chuť, čich. Paměťové stopy mají materiální charakter, kdy dochází ke změně biochemického složení jednotlivých mozkových buněk, nicméně tyto změny nejsou doposud přesně vyhodnotitelné a z tohoto důvodu jsou paměťové stopy považovány za výlučné a je tak s nimi pracováno.[31]

Přesto paměťové stopy u kybernetické kriminality mají taktéž význam stejně tak jako digitální stopa. Jedná se o stopu, která obsahuje informace. Je potřeba si taktéž uvědomit, že ne vždy se digitální stopu podaří na místě činu zajistit. Proto jsou paměťové stopy nepostradatelné a nenahraditelné. Z výše uvedeného je patrné, že paměťová stopa vzniká v mozku člověka. Reprodukce těchto stop závisí na mnoha faktorech, jako je například samotná paměť, respektive schopnost vnímání a následná fixace. Dále je to

[27] KOLOUCH, J. *CyberCrime*. Praha, 2016. s. 134–135.
[28] RAK, R., PORADA, V. Digitální stopy v kriminalistice a forenzních vědách. *Soudní inženýrství* [online]. 2005, roč. 17, č. 1 [cit. 02.11.2022]. ISSN 1411-443X. Dostupné z WWW: <http://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf>.
[29] PORADA, V., STRAUS, J. *Kriminalistické stopy. Teorie, metodologie, praxe.* Plzeň, 2012. s. 306 a násl.
[30] § 112 odst. 1, odst. 2 zák. č. 141/1961 Sb., o trestním řízení soudním (trestní řád).
[31] PORADA, V., et al. *Kriminalistika (teorie, metody, metodologie).* Plzeň, 2014. s. 169–170.

vůle, ochota poskytnout orgánům činným v trestním řízení nějaké informace. Využity jsou zejména u obětí kybernetických útoků. Své uplatnění mají tedy především z pohledu kriminalistické taktiky, neboť jsou východiskem pro výslech.[32] Oběť tedy může popsat, co se vlastně stalo, poskytnout cenné informace o pachateli, způsobené škodě, za jakých okolností a jakým způsobem, odkud a kde došlo „k útoku" a celkově o situaci, jež mají význam a využití pro objasňování kriminalisticky relevantních událostí.

## 2.3 Kyberprostor

Klíčovým prvkem kybernetické kriminality je shora zmiňovaný kyberprostor, jehož základní vlastností je globální pokrytí. Obdobně jako u kybernetické kriminality ani pro kyberprostor neexistuje jednotná definice. *„Lze říci, že kyberprostor je virtuální realitou, nemající konec ani začátek. Tato virtuální realita je však závislá na materiální podstatě, tedy technologiích nacházejících se ve světě reálném."*[33]

*„Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts ... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non space of the mind, clusters and constellations of data. Like city lights, receding ,..."*[34]

V zákoně o kybernetické bezpečnosti se kybernetickým prostorem rozumí digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.[35]

V kyberprostoru se odráží všechny znaky současné společnosti, nicméně život v této realitě si vytváří vlastní pravidla, která vybočují z přirozeného řádu, ve kterém lidstvo žilo po staletí. Pro přežití lidské společnosti v kyberprostoru je nutné přizpůsobit stará pravidla chování, vytvořit nové zvyklosti a naučit se existovat v tomto pátém rozměru života. Přináší to ovšem modifikovaná a nová nebezpečí a chování, se kterými je nutné se vypořádat, akceptovat nebo najít způsoby, jak jim vzdorovat.[36]

---

[32] VICHLENDA, M. *Kriminalistika* [online]. Karviná, 2011 [cit. 03.11.2022]. Dostupné z WWW: <http://www.sosoom-zlin.cz/media/skripta/kriminalistika.pdf>.
[33] KOLOUCH, J. *CyberCrime*. Praha, 2016. s. 43.
[34] GIBSON, W. *Neuromancer.* New york, 1984. s. 37.
[35] § 2, písm. a) zák. č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).
[36] JIRKOVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha, 2007. s. 16.

## 2.4 Internet

*„Internet jako takový je bezpečný, nebezpeční jsou na něm jen lidé.“*[37]

Net, síť, web to jsou ekvivalenty pro internet. Jedná se o největší celosvětovou propojenou síť, ve které mezi sebou počítače, laptopy, mobilní telefony a další podobné prostředky komunikují pomocí protokolů. *„Jedná se o standardy či konvence, které definují způsob komunikace mezi dvěma body v síti. Tento nejznámější se plným názvem píše Transmission Control Protocol/Internet Protocol neboli primární přenosový protokol/protokol síťové vrstvy.“*[38] Každý z těchto vyjmenovaných prostředků připojených k internetu má v rámci protokolů svoji IP adresu. Prostřednictvím internetu je pak umožněno komunikovat na dálku, vyměňovat si a sdílet informace či data. Internet nám bez nadsázky propojuje celý svět.

Internet lze taktéž definovat jako soubor komunikačních (počítačových) sítí, jež jsou recipročně propojeny na základě multiraterálních a bilaterálních smluv a vytvářejí tak celosvětovou síť. V souvislosti s touto množinou mohou uživatelé využívat jak přenosových kapacit sítí, tak zdrojů, které jsou do sítí připojeny (data, služby, servery, počítače).[39]

Světové počátky Internetu se datují do 50. let 20. století. Jedná se o nezbytnou materiální podstatu kyberprostoru.[40] Hmotnou podstatou Internetu, je páteřní síť, která vede signál vzduchem, kabely, či jinými přenosovými médii.[41] Internet nemá právní subjektivitu. Podle nového občanského zákoníku bychom mohli Internet nazvat věcí dokonce veřejným statkem.[42]

Geneze Internetu by se dala přirovnat k vynálezu telefonu, automobilu či letadla. Internet nám pomáhá zkracovat vzdálenost mezi lidmi, státy, světadíly a usnadňuje tak komunikaci. Internet se ovšem stal mnohem vlivnějším činitelem v našem životě než výše uvedené vynálezy. Používání celosvětové sítě vedlo, vede a určitě i nadále povede k velkým změnám. Internet mění styl zábavy, komunikace, chování, styl práce, mění místa provádění práce, mění naše životy.[43]

---

[37] KOŽÍŠEK, M., PÍSECKÝ, V. *Bezpečně na internetu: průvodce chováním ve světě online.* Praha, 2016. s. 139.
[38] SMEJKAL, V. *Kybernetická kriminalita.* 3. vydání. Plzeň, 2022. s. 77.
[39] HINDLS. R., HOLMAN, R., HRONOVÁ, S., et al. *Ekonomický slovník.* Praha, 2003. s. 164.
[40] KOLOUCH, J. *CyberCrime*. Praha, 2016. s. 42.
[41] Tamtéž. s. 43.
[42] SMEJKAL, V. *Kybernetická kriminalita.* 3. vydání. Plzeň, 2022. s. 79.
[43] HULANOVÁ, L. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha, 2012. s. 16.

# 3 Projevy kybernetické kriminality

Kybernetická kriminalita páchaná na nezletilých dětech souvisí zejména s trestnou činností mravnostního charakteru. Nejčastěji se jedná o šíření nebo držení dětské pornografie, navazování kontaktu s dětmi s cílem od nich vylákat erotické materiály a v menší míře také sexuální nátlak. Komunikace mezi pachateli a dětmi se odehrává obvykle v uzavřených diskusních fórech, na šifrovaných mobilních platformách nebo na zahraničních komunikačních službách, což velmi ztěžuje samotné odhalení takového jednání a také přesné zadokumentování důkazních materiálů.[44] Sexuálně motivované trestné činy jsou tedy nejčastějším projevem kriminality páchané na dětech v kyberprostoru. Řadíme sem zejména níže uvedené ustanovení trestního zákoníku:

- § 186 sexuální nátlak
- § 191 šíření pornografie
- § 192 výroba a jiné nakládání s dětskou pornografií
- § 193 zneužití dítěte k výrobě pornografie
- § 193a účast na pornografickém představení
- § 193b navazování nedovolených kontaktů s dítětem
- § 202 svádění k pohlavnímu styku

Nejedná se o všem jen o trestné činy sexuálně motivované. Lze se setkat taktéž s trestnými činy proti životu a zdraví, svobodě a právům na ochranu osobnosti, soukromí a listovního tajemství, rodině a dětem, pořádku ve věcech veřejných apod. Mezi tyto činy je možné zařadit například:

- § 144 účast na sebevraždě
- § 175 vydírání
- § 184 pomluva
- § 201 ohrožování výchovy dítěte
- § 353 nebezpečné vyhrožování
- § 354 nebezpečné pronásledování

[44] MORAVČÍK, O. Vývoj registrované kriminality v roce 2021. *Policie České republiky* [online]. 2021 [cit. 28.10.2022]. Dostupné z WWW: <https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2021.aspx>.

## 3.1 Vybrané projevy kybernetické kriminality

Kybergrooming, sexting, kyberšikana a kyberstalking jsou dalšími častými projevy předmětné kriminality páchané na nezletilých dětech. Jedná se o kybernetické útoky, které se odehrávají primárně v prostředí sociálních sítí.[45] Uvedené projevy nejsou přímo skutkovými podstatami trestných činů, nicméně tato jednání zahrnují právě řadu protiprávních jednání postižitelné trestně-právními normami.

### 3.1.1 Kybergrooming

Pojem kybergrooming, též child grooming či online grooming, označuje chování predátorů (kybergroomerů), jež prostřednictvím internetu má v oběti vyvolat falešnou důvěru a přimět ji k osobnímu setkání v reálném světě. Sexuální zneužití oběti, fyzické násilí na oběti, zneužití oběti pro dětskou prostituci, výroba dětské pornografie apod. můžou být výsledkem této osobní schůzky. Jedná se vlastně o druh psychické manipulace, ve které dospělý uživatel často pod falešnou identitou komunikuje s dítětem. Při komunikaci používá řadu strategií, jako je např. zrcadlení, phishing, profilování oběti, vábení a uplácení, strategie snižování zábran dětí a mládeže zaváděním sexuálního obsahu do konverzace, izolační metody, strategie manipulace dětí prostřednictvím fotografií opačného pohlaví, webcam trolling apod.[46]

Kohout ve své příručce pro děti od 6 do 12 let[47] ke kybergroomingu uvádí, že pod záminkou osobní schůzky si útočník vymýšlí a lže oběti. Na schůzce jí chce ublížit nebo ji chce sexuálně zneužít. Většinou komunikuje prostřednictvím sociální sítě Facebook, kdy se snaží různými způsoby získat důvěru oběti.

Chování kybergroomera:

- *„chválí, lichotí a předstírá zájem,*
- *chce, aby se mu oběť se vším svěřovala,*
- *pomlouvá její rodiče, kamarády atd. (aby ji „měl“ jen pro sebe),*
- *snaží se ji podplatit: novým mobilem, penězi, dobitím kreditu atd.,*
- *chce ji mít „v hrsti“ tím, že získá její nahé fotky, videa apod.,*
- *udělá cokoliv, aby přišla na osobní schůzku,*

[45] KOLOUCH, J. *CyberCrime*. Praha, 2016. s. 309.
[46] *Co je kybergrooming?* [online]. 14.01.2019 [cit. 12.11.2022]. Dostupné z WWW: <https://www.e-bezpeci.cz/index.php/71-trivium/1421-co-je-kybergrooming>.
[47] KOHOUT, R. *Internetem Bezpečně.* Karlovy Vary, 2017. s. 24.

- *může ji různě vydírat, aby ji donutil přijít (např. chce její fotky a videa poslat rodičům),*
- *na osobní schůzce ji ublíží, zneužije ji nebo znásilní,*
- *dál ji může vydírat, aby to nikomu neříkala.“*[48]

**Kazuistika**

Poměrně výstižně ukazuje zneužívání dětí na internetu úspěšný český dokumentární film Víta Klusáka a Barbory Chalupové „V síti“[49]. Film pojednává o tzv. kybergroomingu, kdy uživatelé sociálních sítí a komunikačních prostředků prostřednictvím internetu oslovují a navazují kontakty se svými obětmi s prakticky jediným cílem, vylákání sexuálních fotografií a videí potažmo sexuálního násilí. V tomto případě byly obětmi tři vybrané dospělé herečky, které se ve filmu svým vzhledem, vystupováním a vybraným prostředím záměrně vydávaly za dívky ve věku kolem 12 let, jež si po založení účtu na komunikačním portálu psaly a dále telefonovaly s „predátory“. Pravidla pro herečky byla jasná, žádné podněcování a provokování potencionálních útočníku k sexuálnímu svádění apod. Bylo až k nevíře, v jak krátkém časovém odstupu od založení profilu útočníci oslovili svoji oběť. Po navázání důvěrného vztahu pachatel vyzval svoji oběť mimo jiné k osobnímu setkání, jehož cílem bylo zejména sexuální zneužití. Štáb z vlastní iniciativy za účelem zjištění, z jakého důvodu zasílal porno dívkám, konfrontoval pachatele s přezdívkou „Ústečan“, jenž se bránil tím, že je to de facto chyba rodičů a jejich výchovy. Smyslem dokumentu bylo ukázat společnosti nebezpečí pro děti, které představuje používání sociálních sítí a obecně internetu. Jedná se o reálný a smutný odraz toho, co se děje našim dětem. Což dokazuje fakt, že se predátoři mohli dopustit hned několika trestných činů, jako je například vydírání, šíření pornografie, sexuální nátlak, navazování nedovolených kontaktů s dítětem. Navíc došlo k útoku na děti, jež se z důvodu bezbrannosti, zvědavosti či neznalosti mohou stát snadno obětí kybernetické kriminality.

Jako značně znepokojující se jeví skutečnost, že během 10 dnů, kdy probíhal experiment, oslovilo dívky 2458 mužů.[50]

[48] KOHOUT, R. *Internetem Bezpečně.* Karlovy Vary, 2017. s. 24.
[49] *V síti* [dokument]. Režie Barbora CHALUPOVÁ, Vít KLUSÁK. 2020.
[50] HLOUŠKOVÁ, L. Je mi dvanáct aneb 2458 sexuálních predátorů nachytaných V síti. *Borgis a.s.* [online]. 16.01.2020 [cit. 08.11.2022]. Dostupné z: <https://www.novinky.cz/kultura/filmy-serialy/clanek/je-mi-dvanact-aneb-2458-sexualnich-predatoru-nachytanych-v-siti-40310059>.

*Obrázek 2 Herečky vydávající se za nezletilé dívky*[51]

Případ osmačtyřicetiletého Martina K. alias Ústečana, jenž si jako jediný psal se všemi třemi protagonistkami, kdy po nich žádal zaslání jejich intimních fotografií, a sám jim je také zasílal, dále si s jednou dívkou domluvil schůzku, na kterou nakonec nedorazil, byl vyšetřován policií do října roku 2020 s tím, že v prosinci 2020 byla podaná obžaloba. Obžalovaný se hájil tím, že věděl, že herečkám není 12 let a komunikoval s nimi v soukromí, přičemž „komunikace mu vyprázdnila hlavu“. Obžalovaný v řízení před soudem přiznal, že přechovává stovky jiných snímků obnažených dívek v dětském věku. Ze znaleckého posudku vyplynulo, že Martin K. nemá sexuální poruchu, nicméně trpí poruchou osobnosti ve smyslu disociality a velké nezdrženlivosti, svoji vinu bagatelizuje a přehazuje ji na ostatní. Okresní soud v Ústí nad Labem jej začátkem dubna 2021 nakonec jako prvního predátora z dokumentu odsoudil za trestný čin ohrožování výchovy dítěte, zneužití dítěte k výrobě pornografie, navazování nedovolených kontaktů s dítětem a šíření pornografie a výroby a jiné nakládání s dětskou pornografií, vše spáchané ve stádiu pokusu, nepodmíněně na dva roky ve věznici s ostrahou.[52]

[51] STEJSKAL, T. V síti se lapili směšní i odporní predátoři. Klusákův film ukazuje bezohlednost ve společnosti. In *Hospodářské noviny* [online]. Economia 28.02.2020 [cit. 08.11.2022]. Dostupné z WWW: <https://archiv.hn.cz/c1-66727610-v-siti-se-lapili-smesni-i-odporni-predatori>.

[52] KUBIŠTOVÁ, D. První nepodmíněný trest pro predátora z filmu V síti. ‚Ústečan‘ má jít na dva roky za mříže. In *iROZHLAS* [online]. Český rozhlas 01.04.2021 [cit. 09.11.2022]. Dostupné z WWW: <https://www.irozhlas.cz/zpravy-domov/v-siti-ustecan-martin-ustecak-usti-nad-labem-soud-rozsudek_2104011325_ako>.

### 3.1.2 Sexting

Další nebezpečnou formou kybernetické kriminality spojovanou s dětmi je sexting. Uvedený termín je složenina dvou slov, „sex“ a „textování“. Spočívá tedy v zasílání textových zpráv, fotografií či videí se sexuálním obsahem.[53] Komunikace a šíření obsahu probíhá pomocí technologií, jako je např. chytrý telefon, tablet, počítač apod. Sexting je zdrojem mnoha trestných činů, např. výroba a jiné nakládání s dětskou pornografií.[54]

Sexting je považován za jedno z nejrizikovějších chování, jehož důsledky mohou být tragické. Nátlak, který je v některých případech vyvíjen na oběť, může končit dehonestací, sebepoškozováním nebo sebevraždou.[55]

Důvody, proč je sexting rizikový:

- Po odeslání zpráv s citlivým materiálem ztrácíme nad nimi kontrolu. Tento obsah se může kdykoli objevit na internetu či jiných místech. Přestože vás příjemce může ubezpečit, že se tento materiál nikde neobjeví, tak se jim nedá nikdy stoprocentně věřit.
- Zaslaný materiál může být kdykoli zneužit. Sexting je velice často spojen s vydíráním. S ohledem na možnou dehonestaci oběti v případě jeho zveřejnění nebo pouhou hrozbou, že tak bude učiněno, je důvodem, proč je nátlaku ze strany útočníka velice těžké odolat.
- O intimní tématiku s nezletilými je na internetu obrovský zájem a je velice často vyhledávána. Sexting s osobami mladšími patnácti let je považován za obzvláště závažný a je často posuzován jako ohrožování mravní výchovy, šíření dětské pornografie apod.
- V případě, že zaslaný materiál unikne do veřejného prostoru internetu, musíme počítat s tím, že životnost dat je obrovská a prakticky nejdou smazat. Materiály se často šíří virálně, kdy během několika málo hodin mohou být na desítkách stránek po celém světě.[56]

Důvodů, proč děti provozují sexting, je celá řada. Sexting je vnímán jako součást romantických vztahů, ovšem někdy se intimní materiály stávají nástroji pomsty. Může

[53] MULLER, M. *Jak ochránit děti před pornografií na internetu.* Praha, 2014. s. 107.
[54] § 192 odst. 1 zák. č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.
[55] KOŽÍŠEK, M., PÍSECKÝ, V. *Bezpečně na internetu: průvodce chováním ve světě online.* Praha, 2016. s. 83.
[56] Tamtéž.

být produktem konzumní společnosti a nástrojem sebeprezentace. Dále umožňuje potlačit nudu. Sexting může vzniknout také jako produkt sociálního tlaku.[57]

**Kazuistika**

Nezletilá dívka navštěvující devátou třídu Základní školy v Měříně pořídila svojí vlastní intimní fotografii pro svého kamaráda, kterého pravděpodobně chtěla získat. Chlapec ale snímek rozeslal dalším přátelům, kteří začali snímek rozesílat dál. Přes 30 dětí se zapojilo do šíření fotografie. Tato se dostala až k učitelům, kteří dívku identifikovali podle řetízku na krku a událost ohlásili policistům s podezřením ze šíření dětské pornografie. Právní norma považuje posílání pornografických snímků osob mladších 18 let za šíření dětské pornografie, za které hrozí až tři roky odnětí svobody, přičemž u mladistvého se trest obvykle krátí na polovinu. Pokud se ovšem ukáže, že mladiství aktéři se v minulosti ničeho závažného nedopustili, může soud upustit od potrestání. Osoby mladší patnácti let, jež rozesílaly předmětnou fotografii, nelze trestně stíhat. Hlavní aktérce trest od soudu nehrozí. Nicméně pouhé policejní vyšetřování přinese dívce i její rodině těžké chvíle. Případ byl nakonec ukončen v říjnu 2009. Mladiství žáci, kteří se zapojili do šíření snímku, byli potrestáni tresty společensky prospěšných činností.[58]

Hope Witsell, 13letá žákyně 7. třídy floridské základní školy, spáchala z důvodu sextingu sebevraždu. Dívka chtěla upoutat pozornost chlapce, Alexe Eargooda, který se jí líbil a zaslala mu mobilním telefonem svoji nahou fotografii. Této si ale v autobuse všimla spolužačka chlapce, která si od něj zapůjčila mobilní telefon. Intimní fotografii pak dívka přeposlala dalším spolužákům a spolužačkám ze školy, kdy během několika hodin začala fotografie kolovat po několika okolních základních a středních školách. Od této chvíle začala probíhat ve škole šikana. Spolužáci se Hope smáli, uráželi jí a říkali o ní, že je coura a děvka. Když se vedení školy o sextingu Hope a o její nahé fotografii šířící se školou dozvědělo, vyloučilo Hope na týden ze školy. Pod tlakem neustálého posměchu a urážení se Hope nakonec uvedeného dne oběsila ve svém pokoji.[59]

[57] KOPECKÝ, K., KOŽÍŠEK, M. Fenomén sexting v teorii a praxi (díl 1). In *e-bezpečí.cz* [online]. 01.03.2015 [cit. 12.11.2022]. Dostupné z WWW: <https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/sexting/994-fenomensexting1>.
[58] *Kazuistika* [online]. [cit. 12.11.2022]. Dostupné z WWW: <https://www.sexting.cz>.
[59] Tamtéž.

### 3.1.3 Kyberšikana

Kyberšikanu lze charakterizovat jako úmyslné, nepřátelské chování, které se opakuje, jehož cílem je ublížit oběti za použití informačních a komunikačních technologií.[60] Email, SMS zprávy a obtěžující volání na mobilní telefon, sociální sítě, komunikační programy (Messenger, WhatsApp, Skype apod.), webové stránky, diskusní fóra a webkamery jsou prostředky online prostředí, kde se můžeme setkat s virtuální šikanou.[61] Kyberšikana má řadu projevů. Projevuje se např. tím, když pachatel posílá oběti urážlivé a zastrašující zprávy nebo pomluvy. Dále natáčí videa nebo pořizuje fotografie a následně je zveřejní na internetu bez souhlasu aktérů. Agresor může taktéž vytvořit webové stránky, kde oběť uráží, pomlouvá nebo ponižuje. Dalším standardním projevem je provokování a napadání uživatelů v diskusních fórech, odhaluje cizí tajemství a vydírá je pomocí moderních technologií. Řadíme sem dále obtěžování a pronásledování, které se děje v kyberprostoru. A v neposlední řadě se taktéž jedná o krádež identity.[62] Aby se jednalo o kyberšikanu, musí tam být obsažen prvek dlouhodobosti.

Znaky kyberšikany:

- útočník se domnívá, že vystupuje anonymně,
- šikanovat může i slabší silnějšího, neboť na internetu nerozhoduje síla,
- oběť neví, kdy a kde přijde útok,
- publikum pomáhá agresorovi v šíření kyberšikany,
- není jednoduché rozeznat dopady kyberšikany na oběť,
- virtuální šikana může být jako nepovedený vtip způsobena i neúmyslně,
- mnohdy je spojena s tradiční šikanou.[63]

Pojem kyberšikana úzce souvisí s klasickou šikanou. Vzájemně se od sebe odlišují tím, že si útočníci mohou zachovat určitý odstup od svých obětí, neboť při páchání šikany jsou agresoři a oběti v přímém kontaktu. Odstup tedy dává pachatelům jistou dávku anonymity a pocit bezpečí, kdy se domnívají, že na ně nikdo nepřijde. Současně je pro ně jednodušší „zapomenout“ na své chování a snižovat pocit viny, neboť nevidí způsobené újmy. Tímto oběť může ztratit důvěru k ostatním lidem, když nezná pravou identitu

[60] ŠMAHAJ, J. *Kyberšikana jako společenský problém.* Olomouc, 2014. s. 11.
[61] ŠVESTKOVÁ, R., SOLDÁN, L., ŘEHKA, M. *Kyberšikana.* České Budějovice, 2019. s. 18–22.
[62] KOHOUT, R. *Internetem Bezpečně.* Karlovy Vary, 2017. s. 18.
[63] Tamtéž. s. 19.

pachatele.[64] Oběť šikany se mnohdy stává obětí virtuální šikany a naopak.[65] Kyberšikana je na rozdíl od klasické šikany četnější, stupňující se a oběť nemá možnost jí předvídat.[66]

**Kazuistika**

Katka, žákyně deváté třídy základní školy, měla mít na vysvědčení čtyřku z fyziky. Dívka využila ještě jednu šanci, kterou ji dal učitel, a opravila si známku na trojku. Protože se spolužačka Adéla nemohla s touto skutečností smířit, začala o Katce šířit pomluvy s tím, že si známku vyplakala. Dokonce ji na sociální síti Facebook pomluvila s dalšími děvčaty, že „v kabinetě dala učitelovi", proto dostala na vysvědčení lepší známku. Adéla spolu se třemi spolužačkami dále natočila zesměšňující video, ve kterém se vyjadřovala o Katce jako o psovi a materiál vyvěsila na Facebook. Pomluvy šířila jak ve třídě, tak mino ni, kdy postupně zmanipulovala většinu spolužáků a poštvala je proti dívce. Posměšky, vulgární nadávky a nevhodné poznámky byly na denním pořádku. Katka si nejdřív myslela, že ji Adéla přestane ubližovat, případně se jí omluví, a vše přestane. Tak se ale nestalo, proto se oběť spolu se svoji kamarádkou obrátila s problémem ubližování, posmívání, pomlouvání na Facebooku na ředitele školy a požádala jej o pomoc a řešení situace. Provedeným šetřením se tvrzení obou dívek potvrdilo, navíc bylo zjištěno, že šikanování v této třídě má hlubší kořeny a více obětí. Řešením kyberšikany se podařilo situaci zklidnit a aktéři šikanování byli adekvátně potrestáni. Ačkoliv byl učitel fyziky na sociální síti objektem lží, byl nařčen z pohlavního styku s žákyní, zaujmul proti nim shovívavý postoj a odmítl podat trestní oznámení na Policii České republiky.[67]

Zdokumentovaný příběh ukazuje, jak je internet, potažmo sociální sítě nebezpečný. Ačkoliv je patrné, že anonymita útočníka nehrála v tomto případě až takovou roli a nebyl zde „splněn" znak utajení, přesto se jednalo o ukázkový projev kyberšikany, kdy útočnice jednala opakovaně s úmyslem poškodit oběť. Výše popsaná kazuistika mimo jiné dokazuje, že kyberšikana je spjatá s tradiční šikanou a vzájemně se doprovázejí. Klíčovou roli pro odvrácení fatálních následků sehrála samotná reflexe oběti a její kamarádky, jež se obrátily na zodpovědnou osobu ve škole, kdy následně přišla pomoc ze strany pedagogů.

[64] ROGERS, V. *Kyberšikana: pracovní materiály pro učitele a žáky i studenty.* Praha, 2011. s. 32.
[65] Tamtéž. s. 13.
[66] KOŽÍŠEK, M., PÍSECKÝ, V. *Bezpečně na internetu: průvodce chováním ve světě online.* Praha, 2016. s. 62.
[67] ROGERS, V. *Kyberšikana: pracovní materiály pro učitele a žáky i studenty.* Praha, 2011. s. 22.

### 3.1.4 Kyberstalking

Kyberstalking, další rizikový jev kyberkriminality ohrožující bezpečnost dětí, vychází z tradičního stalkingu s tím rozdílem, že k němu dochází v kyberprostoru. Hlavní roli sehrávají opět moderní technologie, internet, sociální sítě apod. Kyberstalking se svým jednáním podobá kyberšikaně.

*„Díky internetu (a občas i lidské důvěřivosti) se stalker ani nemusí moc namáhat, aby získal dostatek informací o nás a naší každodenní rutině. Ochotně je celému světu servírujeme přes příspěvky a fotky na svých sociálních sítích. I s roztomilými a o to cennějšími detaily.“*[68]

Termín kyberstalking označuje jednání, které spočívá v opakovaném kontaktování oběti např. telefonáty, VoIP, messengery, zasíláním SMS zpráv, e-mailů aj. Útoky agresorů se zpravidla stupňují a většinou vyvolá u oběti obavy o svoje soukromí, zdraví či život. Pro útočníky je typická jejich systematičnost a vytrvalost, přičemž není neobvyklé, když kyberstalker ke kontaktování obětí využívá vytvořenou celou řadu falešných identit. Útočník může dát najevo i svoji sílu a moc např. tím, že zveřejní informace ze života oběti, jež může získat z různých online zdrojů. Kyberstalking spáchaný na dítěti je možné za splnění konkrétních podmínek subsumovat pod ustanovení § 354 odst. 2, písm. a) zák. č. 40/2009 Sb., trestního zákoníku, ve znění pozdějších předpisů, kdy se jedná se o trestný čin nebezpečné pronásledování.[69]

Kohout ve své příručce Internetem Bezpečně[70] ke kyberstalkingu uvádí, že tento nastává, když útočník neustále oběti píše zprávy nebo ji kontaktuje zasíláním SMS zpráv, na zdi na Facebooku, na chatu, pomocí messengerů apod., případně ji neustále sleduje pomocí moderních technologií. Pachatel chce tedy oběti znepříjemnit život, kdy nevhodně komentuje její příspěvky na sociální síti atd. Neustále sleduje, s kým se stýká a s kým si píše. Dokonce může obtěžovat zprávami i její kamarádky.

Je nutné si uvědomit, že kyberstalking je vytrvalé a nepředvídatelné pronásledování ve virtuálním světě, kdy se nejedná tedy o jednorázovou činnost, nýbrž probíhá systematicky a trvá i několik let. Odtud pramení i následky, kterými oběť trpí. U oběti je výrazně narušen její dosavadní životní styl a velmi často přeruší veškeré své dosavadní společenské aktivity. U oběti se dále objevují poruchy spánku, může se zhoršit

[68] *Co je kyberstalking* [online]. [cit. 15.11.2022]. Dostupné z WWW: <https://vyuka.o2chytraskola.cz/clanek/26/kyberstalking/>.
[69] KOLOUCH, J. *CyberCrime*. Praha, 2016. s. 318.
[70] KOHOUT, R. *Internetem Bezpečně.* Karlovy Vary, 2017. s. 26–27.

její duševní stav spočívající ve stresové poruše, depresích či úzkostí. Astma, lupénka, zvýšený krevní tlak, nevolnost, únava, ale i naopak nadměrná bdělost, to jsou další zdravotní problémy spojené s následky kyberstalkingu. V nejhorším případě se objevují sebevražedné myšlenky či pokusy o sebevraždu.[71]

**Kazuistika**

Lenku, 14 let, vždy každý chválil, jak se umí výborně obléknout a že má na to talent. Kamarádka ji přemluvila, aby si spolu založily módní blog, kde budou sdílet svoje denní outfity. Zprvu sdílely jen ty nejpovedenější fotografie, nicméně lidé, kteří to četli, byli z blogu nadšení a žádali je i o další fotografie z toho, co dívky dělají celý den. A tak si dívky říkaly, vlastně proč ne, přece trocha umění a legrace nemůže přinést nic špatného a začaly tedy popisovat více věcí ze svých životů. Lenky kamarádce to brzy zakázali rodiče s tím, že se na internetu nemusí tak odhalovat. Lence ale přišlo, že ztráta trošky soukromí přece stojí za ty nadšené komentáře. Standa, kluk z vedlejší školy, se brzy stal nejvěrnějším fanouškem blogu. Komentoval a „lajkoval" snad všechno. Zezačátku to zejména Lenka nebrala jako něco špatného, několikrát si s ním i psala. Také jí přišlo milé, jak byl z blogu a hlavně z ní unešený. *„Brzy ale začalo být Standy všude až moc."* Postupně ho Lenka i čím dál tím častěji „náhodně" potkávala v knihovně nebo ve své oblíbené kavárně, taktéž si párkrát všimla, jak odpoledne chodí kolem její školy. Lenka nechtěla být na chlapce nepříjemná, zprvu s ním vždycky prohodila několik slov, postupem času jí to ale přišlo víc a víc otravné, až začínala mít z chlapce strach, jak byl téměř všude, kam se hnula. Lenka si později uvědomila, že toho o sobě na blogu říká až moc, proto zjistil všechny její zvyky a oblíbená místa, kdy mu tak dala přesný návod, kde a kdy ji může zastihnout.[72]

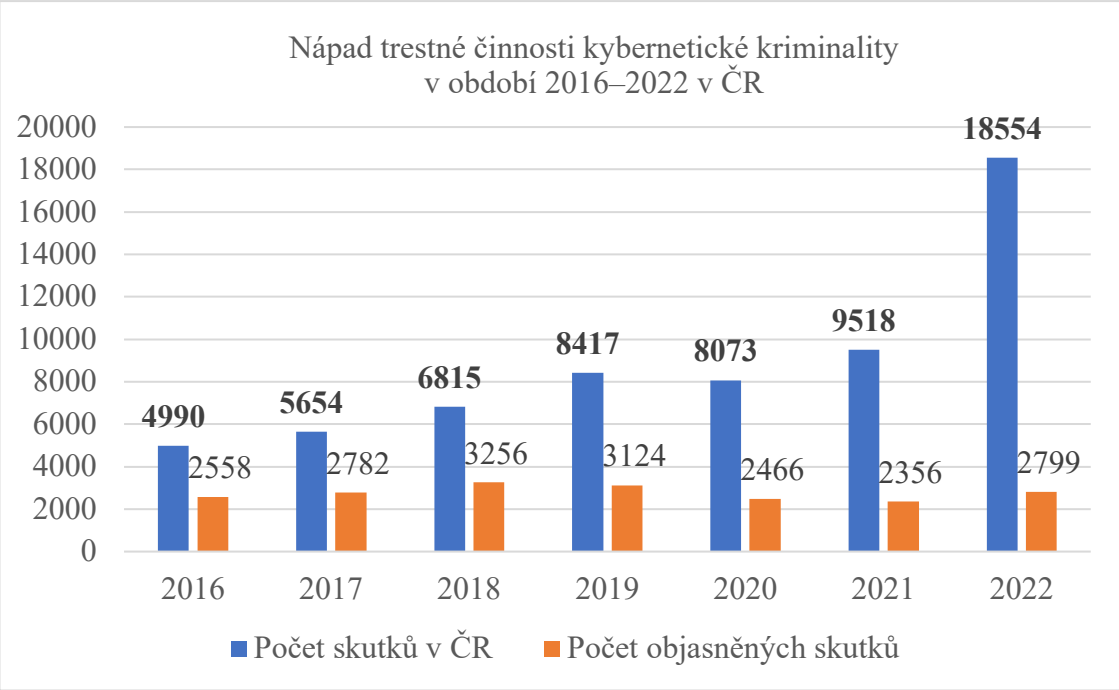
Tohle je ilustrativní případ, který vychází ze situace, se kterou se operátor setkal na lince důvěry[73], jež provozuje nestátní nezisková organizace Dětské krizové centrum specializovaná na odbornou pomoc týraným, sexuálně zneužívaným či zanedbávaným dětem.[74]

---

[71] HULANOVÁ, L. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha, 2012. s. 81–82.
[72] *Rizika kyberprostoru: průvodce pro děti, rodiče a učitele* [online]. Praha: Dětské krizové centrum, 2017 [cit. 15.11.2022]. Dostupné z WWW: <https://www.ditekrize.cz/app/uploads/2019/10/brozura_prezentace.pdf>.
[73] Tamtéž.
[74] Dětské krizové centrum. O nás. *Ditekrize.cz* [online]. [cit. 15.11.2022]. Dostupné z WWW: <https://www.ditekrize.cz/o-detskem-krizovem-centru/>.

## 3.2 Vývoj kybernetické kriminality v ČR

*Graf 1 Nápad trestné činnosti kybernetické kriminality v období 2016–2022 v ČR*[75]

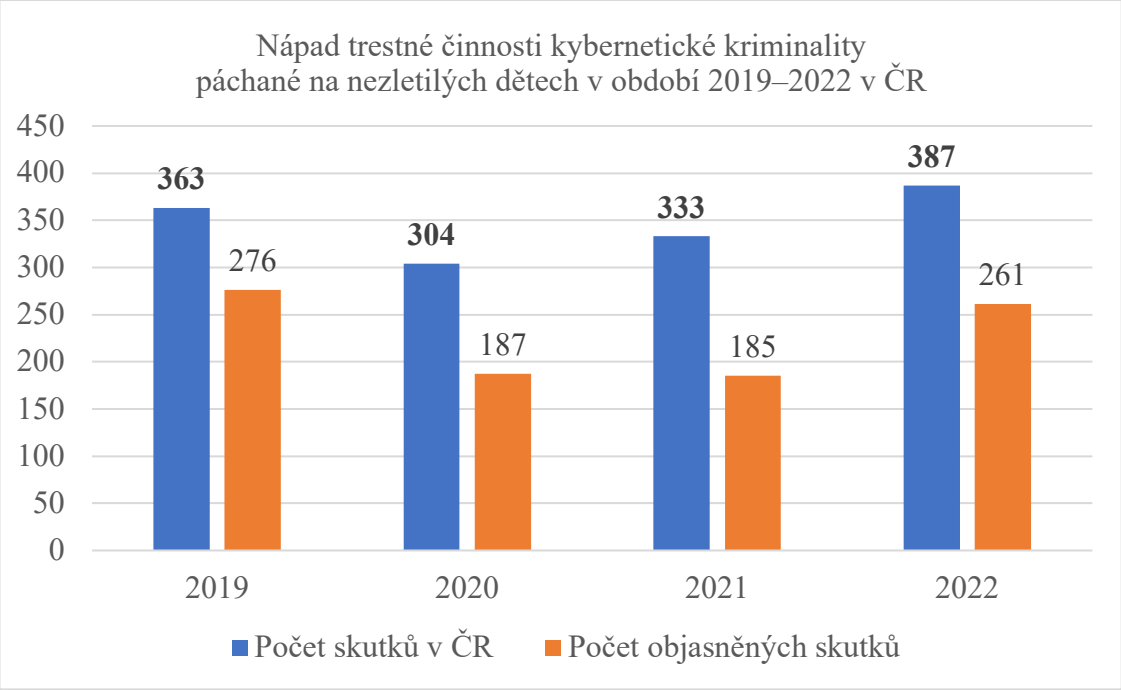



Uvedený graf č. 1 znázorňuje vývoj kybernetické kriminality v období od roku 2016 do roku 2022. Statistická data o kriminalitě zpracovává a vydává Úřad služby kriminální policie a vyšetřování, odbor věcných gescí a statistik. Jedná se o interní statistiku Policie České republiky. Za rok 2022 bylo celkově registrováno 18 554 skutků, které spadají do kategorie kybernetické kriminality a ostatní kriminality páchané v kyberprostoru, kdy z tohoto bylo objasněno 2799 skutků. Meziročně se tak jedná o 94,9% nárůst (9 036 skutků). Opětovně nejrozšířenější oblastí trestných činů v rámci ostatní kriminality páchané v kyberprostoru je majetková trestná činnost, nejčastěji různá jednání kvalifikovaná jako podvod (§ 209 trestního zákoníku). Z hospodářských trestných činů byl zaznamenán velký počet skutků v oblasti neoprávněného držení platebního prostředku. Dále byly ve větším množství páchány trestné činy pomocí internetu v oblasti poškozování a zneužití záznamu na nosiči informací (§ 230, 231 a 232 trestního zákoníku), v oblasti mravnostních trestných činů a v oblasti porušování autorského práva, práv souvisejících s právem autorským a práv k databázi (§ 270 trestního zákoníku).[76]

[75] Interní zdroj PČR.
[76] Tamtéž.

Jestliže pro současný stav kriminality platí, že registrovaná kriminalita klesá[77], tak uvedené se nedá vztahovat ke kybernetické kriminalitě, kdy z grafu je patrné, že vyjma roku 2020, byla předmětná kriminalita na vzestupu. Ve vztahu k vývoji kyberkriminality byly dále pro zajímavost doplněny data týkající se objasněnosti.

*Graf 2 Nápad trestné činnosti kybernetické kriminality páchané na nezletilých dětech v období 2019–2022 v ČR*[78]

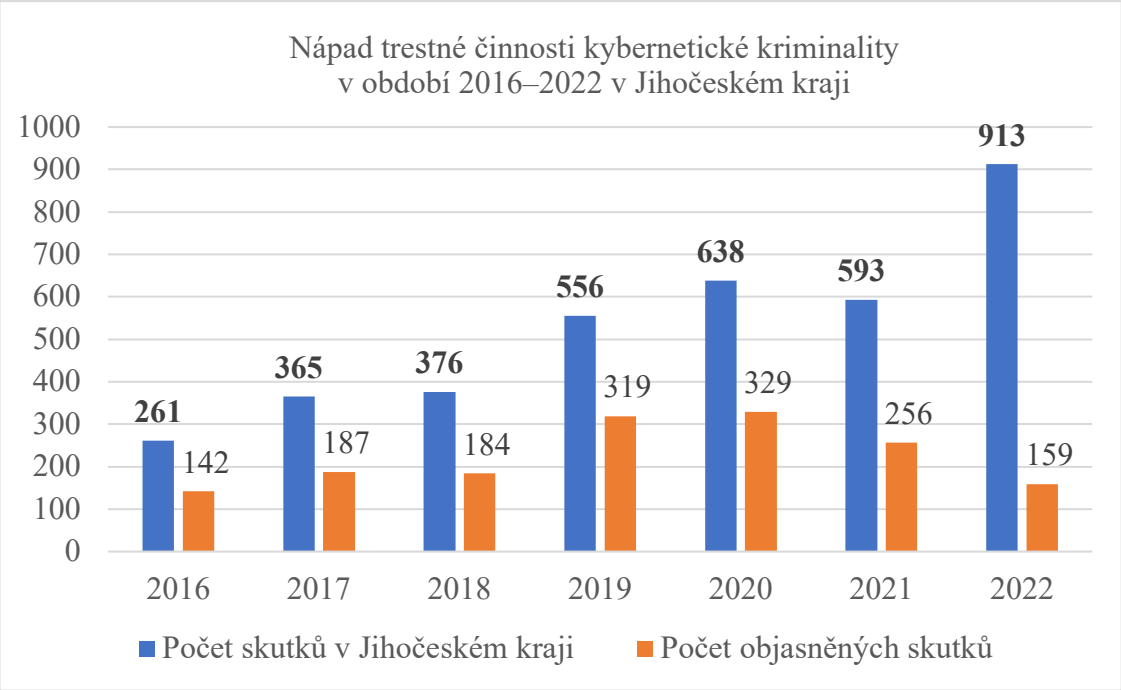



Graf č. 2 zobrazuje nápad trestné činnosti kybernetické kriminality páchané na nezletilých dětech v období od roku 2019 do roku 2022 v České republice. K tomuto je potřeba dodat, že Policie ČR statisticky eviduje objekt napadení, který koresponduje se znakem trestného činu a zachycuje i některé objektivní stránky. Policie České republiky statisticky nikdy neevidovala a neeviduje oběti trestné činnosti. Objekt napadení nelze zaměňovat s obětí trestného činu. Je-li objektem napadení osoba, je vždy i obětí, ale každá oběť trestného činu nemusí být objektem napadení. Statistická data ohledně počtů objektu napadení z předchozích let nejsou k dispozici.[79] Z tohoto grafu je patrné, že v uvedeném období se počty skutků pohybují řádově kolem tří stovek, jsou de facto konstantní, respektive data nevybočují v takové míře jako data týkající se všech registrovaných skutků.

[77] Srov. podkapitola 2.1 kriminalita.
[78] Interní zdroj PČR.
[79] Tamtéž.

## 3.3 Vývoj kybernetické kriminality v Jihočeském kraji

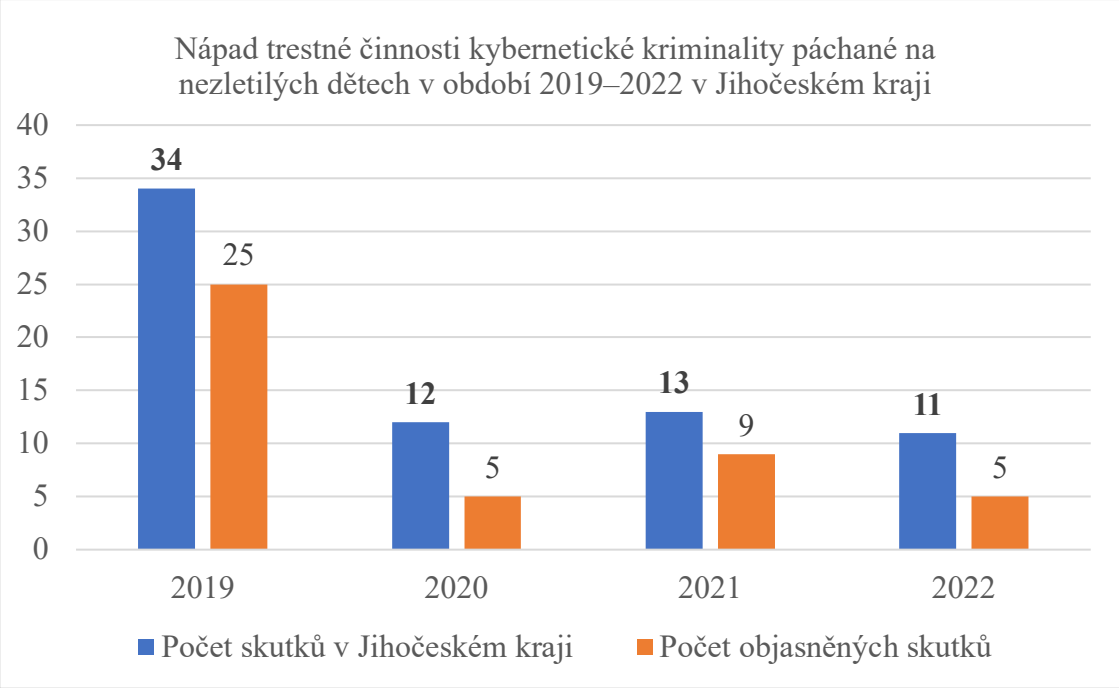
*Graf 3 Nápad trestné činnosti kybernetické kriminality v období 2016–2022 v Jihočeském kraji*[80]




Graf č. 3 vyjadřuje, jaký byl nápad trestné činnosti kybernetické kriminality v období od roku 2016 do roku 2022 v Jihočeském kraji. Celkově bylo za rok 2022 registrováno 913 skutků spadajících do kategorie kybernetické kriminality a ostatní kriminality páchané v kyberprostoru, kdy z tohoto bylo objasněno 159 skutků. Meziročně se jedná o 54% nárůst (320 skutků). Stejně tak jako u nápadu trestné činnosti kybernetické kriminality ve sledovaném období v ČR je i v Jihočeském kraji nejrozšířenější oblastí trestných činů v rámci ostatní kriminality páchané v kyberprostoru majetková trestná činnost, nejčastěji různá jednání kvalifikovaná jako podvod (§ 209 trestního zákoníku). Taktéž z hospodářských trestných činů byl zaznamenán velký počet skutků v oblasti neoprávněného držení platebního prostředku. Opět byly ve větší míře páchány trestné činy pomocí internetu v oblasti poškozování a zneužití záznamu na nosiči informací (§ 230, 231 a 232 trestního zákoníku), v oblasti mravnostních trestných činů a v oblasti porušování autorského práva, práv souvisejících s právem autorským a práv k databázi (§ 270 trestního zákoníku). Struktura trestných činů ve vztahu ke kybernetické kriminalitě spáchaných v Jihočeském kraji de facto kopíruje jednání v celé České republice.[81]

[80] Interní zdroj PČR.
[81] Tamtéž.

*Graf 4 Nápad trestné činnosti kybernetické kriminality páchané na nezletilých dětech v období 2019–2022 v Jihočeském kraji*[82]




Graf č. 4 ukazuje počet trestných činů spáchaných na nezletilých dětech v souvislosti s kybernetickou kriminalitou v období od roku do 2019 do roku 2022 v Jihočeském kraji.

Níže uvedené tabulky vyjadřují konkrétní skutkové podstaty trestných činů.

*Tabulka 1 Trestné činy spáchané v roce 2019*[83]

| Trestné činy spáchané v roce 2019 | Počet | Objasněno |
|---|---|---|
| vydírání (§ 175) | 3 | 2 |
| šíření pornografie (§ 191)) | 7 | 6 |
| ostatní mravnostní trestné činy (§ 190, 192-194) - *platná do 2020* | 20 | 14 |
| ohrožování výchovy dítěte (§ 201, 202) - *platná do 2020* | 4 | 3 |

*Tabulka 2 Trestné činy spáchané v roce 2020*[84]

| Trestné činy spáchané v roce 2020 | Počet | Objasněno |
|---|---|---|
| vydírání (§ 175) | 1 | 0 |
| šíření pornografie (§ 191) | 2 | 1 |
| ostatní mravnostní trestné činy (§ 190, 192-194) - *platná do 2020* | 3 | 2 |
| ohrožování výchovy dítěte (§ 201, 202) - *platná do 2020* | 6 | 2 |

[82] Interní zdroj PČR.
[83] Tamtéž.
[84] Tamtéž.

*Tabulka 3 Trestné činy spáchané v roce 2021*[85]

| Trestné činy spáchané v roce 2021 | Počet | Objasněno |
|---|---|---|
| sexuální nátlak (§ 186) | 2 | 2 |
| šíření pornografie (§ 191) | 3 | 3 |
| dětská pornografie a zneužití dítěte k ní (§ 192, 193) - *od 2021* | 2 | 2 |
| navazování nedovolených kontaktů s dítětem (§ 193b) - *od 2021* | 2 | 2 |
| ohrožování výchovy dítěte (§ 201) - *platná od 2021* | 4 | 0 |

*Tabulka 4 Trestné činy spáchané v roce 2022*[86]

| Trestné činy spáchané v roce 2022 | Počet | Objasněno |
|---|---|---|
| nebezpečné vyhrožování (§ 353) | 1 | 0 |
| vydírání (§ 175) | 3 | 1 |
| sexuální nátlak (§ 186) | 1 | 0 |
| dětská pornografie a zneužití dítěte k ní (§ 192, 193) - *od 2021* | 1 | 0 |
| navazování nedovolených kontaktů s dítětem (§ 193b) - *od 2021* | 1 | 1 |
| ohrožování výchovy dítěte (§ 201) - *platná od 2021* | 4 | 3 |

[85] Interní zdroj PČR.
[86] Tamtéž.

# 4 Pachatelé a oběti

V této kapitole budou popsány subjekty kybernetické kriminality, konkrétně její pachatelé a nezletilé oběti.

## 4.1 Pachatelé kybernetické kriminality

Pachatel trestného činu je předmětem zkoumání několika vědních oborů, především trestního práva hmotného a procesního, kriminalistiky a samozřejmě také kriminologie.

Podle platných právních norem trestního práva hmotného může být pachatelem fyzická osoba, starší 15 let, příčetná, která svým jednáním naplnila znaky skutkové podstaty trestného činu, respektive přípravy nebo pokusu trestného činu. Pokud trestný čin spáchalo více osob, jde pak o spolupachatele nebo účastníka. Trestní zákoník dále stanovuje, že *„pachatelem trestného činu je i ten, kdo k provedení činu užil jiné osoby, která není trestně odpovědná pro nedostatek věku, nepříčetnost, omyl, anebo proto, že jednala v nutné obraně, krajní nouzi či za jiné okolnosti vylučující protiprávnost, anebo sama nejednala nebo nejednala zaviněně. Pachatelem trestného činu je i ten, kdo k provedení činu užil takové osoby, která nejednala ve zvláštním úmyslu či z pohnutky předpokládané zákonem; v těchto případech není vyloučena trestní odpovědnost takové osoby za jiný trestný čin, který tímto jednáním spáchala.“*[87] Pachatelem dále může být i právnická osoba, kdy dne 1. ledna 2012 nabyl účinnosti zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, jenž upravuje jejich jednání, které jim lze z hlediska jejich trestní odpovědnosti za trestné činy přičítat ve smyslu ustanovení § 8 citovaného zákona, čili byl spáchán v zájmu právnické osoby nebo v rámci její činnosti, kdy tak jednaly taxativně vyjmenované subjekty, jako jsou např. statutární orgán, osoba ve vedoucím postavení v rámci právnické osoby. Z hlediska trestního práva procesního trestní řád používá pro pachatele podle jeho procesního postavení termíny jako je podezřelý, obviněný, obžalovaný, odsouzený.

Z pohledu kriminologie není podstatné, zda byly splněny podmínky pachatele trestného činu, tedy věk a příčetnost, respektive dovršení 15 roku života a způsobilost být pachatelem podle trestního práva. Tato věda se taktéž zabývá osobami, které si již trest za spáchaný protiprávní čin odpykaly, a osobami, jež se vyznačují sociálně patologickým

[87] § 22 odst. 2 zák. č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

chováním.[88] Oproti trestnímu právu kriminologie vnímá osobu pachatele tedy poněkud trochu šířeji. Kriminologie vytváří svoje koncepty o pachatelích, o jejich osobnosti, kdy tato věda tedy určité poznatky o pachatelích protiprávního jednání zobecňuje a vychází z teoreticky poskytovaného psychologického a sociálního prostředí, respektive zázemí. Je dáno, že osobnost člověka s konkrétními biologickými a psychologickými zvláštnostmi se vyvíjí v souvislosti se sociálními vztahy a společenským prostředím. Pro pochopení kriminální osobnosti je potřeba vnímat a brát v potaz všechny tyto uvedené sociální, psychologické a biologické vrstvy.[89] Zkoumat, kdo je osobou pachatele, jak ho poznat, které motivy určují jeho jednání, jak se s ním přiměřeně a účelně zachází, jak se dle potřeby „potírá" a jak jej přivést zpět do společnosti, platí od prvopočátku za jeden z nejpřednějších úkolů kriminologie.[90]

Co se týče charakteristiky osoby pachatele kybernetické kriminality záleží vždy na druhu či typu protiprávního jednání, kterého se dopouští. Typický pachatel kybernetické kriminality tedy neexistuje. Předpokladem je jen prostá uživatelská znalost kyberprostoru. Vysoká míra anonymity internetu navíc vyvolává u útočníků pocit neodhalitelnosti. Nízký stupeň vnímání průběhu proměny hypotetické oběti v oběť reálnou a způsobených škod znamená menší sociální tlak odrazující od trestné činnosti. Pachatele lze dělit na amatéry a profesionály. Neboť některé typy útoků vyžadují hlubší znalosti práce s moderními komunikačními zařízeními. Naopak tzv. tradiční kriminalita běžně zvláštní uživatelské znalosti nevyžaduje.[91] Vyjma kriminality zaměřující se na obsah, kam se řadí i šíření dětské pornografie, jsou pachatelé kybernetické kriminality spíše nadprůměrně inteligentní. Vlastnosti běžného pachatele kyberkriminality do značné míry ovlivňuje skutečnost, že v kyberprostoru se jen velmi málo vyskytují trestné činy proti životu a zdraví. Proto bude v online prostředí jen málo násilnických typů osoby pachatele. To ale neplatí např. v případě kyberšikany, kyberstalkingu, sadistických pedofilů apod. Kybernetických útoků se čím dál tím víc dopouští i osoby zcela vyspělé, které tak činí zejména z důvodu ukájení svých jiných potřeb, např. u tzv. sexuálních predátorů, s poměrně malým rizikem odhalení. Z genderového pohledu je kyberkriminalita vnímána výrazně jako mužská záležitost.[92] Jednu z kategorií pachatelů

[88] ZOUBKOVÁ, I., et al. *Kriminologický slovník.* Plzeň, 2011. s. 130.
[89] VICHLENDA, M., KRČEK, I. *Kriminologie* [online]. Karviná, 2011 [cit. 23.11.2022]. Dostupné z WWW: <https://www.sosoom-zlin.cz/media/skripta/kriminologie.pdf>.
[90] KAISER, G. *Kriminologie.* Praha, 1994. s. 183–184.
[91] GŘIVNA, T., SCHEINOST, M., ZOUBKOVÁ, I., et al. *Kriminologie.* 5. vydání. Praha, 2019. s 392.
[92] JELÍNEK, J., et al. *Kriminologie*. Praha, 2021. s. 484–485.

představuje organizovaný zločin, jehož příslušníci využívají počítače zejména k výrobě a distribuci pornografie všeho druhu.[93]

Pachatel je pro oběť obvykle zcela neznámá osoba, nicméně mohou to být i lidé z jejího nejbližšího okolí. Zde je těžké posoudit, který z těchto dvou případů představuje pro oběť větší trauma. Zda ten, kdy je pachatel pro oběť zcela neznámý a neví, kdo je na druhé straně a co může od pachatele čekat, nebo ten, kdy oběť pachatele zná a svým jednáním ji ničí a způsobuje ji bolest. Důležitou roli při získávání svých obětí sehrává internet, který pro pachatele přináší především dostupnost obětí bez velkých finančních nákladů a prostřednictvím anonymity získávání obětí z různých koutů jeho země či celého světa. Pachatel využívá slabin oběti, snaží se nad obětí získat co největší kontrolu, aby si získal její důvěru a vzbudil v ní pocit strachu. Na internetu může využívat sexuální či uživatelské nezkušenosti oběti, může využít její zvědavosti, osamělosti či nedostatku finanční hotovosti. Pomocí vyhrožování a vydírání prezentuje oběti své požadavky. Oběť je zastrašována různými výhružkami a je na ni vyvíjen velký nátlak psychického charakteru. Někdy se pachatel snaží v obětech vyvolat pocit, že jsou to oni, kdo způsobil vzniklou situaci. Manipuluje jimi a výhružkami je zastrašuje a odrazuje od toho, aby se někomu svěřily se svým utrpením.[94]

Vědomí, že pachatelům kybernetické kriminality nehrozí žádné fyzické nebezpečí, přispívá k páchání trestných činů v kyberprostoru. Sexuálně motivovaní útočníci, kteří zneužívají děti, se hodně rychle naučili komunikovat s dětmi a jak je k sobě nalákat. Možnost kontaktovat dítě přes počítač z vlastního domova jim dává mnohem větší pocit bezpečí. Nemusejí tak číhat v parku, u nákupního střediska nebo u školy a mohou to provádět v kteroukoli denní či noční hodinu. Stačí jim pouze přístup na internet nebo nějakou online službu, aby mohli děti kontaktovat.[95] Internetové prostředí dále umožňuje pachatelům zvýšenou anonymitu, kdy pachatel se vydává jménem jiné osoby nebo si vytvoří vlastní identitu, případně ji úplně zastírá, což znesnadňuje odhalování a vyšetřování. Trestná činnost je většinou páchána z předem stanoveného místa, v úvodní fázi jednání pachatele se prakticky nejedná o žádnou nahodilou situaci,

[93] VÁLKOVÁ, H., KUCHTA, J., HULMÁKOVÁ, J., et al. *Základy kriminologie a trestní politiky.* 3. vydání. Praha, 2019. s. 551.
[94] HULANOVÁ, L. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha, 2012. s. 141–142.
[95] MULLER, M. Jak ochránit děti před pornografií na internetu. In HARMER, J., SMITH, J. B. *The Sex Industrial Complex.* Praha, 2014. s. 50.

kdy pachatel si předem určí místo, ze kterého dojde k „útoku“, nedostane se tak přímo do osobního kontaktu s obětí. Tyto faktory mohou usnadňovat páchání trestné činnosti.

Mezi specifické kriminogenní faktory v oblasti kybernetické kriminality patří:

- vysoká míra latence,
- pocit převahy nad ostatními subjekty,
- pocit beztrestnosti a neodhalitelnosti,
- vysoká dostupnost počítačových zařízení,
- možnost distančního přístupu prostřednictvím počítačových sítí,
- anonymita uživatele, možnost podvržení nepravdivých identifikačních údajů a metadat,
- nesoulad mezi teritorialitou práva a globalitou Internetu,
- spletitost kyberprostoru a jeho součástí,
- nesnadno definovatelné skutkové podstaty,
- nesmírně rychlá proměnlivost kyberprostoru a jeho částí v čase.[96]

## 4.2 Nezletilé oběti

Trestní zákoník dle ustanovení § 126 vymezuje dítě jako osobu mladší 18 let, pokud trestní zákon nestanoví jinak. Nezletilým dítětem se pro účely této práce rozumí tedy každá osoba mladší 15 let.

V trestním právu, konkrétně zákon č. 141/191 Sb., o trestním řízením soudním, jenž je stěžejním pramenem trestního práva procesního, nedefinuje doslova pojem oběť. Ekvivalentem bude pojem poškozený, který upravuje § 43 uvedeného zákona. Poškozená osoba je v tomto případě subjektem trestního řízení a zákon jí k tomu dává určitá práva a povinnosti. V případě, že oběť bude mít současně i procesní postavení svědka, tak má povinnost mimo jiné svědčit. Oběť trestného činu má tedy v trestním řízení v případech stanoveným zákonem procesní postavení poškozeného. Aby se jednalo o poškozeného podle trestní řádu, musí tedy dojít k porušení či ohrožení zájmů chráněných zákonem. Naopak poškozeným není ten, kdy vzniklá újma nebyla způsobena pachatelem trestného činu nebo nebyla v příčinné souvislosti s trestným činem.

Právní norma trestního práva, jež upravuje oběť, je zákon č. 45/2013 Sb., o obětech trestných činů a o změně některých zákonů (zákon o obětech trestných činů),

[96] VÁLKOVÁ, H., KUCHTA, J., HULMÁKOVÁ, J., et al. *Základy kriminologie a trestní politiky.* 3. vydání. Praha, 2019. s. 548.

který by měl do jisté míry zlepšit postavení obětí trestných činů i mimo trestní řízení, zajistit dostatečnou právní záruku, aby nebyla porušena či ohrožena důstojnost obětí a zabránit tak dalšímu poškození obětí ze strany PČR nebo jiných orgánů činných v trestním řízení. Dítě je tímto zákonem definováno jako zvlášť zranitelnou obětí.[97] Zásadní rozdíl oproti trestnímu řádu je ten, že podle tohoto zákona je obětí trestného činu pouze fyzická osoba, nikoli právnický subjekt s tím, že za oběť je považována každá osoba, která se cítí být obětí spáchaného trestného činu, pokud nevyjde najevo opak nebo pokud nejde zjevně o zneužití postavení oběti. Další rozdíl s porovnáním s trestním řádem je ten, že na postavení oběti nemá vliv trestní odpovědnost pachatele (věk, příčetnost).

Vědní obor, který se zabývá obětmi, představuje viktimologie. Název je odvozen od latinského slova victima (oběť) a řeckého slova logos (věda).[98] Na viktimologii lze pohlížet ve dvou rovinách. V širším pojetí se za oběť považují osoby postižené přírodními katastrofami, válkami, následky dopravních nehod apod. V práci se autor bude věnovat obětem z užšího pohledu, kdy se za oběti považují osoby postižené trestnou činností.[99] Viktimologie v úzkém slova smyslu zkoumá důvody vzniku trestných činů, vzájemné působení pachatele a oběti a úlohy v trestním řízení.[100] Oběť a její chování jsou z kriminologické stránky v mnohém ohledu významné. To se ukazuje jak ve vztazích k samotnému pachateli, k činu a k dynamice kriminality, tak ve spojitosti s kontrolou zločinnosti a trestní politikou.[101]

Předmětem zkoumání viktimologie lze tedy třídit do šesti skupin jevů:

- *„osobnost oběti (její biologické, psychické a sociální vlastnosti),*
- *vztahy mezi obětí a pachatelem, jejich vzájemná interakce,*
- *proces viktimizace a zejména úloha oběti v něm,*
- *úloha oběti v procesu odhalování, objasňování i soudního projednávání věci,*
- *pomoc oběti, způsoby jejího odškodnění a rehabilitace,*
- *předcházení viktimizaci.“*[102]

[97] Upravuje § 2 odst. 4, písm. a) zák. č. 45/2013 Sb., o obětech trestných činů a o změně některých zákonů (zákon o obětech trestných činů).
[98] VELIKOVSKÁ, M. *Psychologie obětí trestných činů.* Praha, 2016. s. 9.
[99] SVATOŠ, R. *Kriminologie.* Plzeň, 2012. s. 53.
[100] JELÍNEK, J., et al. *Kriminologie*. Praha, 2021. s. 169.
[101] KAISER, G. *Kriminologie.* Praha, 1994. s. 221.
[102] JELÍNEK, J., et al. *Kriminologie*. Praha, 2021. s. 172–173.

Prakticky každý může být obětí trestného činu. Jinými slovy, každý z nás má nějaký předpoklad k tomu, aby se stal obětí trestného činu, ale pouze část populace se jí skutečně stane. Jedná se o tzv. viktimnost, která je závislá na věku oběti, její profesi či zaměstnání, psychických vlastnostech (lehkomyslnost, agresivita) a na dalších sociálních charakteristikách, např. homosexuálové, osoby retardované, osoby jiné barvy pleti apod.[103]

V případě kybernetické kriminality děti pravidelně užívající internetovou technologii a počítačové systémy mají vyšší stupeň viktimnosti a mnohdy se stávají obětí opakovaně. Rodiče jsou významným subjektem ovlivňujícím chování a jednání dítěte, kdy neznalost potenciálních rizik v online prostředí může být kriminogenním faktorem s rizikovým potenciálem zvyšovat viktimnost dítěte. K tomuto Eckertová a Dočekal ve svém díle[104] uvádí, že rodiče si nepřipouští, že se zrovna jejich dítě setká s kyberšikanou, přičemž mohou mít pocit, že v dobré škole, ve společnosti přátel a v jejich péči dítěti nic takového nehrozí. Avšak k roli oběti kyberšikany jsou náchylnější děti citlivé a výrazně se lišící, tedy hendikepované, nadprůměrně inteligentní, děti studium zanedbávající, ale i příliš poctivé atd.

S viktimologií dále úzce souvisí tzv. viktimizace, kdy se jedná o průběh proměny hypotetické oběti v oběť reálnou.[105] Tento proces trvá nějakou dobu již před samotným naplněním skutkové podstaty trestného činu a v průběhu páchání protiprávního jednání. Průběh proměny zahrnuje všechny roviny deliktu, jako je zmíněný vztah pachatele a oběti, chování oběti a míru viktimnosti.[106] Viktimizaci obvykle představuje souhrn několika silně stresujících událostí, jež bývají náhlé, zprvu dozajista nepředvídatelné a s nimiž je ohromně těžké se vypořádat.[107]

Pokud jde o chování nezletilých dětí v kyberprostoru, tak v mnoha případech stačí jedno kliknutí, jedno neuvážené rozhodnutí, nepozornost, neznalost, hloupost, důvěra, ale i zvídavost a „malér je na světě“. Někdy dítě ani nemusí tušit, že se stalo obětí kybernetické kriminality, a když už se to dozví, tak někdy bohužel neví, jak postupovat, zda věc oznámit rodičům, jak se bránit a celkově, jak věc vlastně řešit. Může se tedy jednat spíše o latentní oběti. Názorným příkladem může být opět dítě, které se stalo obětí

[103] SVATOŠ, R. *Kriminologie.* Plzeň, 2012. s. 55.
[104] ECKERTOVÁ, L., DOČEKAL, D. *Bezpečnost dětí na Internetu: rádce zodpovědného rodiče.* Brno, 2013. s. 75.
[105] ZOUBKOVÁ, I., et al. *Kriminologický slovník.* Plzeň, 2011. s. 217.
[106] VÁLKOVÁ, H., KUCHTA, J., HULMÁKOVÁ, J., et al. *Základy kriminologie a trestní politiky.* 3. vydání. Praha, 2019. s. 172.
[107] VELIKOVSKÁ, M. *Psychologie obětí trestných činů.* Praha, 2016. s. 16.

kyberšikany, kdy se se svojí negativní zkušeností zpravidla nesvěřuje. Nikoliv v důsledku nedůvěry k rodičům. I dítě potřebuje být v očích rodičů úspěšné a oblíbené. Šikanované dítě se potýká s pocity studu, ponížení, viny a může se domnívat, že kamarádům opravdu nestačí a útoky si zaslouží. Taktéž se může obávat, že když se svěří, tak bude označeno za „práskače" a ústrky ještě zesílí. Většinou se svěří až v krajní situaci, když je vyčerpané dlouhodobým trápením a bezradné, nebo když je odhalen nějaký útok.[108] Případně oběti usnadňují práci pachateli tím, že se samy sebe natáčejí v různých, obvykle intimních situacích, např. na mobilní telefony, při online komunikaci používají webkameru, vytvářejí blogy, navštěvují chatovací místnosti, uvádějí své identifikační údaje v profilech na sociálních sítích apod. Získat oběť na internetu je skutečně velmi jednoduché, kdy toto riziko by nemělo být nikým podceňováno. Zde platí, že větší informovanost nejen dětí, ale i dospělých osob by mohla snížit riziko viktimizace na minimum.[109] Co se dále týče proměny hypotetické oběti v oběť reálnou, tak se lze přiklánět k tomu, že si nezletilé oběti v mnoha případech zaviní svoji viktimizaci.

Jednotlivé stádia viktimizace se v obecné rovině rozdělují na primární, sekundární a terciární.[110] Primární újma způsobená oběti má přímý kontext s trestným jednáním pachatele. V některých případech může mít vážnější následky sekundární újma, která vzniká procesy po spáchání protiprávního jednání. Jedná se např. o nesprávnou činnost orgánů činných v trestním řízení, kupříkladu opakované výslechy dětí, dále následné chování pachatele, který např. zastrašuje své oběti, a sociální prostředí, kdy se jedná o např. o působení tisku. Terciární újma představuje situaci, kdy se oběť nevyrovná s traumatickou zkušeností, ačkoliv došlo k uzdravení a restauraci sociálních vztahů. Projevem můžou být pocit viny, strachu, podrážděnosti, ztráta sebedůvěry, náladovost, snížení koncentrace apod. Po fyzické stránce se jedná např. o tělesnou slabost, srdeční potíže, bolest hlavy, plačtivost atd.[111]

U nezletilých obětí ve vztahu ke kyberkriminalitě může být zdrojem sekundární viktimizace taktéž např. reakce samotných rodičů, ale i chování přátel a sourozenců, jež může negativně ovlivnit jejich psychologické aspekty jako je jejich sebevědomí apod. Autor práce se prakticky nesetkal s tím, že by obecně oběti kybernetické kriminality

[108] ECKERTOVÁ, L., DOČEKAL, D. *Bezpečnost dětí na Internetu: rádce zodpovědného rodiče.* Brno, 2013. s. 76.
[109] HULANOVÁ, L. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha, 2012. s. 141–142.
[110] ZOUBKOVÁ, I., et al. *Kriminologický slovník.* Plzeň, 2011. s. 217.
[111] SVATOŠ, R. Kriminologie. In ZOUBKOVÁ, I., MOULISOVÁ, M. *Kriminologie a prevence kriminality.* Praha: Armex Publishing, 2004. s. 31–32. ISBN 80-86795-05-5.

zveličovaly skutečně utrpěnou újmu, tak jako třeba u jiných druhů kriminalit. Z druhé strany bylo vnímáno, že ten, kdo bral na lehkou váhu způsobené jednání, byly spíše orgány, které přijímaly dané oznámení. Svými nevhodnými poznámkami a následným nesprávným postupem, kdy např. byla věc chybně kvalifikována a daný trestný čin již neumožňoval využití institutů, které trestní řád nabízí, docházelo tímto k sekundární viktimizaci, tedy došlo k újmě, která byla způsobena druhotně po spáchaní trestného činu.

Stejně tak viktimologie rozlišuje oběti na primární, sekundární a terciární. Primární oběti, jsou bezprostředně dotčené trestným činem, respektive jsou přímou obětí kriminálního činu. Příbuzní nebo blízcí oběti, kteří jsou s obětí v přímém kontaktu, se považují za sekundární oběti. Terciární oběti jsou příslušníci komunity, veřejnost, média, jež zprostředkovávají újmy způsobené oběti v důsledku trestného činu.[112] Nezletilé děti, na nichž je páchána trestná činnost v souvislosti s kybernetickou kriminalitou, se tak stávají primární obětí s tím, že zejména rodiče budou v tomto případě sekundární obětí.

Důležitou roli sehrává oběť kybernetické kriminality taktéž v kriminalistice. Tato věda chápe osobu oběti jako nezastupitelnou součást spáchaného trestného činu. Význam role oběti při vyšetřování trestného činu spočívá v tom, že se zpravidla současně jedná o stěžejního svědka a často i oznamovatele činu.[113] Oběť je nositelem mimo jiné paměťové stopy.[114] Dále je klíčem k objasnění vztahů pachatele, odhalení motivů jeho jednání a v neposlední řadě i zdrojem informací napomáhajících dějů, jež nalezly odraz ve stopách na místě činu. Z pohledu kriminalistiky je v ohnisku zájmu poznání osobnosti oběti, jejích vztahů nejen s pachatelem, jakož i její působení na průběh činu a následné vyšetřování. Kriminalistika se zabývá obětí představovanou pouze fyzickými osobami, a to z toho důvodu, že oběť je hned po pachateli nejbohatším zdrojem informací využitelných právě k objasnění motivu, průběhu a okolností případu.[115] Oběť z kriminalistického aspektu představuje zejména toho účastníka trestného činu, kterému vznikla škoda v důsledku konání pachatele. Škoda může mít rysy újmy na majetku, na zdraví, morální, někdy může mít charakter ohrožení či omezení svobody, zprostředkovaně může být způsobena i blízké osobě, příbuzné osobě apod.[116]

[112] JELÍNEK, J., et al. *Kriminologie*. Praha, 2021. s. 175.
[113] V případě kybernetické kriminality páchané na nezletilých dětech budou v roli oznamovatele trestného činu spíše zákonní zástupci, osvojitelé, opatrovníci apod.
[114] Viz kapitola 2.2.3 Kriminalistické stopy u kybernetické kriminality.
[115] NĚMEC, M., et al. *Teorie a metodologie kriminalistiky pro magisterské studium – I. díl. Aktuální problémy kriminalistické teorie.* Praha, 2018. s. 158–161.
[116] PORADA, V., et al. *Kriminalistika (teorie, metody, metodologie).* Plzeň, 2014. s. 131.

# 5 Prevence kybernetické kriminality

Zločin lze omezovat různými způsoby. Mezi dva základní přístupy patří strategie represivní a strategie preventivní. Pro první z nich je charakteristické, že představují reakci na již spáchaný trestný čin, a mají proto zejména trestněprávní charakter. Zatímco preventivní strategie se orientují na aktivní předcházení zločinu. V praxi se však oba postoje prolínají, neboť účelná kriminální politika přepokládá, že budou rozvíjeny současně a společně se podpoří.[117] Obdobně tuto úvahu vnímá Matějka[118], který k počítačové kriminalitě uvádí, že boj proti ní se ve své podstatě nikterak neliší od boje proti všem formám kriminality obecně, kdy represe a prevence představují neoddělitelné a nezastupitelné složky, přičemž jedna bez druhé nemůže dost dobře existovat a žádný boj proti kriminalitě nemůže být efektivní bez působení prevence i represe zároveň.

Ovšem z poznatků spousta vědních oborů posledních dekád se ukazuje, že negativním jevům, které se vyskytují napříč společností, je mnohem efektivnější předcházet, než je poté komplikovaně řešit. To samé platí i o kriminalitě. Represivní řešení, jakožto reakce na spáchané protiprávní jednání, se jeví jako méně efektivní, kdy preventivní strategie představují vedle strategií represivních rovnocennou, v současné době spíše upřednostňovanou, složkou kontroly kriminality.[119] Prevence kriminality po dlouhou dobu platí jako přednostní cíl sociální a trestní politiky.[120]

Prevence kriminality je neoddělitelnou součástí kriminologické nauky, jež s ohledem na její předmět nabývá interdisciplinárního charakteru. Proto samotné vymezení pojmu a obsahu prevence kriminality není jednoduchou záležitostí a v odborné literatuře ani jednotné vymezení nenacházíme.[121]

Gřivna, Scheinost a Zoubková[122] charakterizují prevenci kriminality jako soubor nejrůznějších společenských aktivit orientovaných na odstranění, oslabení či neutralizaci rizikových činitelů, které motivují, vyvolávají, usnadňují nebo podporují páchání trestných činů.

[117] TOMÁŠEK, J. *Úvod do kriminologie: Jak studovat zločin.* Praha, 2010. s. 169.
[118] MATĚJKA, M. *Počítačová kriminalita.* Praha, 2002. s. 77.
[119] VÁLKOVÁ, H., KUCHTA, J., HULMÁKOVÁ, J., et al. *Základy kriminologie a trestní politiky.* 3. vydání. Praha, 2019. s. 256.
[120] KAISER, G. *Kriminologie.* Praha, 1994. s. 91.
[121] VÁLKOVÁ, H., KUCHTA, J., HULMÁKOVÁ, J., et al. *Základy kriminologie a trestní politiky.* 3. vydání. Praha, 2019. s. 257.
[122] GŘIVNA, T., SCHEINOST, M., ZOUBKOVÁ, I., et al. *Kriminologie.* 5. vydání. Praha, 2019. s 151.

V kriminologickém slovníku[123] je k pojmu prevence kriminality uvedeno, že se jedná o společenská opatření, která se orientují na předcházení sociálně patologickým jevům ve společnosti, zejména pak kriminalitě. Může mít podobu souhrnu opatření specifikovaných jako preventivní programy prevence, preventivní strategie, plány prevence apod. Kriminální prevence je podle obsahového zaměření označována jako sociální, situační a viktimologická prevence. Dále lze prevenci kriminality třídit podle okruhu adresátů na prevenci primární, sekundární a terciární.

Podle Kaisera[124] rozumíme pod prevencí zločinnosti ta opatření, jejichž účelem je snížit míru a váhu kriminality, ať už omezením příležitostí vyvolávajících zločin, podle potřeby přítomností schopného ochránce nebo sousedskou kontrolou či působením na pachatele a veřejnost.

Svatoš ve svém díle[125] uvádí, že termín prevenci kriminality lze shrnout tak, že se jedná vedle trestní represe o druhou formu kontroly kriminality s tím, že představuje soubor nejrůznějších aktivit mimotrestního charakteru orientovaných na odstranění, oslabení či neutralizaci kriminogenních faktorů, jejichž cílem je zastavit růst kriminality nebo docílit jeho zmenšení. Jedná se o působení na činitele kriminality, příležitosti k páchání zločinu, podněty k páchání kriminality, potenciální pachatele a oběti. Jde o vytváření zábran proti páchání trestné činnosti.

Co se týče kybernetické kriminality tak zejména s ohledem na obrovskou míru její latence snad více než u jiných kriminalit platí, že důležitější je prevence než represe. Kdyby byla oběť lépe informována, lze řadě typů kybernetických útoků zcela zabránit. Preventivní opatření k zabránění kybernetické kriminality lze v zásadě rozdělit do dvou skupin, a to na osvětová opatření a bezpečnostní opatření.[126]

První z uvedených pojmů by měl směřovat k seznámení široké veřejnosti s jednotlivými typy kybernetických útoků a nabádat společnost k vyšší míře opatrnosti a zdrženlivosti v kyberprostoru. Lidé totiž mívají vyšší důvěru k informacím a počítačovým datům, aniž by si tyto jakýmkoliv způsobem ověřili. Každý by měl pochopit, že nasdílením fotografií nebo vyplněním svých osobních údajů apod. na mnohé webové stránky nad nimi ztrácí kontrolu a jejich získání zpět nebo vymazání bývá fakticky nemožné. Poučení společnosti před kybernetickou kriminalitou by měla začít již

[123] ZOUBKOVÁ, I., et al. *Kriminologický slovník.* Plzeň, 2011. s. 141.
[124] KAISER, G. *Kriminologie.* Praha, 1994. s. 92.
[125] SVATOŠ, R. *Kriminologie.* Plzeň, 2012. s. 87.
[126] JELÍNEK, J., et al. *Kriminologie*. Praha, 2021. s. 501.

na školách, neboť ačkoliv jsou mladé generace již zcela zvyklé na život s moderními informačními technologiemi, neznamená to, že si vedle jejich užitku uvědomují také jejich rizika. Zejména kybergrooming a některé další kyberútoky je přitom na mladé generace přímo zaměřený a jejich vědomost mezi potencionálními obětmi by jistě vedla ke snížení jejich úspěšnosti.[127] Osvěta je cílena především na zranitelné skupiny osob, kam spadají mimo jiné i děti, které kyberprostor užívají zpravidla zdatněji a častěji než jejich rodiče, leč neopatrně a důvěřivě, což může plynout z neznalosti fungování kyberprostoru a rizik s ním spojených. K ochraně před nevhodným obsahem lze použít filtrování obsahu internetu a různé formy tzv. rodičovské kontroly, např. znemožnění spuštění aplikace, omezení času používání zařízení atd. V rámci České republiky se prevencí v oblasti kyberprostoru angažují např. Národní centrum kybernetické bezpečnosti, Centrum prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci, Národní centrum bezpečnějšího internetu, z. s., CZ.NIC, E-Bezpečí, Better Internet for Kids aj.[128]

Druhá skupina je zaměřena na preventivní opatření především na ochranu integrity dat.[129] Nicméně tato skupina opatření s ohledem na charakter trestné činnosti až tak s kybernetickou kriminalitou páchanou na nezletilých dětech v Jihočeském regionu přímo nesouvisí. Faktem ovšem je, že závislost civilizace na informačních a komunikačních technologií roste, následkem čehož se stává zranitelnost informačních systémů a informačních technologií významnou hrozbou, jež lze eliminovat právě hlavním nástrojem obrany, a to prevencí spočívající v budování informačních systémů jako systémy zabezpečené. Tímto dojde k eliminování zranitelnosti, a tedy i k zábraně hrozeb, které pocházejí z řad pachatelů kyberkriminality.[130] Minimálním předpokladem udržitelné provozuschopnosti jakéhokoli zařízení vstupující do kyberprostoru je antivir, jehož součástí bývá i firewall a antispyware. Sebelepší software ovšem neochrání neopatrného uživatele. Kromě vlastní obezřetnosti jednotlivých uživatelů je klíčová i fyzická ochrana jednotlivých zařízení, např. přístup k počítači, tabletu, mobilnímu telefonu apod.[131]

[127] JELÍNEK, J., et al. *Kriminologie*. Praha, 2021. s. 501–502.
[128] GŘIVNA, T., SCHEINOST, M., ZOUBKOVÁ, I., et al. *Kriminologie.* 5. vydání. Praha, 2019. s 407.
[129] JELÍNEK, J., et al. *Kriminologie*. Praha, 2021. s. 502.
[130] VÁLKOVÁ, H., KUCHTA, J., HULMÁKOVÁ, J., et al. *Základy kriminologie a trestní politiky.* 3. vydání. Praha, 2019. s. 552.
[131] GŘIVNA, T., SCHEINOST, M., ZOUBKOVÁ, I., et al. *Kriminologie.* 5. vydání. Praha, 2019. s 406–407.

## 5.1 Ochrana dětí v kyberprostoru

Důležitou roli pro ochranu dětí v kyberprostoru sehrává zejména sociální prevence, jež je zaměřena na vytváření příznivých podmínek společenského života mimo jiné v sociální, výchovně-vzdělávací, volnočasové, psychologické oblasti apod. Orientuje se na změnu nepříznivých aspektů života jednotlivce a společnosti jako celku, jež se mohou stát ve svém důsledku vlivnými kriminogenními faktory. Rodina a školní prostředí patří mezi typické objekty opatření sociální prevence. V procesu socializace dítěte sehrává nejdůležitější úlohu rodinné prostředí, kdy se jedná o životní prioritní prostředí jedince. Především v období raného dětství výrazně formuje osobnost každého z nás, kdy jsme ke všem vlivům působícím z vnějšího prostředí patrně nejcitlivější, nejvnímavější. Dítě se v rodině učí, pozoruje jednání a chování rodinných příslušníků, které následně napodobuje. Rodina tak z pohledu prevence sehrává zásadní roli. Škola jako významný socializační činitel nastupuje v procesu socializace jedince kolem šestého roku věku dítěte. Školní prostředí formuje osobnost mladého jedince, pečuje o rozvoj jeho individuálních osobnostních dispozic, kdy tak významným způsobem zasahuje do výchovného procesu. Dítě se současně dostává do nové sociální role. Objevují se nové příležitosti k četnějším interakcím, kdy mu jsou zprostředkovány společenské hodnoty, pravidla, a to často odlišným způsobem, než tomu bylo doposud v rámci rodinného prostředí. Škola se tak stává dalším významným socializačním faktorem v rámci dotváření určitého životního stylu počítaje postojové a hodnotové orientace dítěte. Prostřednictvím školního prostředí na všech úrovních a typech škol je v praxi realizováno mnoho preventivních aktivit ať již za úzké součinnosti pedagogických pracovníků nebo pouze na základě iniciativy subjektů prevence kriminality provádějících různé preventivní programy cílené právě na adresáty z řad mládeže.[132]

Hulanová ve své knize uvádí[133], když se děti budou učit základním pravidlům bezpečného používání internetu, tak je velká pravděpodobnost, že se z nich nestanou online oběti. Děti je potřeba učit, aby nikomu, s kým se seznámily prostřednictvím internetu, nesdělovaly informace o své osobě. Zejména je nežádoucí uvádět např. adresu bydliště, telefonní číslo domů, adresu školy, jména, adresy, telefonní čísla rodičů apod. Stejná pravidla platí i pro vytváření profilů na různých sociálních sítí. Informace, které

[132] VÁLKOVÁ, H., KUCHTA, J., HULMÁKOVÁ, J., et al. *Základy kriminologie a trestní politiky.* 3. vydání. Praha, 2019. s. 258–259.
[133] HULANOVÁ, L. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha, 2012. s. 108–109.

sdělí do veřejného prostoru, se stanou dostupnými pro mnoho dalších lidí, kteří je mohou následně šířit a zneužívat. Pokud se děti neporadí s rodiči nebo s osobami, které o ně pečují, neměly by nikomu prostřednictvím internetu posílat své fotografie či videonahrávky. To samé platí o domlouvání schůzek s někým, koho poznaly na internetu, a když už na takovou schůzku půjdou, měly by se scházet na místech veřejně dostupných a nechodit na schůzku samy. Dále by neměly ani nejlepšímu příteli prozrazovat heslo nebo přihlašovací údaje své internetové stránky nebo počítače. Když se bude dětem zdát, že se na internetu probírají věci, které je děsí nebo je přivádějí do rozpaků, měly by přestat v komunikaci na internetu. Taktéž je dobré neodpovídat na zlé, urážlivé, hrubé a nevkusné emaily či jiné zprávy. Pokud k něčemu takovému dojde, měly by vědět, že to není jejich vina, a že by se měly o takovém či o všech podobných nepříjemných zážitků svěřit svým rodičům nebo někomu z dospělých, komu důvěřují. Děti je dále potřeba učit, že ten, kdo je na druhé straně při online komunikaci či psaní SMS, nemusí být tím, za koho se vydává, kdy v online prostředí je snadné změnit svoji identitu. Je nebezpečné, aby otvíraly soubory přiložené k emailům, samotné emaily či chatové zprávy, které přijdou od lidí nebo z míst, jež neznají, kdy tyto zprávy mohou obsahovat viry nebo jiné programy, jež by mohly zničit důležité informace a poškodit software zařízení. Neměly by reagovat na výzvy zpětného volání, které obdrží prostřednictvím SMS nebo emailem a které je informují o výhře. Neuvážené používání služeb, které poskytují např. mobilní telefony, je může stát spousta peněz, a proto by měly přemýšlet nad jejich používáním.

## 5.2 Pravidla bezpečné komunikace

Následující podkapitola se bude věnovat obecným doporučením chování při komunikaci v kyberprostoru. Samozřejmě nelze zcela zaručit, že se dětem nic nestane, když budou dodržovat následující doporučení, nicméně se jedná o nástroj prevence, jak alespoň snížit riziko potenciální oběti. Nutno podotknout, že tato podkapitola úzce souvisí s předcházející podkapitolou, kdy jednotlivá pravidla používání internetu se můžou opakovat nebo vzájemně prolínat s pravidly bezpečné komunikace. Nicméně s ohledem na skutečnost, že ať už je to kybergrooming, sexting, kyberšikana nebo kyberstalking, tak všechny uvedené formy kybernetické kriminality páchané na nezletilých dětech vychází obvykle z předchozí komunikace. Proto je tato část týkající se pravidel bezpečné komunikace vedena samostatně.

Internet dětem nabízí široké možnosti komunikace, i tady ale platí jistá pravidla, která je potřeba znát.[134] Tato pravidla lze shrnout do níže uvedených bodů.

Pravidla bezpečné komunikace:

- *„Ignoruj neslušné zprávy a neodpovídej na ně. Nikdy.*
- *Pokud s někým nechceš komunikovat, nekomunikuj.*
- *Zprávy od neznámých osob hned smaž. Může to být podvodník nebo se ve zprávě může nacházet počítačový vir.*
- *Na profilech sociálních sítí nikdy neuváděj své telefonní číslo, rodné číslo nebo adresu.*
- *Své telefonní číslo nebo adresu nikomu neposílej ani v soukromé zprávě. Ten, kdo ji chce, může být někdo úplně jiný než sám/sama říká, že je.*
- *Nedomlouvej si schůzky přes internet. Na schůzku domluvenou přes internet nechoď, aniž bys o tom řekl někomu dalšímu.*
- *Nikomu neposílej své nahé fotografie, protože můžou být rozesílány dalším lidem. Pokud po tobě někdo chce intimní fotografie, přestaň s ním ihned komunikovat.*
- *Mysli na své digitální já - mysli dvakrát, než na internet napíšeš něco nevhodného nebo urážlivého.*
- *Při používání webové kamery buď opatrný, kdokoli může na druhé straně hovor nahrávat.*
- *Uzamkni svůj počítač nebo telefon, pokud s ním dál nebudeš pracovat. Nastav si automatické uzamknutí při delší nečinnosti.“*[135]

[134] KOHOUT, R. *Internetem Bezpečně.* Karlovy Vary, 2017. s. 16.
[135] Tamtéž. s. 17.

# 6 Empirický výzkum

Praktická část bakalářské práce je tvořena dotazníkovým šetřením. Hlavním cílem práce je zjistit, jak rodiče nezletilých dětí vnímají rizika online prostředí s explicitním zaměřením na konkrétní formy kyberkriminality, tedy zhodnocení vnímání kybernetické kriminality mezi rodiči. K dosažení hlavního cíle práce byla využita kvantitativní strategie za využití metody dotazníkového šetření mezi rodiči nezletilých dětí navštěvující základní školy v Jihočeském regionu, kdy vhodnou kombinací otázek bylo identifikováno vnímaní kybernetické kriminality mezi rodiči, byla zjišťována existence a realizace preventivních opatření rodičů ve vztahu k definované kriminalitě a jaké si stanoví opatření, aby ochránili své děti.

## 6.1 Sběr dat

Dotazník byl vytvořen pomocí internetového portálu survio.com. Vygenerovaný odkaz byl sdílen ve sportovních klubech v Českých Budějovicích, jako např. fotbalová akademie SK Dynamo České Budějovice, taneční škola NG Dance Crew a TJ Karate České Budějovice, ve společnosti E.ON Česká republika, s.r.o., v bankovních institucích v Českých Budějovicích, jako např. Česká spořitelna a MONETA Money Bank, na základních školách v Jihočeském kraji, jako např. ZŠ Grünwaldova, ZŠ v Dubném. Dotazník byl dále sdílen napříč územními odbory Policie České republiky v Jihočeském regionu.

Sběr dat probíhal od 11.12.2022 do 31.01.2023. Na dotazník odpovědělo celkem 425 respondentů. Dotazník se nachází na internetové adrese: https://www.survio.com/survey/d/F9J2O4F9D9D4Q1J2N. Po ukončení sběru dat, byla provedena kontrola jednotlivých responzí, kdy následně bylo z důvodu nelogických odpovědí vyřazeno celkem 45 respondentů. Data jsou tedy hodnocena z platných 380 odpovědí. Celková návratnost dotazníku byla 75,1 %. Dotazníkové šetření obsahuje 18 otázek. Nacházely se zde otázky jak uzavřené, tak otevřené, kdy průměrný čas zodpovězení otázek byl 5 až 10 minut. Výsledky zkoumání jsou krátce okomentovány v níže uvedených grafech.

## 6.2 Struktura dotazníkového šetření

Po otevření internetového odkazu se respondentovi zobrazí úvodní informace, který je mimo jiné informován, že dotazník je určen pro rodiče nezletilých dětí, které nedovršily 15. rok věku navštěvující základní školy v Jihočeském regionu.

První otázka identifikuje respondenta, kdy se autor práce dotazuje na jeho pohlaví.

Ve druhé otázce respondent odpovídá na svůj věk. Zde může rodič zvolit mezi 5 nabízenými odpověďmi, a to: do 25 let, 26–35 let, 36–45 let, 46–55 let, 56 let a více.

V následující otázce respondent odpovídá na uzavřenou otázku, zda se někdy předtím setkal s pojmem kybernetická kriminalita, přičemž mu je poskytnuta informace, že tuto lze jednoduše charakterizovat jako protiprávní jednání, ke kterému dochází v kyberprostoru, kdy se jedná tedy o souhrn spáchaných trestných činů v určitém prostředí, a že v současné době je převážná část kybernetické kriminality páchána prostřednictvím internetu.

V otázce č. 4 je uzavřenou otázkou zjišťováno, zda se respondent v minulosti stal obětí kybernetické kriminality.

V páté otázce je respondent dotazován, jestli je jejich dítě uživatelem informačních a komunikačních technologií s tím, že je mu poskytnuta informace, že tyto zahrnují veškeré informační technologie pro komunikaci a informatiku, např. PC, notebook, mobilní telefon, tablet apod., respektive zda jejich nezletilé dítě používá např. internet, sociální sítě, zařízení na hraní her apod.

Šestá otázka pojednává o tom, jak rodič vnímá nebezpečí v online prostředí, které hrozí nezletilým dětem, kdy odpovídající může zvolit mezi odpověďmi: „nebezpečí vnímám, ale neřeším to“, „nebezpečí vnímám a mám preventivní opatření“, „nebezpečí nevnímám“ a „nebezpečí neexistuje“.

Sedmá otázka se ptá: „Kolik registrovaných trestných činů je podle Vás ročně spácháno na nezletilých dětech v ČR v souvislosti s kybernetickou kriminalitou?“ Na výběr bylo celkem 5 možností, a to: 0–100, 101–200, 201–300, 301–400, 401 a více.

V osmé otázce se zjišťuje, jaká je dle rodičovo názoru objasněnost registrovaných trestných činů spáchaných na nezletilých dětech v ČR v souvislosti s kybernetickou kriminalitou, kdy má možnost zvolit: do 20 %, 21–40 %, 41–60 %, 61–80 %, 81–100 %.

V otázce č. 9 je respondent dotazován, kolik registrovaných trestných činů je podle něj ročně spácháno na nezletilých dětech v Jihočeském kraji v souvislosti s kybernetickou kriminalitou, kdy má na výběr odpovědi: 0–10, 11–20, 21–30, 31–40, 41 a více.

Na desátou uzavřenou otázku rodič odpovídá, zda si připouští, že by se zrovna jeho dítě mohlo stát obětí kybernetické kriminality.

Jedenáctou otázkou je zjišťováno, zda rodič ví, co znamenají pojmy: sexting, kybergrooming, kyberšikana a kyberstalking.

Ve dvanácté otázce respondent odpovídá, jaký z předchozích uvedených projevů kybernetické kriminality páchané na nezletilých dětech považuje za nejnebezpečnější, kdy může označit pouze jednu možnost, přičemž ke každému pojmu má informace, jak se dané jednání projevuje.

V otázce č. 13 rodič hodnotí závažnost jednotlivých projevů kybernetické kriminality páchané na nezletilých dětech. Opět se jedná o sexting, kybergrooming, kyberšikana a kyberstalking, kdy mezi tyto uvedené formy, má rozdělit 100 bodů, přičemž více bodů znamená větší závažnost.

Čtrnáctá otázka zní: „Jaké z těchto trestných činů spáchaných na nezletilých dětech ve vztahu ke kybernetické kriminalitě považujete za nejškodlivější?“ Zde může odpovídající zvolit mezi 5 nabízenými odpověďmi, a to:

- Trestné činy proti lidské důstojnosti v sexuální oblasti (např. sexuální nátlak, šíření pornografie)
- Trestné činy proti životu a zdraví (např. účast na sebevraždě)
- Trestné činy proti svobodě a právům na ochranu osobnosti, soukromí a listovního tajemství (např. vydírání, pomluva)
- Trestné činy proti rodině a dětem (např. ohrožování výchovy dítěte)
- Trestné činy proti pořádku ve věcech veřejných (např. nebezpečné vyhrožování, nebezpečné pronásledování)

V patnácté otázce měl respondent uvést, jaké má preventivní opatření ve vztahu k definované kybernetické kriminalitě (aby se dítě nestalo obětí), kdy na výběr měl následující možnosti:

- Žádné

- Používání rodičovského zámku – omezení a blokace používání webových stránek
- Kontrola historie vyhledávání na internetu
- Provádění situační výchovy a procvičování s dětmi hypotetických scénářů (např. simulovat, co by dělalo v případě kyberšikany apod.)
- Jednorázová edukace a osvěta v dané problematice
- Využití dostupných aplikací a programů k monitorování dítěte na internetu
- Pravidelná komunikace s nezletilým dítětem o možném nebezpečí, které online prostředí představuje
- Nezletilé dítě není při používání internetu bez dozoru
- Preventivní opatření řeší jiný člen rodiny
- Jiné

V šestnácté otázce je rodič uzavřenou otázkou dotazován, zda plánuje do budoucna přijmout nějaké opatření.

Sedmnáctá otázka byla pouze pro rodiče, kteří odpověděli v předchozí otázce, že plánují přijmou nějaké opatření, kdy měli uvést jaké.

Závěrečná osmnáctá otázka je ve znění: „Kde by se podle Vás mělo nezletilé dítě zejména dozvědět, jak by se mělo bezpečně chovat na internetu?“ Respondent má na výběr možnosti: „Ve škole“, „Od policie“, „V rámci zájmových kroužků“, „V médiích“, „V rodině“, „Jinde“, přičemž mají možnost uvést kde.

## 6.3 Hypotézy výzkumu

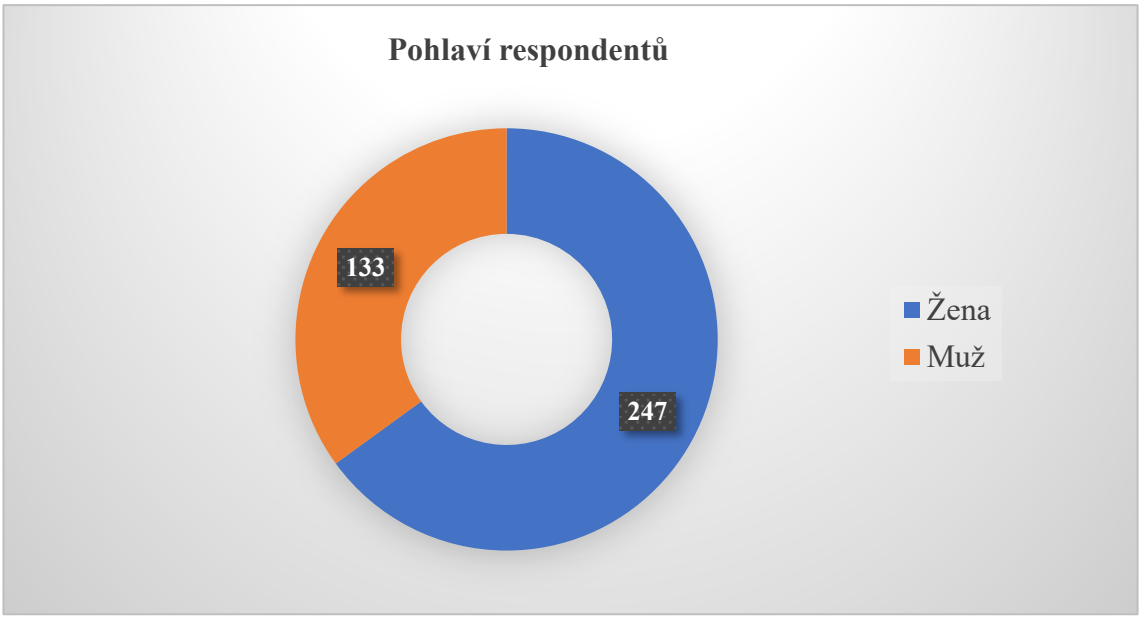
**H1:** Více jak 30 % respondentů, kterých uvedlo, že se nestali obětí kybernetické kriminality, si nepřipouští, že by se zrovna jejich nezletilé dítě stalo obětí kyberkriminality.

**H2:** Respondenti, kteří uvedli, že se setkali s pojmem kybernetická kriminalita, realizují ve větší míře 3 a více opatření než respondenti, kteří uvedli opak.

## 6.4 Interpretace výsledků zkoumání

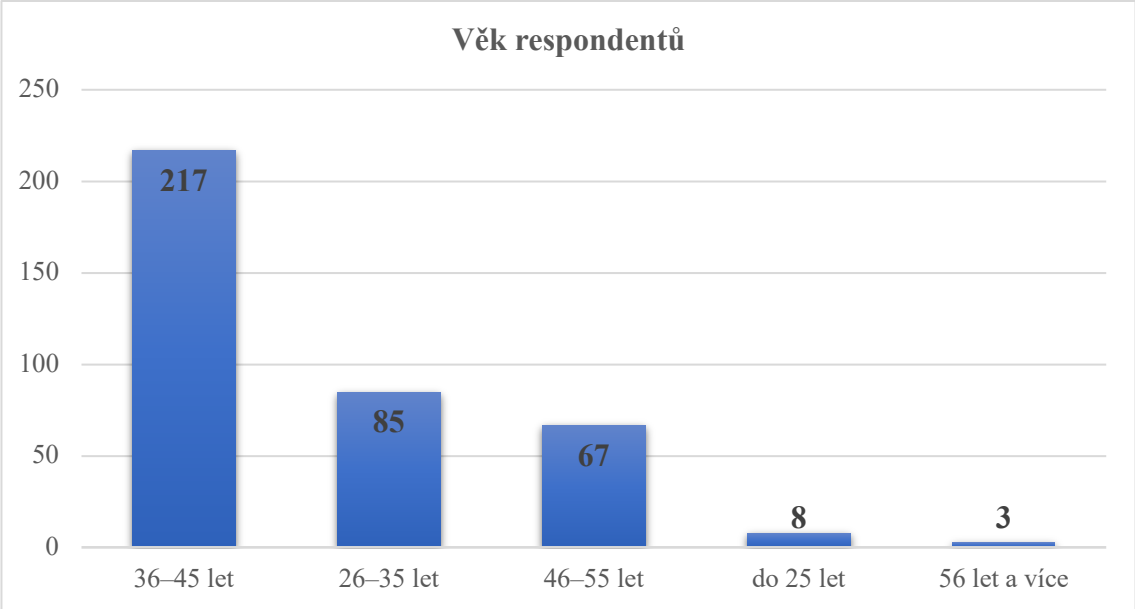
V následujících bodech jsou uvedeny výsledky výzkumu, jež jsou pro přehlednější orientaci čtenáře graficky znázorněny a krátce okomentovány.

*Graf 5 Poměr můžu a žen, kteří se zúčastnili výzkumu*[136]




První otázka sloužila k identifikaci rodiče podle pohlaví, kdy z celkového počtu 380 respondentů odpovídaly ve větší míře ženy, a to v počtu 247 (65 %), přičemž zbytek respondentů v počtu 133 (35 %) zaujímali muži.

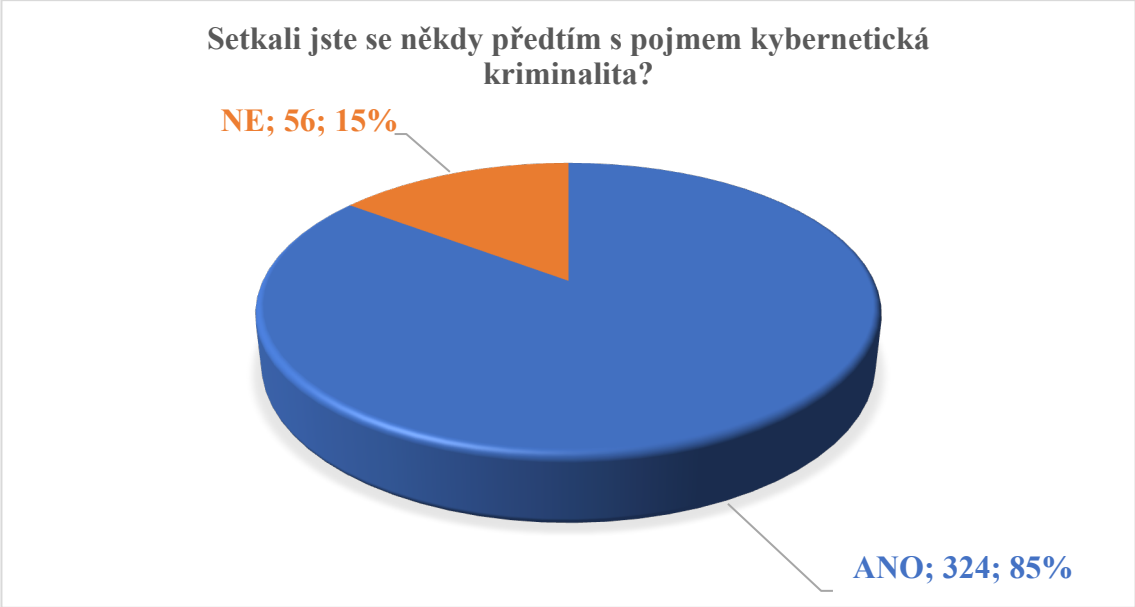
*Graf 6 Věkové rozložení respondentů*[137]




Z druhé otázky je patrné, že nejvíce odpovídali rodičové ve věku od 36 do 45 let, a naopak nejméně respondenti ve věku 56 let a více.

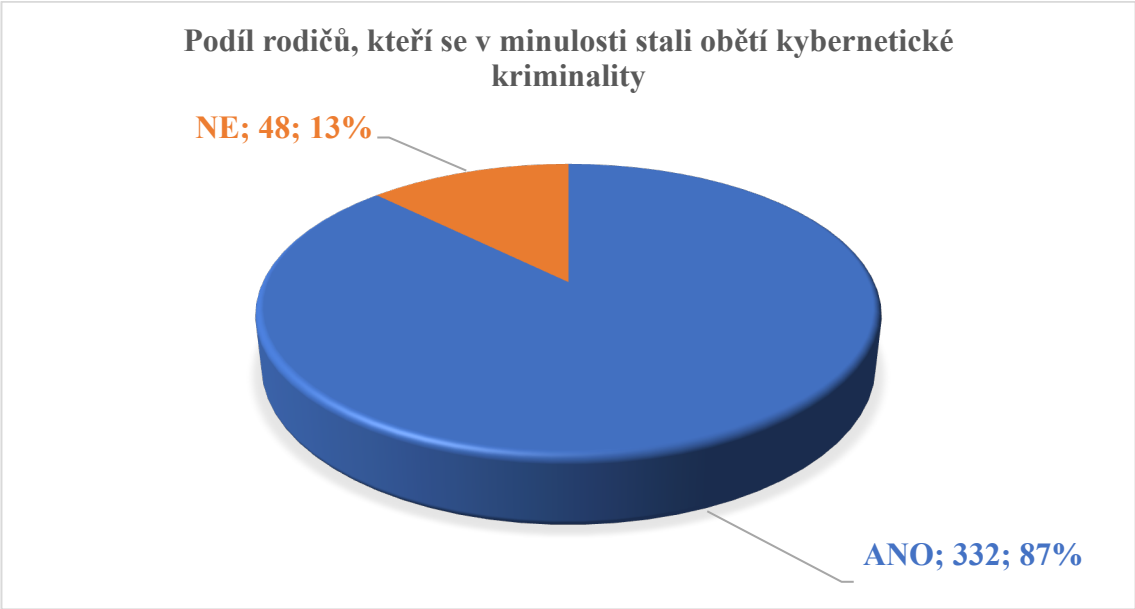
[136] Vlastní zdroj.
[137] Vlastní zdroj.

*Graf 7 Počet rodičů, kteří se v minulosti setkali s pojmem kybernetická kriminalita*[138]




Graf č. 7 ukazuje, v jakém poměru rodičové znají pojem kybernetická kriminalita, kdy 324 respondentů odpovědělo, že se s tímto pojmem již v minulosti setkali.

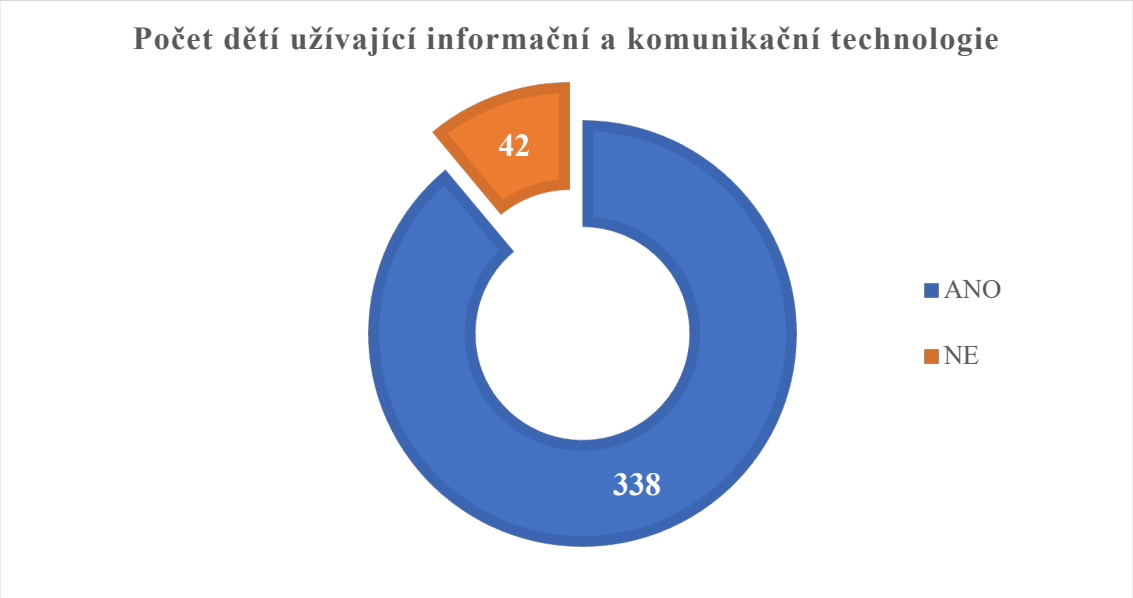
*Graf 8 Podíl rodičů, kteří se v minulosti stali obětí kybernetické kriminality*[139]




Graf č. 8 zobrazuje, že 13 % dotázaných rodičů se v minulosti stalo obětí kybernetické kriminality.

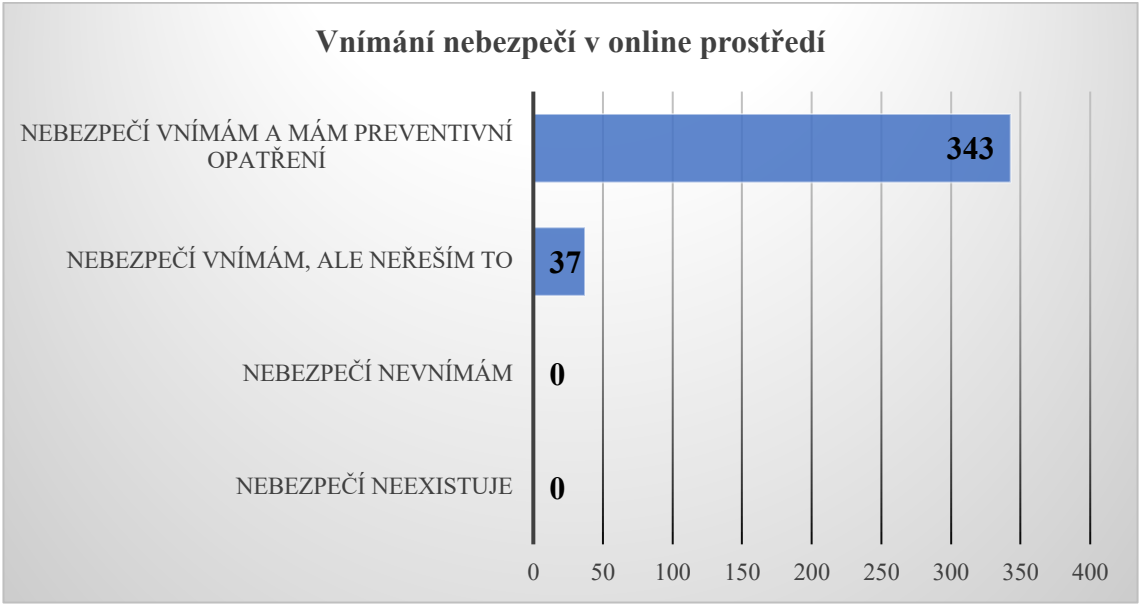
[138] Vlastní zdroj.
[139] Vlastní zdroj.

*Graf 9 Poměr dětí užívající informační a komunikační technologie*[140]




Z odpovědí rodičů na pátou otázku bylo překvapivě zjištěno, že 42 nezletilých dětí z celkové počtu 380 nepoužívá zatím např. PC, notebook, mobilní telefon apod.

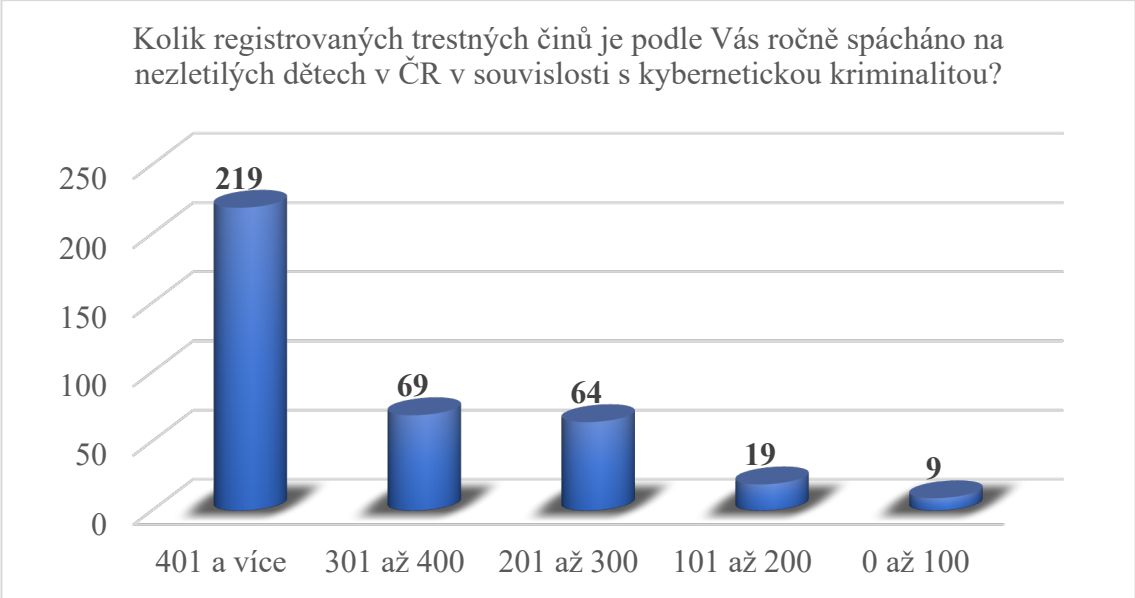
*Graf 10 Jak rodiče vnímají nebezpečí v online prostředí, jež hrozí nezletilým dětem*[141]




Dále bylo v dotazníku řešeno, jak rodiče vnímají nebezpečí v online prostředí, které hrozí nezletilým dětem. Díky této otázce můžeme konstatovat, že 343 respondentů z 380 dotázaných nebezpečí vnímá a realizuje preventivní opatření, aby ochránili své děti v kyberprostoru.

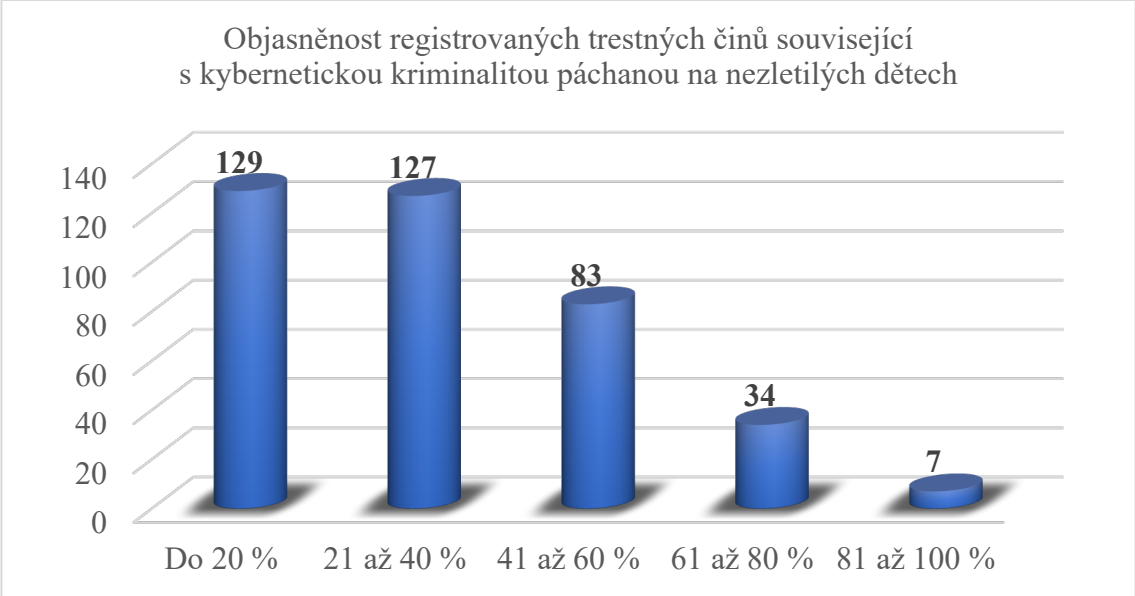
[140] Vlastní zdroj.
[141] Vlastní zdroj

*Graf 11 Názor rodičů na počet registrovaných trestných činů v ČR*[142]




Graf č. 11 zobrazuje mínění rodičů o stavu kybernetické kriminality páchané na nezletilých dětech v ČR. Největší počet respondentů 219 (58 %) se domnívá, že ročně je registrováno 401 a více trestných činů.

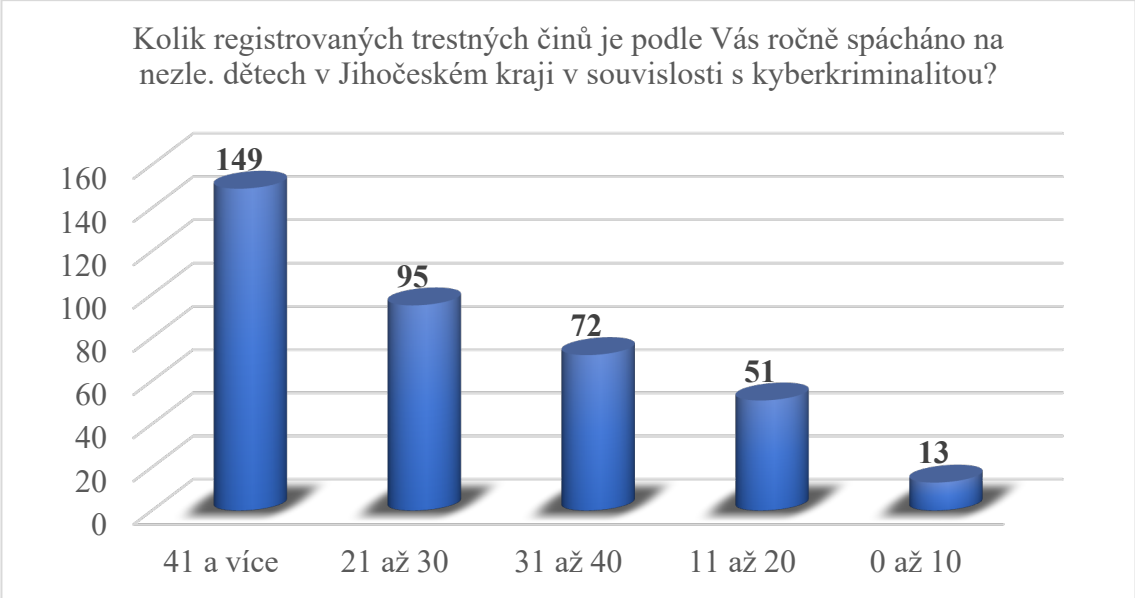
*Graf 12 Názor rodičů na objasněnost registrovaných trestných činů v ČR*[143]




Další otázka zjišťovala názor respondentů na činnost PČR, respektive do jaké míry se daří orgánům činným v trestním řízení objasňovat trestnou činnost související s kybernetickou kriminalitou páchanou na nezletilých dětech, kdy v největší míře rodiče odpovídali, že objasněnost je do 20 % a dále v rozmezí od 21 do 40 %.

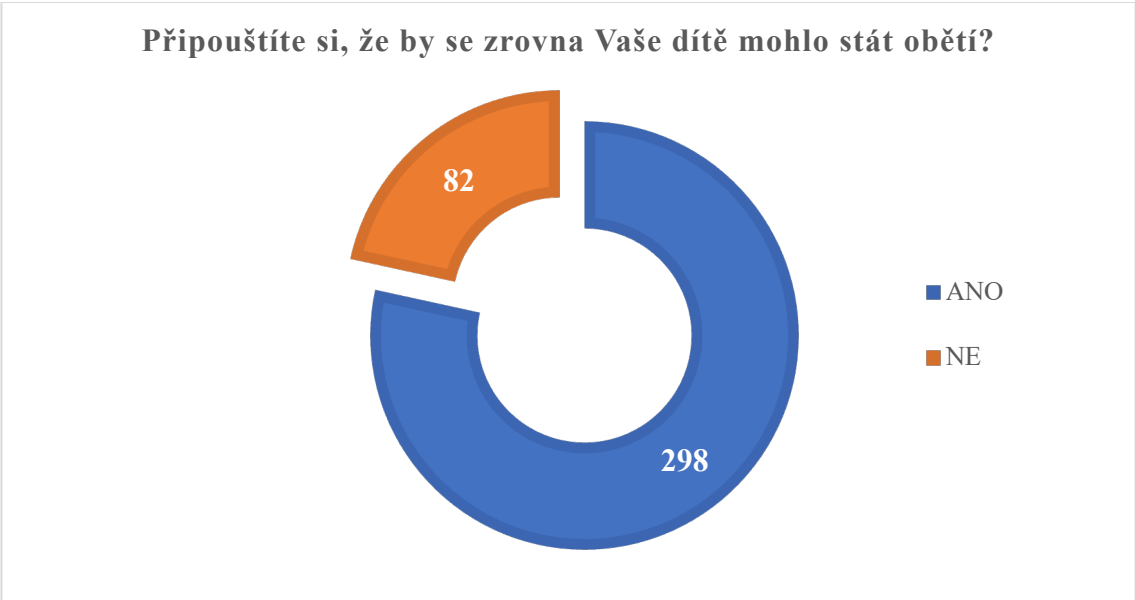
[142] Vlastní zdroj.
[143] Vlastní zdroj.

*Graf 13 Názor rodičů na počet registrovaných trestných činů v Jihočeském kraji*[144]




Graf č. 13 zobrazuje mínění rodičů o stavu kybernetické kriminality páchané na nezletilých dětech v Jihočeském kraji. Největší počet respondentů 149 (39,2 %) se domnívá, že ročně je registrováno 41 a více trestných činů.

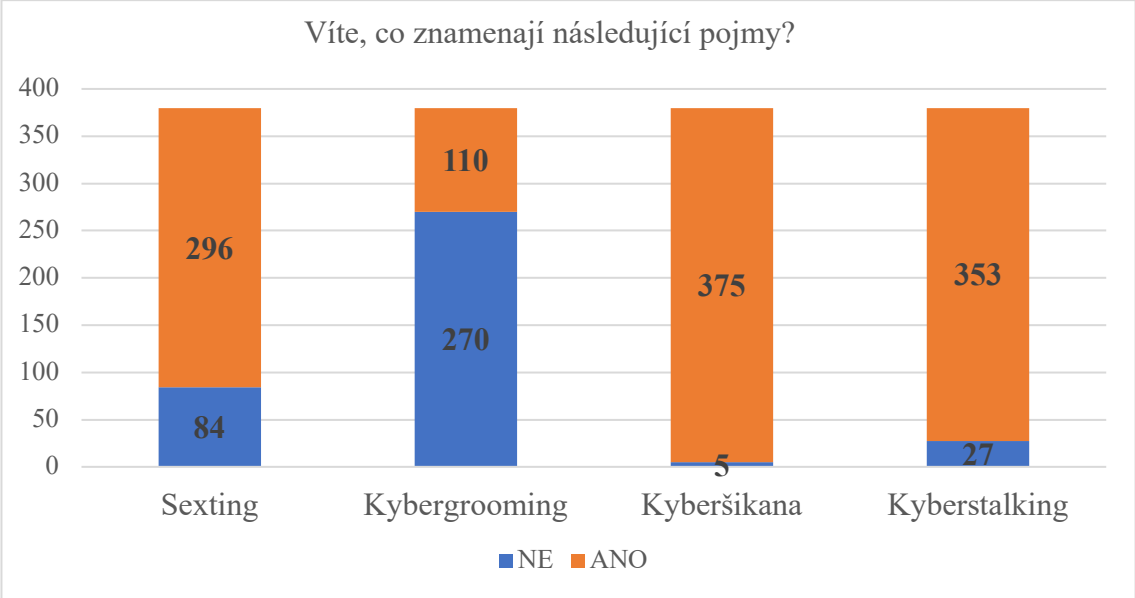
*Graf 14 Jak si rodiče připouští, že by se jejich dítě mohlo stát obětí kybernetické kriminality*[145]




Z grafu č. 14 je zřejmé, že většina rodičů si připouští, že by se zrovna jejich dítě mohlo stát obětí kybernetické kriminality.

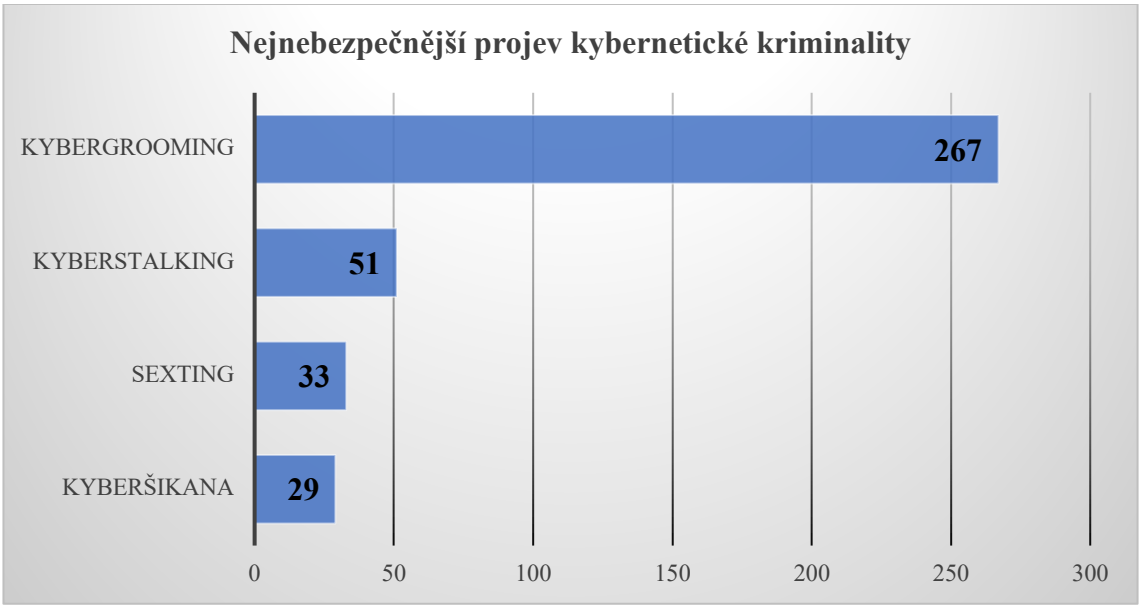
[144] Vlastní zdroj.
[145] Vlastní zdroj.

*Graf 15 Počet rodičů, jež znají daný pojem*[146]




Z uvedených projevů kybernetické kriminality je neznámějším pojmem kyberšikana. Ze všech tázaných ho zná téměř 99 %. Naopak nejméně známým termínem je kybergrooming, který zná pouze 110 (26 %) rodičů.

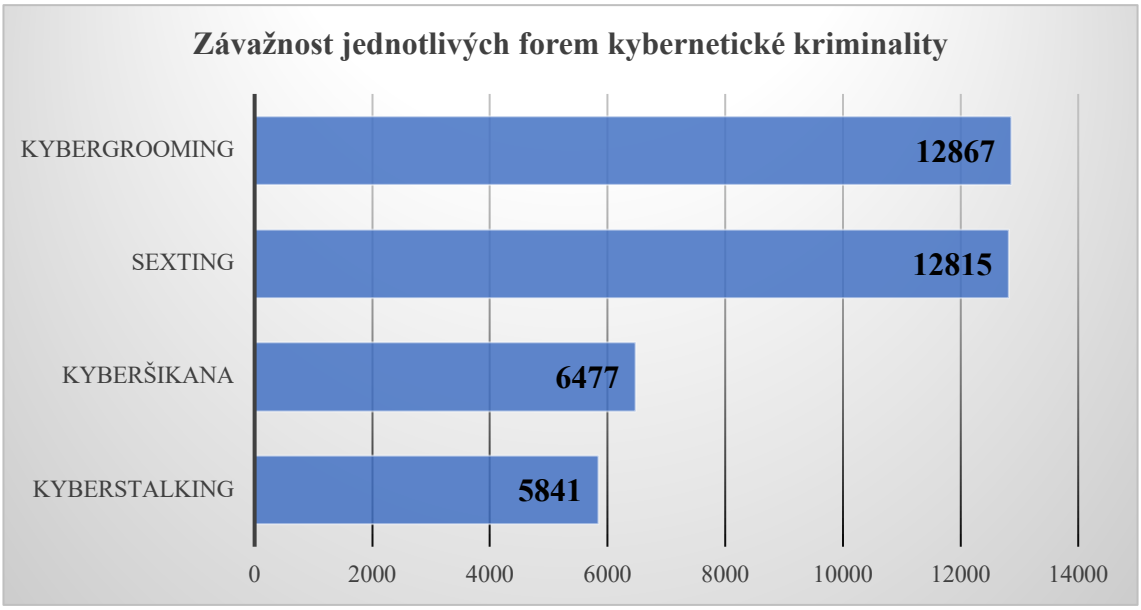
*Graf 16 Nejnebezpečnější projev kyberkriminality páchaná na nezletilých dětech*[147]




Po vysvětlení výše uvedených pojmů je mezi rodiči za nejnebezpečnější projev kybernetické kriminality ve vztahu k nezletilým dětem považován kybergrooming, který zaujímá 70% podíl ze všech responzí.

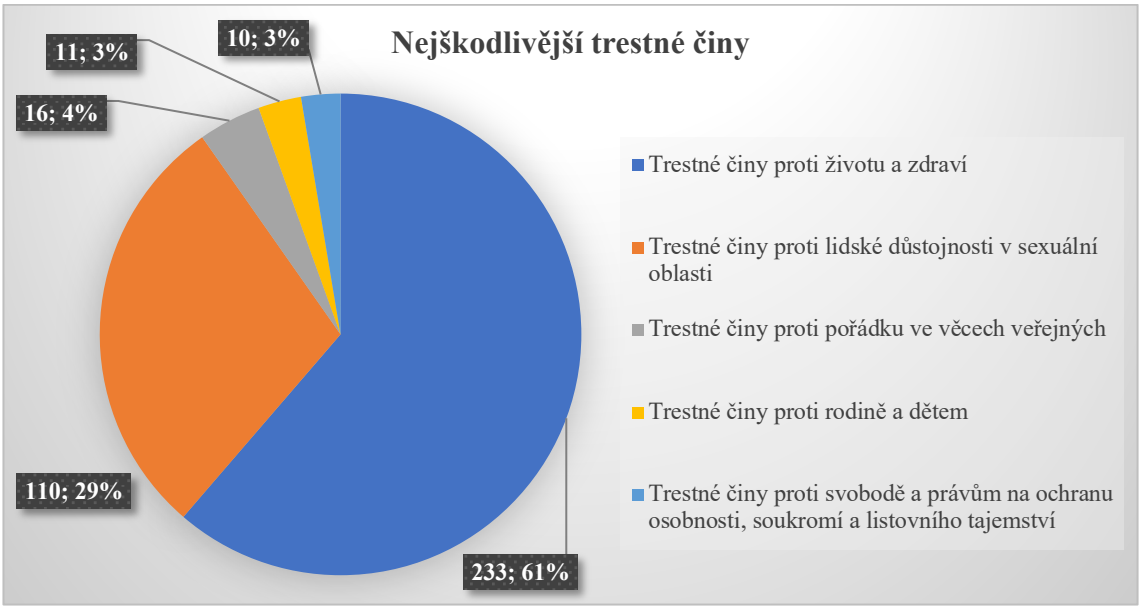
[146] Vlastní zdroj.
[147] Vlastní zdroj.

*Graf 17 Závažnost forem kybernetické kriminality páchané na nezletilých dětech*[148]




Kybergrooming (12867 bodů) a sexting (12815 bodů) je mezi rodiči ohodnocen za nejzávažnější projev kybernetické kriminality ve vztahu k nezletilým dětem.

*Graf 18 Nejškodlivější trestné činy spáchané na nezletilých dětech v souvislosti s kybernetickou kriminalitou*[149]




Trestné činy proti životu a zdraví (např. účast na sebevraždě) jsou mezi rodiči v počtu 233 odpovědí vnímány za nejškodlivější. Naopak Trestné činy proti svobodě a právům na ochranu osobnosti, soukromí a listovního tajemství (např. vydírání, pomluva) v počtu 10 odpovědí představují z možného výběru poslední místo.

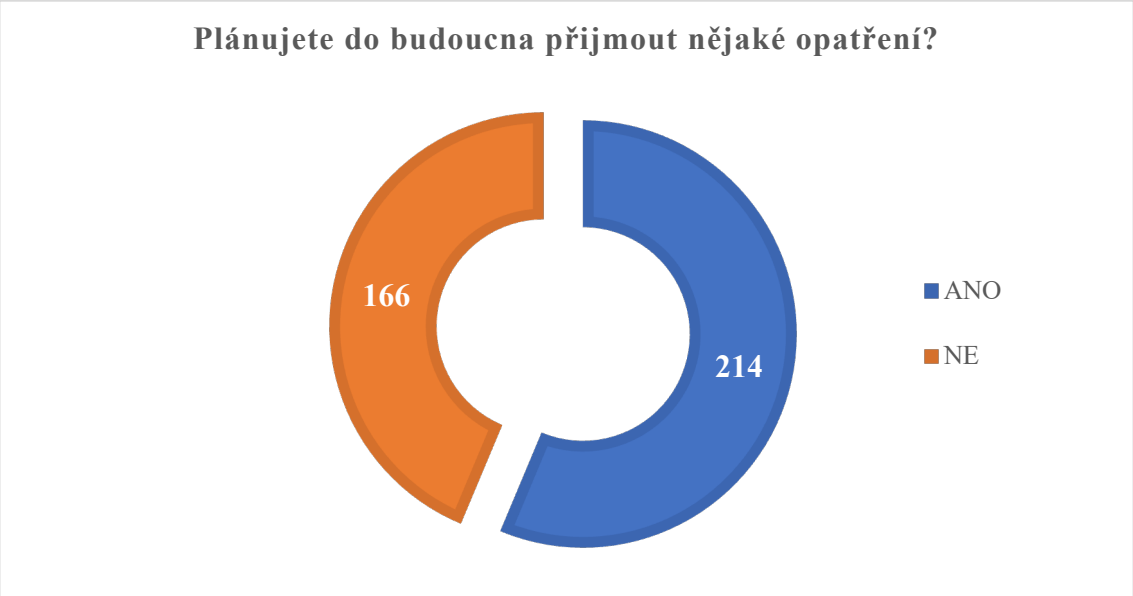
[148] Vlastní zdroj.
[149] Vlastní zdroj.

*Tabulka 5 Přehled realizovaných preventivních opatření*[150]

| Odpověď | Počet | Podíl |
|---|---|---|
| Pravidelná komunikace s nezletilým dítětem o možném nebezpečí, které online prostředí představuje | 272 | 28 % |
| Používání rodičovského zámku – omezení a blokace používání webových stránek | 178 | 18,4 % |
| Kontrola historie vyhledávání na internetu | 157 | 16,2 % |
| Využití dostupných aplikací a programů k monitorování dítěte na internetu | 100 | 10,3 % |
| Provádění situační výchovy a procvičování s dětmi hypotetických scénářů | 99 | 10,2 % |
| Jednorázová edukace a osvěta v dané problematice | 82 | 8,5 % |
| Nezletilé dítě není při používání internetu bez dozoru | 43 | 4,4 % |
| Žádné | 20 | 2,1 % |
| Preventivní opatření řeší jiný člen rodiny | 16 | 1,6 % |
| Jiné | 3 | 0,3 % |

Klíčová tabulka zobrazuje přehled realizovaných preventivních opatření, kdy rodiče měli na výběr výše uvedené možnosti, přičemž mohli označit více opatření. Z odpovědí bylo zjištěno, že nejvíce je k ochraně dětí využívána „pravidelná komunikace s nezletilým dítětem o možném nebezpečí, které online prostředí představuje“.

*Graf 19 Počet rodičů, kteří v budoucnu přijmou opatření proti kyberkriminalitě*[151]




Graf č. 19 zobrazuje počet respondentů, kteří v budoucnu přijmou nějaké opatření, aby snížili riziko viktimnosti dítěte.

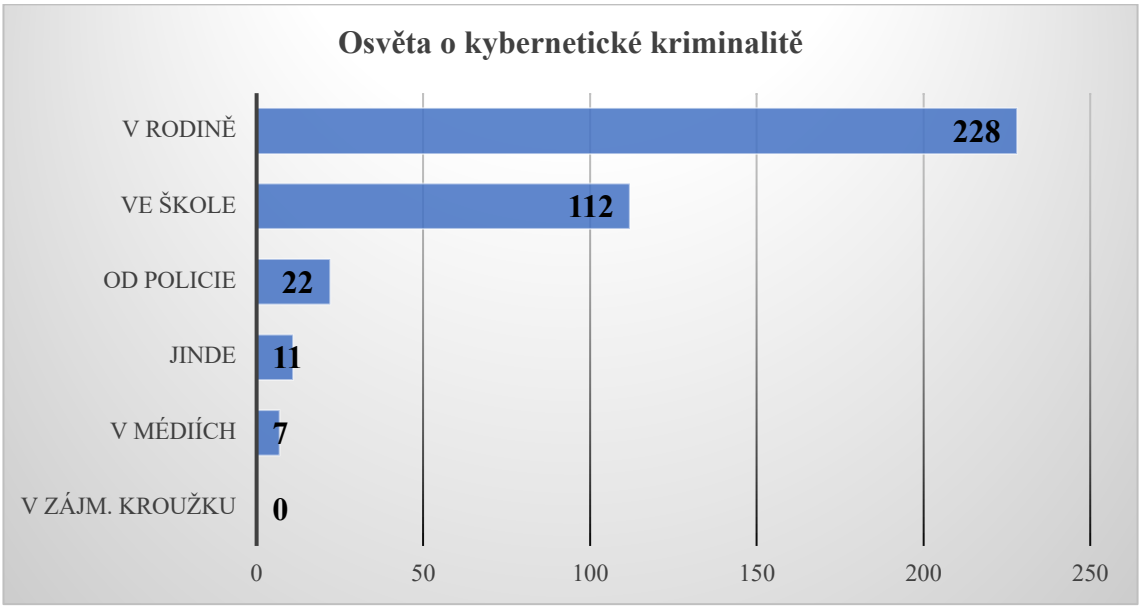
[150] Vlastní zdroj.
[151] Vlastní zdroj.

*Tabulka 6 Přehled do budoucna realizovaných preventivních opatření*[152]

| Odpověď | Počet | Podíl |
|---|---|---|
| Pravidelná komunikace s dítětem | 54 | 27,5 % |
| Používání rodičovského zámku – omezení a blokace používání webových stránek | 46 | 23,5 % |
| Využití dostupných aplikací a programů k monitorování dítěte na internetu | 34 | 17,4 % |
| Kontrola historie vyhledávání na internetu | 19 | 9,7 % |
| Jednorázová edukace a osvěta v dané problematice | 19 | 9,7 % |
| Ještě nevím | 10 | 5,1 % |
| Provádění situační výchovy a procvičování s dětmi hypotetických scénářů | 7 | 3,6 % |
| Zabezpečení zařízení a domácí sítě | 4 | 2 % |
| Omezení času na internetu | 2 | 1 % |
| Nezletilé dítě není při používání internetu bez dozoru | 1 | 0,5 % |

Výše uvedená tabulka zobrazuje přehled preventivních opatření, které rodiče chtějí do budoucna realizovat. Jednalo se o nepovinnou otázku, na kterou přesto odpovědělo 196 rodičů z celkově možných 214, jež v předchozí otázce odpověděli, že do budoucna přijmou nějaké opatření.

*Graf 20 Názor rodičů, kde by měla probíhat osvěta o kybernetické kriminalitě*[153]




Graf č. 20 zobrazuje, že 228 rodičů, respektive 60 % odpovídajících se domnívá, že je to zejména rodina, kde by měla proběhnout osvěta, jak se bezpečně chovat na internetu.

[152] Vlastní zdroj.
[153] Vlastní zdroj.

## 6.5 Výsledky stanovených hypotéz

**H1:** Více jak 30 % respondentů, kterých uvedlo, že se nestali obětí kybernetické kriminality, si nepřipouští, že by se zrovna jejich nezletilé dítě stalo obětí kyberkriminality.

V souvislosti s touto hypotézou byla respondentům položena otázka č. 4: „Stali jste se v minulosti obětí kybernetické kriminality?“ a otázka č. 10: „Připouštíte si, že by se zrovna Vaše dítě mohlo stát obětí kybernetické kriminality?“ Z výsledků vyplývá, že **tato hypotéza se nepotvrdila**, neboť z 332 rodičů, kteří se nestali obětí, si „pouze“ 23 % nepřipouští, že by se jejich dítě stalo obětí kyberkriminality.

**H2:** Respondenti, kteří uvedli, že se setkali s pojmem kybernetická kriminalita, realizují ve větší míře 3 a více opatření než respondenti, kteří uvedli opak.

V souvislosti s touto hypotézou byla respondentům položena otázka č. 3: „Setkali jste se někdy předtím s pojmem kybernetická kriminalita?“ a otázka č. 15: „Jaké máte preventivní opatření ve vztahu k definované kybernetické kriminalitě (aby se dítě nestalo obětí)?“ Z výsledků vyplývá, že **tato hypotéza se potvrdila**, neboť u 167 respondentů z 324, to je 52 %, kteří se setkali s pojmem kybernetická kriminalita, realizují 3 a více opatření, zatímco u respondentů, kteří se s pojmem předtím nesetkali, je to pouhých 17 % rodičů, kteří realizují 3 a více opatření.

# Závěr

Práce se zabývá tématem kybernetická kriminalita páchaná na dětech v Jihočeském kraji. Snaží se najít odpověď na otázku, zda mají rodiče povědomí o kybernetické kriminalitě a jaké mají preventivní opatření, aby ochránili své děti před tímto negativním jevem. Práce se skládá ze dvou částí, teoretické a empirické.

Snahou teoretické části práce bylo zejména vysvětlit, co je kybernetická kriminalita, která patří mezi nejmladší ale zároveň velice dynamické kriminální odvětví, a blíže charakterizovat a specifikovat kyberkriminalitu páchanou na nezletilých dětech. Analýzou a vyhodnocením statistických dat bylo zjištěno, že v České republice je každoročně spácháno řádově od tří do čtyř stovek trestných činů. V Jihočeském kraji se nápad trestné činnosti kybernetické kriminality páchané na nezletilých dětech udržuje kolem jedné desítky, kdy konkrétně v roce 2022 bylo spácháno 11 trestných činů. Jedná se zejména o sexuálně motivované trestné činy, jako např. sexuální nátlak, šíření pornografie, dětská pornografie a zneužití dítěte k ní a navazování nedovolených kontaktů s dítětem. Své místo ve statistikách taktéž zaujímá trestný čin ohrožování výchovy dítěte a vydírání. Z obsahové analýzy literárních a dalších zdrojů vyplývá, že mezi základní projevy řadíme kybergrooming, sexting, kyberšikanu a kyberstalking. Uvedenými metodami bylo dosaženo vedlejšího cíle práce.

Empirická část práce se zabývá zpracováním a vyhodnocením užitého výzkumného (dotazníkového) šetření u rodičů nezletilých dětí v Jihočeském kraji, jejímž prostřednictvím bylo dosaženo hlavního cíle práce.

V rámci interakce s laickou veřejností bylo zjištěno, že rodiče mají ve větší míře povědomí o předmětné kriminalitě, nicméně 15 % respondentů se s tímto pojmem předtím nesetkalo. Téměř 10 % dotázaných sice nebezpečí online prostředí vnímá, nicméně věc sami neřeší, přičemž 20 rodičů (5 %) nemá žádné preventivní opatření. Při analýze dat výzkumného (dotazníkového) šetření bylo dále zjištěno, že 22 % respondentů si nepřipouští, že by se zrovna jejich dítě stalo obětí kybernetické kriminality. Nejméně známým projevem je kybergrooming, avšak po seznámení rodičů s tímto pojmem, je mezi nimi tato forma považována za nejnebezpečnější a nejzávažnější.

Z realizovaného výzkumného (dotazníkového) šetření dále vyplývá, že nejčastějším preventivním opatřením, které rodiče realizují, je pravidelná komunikace s nezletilým dítětem o možném nebezpečí, které online prostředí představuje a používání

rodičovského zámku, respektive omezení a blokace používání webových stránek. Rodiče dále využívají dostupné aplikace a programy k monitorování dítěte na internetu.

Zásadní zjištění je, že více jak 55 % respondentů se chystá do budoucna přijmout další preventivní opatření, kdy mezi těmito je i 19 rodičů z 20, kterých uvedlo, že nemají žádné preventivní opatření. Přínos práce je tedy spatřován už jenom v tom, že se rodiče dozvěděli o možných formách spáchání protiprávního jednání na jejich dětech a o možnostech prevence a snížení viktimnosti dítěte.

Kybernetická kriminalita je negativní jev, se kterým se společnost potýká v posledních desetiletích, a to nejen na území České republiky, ale téměř po celém světě, lépe řečeno všude, kde jsme obklopeni informačními a komunikačními technologiemi, přičemž je nepravděpodobné, že se podaří tento jev vymýtit, ostatně jako i u ostatních druhů kriminalit. Podle názoru autora práce není potřebná významná změna právní úpravy v České republice a ani vytvoření nové právní úpravy, která by se věnovala speciálně kybernetickým trestným činům ve vztahu k nezletilým dětem. V současné době jsou legislativní a represivní opatření dostačující. Z uvedeného důvodu se autor práce domnívá, že boj s kybernetickou kriminalitou páchanou na nezletilých dětech je potřeba vést prostřednictví preventivních opatření, která by primárně zabránila okolnostem přispívajícím ke vzniku tohoto fenoménu.

Cestou ke snížení rizika v online prostředí, respektive užíváním moderních informačních a komunikačních technologií, je minimálně bezesporu prevence ve smyslu základní osvěty, kdy hlavním pilířem pro nezletilé děti by měla být rodina a taktéž vzdělávací zařízení počínaje minimálně základními školami. K vyřešení této problematiky by mohlo pomoci např. více zainteresovat po finanční stránce základní školy a následně se zaměřit na informovanost rodičů prostřednictvím preventivních programů ve školství, např. přednáškami a poradenstvím během třídních schůzek. V dotazníkovém šetření se totiž ukázalo, že rodiče plánují do budoucna přijmout jako opatření, jak chránit své děti před kybernetickou kriminalitou, zejména pravidelnou komunikaci. Tuto je potřeba vést ale jak k dětem, tak i k rodičům. Závěrem je možné doporučit medializovat a připomínat již registrované a objasněné případy, což by mohlo přispět ke zvýšení obecného povědomí o kybernetické kriminalitě páchané na nezletilých dětech.

# Seznam použitých zdrojů

**Literární zdroje**


1. CASEY, E. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet.* 2. edition. London: Academic Press, 2004. 677 s. ISBN 0-12-163104-4.
2. ECKERTOVÁ, L., DOČEKAL, D. *Bezpečnost dětí na Internetu: rádce zodpovědného rodiče.* Brno: Computer Press, 2013. 224 s. ISBN 978-80-251-3804-5.
3. GIBSON, W. *Neuromancer.* New york: Berkley Publishing Group, 1984. 271 s. ISBN 0-441-56958-7.
4. GŘIVNA, T., SCHEINOST, M., ZOUBKOVÁ, I., et al. *Kriminologie.* 5. vydání. Praha: Wolters Kluwer ČR, 2019. 588 s. ISBN 978-80-7598-554-5.
5. HINDLS. R., HOLMAN, R., HRONOVÁ, S., et al. *Ekonomický slovník.* Praha: C. H. Beck, 2003. 620 s. ISBN 80-7179-819-3.
6. HULANOVÁ, L. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. 217 s. ISBN 978-80-7387-545-9.
7. CHROMÝ, J. *Kriminalita páchaná na mládeži: aktuální jevy a nová právní úprava v České republice.* Praha: Linde, 2010. 239 s. ISBN 978-80-7201-825-3
8. JELÍNEK, J., et al. *Kriminologie*. Praha: Leges, 2021. 631 s. ISBN 978-80-7502-499-2.
9. JIRKOVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, 2007. 288 s. ISBN 978-80-247-1561-2.
10. KAISER, G. *Kriminologie.* Praha: C. H. Beck, 1994. 268 s. ISBN 80-7179-002-8.
11. KOHOUT, R. *Internetem Bezpečně.* Karlovy Vary: Biblio Karlovy Vary, 2017. 31 s. ISBN 978-80-270-1148-3.
12. KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z. s. p. o., 2016. 524 s. ISBN 978-80-88168-15-7.
13. KOŽÍŠEK, M., PÍSECKÝ, V. *Bezpečně na internetu: průvodce chováním ve světě online.* Praha: Grada Publishing, 2016. 176 s. ISBN 978-80-247-5595-3.

14. MATĚJKA, M. *Počítačová kriminalita.* Praha: Computer Press, 2002. 106 s. ISBN 80-7226-419-2.
15. MULLER, M. *Jak ochránit děti před pornografií na internetu.* Praha: Portál, 2014. 168 s. ISBN 978-80-262-0694-1.
16. NĚMEC, M., et al. *Teorie a metodologie kriminalistiky pro magisterské studium – I. díl. Aktuální problémy kriminalistické teorie.* Praha: ABOOK, 2018. 491 s. ISBN 978-80-906974-1-6.
17. PORADA, V., et al. *Kriminalistika (teorie, metody, metodologie).* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2014. 459 s. ISBN 978-80-7380-490-9.
18. PORADA, V., STRAUS, J. *Kriminalistické stopy. Teorie, metodologie, praxe.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2012. 506 s. ISBN 978-80-7380-396-4.
19. ROGERS, V. *Kyberšikana: pracovní materiály pro učitele a žáky i studenty.* Praha: Portál, 2011. 104 s. ISBN 978-80-7367-984-2.
20. SMEJKAL, V. *Kybernetická kriminalita.* 3. vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. 1166 s. ISBN 978-80-7380-849-5.
21. SVATOŠ, R. *Kriminologie.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2012. 290 s. ISBN 978-80-7380-389-6.
22. STRAUS, J., et al. *Kriminalistická metodika.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2006. 310 s. ISBN 80-86898-66-0.
23. ŠMAHAJ, J. *Kyberšikana jako společenský problém.* Olomouc: Univerzita Palackého v Olomouci, 2014. 232 s. ISBN 978-80-244-4227-3.
24. ŠVESTKOVÁ, R., SOLDÁN, L., ŘEHKA, M. *Kyberšikana.* České Budějovice: ZSF JU v Českých Budějovicích, 2019. 81 s. ISBN 978-80-7394-752-1.
25. TOMÁŠEK, J. *Úvod do kriminologie: Jak studovat zločin.* Praha: Grada Publishing, 2010. 216 s. ISBN 978-80-247-2982-4.
26. VÁLKOVÁ, H., KUCHTA, J., HULMÁKOVÁ, J., et al. *Základy kriminologie a trestní politiky.* 3. vydání. Praha: C. H. Beck, 2019. 616 s. ISBN 978-80-7400-732-3.
27. VELIKOVSKÁ, M. *Psychologie obětí trestných činů.* Praha: Grada Publishing, 2016. 168 s. ISBN 978-80-247-4849-8.
28. ZOUBKOVÁ, I., et al. *Kriminologický slovník.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2011. 251 s. ISBN 978-80-7380-312-4.

**Elektronické zdroje**


1. *Co je kybergrooming?* [online]. 14.01.2019 [cit. 12.11.2022]. Dostupné z WWW: <https://www.e-bezpeci.cz/index.php/71-trivium/1421-co-je-kybergrooming>.
2. *Co je kyberstalking* [online]. [cit. 15.11.2022]. Dostupné z WWW: <https://vyuka.o2chytraskola.cz/clanek/26/kyberstalking/>.
3. Dětské krizové centrum. O nás. *Ditekrize.cz* [online]. [cit. 15.11.2022]. Dostupné z WWW: <https://www.ditekrize.cz/o-detskem-krizovem-centru/>.
4. HLOUŠKOVÁ, L. Je mi dvanáct aneb 2458 sexuálních predátorů nachytaných V síti. In *Novinky.cz* [online]. Borgis 16.01.2020 [cit. 08.11.2022]. Dostupné z WWW: <https://www.novinky.cz/kultura/filmy-serialy/clanek/je-mi-dvanact-aneb-2458-sexualnich-predatoru-nachytanych-v-siti-40310059>.
5. *Kazuistika* [online]. [cit. 12.11.2022]. Dostupné z WWW: <https://www.sexting.cz>.
6. KOPECKÝ, K., KOŽÍŠEK, M. Fenomén sexting v teorii a praxi (díl 1). In *e-bezpečí.cz* [online]. 01.03.2015 [cit. 12.11.2022]. Dostupné z WWW: <https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/sexting/994-fenomensexting1>.
7. KUBIŠTOVÁ, D. První nepodmíněný trest pro predátora z filmu V síti. ‚Ústečan' má jít na dva roky za mříže. In *iROZHLAS* [online]. Český rozhlas 01.04.2021 [cit. 09.11.2022]. Dostupné z WWW: <https://www.irozhlas.cz/zpravy-domov/v-siti-ustecan-martin-ustecak-usti-nad-labem-soud-rozsudek_2104011325_ako>.
8. MORAVČÍK, O. Vývoj registrované kriminality v roce 2021. *Policie České republiky* [online]. 2021 [cit. 28.10.2022]. Dostupné z WWW: <https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2021.aspx>.
9. RAK, R., PORADA, V. Digitální stopy v kriminalistice a forenzních vědách. *Soudní inženýrství* [online]. 2005, roč. 17, č. 1 [cit. 02.11.2022]. ISSN 1411-443X. Dostupné z WWW: <http://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf>.
10. *Rizika kyberprostoru: průvodce pro děti, rodiče a učitele* [online]. Praha: Dětské krizové centrum, 2017 [cit. 15.11.2022]. Dostupné z WWW: <https://www.ditekrize.cz/app/uploads/2019/10/brozura_prezentace.pdf>.
11. STEJSKAL, T. V síti se lapili směšní i odporní predátoři. Klusákův film ukazuje bezohlednost ve společnosti. In *Hospodářské noviny* [online]. Economia

28.02.2020 [cit. 08.11.2022]. Dostupné z WWW: <https://archiv.hn.cz/c1-66727610-v-siti-se-lapili-smesni-i-odporni-predatori>.

12. VICHLENDA, M. *Kriminalistika* [online]. Karviná, 2011 [cit. 03.11.2022]. Dostupné z WWW: <http://www.sosoom-zlin.cz/media/skripta/kriminalistika.pdf>.
13. VICHLENDA, M., KRČEK, I. *Kriminologie* [online]. Karviná, 2011 [cit. 23.11.2022]. Dostupné z WWW: <https://www.sosoom-zlin.cz/media/skripta/kriminologie.pdf>.

**Legislativní dokumenty**

1. ČESKO. Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů. In *Sbírka zákonů České republiky*. 1993. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/1993-2>.
2. ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In *Sbírka zákonů České republiky*. 2014. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2014-181>.
3. ČESKO. Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád). In *Sbírka zákonů České republiky*. 1961. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/1961-141>.
4. ČESKO. Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů. In *Sbírka zákonů České republiky*. 2009. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2009-40>.

**Ostatní zdroje**

Kromě výše uvedených zdrojů byly při zpracování bakalářské práce využity následující materiály:

- *V síti* [dokument]. Režie Barbora CHALUPOVÁ, Vít KLUSÁK. ČR: Česká televize, 2020.
- Interní zdroj PČR. Statistiky kybernetické kriminality [cit. 25.01.2023]. Data jsou přístupná pro veřejnost na základě žádosti o poskytnutí informací ve smyslu zákona č. 106/1999 Sb., o svobodném přístupu k informacím.

# Seznam tabulek a grafů

# Seznam příloh

# Přílohy

Příloha 1 Formulář dotazníkového šetření

## Kybernetická kriminalita páchaná na dětech v Jihočeském kraji

Dobrý den, věnujte prosím několik minut svého času vyplněním následujícího anonymního dotazníku, jenž se týká kybernetické kriminality páchané na dětech v Jihočeském kraji.

Rodiče jsou významným subjektem ovlivňujícím chování a jednání dítěte, kdy neznalost potenciálních rizik v online prostředí může být kriminogenním faktorem s rizikovým potenciálem zvyšovat viktimnost dítěte. Cílem výzkumu je zjistit, jak rodiče nezletilých dětí vnímají rizika online prostředí s explicitním zaměřením na konkrétní formy kyberkriminality.

**Dotazník je určen pro rodiče nezletilých dětí, které nedovršily 15. rok věku navštěvující základní školy v Jihočeském regionu**.

Pro účely tohoto výzkumu je za nezletilé dítě považováno tedy každé dítě, které nedovršilo 15. rok věku.

Děkuji za vyplnění dotazníku. Martin Valert

### 1 Jaké je Vaše pohlaví?

◯ Muž ◯ Žena

### 2 Do jaké věkové kategorie spadáte?

◯ do 25 let ◯ 26 - 35 let ◯ 36 - 45 let ◯ 46 - 55 let ◯ 56 let a více

### 3 Setkali jste se někdy předtím s pojmem kybernetická kriminalita?

Nápověda k otázce: *Kybernetickou kriminalitu lze jednoduše charakterizovat jako protiprávní jednání, ke kterému dochází v kyberprostoru. Jedná se tedy o souhrn spáchaných trestných činů v určitém prostředí. V současné době je převážná část kybernetické kriminality páchána prostřednictvím internetu. Charakteristické pro kybernetickou kriminalitu je zejména vysoká míra latence.*

◯ Ano ◯ Ne

### 4 Stali jste se v minulosti obětí kybernetické kriminality?

◯ Ano ◯ Ne

### 5 Užívá Vaše dítě informační a komunikační technologie?

Nápověda k otázce: *Informační a komunikační technologie zahrnují veškeré informační technologie pro komunikaci a informatiku, např. PC, notebook, mobilní telefon, tablet apod. Tedy zda Vaše nezletilé dítě používá např. internet, sociální sítě, zařízení na hraní her apod.*

◯ Ano ◯ Ne

---

6 Jak vnímáte nebezpečí v online prostředí, které hrozí nezletilým dětem?

Nápověda k otázce: *Vyberte jednu odpověď*

☐ Nebezpečí vnímám, ale neřeším to ☐ Nebezpečí vnímám a mám preventivní opatření ☐ Nebezpečí nevnímám ☐ Nebezpečí neexistuje

7 Kolik registrovaných trestných činů je podle Vás ročně spácháno na nezletilých dětech v ČR v souvislosti s kybernetickou kriminalitou?

Nápověda k otázce: *Vyberte jednu odpověď*

◯ 0 až 100 ◯ 101 až 200 ◯ 201 až 300 ◯ 301 až 400 ◯ 401 a více

8 Jaká je dle Vašeho názoru objasněnost registrovaných trestných činů spáchaných na nezletilých dětech v ČR v souvislosti s kybernetickou kriminalitou?

Nápověda k otázce: *Vyberte jednu odpověď*

◯ Do 20% ◯ 21 až 40% ◯ 41 až 60% ◯ 61 až 80% ◯ 81 až 100%

9 Kolik registrovaných trestných činů je podle Vás ročně spácháno na nezletilých dětech v Jihočeském kraji v souvislosti s kybernetickou kriminalitou?

Nápověda k otázce: *Vyberte jednu odpověď*

◯ 0 až 10 ◯ 11 až 20 ◯ 21 až 30 ◯ 31 až 40 ◯ 41 a více

10 Připouštíte si, že by se zrovna Vaše dítě mohlo stát obětí kybernetické kriminality?

◯ Ano ◯ Ne

11 Víte, co znamenají následující pojmy?

Nápověda k otázce: *Vyberte jednu odpověď v každém řádku*

| | ANO | NE |
|---|---|---|
| Sexting | ◯ | ◯ |
| Kybergrooming | ◯ | ◯ |
| Kyberšikana | ◯ | ◯ |

| | | |
|---|---|---|
| Kyberstalking | ◯ | ◯ |

## 12 Jaký z těchto projevů kybernetické kriminality páchané na nezletilých dětech považujete za nejnebezpečnější?

◯ Sexting – spočívá v zasílání textových zpráv, fotografií či videí se sexuálním obsahem

◯ Kybergrooming – označuje chování predátorů, jež má prostřednictvím internetu v oběti vyvolat falešnou důvěru a přimět ji k osobnímu setkání, kdy jí chce ublížit nebo ji chce sexuálně zneužít

◯ Kyberšikana – lze charakterizovat jako úmyslné, nepřátelské chování, které se opakuje, jehož cílem je ublížit oběti za použití informačních a komunikačních technologií

◯ Kyberstalking – označuje jednání, které spočívá v opakovaném kontaktování oběti, přičemž útoky agresorů se zpravidla stupňují a většinou vyvolá u oběti obavy o svoje soukromí, zdraví či život

## 13 Ohodnoťte závažnost jednotlivých forem kybernetické kriminality páchané na nezletilých dětech.

Nápověda k otázce: *Rozdělte následujících 100 bodů mezi níže uvedené formy, přičemž více bodů znamená větší závažnost.*

Rozdělte: 100 bodů

| | |
|---|---|
| Sexting | |
| Kybergroomig | |
| Kyberšikana | |
| Kyberstalking | |

## 14 Jaké z těchto trestných činů spáchaných na nezletilých dětech ve vztahu ke kybernetické kriminalitě považujete za nejškodlivější?

Nápověda k otázce: *Vyberte jednu odpověď*

◯ Trestné činy proti lidské důstojnosti v sexuální oblasti (např. sexuální nátlak, šíření pornografie)

◯ Trestné činy proti životu a zdraví (např. účast na sebevraždě)

◯ Trestné činy proti svobodě a právům na ochranu osobnosti, soukromí a listovního tajemství (např. vydírání, pomluva)

◯ Trestné činy proti rodině a dětem (např. ohrožování výchovy dítěte)

◯ Trestné činy proti pořádku ve věcech veřejných (např. nebezpečné vyhrožování, nebezpečné pronásledování)

## 15 Jaké máte preventivní opatření ve vztahu k definované kybernetické kriminalitě (aby se dítě nestalo obětí)?

Nápověda k otázce: *Vyberte jednu nebo více odpovědí*

- ☐ Žádné
- ☐ Používání rodičovského zámku – omezení a blokace používání webových stránek
- ☐ Kontrola historie vyhledávání na internetu
- ☐ Provádění situační výchovy a procvičování s dětmi hypotetických scénářů (např. simulovat, co by dělalo v případě kyberšikany apod.)
- ☐ Jednorázová edukace a osvěta v dané problematice
- ☐ Využití dostupných aplikací a programů k monitorování dítěte na internetu
- ☐ Pravidelná komunikace s nezletilým dítětem o možném nebezpečí, které online prostředí představuje
- ☐ Nezletilé dítě není při používání internetu bez dozoru
- ☐ Preventivní opatření řeší jiný člen rodiny
- ☐ Jiné

## 16 Plánujete do budoucna přijmout nějaké opatření?

Nápověda k otázce: *Vyberte jednu odpověď*

◯ Ano ◯ Ne

## 17 Pokud ano, uveďte jaké:

## 18 Kde by se podle Vás mělo nezletilé dítě zejména dozvědět, jak by se mělo bezpečně chovat na internetu?

Nápověda k otázce: *Vyberte jednu odpověď*

◯ Ve škole ◯ Od policie ◯ V rámci zájmových kroužků ◯ V médiích ◯ V rodině

◯ Jinde