POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostního managementu

Katedra managementu a informatiky

Kyberkriminalita v sociálních sítích

Diplomová práce

Cybercrime in social networks
Masters thesis

VEDOUCÍ PRÁCE
PhDr. Mgr. Eliška Jonášová, Ph.D.

AUTOR PRÁCE
Bc. Jiřina Karevová

PRAHA
2022

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

V Praze dne

Bc. Jiřina Karevová

ANOTACE

Tématem práce je stále aktuálnější a závažnější problém počítačové kriminality, a to zvláště na sociálních sítích. V práci jsou popsány jak nejrozšířenější sociální sítě (Facebook/Meta, YouTube, Instagram, Tweeter, VKontakte, imageboardy, TikTok), tak jednotlivé typy kyberkriminality, které se na těchto sociálních sítích nejvíce vyskytují (kyberšikana, kyberstalking, kybergrooming, krádež identity, šíření poplašné zprávy, sexting, sextortion). Podrobněji se pak práce zabývá problematikou dětské pornografie na sociálních sítích. V rámci praktické části této práce bylo dotazníkovým šetřením zjišťováno, nakolik jsou běžní uživatelé seznámeni se základními pojmy v této oblasti a nakolik jsou schopni vyhodnotit a reagovat na tyto jevy, pokud se s nimi na sociálních sítích setkají. Z vyhodnocení dotazníkového výzkumu pak vyplývá, že existuje prostor pro zlepšení jak na úrovni osvěty, tak na úrovni činnosti státních orgánů.

KLÍČOVÁ SLOVA

Kyberkriminalita, sociální sítě, kyberšikana, kyberstalking, kybergrooming, krádež identity, sexting, sextortion, dětská pornografie

ANNOTATION

The topic of the thesis is the increasingly current and serious problem of cybercrime, especially on social networks. The thesis describes both the most widespread social networks (Facebook/Meta, YouTube, Instagram, Tweeter, VKontakte, imageboardy, TikTok) and the specific types of cybercrime that are most commonly encountered on these social networks (cyberbullying, cyberstalking, cybergrooming, identity theft, spreading of false alarms, sexting, sextortion). The thesis deals in more detail with the issue of child pornography on social networks. As practical part of this thesis, a questionnaire survey was conducted to find out to what extent ordinary users are acquainted with the basic concepts in this area and to what extent they are able to evaluate and respond to these phenomena should they encounter them on social networks. The evaluation of the questionnaire survey shows that there is room for improvement both at the level of rising of public awareness and at the level of activity of state authorities.

KEYWORDS

Cybercrime, social networks, cyberbullying, cyberstalking, cybergrooming, identity theft, sexting, sextortion, child pornography

Obsah

Úvod ... 6
1 Vymezení základních pojmů ... 8
1.1 Kyberprostor ... 8
1.2 Internet ... 9
1.2.1 Využití internetu ... 11
1.2.2 Darknet a Clearnet ... 12
1.2.3 Onion routing a Tor ... 12
1.3 Kyberkriminalita ... 13
1.4 Sociální sítě ... 14
2 Sociální sítě ... 16
2.1 Statistiky používání sociálních médií ... 18
2.2 Facebook/Meta ... 19
2.2.1 Podmínky založení účtu na Facebooku ... 20
2.2.2 Aféry spojené se společností Facebook ... 21
2.3 YouTube ... 24
2.4 Instagram ... 24
2.5 Twiter ... 26
2.6 VKontakte ... 27
2.6.1 Podmínky založení účtu VK ... 27
2.7 Imageboardy ... 28
2.8 TikTok ... 29
2.8.1 Známá rizika užívání sítě TikTok ... 30
3 Kyberkriminalita na sociálních sítích ... 32
3.1 Kyberšikana ... 33
3.1.1 Rozdíl mezi tradiční šikanou a kyberšikanou ... 34
3.1.2 Nejčastější projevy kyberšikany ... 36
3.1.3 Kyberšikana a právo ... 37
3.2 Kyberstalking ... 38
3.2.1 Pachatelé kyberstalkingu ... 38
3.2.2 Typy stalkerů ... 39
3.2.3 Motivace stalkerů ... 39
3.2.4 Třífázový model vývoje stalkingu ... 39
3.2.5 Typické projevy nebezpečného pronásledování ... 40
3.2.6 Demonstrování moci a síly stalkera ... 40
3.2.7 Destrukce věcí oběti ... 41
3.2.8 Stalker se vydává za oběť ... 41

3.2.9 Snaha poškodit reputaci oběti stalkerem 41
3.2.10 Kyberstalking a právo 41
3.3 Kybergrooming 42
3.3.1 Kde ke kybergroomingu dochází? 43
3.3.2 Kdo jsou pachatelé 43
3.3.3 Kdo jsou oběti 44
3.3.4 Kybergrooming a právo 44
3.4 Krádež identity 45
3.4.1 Krádež identity a právo 46
3.5 Šíření poplašné zprávy 46
3.5.1 Šíření poplašné zprávy a právo 47
3.6 Sexting 47
3.6.1 Sexting a právo 48
3.7 Sextortion 49
4 Definice dítěte 50
4.1 Definice dětské pornografie 50
4.2 Dětská pornografie a právo 51
4.2.1 Mezinárodněprávní úprava 51
4.2.2 Úprava v právu Evropské unie 53
4.2.3 Úprava ve vnitrostátním právu 54
5 Internet a dětská pornografie 56
5.1 Dítě jako oběť, ale i osoba, která zprostředkovává dětskou pornografii 56
5.2 Fotografie na sociálních sítích 57
6 Rodičovská kontrola aktivit dětí na počítači, tabletu či mobilním telefonu 59
6.1 Operační systém Windows a MacOS 59
6.2 Mobilní zařízení 60
6.3 Software třetích stran 60
7 Vlastní dotazníkový průzkum 62
7.1 Vyhodnocení dotazníku 63
7.2 Závěrečná analýza dotazníku 71
8 Závěr 73
Seznam použité literatury 76

Úvod

„*Kyberkriminalita se na internetu skrývá za maskou anonymity a nepotřebuje přímý fyzický přístup ke svým obětem na to, aby způsobila nepředstavitelnou újmu*.“ — Anna Maria Chavez[1]

Dříve tak běžný mezilidský kontakt se dnes ve velké míře přesouvá na internet. Vznikají sociální sítě, které přímý lidský kontakt v určitých oblastech zcela nahradily. Díky sociálním sítím se celý svět propojil. Mohou spolu komunikovat lidé z různých států, různého vyznání či sociálních skupin. Díky těmto skutečnostem se se sociálními sítěmi setkáváme téměř na každém našem kroku, a to nejen na internetu, ale už i v reálném životě. To, že máme založený profil na nějaké sociální síti, se stává samozřejmostí a v některých kruzích dokonce společenskou povinností.

Obrovský rozmach informačních technologií v posledních letech s sebou přináší i mnoho problémů ve všech oblastech života, právo nevyjímaje. Právě právo by mělo hrát hlavní roli v otázce bezpečnosti všech informačních technologií. Vyspělost a rozvoj technologií se neustále zrychlují a vyvíjí, sociální sítě se stávají masovou a velice oblíbenou záležitostí. Vytváří se obrovský prostor pro lidskou tvořivost. Na sociálních sítích se lidé nejenom realizují, ale hledají rozptýlení, zábavu, přátele, partnery, sdílejí pocity, postoje, osobní zážitky, fotografie. Mít založený profil na sociální síti je mezi mládeží a mladými lidmi takřka automatické. Tato skutečnost kromě svých výhod přináší ale i nevýhody, a dokonce mnohdy závažné problémy. Kromě toho, že se ztrácí a eliminují osobní kontakty, vzniká také obrovský prostor pro systém, který se vyvíjí velice rychle a právo není schopno reagovat natolik pružně a efektivně, natož ho regulovat. Vzniká i závislost, kterou je možné srovnat s jinými závislostmi, jako jsou například alkoholismus, narkomanie atd. Počítačová kriminalita je velmi široký pojem, zasahuje téměř do všech oblastí života a je obtížné ho obsáhnout jako celek.

---

[1] SOCIAL MEDIA PLATFORMS AND CYBER CRIME - The Daily Guardian. Latest News | Today's News | Breaking News & India News - The Daily Guardian [online]. Copyright © 2020 TheDailyGuardian [cit. 09.02.2022]. Dostupné z: https://thedailyguardian.com/social-media-platforms-and-cyber-crime/

Kyberkriminalita přímo souvisí a počítá s lidskou otevřeností na sociálních sítích. Aniž bychom si to mnohdy uvědomili, poskytujeme ze svého soukromí cenné údaje a informace osobám, které je mohou využít a zneužít v náš neprospěch. Obětí kyberzločinů stále přibývá a přibližně 2/3 uživatelů sociálních sítí se s ním setkaly a byly postiženy. Kyberkriminalita je problém, který si zaslouží podrobnou analýzu a charakteristiku způsobů ochrany a řešení tohoto problému.

Cílem mé práce je zdůraznit nebezpečnost počítačové kriminality na sociálních sítích a ukázat stále větší vliv a působení sociálních sítí v běžném životě. Objasním základní pojmy kyberkriminality, vysvětlím, co znamenají sociální sítě jako takové a jaké nejčastější sociální sítě používáme a popíši nejrozšířenější druhy kyberkriminality. Protože jedním z nejzávažnějších druhů kyberzločinu je šíření dětské pornografie, nejvíce se zaměřím právě na tuto problematiku, a to konkrétně na sociálních sítích, na něž se šíření dětské pornografie stále více přesouvá a na nichž je díky jejich anonymitě zvýšeně nebezpečné. V neposlední řadě analyzuji dotazník, který jsem vytvořila pro běžné uživatele internetu s cílem zmapovat jejich znalosti o problematice dětské pornografie a sociálních sítí.

1 Vymezení základních pojmů

Pro pochopení problematiky kybernetické kriminality na sociálních sítích je potřeba nejdříve uvést výčet těch nejzákladnějších pojmů, které užívám ve své diplomové práci. Pokusím se o jejich popis a objasním jejich význam.

1.1 Kyberprostor

Pojem kyberprostor byl poprvé použit Williamem Gibsonem v povídce „Burning Chrome“ v roce 1982. Dále termín Gibson více rozvedl v románu Neuromancer, kde je kyberprostor definován takto: „*Kyberprostor. Sdílená halucinace každý den pociťovaná miliardami oprávněných operátorů všech národů, dětmi, které se učí základům matematiky…Grafická reprezentace dat abstrahovaných z bank všech počítačů lidského systému. Nedomyslitelná komplexnost. Linie světla seřazené v neprostoru mysli, shluky a souhvězdí dat. Jako světla města, ustupující*…“[2]

Aktuální znění definice kyberprostoru podle zákona o kybernetické bezpečnosti je: „digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací“.[3]

Kyberprostor je označení pro virtuální počítačový svět, konkrétně elektronické médium, které se používá k usnadnění online komunikace. Kyberprostor je tedy místo, kde mohou uživatelé sdílet různé informace, vyměňovat si nápady, komunikovat, hrát hry a zapojovat se do různých sociálních fór. Mohou zde podnikat a věnovat se různým aktivitám. Globální obsah lze použít pro různé účely, které mohou zahrnovat zábavu, vzdělávání, ale i například obchod. To, co dělá a vytváří lidská společnost, je to, co definuje kyberprostor.[4]

---

[2] Neurčité sny a sdílené halucinace - Lupa.cz. *Lupa.cz - server o českém Internetu* [online]. Copyright © 1998 [cit. 11.02.2022]. Dostupné z: https://www.lupa.cz/clanky/neurcite-sny-a-sdilene-halucinace/

[3] § 2 písm. a) zákona č. 181/2014 Sb., o kybernetické bezpečnosti.

[4] What is Cyberspace? - Definition from Techopedia. Techopedia: Educating IT Professionals To Make Smarter Decisions [online]. Copyright © 2022 [cit. 12.02.2022]. Dostupné z: https://www.techopedia.com/definition/2493/cyberspace

V dnešní době je kyberprostor neodmyslitelnou součástí lidského života. Ulehčuje práci a usnadňuje život všem. S jeho výhodami však přichází i některé strasti. Snadné vykonávání práce prostřednictvím kyberprostoru způsobilo také některé vážné problémy s osobní bezpečností a ochranou jednotlivce. Roste počet incidentů spojených s kybernetickou kriminalitou, která je na vzestupu. Falešné hovory, hackerské útoky a online podvody se nyní staly každodenní záležitostí. A právě kyberprostor je jejich dějištěm.

Kvůli neregulovanému a nekontrolovanému rozvoji internetu jsou nyní lidé vystaveni mnoha druhům nežádoucích nebezpečí. Děti jsou na internetu vystaveny nevhodnému obsahu, ke kterému mají snadný přístup. Mohou hrát nevhodné hry, které mají tendenci ovlivňovat jejich mysl. Kyberprostor zvyšuje neproduktivní práci, což následně vede k plýtvání časem. Ovlivňuje také duševní a fyzické zdraví. Dlouhé vysedávání před obrazovkou počítače nebo televize má vážný dopad na zdraví.[5]

Je však potřeba podotknout, že ne vše je špatné, že výhod, které kyberprostor nabízí, je více než dost a že je velice nezbytný pro růst a rozvoj komunity. Při používání kyberprostoru je však třeba dbát na přiměřenou opatrnost a bezpečnostní opatření. Vláda by se také měla zapojit a přijmout vhodná opatření, aby nedocházelo ke zneužívání kyberprostoru a aby mohl být využíván ke zlepšení lidské společnosti.[6]

1.2 Internet

Definice internetu podle prof. Soni Makulové z Filosofické fakulty Masarykovy univerzity v Brně: *„Internet je komplexní globální síť skládající se z tisíce dalších nezávislých sítí, které jsou provozované vládními agenturami,*

[5] How Does Excessive Use Of Electronic Devices Affect The Mental Health Of Kids?. Get Latest News, India News, Breaking News, Today's News - NDTV.com [online]. Copyright © COPYRIGHT NDTV CONVERGENCE LIMITED 2022. ALL RIGHTS RESERVED. [cit. 12.02.2022]. Dostupné z: https://www.ndtv.com/health/how-does-excessive-use-of-electronic-devices-affect-the-mental-health-of-kids-2753503

[6] What is Cyberspace? - Definition from Techopedia. Techopedia: Educating IT Professionals To Make Smarter Decisions [online]. Copyright © 2022 [cit. 27.01.2022]. Dostupné z: https://www.techopedia.com/definition/2493/cyberspace

výchovně-vzdělávacími a výzkumnými institucemi a soukromými obchodními společnostmi.“[7]

Internet je nejdůležitějším nástrojem a významným zdrojem, který využívá téměř každý člověk po celém světě. Propojuje miliony počítačů, webových stránek, webů a serverů. Pomocí internetu můžeme posílat e-maily, fotografie, videa a zprávy svým blízkým. Jinými slovy, internet je rozsáhlá propojená síť počítačů a elektronických zařízení (podporujících internet). Vytváří komunikační médium pro sdílení a získávání informací online. Pokud je vaše zařízení připojeno k internetu, máte přístup ke všem aplikacím, webovým stránkám, aplikacím sociálních médií a mnoha dalším službám. Internet je v dnešní době považován za nejrychlejší médium pro odesílání a přijímání informací.

Internet je ovšem také prostředek k páchání kybernetických trestných činů. K trestné činnosti páchané na dětech dochází ve velké míře prostřednictvím médií, kterými jsou zejména sociální sítě, webové stránky, elektronická pošta (e-mail), chatovací místnosti nebo služby pro okamžité zasílání zpráv.[8]

Internet vznikl v roce 1960 vytvořením prvního funkčního modelu nazvaného ARPANET (Advanced Research Projects Agency). Umožňoval práci více počítačů v jedné síti, což byl v té době jejich největší úspěch. ARPANET využíval přepínání paketů ke komunikaci více počítačových systémů v rámci jedné sítě. V říjnu 1969 byla pomocí sítě ARPANET přenesena první zpráva z jednoho počítače do druhého. Poté se technologie dále rozvíjela.[9]

Československo se oficiálně připojilo k internetu 13. února 1992. Tato událost se uskutečnila v posluchárně ČVUT pod vedením týmu expertů elektrotechnické fakulty. Připojení se zprovoznilo díky pronajatému pevnému telefonnímu okruhu. Ten vedl z dejvického kampusu ČVUT do výpočetního centra Univerzity Jana Keplera v rakouském Linci.[10]

---

[7] Definice Internetu. Home [online]. Dostupné z: http://ijs.8u.cz/index.php/internet/definice-internetu

[8] ČERNÁ, Alena. Kyberšikana: průvodce novým fenoménem. Praha: Grada, 2013. Psyché (Grada). ISBN 978-80-247-4577-0, str. 28

[9] What is Internet? Definition, Uses, Working, Advantages and Disadvantages - GeeksforGeeks. GeeksforGeeks | A computer science portal for geeks [online]. Dostupné z: https://www.geeksforgeeks.org/what-is-internet-definition-uses-working-advantages-and-disadvantages/

[10] Internet v Česku slaví 25 let, jako první se připojil tunový počítač - Deník.cz. Deník.cz - informace, které jsou vám nejblíž [online]. Copyright © [cit. 12.02.2022]. Dostupné z:

Československo bylo 39. zemí, která se tehdy připojila k internetu. Internet na počátku devadesátých let nebyl otevřeným prostředím. S připojením musela souhlasit americká agentura National Science Foundation (NSF), která provozovala a finančně zastřešovala v té době jedinou páteřní síť internetu. Výhradní podmínkou připojení bylo akademické využití, komerční provoz nebyl možný.[11]

V roce 1996 došlo díky dohodě rektorů k mnohem většímu rozmachu internetu, vzniklo sdružení CESNET. Zhruba v polovině devadesátých let se internet začal už otevírat i komerčním účelům a soukromým osobám. Největší internetová firma v České republice je Seznam.cz.[12]

1.2.1 Využití internetu

Obecně lze internet využít ke komunikaci na velké i malé vzdálenosti, ke sdílení informací z jakéhokoliv místa na světě a k získání informací nebo odpovědí na téměř jakoukoliv otázku během několika okamžiků.

Internet se dá využít především k přístupu na sociální média a sdílení obsahu na jejich stránkách, dále jde o formu komunikace přes e-mail, nebo videokonferenci, nebo například internetové telefonování (FaceTime), další možností je vzdělávání se a sebezdokonalování se pomocí přístupu k online studijním programům, seminářům, kurzům apod. Internet je také vhodným místem pro vyhledávání volných pracovních míst. Je to místo, kde se dá hrát online hry, kde se může volně diskutovat, seznamovat se, dají se tu číst elektronické knížky a časopisy, nebo se může provádět výzkum a v neposlední řadě je to místo kde se dá online nakupovat.[13]

---

https://www.denik.cz/ekonomika/internet-v-cesku-slavi-25-let-jako-prvni-se-pripojil-tunovy-pocitac-20170214.html

[11] Tamtéž.

[12] Tamtéž.

[13] What is the Internet? Definition from WhatIs.com.. Computer Glossary, Computer Terms - Technology Definitions and Cheat Sheets from WhatIs.com - The Tech Dictionary and IT Encyclopedia [online]. Dostupné z: https://whatis.techtarget.com/definition/Internet

1.2.2 Darknet a Clearnet

Darknet je součástí takzvaného Deepwebu, tedy části internetu, jejíž stránky nejsou indexovány. Jednoduše to znamená, že internet lze rozdělit na dvě části, Clearnet a Deepweb. Clearnet tvoří všechny stránky, které lze najít pomocí běžných vyhledávačů, jako je například Google. Deepweb je vše ostatní, to znamená všechny stránky, které nelze najít pomocí běžných vyhledávačů. Sítě v rámci Deepwebu tvoří Darknet. Do těchto sítí lze však vstoupit pouze prostřednictvím speciálních přístupových bodů. Data jsou v těchto sítích při předávání šifrována.

Na rozdíl od sítě Clearnet, kde lze shromažďovat veškerá data uživatelů (např. odesílatele a příjemce zpráv), je v Darknetu možné posílat zprávy anonymně. Darknet je svobodnější, takřka necenzurovaný, protože díky anonymním serverům a šifrovanému přístupu není možná cenzura. To činí z darknetu nekontrolovatelnou oblast internetu.

Na jedné straně to nabízí vhodnou platformu pro nelegální aktivity, na straně druhé se na darknetu mohou anonymně a nekontrolovatelně pohybovat lidé, kteří například z důvodu cenzury internetu té dané země nemohou získat a vyměňovat si informace.

Tato technologie, stejně jako jakákoliv jiná, není sama o sobě plošně negativní, jelikož jen společnost rozhoduje o tom, co s touto technologií udělá a jak ji využije.[14]

1.2.3 Onion routing a Tor

Pro přístup do Darknetu nestačí obyčejný prohlížeč, je zapotřebí mít jako doplněk pro anonymizaci aplikaci s názvem Tor. Tato aplikace může být nainstalována do prohlížeč Firefox během několika sekund.

Onion routing je vlastně složitá technika pro anonymizaci, která dokáže přepravit data díky řadě stále se měnících a šifrovacích proxy serverů.

---

[14] Clearnet, Deepweb, Darknet – OTH Amberg-Weiden. OTH Amberg-Weiden [online]. Dostupné z: https://www.oth-aw.de/informieren-und-entdecken/aktuelles/neuigkeiten/201612203660-clearnet-deepweb-darknet/

Darknet neobsahuje klasické URL adresy, pro přístup na požadované webové stránky je potřeba znát a následně i zadat speciální kombinaci čísel a písmen a je potřeba znát příponu neboli onion. Díky neustálé změně těchto adres, je přístup k vybraným zdrojům a adresám pokaždé jiný.[15]

1.3 Kyberkriminalita

Dle výkladového slovníku *„Kyberkriminalita zahrnuje všechny trestné činy provedené pomocí nebo v kontextu počítačů a kybernetické infrastruktury, tedy nejen hacking, phishing atd., ale také kriminální chování na internetu, včetně trestného chování na sociálních sítích. Naproti tomu za kybernetický útok se obvykle považuje pouze napadení počítače nebo infrastruktury, často spojené s neoprávněným přístupem k určitým datům.*“[16]

Kolouch a Bašta definují kybernetický útok jako *„jednání útočníka nebo skupiny útočníků, které využívá informační a komunikační infrastrukturu, ať už s cílem narušit dostupnost, důvěrnost nebo integritu dat“.*[17]

Kyberkriminalita, nazývaná také počítačová kriminalita, je použití počítače jako nástroje k dosažení nezákonných cílů, jako je páchání podvodů, šíření dětské pornografie, porušování práv k duševnímu vlastnictví, krádež identity nebo narušení soukromí, šíření xenofobie a podpora hnutí prosazujících omezení základních práv a svobod atd. Kyberkriminalita, zejména prostřednictvím internetu a sociálních sítí, nabývá na významu s tím, jak se počítač a internet staly ústředními prvky obchodu, zábavy a státní správy.

Nové technologie vytváří nové kriminální příležitosti, ale jen málo nových druhů trestné činnosti. Čím se kyberkriminalita liší od tradiční trestné činnosti? Je zřejmé, že jedním z rozdílů je používání počítače, ale samotná technologie

---

[15] Darknet: temná strana internetu | Chip.cz - recenze a testy. Informace, testy a novinky o hardware, software a internetu – CHIP.cz [online]. Copyright © 2003 [cit. 08.02.2022]. Dostupné z: https://www.chip.cz/casopis-chip/earchiv/vydani/r-2012/chip-02-12/darknet/

[16] Výkladový slovník Kybernetické bezpečnosti - PDF Free Download. Představujeme Vám pohodlné a bezplatné nástroje pro publikování a sdílení informací. [online]. Copyright © DocPlayer.cz [cit. 04.12.2021]. Dostupné z: https://docplayer.cz/2694910-Vykladovy-slovnik-kyberneticke-bezpecnosti.html

[17] KOLOUCH, Jan a Pavel BAŠTA. CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7, str. 83

nestačí k tomu, aby bylo možné rozlišovat mezi různými oblastmi trestné činnosti. Zločinci nepotřebují počítač k tomu, aby mohli páchat podvody, šířit dětskou pornografii a porušovat práva k duševnímu vlastnictví, ukrást identitu nebo narušit něčí soukromí, šířit xenofobii a podporovat hnutí prosazující omezení základních práv a svobod atd. Všechny tyto činnosti existovaly ještě předtím, než se předpona "kybernetický" stala všudypřítomnou. Kyberkriminalita, zejména ta, která se týká internetu a sociálních sítí, představuje rozšíření stávajícího kriminálního chování spolu s některými novými nezákonnými činnostmi.[18]

Vyhledávání, vyšetřování a trestní postih kyberkriminality významně komplikuje skutečnost, že se ve značné míře jedná o trestnou činnost přeshraniční, resp. nadnárodní. To vyžaduje intenzivní využívání nástrojů mezinárodní policejní spolupráce a mezinárodní justiční spolupráce v trestních věcech, a to jak pomocí jejich tradičních nástrojů (pátrání po osobách, provádění domovních prohlídek, zajištění důkazního materiálu, výslechy osob a doručování písemností), tak specifických nástrojů vytvářených pro boj právě s kyberzločinem. Úmluva o boji proti počítačové kriminalitě (Budapešť, 23. 11. 2001; č. 104/2013 Sb. m. s.; tzv. Budapešťská úmluva) např. upravuje urychlené uchovávání uložených počítačových dat (až na 90 dnů), tj. formu zajištění, která umožní pozdější podání vydání příkazu k jejich zpřístupnění (čl. 16 až 18), prohlídku a zajištění uložených počítačových dat (čl. 19), shromažďování provozních dat v reálném čase (čl. 20) a odposlech obsahových dat (čl. 21). Tyto specifické nástroje, které jsou smluvní strany Úmluvy primárně povinny zavést vnitrostátně, jsou pak využitelné i mezistátně na základě čl. 29 a násl. v rámci mezinárodní policejní spolupráce a vzájemné právní pomoci v trestních věcech.

1.4 Sociální sítě

Termín sociální sítě (Social Networking Sites/SNS) označuje používání internetových sociálních médií k udržování kontaktu s přáteli, rodinou, kolegy, zákazníky nebo klienty, ale i se zcela neznámými lidmi. Lidé na sociálních sítích

[18] Cybercrime | Definition, Statistics, & Examples | Britannica. Encyclopedia Britannica | Britannica [online]. Copyright © Ivan Kruk [cit. 27.01.2022]. Dostupné z: https://www.britannica.com/topic/cybercrime

komunikují buď veřejně, nebo soukromě. Za sociální síť můžeme považovat i diskusní fórum, kdy jednotliví uživatelé diskutují a vyměňují si názory na konkrétní témata. Komunikace mezi uživateli sociálních sítí může probíhat buď soukromě mezi dvěma uživateli, ale stejně tak hromadně mezi uživatelem a skupinou, která je s ním v jedné skupině propojená.

Jedná se vlastně o webové stránky, které svým uživatelům umožní vytvořit si vlastní profil a upravit si jej podle svých představ, mohou se přátelit s jinými uživateli, nahrávat a sdílet fotografie, videa a jiné materiály, také si můžou vytvořit seznam přátel. Nejdůležitější faktorem je, kontakt s ostatními a sledování toho co druzí dělají.[19]

[19] ČERNÁ, Alena. Kyberšikana: průvodce novým fenoménem. Praha: Grada, 2013. Psyché (Grada). ISBN 978-80-247-4577-0, str. 28

2 Sociální sítě

Od svého vzniku v roce 1996 se sociálním médiím podařilo oslovit minimálně 7,7 miliardy lidí. Platformy sociálních sítí za posledních deset let téměř ztrojnásobily svou celkovou uživatelskou základnu z 970 milionů v roce 2010 na číslo překračující 4,48 miliardy uživatelů v červenci 2021.

Rychlý růst nových uživatelů na sociálních platformách se však zpomaluje. Nyní se spoléhá na neustálý růst počtu lidí s přístupem k internetu a chytrými telefony, zejména v rozvojových regionech. Mobilní užívání sociální sítě je dle výzkumů nejoblíbenější aktivitou při užívání smartphonu, až poté následuje samotné telefonování, posílání zpráv, pořizování fotografií a hraní her pro mobilní platformy.[20]

Sociální sítě změnily způsob, jakým komunikujeme, obchodujeme, získáváme každodenní informace, jednoduše řečeno změnily to, jak žijeme. Profil na Facebooku může být dobrým startem pro nového majitele firmy, nebo naopak to může být místo, kde je mladý dospívající či dítě vystaveno negativnímu vlivu a nevhodným poznámkám vůči jejich osobě. Všechno v životě má svá pro a proti, a to se týká i sociálních sítí.

Jedním z největších kladů používání sociálních sítí je možnost okamžitě se spojit s lidmi odkudkoliv. Pomocí Facebooku můžete zůstat v kontaktu se svými starými kamarády, kteří se přestěhovali téměř po celé zeměkouli.

Díky sociálním sítím je komunikace mezi lidmi z různých částí země velice snadná a rychlá. Sociální sítě jsou velice rychlým zdrojem informací, které můžeme získat v podstatě v reálném čase, a to i z toho nejvzdálenějšího koutu planety. Sociální sítě jsou také skvělou příležitostí pro podnikání. Majitelé firem a dalších typů profesních organizací se mohou pomocí sociálních médií spojit se stávajícími zákazníky, prodávat své produkty a rozšiřovat svůj dosah. Existuje

[20] How Many People Use Social Media in 2022? (65+ Statistics). SEO Training and Link Building Strategies – Backlinko [online]. Copyright © 2022 Backlinko is a Trademark of Backlinko LLC [cit. 09.02.2022]. Dostupné z: https://backlinko.com/social-media-users

spousta podnikatelů a firem, kteří prosperují téměř výhradně na sociálních sítích a bez nich by ani nemohly fungovat. Tato činnost se jim daří pomocí reklamy.[21]

V neposlední řadě je třeba zmínit, jak jsou sociální sítě důležité pro handicapované osoby. Lidé s určitým postižením se mohou začlenit do lidské společnosti, mohou být členy různých skupin a účastnit se různých diskusí. Zůstávají stále v „centru dění“, neizolují se do samoty svých domovů a snáze překonávají komunikační překážky.[22]

Není žádným tajemstvím, že sociální sítě mají i stinnou stránku. Nezřídka se veřejně kladou otázky typu, jak se můžou nevýhody sociálních sítí co nejvíce a nejčastěji minimalizovat.

Pokud jsou sociální sítě hlavním zdrojem zpráv a dalších informací, může se jejich uživatel ocitnout ve filtrační bublině, kdy se izoluje od nových informací a kontaktů s lidmi, kteří mají jiný pohled na věc.

Z mého pohledu spočívá největší problém sociálních sítí v udržení si soukromí. V dnešní době se toho na internetu sdílí tolik, že se otázky soukromí stávají stále větším úskalím. Ať už jde o to, že sociální sítě vlastní váš uveřejněný obsah nebo že se jejich uživatel stane možným terčem po sdílení své online polohy nebo dokonce o to, že se dostane do problémů v práci poté, co uživatel sdílí, nebo napíše něco nevhodného. Přílišné sdílení s veřejností může otevřít nejrůznější aspekty problémů, které mívají důsledky nevratitelné podoby.

Dále vidím jako významný problém plynoucí z častého používání sociálních sítí pocit sociální izolace. Vzhledem k tomu, že jsou lidé dnes neustále připojeni, je mnohem snazší používat online interakci jako náhradu za osobní interakci. Někteří lidé tvrdí, že sociální média ve skutečnosti podporují asociální chování lidí.[23]

---

[21] The Pros and Cons of Social Networking. Lifewire: Tech News, Reviews, Help & How-Tos [online]. Dostupné z: https://www.lifewire.com/advantages-and-disadvantages-of-social-networking-3486020

[22] Jak na Internet - Internet a handicapovaní. Jak na Internet - Jak na Internet [online]. Copyright © 2022 CZ.NIC, z. s. p. o. [cit. 12.02.2022]. Dostupné z: https://www.jaknainternet.cz/page/1653/internet-a-handicapovani/

[23] The Pros and Cons of Social Networking. Lifewire: Tech News, Reviews, Help & How-Tos [online]. Dostupné z: https://www.lifewire.com/advantages-and-disadvantages-of-social-networking-3486020

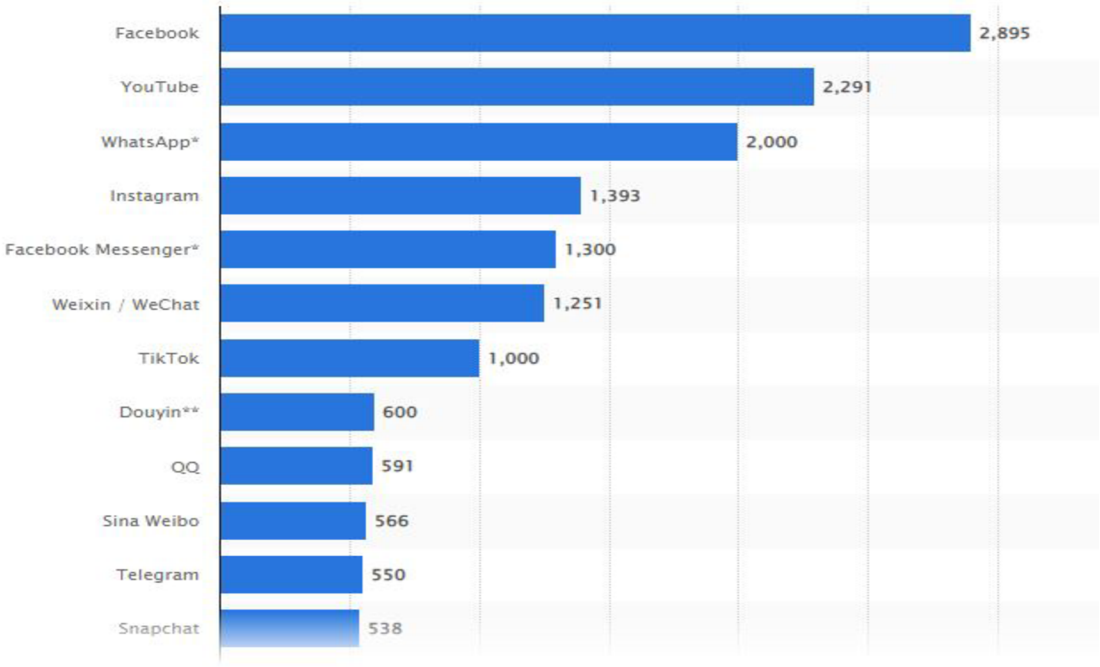
Dalším velice negativním aspektem sociálních sítí je ohromná časová náročnost, které je uživatel vystaven. Dále rozvoj závislosti (tzv. netholismus), a samozřejmě v neposlední řadě kyberšikana.

2.1 Statistiky používání sociálních médií

Ze statistiky publikované v roce 2022[24] vyplývá, že:

- Sociální média v současné době používá 4,48 miliardy lidí na celém světě, což je více než dvojnásobek oproti 2,07 miliardy v roce 2015.
- Průměrný uživatel sociálních médií se zapojuje v průměru do 6,6 různých platforem sociálních médií.
- Tempo růstu sociálních médií od roku 2015 činí v průměru 12,5 % meziročně. Růst však klesá, přičemž údaje za roky 2019-2020 ukazují 9,2% tempo růstu.
- Podle regionů je růst sociálních médií v letech 2019-2020 veden Asií: +16,98 %, Afrika +13,92 %, Jižní Amerika +8,00 %, Severní Amerika +6,96 %, Evropa +4,32 % a Australasie +4,9 %.
- 60,99 % ze 7,87 miliardy lidí na světě používá sociální média, z oprávněného publika ve věku 13+ je 63 % aktivních uživatelů.
- Ze 4,48 miliardy uživatelů sociálních médií jich 99 % přistupuje k webovým stránkám nebo aplikacím prostřednictvím mobilního zařízení, pouze 1,32 % přistupuje k platformám výhradně prostřednictvím stolního počítače.
- Celosvětově stráví člověk na sociálních sítích v průměru 2 hodiny a 24 minut denně; pokud by se někdo zaregistroval v 16 letech a dožil se 70 let, strávil by na nich 5,7 roku svého života.

[24] How Many People Use Social Media in 2022? (65+ Statistics). SEO Training and Link Building Strategies – Backlinko [online]. Copyright © 2022 Backlinko is a Trademark of Backlinko LLC [cit. 29.01.2022]. Dostupné z: https://backlinko.com/social-media-users#most-popular-social-media-platforms



Obrázek č. 1: Nejpopulárnější sociální sítě (čísla jsou uvedena v milionech)[25]

2.2 Facebook/Meta

Sociální síť Facebook, je americká online sociální síť, která je součástí společnosti Meta Platforms. Facebook založili v roce 2004 Mark Zuckerberg, Eduardo Saverin, Dustin Moskovitz a Chris Hughes, kteří byli studenty Harvardovy univerzity. Facebook se stal největší sociální sítí na světě, od roku 2021 měl téměř tři miliardy uživatelů a přibližně polovina z tohoto počtu používala Facebook každý den. Sídlo společnosti se nachází v Menlo Parku v Kalifornii.[26]

Sociální síť TheFacebook.com byla spuštěna v únoru 2004. Studenti Harvardu, kteří se do této služby zaregistrovali, mohli zveřejňovat své fotografie a osobní informace o svém životě, například rozvrhy hodin a kluby, do kterých patří. Její popularita rostla a brzy se k ní mohli připojit i studenti z dalších

[25] Most used social media 2021 | Statista. • Statista - The Statistics Portal for Market Data, Market Research and Market Studies [online]. Copyright © Statista 2021 [cit. 04.12.2021]. Dostupné z: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/
[26] What is Facebook?. Computer Glossary, Computer Terms - Technology Definitions and Cheat Sheets from WhatIs.com - The Tech Dictionary and IT Encyclopedia [online]. Dostupné z: https://whatis.techtarget.com/definition/Facebook

prestižních škol, například z univerzit Yale a Stanford. Do června 2004 se zaregistrovalo více než 250 000 studentů z 34 škol.[27]

Přístup na Facebook je zdarma a společnost vydělává většinu peněz z reklamy na webu. Noví uživatelé si mohou vytvářet profily, nahrávat fotografie, připojovat se k již existujícím skupinám a zakládat nové skupiny. Stránka má mnoho součástí, včetně Timeline, prostoru na profilové stránce každého uživatele, kde mohou uživatelé zveřejňovat svůj obsah a přátelé jim mohou posílat zprávy (Messenger) a videa, včetně streamování přímých přenosů (FaceTime).

V říjnu 2021 Facebook oznámil, že mění název své mateřské společnosti na Meta Platforms. Změna názvu odrážela důraz na "metaverzi", v níž budou uživatelé komunikovat v prostředí virtuální reality. S velkou kritikou se změna jména setkala nejen u laické, ale i odborné veřejnosti, a to s ohledem na pochybnosti o jejích důvodech, zejména zda skutečným záměrem není odvést pozornost a zastřít přetrvávající systémové problémy a chyby této platformy a služeb poskytovaných Facebookem. Nepříznivě se vyjádřilo i několik amerických senátorů. *„Kritici společnosti mají za to, že se jedná o zastírací manévr, který firmu problémů nezbaví. Změna názvu totiž přichází v době, kdy americký internetový gigant bojuje s kritikou zákonodárců i regulačních orgánů ohledně své tržní síly, algoritmických rozhodnutí a toho, jak na svých platformách přistupuje k projevům nenávisti či dezinformacím.“*[28]

2.2.1 Podmínky založení účtu na Facebooku

Facebook vyžaduje, aby všichni uživatelé uváděli svá data narození. V případě, že vyvstane podezření, že datum uvedené konkrétním uživatelem není pravdivé a že se ve skutečnosti jedná o uživatele mladšího 13 let, může si Facebook vyžádat zaslání kopie (scan) osobního dokladu (např. občanský průkaz, cestovní pas) nebo zadání čísla bankovní karty. Tento způsob ověřování

[27] Facebook | Overview, History, & Facts | Britannica. Encyclopedia Britannica | Britannica [online]. Copyright © Anatoli Styf [cit. 09.02.2022]. Dostupné z: https://www.britannica.com/topic/Facebook
[28] Facebooku budeme dál říkat pravým jménem. Hrozba, zní od kritiků - Seznam Zprávy. Seznam Zprávy [online]. Copyright © 1996 [cit. 20.01.2022]. Dostupné z: https://www.seznamzpravy.cz/clanek/meta-misto-facebooku-budeme-mu-rikat-pravym-jmenem-hrozba-zni-od-kritiku-179077

identity se nicméně nezdá být příliš efektivní, neboť kopie (scan) osobního dokladu může být snadno pozměněna, resp. může dojít k zadání čísla cizí bankovní karty (např. bankovní karty rodičů). Facebook běžně odstraňuje účty nezletilých uživatelů, pokud je identifikuje. Před několika lety Facebook zveřejnil, že denně odstraní účty 20 000 nezletilých uživatelů.

Na rozdíl od mnoha online služeb Facebook nepoužívá, resp. oficiálně nepovoluje vymyšlená uživatelská jména. Budoucí uživatel se musí registrovat pod svým skutečným jménem. Stejně jako v případě dat narození se však uživatelé často registrují pod falešnými jmény, ale Facebook používá různé techniky k odhalení falešných jmen a tyto účty běžně čistí. Po vytvoření uživatelského účtu mohou uživatelé přidat alternativní jména, která označují předchozí příjmení, přezdívku nebo profesní jméno. Poté, co si uživatel vytvoří osobní uživatelský účet, může si na Facebooku vytvořit stránku pro svou firmu nebo jinou organizaci s jakýmkoliv jménem, které podle jeho názoru reprezentuje jeho podnikání.

Kromě data narození označujícího, že je uživateli více než 13 let, a skutečného jména musí uživatel uvést své pohlaví a e-mailovou adresu. Účet musí být do tří dnů potvrzen e-mailem a pro plný přístup ke všem funkcím je vyžadováno číslo mobilního telefonu. Mobilní telefonní číslo je povinné, při registraci z mobilního či jiného zařízení.

Účet na Facebooku vyžaduje heslo. Kvůli ochraně bezpečnosti účtu na Facebooku, včetně všech přidružených firemních stránek na Facebooku, by heslo mělo být jedinečné a obtížně uhodnutelné. Heslo musí mít alespoň šest znaků a mělo by být kombinací velkých a malých písmen, číslic a interpunkčních znamének.[29]

2.2.2 Aféry spojené se společností Facebook

Díky svému obrovskému dosahu se zejména v poslední dekádě stal Facebook terčem několika skandálů a obvinění. Většina těchto problémů se týkala

[29] What Are the Requirements to Create an Account in Facebook? | Small Business - Chron.com. Small Business - Chron.com [online]. Copyright © 2022 Hearst [cit. 21.01.2022]. Dostupné z: https://smallbusiness.chron.com/requirements-create-account-facebook-56591.html

zejména boje s dezinformacemi, ochrany soukromí, potíží s moderováním obsahu, obvinění z protisoutěžního chování a vlivu na politické procedury v USA i v cizích zemích.

Níže uvádím několik skandálů, kterým Facebook, potažmo jeho představitelé čelili.

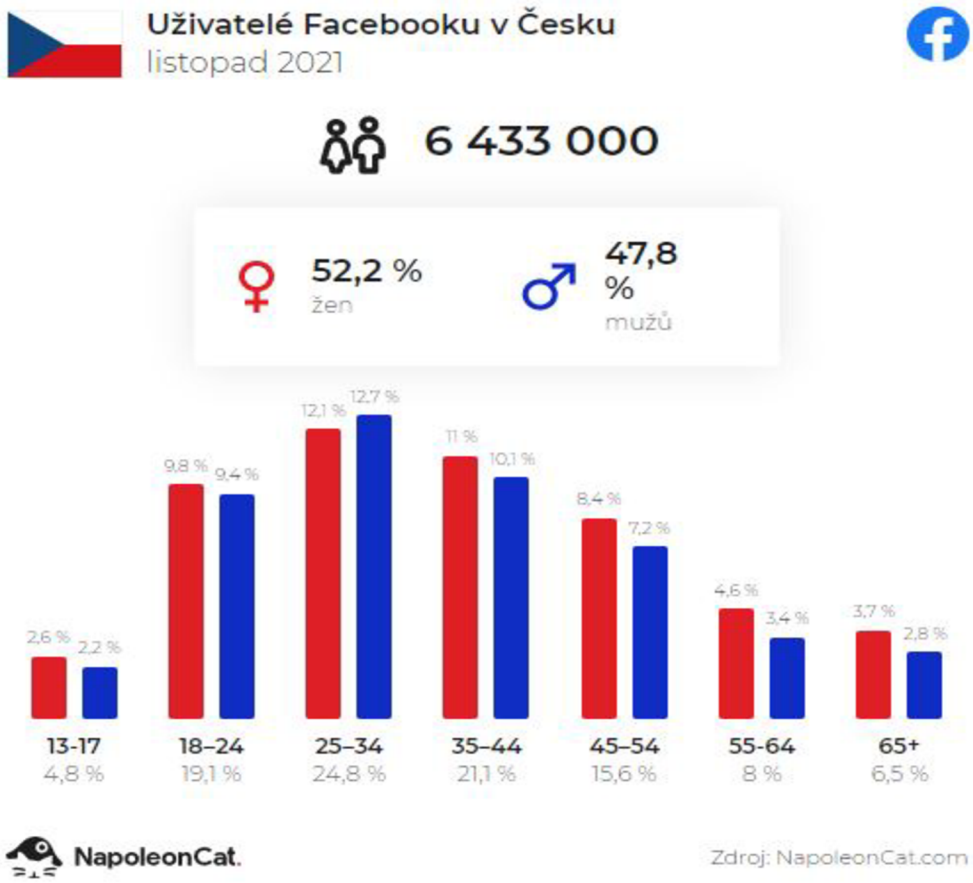
- Společnost čelila ostré kritice za dezinformace kolem amerických prezidentských voleb v roce 2016, zejména poté, co zpráva Buzzfeedu ukázala, že falešné zprávy předčily ty skutečné. Mark Zuckerberg zveřejnil na Facebooku omluvu a uvedl, že se společnost hodlá zlepšit.
- V roce 2018, unikla zpráva o skandálu Cambridge Analytica, která odhalila, že tato datově-analytická firma neoprávněně získala data desítek milionů uživatelů Facebooku pro cílení reklamy během amerických voleb v roce 2016.[30]
- Rok 2018 byl také ve znamení jednoho z nejtemnějších okamžiků v historii Facebooku, neboť se objevily zprávy, že sociální síť byla vojenskými představiteli této země využívána k podněcování genocidy proti muslimské menšině Rohingů v Myanmaru. Představitelé Rohingů dokonce v prosinci 2021 podali na společnost Facebook/Meta žalobu a jako odškodnění požadují v přepočtu téměř 3,5 miliardy korun. Dle žaloby podané ve Spojených státech tak „*firma upřednostnila vlastní pozici na trhu před životy Rohingů. Společnost Meta se zatím k žalobě nevyjádřila. V roce 2018 ale vedení firmy uznalo, že její sociální sítě byly zdrojem násilí.*“[31]
- V roce 2019 udělila FTC (Federal Trade Commission je americká federální komise zabývající se ochranou spotřebitelů) společnosti Facebook pokutu

[30] The 16 Biggest Facebook Scandals Mark Zuckerberg Faced. Insider [online]. Copyright © 2022 [cit. 09.02.2022]. Dostupné z: https://www.businessinsider.com/mark-zuckerberg-scandals-last-decade-while-running-facebook-2019-12#5-2018-also-marked-one-of-the-darkest-moments-in-facebooks-history-as-reports-revealed-that-the-social-network-was-used-to-incite-genocide-against-the-muslim-rohingya-minority-in-myanmar-by-the-countrys-military-officials-6

[31] Barmská menšina Rohingů žaluje sociální sítě za podněcování násilí, chce odškodnění 3,5 miliardy | iROZHLAS - spolehlivé zprávy. iROZHLAS - spolehlivé a rychlé zprávy [online]. Copyright © 1997 [cit. 29.01.2022]. Dostupné z: https://www.irozhlas.cz/zpravy-svet/rohingove-mensina-meta-zaloba-odskodneni-nasili-podnecovani_2112071221_pik

ve výši 5 miliard dolarů za porušování soukromí uživatelů, což byla pro technologickou společnost rekordní pokuta.[32]

- O velikonočním víkendu v roce 2021 prosákl na povrch do té doby největší únik osobních dat 533 miliónů uživatelů Facebooku ze 106 zemí světa. V případě České republiky mělo jít o 1 375 988 kontaktů s plnými detaily: jméno, Facebook ID, datum narození, telefonní číslo, e-mailová adresa, lokace a další. Tento únik osobních údajů uživatelů je chápán jako obrovské narušení důvěry.[33]



Obrázek 2: Uživatelé sociální sítě Facebook v ČR v listopadu 2021[34]

[32] Facebook to pay record $5 billion U.S. fine over privacy; faces antitrust probe | Reuters. Breaking International News & Views | Reuters [online]. Copyright © 0 Reuters. All Rights Reserved. [cit. 09.02.2022]. Dostupné z: https://www.reuters.com/article/us-facebook-ftc-idUSKCN1UJ1L9

[33] Stolen Data of 533 Million Facebook Users Leaked Online. Insider [online]. Copyright © 2022 [cit. 29.01.2022]. Dostupné z: https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4

[34] Facebook users in Czechia - November 2021 | NapoleonCat. Engage and Support Customers on Social Media – NapoleonCat [online]. Copyright © Napoleon Sp. z o.o. [cit. 12.12.2021]. Dostupné z: https://napoleoncat.com/stats/facebook-users-in-czechia/2021/11/

2.3 YouTube

YouTube je bezplatná webová stránka pro sdílení videí, která usnadňuje sledování online videí. Uživatel může vytvářet a nahrávat vlastní videa a sdílet je s ostatními. YouTube, původně vytvořený v roce 2005, je nyní jednou z nejoblíbenějších webových stránek vůbec. YouTube patří mezi bezplatnou službu, kterou používá 2 miliardy lidí po celém světě. Mezi hlavní funkce patří sledování hudebních videí, komediálních pořadů, receptů, různých návodů a i vytváření vlastního obsahu ve formě videí. Účet v aplikaci YouTube si mohou založit uživatelé starší 18 let nebo starší 13 let pouze se souhlasem rodičů.[35] V praxi probíhá ověřování identity obdobně jako v případě Facebooku (viz výše sub 2.2.1).

2.4 Instagram

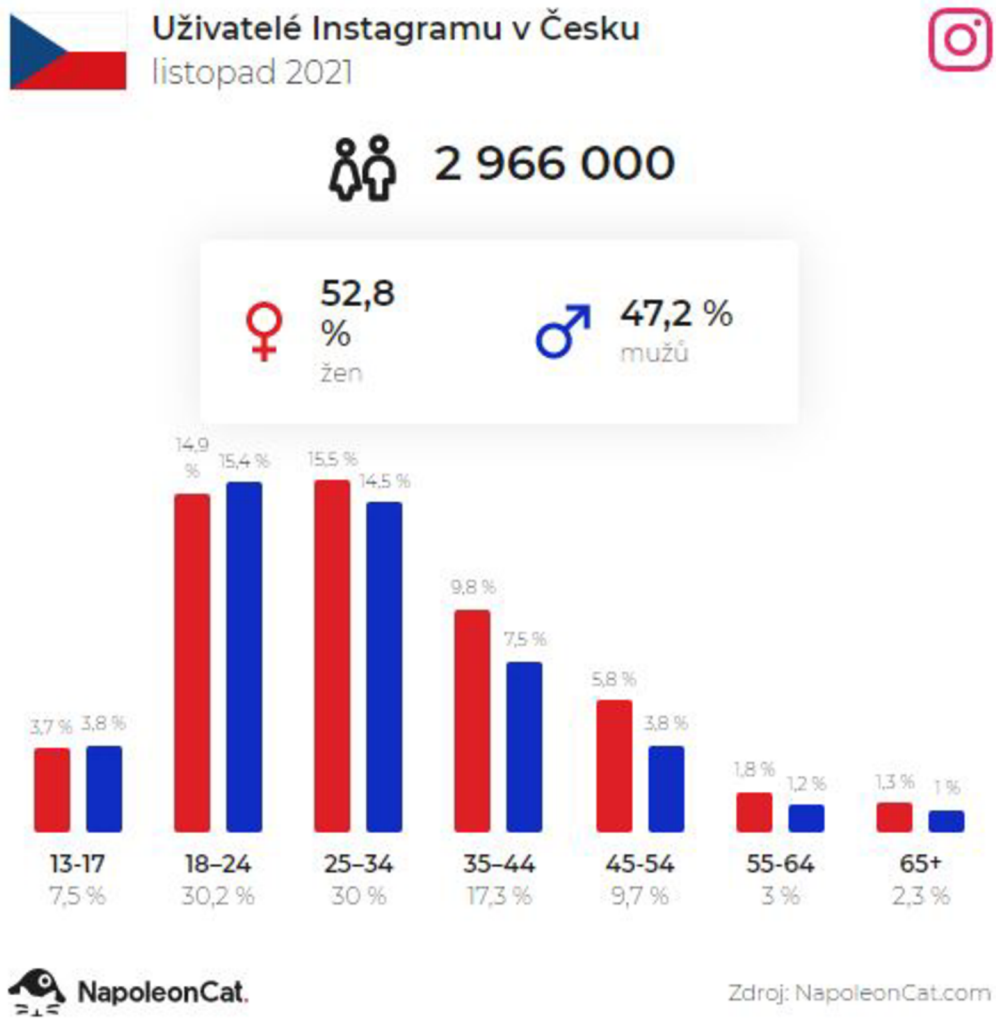
Instagram je sociální síť zaměřená na sdílení videí a fotografií. Tuto síť provozuje společnost Meta Platforms (Facebook). Síť Instagram je primárně určená pro mobilní telefony. Uživatelé mohou upravovat své fotografie a videa pomocí filtrů. Síť je financována z reklamy. Většina obsahu není bez účtu dostupná.

V červenci 2011 Instagram oznámil, že překročil hranici 100 milionů nahraných fotografií, a v srpnu jejich počet dosáhl 150 milionů. V prosinci 2013 bylo hlášeno číslo 16 miliard, přičemž denně bylo nahráno v průměru 55 milionů fotografií obrázků a 20 milionů nových denně. Novější statistiky uvádí, že každou minutu je nahráno více než 40 000 fotografií a videí, což znamená téměř 60 milionů příspěvků denně.[36]

Instagram je k dispozici na zařízeních se systémem iOS, nebo Android. Před použitím služby Instagram je nutné vytvořit si bezplatný účet. Registrace

[35] Explained: What is YouTube? [online]. Copyright © 2019 Sucuri Inc. All rights reserved. [cit. 05.02.2022]. Dostupné z: https://www.webwise.ie/parents/what-is-youtube/
[36] Instagram – Wikipedia. [online]. Dostupné z: https://de.wikipedia.org/wiki/Instagram

se provede pomocí stávajícího účtu na Facebooku nebo pomocí e-mailové adresy.[37]



Obrázek 3: Uživatelé sociální sítě Instagram v ČR v listopadu 2021[38]

[37] What Is Instagram and Why Should You Be Using It?. Lifewire: Tech News, Reviews, Help & How-Tos [online]. Dostupné z: https://www.lifewire.com/what-is-instagram-3486316

[38] Instagram users in Czechia - November 2021 | NapoleonCat. Engage and Support Customers on Social Media – NapoleonCat [online]. Copyright © Napoleon Sp. z o.o. [cit. 12.12.2021]. Dostupné z: https://napoleoncat.com/stats/instagram-users-in-czechia/2021/11/

2.5 Twiter

Twitter je mikroblogovací služba a sociální síť. Všichni registrovaní uživatelé, kteří se mohou stát součástí služby zdarma, mají možnost posílat prostřednictvím sítě krátké zprávy o maximální délce 280 znaků. Těmto zprávám se říká "tweety". Celkově se Twitter vyznačuje svou rychlostí. Koneckonců všechny hlavní redakce novin a mnoho jejich redaktorů jsou zastoupeny na Twitteru a šíří své zprávy i tímto způsobem. Další praktickou funkcí je rychlá a snadná interakce s ostatními uživateli, protože 280 znaků se píše rychle. Součástí tweetů mohou být rovněž fotografie, videa a prostřednictvím Twitteru lze také streamovat přímé přenosy.

Stejně jako u mnoha jiných sociálních sítí i zde existují rizika pro mladou populaci. A mnohá z těchto rizik jsou stejná jako rizika, která jsou spojena se všemi ostatními sociálními sítěmi. Twitter je velmi veřejné fórum. Uživatelé sice mohou své profily uzamknout, aby jejich tweety viděli pouze sledující, ale obecně se jedná o velmi otevřenou službu. To znamená, že se téměř kdokoliv může přihlásit a prohlédnout si, co konkrétní osoba od svého vstupu na web řekla.[39]

Vzhledem k tomu, že existují predátoři a bezohlední podvodníci, je množství osobních informací, které mladí lidé na této stránce zveřejňují, ať už jde o místa, fotografie, školní akce atd., nebezpečné. Stejně jako na většině sociálních sítí i zde existují věci, které bychom raději, aby naše děti neviděly, a na Twitteru neexistuje žádná nebo jen malá překážka, která by zabránila retweetování (sdílení tweetu/zprávy někoho jiného) nevhodných obrázků nebo zpráv a jejich šíření po webu.

Navíc je na Twitteru velkým problémem kyberšikana. Vzhledem k jeho okamžité a virální povaze lze na Twitter snadno posílat nepříjemné zprávy uživatelům a opakovat je znovu a znovu. Jako vždy, ale není vše pouze černobílé a i Twitter může být velmi nápomocný například při zvládání krizových situací, nebo situací, kde je potřeba především rychlá výměna informací.[40]

---

[39] Was ist Twitter? Einfach erklärt - CHIP. Praxistipps zu Problemen mit Windows, Android, iOS, Office, MacOS - CHIP [online]. Copyright © BurdaForward GmbH 2022 [cit. 06.02.2022]. Dostupné z: https://praxistipps.chip.de/was-ist-twitter-einfach-erklaert_49887

[40] Explained: What is YouTube? [online]. Copyright © 2019 Sucuri Inc. All rights reserved. [cit. 06.02.2022]. Dostupné z: https://www.webwise.ie/parents/explained-what-is-twitter-2/

2.6 VKontakte

Sociální síť VKontakte (VK) je známá také jako „ruský Facebook“. Je to největší sociální síť používaná v Rusku. Založil ji Pavel Durov v roce 2006 a okamžitě si našla své příznivce v zemích bývalého Sovětského svazu. VKontakte se řadí mezi nejnavštěvovanější webové stránky na světě, denně ji navštíví až 60 milionů uživatelů a podporuje více než 80 jazyků.

Rozhodující podíl ve společnosti, pod kterou tato síť s přibližně 650 miliony profily spadá, vlastní společnost Sogaz.[41]

Stejně jako v mnoha jiných sociálních sítích mohou členové VKontakte kontaktovat své přátele a známé, posílat jim soukromé nebo veřejné zprávy, sami vytvářet skupiny, zakládat veřejné stránky a události, sdílet obrázky a označovat na nich lidi, přehrávat videa a audio a hrát hry v prohlížeči. Je také možné používat hashtagy.

K dispozici je i obrovská databáze MP3, kde si můžete zdarma poslechnout nejnovější skladby.[42] Zajímavá je na této skupině především politika autorských práv. Dá se mluvit až o absenci autorský práv. Uživatelé mohou sdílet skladby, aniž by je tato otázka trápila.

Je dobré ještě zmínit, že platforma VK je nejlepším místem pro reklamu ruských podnikatelů. Pro komerční účely využívá společnost VK 400 000 společností a VK také umožňuje svým uživatelům nakupovat zboží díky vlastnímu platebnímu systému.[43]

2.6.1 Podmínky založení účtu VK

Registrace je velice snadná, pokud má uživatel už účet na Facebooku, může jej použít pro přístup do VK. Údaje se importují z Facebooku do VK, jen je nezbytné použít telefonní číslo a zadat kód, který uživateli VKontaktě zašle

---

[41] Mail.ru koupilo VKontakte, „ruský Facebook“ mění majitele - Lupa.cz. Lupa.cz - server o českém Internetu [online]. Copyright © 1998 [cit. 08.02.2022]. Dostupné z: https://www.lupa.cz/clanky/mail-ru-koupilo-vkontakte-rusky-facebook-meni-majitele/

[42] vKontakte: Bei VK.com anmelden und das deutsche VK Login. WC0.de: Die Urlaubs Inspirations Seite für Weltenbummler [online]. Dostupné z: https://www.wc0.de/vkontakte/

[43] What Is VK? (VKontakte Explained) | InstaFollowers. Buy Instagram Followers - *%100 Real, Instant | Only $0.59 [online]. Dostupné z:* https://www.instafollowers.co/blog/what-is-vk

pro přihlášení. Pokud účet na Facebooku nemá, nebo jej uživatel použít nechce, vytvoří si účet od začátku. To znamená, že zadá jméno, příjmení, pohlaví, datum narození, telefonní číslo a opět použije kód, který od VK obdrží. Po vytvoření účtu si může přidat profilový obrázek. Osobní údaje se dají kdykoliv pozměnit. Uživatelé si také mohou nastavit viditelnost svého profilu, osobních informací a příspěvků.

2.7 Imageboardy

Imageboard, hovorově také nazývána chan, je druhem internetového fóra, kde mohou být texty, a především obrázky anonymně publikovány. Tento koncept vznikl v Japonsku koncem roku 1990 v rámci subkultury tzv. anime a manga, ale od roku 2000 byl rozšířen do celého světa.

Nejznámější imageboard je 4chan. Od roku 2001 mohly být obrázky zveřejňovány také na bývalé desce Futuba Channel (2chan), což byla jedna z prvních imageboardů. Následně byly vytvořeny další imageboardy. 4chan vytvořil v roce 2003 v USA tehdy pouze patnáctiletý chlapec Christopher Poole.

Imageboardy lze nastavit a provozovat relativně snadno a levně, proto jsou provozovány soukromými osobami a jen velké chany jsou profesionálně organizovány.

Na imageboardech se obvykle příspěvky skládají z obrázkového souboru a textu, nebo pouze jedním z nich. Místo obrázků lze použít i videa či více obrázků současně. Příspěvky mohou obsahovat i odkazy a jsou číslovány, takže lze odkazovat na jednotlivé z nich. Jedná se vlastně o sociální síť svého druhu.

Posty lze vytvářet bez přihlášení a registrace, na imageboardech nejsou klasické účty. Identifikační informace se opakují v každém příspěvku. Ty je možno psát anonymně, ale může se uvést i jméno. Aby stejné jméno nemohlo používat víc lidí, mohou být příspěvky ověřeny tripcodem.

Webová stránka imageboardu obvykle obsahuje několik podfór neboli boardy. V jejich rámci jsou zobrazeny pomocí diskusních vláken. Celý imageboard mívá často pevné téma, například hudba, origami.

Mezi software využívaný k imageboardům patří například Futallaby, Kusaba, Wakaba, Yotsuba.

Ve srovnání s jinými internetovými fóry, jsou chany považovány za obzvlášť nepřátelské, existuje na nich hojně provokace, trollové, šokující obrázky, kyberšikana, pornografie (včetně dětské), sexismus, rasismus, politický extremismus. Obvykle nejsou potrestány, neboť vyhledání a identifikace pachatelů je zvlášť obtížná. Často se maže pouze dětská pornografie, či pokud jsou porušována autorská práva, a to pouze na požádání.[44]

2.8 TikTok

TikTok vznikl spojením dvou již populárních aplikací Douyin a Musical.ly. Jde především o aplikaci pro sociální média, kde mohou uživatelé vytvářet a sledovat krátké videoklipy, často doprovázené hudbou. Za dva roky od svého spuštění aplikace nashromáždila více než 800 milionů aktivních uživatelů. Videa jsou často hravá a maximálně využívají nástroje pro úpravy, aby bylo 15 sekund videa co nejpamátnějších. Přestože většina jejího obsahu je optimistická a vtipná, lidé tuto platformu využívají také k reakci na aktuální události, jako je kampaň #BlackLivesMatter a pandemie COVID-19. To v minulosti vedlo ke kontroverzi. TikTok byl obviněn z cenzury politicky laděného obsahu, který byl obzvláště kritický vůči čínské vládě.

Uživatelé nepotřebují účet, aby mohli sledovat videa na TikToku, ale pokud chtějí lajkovat, komentovat, přizpůsobovat svůj kanál nebo vytvářet vlastní videoobsah, budou vyzváni k registraci bezplatného účtu.

Stejně jako většina platforem sociálních médií i TikTok vyžaduje, aby uživatelům bylo alespoň 13 let, ačkoli zde není zavedeno žádné důkladné ověřování věku. Při prvním přihlášení bude uživatel vyzván, aby se přihlásil buď pomocí svého e-mailu, účtu Google, nebo propojením TikToku s některým ze svých dalších účtů na sociálních sítích, například na Facebooku nebo Twitteru. Na rozdíl od většiny svých konkurentů TikTok nevyžaduje, aby uživatel do svého profilu přidával jakékoli informace, to znamená, že je mu přiděleno uživatelské číslo, ale to, zda si přidá jméno, profilový obrázek nebo jiné osobní údaje, je na jeho rozhodnutí.

[44] Imageboard – Wikipedia. [online]. Dostupné z: https://de.wikipedia.org/wiki/Imageboard

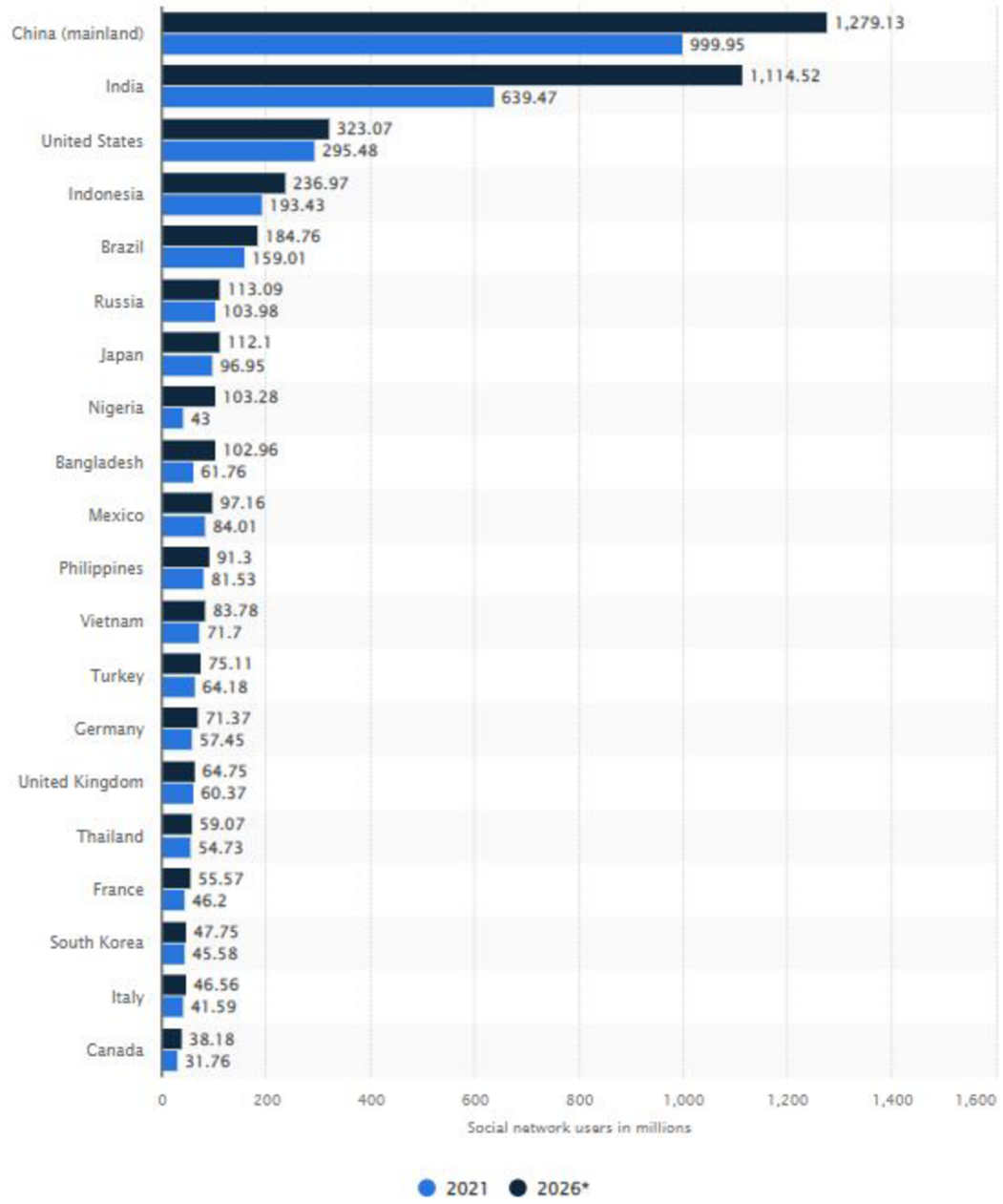
2.8.1 Známá rizika užívání sítě TikTok

Mezi známá rizika, která byla s touto sociální sítí spojována, patří především, sběr dat, který sloužil k nezákonnému shromažďování údajů dětí mladších 13 let, což vyústilo v rekordní pokutu 4,2 milionu dolarů.[45] Dále je TikTok znám pro virální výzvy, které jsou pro mnoho uživatelů velkým lákadlem, ačkoli mohou svým obsahem být i nebezpečné (porušování pravidel silničního provozu při běhu vedle jedoucího automobilu za zpěvu populárních písní, požívání nebezpečných látek atp.). TikTok si např. vysloužil mnoho kritiky za to, že na své platformě umožnil šíření výzev Skullbreaker (jedná se o výzvu, kdy dva lidé oklamou třetí osobu, která vyskočí do vzduchu, a podkopnou jí nohy, dochází potom ke zranění této třetí osoby – rozbití lebky)[46] a Outlet Challenge (ta znamená, že nejprve uživatel zástrčku nabíječky mobilního zařízení zastrčí částečně do zásuvky, přičemž kovové kolíky zůstanou stále odkryté a přístupné; poté se vezme mince a zasune do prostoru mezi zástrčku a zásuvku tak, aby se dotýkala těchto odkrytých hrotů, jde o to vidět jiskry a cítit kouř)[47].

[45] TikTok: everything you need to know about the video production app | Parent Zone. Home | Parent Zone [online]. Copyright © 2022 Parent Zone All rights reserved. [cit. 09.02.2022]. Dostupné z: https://parentzone.org.uk/article/tiktok-everything-you-need-know-about-video-production-app

[46] Dangerous TikTok 'skull-breaker challenge' causes child head injuries - ABC13 Houston. KTRK Houston news, weather and traffic - Latest Texas news and weather [online]. Copyright © 2022 ABC, Inc. [cit. 10.02.2022]. Dostupné z: https://abc13.com/tiktok-skill-breaker-challenge-skull-breaker-causes-children-injuries-causing/5959067/

[47] What Is The 'Outlet Challenge'? How It Can Electrocute Or Burn You. Forbes [online]. Copyright © 2022 Forbes Media LLC. All Rights Reserved [cit. 10.02.2022]. Dostupné z: https://www.forbes.com/sites/brucelee/2020/02/23/what-is-the-outlet-challenge-how-it-can-electrocute-or-burn-you/?sh=6b7868511e62



Obrázek 4: Počet uživatelů sociálních sítí ve vybraných zemích v letech 2021 a 2026 (v milionech)[48]

[48] Social network users in leading markets 2026 | Statista. • Statista - The Statistics Portal for Market Data, Market Research and Market Studies [online]. Copyright © Statista 2022 [cit. 06.02.2022]. Dostupné z: https://www.statista.com/statistics/278341/number-of-social-network-users-in-selected-countries/

3 Kyberkriminalita na sociálních sítích

Pojem kybernetická kriminalita je velice těžce uchopitelný. Existuje mnoho různých vymezení od různých autorů. Neexistuje jednoznačná definice daného termínu. Kyberkriminalitu můžeme nazvat i kriminalitou počítačovou nebo také internetovou, nebo jednoduše řečeno to může být trestná činnost, která souvisí s počítačem.

Podle Jirovského je kybernetická kriminalita definována *jako činnost, kterou je porušován zákon nebo je v rozporu s morálními pravidly společnosti. Tato kriminalita může být namířena přímo proti počítačům, jejich hardwaru, softwaru, datům, sítím apod. nebo v ní vystupuje počítač pouze jako nástroj pro páchání trestného činu, případně počítačová síť a k ní připojená zařízení jsou prostředím, v němž se taková činnost odehrává.*[49]

Kyberkriminalita je tedy jakákoliv trestná činnost, která zahrnuje počítač, síťové zařízení nebo síť. Většina kybernetických trestných činů je páchána za účelem dosažení zisku pro kyberzločince. Současně však řada kyberzločinců páchá trestné činy formou pouhého šíření nelegálních informací, obrázků nebo jiných materiálů, aniž by k bezprostřednímu generování zisku docházelo.

Kyberkriminalita i na sociálních sítích může zahrnovat mnoho různých typů trestné činnosti zaměřených na zisk, včetně útoků pomocí ransomware (druh škodlivého programu, pokud je např. prostřednictvím sociálních sítí šířen), e-mailových a internetových podvodů a podvodů s identitou.

Kyberzločinci se mohou zaměřit na soukromé informace jednotlivců nebo firemní údaje, které chtějí odcizit a dále prodat. Sociálních sítí mohou využívat i k tzv. sociálnímu inženýrství (technická manipulace, která využívá lidské chyby k získání soukromých informací, přístupu nebo cenností, s jejíž pomocí z uživatelů takové informace vylákají, např. phishing, baiting)[50]. Vzhledem k tomu, že se mnoho pracovníků kvůli pandemii COVID-19 ocitlo v pracovním režimu

[49] JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. ISBN 978-80-247-1561-2, str.19

[50] What is Social Engineering? | Definition | Kaspersky. Kaspersky Cyber Security Solutions for Home & Business | Kaspersky [online]. Copyright © [cit. 12.02.2022]. Dostupné z: https://usa.kaspersky.com/resource-center/definitions/what-is-social-engineering

na dálku neboli home office, očekává se, že kybernetická kriminalita bude v roce 2022 narůstat.[51]

3.1 Kyberšikana

Než se pokusím objasnit pojem kyberšikana je potřeba si něco blíže říci k šikaně jako takové. Podle Dana Olweuse se specifikace šikany skládá z těchto kritérií:

- jde o úmyslné chování,
- toto jednání je opakované,
- mezi obětí a agresorem existuje mocenská nerovnováha.[52]

Toto je ovšem pouze základní definice, dále je potřeba vzít v úvahu fakt, že oběť agresora nijak neprovokuje, a že k těmto jevům dochází v místech, která nelze dobře opustit (třída, škola atd.). Šikanu lze dále rozdělit na přímou (bití, plivání, vulgární nadávky, výhrůžky, příkazy, vysmívání se, ničení/schovávání/kradení věcí atd.) a nepřímou (ignorace, izolování žáka, skryté ničení, pomluvy, ponižování).[53]

Kyberšikana je tedy nerozlučně spjata s tradiční (školní) šikanou. Má společné rysy:

- děje se prostřednictvím elektronických médií,
- opakovanost,
- záměrnost agresivního aktu ze strany útočníka,
- mocenská nerovnováha,
- oběť vnímá toto jednání jako nepříjemné, ubližující.[54]

[51] What is cybercrime? Definition from SearchSecurity. Purchase Intent Data for Enterprise Tech Sales and Marketing - TechTarget [online]. Dostupné z: https://www.techtarget.com/searchsecurity/definition/cybercrime
[52] ČERNÁ, Alena. Kyberšikana: průvodce novým fenoménem. Praha: Grada, 2013. Psyché (Grada). ISBN 978-80-247-4577-0. str. 19
[53] Tamtéž, str. 19, 20.
[54] Tamtéž, str. 21.

Podle Černé lze kyberšikanu chápat jako záměrné agresivní chování, prováděno jednotlivcem nebo skupinou prostřednictvím elektronických médií vůči člověku, jenž se v danou chvíli nemůže útoku bránit.[55]

Termínem kyberšikana (též kybernetická šikana, počítačová šikana či cyberbullying) lze tedy označit nebezpečné komunikační akty realizované pomocí informačních a komunikačních technologií (např. pomocí mobilních telefonů nebo služeb v rámci internetu). Ty mají za následek ublížení či jiné poškození oběti. Může se jednat o záměr ze strany útočníka, ale také to může být pouze hloupý vtip či nedorozumění mezi obětí a útočníkem, nedomyšlením důsledků jednání ze strany útočníka atd. Je důležité zdůraznit, že se jedná o opakované poškozování oběti, ať už útočníkem původním nebo velice často dochází k zapojení i ostatních osob do kyberšikany. Kyberšikana je druhem psychické šikany.[56]

3.1.1 Rozdíl mezi tradiční šikanou a kyberšikanou

Kyberšikana se odehrává ve virtuálním světě. Tak, jako se liší virtuální svět od světa reálného, liší se i kyberšikana od klasické šikany. Podle dostupných studií se v případě kyberšikany jedná nejčastěji o rozšíření šikany tradiční, což znamená, že se tradiční šikana přesouvá z offline světa do světa online.[57]

- Místo a čas útoku

U tradiční šikany lze většinou předpokládat, kdy a kde k útoku dojde (např. ve škole, na hřišti), na rozdíl od kyberšikany. Zde místo ani čas nikdy není známo. Vždy při připojení k internetu, může dojít k možnému útoku, kdy si agresor svou oběť vyhlédne a není se kam schovat. Útočník si svou oběť najde třeba i o půlnoci v „bezpečí domova“.

---

[55] Tamtéž, str. 9

[56] Kyberšikana. | e-besedy.cz [online]. Copyright © [cit. 28.12.2021]. Dostupné z: http://www.e-besedy.cz/internetova-bezpecnost/kybersikana.html

[57] ČERNÁ, Alena. *Kyberšikana: průvodce novým fenoménem*. Praha: Grada, 2013. Psyché (Grada). ISBN 978-80-247-4577-0. str. 20

- Útočník

Pachatel kyberšikany bývá většinou anonymní, je skrytý za svou přezdívkou či jiným identifikačním znakem. Z toho plyne většina rozdílů mezi pachateli kyberšikany a tradiční šikany. Díky anonymitě virtuálního světa, dochází ke smazávání rozdílů mezi lidmi (věk, pohlaví, sociální pozice, fyzické dispozice, odvaha zaútočit). Toto virtuální prostředí zprostředkovává možný útok provést i těm, kteří dostatečně nedisponují těmito možnostmi. Původcem kyberšikany se může stát kdokoliv, kdo má potřebné znalosti informačních a komunikačních technologií. Agresoři tráví na internetu mnohem více času, a to většinou bez dohledu rodičů, což považuji za zásadní problém.

- Sekundární útočníci (diváci a šiřitelé)

V tomto případě může být množství diváků kyberšikany podstatně větší než v případě tradiční šikany. U kyberšikany se může přihlížejícím stát v podstatě každá osoba s přístupem na internet, můžou to být až miliony diváků z celého světa. Nejenom diváci jsou ti, co se do počítačové šikany zapojují, jsou to i šiřitelé počítačové kriminality. Jedná se o lidi, rozesílající informace o kyberšikaně (posílají například odkazy na stránky, kde se tato šikana objevila) a tak se vědomě či nevědomě do kyberšikany sami zapojují. Tento fakt zmnohonásobuje dopady útoku na možnou oběť. Tímto způsobem vlastně poškozují oběť mnohem více než primární útočník a stávají se útočníky sekundárními.

- Oběť

U obětí kyberšikany nezáleží na věku, pohlaví, sociální pozici, fyzické síle či oblíbenosti nebo úspěšnosti v té dané společnosti. Je to stejné jako u původce kyberšikany. Tyto zmíněné aspekty jsou naprosto potlačeny v elektronické formě komunikace, nemají takový význam jako při osobním kontaktu. Podle dostupných výzkumů vyplývá, že oběti tradiční šikany jsou dost často také oběťmi šikany počítačové. Také se můžeme dočíst z různých výzkumů, že oběti kyberšikany tráví na internetu více času a nejsou obeznámeni s možnými riziky, a tím pádem

se nechovají dostatečně opatrně. Je potřeba zdůraznit, že velice často je útočník i oběť mladistvý či dokonce dítě, což dále zvyšuje míru nebezpečnosti.

- Útok a jeho dopad na oběť

Při kyberútoku nejde o osobní kontakt mezi útočníkem a obětí (velice často útočník svou oběť vůbec nezná a pouze si ji vytipuje například podle přezdívky, věku, či jen dostupné fotografie). Protože nedochází k dostatečné zpětné vazbě z reakce oběti, rozvíjí to v mnohem větší míře agresivitu a impulsivnost tohoto útoku. Dopady vlivu informací zveřejněných na internetu jsou mnohem dalekosáhlejší než pouhé „pomluvy a nadávky“ ve světě reálném. Ty v krátkém čase odezní a zapomene se na ně. Ve virtuálním světě tyto inkriminující materiály zůstanou uložené a kdykoliv se mohou znovu a znovu vynořit a poškozovat oběť. Jsou dostupné kdykoliv, komukoliv a odkudkoliv. V obětech to prohlubuje pocity úzkosti a beznaděje, protože existují pouze minimální možnosti obrany proti útočníkovi. Tyto citlivé materiály užívané dětmi mezi sebou pro účely kyberšikany mohou být dospělými šiřiteli zneužity jako dětská pornografie.

- Diagnostika

Poznat oběť kyberšikany je velice složité. Je to stejný problém jako u jakéhokoliv jiného psychického týrání. Na oběti nejsou vidět žádné fyzické následky (modřiny, šrámy). Tyto oběti bývají velice často nemluvné, uzavřené do sebe. Bývá to z důvodu strachu, studu, dítě často nechápe, že jde o projev šikany, bojí se, že mu například rodiče zakážou přístup na internet. Oběti kyberšikany často řešení tohoto problému nezvládnou, protože nevyhledají pomoc a jsou odkázáni sami na sebe.[58]

3.1.2 Nejčastější projevy kyberšikany

Projevy počítačové šikany můžou být různé. Jde jak o dlouhodobé, tak krátkodobé útoky s různou intenzitou a využitím mnoho druhů nástrojů. Při útoku

[58] Kyberšikana, Uherské Hradiště. Uherské Hradiště [online]. Copyright © 2001 [cit. 28.12.2021]. Dostupné z: https://www.mesto-uh.cz/kybersikana

jde o kombinaci více typů napadení. Tradiční šikana často předchází kyberšikanování. Mezi nejznámější projevy patří:

- publikování ponižujících záznamů nebo fotografií,
- ponižování a pomlouvání v rámci sociálních sítí, blogů nebo jiných webových stránek,
- krádež identity, zneužití cizí identity ke kyberšikaně nebo dalšímu sociálně patologickému jednání,
- ztrapňování pomocí falešných profilů,
- provokování a napadání uživatelů v online komunikaci, především v rámci veřejných chatů a diskuzí,
- zveřejňování cizích tajemství s cílem poškodit oběť,
- vyloučení z virtuální komunity,
- obtěžování.

Mezi další projevy kyberšikany řadíme i projevy tradiční šikany posílené o využití informační a komunikační technologie, např.:

- dehonestování (ponižování, nadávání, urážení),
- vyhrožování a zastrašování,
- vydírání,
- očerňování (pomlouvání) a další.

K těmto projevům jsou zneužívány především SMS zprávy, emaily, chat, diskuze, blogy, sociální sítě nebo jiné webové stránky.[59]

3.1.3 Kyberšikana a právo

Neomezená virtuální svoboda a anonymita má i na sociálních sítích právní rámec a hranice. Svým příspěvkem či jen komentářem se může naplnit skutková podstata hned několika trestných činů, např. poškození cizích práv (§ 181 trestního zákoníku), pomluva (§ 184 trestního zákoníku), křivé obvinění (§ 345 trestního zákoníku), nebezpečné pronásledování (§ 354 trestního zákoníku), hanobení národa, rasy, etnické nebo jiné skupiny (§ 355 trestního zákoníku) atp.

[59] Kyberšikana. | e-besedy.cz [online]. Copyright © [cit. 28.12.2021]. Dostupné z: http://www.e-besedy.cz/internetova-bezpecnost/kybersikana.html

3.2 Kyberstalking

Stalking jinak řečeno lov či pronásledování je termín, označující opakované a stupňované obtěžování. Tento termín má řadu různých forem a různou intenzitu. Agresor svou oběť například obtěžuje neustálým zasíláním SMS zpráv, telefonáty, e-maily či různými dárky, které oběť nechce. Ve spojení s využitím informačních a komunikačních technologií u útočníka hovoříme o termínu kyberstalking (cyber-stalking). Je to pronásledování na dálku. V tomto případě jde o zasílání různých zpráv pomocí instant messengerů, chatu, prostřednictvím VoIP (Voice over IP je technologie umožňující používat internet k uskutečňování a přijímání telefonních hovorů) technologií apod. Nejčastějšími obětmi stalkingu jsou známé osobnosti, bývalý partneři, politici, lidé zhrzení v lásce atd.[60]

Od kyberšikany se kyberstalking liší především tím, že kyberstalker obtěžuje oběť, sleduje ji, „bombarduje“ zprávami z důvodu pomsty či kontroly, zatímco pachatel kyberšikany úmyslně ubližuje oběti, uráží ji, vyhrožuje, šíří o ní pomluvy atd.

3.2.1 Pachatelé kyberstalkingu

Většinou se jedná o muže, více obětí najdeme mezi ženami. Ženy stalkerky bývají vynalézavější a cílevědomější (co se týče šíření negativních zpráv o oběti). Jednání pronásledovatele není pouhým momentálním nápadem pachatele, skrývá se za tím určitý záměr, umanutost či pouhý blud.[61]

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

[61] O nás [online]. Copyright © [cit. 28.12.2021], str. 15. Dostupné z: https://www.ncbi.cz/odborna-knihovna/category/6-metodiky-ucebni-materialy.html?download=37:metodika-kybergrooming-a-kyberstalking

3.2.2 Typy stalkerů

• Bývalý partner – nedokáže unést rozchod či ukončení jiného vztahu než partnerského (pracovní, obchodní, terapeutický vztah atd.).
• Uctívač – pachatel touží po vztahu s osobou, která jej zaujala, většinou se jedná o někoho známého z prostředí showbusinessu, doufá, že osoba bude city opětovat.
• Neobratný nápadník – díky svým sociálním a komunikačním obtížím není schopen intimního vztahu, ale velmi po něm prahne.
• Ublížený pronásledovatel – chce pomstu, ať už z důvodu skutečného nebo smyšleného ublížení obětí, bývá velice vytrvalý.
• Poblouzněný milovník – myslí si, že je do něj oběť zamilovaná, vše co oběť udělá, si převede ke svým vytouženým představám, podporuje tím svou iluzi (oběť mívá většinou vysokou sociální pozici).[62]

3.2.3 Motivace stalkerů

• Absolutní moc a kontrola nad obětí – výhrou je v tomto případě pro stalkera naprostá kontrola nad životem sledovaného, jedná se především o sexuální zájem, může končit i sexuálně motivovanou vraždou.
• Starost a péče o oběť – zde je ziskem pro stalkera vztah s obětí, kterou je zaujat.
• Zničit blaho oběti z důvodu nepřátelství a zášti – za výhru stalker považuje zničení dosavadního života oběti, pracovních, rodinných a jiných vztahů, dovede oběť k naprosté osamělosti, může dojít i k sebevraždě oběti.[63]

3.2.4 Třífázový model vývoje stalkingu

Existuje třífázový model vývoje stalkingu, a to fáze pýchy, kdy je pronásledovatel plný očekávání, nadějí a vykazuje chování typu namlouvání a dvoření. Druhou fází je fáze zklamání, kdy stalker pociťuje obavy, cítí

[62] Tamtéž, str. 15.
[63] Tamtéž, str. 16.

se podveden, zhrzen, oběť falešně obviňuje a pronásleduje výčitkami a poslední fází je fáze hněvu, pronásledovatel začíná pomocí agrese vydírat a vyhrožovat.[64]

3.2.5 Typické projevy nebezpečného pronásledování

Jde o opakované a dlouhodobé pokusy kontaktovat oběť pomocí dopisů, e-mailů, telefonátů, SMS zpráv, zasíláním různých zásilek s dárky, zasíláním vzkazů na Skype, různé druhy chatu, VoIP apod.

Obsah těchto zpráv se může lišit, může se jednat o vtipné a veselé zprávy, ale také může jít o urážky či zastrašování. Často jsou to zprvu zprávy příjemné, kdy se pronásledovatel snaží vetřít do přízně oběti a snaží se získat odpověď a kontakt oběti. Posléze to vyústí ve zprávy nevkusné, zastrašující, urážlivé.

3.2.6 Demonstrování moci a síly stalkera

- V tomto případě stalker ve svých projevech dává důraz na přímé či nepřímé výhrůžky, které v oběti budí oprávněný strach a obavy. Do této kategorie patří například fyzické pronásledování oběti cestou do práce, na nákup nebo naopak zpět k domovu, pronásledování autem, čekání na oběť před domem apod. Výjimkou zde nejsou ani výhrůžky přímým násilím, vyhrůžky zabitím apod. V případě sadistického pronásledovatele, který se snaží důsledně a zcela kontrolovat život oběti, je riziko napadení včetně usmrcení oběti podstatně vyšší. Pronásledovaná oběť pak bývá častou obětí sexuálně motivované vraždy.[65] V oblasti elektronických médií se stalker většinou omezuje na různé druhy výhrůžek, které opírá o znalosti o oběti (vím, kde jsi, co děláš, vidím tě, vím, co máš na sobě apod.).

[64] Tamtéž, str. 16.
[65] Co je to stalking a cyberstalking - E-Bezpečí. Projekt E-bezpečí - E-Bezpečí [online]. Dostupné z: https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/kyberstalking/66-23

3.2.7 Destrukce věcí oběti

- Další charakteristické fáze stalkingu jsou poškozování a ničení věcí oběti, sem řadíme v rámci kyberstalkingu zasílání virů pomocí e-mailu. Ty můžou mít za následek velké škody v počítači oběti, například ztrátu dat či pokusy dostat se k osobním údajům oběti díky elektronickým kanálům.

3.2.8 Stalker se vydává za oběť

- Častým jevem je, že stalker sám sebe označuje za oběť a předstírá, že se mu oběť mstí. Dokonce může na oběť podat i trestní oznámení či se snaží ji jinak očernit.

3.2.9 Snaha poškodit reputaci oběti stalkerem

- Při kyberstalkingu dochází ke snaze stalkera pohanit oběť. Stalker se snaží vířit nepravdivé informace v okolí oběti. Útočník například vytvoří falešnou internetovou stránku, na kterou uvede nepravdy o oběti. Snaží se tím o snížení reputace a důvěryhodnosti oběti. Tyto lži šíří všemi možnými druhy internetové komunikace.[66]

3.2.10 Kyberstalking a právo

Kyberstalkingem se lze dopustit trestného činu nebezpečného pronásledování (§ 354 trestní zákoník), jde-li o dlouhodobé pronásledování způsobilé vzbudit tzv. důvodnou obavu o život a zdraví oběti nebo jejích osob blízkých, a to některým z uvedených jednání či jejich kombinací:

• vyhrožováním ublížením na zdraví nebo jinou újmou oběti či jejím osobám blízkým,
• vyhledáváním osobní blízkosti oběti nebo jejím sledováním,
• vytrvalým kontaktováním (elektronicky, písemně či jinak),

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

• omezováním oběti v obvyklém způsobu života,
• zneužitím osobních údajů oběti za účelem získání osobního či jiného kontaktu.[67]

3.3 Kybergrooming

V případě kybergroomingu (child grooming) se jedná o rizikovou formu komunikace v online prostředí, jejímž cílem je zmanipulovat vyhlédnutou oběť (dítě) a přimět ji k osobní schůzce v reálném světě.[68]

Při kybergroomingu se pachatel nejprve pokouší navázat důvěrný kontakt s dítětem, staví se do role kamaráda oběti, následuje izolování dítěte kybergroomerem od svého okolí tím, že mu zakazuje o jejich konverzaci říct rodině, kamarádům, spolužákům (z důvodu, že by oběť neměli rádi atd.) a ve většině případů již získá telefonní číslo, adresu oběti či školy. V další fázi útočník začíná svou oběť podplácet různými dárky (lístky do kina, oblečení, mobilní telefon) a ve třetí fázi je už patrná emoční závislost oběti na útočníkovi. Kybergroomer už o dítěti ví v podstatě vše. Děti se nesvěřují rodičům a neustále lžou o tom, s kým se stýkají. Poslední, čtvrtá fáze je nejvíc nebezpečná, protože už dochází k osobnímu setkání (procházka, kino, návštěva bytu útočníka). Zde již dochází k možnému znásilnění a sexuálnímu obtěžování ze strany kybergroomera.[69]

Tento popis kybergroomingu a především kybergroomera je v rozporu s tím co uvádí Anna Ševčíková. Podle ní je tato stereotypní představa v mnohém mylná a zavádějící. Děti se s neznámými lidmi setkávají jen ve velmi malé míře, většina takových setkání se uskuteční s osobou přibližně stejného věku, a i v rámci „nepříjemných setkání" je sexuální napadení málo časté.[70]

Kybergrooming je vlastně psychická manipulace, ve které komunikuje dospělý uživatel (často pod falešnou identitou) s dítětem, přičemž využívá celou

---

[67] O nás [online]. Copyright © [cit. 28.12.2021], str. 14. Dostupné z: https://www.ncbi.cz/odborna-knihovna/category/6-metodiky-ucebni-materialy.html?download=37:metodika-kybergrooming-a-kyberstalking

[68] Kybergrooming: Online predátoři a kybergrooming. Kybergrooming: Online predátoři a kybergrooming [online]. Dostupné z: http://www.kybergrooming.cz/

[69] HULANOVÁ, Lenka. Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality. Praha: Triton, 2012. ISBN 978-80-7387-545-9, str.52,53

[70] ŠEVČÍKOVÁ, Anna. Děti a dospívající online: vybraná rizika používání internetu. Praha: Grada, 2014. Psyché (Grada). ISBN 978-80-247-5010-1, str. 89

řadu strategií - např. zrcadlení (mirroring), phishing, profilování oběti, vábení a uplácení (luring), strategie snižování zábran dětí a mládeže zaváděním sexuálního obsahu do konverzace, izolační metody, strategie manipulace dětí prostřednictvím fotografií opačného pohlaví, webcam trolling apod.

Při kybergroomingu může docházet k páchání řady trestných činů (např. vydírání § 175 trestního zákoníku, sexuální nátlak § 186 trestního zákoníku, navazování nedovolených kontaktů s dítětem § 193b trestního zákoníku).

U kybergroomingu existuje vysoký stupeň latence, velké množství obětí tohoto typu útoku incident nenahlásí. Seriózní odhady hovoří o tom, že kybergrooming ohlásí maximálně 10 % zneužitých.[71]

3.3.1 Kde ke kybergroomingu dochází?

Kybergrooming se odehrává především v prostředí sociálních sítí, veřejných chatů, internetových seznamek, instant messengerů, inzertních a herních portálů a různých specializovaných portálů pro nezletilé uživatele.[72]

3.3.2 Kdo jsou pachatelé

Pachatelé kybergroomingu jsou nejčastěji muži, jedná se o heterogenní skupinu, kde jsou uživatelé s nízkým i vysokým sociálním statutem. Často jde o osamělé muže (rozvedené, svobodné), jsou však dostupné i případy, kdy měli pachatelé vlastní rodinu a vlastní děti. Pro kybergroomera je komunikace s dětmi přednější než s dospělými, protože se s dětmi cítí bezpečněji, je to pro něj méně ohrožující.

Velice často oběť útočníka zná, může se jednat o příbuzného nebo známého rodiny. U většiny predátorů byl diagnostikován patologický zájem o děti (na různé úrovni, z různých důvodů – nejenom sexuálních). Maximálně 10 % útočníků trpí pedofilní deviací s orientací na děti předpubertálního věku, větší část

[71] Kybergrooming: Online predátoři a kybergrooming. Kybergrooming: Online predátoři a kybergrooming [online]. Dostupné z: http://www.kybergrooming.cz/
[72] Tamtéž.

pachatelů tvoří víceméně heterogenní skupinu, která zahrnuje hebefily, efebofily, sadisty, jedince trpící asociální poruchou osobnosti, infantilismem, ale také např. různými sexuálními agresemi, exhibicionismem apod. V mnoha případech predátor na oběť zaútočil právě proto, že ji vnímal jako přístupnější, čímž u něj nedochází k poruše sexuální preference, ale jeho konání má za následek rozumový deficit.

Pachatelé mohou být všech věkových skupin (od 17 do 70let). Velice často bývají pachatelé věkově blízcí obětem.[73]

V českém prostředí se v kontextu s kybergroomingem a filmem „V síti“ hovoří o pachatelích jako o tzv. online predátorech. Tento termín je poměrně široký, může jít jak o osoby s vysokým, tak i nízkým stupněm společenské nebezpečnosti.

3.3.3 Kdo jsou oběti

V případě kybergroomingu nezáleží na pohlaví oběti. Dívky a chlapci jsou ve vyrovnaném poměru 50:50, nejčastější věk oběti je 11 až 17 let.

Velice často bývá typickou obětí dítě s malým sebevědomím, s nízkou mírou sebeúcty, nedostatkem sebedůvěry, děti mají emocionální problémy, jsou v nouzi, naivní nebo přehnaně důvěřivé. Není výjimkou i dítě, které je materiálně zajištěné a má v podstatě vše co potřebuje, ale chybí mu čas věnovaný rodiči. Dítě strádá nedostatkem emocionální péče a zájmu ze strany rodiče. Dalším typickým příkladem jsou děti, které si vyhledávají informace o sexu z důvodu pouhé zvědavosti a predátoři jim tyto informace velice rádi sdělují a poskytují.

3.3.4 Kybergrooming a právo

Předmětný trestný čin je upraven v ustanovení § 193b trestního zákoníku. Právnická nebo fyzická osoba, která dítěti mladšímu patnácti let, tedy dítěti, které není schopno dát zodpovědný souhlas k pohlavnímu styku, navrhne setkání s cílem spáchat na něm trestný čin pohlavního zneužití, výroby a jiného nakládání

[73] Tamtéž.

s dětskou pornografií, zneužití dítěte k výrobě pornografie a svádění k pohlavnímu styku, popř. jiný trestný čin se sexuální pohnutkou (může jít např. o trestný čin obchodování s lidmi či trestný čin sexuálního nátlaku) naplní objektivní stránku skutkové podstaty trestného činu navazování nedovolených kontaktů s dítětem.[74]

Kybergrooming i kyberstalking jsou formy počítačové kriminality, vykonávané s cílem způsobit druhému bolest či jej jinak poškodit. Pachatelé, ale své počínání takto nevidí, potřebují především uspokojit své vlastní potřeby a představy a sebekontrola u nich nefunguje.[75]

3.4 Krádež identity

Za krádež identity (označováno jako identity theft) se považuje zmocnění se virtuální identity oběti pachatelem. Dochází ke krádeži přístupových údajů k emailovým schránkám, uživatelským účtům na různých sociálních sítích, nebo také může jít o přístupové údaje k počítačovým hrám a následné vydávání se pachatele za oběť.

V případě neúspěšného napadení ze strany útočníka, kdy se mu nepodaří získat přihlašovací údaje oběti (na sociální síť apod.), stáhne si útočník veškerá dostupná data o oběti (profilový obrázek, jméno apod.) a tyto informace použije k vytvoření duplicitního profilu oběti, a poté oslovuje přátele poškozeného.[76]

Odcizenou identitu v pojetí kyberšikany útočník využívá nejčastěji k:

- poškození oběti (přidáváním nevhodných statusů, komentářů, nevhodná komunikace s přáteli či známými oběti),
- krádež citlivých dat oběti (např. za účelem následného vydírání),

[74] Kybergrooming - INTERNETEM BEZPEČNĚ. INTERNETEM BEZPEČNĚ - Užívejme internet bezpečnějším způsobem [online]. Copyright © 2018 INTERNETEM BEZPEČNĚ. Všechna práva vyhrazena. [cit. 02.03.2022]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybergrooming/

[75] O nás [online]. Copyright © [cit. 28.12.2021], str. 15. Dostupné z: https://www.ncbi.cz/odborna-knihovna/category/6-metodiky-ucebni-materialy.html?download=37:metodika-kybergrooming-a-kyberstalking

[76] Krádež identity - INTERNETEM BEZPEČNĚ. INTERNETEM BEZPEČNĚ - Užívejme internet bezpečnějším způsobem [online]. Copyright © 2018 INTERNETEM BEZPEČNĚ. Všechna práva vyhrazena. [cit. 10.02.2022]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/kradez-identity/

- zisk citlivých dat důvěrného přítele oběti (informace, které by přítel oběti sdělil pouze jí),
- páchání trestné činnosti jménem oběti.

Odcizenou identitu v pojetí kybernetické trestné činnosti útočník využívá k:

- k phishingovým a malwarovým útokům na osoby, se kterými oběť často komunikuje,
- rozesílání spamu,
- zisku veřejně nedostupných informací (např. informace o společnosti, nastavení bezpečnosti ostatních služeb apod.),
- získání přístupů do jiných služeb (řada online služeb umožní, pouze na základě zadání e-mailové adresy, změnu hesla. Díky tomu, že útočník ovládá e-mailovou schránku napadeného, získá tím i přístup do dalších online služeb oběti).[77]

3.4.1 Krádež identity a právo

- Krádeží identity může dojít k naplnění skutkové podstaty zejména trestného činu neoprávněný přístup k počítačovému systému a nosiči informací (§ 230 trestního zákoníku), opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 trestního zákoníku), porušení tajemství dopravovaných zpráv (§ 182 trestního zákoníku), poškození cizích práv (§ 181 trestního zákoníku).

3.5 Šíření poplašné zprávy

Jedním z trestných činů, k jejichž páchání dochází v rámci sociálních sítí, a které jsou v tomto prostředí zvýšeně nebezpečné, neboť jsou zde i více efektivní, je šíření poplašné zprávy (§ 357 trestního zákoníku). To se ukázalo

[77] Krádež identity - INTERNETEM BEZPEČNĚ. INTERNETEM BEZPEČNĚ - Užívejme internet bezpečnějším způsobem [online]. Copyright © 2018 INTERNETEM BEZPEČNĚ. Všechna práva vyhrazena. [cit. 23.02.2022]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/kradez-identity/

mj. i v souvislosti s onemocněním COVID-19 a následnou koronavirovou pandemií.

3.5.1 Šíření poplašné zprávy a právo

Aby se jednalo o trestný čin šíření poplašné zprávy, musí se jednat o zprávu nepravdivou, a to buďto poplašnou či i jinou, každopádně vždy musí tato zpráva vyvolat opatření, které vede ke znepokojení, obavám z ohrožení života, zdraví, majetku, základních práv a svobod, a to v důsledku nějakých událostí, musí vést k panice, úzkosti, strachu, zmatkům a zmatečnému a neúčelnému chování nebo vede k malomyslnosti či poraženecké náladě minimálně určité části obyvatel na určitém místě nebo musí být zbytečně povoláni pracovníci Integrovaného záchranného systému podle § 357 trestního zákoníku.[78]

3.6 Sexting

Sexting je poměrně nový fenomén, který je úzce spjat s používáním informačních a komunikačních technologií mladými, dětmi i dospělými. Slovo sexting je složenina vzniklá ze slov sex a textování a znamená elektronické rozesílání textových zpráv (SMS), fotografií či videí se sexuálním obsahem. Tyto záznamy (fotografie, videa) jsou pak často zveřejněny na internetu, především tehdy, pokud dojde k ukončení vztahu. První případy sextingu byly zaznamenány již v roce 2005.[79]

Pokud je účastníkem sextingu mladistvý nebo dítě, velice často při něm dochází k šíření dětské pornografie. V našich podmínkách se každý jednotlivý případ sextingu řeší individuálně, někdy se případy vyhodnocují pouze jako přestupek, ale dost často také jako trestný čin (záleží na druhu fotografií a jiného

[78] Jiří Jelínek: K trestnímu postihu šíření poplašné zprávy (nejen o koronaviru) - Česká justice. Homepage - Česká justice [online]. Dostupné z: https://www.ceska-justice.cz/2020/06/jiri-jelinek-k-trestnimu-postihu-sireni-poplasne-zpravy-nejen-koronaviru/

[79] Co je sexting - E-Bezpečí. Projekt E-bezpečí - E-Bezpečí [online]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/sexting/137-154

podobného materiálu a způsobu jejich pořízení), u mladých lidí může být tato forma komunikace považována za trestný čin ohrožování výchovy dítěte (§ 201 trestního zákoníku).[80]

3.6.1 Sexting a právo

I když sexting jako takový není trestním zákoníkem specificky definován jako trestné jednání, je spojován s celou řadou trestných činů a velice často je jejich páchání jeho neoddělitelnou součástí. Judikatura s tímto termínem už aktivně pracuje. Podle ní je to forma autopornografického díla, kterou děti a dospívající velmi lehce vytvoří a sdílí.[81]

Východisko právního rámce sextingu představuje premisa, že osoby mladší 18 let sice mohou mít sex [v zájmu stručnosti ponechávám stranou složitější problematiku věkové hranice trestného činu pohlavního zneužití podle § 187 trestního zákoníku a otázku trestní odpovědnosti mladistvých za jeho spáchání podle zákona č. 218/2003 Sb., zákona o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů (zákon o soudnictví ve věcech mládeže), neboť by to tuto část nepřiměřeně zatížilo], nesmí se však při sexuálním styku fotografovat či natáčet. Pak by se totiž mohlo jednat o trestný čin výroby a nakládání s dětskou pornografií dle § 192 trestního zákoníku.[82]

Při sextingu může dojít k naplnění skutkové podstaty hned několika trestných činů, např. znásilněni (§ 185 trestního zákoníku), sexuální nátlak (§ 186 trestního zákoníku), pohlavní zneužití (§ 187 trestního zákoníku), šíření pornografie (§ 191 trestního zákoníku), výroba a jiné nakládání s dětskou pornografií (§ 192 trestního zákoníku), zneužití dítěte k výrobě pornografie (§ 193a

---

[80] Sexting.cz - vše, co chcete vědět o sextingu. Sexting.cz - vše, co chcete vědět o sextingu [online]. Dostupné z: https://www.sexting.cz/

[81] Tamtéž.

[82] Sexting - INTERNETEM BEZPEČNĚ. INTERNETEM BEZPEČNĚ - Užívejme internet bezpečnějším způsobem [online]. Copyright © 2018 INTERNETEM BEZPEČNĚ. Všechna práva vyhrazena. [cit. 08.01.2022]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/sexting/

trestní zákoníku), navazování nedovolených kontaktů s dítětem (§193b trestního zákoníku), svádění k pohlavnímu činu (§ 202 trestního zákoníku).

3.7 Sextortion

V této poslední kapitole věnované pouze vybraným druhům kyberkriminality bych ještě chtěla zmínit v poslední době nový termín počítačové kriminality, a to sextortion. Tento název vznikl opět spojením dvou slov sex + extortion (sex + vydírání). Jde tedy o sexuální vydírání, kdy pachatel využije intimní materiály (fotografie či videa) proti oběti.[83]

Sextortion může být zacílen na jednotlivce (kterého si pachatel vytipuje např. na sociálních sítích) nebo může mít podobu e-mailového spamu (není zaměřen konkrétně na jednu osobu, ale jde o masové rozesílání).

Tyto dva typy se od sebe liší takto:

- Sextortion zaměřený na jednotlivce znamená, že oběť je oslovena na sociální síti či komunikační aplikaci (např. Messenger, WhatsApp) pachatelem s cílem si popovídat, následuje výměna fotografií, často to končí fotografiemi intimními. Pokud dojde k webkamerové komunikaci, nezřídka pachatel přiměje oběť k různým praktikám (např. masturbace, obnažování). Tento pornografický materiál si pachatel nahraje a uloží a začne oběť vydírat z uveřejnění tohoto materiálu. Pachatel chce další obrázky, videa s pornografickým vyobrazením oběti, nebo finanční obnos.
- Sextortion v podobě e-mailů znamená obdržení e-mailového spamu, kde se píše o nabourání se hackerem do počítače oběti a zisku důvěrných informací z počítačových složek oběti. Pachatel může vyhrožovat i sledováním oběti přes webkameru. Opět jde o vydírání a zastrašování oběti. Cílem pachatele je nejčastěji ziskuchtivost.[84]

[83] Co je sextortion - E-Bezpečí. Projekt E-bezpečí - E-Bezpečí [online]. Dostupné z: https://www.e-bezpeci.cz/index.php/z-nasi-kuchyne/71-trivium/2421-co-je-sextortion
[84] Tamtéž.

4 Definice dítěte

Za dítě je podle českého právního řádu pro tyto účely považována osoba mladší 18 let (§ 126 trestního zákoníku). Legislativa neumožňuje těmto osobám z hlediska psychické a rozumové vyspělosti se plně svobodně a volně rozhodovat, jestli chtějí být zobrazovány pornograficky. Nemůžou být fotografovány, natáčeny či jinak zachycovány v situacích, které lze označit za pornografické.[85]

Český právní řád ovšem jako dětskou pornografii postihuje i zobrazení osob pouze se jevících být dítětem. Definici takové osoby nicméně neobsahuje.

4.1 Definice dětské pornografie

Pojem dětské pornografie lze definovat mnoha způsoby. Pokaždé se ale jedná o formu fotografického, nahraného či jinak zachyceného záznamu sexuálního motivu či činnosti, kde je zachyceno dítě jako sexuální aktér nebo objekt. Toto jednání je prováděno za účelem vyvolání pohlavního vzrušení. Jde o snímky či jiné záznamy obnažených dětí zachycující polohy skutečného či předstíraného styku, či snímky obnažených dětí v polohách, kde předvádí pohlavní orgány.[86]

Pornografii, resp. dětskou pornografii je třeba definovat zejména pomocí odborné literatury.

Jan Chmelík podal stručně a jasně definici dětské pornografie takto: „*zobrazení dětských pohlavních orgánů, pohlavního nebo jiného sexuálního styku s dítětem nebo mezi dětmi.*“[87]

Legální definici pornografie, resp. dětské pornografie obsahuje např. čl. 9 odst. 2 Úmluvy o počítačové kriminalitě.[88] Podle českého práva je zakázáno, zveřejňovat, zprostředkovávat, nabízet, či jinak dávat do oběhu a zpřístupňovat

[85] Počítačová mravnostní kriminalita - Policie České republiky. Úvodní strana - Policie České republiky [online]. Copyright © 2021 Policie ČR, všechna práva vyhrazena [cit. 04.02.2022]. Dostupné z: https://www.policie.cz/clanek/pocitacova-mravnostni-kriminalita.aspx
[86] Tamtéž.
[87] CHMELÍK, Jan. Mravnost, pornografie a mravnostní kriminalita. Praha: Portál, 2003. ISBN 80-7178-739-6, str. 216
[88] Viz níže sub 4.2.1.

dětskou pornografii. Bohužel je třeba uvést, že i dítě může být tím, kdo pornografii vyrábí či šíří.[89]

Šíření dětské pornografie patří do skupiny nežádoucích sociálně patologických jevů, pachateli bývají lidé trpící parafilií či určitou sexuální deviací (pedofilie), ale mohou to být i osoby, jejichž hlavní a zásadní důvod takového jednání je zisk.[90]

Právě internet, sociální sítě a různá diskusní fóra nahrávají pachatelům, aby mezi sebou mohli vzájemně komunikovat a vyměňovat si již zmíněný materiál. Predátoři využívají hojně výměnnou internetovou síť (peer-to-peer connection), kdy se po předchozí komunikaci spojí dva počítače a probíhá výměna pornografického materiálu.

Bohužel je třeba podotknout, že počty případů dětské pornografie stále narůstají, a rozhodně neklesají. Nicméně díky neustále se vyvíjejícím moderním technikám v oblasti kriminalistiky je určitě snadnější tyto případy odhalit a usvědčit.[91]

4.2 Dětská pornografie a právo

V této kapitole stručně popíši základní prvky trestněprávní úpravy postihu dětské pornografie a jednání spojených s její výrobou a držením.

4.2.1 Mezinárodněprávní úprava

Základním dokumentem mezinárodního práva v oblasti dětské pornografie jako kyberzločinu je Úmluva o počítačové kriminalitě (Budapešť, 23. 11. 2001; č. 104/2013 Sb. m. s.; tzv. Budapešťská úmluva).

---

[89] Sexting.cz - vše, co chcete vědět o sextingu. Sexting.cz - vše, co chcete vědět o sextingu [online]. Dostupné z: http://sexting.cz

[90] Pedofilie, hebefilie a efebofilie | Parafilik.cz. Parafilik.cz - Nemůžete za své pocity, můžete za své činy [online]. Dostupné z: https://parafilik.cz/info/parafilie/pedofilie/

[91] Sdílení souborů na Internetu a sítě P2P - základní technologický přehled - PCWorld.cz. PCWorld.cz | Novinky ze světa softwaru hardwaru a internetu [online]. Copyright © 2020 [cit. 04.02.2022]. Dostupné z: https://www.pcworld.cz/clanky/sdileni-souboru-na-internetu-a-site-p2p-zakladni-technologicky-prehled/

Tato úmluva ukládá povinnost smluvním státům své právní řády upravit tak, aby byl zajištěn pokud možno jednotný trestněprávní postih pachatelů bez ohledu na místo, kde je trestný čin spáchán.

Úmluva upravuje podrobněji oblast dětské pornografie v rámci informačních technologií především v čl. 9 (Trestné činy související s dětskou pornografií). Tato jednání se podle Budapešťské úmluvy klasifikují jako tzv. trestné činy související s obsahem. Mezi tento druh počítačové kriminality patří výroba dětské pornografie za účelem její distribuce prostřednictvím počítačového systému, nabízení nebo zpřístupnění dětské pornografie prostřednictvím počítačového systému, distribuce nebo přenos dětské pornografie prostřednictvím počítačového systému, opatřování dětské pornografie prostřednictvím počítačového systému pro sebe nebo jinou osobu a uchovávání dětské pornografie v počítačovém systému nebo jiném takovém zařízení pro uchovávání počítačových dat.

Podle Úmluvy se za dětskou pornografii považuje pornografický materiál, který vizuálně zobrazuje nezletilou osobu, která provozuje jednoznačný sexuální akt, osobu vypadající jako nezletilá, která provozuje jednoznačný sexuální akt či realistické zobrazení s nezletilou osobou provozující jednoznačný sexuální akt.

Za nezletilou osobu je považována osoba, která je mladší 18 let, je zde ovšem dána možnost smluvním státům tuto věkovou hranici upravit podle jejich vlastního právního řádu. Nejnižší možná hranice je však Úmluvou určena na 16 let.[92]

Také je ponecháno na rozhodnutí státu, zda bude jako trestný čin postihovat opatřování či uchovávání dětské pornografie prostřednictvím počítačového systému pro sebe nebo jinou osobu, či zda bude za dětskou pornografii považovat pouze zobrazení nezletilé osoby provozující jednoznačný sexuální akt.

Úmluva zavazuje smluvní strany k postihu rovněž právnických osob, pokud se dopustily či podílely na trestných činech, které Úmluva upravuje (čl. 12). Tento postih může mít podobu buď trestněprávní (v ČR by se mohlo jednat o postih podle

[92] GŘIVNA, T. Trestné činy proti lidské důstojnosti v sexuální oblasti v novém trestním zákoníku. Bulletin advokacie, 2009, č. 10, s. 70

zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim), anebo občanskoprávní či správní (odpovědnost za přestupek).

V rovině procesního práva, upravuje Úmluva nejpodrobněji některé instituty mezinárodní justiční spolupráce, zejména vydávání osob (čl. 24), právní pomoc (čl. 25 a násl.), jakož i některé nástroje specifické pro počítačovou kriminalitu (čl. 29 až 34)[93]. Pokud jde o mezinárodní policejní spolupráci, zavazuje Úmluva k vytvoření sítě 24/7 a k určení kontaktních bodů (za ČR je tímto kontaktním bodem Policejní prezidium[94]).

4.2.2 Úprava v právu Evropské unie

Na úrovni unijního práva se trestním postihem dětské pornografie zabývá zejména Směrnice Evropského parlamentu a Rady 2011/93/EU ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV.

Směrnice definuje dětskou pornografii v čl. 2 písm. c) jako jakýkoliv materiál, kde je zobrazováno dítě či osoba jevící se jako dítě při skutečném nebo předstíraném sexuálním chování, dále zobrazení pohlavních orgánů dítěte nebo osoby jevící se jako dítě pro sexuální účely a stejně tak realistické zobrazení dítěte při sexuálním chování a realistické vyobrazení pohlavních orgánů pro sexuální účely. Oproti Budapešťské úmluvě definuje Směrnice výslovně rovněž pornografické představení.

Podle této směrnice jsou členské státy EU povinny upravit trestné činy týkající se pohlavního zneužívání (čl. 3), trestné činy týkající se sexuálního vykořisťování (čl. 4), trestné činy týkající se dětské pornografie (čl. 5) a navazování kontaktu s dětmi k sexuálním účelům (čl. 6).

Mezi trestné činy týkající se dětské pornografie Směrnice řadí zejména nabývaní nebo držení dětské pornografie, vědomé získání přístupu k dětské pornografii prostřednictvím informačních a komunikačních technologií, šíření nebo

[93] Viz výše sub kapitola 1.3.
[94] Viz prohlášení ČR podle čl. 35 Úmluvy.

přenos dětské pornografie, nabízení, dodávání nebo zpřístupňování dětské pornografie a výrobu dětské pornografie.

Mezi trestné činy týkající se kontaktu s dětmi k sexuálním účelům Směrnice řadí zejména návrh dospělé osoby na setkání s dítětem, které nedosáhlo věku pohlavní dospělosti, prostřednictvím informačních a komunikačních technologií za účelem spáchání některého z trestných činů uvedených v čl. 3 odst. 4 a čl. 5 odst. 6 Směrnice.

Podobně jako Budapešťská úmluva zavazuje i Směrnice k postihu právnických osob (čl. 13). Závazek ze směrnice je nicméně více orientován na postih trestní, případně správní.

S ohledem na skutečnost, že jednotlivé instituty mezinárodní justiční spolupráce a mezinárodní policejní spolupráce jsou upraveny obecnými předpisy EU, je procesně-právní úprava obsažená ve Směrnici zaměřena více na prevenci, na pomoc, podporu a ochranu dětských obětí, na ochranu dětských obětí při vyšetřování trestných činů a řízeních, opatření proti příležitostem ke zneužívání reklamy a sexuální turistiky zaměřené na děti, programy či opatření preventivní intervence, prevenci, intervenční programy či opatření na dobrovolném základě v průběhu trestního řízení nebo po jeho skončení, opatření proti internetovým stránkám obsahujícím či šířícím dětskou pornografii.

4.2.3 Úprava ve vnitrostátním právu

Trestné činy související s dětskou pornografií jsou zařazeny do 2. části trestního zákoníku, zvláštní části, hlavy III. nazvané trestné činy proti lidské důstojnosti v sexuální oblasti.

Konkrétně se jedná o trestný čin výroby a jiného nakládání s dětskou pornografií (§ 192 trestního zákoníku), trestný čin zneužití dítěte k výrobě pornografie (§ 193 trestního zákoníku), trestný čin účasti na pornografickém představení (§ 193a trestního zákoníku) a trestný čin navazování nedovolených kontaktů s dítětem (§ 193b trestního zákoníku).

Výroba a jiné nakládání s dětskou pornografií (§192 trestního zákoníku)

Skutková podstata trestného činu výroby a jiného nakládání s dětskou pornografií je naplněna, pokud někdo:

a) přechovává fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě nebo osobu, která se jeví být dítětem,

b) prostřednictvím informační nebo komunikační technologie získá přístup k dětské pornografii,

c) někomu jinému opatří (vyrobí, doveze, vyveze, proveze, nabídne, veřejně zpřístupní, zprostředkuje, uvede do oběhu, prodá či jinak opatří) pornografické dílo, které zobrazuje nebo jinak využívá dítě nebo osobu, jež se jeví být dítětem, anebo kdo z takového pornografického díla kořistí.

Podle trestního zákoníku může mít tedy dětská pornografie podobu fotografickou, filmovou, počítačovou, elektronickou, jinou (například modelové ztvárnění, písemný projev).

Zneužití dítěte k výrobě pornografie (§ 193 trestního zákoníku)

Skutková podstata trestného činu zneužití dítěte k výrobě pornografie spočívá v úmyslném zlákání, svedení nebo zneužití dítěte (kdo přiměje, zjedná, najme) k výrobě pornografického díla nebo v kořistění z účasti dítěte na takovém pornografickém díle.

Účast na pornografickém představení (§ 193a trestního zákoníku)

Skutková podstata tohoto trestného činu je naplněna, pokud se někdo účastní pornografického představení nebo jiného obdobného vystoupení, ve kterém účinkuje dítě.

Navazování nedovolených kontaktů s dítětem (§ 193b trestního zákoníku)

V tomto případě je skutková podstata naplněna tehdy, když někdo navrhne setkání dítěti mladšímu 15 let, za účelem spáchat trestný či jiný sexuálně motivovaný čin (podle § 187 odst. 1, § 192, § 193, § 202 odst. 3). Jedná se tedy o specifickou formu přípravného jednání.

5 Internet a dětská pornografie

Dětská pornografie neexistuje pouze na internetu, ale je potřeba zdůraznit, že internet patří mezi největší druhy rizika přenosu pornografického materiálu. Prakticky umožňuje dostat materiál z bodu A (pachatel) do bodu B (zájemce). Hraje zde velikou roli anonymita poskytovaná kyberprostředím pro pachatele i možného zájemce. Předmětná data se navíc šíří prostřednictvím serverů fyzicky umístěných často v mnoha různých státech, což dále ztěžuje odhalení a postih pachatelů.

5.1 Dítě jako oběť, ale i osoba, která zprostředkovává dětskou pornografii

Díky dnešní době, která je provázaná vymoženostmi všech moderních technologií, se můžeme připojit k internetu prakticky kdykoliv a kdekoliv pomocí chytrých zařízení (tabletů, mobilů, notebooků). To znamená, že děti mají přístup ke všem možným sociálním sítím, seznamkám, či různým diskuzním portálům. Můžou se zde realizovat, psát o sobě důvěrné informace typu, kde bydlí, jakou školu navštěvují, mohou psát o tom, jak se cítí, nebo jakou mají náladu. Díky těmto funkcím, které internet a sociální sítě zvláště umožňují, mohou děti a mladistvé oslovit, sledovat a poznat cizí lidé. Děti a mládež se tak stávají lehce obětmi kyberkriminality. Toto se samozřejmě netýká pouze dětí, ale i všech věkových skupin. Distributoři dětské pornografie a jiní sexuální delikventi jsou si toho samozřejmě velice dobře vědomi a díky sociálním sítím snáze hledají možné dětské oběti. Této praktice – vylákání dítěte na schůzku za účelem jeho zneužití nebo vylákání pro získání pornografického materiálu – se odborně říká kybergrooming a již jsem se o něm zmiňovala v předchozí kapitole.

Je ovšem důležité zdůraznit, že dítě se může stát nejen obětí pro účely dětské pornografie, ale i zprostředkovatelem, či dokonce tím, kdo tento materiál rozesílá dál. V tomto opačném případě si pachatel vyhledá na sociální síti, různých fórech či chatech možnou oběť, vzbudí v ní důvěru, dokonce může dojít i k citové vazbě a následně vše použije proti dítěti. Pachatel se snaží vylákat z dítěte fotografie, kde je vyobrazeno jeho nahé tělo, nebo ho přesvědčí se svléknout před

web kamerou s cílem si tuto nahrávku uložit, popřípadě zneužít a následně zveřejnit. V momentě, kdy dítě tyto fotografie či nahrávky nafotí a odešle, sdílí tím zmiňovaný materiál pomocí informačních technologií a tím dojde k tomu, že samotné dítě materiál dál šíří a stává se z něj automaticky zprostředkovatel, ba dokonce možný pachatel trestného činu, resp. provinění (podle zákona č. 218/2003 Sb., o soudnictví ve věcech mládeže). Tento způsob se nazývá sexting a již jsem jej také podrobněji popsala v přechozí kapitole. Jde tedy o vylákání intimních fotografií či nahrávek z nezletilého dítěte.[95]

Opět se nejedná pouze o problém dětí, do této situace se může dostat i dospělá osoba.

Mnohdy si oběť uvědomí riziko, kterému se vystavila, a odmítne opětovně zaslat pornografický materiál agresorovi. Pak nastává situace, kdy agresor/pachatel začne oběť vydírat a nezletilá osoba ze strachu, že se možné nahrávky a fotografie zveřejní na přístupných místech, pošle nové fotografie a stane se z toho začarovaný kruh. Nezletilý si vlastně vůbec neuvědomuje, že zaslaný materiál je již ve většině případů zveřejněn, a místo toho, aby se svěřil rodičům či to řádně nahlásil policii, v tomto protiprávním počínání pokračuje.

5.2 Fotografie na sociálních sítích

Problém publikování rodinných fotografií, kde jsou zobrazeny děti, si dost často rodiče ani prarodiče neuvědomují. Sdílí fotografie dětí či vnoučat například při koupání ve vaně nebo z dovolené u moře na sociálních sítích. Je třeba vědět, že tyto fotografie, pokud zobrazují nahé dítě, mohou být zneužity jako pornografie a s jejich využitím být spáchán trestný čin.[96]

Sociální sítě typu Facebook, Twitter, YouTube a další se snaží potírat všechny formy nezákonného obsahu těchto příspěvků. Tyto společnosti při tom spolupracují s orgány činnými v trestním řízení, což vede k efektivnějšímu vyhledávání a postihu této trestné činnosti. Ale pravdou je, že to stále nestačí.

---

[95] Sexting.cz - vše, co chcete vědět o sextingu. Sexting.cz - vše, co chcete vědět o sextingu [online]. Dostupné z: http://sexting.cz/

[96] Child pornography allegations in the age of social media - The Law Office of Brian Jones, LLC. Delaware Criminal Defense Attorneys | Ohio | The Law Office of Brian Jones, LLC [online]. Dostupné z: https://thelawofficeofbrianjones.com/child-pornography-allegations-in-the-age-of-social-media/

Přestože Facebook, Instagram a další online platformy provedly určité změny, což znamená mazání nevhodného obsahu. Nejsou tato opatření zdaleka dostatečná a nejsou zaváděna tak rychle a efektivně jak situace vyžaduje.[97]

Odstranění nevhodného obsahu je obvykle prováděno pomocí automatického filtru nebo díky uživatelům služby, kteří obsah označí jako nevhodný. Je zcela nemožné, aby lidé prozkoumávali každý jednotlivý příspěvek uveřejněný na sociálních sítích.[98]

Společnosti nechtějí být spojovány se zneužíváním dětí, a proto se snaží škodlivý obsah co nejrychleji odstranit. Společnost Apple přišla nedávno se zajímavou možností prověřování v úložišti iCloud uživatelů. Pomocí automatizovaných algoritmů se snaží porovnávat nahrané soubory uživatelů se snímky v databázi orgánů činných v trestním řízení. Toto automatizované vyhledávání však může být spojeno i s řadou rizik (např. falešné shody). Navíc je zde i otázka velkých kulturních rozdílů ve vnímání nahoty, včetně té dětské.[99]

Z pohledu ochrany soukromí to tedy není příliš dokonalé, ale určitě je to dobrý kompromis, který v případě technického zdokonalení napomůže odhalování a postihu této trestné činnosti.[100]

[97] The rising tide of child abuse content on social media across the world – COUNTERVIEW.ORG. COUNTERVIEW.ORG – Voluntary blogging platform [online]. Dostupné z: https://counterview.org/2021/07/19/the-rising-tide-of-child-abuse-content-on-social-media-across-the-world/
[98] Tamtéž.
[99] Tamtéž.
[100] Tamtéž.

6 Rodičovská kontrola aktivit dětí na počítači, tabletu či mobilním telefonu

Moderní doba se již vůbec nepodobá té době, ve které jsme vyrůstali my. Rodiče se vůbec nemuseli starat o naše online aktivity, protože žádné neexistovaly. Současnost je v tomto směru bohužel velmi odlišná. Vzhledem k tomu, že stále více času trávíme prací a školou z domova, je nezbytné mít správnou kontrolu nad tím, co děti na počítači, tabletu či mobilním telefonu dělají. Všechen potenciálně nebezpečný obsah zcela odfiltrovat samozřejmě nelze, ale lze ho alespoň částečně omezit. Měli bychom mít ale na paměti, že dítě je častěji zdatnější v oblasti IT nežli rodič a většinou si cestu, jak aspoň částečně obejít restrikce a omezení najde.

Omezit aktivitu nezletilých a dětí na počítači, tabletu či mobilním telefonu a k tomu navíc i zaznamenat, co se na něm děje, dnes dokáže každý operační systém. V této kapitole bych ráda nastínila alespoň základní možnosti rodičovské kontroly.

6.1 Operační systém Windows a MacOS

Oba počítačové operační systémy mají v sobě integrovanou základní rodičovskou kontrolu. Microsoft tuto funkci použil poprvé ve versi Windows 7, ovšem sofistikovanější nastavení se objevilo až s verzí Windows 10. Apple možnost rodičovské kontroly integroval do svého operačního systému již před mnoha lety a s každou novou verzí tuto funkcionalitu vylepšuje

V obou operačních systémech může rodič nastavit časové limity pro používání počítače, či doby připojení k internetu, nebo které aplikace a hry může dítě používat. Dále lze blokovat nežádoucí weby, a jelikož je systém propojen s cloudem, mohou rodiče dostávat pravidelné zprávy o používání počítače. V neposlední řadě je tu možnost omezit nákup věcí z obchodů Microsoft Store či Appstore. Placené stahování může být úplně zakázáno, nebo je rodičům zaslán e-mail s žádostí o povolení nákupu a instalace dříve, než se něco stane. Používání je jednoduché. Jedinou a skutečnou nevýhodou je, že se musí dítěti zřídit účet.

6.2 Mobilní zařízení

V kategorii tabletů a mobilních telefonů se v podstatě setkáváme jen se dvěma operačními systémy a tím je Android od společnosti Google a iOS od společnosti Apple. Jelikož se mobilní operační systémy stále více a více přibližují těm počítačovým, jsou i jejich funkce velice podobné. Stejně jako na PC lze i u mobilních zařízení omezit dobu připojení k internetu, lze omezit používané aplikace a hry a zamezit jejich stahování a instalování. U mobilních zařízení lze díky integrované GPS sledovat jejich aktuální polohu. Lze vymezit perimetr, kde se může dítě s mobilním telefonem pohybovat. Po opuštění tohoto prostoru přijde rodičům SMS zpráva o jeho opuštění.

6.3 Software třetích stran

Pro sofistikovanější rodičovskou kontrolu můžeme použít software třetích stran. Na trhu je v tomto směru velice štědrá nabídka jak bezplatných, tak placených softwarů od renomovaných společností, které se zabývají ochranou dat. Většina softwarových společností poskytuje například 14denní zkušební verzi, během které si rodič může tyto produkty vyzkoušet. Většina těchto programů se skládá ze dvou částí. Klientské a webové. Klientská část se nainstaluje na sledované zařízení a pomocí webové části se tento program spravuje. Tyto specializované softwary mají daleko více funkcí a nastavení než ty integrované v operačním systému. Kupříkladu u mobilních telefonů takový software přebírá veškerou správu. Takový telefon lze odposlouchávat, číst veškeré zaslané a přijaté SMS, nebo komunikaci na sociálních sítích. Tyto softwary běží skrytě na pozadí systému a udržují informace o všech navštívených internetových stránkách a spuštěných programech. Ty nejlepší softwary analyzují obsah stránek, filtrují vulgarismy a umožňují přidávat vlastní klíčová slova a kategorie,

které chcete blokovat. V současnosti začíná být standardní dvoufázové ověření pro přístup k účtu.[101]

[101] The Best Parental Control Software for 2022 | PCMag. The Latest Technology Product Reviews, News, Tips, and Deals | PCMag [online]. Copyright © 1996 [cit. 13.02.2022]. Dostupné z: https://www.pcmag.com/picks/the-best-parental-control-software

7 Vlastní dotazníkový průzkum

Státní orgány by se měly snažit trestnou činnost nejen pouze represivně postihovat, ale pokud možno jí i předcházet. Pro účinnou prevenci je přitom zásadní dostatečné povědomí veřejnosti o tom, jaká jednání jsou vlastně trestná. Pro zjištění toho, jak běžní uživatelé informačních technologií vnímají počítačovou kriminalitu, a především pak problematiku dětské pornografie na sociálních sítích, jsem sestavila malý průzkum.

Šetření jsem provedla formou tištěného dotazníku v mém zaměstnání (Ministerstvo zahraničních věcí), v zaměstnání mého manžela (Technický ústav požární ochrany) a v mém okolí (rodina, přátelé).

Dotazník byl sestaven a formulován pro běžné uživatele internetu. Dotazníkem jsem se snažila analyzovat, jaké máme znalosti v oblasti dětské pornografie na sociálních sítích, a také mě zajímalo, na jakých sítích jsme nejvíce aktivní a kolik času na nich trávíme.

Dotazník byl rozdán mezi cca 70 lidí a vyplněných se mi jich vrátilo 60. Dotazník obsahuje 17 otázek.

Výsledky, kterých jsem dosáhla vyhodnocením mého dotazníku, nepředstavují všeobecný názor všech občanů žijících v ČR, ale analýza nám dostatečně poslouží určit, jaké vědomosti máme v oblasti dětské pornografie na sociálních sítích, jaké sociální sítě navštěvujeme, co na nich hledáme a co sdílíme.

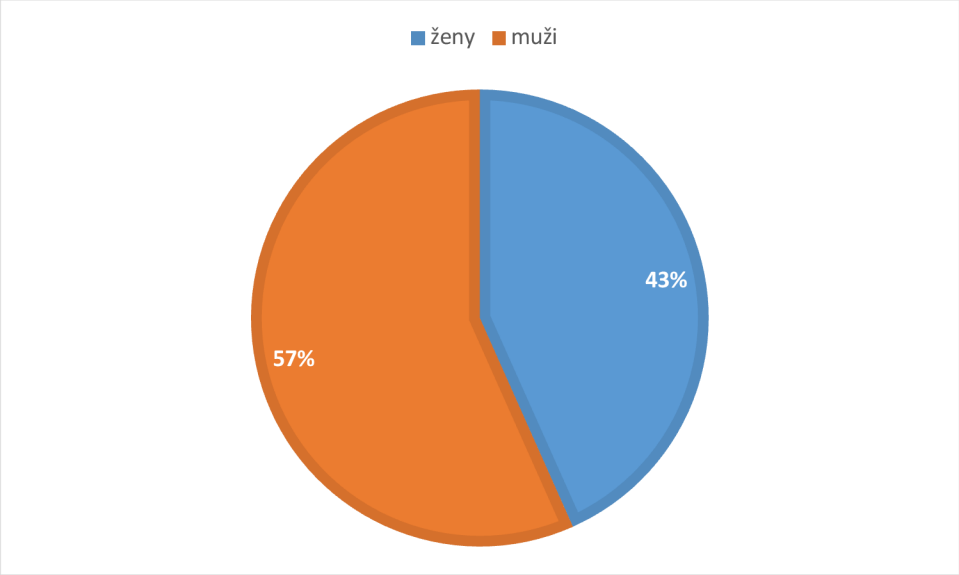
Dotazník

1. Pohlaví
2. Věk
3. Vzdělání
4. Používáte sociální sítě?
5. Na jaké sociální síti trávíte nejvíce času?
6. Kolik času trávíte na sociálních sítích?
7. Jaký obsah na sociálních sítích nejvíce vyhledáváte?
8. Sdílíte soukromé fotografie svých dětí na sociálních sítích?

9. Víte, co znamená pojem dětská pornografie?
10. Víte, od kterého věku zobrazované osoby se může jednat o dětskou pornografii?
11. Je každé zobrazení nahého či polonahého dítěte dětskou pornografií?
12. Může být za některých okolností zobrazení dospělé osoby považováno za dětskou pornografii?
13. Podle čeho posuzujeme věk zobrazované osoby?
14. Setkali jste se na sociálních sítích s dětskou pornografií?
15. Pokud ano, na kterých sociálních sítích?
16. Měl by stát více aktivněji přispívat k potírání kyberkriminality v oblasti dětské pornografie?
17. Pokud ano, jakým způsobem?

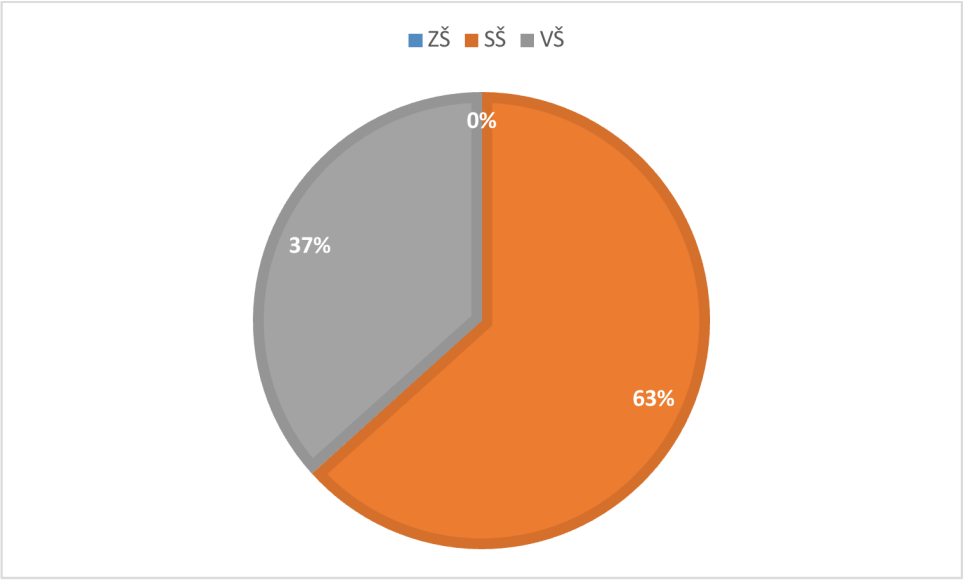
7.1 Vyhodnocení dotazníku

Otázky č. 1 a 2 byly zaměřené na pohlaví a věk respondentů. V mém případě tvoří zastoupení mužů 57 %, ženy tvoří 43 %. Při hlubší analýze vyplynulo, že průměrný věk mužů je 32 let a průměrný věk žen 29 let.



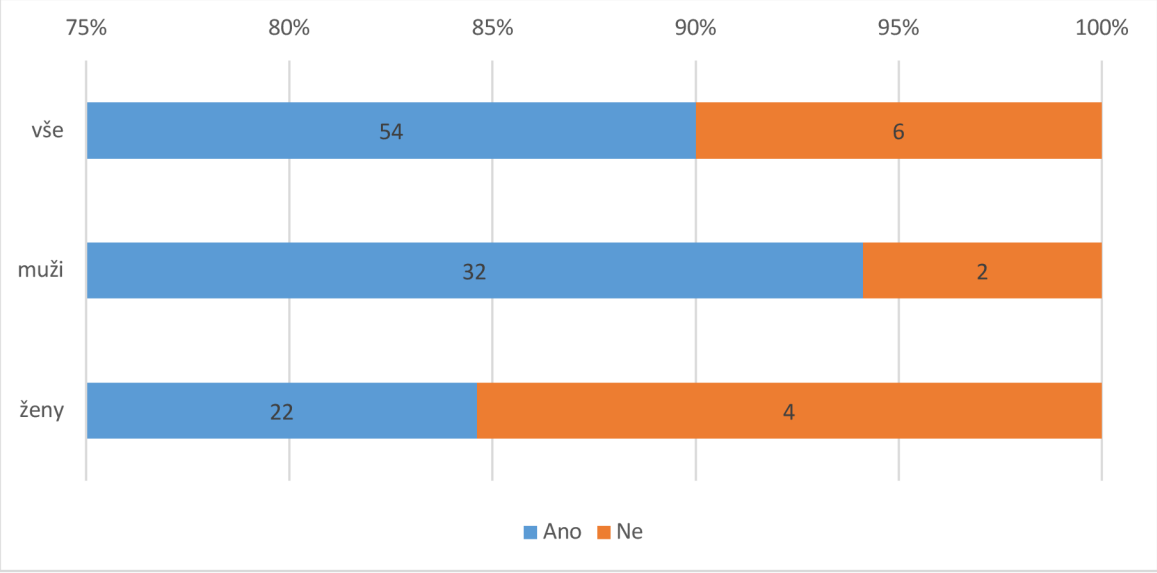
Obrázek č. 5: Věk a pohlaví respondentů (zdroj: vlastní)

Otázka číslo 3 byla zaměřena na vzdělání. Ani jeden z respondentů neměl jen základní vzdělání. Největší část, a to 63 % tvořilo středoškolské vzdělání. 37 % respondentů mělo vysokoškolské vzdělání. Větší část tvořili vysokoškolsky vzdělaní muži.



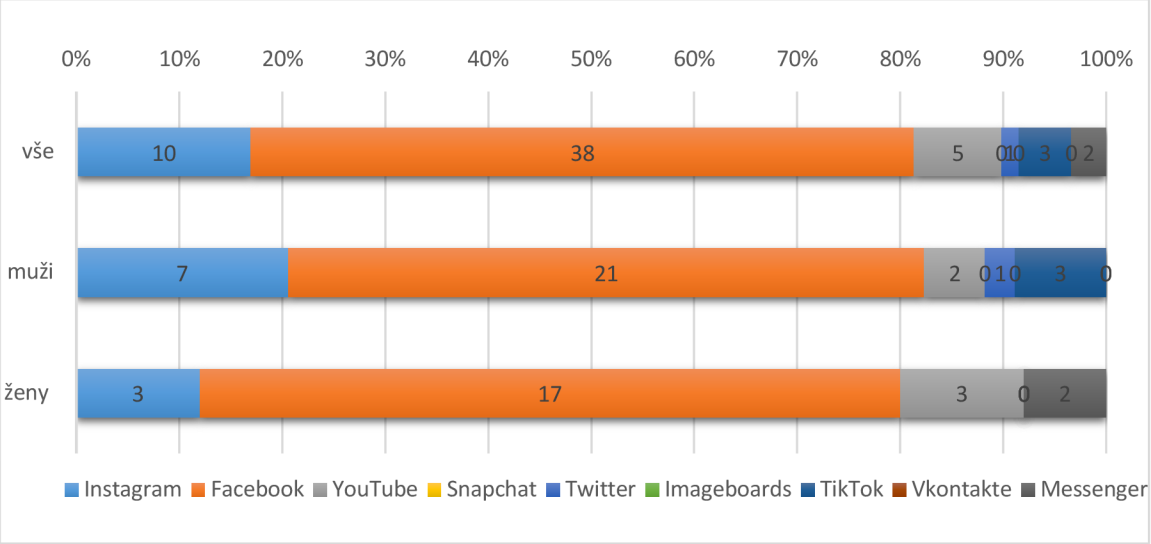
Obrázek č. 6: Používáte sociální sítě?

Otázka č. 4 směřovala na to, zda respondenti používají pravidelně sociální sítě. Jak je vidět z grafu níže, většina dotazovaných sociální sítě pravidelně využívá. Bylo to předem jasné. Z grafu můžeme vidět, že muži jsou na sociálních sítích častěji než ženy.



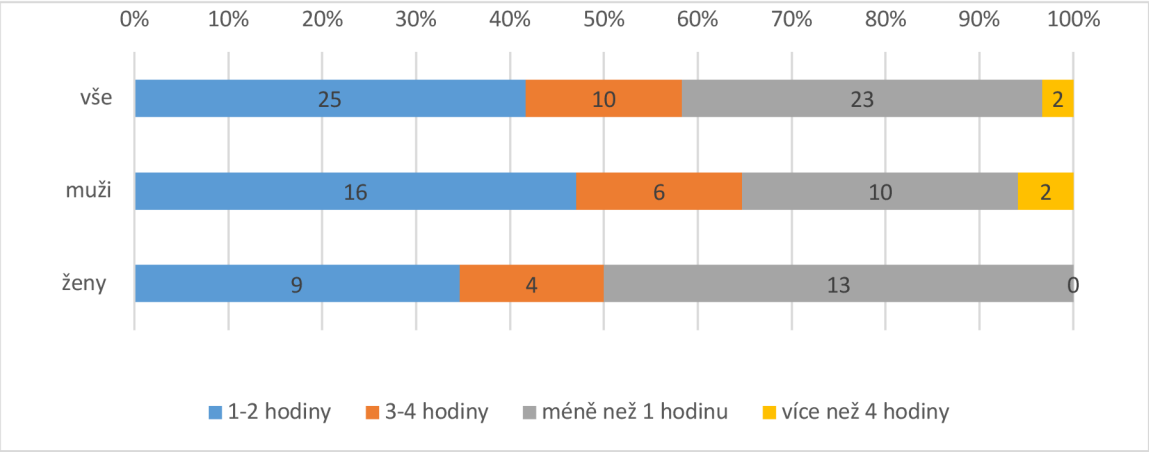
Obrázek č. 7: Na jaké sociální síti trávíte nejvíc času?

Otázka č. 5 směřovala už na konkrétní sociální sítě. Dotazovala jsem se respondentů, na jakých sociálních sítích tráví nejvíce času. Jak je vidět z grafu, data získaná v dotazníku korespondují s oficiálními statistikami uváděnými na internetu. Nejvíce respondentů tráví čas na Facebooku, dále následuje Instagram, poté v menší míře YouTube. Ostatní sociální sítě jsou vyloženě okrajovou záležitostí. Otázka pohlaví, zde nehraje skoro žádnou roli.



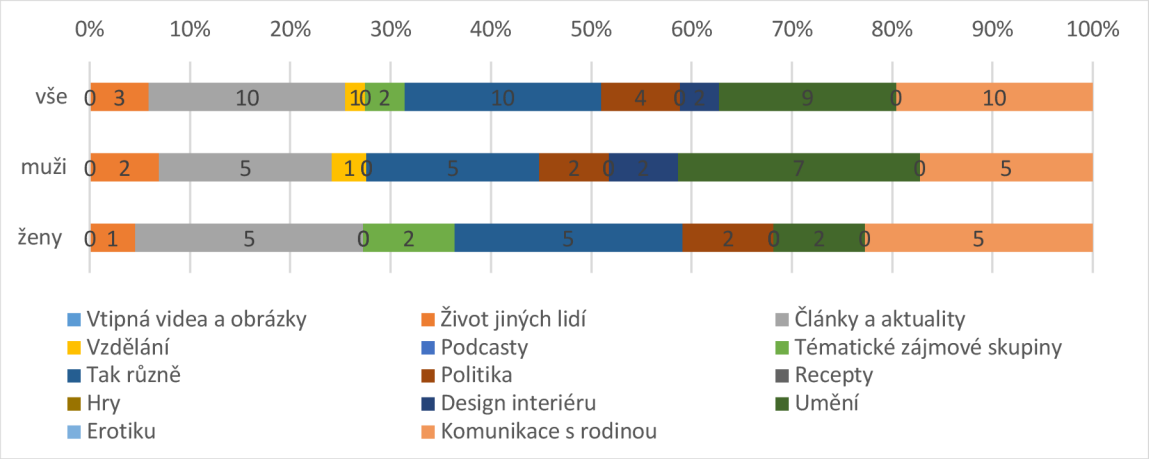
Obrázek č. 8: Na jaké sociální síti trávíte nejvíce času?

Otázka č. 6 měla za úkol zjistit, kolik času tráví respondenti na sociálních sítích. Jak je z grafu patrné, velká část dotazovaných tráví na sociálních sítích maximálně 2 hodiny denně. U žen je čas strávený na sociálních sítích ještě kratší. Větší část žen tráví na sociálních sítích méně než hodinu a jen 4 dotazované ženy na nich tráví více než 3 hodiny denně. U mužů je trend malinko jiný. Muži tráví na sociálních sítích více času, větší část dotazovaných do dvou hodin denně. Vysvětlení, proč muži tráví na sociálních sítích více času než ženy, může dle mého názoru souviset s trávením volného času, kdy se ženy musí více starat o domácnost a péči o děti než muži.



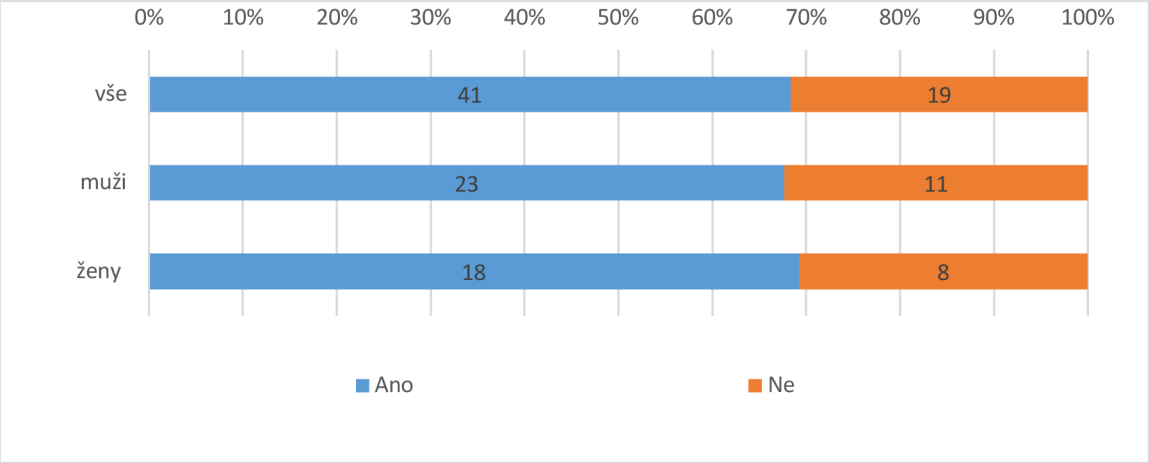
Obrázek č. 9: Kolik času trávíte na sociálních sítích?

Otázka č. 7 měla ukázat, co respondenti nejčastěji vyhledávají na sociálních sítích, obávám se, že tím, že nikdo nepřiznal i erotiku, tak průzkum v této otázce nebyl zcela upřímný.



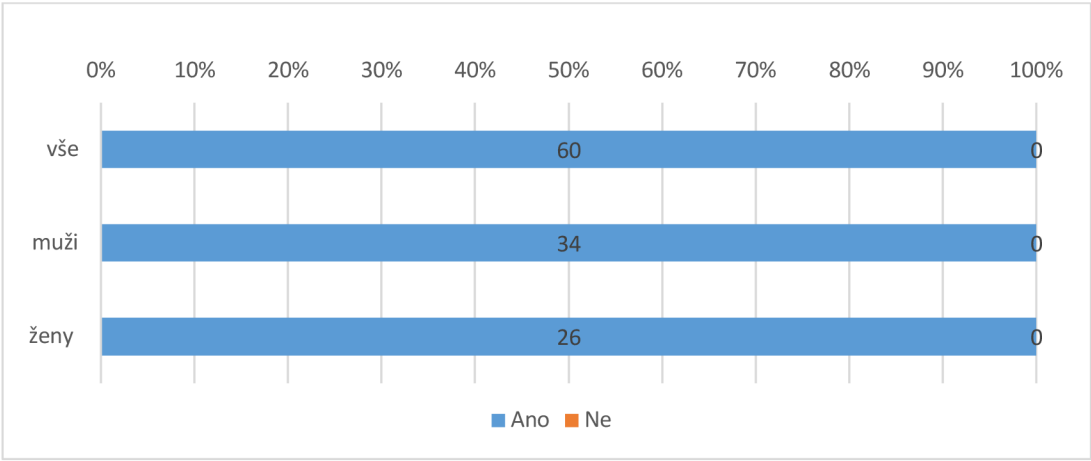
Obrázek č 10: Jaký obsah na sociálních sítích nejvíce vyhledáváte?

Otázka č. 8 směřovala ke zjištění, zda dotazovaní sdílejí na sociálních sítích fotografie svých dětí například z dovolených, výletů, či jiných rodinných aktivit. V tomto případě není žádný rozdíl, obě pohlaví vyšla v podstatě nastejno. Dá se říct, že 2/3 dotazovaných někdy fotku dítěte na sociální síti sdílelo.



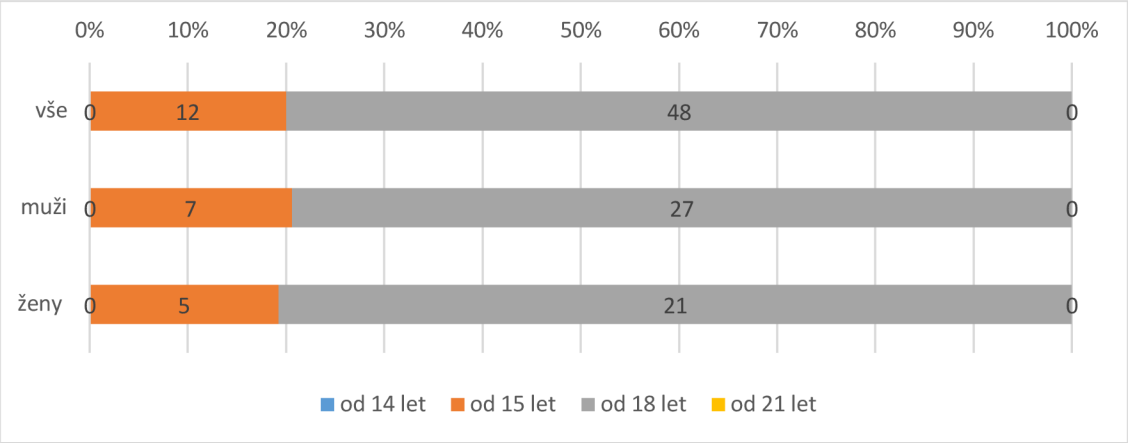
Obrázek č. 11: Sdílíte soukromé fotografie svých dětí na sociálních sítích?

Otázka č. 9 zněla „Víte, co znamená pojem dětská pornografie?“ Nebylo žádným překvapením, že 100 % respondentů si myslí, že ví, co to dětská pornografie je. Jak je patrné z odpovědí na následující otázku, ne vždy tomu tak však skutečně bylo.



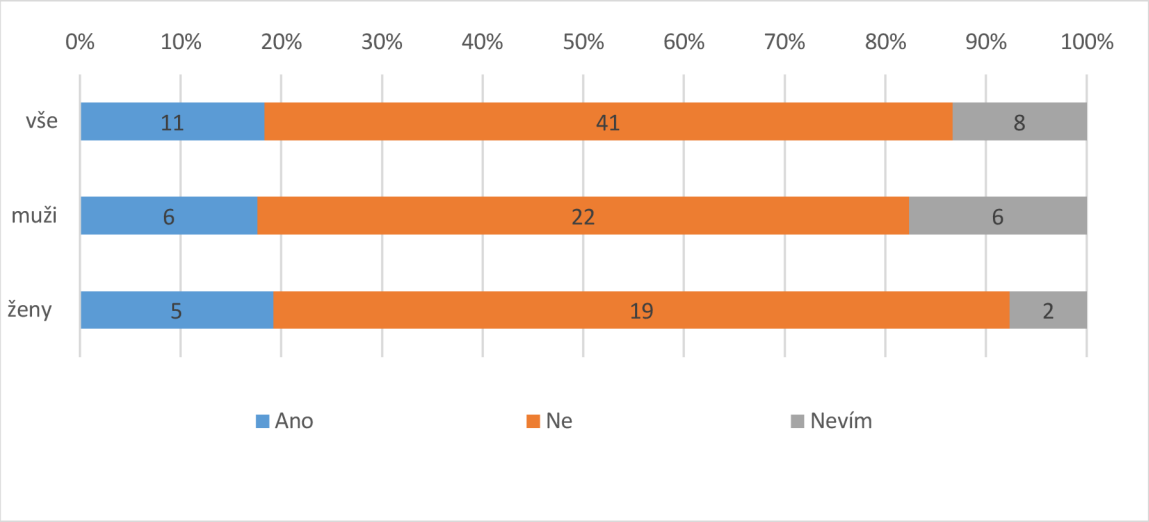
Obrázek č. 12: Víte, co znamená pojem dětská pornografie?

V otázce č. 10 jsem se zjišťovala, zda dotazovaní ví, od kterého věku zobrazované osoby se může jednat o dětskou pornografii. Na výběr bylo ze čtyř možností a to od 14 let, od 15 let, od 18 let, nebo od 21 let. Zde nejvíce lidí odpovědělo správně.



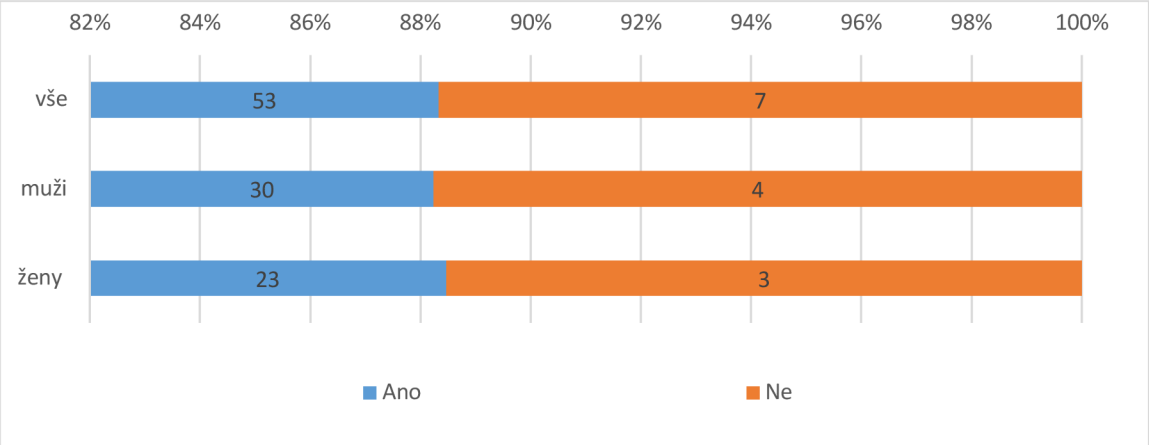
Obrázek č. 13: Víte, od kterého věku zobrazované osoby se může jednat o dětskou pornografii?

Otázka č. 11 ukázala, že veřejnost si není zcela jista odpovědí, neboť 2/3 dotazovaných odpovědělo nevím.



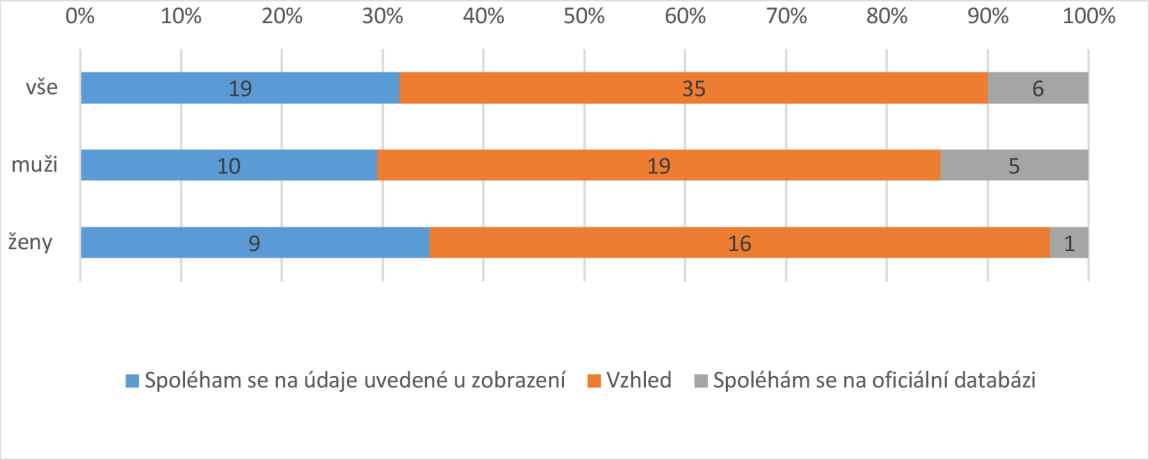
Obrázek č. 14: Je každé zobrazení nahého či polonahého dítěte dětskou pornografií?

Otázka č. 12 potvrdila i v tomto bodě neznalost dotazovaných ohledně dětské pornografie, 7 dotazovaných odpovědělo chybně. Podle českého právního řádu se postihuje i zobrazení osob, jevících se být dítětem.



Obrázek č. 15: Může být za některých okolností zobrazení dospělé osoby považováno za dětskou pornografii?

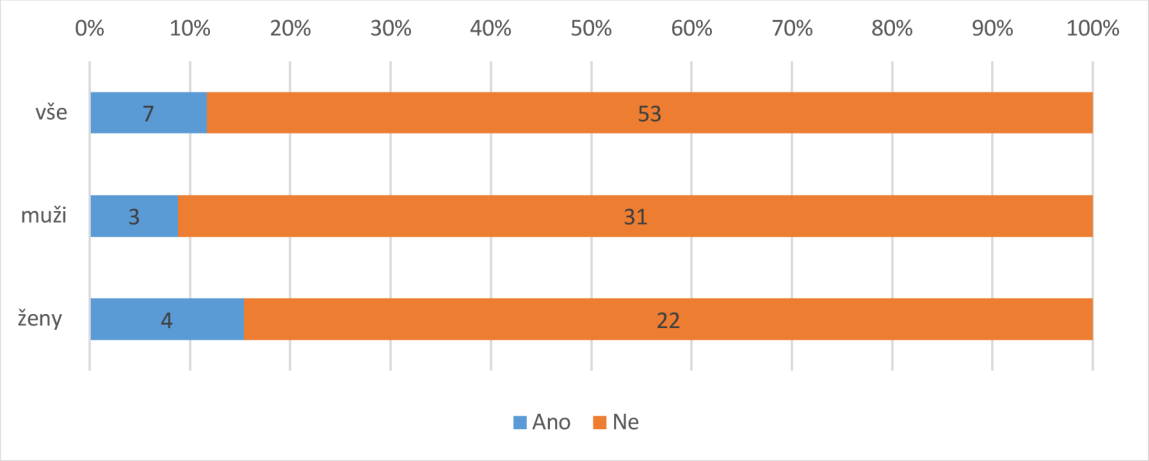
V otázce č. 13 jsem zjišťovala, podle čeho dotazovaní posuzují věk zobrazované osoby. Největší část respondentů posuzuje věk osoby podle vzhledu, zhruba 30 % spoléhá na údaje uvedené u zobrazení a jen 10 % se spoléhá na oficiální databázi. Je vidět, že v této otázce si dotazovaní nejsou jisti. Z toho, že někdo odpověděl i poslední možnost, je vidět, že se o daný problém nikdy nezajímal.



Obrázek č. 16: Podle čeho posuzujeme věk zobrazované osoby?

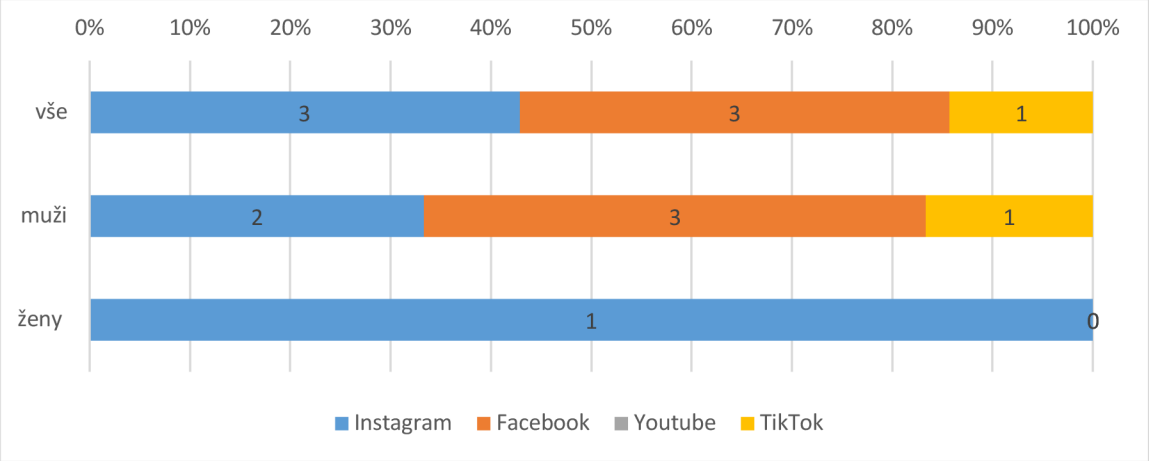
Otázka č. 14 měla za úkol zjistit, zda se dotazovaní setkali na sociálních sítích s dětskou pornografií. 90 % dotazovaných uvedlo, že se s dětskou pornografií nesetkalo. Z dotazovaných mužů jen 3 uvedli, že se s dětskou pornografií na sociálních sítích setkali. Poněkud překvapivé je, že se s dětskou

pornografií setkaly 4 respondentky, tj. počet žen převažuje. To však může být způsobeno i lepším odhadem věku. Rozdíl nicméně není statisticky významný.



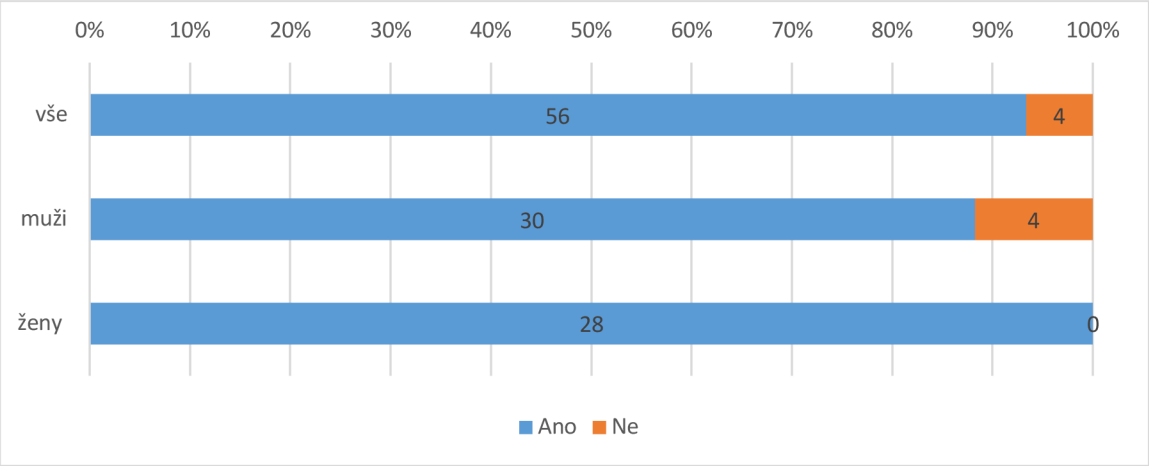
Obrázek č. 17: Setkali jste se na sociálních sítích s dětskou pornografií?

V otázce č. 15 se vyjádřili pouze ti, kteří v předchozí otázce odpověděli kladně.



Obrázek č. 18: Pokud ano, na kterých sociálních sítích?

V otázce číslo 16 jsem se respondentů dotazovala, zda by měl stát být aktivnější k potírání PC kriminality v oblasti dětské pornografie. Zde panovala u dotazovaných shoda s tím, že by stát měl být aktivnější v této oblasti. Já sama si to myslím také.



Obrázek č. 19: Měl by stát více aktivněji přispívat k potírání kyberkriminality v oblasti dětské pornografie?

Otázka číslo 17 byla dobrovolná a týkala se způsobu, jakým by měl stát být aktivnější při potírání počítačové kriminality. Jako nejčastější se objevovaly odpovědi:

a) osvěta mezi mládeží
b) zvýšený dohled nad dodržováním pravidel na sociálních sítích ze strany jejich provozovatelů
c) zpřísnění trestních sankcí (zvýšení sazeb trestu odnětí svobody)

7.2 Závěrečná analýza dotazníku

Cílem mého dotazníkového šetření bylo zjistit, jak dotazované skupiny respondentů vnímají kyberkriminalitu na sociálních sítích. Zaměřila jsem se především na dětskou pornografii na sociálních sítích. Zajímalo mě, zda dotazovaní ví, co dětská pornografie je a jestli mají respondenti alespoň základní právní znalosti v této problematice. Dále jsem chtěla analyzovat, jaké sociální sítě dotazovaní nejvíce používají, jak na nich tráví svůj čas, a hlavně kolik času jim věnují. To může být významné z hlediska pravděpodobnosti výskytu takového závadného obsahu, neboť ne všechny sítě tento obsah vyhledávají a odstraňují (a pokud ano, ne se stejnou efektivitou).

Z mého šetření je vidět, že poměr žen a mužů je téměř vyrovnaný a že se sociální sítě staly už běžnou součástí našich životů a patří k naší každodennosti.

Podle mého názoru si stále mnoho lidí neuvědomuje rizika spojená se sdílením osobních informací (fotografie a další média, názory, příspěvky), což bylo ukázáno ve výsledcích mého dotazníku, a tím se velice snadno mohou stát obětmi pachatelů různých forem počítačové kriminality.

Dále je z mého dotazníkového šetření patrné, že všichni dotazovaní používají sociální sítě a jsou na nich aktivní. Nejvíce populární sociální sítí je Facebook, na druhém místě je Instagram, což se shoduje s realitou dle statistik uvedených v předchozích kapitolách.

Co se týče obsahu, který lidi nejvíce zajímá, tak vede zábava a komunikace, dále odborné články a materiály potřebné k práci a vzdělání.

Lidé by si měli především dávat pozor na to, co na internetu dělají, jaké důvěrné informace o sobě poskytují, neměli by být naivní, protože internet rozhodně není místo, kde se nemusí dodržovat určitá pravidla. Technologicko-informační prostředí se neustále mění a je plné nových možností a příležitostí, bohužel však ne vždy správných, pozitivních, a hlavně v souladu se zákonem.

8 Závěr

Ve své práci jsem se snažila ukázat na to, s čím se potýkáme každý den v našich životech, a to především na naši aktivitu na sociálních sítích. Snažila jsem se zhodnotit a analyzovat kyberkriminalitu v sociálních sítích, její hrozbu pro společnost, ale i ve světě ostatních chytrých technologií. Kyberkriminalita vznikla a vyvíjela se od počátku vytvoření technologií, které její vznik a působení umožňují.

Sociální sítě se staly součástí našich životů, máme pocit, že jakoukoliv informaci musíme na jejich stránkách sdílet s ostatními. Kdo není na sociální síti, jako by neexistoval. Málokdo si uvědomuje ohromné riziko, které je s tím spojené, a to kyberkriminalitu. Rozvoj informačních technologií a počítačových systémů a stejně tak celé společnosti je tak rychlý, že se nedaří dostatečně pružně reagovat ze strany zákonodárců. Proto se celosvětově věnuje obrovské úsilí s cílem regulovat tento druh kriminality a předcházet problémům, vyvíjet nové technologie na větší ochranu, předvídání a stíhání této kriminální činnosti.

Toto tvoří z kyberkriminality fenomén hodný naší pozornosti a hloubkového zpracování. Počty případů této nedovolené činnosti neustále rostou. Důvodů pro to je několik. Internet poskytuje pocit anonymity, počítačová kriminalita může být páchána po celém světě, může překonávat velké vzdálenosti mezi poškozeným a pachatelem. Typickým příkladem je právě dětská pornografie, která se díky internetu a sociálním sítím šíří ohromnou rychlostí.

Dostupnost počítačů a jiných technologických zařízení, jejich nízká cena a zvyšující se výkon umožňují stále více lidem přijít do styku s tímto druhem kriminality jak na straně oběti, tak pachatele. Proto je velice důležité výchovně působit a neustále šířit osvětu a preventivní opatření, aby se aspoň trochu zamezilo a redukovalo protiprávní jednání v kyberprostředí. Jak ukázalo mé dotazníkové šetření, osvěta není zcela účinná a v povědomí veřejnosti stále existují mezery.

Díky internetu prakticky neexistují hranice států a spojuje celý svět na jednom místě. Proto tento problém není otázkou národní, ale celosvětovou.

Při odhalování a postihu počítačové kriminality, dětskou pornografii nevyjímaje, je tedy zcela zásadní mezinárodní spolupráce orgánů činných v trestním řízení.

Je pravda, že počítače, internet a chytré telefony patří dnes už do základního vybavení téměř každé domácnosti. Slouží nám jako zdroj zábavy, usnadňují nám životy, snadno si díky nim můžeme vyměňovat informace. Děti, které v tomto digitálním světě vyrůstají odmala, se velice rychle učí ovládat všechny možné technologie, a ne vždy jsou tyto technická vybavení ke škodě, děti si díky nim mohou procvičovat různá cvičení, můžou se díky nim rozvíjet. Ale stejně jak může být využívání chytrých zařízení a internetu prospěšné stejně tak tomu může být naopak a je potřeba znát různá omezení, která se dají nainstalovat v podobě různých softwarů na ochranu dětí, což jasně a efektivně omezí jejich možnosti prohlížení si různých nepříznivých stránek na internetu.

Neexistuje zaručený způsob, jak se dá ochránit proti počítačové kriminalitě, ale mnohdy úplně stačí pouhé dodržování základních pravidel bezpečného užívání internetu, a to především při obyčejném prohlížení a surfování po internetové síti a komunikaci na sociálních sítích. Musíme mít stále na paměti, že internet není prostředí, kde dodržování pravidel není potřeba – nejedná se o bezpečné prostředí. Je to obrovský prostor, kde číhá řada nebezpečí. Není žádoucí o sobě uvádět příliš mnoho důvěrných informací, je třeba mít na paměti, že cokoliv se někdy vloží na sociální sítě, stává se součástí veřejného prostoru a může s tím kdokoliv a jakkoliv nakládat, nemluvě o tom, že se to stává majetkem té dané sítě a ta s tímto obsahem může nakládat, jak se jí zlíbí a tvořit si vlastní databáze atd. Je důležité vlastnit dobrý a spolehlivý antivirový systém, který nám pomůže předejít případným kyberútokům na našem zařízení a hlavně používat „selský rozum“.

Podle mého názoru by se o problémech kyberkriminality na sociálních sítích mělo více mluvit hlavně ve školách formou přednášek, diskusí a možná i tento problém začlenit do školních osnov v rámci počítačové gramotnosti a neuškodilo by i více mediální pozornosti, protože nejvíce ohroženou skupinou jsou děti a dospívající. Jsou vystavováni neustálému sociálnímu tlaku a často si vůbec nestihnou uvědomit rizika spojené s jejich aktivitou na sociálních sítích.

Bohužel dnešní uspěchaná doba nahrává skutečnosti, že rodiče velice často nedokážou zhodnotit míru škodlivosti a využívání sociálních sítí z důvodu své zaneprázdněnosti a neinformovanosti o možných nových úskalích v této oblasti a jiných okolností. Toto je velmi závažný problém, který vyžaduje pečlivou analýzu a ochranu dětí a mládeže před touto hrozbou. To ovšem neznamená, že dospělí jsou odolní, imunní a neovlivnitelní. Ochrana před riziky by se měla vztahovat na celou společnost a ta by měla vynaložit mimořádné úsilí v zájmu zdravého života a rozvoje všech svých občanů.

Seznam použité literatury

1. Monografie

[1] ČERNÁ, Alena. Kyberšikana: průvodce novým fenoménem. Praha: Grada, 2013. Psyché (Grada). ISBN 978-80-247-4577-0.

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

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

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

[5] KOLOUCH, Jan a Pavel BAŠTA. CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.

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

[7] ŠEVČÍKOVÁ, Anna. Děti a dospívající online: vybraná rizika používání internetu. Praha: Grada, 2014. Psyché (Grada). ISBN 978-80-247-5010-1.

[8] ŠMAHAJ, Jan. *Kyberšikana jako společenský problém: Cyberbullying as a social problem*. Olomouc: Univerzita Palackého v Olomouci, 2014. ISBN 978-80-244-4227-3.

2. Odborné články

[1] GŘIVNA, T. Trestné činy proti lidské důstojnosti v sexuální oblasti v novém trestním zákoníku. Bulletin advokacie, 2009, č. 10.

3. Prameny práva

a) Mezinárodní smlouvy

Úmluva o boji proti počítačové kriminalitě (Budapešť, 23. 11. 2001; č. 104/2013 Sb. m. s.)

b) Předpisy Evropské unie

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

c) Vnitrostátní právní předpisy

[1] zákon č. 218/2003 Sb., zákona o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů (zákon o soudnictví ve věcech mládeže)
[2] zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů
[3] zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim
[4] zákon č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů

4. Internetové zdroje

[1] Barmská menšina Rohingů žaluje sociální sítě za podněcování násilí, chce odškodnění 3,5 miliardy | iROZHLAS - spolehlivé zprávy. iROZHLAS - spolehlivé a rychlé zprávy [online]. Copyright © 1997 [cit. 29.01.2022]. Dostupné z: https://www.irozhlas.cz/zpravy-svet/rohingove-mensina-meta-zaloba-odskodneni-nasili-podnecovani_2112071221_pik

[2] Clearnet, Deepweb, Darknet – OTH Amberg-Weiden. OTH Amberg-Weiden [online]. Dostupné z: https://www.oth-aw.de/informieren-und-entdecken/aktuelles/neuigkeiten/201612203660-clearnet-deepweb-darknet/

[3] Co je sexting - E-Bezpečí. Projekt E-bezpečí - E-Bezpečí [online]. Dostupné z:https://www.e-bezpeci.cz/index.php/temata/sexting/137-154

[4] Co je sextortion - E-Bezpečí. Projekt E-bezpečí - E-Bezpečí [online]. Dostupné z: https://www.e-bezpeci.cz/index.php/z-nasi-kuchyne/71-trivium/2421-co-je-sextortion

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

[6] Cybercrime | Definition, Statistics, & Examples | Britannica. Encyclopedia Britannica | Britannica [online]. Copyright © Ivan Kruk [cit. 27.01.2022]. Dostupné z: https://www.britannica.com/topic/cybercrime

[7] Dangerous TikTok 'skull-breaker challenge' causes child head injuries - ABC13 Houston. KTRK Houston news, weather and traffic - Latest Texas news and weather [online]. Copyright © 2022 ABC, Inc. [cit. 10.02.2022]. Dostupné z: https://abc13.com/tiktok-skill-breaker-challenge-skull-breaker-causes-children-injuries-causing/5959067/

[8] Darknet: temná strana internetu | Chip.cz - recenze a testy. Informace, testy a novinky o hardware, software a internetu – CHIP.cz [online]. Copyright © 2003 [cit. 08.02.2022]. Dostupné z:https://www.chip.cz/casopis-chip/earchiv/vydani/r-2012/chip-02-12/darknet/

[9] Definice Internetu. Home [online]. Dostupné z: http://ijs.8u.cz/index.php/internet/definice-internetu

[10] Facebook | Overview, History, & Facts | Britannica. Encyclopedia Britannica | Britannica [online]. Copyright © Anatoli Styf [cit. 09.02.2022]. Dostupné z: https://www.britannica.com/topic/Facebook

[11] Facebooku budeme dál říkat pravým jménem. Hrozba, zní od kritiků - Seznam Zprávy. Seznam Zprávy [online]. Copyright © 1996 [cit. 20.01.2022]. Dostupné z: https://www.seznamzpravy.cz/clanek/meta-misto-facebooku-budeme-mu-rikat-pravym-jmenem-hrozba-zni-od-kritiku-179077

[12] Facebook to pay record $5 billion U.S. fine over privacy; faces antitrust probe | Reuters. Breaking International News & Views | Reuters [online]. Copyright © 0 Reuters. All Rights Reserved. [cit. 09.02.2022]. Dostupné z: https://www.reuters.com/article/us-facebook-ftc-idUSKCN1UJ1L9

[13] Facebook users in Czechia - November 2021 | NapoleonCat. Engage and Support Customers on Social Media – NapoleonCat [online]. Copyright © Napoleon Sp. z o.o. [cit. 12.12.2021]. Dostupné z: https://napoleoncat.com/stats/facebook-users-in-czechia/2021/11/

[14] How Does Excessive Use Of Electronic Devices Affect The Mental Health Of Kids?. Get Latest News, India News, Breaking News, Today's News - NDTV.com [online]. Copyright © COPYRIGHT NDTV CONVERGENCE LIMITED 2022. ALL RIGHTS RESERVED. [cit. 12.02.2022]. Dostupné z:https://www.ndtv.com/health/how-does-excessive-use-of-electronic-devices-affect-the-mental-health-of-kids-2753503

[15] How Many People Use Social Media in 2022? (65+ Statistics). SEO Training and Link Building Strategies – Backlinko [online]. Copyright © 2022 Backlinko is a Trademark of Backlinko LLC [cit. 09.02.2022]. Dostupné z: https://backlinko.com/social-media-users

[16] How Many People Use Social Media in 2022? (65+ Statistics). SEO Training and Link Building Strategies – Backlinko [online]. Copyright © 2022 Backlinko is a Trademark of Backlinko LLC [cit. 29.01.2022]. Dostupné z: https://backlinko.com/social-media-users#most-popular-social-media-platforms

[17] Child pornography allegations in the age of social media - The Law Office of Brian Jones, LLC. Delaware Criminal Defense Attorneys | Ohio | The Law Office of Brian Jones, LLC [online]. Dostupné z: https://thelawofficeofbrianjones.com/child-pornography-allegations-in-the-age-of-social-media/

[18] Imageboard – Wikipedia. [online]. Dostupné z: https://de.wikipedia.org/wiki/Imageboard

[19] Instagram – Wikipedia. [online]. Dostupné z: https://de.wikipedia.org/wiki/Instagram

[20] Instagram users in Czechia - November 2021 | NapoleonCat. Engage and Support Customers on Social Media – NapoleonCat [online]. Copyright © Napoleon Sp. z o.o. [cit. 12.12.2021]. Dostupné z: https://napoleoncat.com/stats/instagram-users-in-czechia/2021/11/

[21] Internet v Česku slaví 25 let, jako první se připojil tunový počítač - Deník.cz. Deník.cz - informace, které jsou vám nejblíž [online]. Copyright © [cit. 12.02.2022]. Dostupné z: https://www.denik.cz/ekonomika/internet-v-cesku-slavi-25-let-jako-prvni-se-pripojil-tunovy-pocitac-20170214.html

[22] Jak na Internet - Internet a handicapovaní. Jak na Internet - Jak na Internet [online]. Copyright © 2022 CZ.NIC, z. s. p. o. [cit. 12.02.2022]. Dostupné z: https://www.jaknainternet.cz/page/1653/internet-a-handicapovani/

[23] Jiří Jelínek: K trestnímu postihu šíření poplašné zprávy (nejen o koronaviru) - Česká justice. Homepage - Česká justice [online]. Dostupné z: https://www.ceska-justice.cz/2020/06/jiri-jelinek-k-trestnimu-postihu-sireni-poplasne-zpravy-nejen-koronaviru/

[24] Krádež identity - INTERNETEM BEZPEČNĚ. INTERNETEM BEZPEČNĚ - Užívejme internet bezpečnějším způsobem [online]. Copyright © 2018 INTERNETEM BEZPEČNĚ. Všechna práva vyhrazena. [cit. 08.01.2022]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/kradez-identity/

[25] Kybergrooming - INTERNETEM BEZPEČNĚ. INTERNETEM BEZPEČNĚ - Užívejme internet bezpečnějším způsobem [online]. Copyright © 2018 INTERNETEM BEZPEČNĚ. Všechna práva vyhrazena. [cit. 02.03.2022]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybergrooming/

[26] Kybergrooming: Online predátoři a kybergrooming. Kybergrooming: Online predátoři a kybergrooming [online]. Dostupné z: http://www.kybergrooming.cz/

[27] Kyberšikana, Uherské Hradiště. Uherské Hradiště [online]. Copyright © 2001 [cit. 28.12.2021]. Dostupné z: https://www.mesto-uh.cz/kybersikana

[28] Kyberšikana. | e-besedy.cz [online]. Copyright © [cit. 28.12.2021]. Dostupné z: http://www.e-besedy.cz/internetova-bezpecnost/kybersikana.html

[29] Most used social media 2021 | Statista. • Statista - The Statistics Portal for Market Data, Market Research and Market Studies [online]. Copyright © Statista 2021 [cit. 04.12.2021]. Dostupné z: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

[30] Mail.ru koupilo VKontakte, „ruský Facebook“ mění majitele - Lupa.cz. Lupa.cz - server o českém Internetu [online]. Copyright © 1998 [cit. 08.02.2022]. Dostupné z: https://www.lupa.cz/clanky/mail-ru-koupilo-vkontakte-rusky-facebook-meni-majitele/

[31] Neurčité sny a sdílené halucinace - Lupa.cz. Lupa.cz - server o českém Internetu [online]. Copyright © 1998 [cit. 11.02.2022]. Dostupné z: https://www.lupa.cz/clanky/neurcite-sny-a-sdilene-halucinace/

[32] O nás [online]. Copyright © [cit. 28.12.2021]. Dostupné z: https://www.ncbi.cz/odborna-knihovna/category/6-metodiky-ucebni-materialy.html?download=37:metodika-kybergrooming-a-kyberstalking

[33] Pedofilie, hebefilie a efebofilie | Parafilik.cz. Parafilik.cz - Nemůžete za své pocity, můžete za své činy [online]. Dostupné z: https://parafilik.cz/info/parafilie/pedofilie/

[34] Počítačová mravnostní kriminalita - Policie České republiky. Úvodní strana - Policie České republiky [online]. Copyright © 2021 Policie ČR, všechna práva vyhrazena [cit. 04.02.2022]. Dostupné z: https://www.policie.cz/clanek/pocitacova-mravnostni-kriminalita.aspx

[35] Sdílení souborů na Internetu a sítě P2P - základní technologický přehled - PCWorld.cz. PCWorld.cz | Novinky ze světa softwaru hardwaru a internetu [online]. Copyright © 2020 [cit. 04.02.2022]. Dostupné z: https://www.pcworld.cz/clanky/sdileni-souboru-na-internetu-a-site-p2p-zakladni-technologicky-prehled/

[36] Sexting.cz - vše, co chcete vědět o sextingu. Sexting.cz - vše, co chcete vědět o sextingu [online]. Dostupné z: http://sexting.cz/

[37] Sexting - INTERNETEM BEZPEČNĚ. INTERNETEM BEZPEČNĚ - Užívejme internet bezpečnějším způsobem [online]. Copyright © 2018 INTERNETEM BEZPEČNĚ. Všechna práva vyhrazena. [cit. 08.01.2022].

Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/sexting/

[38] SOCIAL MEDIA PLATFORMS AND CYBER CRIME - The Daily Guardian. Latest News | Today's News | Breaking News & India News - The Daily Guardian [online]. Copyright © 2020 TheDailyGuardian [cit. 09.02.2022]. Dostupné z: https://thedailyguardian.com/social-media-platforms-and-cyber-crime/

[39] Social network users in leading markets 2026 | Statista. • Statista - The Statistics Portal for Market Data, Market Research and Market Studies [online]. Copyright © Statista 2022 [cit. 06.02.2022]. Dostupné z: https://www.statista.com/statistics/278341/number-of-social-network-users-in-selected-countries/

[40] Stolen Data of 533 Million Facebook Users Leaked Online. Insider [online]. Copyright © 2022 [cit. 29.01.2022]. Dostupné z: https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-

[41] Explained: What is YouTube? [online]. Copyright © 2019 Sucuri Inc. All rights reserved. [cit. 05.02.2022]. Dostupné z: https://www.webwise.ie/parents/what-is-youtube/

[42] The Best Parental Control Software for 2022 | PCMag. The Latest Technology Product Reviews, News, Tips, and Deals | PCMag [online]. Copyright © 1996 [cit. 13.02.2022]. Dostupné z: https://www.pcmag.com/picks/the-best-parental-control-software

[43] The 16 Biggest Facebook Scandals Mark Zuckerberg Faced. Insider [online]. Copyright © 2022 [cit. 09.02.2022]. Dostupné z: https://www.businessinsider.com/mark-zuckerberg-scandals-last-decade-while-running-facebook-2019-12#5-2018-also-marked-one-of-the-darkest-moments-in-facebooks-history-as-reports-revealed-that-the-social-network-was-used-to-incite-genocide-against-the-muslim-rohingya-minority-in-myanmar-by-the-countrys-military-officials-6

[44] The Pros and Cons of Social Networking. Lifewire: Tech News, Reviews, Help & How-Tos [online]. Dostupné z: https://www.lifewire.com/advantages-and-disadvantages-of-social-networking-3486020

[45] The rising tide of child abuse content on social media across the world – COUNTERVIEW.ORG. COUNTERVIEW.ORG – Voluntary blogging platform [online]. Dostupné z: https://counterview.org/2021/07/19/the-rising-tide-of-child-abuse-content-on-social-media-across-the-world/

[46] TikTok: everything you need to know about the video production app | Parent Zone. Home | Parent Zone [online]. Copyright © 2022 Parent Zone All rights reserved. [cit. 09.02.2022]. Dostupné z: https://parentzone.org.uk/article/tiktok-everything-you-need-know-about-video-production-app

[47] vKontakte: Bei VK.com anmelden und das deutsche VK Login. WC0.de: Die Urlaubs Inspirations Seite für Weltenbummler [online]. Dostupné z: https://www.wc0.de/vkontakte/

[48] Výkladový slovník Kybernetické bezpečnosti - PDF Free Download. Představujeme Vám pohodlné a bezplatné nástroje pro publikování a sdílení informací. [online]. Copyright © DocPlayer.cz [cit. 04.12.2021]. Dostupné z: https://docplayer.cz/2694910-Vykladovy-slovnik-kybernetickebezpecnosti.html

[49] Was ist Twitter? Einfach erklärt - CHIP. Praxistipps zu Problemen mit Windows, Android, iOS, Office, MacOS - CHIP [online]. Copyright © BurdaForward GmbH 2022 [cit. 06.02.2022]. Dostupné z: https://praxistipps.chip.de/was-ist-twitter-einfach-erklaert_49887

[50] What Are the Requirements to Create an Account in Facebook? | Small Business - Chron.com. Small Business - Chron.com [online]. Copyright © 2022 Hearst [cit. 21.01.2022]. Dostupné z: https://smallbusiness.chron.com/requirements-create-account-facebook-56591.html

[51] What is cybercrime? Definition from SearchSecurity. Purchase Intent Data for Enterprise Tech Sales and Marketing - TechTarget [online]. Dostupné z: https://www.techtarget.com/searchsecurity/definition/cybercrime

[52] What is Facebook?. Computer Glossary, Computer Terms - Technology Definitions and Cheat Sheets from WhatIs.com - The Tech Dictionary and IT Encyclopedia [online]. Dostupné z: https://whatis.techtarget.com/definition/Facebook

[53] What is Cyberspace? - Definition from Techopedia. Techopedia: Educating IT Professionals To Make Smarter Decisions [online]. Copyright © 2022 [cit. 27.01.2022]. Dostupné z: https://www.techopedia.com/definition/2493/cyberspace

[54] What is the Internet? Definition from WhatIs.com.. Computer Glossary, Computer Terms - Technology Definitions and Cheat Sheets from WhatIs.com - The Tech Dictionary and IT Encyclopedia [online]. Dostupné z: https://whatis.techtarget.com/definition/Internet

[55] What Is Instagram and Why Should You Be Using It?. Lifewire: Tech News, Reviews, Help & How-Tos [online]. Dostupné z: https://www.lifewire.com/what-is-instagram-3486316

[56] What is Internet? Definition, Uses, Working, Advantages and Disadvantages - GeeksforGeeks. GeeksforGeeks | A computer science portal for geeks [online]. Dostupné z: https://www.geeksforgeeks.org/what-is-internet-definition-uses-working-advantages-and-disadvantages/

[57] What is Social Engineering? | Definition | Kaspersky. Kaspersky Cyber Security Solutions for Home & Business | Kaspersky [online]. Copyright © [cit. 12.02.2022]. Dostupné z: https://usa.kaspersky.com/resource-center/definitions/what-is-social-engineering

[58] What Is The 'Outlet Challenge'? How It Can Electrocute Or Burn You. Forbes [online]. Copyright © 2022 Forbes Media LLC. All Rights Reserved [cit. 10.02.2022]. Dostupné z: https://www.forbes.com/sites/brucelee/2020/02/23/what-is-the-outlet-challenge-how-it-can-electrocute-or-burn-you/?sh=6b7868511e62

[59] What Is VK? (VKontakte Explained) | InstaFollowers. Buy Instagram Followers - %100 Real, Instant | Only $0.59 [online]. Dostupné z: https://www.instafollowers.co/blog/what-is-vk