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

BAKALÁŘSKÁ PRÁCE

SOCIÁLNÍ SÍTĚ – PROSTŘEDÍ PRO TRESTNOU ČINNOST

Autor práce: Kateřina PILÍKOVÁ, DiS.

Studijní obor: Bezpečnostně právní činnost ve veřejné správě

Forma studia: Kombinovaná

Vedoucí práce: Mgr. Romana Morongová

Katedra: Katedra právních oborů a bezpečnostních studií

2020

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

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Kateřina PILÍKOVÁ, DiS.

Studijní program: Bezpečnostně právní činnost
Studijní obor: Bezpečnostně právní činnost ve veřejné správě
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce: Sociální sítě – prostředí pro trestnou činnost

Název bakalářské práce v anglickém jazyce: Social networks - Climate for Crime

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce (jméno a příjmení, titul): Mgr. Romana Morongová

Datum zadání bakalářské práce: říjen 2019

CÍL BAKALÁŘSKÉ PRÁCE:

Cílem této bakalářské práce je zanalyzovat problematiku sociálních sítí jako prostředí trestné činnosti. Konkrétně pro teoretickou část bakalářské práce budou vybrány a blíže rozebrány některé z možných útoků, ke kterým může na sociálních sítí dojít, stejně tak základní pojmy týkající se sociálních sítí a kyberkriminality. V praktické části bude provedena případová studie a návrh vytvoření preventivního programu zaměřujícího se na bezpečné užívání sociálních sítí dětmi a mladistvými.

Student: Kateřina Pilíková, DiS.	26.10.19 *datum*	Pilíková *podpis*
Vedoucí práce: Mgr. Romana Morongová	26.10.19 *datum*	 *podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	4.11.19 *datum*	 *podpis*
Prorektorka pro studium a vnitřní záležitosti: RNDr. Růžena Ferebauerová	12.11.19 *datum*	Ferebauerová *podpis*
Pověřený rektor: doc. Ing. Jiří Dušek, Ph.D.	13.11.2019 *datum*	 *podpis*

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

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

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

.....

Děkuji vedoucí bakalářské práce Mgr. Romaně Morongové za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

PILÍKOVÁ, K. *Sociální sítě – prostředí pro trestnou činnost : bakalářská práce.* České Budějovice : Vysoká škola evropských a regionálních studií, 2020. 67 s. Vedoucí bakalářské práce : Mgr. Romana Morongová.

Klíčová slova: sociální sítě, kyberkriminalita, kyberšikana, kyberstalking, kybergrooming, sexting, prevence

Bakalářská práce pojednává o sociálních sítích, jejichž uživatelé svým rizikovým chováním dovolili, aby se tyto internetové služby proměnily v prostředí, ve kterém v některých případech dochází k nemorálnímu či dokonce protiprávnímu jednání.

První, teoretická část této bakalářské práce sociální sítě analyzuje, rozebírá základní pojmy se sociálními sítěmi související, včetně pojmů souvisejících s kyberkriminalitou. Dále popisuje konkrétní sociální sítě, se kterými se mohou uživatelé internetu setkat. Velký důraz je kladen na analýzu útoků v prostředí sociálních sítí, včetně uvedení možností, jak se jim bránit či jim dokonce zcela předcházet.

Ve zvláštní části této práce je provedena případová studie trestného činu nebezpečného pronásledování, k němuž bylo pachatelem mimo jiné využito sociální sítě Facebook. Druhým výstupem zvláštní části je vytvoření preventivního programu cíleného na děti a mládež, kteří téměř denně sociální sítě využívají, avšak plně si neuvědomují rizika s jejich používáním spojená.

ABSTRACT

PILÍKOVÁ, K. *Social Networks – Climate For Crime : Bachelor Thesis.* České Budějovice : The College of European and Regional Studies, 2020. 67 p. Supervisor : Mgr. Romana Morongová.

Key words: social networks, cybercrime, cyberbully, cyberstalking, cybergrooming, sexting, prevention

This bachelor thesis concerns itself with social networks, whose users with their risky behaviour allowed for them to turn into an environment, in which sometimes immoral or even unlawful behaviour may occur.

First, theoretical part of this bachelor thesis analyses social networks, describes fundamental terms used regarding cybercriminality. Furthermore, it describes particular social networks that may be encountered by the internet users. Strong emphasis is put on analysis of attacks in social networks environment, including possibilities on how one may protect himself from these situations or completely prevent them.

In special part of this thesis a case study of a crime of dangerous persecution is conducted, to which the perpetrator used, among other means, social network Facebook. The second foreground of the special part is the creation of precautionary programme targeted towards children and youth, that almost daily use social networks, although without completely realizing the risks tied to their usage.

Obsah

Úvod

Sociální sítě se staly důležitou a téměř neodmyslitelnou záležitostí dnešní doby, neboť je to právě internet, konkrétně tyto internetové služby v podobě sociálních sítí, kam se přesunula značná část lidského chování, ať už jde o sociální interakce, kulturní a společenské vyžití, hledání informací a další činnosti běžného života. Mezi základní vlastnosti sociálních sítí patří zejména globálnost, která jejich uživatelům dává možnost komunikace bez ohledu na světadíl, časová pásma či konkrétní místo, na kterém se právě nacházejí. Jednou z dalších možností, která je uživatelům sociálních sítí nabízena, a může být snadno zneužita, je anonymita uživatele, neboť identitu osoby lze v kyberprostoru snadno pozměnit či zcela změnit.

Fakt, že se sociální sítě staly rizikovým místem hlavně pro mladé uživatele, potvrzuje skutečnost, že se společnost začala více soustředit na chování uživatelů v prostoru internetu a na sociálních sítích, a cílí na jejich bezpečnost. Zcela aktuální je pak reakce na tabuizovanou problematiku zneužívání dětí na internetu v podobě projektu režisérů Víta Klusáka a Barbory Chaloupkové, kdy dokumentaristé s původním cílem vytvořit pouze krátký spot, který by poukázal na nebezpečí číhající na děti a mládež v internetovém prostředí, a jak snadno mohou být zneužity jejich fotografie k vydírání, nakonec dospěli k vytvoření celovečerního dokumentárního filmu s názvem *V síti*. Tento film má dokonce dvě verze. První, s názvem *V síti*, je necenzurovaná verze určená pouze pro osoby starší patnácti let, zatímco druhá, s názvem *V síti: Za školou*, měla omezený přístup, kdy zhlédnout tento film mohly pouze osoby starší dvanácti let. *Osobně* považuji toto dílo za precizní, neboť právě na jeho základě bylo zahájeno trestní stíhání minimálně jedné osoby, tzv. *sexuálního predátora,* za jeho protiprávní jednání, kterého se dopouštěl na mladistvých osobách prostřednictvím sociálních sítí.

Osobní motivací pro výběr takto závažného tématu k vytvoření bakalářské práce je skutečnost, že jako běžná uživatelka sociálních sítí vnímám tyto služby jako velmi rizikové a sama jsem se ve svém osobním životě setkala s neznalostí rizik ostatních uživatelů, s jejich naivitou, avšak v některých případech též s velmi dobrou znalostí nedostatků těchto služeb, které byly leckdy využity k nemorálnímu chování.

1 CÍL A METODIKA BAKALÁŘSKÉ PRÁCE

Objektem ke zkoumání pro účely této bakalářské práce jsem zvolila sociální sítě. Tedy internetové služby, které jsou uživatelům poskytovány zdarma, mj. pro běžnou, každodenní komunikaci mezi sebou, pro sdílení fotek, obrázků, událostí, novinek, a to po neomezený čas. Touto bakalářskou prací cílím na širokou veřejnost, kterou chci prostřednictvím textu níže seznámit s problematikou internetových služeb, konkrétně se sociálními sítěmi, které v dnešní době používá velká část společnosti a v některých případech jsou využívány k páchání trestné činnosti.

První část bakalářské práce je teoretického charakteru, ve které nejprve analyzuji sociální sítě obecně včetně jejich charakteristických prvků, později též některé konkrétní sociální sítě popisuji. Dále se v této bakalářské práci objevuje kapitola věnující se kyberkriminalitě obecně, neboť se útoky páchané skrze sociální sítě, právě z důvodu, že se odehrávají v kyberprostoru, řadí právě mezi kybernetické. Velký důraz v této bakalářské práci je kladen na konkrétní útoky, ke kterým na sociálních sítích dochází mezi jejich uživateli. Využitím účinných právních norem, konkrétně trestního zákoníku, přehledně zdůrazňuji, jakého konkrétního trestného činu se může osoba kyberútočníka dopustit svým rizikovým chováním na sociálních sítích. K této části bakalářské práce jsem využila nejen tuzemskou, ale též zahraniční literaturu a zcela aktuální statistiky. Aby mohla být společnost informována a varována před riziky pojícími se se sociálními sítěmi, je důležité, aby neustále vznikala aktualizovaná preventivní opatření, tedy preventivní programy a nejrůznější preventivní aktivity, díky kterým by se k jednotlivým uživatelům dostalo dostatečné množství informací, které by reagovaly na nejnovější změny v dané problematice a mohla tak být zajištěna jejich dostatečná informovanost a připravenost čelit jednotlivým útokům proti nim směřujícím. Z tohoto důvodu je jedna z kapitol věnována také prevenci kriminality a subjektům na prevenci kriminality se podílejícím.

Druhá, zvláštní část této bakalářské práce je tvořena dvěma výstupy. Jako první jsem vytvořila případovou studii kyberstalkingu, kdy jsem vycházela z rozsudku Nejvyššího soudu. Je tím tak zdůrazněna dlouhodobost jednání útočníka vůči oběti. Druhým výstupem této bakalářské práce je vytvoření preventivního programu, který nese název Bezpečně na sociálních sítích cílícího zejména na děti a mládež a jejich bezpečné chování na sociálních sítích v podobě vytvořených letáků, jejichž obsah je v této bakalářské práci blíže popsán právě ve zvláštní části této práce.

Tento preventivní program je tvořen třemi letáky, jejichž cílovou skupinou jsou studenti, jejich rodiče a jejich učitelé. Pro rodiče a učitele lze tyto letáky využít jako informativní, aby takto získané informace mohli předat dále, svým dětem a studentům a bylo tak zachováno jejich bezpečí.

2 SOCIÁLNÍ SÍTĚ

Sociální sítě jsou v současné době často diskutovaným tématem v běžném či pracovním životě, hlavně díky usnadnění každodenní komunikace mezi uživateli internetu. Bohužel, spolu s rozvojem moderních technologií a snadno dostupných aplikací, se rozvíjí i možnosti páchání trestné činnosti právě skrze zmiňované sociální sítě. [1]

Pojem sociální sítě lze zjednodušeně definovat jako webové služby nebo aplikace, které díky zasílání zpráv, informací, komentářů či obrázků umožňují jejich uživatelům vzájemnou komunikaci a navazování vztahů. [2]

Vzhledem k tomu, že je internet a jím poskytované služby využíván k zábavě, pracovní činnosti, vyhledávání informací nebo nákupu zboží, stává se tak součástí každodenní rutiny, zároveň ale snadným zdrojem zneužití osobních dat dospělých i dětských uživatelů. [3]

Základem používání každé sociální sítě je registrace, díky které si uživatel vytvoří svůj účet, tzv. uživatelský profil. K registraci uživatel využívá své osobní údaje, a aby mohl vlastní registraci dokončit, musí si zvolit heslo, které později bude využívat při přihlašování do účtu. Jako základní prvek pro založení profilu slouží jméno a příjmení, e-mail nebo číslo mobilního telefonu, datum narození a pohlaví. Ostatní informace lze do profilu dobrovolně přidat, ale nejsou součástí registrace, tzn., že uživatel není nucen tyto informace zadávat a sdílet je tak s ostatními uživateli. Doplňující informace mají sloužit pouze ke snazšímu vyhledávání přátel a navazování kontaktů s nimi. Po procesu registrace a vytvoření vlastního profilu je uživateli umožněno začít používat danou sociální síť. [4]

[1] SMEJKAL, Vladimír. *Kybernetická kriminalita.* 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. str. 226-227. ISBN 9788073807207.
[2] LEXICO: UK Dictionary [online]. [cit.2019-10-10]. Dostupné z: https://www.lexico.com/definition/social_network.
[3] KOPECKÝ, Kamil. *Rizikové formy chování českých a slovenských dětí v prostředí internetu.* Olomouc: Univerzita Palackého v Olomouci, 2015. str. 9. ISBN 9788024448619.
[4] Facebook: Centrum nápovědy [online]. [cit. 2019-10-10]. Dostupné z: https://www.facebook.com/help/570785306433644?helpref=hc_global_nav.

2.1 Soukromí

„Nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem.“ [5]

Soukromí představuje osobní informace o jednotlivci či skupině lidí a každý z nás má právo jej chránit před jakýmkoliv zneužíváním. Jedná se o jedno ze základních lidských práv, které je zakotveno mimo jiné ve Všeobecné deklaraci lidských práv (čl. 12) a v Listině základních práv a svobod (čl. 7 a 10). V některých studiích je rozlišováno informační, sociální a psychologické soukromí, jako například ve studii Dienlina a Trepta z roku 2015. Ve smyslu této bakalářské práce se však budu zabývat soukromím na internetu, konkrétně soukromím na sociálních sítích. [6][7]

Jak soukromí, tak bezpečnost jsou velkými problémy sociálních médií. V první řadě je nutné poznamenat, že design ochrany a soukromí na sociálních sítích je slabý, čímž jsou vytvořena zranitelná místa týkající se soukromí a bezpečnosti. Avšak zároveň hlavním účelem sociálních sítí je sdílení informací, které je definováno zejména tím, že s kým jsou informace sdíleny, jaké informace jsou sdíleny a v jakém množství jsou sdíleny, což má nevyhnutelné důsledky v oblasti soukromí a jeho ochrany, kdy zejména chování uživatelů a vnímání rizik uživateli sehrává důležitou roli. [8]

Je tedy nutné, aby sami uživatelé chránili svá data v procesu používání sociálních sítí, jelikož jejich soukromí může být nedostatečnou ochranou přímo ohroženo. V této době však problémy s ochranou soukromí nejsou pouze „běžnými problémy“, ale jsou spíše spojeny s analýzou a výzkumem informací od lidí, uživatelů, a zacíleným předvídáním lidského chování a poznávání jejich osobního stavu. Například provozovatelé sociálních médií mohou pomocí porovnávání a výzkumu informací a dat uživatelů zjisti, kteří rodiče kterých uživatelů jsou uvědomělí, či uvědomělejší návyků utrácení peněžních prostředků svých dětí, a na základě toho mohou nutit uživatelům relevantní reklamní sdělení. [9]

---

[5] Čl. 7 odst. 1 usnesení č. 2/1993 Sb., listina základních práv a svobod.
[6] Čl. 12 *UNITED NATIONS: Všeobecná deklarace lidských práv* [online]. 2015 [cit. 2019-10-13]. Dostupné z: https://www.osn.cz/wp-content/uploads/2015/12/UDHR_2015_11x11_CZ2.pdf.
[7] VAN SCHAIK, Paul, JANSEN, Jurjen, et. Al. Scurity and privacy in online social networking: risk perceptions and precautionary behaviour. In: *Computers in Human Behaviour.* [online]. 2017. [cit. 2019-10-13]. str. 7-8. Dostupné z: https://www.researchgate.net/publication/320288475_Security_and_privacy_in_online_social_networking_Risk_perceptions_and_precautionary_behaviour.pdf. ISSN: 0747-5632.
[8] VAN SCHAIK, tamtéž.
[9] DU, Jun, JIANG, Chunxiao, et. Al. Community-Structured Evolutionary Game for Privacy Protection in Social Networks. In: *IEEE Transactions on Information Forensics and Security, Volume: 13; Issue: 3.*[online] 2018. str. 2 [cit. 2019-10-13]. Dostupné z: http://www.eng.usf.edu/chen/pdf/Community-

2.2 Identita

Dle Fearona se slovo identita dá využívat ve dvou odlišných, ač propojených významech. V prvním významu slova se jedná o sociální kategorii, tedy o skupinu lidí a příslušnosti k této skupině. Ve druhém významu se jedná o „*[…] sociálně významné charakteristiky osoby, které ji slouží jako základ či zdroj individuální sebeúcty a respekt*." V současné literatuře dochází k chápání osobní identity jako těch aspektů či charakteristik, které tvoří základ hodnocení a sebeúcty osoby. [10]

V oblasti kyberprostoru jde spíše o určení toho, kdo kým je v kyberprostoru. Vyvstává tedy otázka, zdali je ta či ona osoba v kyberprostoru taková, jaká je v reálném světě? Na kyberprostoru je totiž zajímavé to, že nabízí lidem možnosti prezentovat se různými způsoby. Je možné, že si člověk upraví svoji identitu pouze lehce, či svoji identitu upraví značným způsobem, kdy mění svůj věk, historii, osobnost, vzhled či dokonce pohlaví. Všechny tyto informace, stejně jako jméno, profilový obrázek, jsou důležitými prvky identity v kyberprostoru. Jelikož každý člověk v životě zastává mnoho rolí (rodič, zaměstnanec, dítě, soused, kamarád, milenec, …), může právě kyberprostor posloužit jako místo, kde může člověk tyto role jednotlivě a různorodě vyjádřit. Člověk nemusí sebe prezentovat tak, jak se prezentuje v osobním styku. Nemusí sdílet to, jak vypadá, jaké má pocity, jak přemýšlí, jak se hýbe apod. V různých prostředí kyberprostoru lze tyto jednotlivé aspekty sdílet a zveřejňovat v různých formách. Ve chvíli, kdy se člověk připojí k nějaké komunitě v kyberprostoru, má tento člověk velmi často možnost zvolit si, kolik a jestli vůbec nějaké osobní informace bude sdílet na svém uživatelském profilu. [11]

2.3 Osobní údaje

Jako takové mají osobní údaje svůj právní podklad, kdy pojem „osobní údaje" výslovně definují právní řády jednotlivých států. V ČR se dle § 4 písmene a) zákona č. 101/2000 Sb., o ochraně osobních údajů (dále jen „ZOOU") osobním údajem pro účely ZOOU rozumí *„jakákoliv informace týkající se určeného nebo určitelného subjektu*

Structured%20Evolutionary%20Game%20for%20Privacy%20Protection%20in%20Social%20Networks.pdf.

[10] VÝROST, Jozef a Ivan SLAMĚNÍK. *Sociální psychologie.* 2. přepracované a rozšířené vydání. Praha 7: Grada Publishing, 2008, str. 113. ISBN 978-80-247-1428-8. Dostupné také z: https://books.google.cz/books?id=czijlGDrBJsC&pg=PA3&dq=v%C3%BDrost+jozef&hl=cs&sa=X&ved=0ahUKEwii9OqDn4noAhUQ-qQKHaFPDMcQ6AEIQDAD#v=onepage&q=v%C3%BDrost%20jozef&f=false.

[11] SULER, John. *Identity Management in Cyberspace*, 2002. [online]. [cit. 2019-10-13]. DOI: 10.1023/A:1020392231924. Dostupné z: https://www.researchgate.net/publication/263498490_Identity_Management_in_Cyberspace.

údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo nebo nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.“ [12] Z výše uvedené definice lze tedy dojít k závěru, že osobní údaj je nedílnou součástí identity člověka. Dle § 3019 zákona č. 89/2012 Sb., občanský zákoník (dále jen „NOZ“), jsou údaji, dle kterých lze člověka zjistit, „*[…] zejména jméno, bydliště a datum narození, popřípadě identifikující údaj podle jiného právního předpisu.“* [13]

Avšak v této době nejdůležitější vymezení osobních údajů vychází z evropského práva, konkrétně z Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů (dále jen „GDPR“). Pro účely GDPR se osobními údaji dle článku 4 odstavce 1 nařízení rozumí *„veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby [.]“* [14] Ze zde uvedeného je zřejmé, že vyčerpávající výčet toho, co je osobním údajem, v tuto chvíli neexistuje a jeho určení v tuto chvíli považuji za téměř nemožné. Proto velmi záleží na konkrétní situaci a okolnostech, aby bylo možné určit, co osobním údajem je, či není. Tak například dle rozhodnutí Soudního dvora Evropské unie ve věci C-582/14, Patrick Breyer proti Bundesrepublik Deutschland bylo Soudním dvorem řečeno, že i dynamická IP adresa je osobním údajem. [15]

Z informací uvedených v této a předchozí kapitole vyplývá, že tyto údaje lze v kyberprostoru velmi svévolně sdílet, měnit a upravovat, čímž dochází k vytváření online identity osob, což vede, jak výše a následně níže specifikováno, k určitým problémům.

[12] § 4 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů.
[13] § 3091 zákona č. 89/2012 Sb., občanský zákoník.
[14] Čl. 4 odst. 1 *Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).* In: EUR-Lex [právní informační systém]. Úřad pro publikace Evropské unie. [cit. 2019-10-14]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex%3A32016R0679.
[15] Rozsudek Soudního dvora ze dne 19. října 2016, Patrick Breyer proti Bundesrepublik Deutschland, C-582/14, EU:C:2016:779, bod49. Dostupné z: http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=CS.

2.4 Anonymita

Anonymita v běžném slova smyslu znamená zůstat bezejmenný, tedy konat a jednat, aniž by byla zjištěna identita osoby, která tak koná či jedná. V době internetu lze však identifikovat osoba na základě jména, adresy, e-mailové adresy, telefonního čísla, či na základě určité kombinace informací, jako třeba výška, barva vlasů, věk, nákupy, cestování, zaměstnání apod. Na základě výše uvedeného, nikoli však vyčerpávajícího, výčtu informací o člověku je v dnešní době možné zjistit jeho identitu, a to i pouze na základě fragmentárních informací, kdy je možné si jednotlivé fragmenty informací poskládat a identitu osoby, které se tyto fragmentární informace týkají, zjistit. A i v případě, že nelze tuto osobu přesně určit, lze ji určit alespoň s vysokou pravděpodobností. [16]

Dle některých autorů je anonymita uživatelů sociálních sítí naivní představou. Ať už jde o užití jakýchkoliv aplikací, programů, internetových stránek a sociálních sítí zejména, jsou o jednotlivých uživatelích shromažďovány informace ve velmi značném množství, které jsou na jednu stranu nutné k fungování těchto aplikací, avšak na druhou stranu nechávají velký prostor k jejich zneužití, ať již jejich provozovatelem, tak i třetí osobou. [17] V počítačovém světě k zaručení anonymity tedy nepostačuje být bezejmenný.

Širší definici anonymity, která je tak spíše aplikovatelná na současnou dobu, poskytuje Kathleen A. Wallace ve svém díle *Ethics and Information Technology*, kdy anonymitu považuje za formu neidentifikovatelnosti, která je definována jako nekoordinovatelnost znaků v jejich daném významu. Dochází tedy k rozšíření konceptu anonymity, která již není spojena pouze s bezejmenností. [18]

[16] NISSENBAUM, Helen. The Meaning of Anonymity in an Information Age. The Information Society [online]. University Center for Human Values, Princeton University, Princeton, New Jersey, USA, 1999, s. 141-144 [cit. 2019-10-20]. Dostupné z: http://crazyjamiejo.pbworks.com/w/file/fetch/69786921/Anonymity%20in%20an%20Information%20Age.pdf.

[17] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. , str. 133. ISBN 978-80-88168-15-7.

[18] WALLACE, Kathleen A. Ethics and Information Technology [online]. Department of Philosophy, Hofstra University, NY, USA, 1999, s. 23-24 [cit. 2019-10-20]. DOI: 10.1023/A:1010066509278. Dostupné z: https://link.springer.com/article/10.1023/A:1010066509278.

2.5 Příklady nejznámějších sociálních sítí

Tato podkapitola je věnována nejznámějším sociálním sítím ve světě. Jejich oblíbenost je vysledována ze statistiky společnosti Statista z dubna 2020 (dále jen „Statistika“) – **viz příloha č. 1.** Pro účely této bakalářské práce jsem vybrala pouze některé sociální sítě, a to především ty, které jsou dobře známy v České republice, a zároveň se často setkáváme s jejich zneužíváním.

2.5.1 Facebook

Jedná se o nejrozšířenější a zároveň nejoblíbenější sociální síť na světě. Dle Statistiky, v dubnu roku 2020 Facebook zaznamenal téměř 2,5 miliardy aktivních uživatelských účtů.

Společnost Facebook Inc. Vznikla v roce 2004, původně výhradně pro studenty Harvardu. Díky úspěšnosti této sociální sítě se však během roku 2005 rozšířila do všech univerzit v USA a Kanadě. Od druhé poloviny roku 2006 je Facebook přístupný, za splnění podmínek, všem. [19]

Prvním krokem k používání (nejen) Facebooku, jak v počítači, tak v mobilním telefonu, je registrace uživatele, ke které je nutná platná e-mailová adresa a heslo. Následně, po registraci, uživatel vyplní svůj profil osobními údaji. Ke kompletaci svého profilu může uživatel přidat fotografii jako svůj profilový obrázek a tím je jeho uživatelský účet vytvořen. Je jen na samotném uživateli, zda svůj profil ponechá veřejný, tj. přístupný všem ostatním uživatelům Facebooku nebo omezí tento přístup pouze lidem, kteří se nacházejí v jeho seznamu přátel nebo lidem, kteří jsou zapsáni ve stejné skupině. Uživatel může na své zdi sdílet příspěvky v podobě fotografií, obrázků, videí, statusů, dle nastavení, se svými přáteli a zároveň zanechávat pod příspěvky ostatních komentáře či reakce, které zprostředkovávají tlačítka reakcí, například To se mi líbí, Super, Mrzí mě to a další. Svůj účet může uživatel využít i ke hraní her, nákupu a prodeji přes Facebook Marketplace anebo k přihlášení k jiným sociálním sítím, kde se tyto účty následně stanou propojenými. [20]

Facebook svým uživatelům nabízí několik možností, jak svůj účet zabezpečit, jak si chránit své soukromí či jak nahlásit zneužívání, které Facebook prověří a dle zásad komunity závadný příspěvek například odebere.

[19] Our History [online]. [cit. 2019-10-20]. Dostupné z: https://newsroom.fb.com/company-info/.
[20] Centrum nápovědy: Vytvoření účtu [online]. [cit. 2019-10-20]. Dostupné z: https://www.facebook.com/help/?helpref=hc_global_nav.

Nedílnou součástí sociální sítě Facebook je aplikace Facebook Messenger, která je dle Statistiky vyhodnocena jako čtvrtá nejoblíbenější sociální síť na světě. Avšak, pro tuto bakalářskou práci bude tato aplikace považována za součást sociální sítě Facebook. Jejím primárním cílem je komunikace s přáteli či s lidmi se stejnými zájmy. K tomuto úkolu slouží tzv. *instant messaging* jako nástroj pro komunikaci v reálném čase a na jakoukoliv vzdálenost. Uživatel je schopen vidět, který z uživatelů, kteří se nachází v jeho seznamu přátel, je aktivní a může využít posílání zpráv, souborů nebo zahájit hovor/videohovor jednoduše a prakticky během několika sekund. [21]

2.5.2 WhatsApp

Další aplikací využívající instant messaging je WhatsApp nebo WhatsApp Messenger. Tato aplikace je dle Statistiky třetí nejoblíbenější sociální síť na světě s dvěma miliardami aktivních uživatelů. Společnost vznikla v roce 2009 v USA a o pět let později byla koupena společností Facebook Inc. Zatímco Facebook Messenger je založen na registraci, WhatsApp využívá pro zasílání zpráv, obrázků, dokumentů, videí či hovory, telefonní číslo uživatele. Aplikace se synchronizuje s telefonními čísly uloženými v seznamu kontaktů a uživatel má tak okamžitý přehled, kdo je v aplikace WhatsApp registrovaný. [22]

2.5.3 Twitter

Tato sociální síť není výhradně určena k vyměňování zpráv mezi jednotlivými uživateli, ale k rychlému a stručnému sdílení informací či pocitů širší veřejnosti. Společnost Twitter byla založena v roce 2006 v USA. Statistika uvádí, že v dubnu 2020 Twitter aktivně používalo 386 milionů aktivních uživatelů. Ke sdílení informací uživatelé používají tzv. *tweety*, krátké zprávy do 280 znaků, ke kterým mohou být připojeny maximálně 4 obrázky. K takovýmto sdělením může uživatel přidat tzv. *hashtag*, označený symbolem #, za kterým následuje klíčové slovo, které vystihuje jejich příspěvek (například *#twitter*). [23]

[21] Instant Messaging [online]. [cit. 2019-11-05]. Dostupné z: https://it-slovnik.cz/pojem/instantmessaging.
[22] WhatsApp Messenger [online]. [cit. 2019-11-05]. Dostupné z: https://play.google.com/store/apps/details?id=com.whatsapp.
[23] Twitter [online]. 2015 [cit. 2019-11-05]. Dostupné z: https://whatis.techtarget.com/definition/Twitter.

2.5.4 Instagram

Instagram je online aplikace a sociální síť, která svým uživatelům zdarma umožňuje sdílet fotografie. Od roku 2012 je vlastněna společností Facebook Inc. Jako takový umožňuje Instagram uživatelům editovat a nahrávat fotografie a krátká videa skrze mobilní aplikaci, kdy uživatelé mohou přidat popisek ke každému z jejich „sdělení“, či postů, a použít hashtagy a geotagy (tagy označující oblast, kde se kdo nachází, kde byla fotografie pořízena, či kde se místo zobrazené na fotce/videu nachází), které umožňují tyto posty vyhledat jinými uživateli aplikace. Každý post jednotlivého uživatele se zobrazí těm, kteří tohoto konkrétního uživatele sledují, zároveň však mohou být zobrazeny i těmi uživateli, kteří daného uživatele nesledují, a to na základě konkrétních hashtagů a geotagů. Uživatel má ale možnost mít účet založený pouze soukromě, kdy se posty tohoto uživatele zobrazí pouze těm uživatelům, kteří tohoto uživatele sledují.

Instagram, stejně jako všechny výše zmíněné sociální sítě, je však také možné použít jako platformu pro business, kdy společnosti mají možnost založit „účet společnosti“ a podporovat svoji značku a produkty. Takovíto uživatelé mají přístup k dalším nástrojům aplikace, který běžní uživatelé nemají. [24]

[24] Instagram [online]. 2017 [cit. 2019-11-05]. Dostupné z: https://searchcio.techtarget.com/definition/Instagram.

3 KYBERKRIMINALITA

Pojmem kyberkriminalita, též kybernetická kriminalita, rozumíme páchání trestné činnosti mířící proti počítači včetně jeho komponentů (hardware, software, data) anebo naopak počítač při páchání této trestné činnosti slouží jako nástroj k jejímu páchání. [25] V rámci kyberkriminality se nemusí vždy jednat pouze o trestné činy, jelikož v některých případech se může jednat pouze o čin nemorální. O trestný čin se dle zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů (dále jen „TZ"), bude jednat pouze v případech, kdy bude spáchán *„[…] protiprávní čin, který trestní zákon označuje za trestný a který vykazuje znaky uvedené v takovém zákoně".* Některými autory bývá jako synonymum k pojmu kyberkriminalita používán pojem počítačová kriminalita, avšak dle Kuchty je toto označování chybné, neboť zatímco kyberkriminalita se může odehrávat pouze v kyberprostoru, počítačová kriminalita se může odehrávat i mimo něj a stává se tak nadřazeným pojmem. Internetová kriminalita se pak od počítačové odlišuje tím, že k páchání trestné činnosti, kromě počítače jako nástroje či objektu trestné činnosti, je nutné využití internetu. [26]

Pachatelem kyberkriminality může být jakákoliv osoba, aniž by měla zvláštní vlastnost, způsobilost nebo postavení a ani věk či pohlaví zde nehraje žádnou roli. Pachatel tohoto druhu kriminality používá pouze své znalosti, zkušenosti a dovednosti. Zde hovoříme o tzv. *hackerovi.* Ovšem, o hackerovi nelze ve všech případech hovořit jako o pachateli trestné činnosti, neboť pod tímto pojmem je označena osoba, která má velmi dobrý přehled o fungování počítačových sítí, počítačových systémech a dobré znalosti a zkušenosti s programováním. Jejich filozofií, kterou se řídí, je chtění poznat, jak jednotlivé systémy fungují a předat tyto informace jiným uživatelům. Díky těmto schopnostem a zkušenostem proto není pro hackera problém nabourat se např. do cizího účtu na sociální síti či do e-mailu a dostat se tak k velmi citlivým informacím o každém uživateli, které může v budoucnu zneužít. [27] Díky vysoké mediální pozornosti jsou proto společnosti známé útoky těchto hackerů, kdy se nabourali do počítačových systémů několika institucí či organizací, a dokonce tak ovlivnili jejich běžné fungování. Typickým příkladem pro toto je případ, který se odehrál v Litvě, kde se skupina hackerů nabourala

[25] JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. ISBN 978-80-247-1561-2.
[26] KUCHTA, Josef. Časopis pro právní vědu a praxi: Aktuální problémy počítačové kriminality včetně její prevence [online]. Brno, 2016, XXIV (1/2016) [cit. 2019-12-12]. ISSN 1805-2789. Dostupné z: https://journals.muni.cz/cpvp/article/view/5260/4344.
[27] ZAVRŠNIK, Aleš. Kyberkriminalita. Praha: Wolters Kluwer, 2017. Právní monografie. ISBN 978-80-7552-758-5.

do počítačové sítě klinik plastické chirurgie, ze kterých následně získali více než 25 tisíc fotografií pacientů. Tímto se také dostali k velmi citlivým informacím o bydlišti, čísle pojištění, a dokonce o konkrétním zákroku, který jednotliví pacienti na klinice prodělali. Následně, skrze tento útok, hackeři vydírali nemocnici i samotné pacienty, aby zaplatili, pod pohrůžkou zveřejnění intimních fotografií pacientů široké veřejnosti. [28] Případy o nabourání počítačových systémů nemocnic jsou známy i v České republice.

V České republice je také znám případ mladíka pocházejícího z Bruntálu, který se ve svém volném čase připojoval na veřejné Wi-Fi sítě tak, aby nebylo možné zjistit jeho IP adresu, přes kterou by byl policií ČR dohledatelný. Takto na internetu navazoval kontakt a komunikoval s dívkami, od kterých postupně vylákal intimní fotografie, následně začal dívkám vyhrožovat jejich zveřejněním, pokud mu nezašlou další, odvážnější fotografie. Zde na pachatele upozornili rodiče jedné z nezletilých dívek, kteří podali na studenta trestní oznámení. Náměstek moravskoslezského policejního ředitele Radim Wita médiím uvedl, že mladík *„byl obviněn ze sexuálního nátlaku, svádění k pohlavnímu styku, zneužití dítěte k výrobě pornografie, výroby a nakládání s dětskou pornografií a ohrožování výchovy dítěte, za což mu hrozí až šest let vězení. V případě, že by byl pachatel dospělý, hrozilo by mu až 12 let“*. I v tomto případě lze hovořit o kyberkriminalitě. [29]

3.1 Kyberprostor

Definice kyberprostoru se napříč literaturou různí. Jednou ze známějších je definice Williama Gibsona, kterou užil ve svém díle Neuromancer z roku 1984. Zde je kyberprostor definován jako *„Konsensuální halucinace každý den zakoušená miliardami oprávněných operátorů všech národů, dětmi, které se učí základy matematiky… Grafická reprezentace dat abstrahovaných z banky všech počítačů lidského systému. Nedomyslitelná komplexnost. Linie světla seřazené v neprostoru myslí, shluky a souhvězdí dat.“* [30]

[28] TN.CZ:*Hackeři ukradli intimní fotky pacientů kliniky. Vydírají tisíce lidí!* [online]. 2017 [cit. 2020-08-18]. Dostupné z: https://tn.nova.cz/clanek/hackeri-ukradli-intimni-fotky-pacientu-kliniky-vydiraji-tisice-lidi.html.
[29] InNovinky.cz: *Student z Bruntálska vydíral dívky prostřednictvím intimních fotek* [online]. 2019 [cit. 2020-08-18]. Dostupné z: https://www.novinky.cz/krimi/clanek/student-z-bruntalska-vydiral-divky-prostrednictvim-intimnich-fotek-40269741.
[30] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z. s. p. o., 2016. s. 42. ISBN 978-80-88168-15-7.

Avšak, ze shrnutí díla Cyberspace: First Steps se dozvídáme, že Benedickt definuje kyberprostor jako *„nekonečný umělý svět, kde lidé brouzdají v prostoru založeném na informacích“* a jako *„ultimátní počítačové-lidské rozhraní.“* [31]

S kyberprostorem bezprostředně souvisí pojem internet, který je nutné identifikovat k bližšímu pochopení toho, co kyberprostor je. Hmotnou podstatou internetu je *„jeho páteřní síť, která vede signál (data) vzduchem, kabely či jinými přenosovými médii. Technicky se jedná o celosvětovou distribuovanou počítačovou síť složenou z jednotlivých menších sítí, které jsou navzájem spojeny pomocí protokolů IP a tím je umožněna komunikace, přenos dat, informací a poskytování služeb mezi subjekty navzájem.“* Proto je možné o kyberprostoru říci, že se jedná o jakousi virtuální realitu, která nemá ani počátek, ani konec, kdy však tato realita je naprosto závislá na své materiální podstatě. Materiální podstatou máme na mysli technologie reálného světa, které právě onu existenci tohoto nehmotného média umožňují, kdy právě při jejich úplném kolapsu může dojít k nenávratnému poškození kyberprostoru či jeho úplnému zániku. [32]

Definice kyberprostoru je také obsažena i v § 2 písmene a) zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „ZKB“), kdy se v ZKB kybernetickým prostorem rozumí *„digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací [.]* [33]

Kyberprostor je možné dále vymezit i pomocí jeho znaků, mezi které lze zařadit decentralizovanost, globálnost, otevřenost, bohatost na informace, interaktivnost, možnost ovlivňování jiných uživatelů, a to až do takové míry, že se toto ovlivňování velmi zřetelně projevuje v reálném světě.

K 30. červnu 2018 bylo z celkového počtu 7.634.758.428 lidí na světě připojeno k internetu 4.208.571.287 osob. [34]

[31] BENEDIKT, Michael. Cyberspace: First Steps [online]. 1991 [cit. 2019-12-12]. Dostupné z: https://archive.org/details/CyberspaceFirstSteps.
[32] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z. s. p. o., 2016. s. 43. ISBN 978-80-88168-15-7.
[33] §2 písm. a) zákona č. 181/2014 Sb., o kybernetické bezpečnosti.
[34] Internet World Stats. INTERNET USAGE STATISTICS. The Big Picture World Internet Users and 2018 Population Stats[online]. 2018. [cit. 2019-12-12]. Dostupné z: https://internetworldstats.com/stats.htm.

3.2 Kybernetická hrozba

Kybernetickou hrozbou je kybernetická bezpečnostní událost, která je dle § 7 odstavce 1 ZKB *„[…] událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikacích“.* [35]

Jako největší hrozby dnešní doby jsou uváděny Darknet (označován také jako Dark Web), malware a botnet.

Zatímco internet, tedy Surface Web (povrchový web) slouží k tomu, aby po zadání fráze či slova do vyhledávače (např. Google, Wikipedia), byla skenováním nalezena shoda, značně větší část internetu je přístupná pomocí jiných než klasických vyhledávačů. Tyto informace nalezené v tzv. *Deep webu* (hluboký web) ve většině případů nejsou nebezpečnými, avšak mohou být těmi, kteří mají špatný záměr, úmyslně zneužity. V tomto případě hovoříme o skryté části internetu zvané Dark Web, neboť zločinci, za použití speciálních softwarů k zamaskování jejich aktivit a zaručení anonymity, páchají trestnou činnosti, jako je například prodej drog, zbraní, obchodování s padělanými odklady totožnosti nebo materiálem spojeným se zneužíváním dětí. Pro lepší představu tohoto kyberprostoru, existuje zobrazení v podobě ledovce – **viz příloha č. 2**, ze kterého je patrné, že samotné sociální sítě patří do té převažující části informací, tedy Deep Webu.

Malware je zkratka pro *„malicious software“*, tedy škodlivý software, který má za cíl poškodit oprávněného uživatele počítače, a to zejména tím, že získá data, osobní informace uživatele nebo dokonce převezme kontrolu nad zařízením za účelem trestné činnosti. Pod souhrnným názvem malware se skrývá například adware (reklamu podporující software), spyware (software k získávání statistických dat o provozu počítače, která jsou bez vědomí uživatele odesílána útočníkovi), trojské koně (programy s latentními funkcemi, o nichž uživatel neví, a které ohrožují bezpečný chod systému) a další.

Pojem botnet bezprostředně souvisí s pojmem malware, jelikož botnet je následek nakažení zařízení malwarem. Útočníkovi je poté umožněno použít počítač oběti k dalším útokům. [36]

[35] §7 odst. 1 zákona č. 181/2014 Sb., o kybernetické bezpečnosti.
[36] The threats [online]. [cit. 2019-12-12]. Dostupné z: https://www.interpol.int/Crimeareas/Cybercrime/The-threats.

3.3 Kyberútok

Zatímco ZKB označuje kybernetickou bezpečnostní událost jako možnou hrozbu, která zatím nemusí být reálná, kybernetickým bezpečnostním incidentem se již rozumí *„[…] narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události“.* [37]

Nejčastěji diskutovanými útoky v rámci kyberprostoru jsou různá podvodná jednání, zejména pak *phishing*, jehož záměrem je shromáždit informace, jako je například heslo, číslo kreditní karty, PIN, a další informace vedoucí ke konkrétnímu uživateli. Typickým příkladem pro phishingový útok je útok skrze internetové bankovní služby. Útočník rozešle phishingový e-mail, který na první pohled nebude vypadat nijak podezřele, a bude po uživateli vyžadovat kliknutí na přiložený odkaz. Takový odkaz uživatele přesměruje na podvodnou webovou stránku, která bude ovšem vypadat na první pohled stejně jako originální. Jedná-li se o webovou stránku internetového bankovnictví a uživatel vyplní své přihlašovací údaje, tato data jsou automaticky odesílána útočníkovi. Běžný uživatel se pak může setkat ještě s dalšími formami phishingu. Těmi jsou například *vishing* (telefonický phishing), kdy se útočník představí pod falešnou identitou a snaží se citlivé údaje od uživatele vylákat; *smishing* (phishing pomocí SMS zpráv). [38] V případě, kdy by se útočník takovýmto způsobem obohatil, může se stát pachatelem trestného činu podvodu ve smyslu § 209 TZ. [39]

[37] § 7 odst. 2 zákona č. 181/2014 Sb., o kybernetické bezpečnosti.
[38] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. str. 246-266. CZ.NIC. ISBN 978-80-88168-15-7.
[39] § 209 zákona č. 40/2009 Sb., trestní zákoník.

4 ÚTOKY V RÁMCI SOCIÁLNÍCH SÍTÍ

Výčet výše uvedených útoků, se kterými se můžeme, jako uživatelé setkat v kyberprostoru, není konečný. Pro tuto bakalářskou práci jsou stěžejní útoky, se kterými se můžeme setkat na sociálních sítích. Konkrétně je tato kapitola určena k podrobnější analýze kyberšikany, kyberstalkingu, kybergroomingu a sextingu. Tyto útoky samy o sobě nejsou trestnými činy, jelikož nejsou trestním zákoníkem konkrétně definovány, avšak útočník tímto nebezpečným jednáním může naplnit skutkovou podstatu některého z trestných činů, které zvláštní část trestního zákoníku taxativně jmenuje. Těmito útoky jsou denně ohrožovány nejen děti a mladiství, ale i dospělí uživatelé.

4.1 Kyberšikana

Abych mohl být lépe definován termín kyberšikana, je důležité definovat klasickou šikanu. Mluvíme o snaze útočníka, aby své oběti opakovaně psychicky či fyzicky ublížil. Může se jednat o fyzické bití, poškozování věcí, ale také o útoky slovní páchané nadávkami, urážkami, ponižováním či dokonce vydíráním. Jsou-li tyto psychické, zejména slovní útoky páchány prostřednictvím informačních a komunikačních technologií nebo prostřednictvím služeb nabízených v kyberprostoru, jedná se o kyberšikanu. [40]

Jako základní znaky kyberšikany jsou uváděny **pocit anonymity** – pocit útočníka, že na internetu nemůže být odhalen; **neomezenost útoku** – útočník nemusí řešit čas ani místo útoku neboť informační a komunikační technologie umožňují páchat útoky vůči komukoliv, kdykoliv a odkudkoliv; **agresorem může být kdokoliv** – kyberšikanující osobou může být kdokoliv bez ohledu na věk, pohlaví, fyzickou převahu či společenské postavení; **neomezenost prostředků a prostoru** – útočník využívající pro kyberšikanu sociální sítě zanechává urážlivé komentáře, fotografie a videa, které může pomocí nejrůznějších programů či aplikací upravovat a to dokonce opakovaně; **obtížné objasňování** – kyberšikana je ve většině případů latentní záležitostí a jelikož útoky směřují zejména proti psychice, navenek nejsou znaky ubližování viditelné; **trvalost** – tento znak vystihuje rčení *„internet nezapomíná“*, neboť stáhnout škodlivý materiál z internetu či sociální sítě je velmi komplikovaný proces, který ovšem nezaručuje, že po

[40] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. str. 309. CZ.NIC. ISBN 978-80-88168-15-7.

odstranění se tento materiál neobjeví na jiné sociální síti či oběti nejsou nadále zasílány urážející a ponižující zprávy. [41]

Stejně jako útoky klasické šikany, taktéž i útoky kyberšikany mohou mít několik podob. Tyto útoky lze primárně rozdělit na dva typy, a to na *přímé* a *nepřímé.* Mezi *přímé útoky*, které jsou pro kyberšikanu typičtější, řadíme tzv. ***blogování***, kdy pachatel vytvoří blog, který má za cíl zesměšnit či jinak poškodit oběť, na kterém může v některých případech zveřejnit intimní fotografie oběti. Dále se může jednat o útoky zvané ***bluejacking***. Zde útočník pomocí mobilního telefonu, e-mailu či jiné aplikace rozesílá videa a fotografie obětí, které se tímto snaží zesměšnit. V aplikacích, jako je například Facebook či Instagram, může probíhat kyberšikana i skrze tzv. ***internetové hlasování***, které útočník vytvoří a vyzývá tak ostatní uživatele těchto aplikací, aby hlasovali o oběti a opět s cílem oběť zesměšnit. Předmětem hlasování zde může být cokoliv, co útočník vytvářející hlasování zadá. Jako tzv. ***outing*** lze označit jednání útočníka, který bez souhlasu uživatele nebo proti vůli tohoto uživatele, získá přístup k jeho uživatelskému profilu, kde následně veřejně na profilové zdi uživatele umístí příspěvek ve smyslu „Jsem gay, nechci to už před vámi tajit".

Jako nepřímé útoky označujeme útoky, které za útočníka vykonává někdo jiný, který se tak vědomě či nevědomě stává spolupachatelem tohoto útočníka. [42]

Ačkoliv kyberšikana není dle platného trestního zákoníku trestným činem, útočník se v průběhu kyberšikany může stát pachatelem trestného činu uvedeného v ustanovení § 353 TZ *Nebezpečné vyhrožování*, a to tím, že výhrůžkami v oběti vzbudí důvodnou obavu, že ji bude ublíženo na zdraví či bude ohrožena na životě. O další, s kyberšikanou spojeny trestný čin, by se jednalo v případě, kdy by pachatel svým jednáním vedl takové vyhrožování proti osobám či jednotlivci, kvůli rase, příslušnosti k etnické skupině, národnosti nebo vyznání. V takovém případě by se dopustil trestného činu *Násilí proti skupině obyvatelů a proti jednotlivci* zakotveném v § 352 TZ. Trestného činu *Pomluva* dle § 184 TZ by se dopustil ten útočník, který by v rámci kyberšikany o oběti sdělil nepravdivý údaj, jehož povahou je možno ohrozit vážnost oběti u spoluobčanů nebo způsobit jinou vážnou újmu, skrze veřejně přístupnou počítačovou síť. K vážným

[41] Co je kyberšikana a jak se projevuje? [online]. [cit. 2019-12-12]. Dostupné z: https://bezpecneonline.saferinternet.cz/pro-rodice-a-ucitele/teenageri-a-komunikace/item/34-co-je-to-kybersikana-a-jakse-projevuje.

[42] MARTÍNEK, Zdeněk. *Agresivita a kriminalita školní mládeže.* 2., aktualizované a rozšířené vydání. Praha: Grada, 2015. Pedagogika. ISBN 978-80-247-5309- 6.

následkům kyberšikany může dojít v případech tzv. *happy slappingu* [43] (z angl. happy – šťastný, spokojený; slapping – fackování), zveřejnění video nahrávky na sociálních sítích, která zachycuje dopředu připravené fyzické napadení oběti. Toto spojení klasické šikany s kyberšikanou může vyústit až k naplnění skutkové podstaty trestného činu dle ustanovení § 146 TZ *Ublížení na zdraví* nebo dle ustanovení § 145 TZ *Těžké ublížení na zdraví*. Tragickým následkem dlouhodobé kyberšikany byla v některých případech dokonce sebevražda oběti. V tomto případě by se útočník mohl stát pachatelem trestného činu *Účast na sebevraždě* dle § 144 TZ. [44]

Před kyberšikanou je možné se chránit tak, že každý uživatel bude mít na paměti základní zásady pro bezpečné užívání internetu a služeb, které nabízí, a to především, že **osoby nemusí být vždy těmi, za které se vydávají** – zde se přehnaná důvěřivost v osoby, které neznáme, nevyplácí; **nezveřejňovat citlivé osobní informace** – adresa, fotografie, hesla k účtům. Poskytnutím těchto informací můžeme dát útočníkům do rukou materiál, který může být snadno použit k dalším útokům; **respekt vůči ostatním uživatelům**. V případě, že se osoba stane obětí kyberšikany, je důležité bránit se, ale nikoliv mstou. V některých případech může postačit působit klidným a vyrovnaným způsobem, či dávat najevo nezájem. Útokům se uživatelé sociálních sítí mohou bránit například i tím, že se útočníka pokusí identifikovat a přestanou s ním komunikovat, zablokují mu možnost, aby je nadále kontaktoval. Uživatelé, kteří se stali obětí kyberšikany by se neměli bát takové útoky oznámit svým známým (v případě dětí dospělým osobám – rodičům, učitelům) nebo na lince 158 přímo Policii ČR, avšak aby mohlo probíhat vyšetřování, je nutné uschovat důkazní materiály (zprávy, komentáře, videozáznamy či internetové odkazy). Poslední, avšak stejně důležitou, je bdělost vůči vlastnímu okolí, vůči dětem a známým. Změny v chování či změny všedních zvyklostí, a to hlavně u dětí školního věku, mohou pomoci odhalit kyberšikanu v raném stádiu. [45] [46]

[43] HAPPY SLAPPING [online]. [cit. 2019-12-12]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/happyslapping/.
[44] Zákon č. 40/2009 Sb., trestní zákoník.
[45] PAPEŽOVÁ, Zdeňka. Policie České republiky: PREVENCE - Kyberšikana [online]. [cit. 2019-12-12]. Dostupné z: https://www.policie.cz/clanek/prevence-kybersikana.aspx.
[46] KOŽÍŠEK, Martin a Václav PÍSECKÝ. Bezpečně na internetu: Průvodce chováním ve světě online. 2016. Praha: Grada Publishing, 2016, str. 65. ISBN ISBN 978-80-271-9074-4.

4.2 Kyberstalking

Stalking, v překladu stopování či sledování, je výraz pro dlouhodobé, opakované obtěžování oběti nevyžádanými zprávami SMS, zprávami skrze sociální sítě, telefonáty, e-maily nebo cíleným sledováním oběti. [47] Pro případ, že by útočník takto pronásledoval a obtěžoval oběť na sociálních sítích, tedy v kyberprostoru, dopustil by se tak kyberstalkingu.

Výkladový slovník kybernetické bezpečnosti kyberstalking definuje jako *„Nejrůznější druhy stopování a obtěžování s využitím elektronického média (zejm. prostřednictvím elektronické pošty a sociálních sítí), jejichž cílem je např. vzbudit v oběti pocit strachu…Často je taková aktivita pouze mezistupněm k trestnému činu, který může zahrnovat výrazné omezování osobních práv oběti nebo zneužití chování oběti k provedení krádeže, podvodu, vydírání apod.“* [48]

Trestní zákoník takové chování specifikuje a označuje za *Nebezpečné pronásledování* v případě, že pachatel oběť *„[…] dlouhodobě pronásleduje tím, že vytrvale jej prostřednictvím prostředků elektronických komunikací, písemně nebo jinak kontaktuje…a toto jednání je způsobilé vzbudit v něm důvodnou obavu o jeho život nebo zdraví [.]“* [49]

Předejít tomu, aby se uživatelé sociálních sítí stali obětmi kyberstalkingu, můžeme použitím stejných zásad, jako u výše uvedené kyberšikany. Na prvním místě bude vždy celková opatrnost při komunikaci na sociálních sítích. Pro konverzování v sexuální rovině by si každý měl určit hranice, které nebude překračovat. Pokud by se útočník kohokoliv, jako uživatele sociální sítě, opakovaně pokoušel kontaktovat a tím i obtěžovat, v určitých případech může posloužit funkce, kterou nabízí nejen sociální síť Facebook, a to *zablokování zpráv*, která zaručuje, že daný uživatel, kterého uživatel zablokuje, nemá příležitost uživatele kontaktovat (poslat zprávu, obrázek či zavolat). Dále může posloužit funkce *odebrání z přátel* a následná *blokace* daného profilu uživatele, ze kterého jsou ze strany obtěžující osoby uživatelé kontaktováni. [50] [51]

[47] PAPEŽOVÁ, Zdeňka. Policie České republiky: PREVENCE - Stalking [online]. [cit. 2019-12-12]. Dostupné z: https://www.policie.cz/clanek/prevence-stalking.aspx.
[48] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti [online]. [cit. 2019-12-12]. Dostupné z: https://www.govcert.cz/download/aktuality/container-nodeid548/slovnikv231nbuwebcolor.pdf.
[49] § 354 zákona č. 40/2009 Sb., trestní zákoník.
[50] Děti a online rizika: sborník studií. Praha: Sdružení Linka bezpečí, 2012. Str. 105. ISBN 978-80-9049202-8.
[51] Facebook: Centrum nápovědy: Odebrání uživatele z přátel nebo zablokování [online]. [cit. 2019-12-12]. Dostupné z: https://www.facebook.com/help/1000976436606344?helpref=hc_global_nav.

4.3 Kybergrooming

Útoky tzv. *kybergroomerů* probíhají skrze informační a komunikační technologie (sociální sítě, mobilní telefony). Jejich cílem je, pomocí psychické manipulace, vyvolat v oběti falešnou důvěru a zlákat ji tak k osobní schůzce, při níž pachatelé fyzicky či sexuálně zaútočí na oběť.

Plánovaný útok v podobě kybergroomingu je ve většině případů dlouhodobá záležitost. Doba útoku se odráží od síly jedince odolávat manipulaci útočníka, a to od přibližně 3 měsíců až, v ojedinělých případech, po dobu 2-3 let. Útok kybergroomera lze rozdělit na etapy. Prvním krokem útočníka je snaha *vzbudit důvěru a izolovat oběť od okolí*, což v praxi vypadá tak, že útočník mění svou identitu na sociální síti a je velmi trpělivý. Další etapou se poté stává *vytvoření přátelského vztahu*. Pomocí manipulace poté útok přechází ve *vyvolání emoční závislosti na útočníkovi*. Útočník chce, aby jejich vztah zůstal v tajnosti a stal se tak jediným přítelem oběti. Následně je už jen otázkou času, kdy se uskuteční *osobní setkání,* v jehož průběhu může dojít k sexuálnímu, fyzickému či jinému útoku. [52] [53]

S kybergroomingem bezprostředně souvisí i pojmy *mirroring* a *luring.* Mirroring, tzv. zrcadlení, je označení pro jednání útočníka v první etapě, kdy napodobuje komunikaci dítěte a snaží se tak dát oběti najevo pochopení. Luring, tzv. vábení, se objevuje ve druhé etapě, kdy se útočník snaží vytvořit kamarádský vztah s obětí a v praxi to vypadá tak, že útočník uplácí oběť dárky, například finančními prostředky, mobilním telefonem či lístky do kina a žádá na oplátku zaslání fotografie nebo jinou citlivou informaci o oběti. [54][55]

Přístupem k online komunikaci mohou uživatelé sociálních sítí zabránit tomu, aby se stali obětmi kybergroomingu. Jako v případech výše zmíněného rizikového chování, je důležité neposkytovat ostatním uživatelům materiály choulostivého charakteru – nezasílat intimní fotografie a v případě konverzace se sexuálním podtextem by si uživatel měl určit hranice, které nebude překračovat a současně se nebude bát říci NE! Nevhodným návrhům ze strany útočníka. Každý uživatel sociálních sítí by se měl seznámit s pravidly dané služby, taktéž i s riziky, která jsou součástí jejich používání.

[52] KOPECKÝ, Kamil. Metodický portál inspirace a zkušeností učitelů: Nebezpečí zvané kybergrooming I.[online]. 2010 [cit. 2019-12-12]. Dostupné z: https://clanky.rvp.cz/clanek/s/Z/9741/NEBEZPECIZVANE-KYBERGROOMING-I.html/.

[53] BURÝŠKOVÁ, Lenka. Policie České republiky: Víte co je KYBERŠIKANA? [online]. [cit. 2019-12-12]. Dostupné z: https://www.policie.cz/clanek/vite-co-je-kybersikana.aspx.

[54] KOPECKÝ, Kamil. Rizikové formy chování českých a slovenských dětí v prostředí internetu. Olomouc: Univerzita Palackého v Olomouci, 2015. str. 35.36. ISBN ISBN978-80-244-4861-9.

[55]MÁČELOVÁ, Karolína. Učení v pohodě: Fáze kybergroomingu: Podezřelé chování virtuálních přátel[online]. [cit. 2019-12-15]. Dostupné z: http://www.uceni-v-pohode.cz/faze-kybergroomingupodezrele-chovani-virtualnich-pratel/.

Riziko útoku kybergroomera lze dodržováním některých ze zásad chování snížit. Uživatel by měl přinejmenším zpozornit v případech, kdy je mu zaslána žádost o přátelství od neznámé osoby, kdy je požádán, aby online přátelství, kterého je aktérem, bylo zachováno v naprosté tajnosti, kdy jsou mu pokládány příliš osobní otázky, kdy mu je slibován milující vztah od osoby, kterou zná pouze přes sociální sítě či pokud ho taková osoba vyzve k osobní schůzce. V případě, že uživatel přijme tato rizika a i přes to se rozhodne k osobní schůzce s osobou, kterou zná pouze cestou informačních a komunikačních technologií, měl by přijmout opatření, kterými by chránil svou osobu, tedy by měl vždy informovat někoho sobě blízkého nebo sjednat schůzku na veřejné místo s vyšší koncentrací osob. [56]

4.4 Sexting

Toto velmi rizikové chování můžeme přeložit jako *„sextování“*, jehož podstatou je rozesílání materiálu se sexuálním obsahem (zprávy, fotografie, videa, audio nahrávky) pomocí informačních a komunikačních technologií, a jehož autory nejsou jen dospělí uživatelé, ale i mladiství a děti. Tento choulostivý materiál může být zveřejněn zejména na sociálních sítích či zaslán přes instant messaging samotným autorem, ale také jinou osobou, které byl takový materiál zaslán, nebo k němu získala přístup jinak. [57]

Důvodů, proč lidé provozují sexting, se uvádí hned několik. Jedním z důvodů dle Kopeckého je *sexting jako součást romantického vztahu*, který partneři ze začátku vztahu mohou realizovat za účelem flirtu, upoutání pozornosti či vzrušení druhého partnera, později z důvodu delšího fyzického odloučení nebo jako důkaz lásky a vzájemné důvěry. Dalším z častých důvodů je *potlačení nudy*, kdy se sexting, zejména mezi vrstevníky, může jevit jako ideální nástroj pro zkrácení dlouhé chvíle. V některých případech se může sexting jevit jako *produkt sociálního tlaku*. Tento tlak může v praxi vzniknout např. ze strany partnera či ze strany spolužáků/spolužaček, pod záminkou vzájemné výměny takových fotografií. Takové fotografie se mohou snadno stát nástrojem ke kyberšikaně nebo veřejnému ponižování. Sexting je dále realizován jako *nástroj sebeprezentace*. Zde je podstatným faktorem vzor chování, které děti a dospívající mohou napodobovat, a díky médiím a sociálním sítím mohou získat mylný dojem, že sdílení choulostivých materiálů je normální, a tedy ani sexting nepovažují za rizikové chování. Posledním z uvedených a velmi vážných důvodů, je zneužívání sexuálně orientovaných fotografií a videí jako

[56] NEBUĎ OBĚŤ: KYBERGROOMING - Jak se bránit kybergroomerovi? [online]. [cit. 2019-12-15]. Dostupné z: http://www.nebudobet.cz/?cat=kybergrooming.
[57] Sexting.cz: Co je vlastně sexting? [online]. [cit. 2019-12-15]. Dostupné z: http://www.sexting.cz/.

nástroj pomsty. [58] V tomto případě sexting úzce souvisí s kybergroomingem, neboť útočník může původně dobrovolně poskytnutý materiál během sextingu zneužít k pozdějšímu vydírání oběti, například v rámci výše zmíněného kybergroomingu anebo za účelem získání finančních prostředků či obnovení vztahu mezi partnery. Pod pohrůžkou zveřejnění fotografií nebo videí může útočník požadovat zaslání dalšího materiálu s cílem sdílet jej na sociálních sítích (internetu) nebo jej uchovat pro vlastní potřebu.

V kontextu této bakalářské práce je důležitý fakt, že trestní zákoník označuje za dítě osobu mladší 18 let. Pokud je tedy pojednáváno o dítěti, může jím být též osoba mladistvá, tedy osoba ve věku 15-18 let. [59] V rámci rizikového sextingu a s ním spojeným zneužíváním choulostivého materiálu se útočník může dopustit trestného činu *Vydírání* uvedeného v § 175 TZ v případě, že nutí oběť k zaslání dalších fotografií či videí a pokud tak neučiní, vyhrožuje zveřejněním již obdrženého materiálu všem příbuzným a přátelům. Trestného činu *Zneužití dítěte k výrobě pornografie* dle § 193 TZ se dopustí ten, kdo přiměje dítě například k obnažování přes web kameru nebo k zaslání fotografie, na které je dítě vyobrazeno nahé. Osoba, která bude vyrábět nebo přechovávat jakékoliv pornografické materiály zobrazující dítě, se dopustí trestného činu *Výroba a jiné nakládání s dětskou pornografií* dle § 192 TZ a pokud taková osoba svým jednáním *„[…] byť i z nedbalosti, ohrozí rozumový, citový nebo mravní vývoj dítěte [.]“* [60], dopustí se tak dle § 201 TZ trestného činu *Ohrožování výchovy dítěte*. [61]

Nejlepší obranou proti tomu, aby se kdokoliv stal obětí sextingu, respektive byl vydírán skrze pořízený choulostivý materiál, je intimní fotografie, videa apod. nepořizovat, a to ani v rámci partnerského vztahu ani z jiných důvodů. Pokud se i přes uvědomění si všech rizik člověk rozhodne pro pořízení těchto fotografií, měl by se ujistit, že na konkrétních fotografiích bude neidentifikovatelný. Současně by měl fotografie ukládat do nějakého zabezpečeného úložiště, ke kterému si nepovolané osoby nemohou sjednat přístup. Pokud autor fotografií bude takovéto fotografie s některou osobou sdílet, například s partnerem, měli by se domluvit na konkrétních pravidlech toho, kde budou fotografie ukládány a zobrazovány. [62]

[58] KOPECKÝ, Kamil. Rizikové formy chování českých a slovenských dětí v prostředí internetu. Olomouc: Univerzita Palackého v Olomouci, 2015. str. 45-46. ISBN ISBN978-80-244-4861-9.
[59] § 126 zákona č. 40/2009 Sb., trestní zákoník.
[60] Zákon č. 40/2009 Sb., trestní zákoník.
[61] Zákon č. 40/2009 Sb., trestní zákoník.
[62] NEBUĎ OBĚŤ: SEXTING - Co je to sexting? [online]. [cit. 2019-12-15]. Dostupné z: www.nebudobet.cz/?cat=sexting.

4.5 Šíření poplašné zprávy

„Hoax“, „Kachna“, „Fake News“. Všechna tato slova a slovní spojení pod sebou skrývají označení pro falešné či poplašné, tedy nepravdivé zprávy, v kybernetickém prostředí též statusy a příspěvky na některých ze sociálních sítí.

Zatímco výše uvedené pojmy obsažené v této bakalářské práci, kterými jsou kyberšikana, kyberstalking, kybergrooming a sexting, jsou pouze formy rizikového chování vyskytující se na sociálních sítích a pouze v konkrétních případech může dojít v rámci tohoto rizikového chování ke spáchání trestného činu, šíření poplašné zprávy je již jedním z taxativně jmenovaných trestných činů v českém trestním zákoníku.

Podstatou trestného činu uvedeného v §357 TZ je úmyslné jednání osoby spočívající v rozšíření poplašné zprávy, která je nepravdivá a svým obsahem je způsobilá vyvolat nebezpečí vážného znepokojení alespoň části obyvatelstva nějakého místa. [63]

Typickým znakem, že se jedná o tzv. *hoax* na sociální síti, je **výzva ke sdílení** – uživatel je již v titulcích zprávy vyzýván, aby zprávu bez prodlení rozšířil dále, mezi své virtuální přátele, kdy někteří nezkušení uživatelé, bez logického uvažování zprávu automaticky sdílí skrze danou sociální síť, a to i opakovaně. Nadpis hoaxové zprávy se snaží **přesvědčit svou důležitostí** – a to zejména tak, že obsahuje slovní spojení jako *„Naléhavá pomoc…“, „Nové nebezpečí…“*. **Odkaz na důvěryhodné zdroje** – autor poplašné zprávy tvrdí, že takové varování vydala všemi známá organizace, např. *„Světová zdravotnická organizace varuje…“, „FBI varuje…“, „Vláda schválila…“* anebo naopak tvrdí, že se jedná o **únik tajné informace** jedné z takovýchto organizací.[64]

Motivem pachatele takového trestného činu, kdy se jedná například o varování před nebezpečím, které ve skutečnosti nehrozí či zveřejnění informace o společensky negativní skutečnosti, může být snaha o vyvolání rozhořčení, paniky nebo dokonce nenávisti mezi obyvateli či různými skupinami obyvatel. V některých případech se může jednat i o snahu o pouhý vtip, který ne vždy musí být ostatními uživateli sociálních sítí jako vtip chápán. Pachatelem trestného činu *Šíření poplašné zprávy* by se tak stal nejen její autor, ale zároveň také každý, kdo by takovou zprávu úmyslně šířil mezi ostatní občany dále, aby dezinformovanost obyvatel podpořil. [65]

Dokonce události v České republice, kde byl dne 12. března 2020 vyhlášen nouzový stav v souvislosti s pandemií koronaviru COVID-19, nezabránily některým

[63] §357 zákona č. 40/2009 Sb., trestní zákoník.
[64] HOAX: Jak hoax poznáme [online]. [cit. 2020-02-12]. Dostupné z: https://www.hoax.cz/hoax/co-je-to-hoax.
[65] KOŽÍŠEK, Martin a Václav PÍSECKÝ. Bezpečně na internetu: Průvodce chováním ve světě online. 2016. Praha: Grada Publishing, 2016, str. 164. ISBN ISBN 978-80-271-9074-4.

osobám, aby svým jednáním, a to zejména na sociálních sítích, způsobily vážné znepokojení u svých spoluobčanů. Trestnímu stíhání za trestný čin *Šíření poplašné zprávy* dle ustanovení §357 odst. 4 TZ, za který tento zákon ukládá trest odnětí svobody v délce trvání až osm let, se vystavila žena, která skrze sociální síť Facebook zveřejnila hlasovou nahrávku o nepravdivém, velmi přísném opatření vlády, a to zavedení zákazu vycházení poté, co počet nakažených osob výše uvedenou nemocí v ČR přesáhne 1000. [66] Trestní zákoník zpřísňuje trest ukládaný za spáchání takového trestného činu právě pro případy, že je skutek spáchán *„[…]za stavu ohrožení státu nebo za válečného stavu, za živelní pohromy nebo jiné události vážně ohrožující život nebo zdraví lidí, veřejný pořádek nebo majetek“*. [67]

Každý uživatel sociálních sítí by měl při nejmenším zpozornit v případě, že se k němu dostane zpráva obsahující výše uvedené znaky a v případě, že narazí na zjevně nepravdivou zprávu, neměl by ji šířit mezi ostatní uživatele a měl by použít nástroj *Nahlásit závadný obsah*, který sociální sítě nabízejí.

4.6 Krádež identity

Jedná se o velmi specifický typ útoku, při kterém dochází k odcizení virtuální identity uživatele sociální sítě. Může se jednat o krátkodobou či trvalou kontrolu útočníka nad danou identitou uživatele. Odcizená identita může být následně použita k útoku na osobu, která identitu vlastnila, či na jinou osobu. Zde se častěji setkáváme se zneužitím identity pro třetí stranu. Útok probíhá tak, že někdo ze svého e-mailu či Facebookového účtu rozesílá spamy, či jinak škodlivý obsah, který po rozkliknutí uživatele žádá o znovu zadání přihlašovacích údajů. Poté, co uživatel zadá své přihlašovací údaje a klikne na tlačítko potvrdit, jeho přihlašovací údaje se odešlou útočníkovi. Jako prevence před tomuto typu útoku nabízí sociální sítě tzv. *dvoufázové ověřování*, kdy osoba po zadání svých přihlašovacích údajů obdrží na telefonní číslo, které si při tvorbě účtu zvolila, ověřovací přístupový kód, který poté zadá ke svým přihlašovacím údajům. Tento kód se pro každé přihlášení liší, tudíž není možné, aby někdo zneužil již jednou obdržený přístupový kód. [68]

[66] IROZHLAS: Po internetu koluje nahrávka o zákazu vycházení v Česku, autorce poplašné zprávy hrozí až 8 let vězení [online]. [cit. 2020-04-04]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/nahravka-zakaz-vychazeni-poplasna-zprava_2003210956_ada.
[67] §357 odst. 4 zákona č. 40/2009 Sb., trestní zákoník.
[68] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. ISBN 8088168155.

5 PREVENCE PŘED ÚTOKY NA SOCIÁLNÍCH SÍTÍCH

Vzhledem ke skutečnosti, že s rozšířením sociálních sítí skrze celosvětovou společnost, se tyto služby staly snadným terčem, v některých případech také nástrojem, pro páchání trestné činnosti, je důležité, aby jejich uživatelé byli o těchto útocích informování, dokázali je včas rozeznat a byli schopni těmto útokům předcházet, či v případě, že k takovému útoku již došlo, zamezit jeho pokračování. Za tímto účelem je důležité vytvářet efektivní preventivní programy, které by s cílem působit na uživatele sociálních sítí, kladly důraz na jejich bezpečí a poskytovaly jim základní rady, jak se nestát obětí trestné činnosti v rámci těchto internetových služeb. K dosažení tohoto cíle je důležité seznámit společnost se základními pojmy souvisejícími s prevencí tohoto druhu kriminality a pomocí preventivních programů a projektů jim tak poskytnout ucelený náhled na zcela aktuální problematiku.

5.1 Prevence

Prevence, slovo mající původ z lat. *praevenire*, tedy předcházet, protíná lidský život téměř od narození, a to zejména ve spojitosti s prevencí lidského zdraví. Dále je napříč společností často zmiňována snaha zabránit výskytu nežádoucích jevů a předcházení problematiky týkající se drog, násilí, dopravních nehod, katastrof v oblasti ekologie anebo dokonce zločinnosti. V případě předcházení zločinnosti, lze hovořit o tzv. *prevenci kriminality*, na kterou je tato kapitola bakalářské práce svým obsahem primárně zaměřena.

Prevence kriminality, též označována jako kriminální prevence, je nástroj státu, konkrétně jeho trestní politiky, k získání kontroly nad kriminalitou a tuto potlačit na úroveň co možná nejnižší. Za tímto účelem trestní politika státu k předcházení kriminality využívá též represi, tedy trestně-právní cestou přiměřeně sankcionuje porušení trestních zákonů, a konkrétní tresty ukládané za jednotlivé trestné činy by tak měli potenciální pachatele od spáchání trestného činu odradit.

5.2 Dělení prevence kriminality

Ke snižování obav z kriminality a k jejímu předcházení jsou využívána opatření cílená na minimalizaci závažnosti a následků kriminality, a to zejména snahou o působení na potenciální či skutečné oběti trestných činů, na potenciální či skutečné pachatele trestných činů, anebo na snížení množství příležitostí ke spáchání trestného činu.

Prevence kriminality je široká škála nejrůznějších aktivit, dle kterých je možno tento druh prevence z několika hledisek rozdělit. Jako první lze kriminální prevenci rozdělit do dvou strategií, a to *přímé* a *nepřímé*. **Strategií přímou** máme na mysli bezprostřední cílení těchto nerepresivních činností proti kriminalitě, zatímco **strategie nepřímá** se snaží kriminalitu omezit například tím, že zlepší podmínky pro život občanů, aby necítili potřebu páchat trestné činy. Opatření nepřímé strategie mohou být zaměřeny na zlepšení možnosti zaměstnání, zlepšení kvality bydlení nebo také zlepšení kvality vzdělání občanů. Co do obsahu zaměření, lze prevenci kriminality rozdělit na **prevenci situační, prevenci sociální** a **prevenci viktimnosti**, někdy též **viktimologickou prevenci**.

Sociální politikou řízená opatření se soustředí hlavně na sociální faktory kriminality, mezi které patří zejména rodina, školství, volný čas a zlepšením podmínek života jedince se snaží odradit od páchání trestné činnosti a pozitivním způsobem tak ovlivnit socializační proces osob od co možná nejnižšího věku života. Z výše uvedeného je evidentní, že tento druhé prevence kriminality je v teorii nazýván **sociální prevencí kriminality**.

Mezi opatření **situační prevence kriminality** lze obecně zařadit ty, které mají za cíl minimalizovat nebo alespoň omezit možnost spáchání trestného činu, a naopak šanci k odhalení pachatele zvýšit. K dosažení tohoto cíle jsou využívány znalosti zejména z kriminologie, a to o určité době, určitém místě a určitých okolnostech, za kterých je páchán určitý druh kriminality. Podmínkou úspěšnosti této prevence je správné zvolení konkrétního opatření spolu s vložením odpovídajících personálních či finančních prostředků.

Prevence viktimnosti se svým obsahem zaměřuje nejen na skutečné oběti trestných činů, ale také na oběti potenciální. Neboť právě slovem viktimnost rozumíme souhrn osobnostních předpokladů jedince a dalších okolností, které jedince mohou ohrožovat a usnadnit tak skutečnost, že se osoba stane obětí trestného činu (věk, pohlaví, zaměstnání, příslušnost k etnickým menšinám apod.). Mezi koncepty, na kterých je prevence viktimnosti založena, patří hlavně bezpečné chování osob, s ohledem na různé situace odlišné. Jedná se o seznámení občanů s technickými prostředky, které mohou ochránit nejen jejich majetek, ale i život a zdraví, seznámení a trénink fyzické sebeobrany, seznámení s rizikovými místy měst, ve kterých občané žijí, právní poradenství, zdravotní a psychologické poradenství, a to jak skupinové, tak individuální.

Kriminální prevenci lze též rozdělit dle adresátů, tedy na základě osob, na které prevence kriminality cílí. Takto rozlišujeme na tři okruhy, konkrétně *primární, sekundární a terciální.*

Okruh **primární prevence kriminality** je vůbec nejširším, neboť ta je zaměřena celkově na veřejnost. Patří sem aktivity hlavně osvětové, výchovné, poradenské, vzdělávací a aktivity pro volný čas. Zde je důležitým záměrem těmito aktivitami pozitivně působit hlavně na děti a mládež, zejména sportovními aktivitami či aktivitami volnočasovými obecně. Je proto logické, že hlavní úkol zde plní školy, rodiny a místní volnočasové organizace.

Již omezenější okruh adresátů má **sekundární prevence kriminality**, která zvláštní péčí hlavně sociálního charakteru cílí na rizikové skupiny osob či jedince, u kterých je vyšší pravděpodobnost přerodu v pachatele nebo oběti trestných činů. K sociálně-patologickým jevům, tedy jevům obecně společností nežádoucím, na které se sekundární prevence kriminality soustředí, řadíme zejména nejrůznější závislosti (např. alkoholové, drogové, gambling), záškoláctví, prostituci, šikanu, domácí násilí a další. Sekundární prevence kriminality se dále zabývá také příčinami vzniku kriminogenních situací. Změnou podmínek a prosazením trestní politiky cílí na odrazení potenciálních pachatelů a ochránění tak potenciálních obětí trestných činů.

Nejúžeji zaměřena je **terciální prevence kriminality**, jejímž zaměřením je resocializace kriminálně závadových osob, tedy osob, které v minulosti již spáchaly některý z trestných činů a snaží se zabránit recidivě, tzn. opakovanému páchání trestných činů. Stejně tak se svými opatřeními zaměřuje na osoby, které se již v minulosti staly obětmi trestného činu a snaží se zabránit viktimologické recidivě. [69] [70]

5.3 Subjekty podílející se na prevenci kyberkriminality

Pod subjekty zabývající se prevencí na úseku kyberkriminality a prevencí kriminality obecně si lze v dnešní době představit širokou škálu organizací na státní i nestátní úrovni. K organizacím nestátního charakteru patří zejména instituce soukromoprávní, nadace, sdružení občanů zájmová či politická anebo také například církve. Na začátku je nutné zmínit, že kriminální prevence je v České republice organizována na třech úrovních, a to na *republikové, krajské a místní*. Již z jejich názvů

[69] *Prevence kriminality: Prevence se musí vyplatit* [online]. 2019 [cit. 2020-08-20]. Dostupné z: https://prevencekriminality.cz/prevence-kriminality/.
[70] JUDr. VICHLENDA, Milan a Ph.D. Ing. Ivan KŘEČEK. *Kriminologie: Studijní opora Střední školy ochrany osob a majetku s.r.o.* [online]. 2011. [cit. 2020-08-20]. Dostupné z: https://www.sosoom-zlin.cz/media/skripta/kriminologie.pdf.

vyplývá, že odlišnost lze spatřovat hlavně v místní působnosti, nárocích na odpovědnost jednotlivých osob působících na dané úrovni a konkrétních kompetencí partnerů podílejících se na prevenci kriminality. Prevence kriminality na republikové úrovni může být v prvním případě meziresortní, v jejíž činnosti spočívá utváření preventivní politiky ve vztahu k páchání kriminality a organizace preventivních aktivit jednotlivých členů *Republikového výboru pro prevenci kriminality* (dále jen „RVPPK"). RVPPK čítá celkem 26 členů a jeho předsedou je ministr vnitra – **viz příloha č. 3**. [71] [72] V případě druhém může být také resortní, jako vedlejší činnosti jednotlivých ministerstev, kdy tak může být ovlivněno vytváření vhodné legislativy. Na místní úrovni prevence kriminality působí zejména obecní instituce, nevládní organizace, orgány VS a též policie. [73]

Policie České republiky je nejtypičtějším subjektem, který se na prevenci konkrétně kyberkriminality podílí. V tomto ohledu mí tento jednotný ozbrojený bezpečnostní sbor nezastupitelné místo. Zatímco v historii bylo policií využívaná činnost ve větší míře represivního charakteru, v dnešní době se působení na úseku prevence značně zvýšilo. Příslušníci tohoto ozbrojeného bezpečnostního sboru jsou mimo jiné povinni dle účinného právního předpisu, konkrétně dle §2 zákona č. 273/2008 Sb., zákon o PČR *„[…] předcházet trestné činnosti"*. [74] Tento zákon dále hovoří v §16 odst. 3, písm. b) o spolupráci policie s obcemi na úseku prevence proti protiprávnímu jednání [75] a dále také v §17 písm. a) bod 1 hovoří o spolupráci s fyzickými i právnickými osobami *„[…] vykonávajícími činnost v oblasti prevence kriminality a sociálně patologických jevů"* [76] a v §17 písm. a) bod 5 o stejné spolupráci v oblasti *„[…] prevence a řešení následků krizových situací a mimořádných událostí na úseku vnitřního pořádku a bezpečnosti"*. [77] Společnost boj proti kyberkriminalitě považuje za velmi důležitý, a proto je této problematice věnována čím dál větší pozornost i právě tímto policejním orgánem, neboť je to právě kybernetický prostor, který dává mnoho možností k narušení bezpečnosti naší společnosti. Kyberkriminalita je Policií ČR označována jako *„[…] trestná činnost, která je páchána v prostředí informačních a komunikačních technologií včetně počítačových sítí. Samotná oblast informačních a komunikačních technologií je buď předmětem útoku,*

[71] *Ministerstvo vnitra České republiky: Systém prevence kriminality v ČR* [online]. [cit. 2020-08-20]. Dostupné z: mvcr.cz/clanek/web-o-nas-prevence-prevence-kriminality.aspx?q=Y2hudW09NA%3d%3d.
[72] *Ministerstvo vnitra České republiky: Prevence kriminality. Republikový výbor pro prevenci kriminality* [online]. [cit. 2020-08-20]. Dostupné z: https://www.mvcr.cz/clanek/rvppk-republikovy-vybor-pro-prevenci-kriminality.aspx.
[73] *Ministerstvo vnitra České republiky: Systém prevence kriminality v ČR* [online]. [cit. 2020-08-20]. Dostupné z: mvcr.cz/clanek/web-o-nas-prevence-prevence-kriminality.aspx?q=Y2hudW09NA%3d%3d.
[74] §2 zákona č. 273/2008 Sb., zákon o Policii ČR
[75] §16 zákona č. 273/2008 Sb., zákon o Policii ČR
[76] §17 písm. a) bod 1 zákona č. 273/2008 Sb., zákon o Policii ČR
[77] §17 písm. a) bod 5 zákona č. 273/2008 Sb., zákon o Policii ČR

nebo je páchána trestná činnost za výrazného využití informačních a komunikačních technologií jakožto významného prostředku k jejímu páchání“. [78]

Skutečnost, že kyberkriminalita je závažným problémem narušujícím bezpečnost, vyplývá i ze samostatných policejních statistik. Z nich lze například vyčíst fakt, že tendence kybernetické kriminality je vzestupná, a to čím dál rychlejším tempem. Zatímco v roce 2011 bylo evidováno celkem 1502 trestných činů v oblasti kybernetické kriminality a kriminality páchané na internetu, v roce 2019 těchto trestných činů bylo evidováno již více než 8400. Pro boj proti kyberkriminalitě proto Policie ČR využívá ty nejlepší a nejvyšší policejní útvary. Národní centrála proti organizovanému zločinu služby kriminální policie a vyšetřování (dále jen „NCOZ) je útvar Policie ČR s celorepublikovou působností, ve kterém pracují zejména fyzicky, psychicky a odborně způsobilí příslušníci. Tento útvar je složen ze sekce kybernetické kriminality, který tvoří odbory kybernetické kriminality a odbor vyšetřování kybernetické kriminality. Náplně práce a kompetence odboru kybernetické kriminality je metodická činnost s přesahem k problematice zneužívání dětí, rozsáhlých podvodů na internetu a krádeží identit. Policie ČR se snaží držet krok s celosvětovou problematikou, a proto se policisté z NCOZ účastní spolupráce i na mezinárodní úrovni, a to zejména s Europolem a Interpolem. [79]

Základním pilířem preventivní činnosti Policie ČR je Oddělení tisku a prevence krajských ředitelství Policie ČR a Preventivně informační skupiny zřizovány na ÚO krajských ředitelství Policie ČR. Cílem takovéto skupiny je představit policejní práci skrze média jako službu veřejnosti a seznámit ji s možnostmi předcházení trestné činnosti. Vytváří tak dobrý image tomuto sboru nebo preventivní materiály, které poté může veřejnost získat například na přednáškách policejního preventisty. [80]

[78] *Policie ČR: Kyberkriminalita* [online]. [cit. 2020-08-20]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx?fbclid=IwAR0obuwnxkkyIToVj7NwtBIfgC-ay_1SE1Cs98RFroyFXeKhmgomjvSJzF8.

[79] plk. JUDr. MAZÁNEK, Jiří. *Policie ČR: Nabídka práce u NCOZ pro policistky a policisty* [online]. [cit. 2020-08-20]. Dostupné z: https://www.policie.cz/clanek/nabidka-prace-u-ncoz-pro-policistky-a-policisty.aspx?fbclid=IwAR22fXe-hOtXlANswXK8vtjCVjBWWFKCmNmuiKSAPvr5C2-xaVQuGKDCLh8.

[80] *Policie ČR: Preventivně informační skupina* [online]. [cit. 2020-08-20]. Dostupné z: https://www.policie.cz/clanek/sprava-stredoceskeho-kraje-odkazy-akce-a-projekty-preventivne-informacni-skupina.aspx?fbclid=IwAR1NH7QtgZq7I_nJRlyzOdYZLlJ6_OEEjPzjXbYQE8lnkfqR4i31H-oZUwA.

6 PŘÍPADOVÁ STUDIE

V následující kapitole budete seznámeni s případem kyberstalkingu, ke kterému došlo v roce 2010 na území České republiky.

Spolu s výše uvedeným bude na případové studii ukázáno, že tyto trestné činy se, mimo jiné specifické znaky, o kterých bylo pojednáno v teoretické části, vyznačují dlouhodobostí. Konečně bude také ukázáno, že i pro tyto trestné činy platí stejná trestněprocesněprávní pravidla, jako pro jiné trestné činy, kdy tato skutečnost bude demonstrována konkrétně tím, že daná studie vychází z rozsudku Nejvyššího soudu.

6.1 Obecný rámec

Případová studie vychází z rozhodnutí Nejvyššího soudu České republiky sp. Zn. 8 Tdo 1503/2011, který, jako dovolací soud, rozhodl o dovolání obviněné proti rozsudku Městského soudu v Praze, který rozhodl jako odvolací soud v trestní věci vedené u Obvodního soudu pro Prahu 4. Nejvyšší soud rozhodl o níže popsaném případu 30. 11. 2011.

6.2 Faktická stránka případu

Obviněná, která pracovala jako uklízečka pro společnost, obtěžovala poškozeného v období od 1. 1. 2010 do 13. 7. 2010, který byl společníkem zmíněné společnosti, svými SMS zprávami, přes různá telefonní čísla, včetně čísel skrytých, faxovými texty, zprávami přes sociální síť Facebook, poštovní korespondencí s vulgárním, ponižujícím, zesměšňujícím a osobu poškozeného urážejícím obsahem. Celkový počet shora uvedených pokusů o kontakt přesáhl nejméně 700. Bezdůvodně se chovala, jako by mezi ní a poškozeným byl intimní vztah, poškozenému tykala a vyzývala ho k setkání, k tomu, aby ji poškozený zatelefonoval, vsugerovávala mu pocity odpovědnosti za její citové rozrušení, a to i přes fakt, že poškozený obviněnou vyzval k tomu, aby svého jednání zanechala.

V tomto konkrétním případě jednání obviněné způsobilo, že se u poškozeného rozvinul úzkostlivě depresivní stav, a byl tak nucen vyhledat pomoc psychoterapeuta, a to během tří schůzek. Psychické zdraví poškozeného bylo narušeno nespavostí a poruchou koncentrace, které ho omezovaly v běžném i pracovním životě.

Obviněná v tomto chování pokračovala výše popsaným způsobem i po převzetí usnesení o zahájení trestního stíhání ze dne 14. 7. 2010 a to v době od 14. 7. 2010 do 29. 10. 2010.

V dovolání se proti rozsudku Městského soudu v Praze obviněná dále vyjádřila, že je přesvědčena o tom, že její jednání nemohlo v poškozeném vyvolat obavu o život a zdraví, byť sama uznala, že její jednání pro poškozeného mohlo být nepříjemné a obtěžující. Obviněná byla názoru, že její jednání bylo do jisté míry vyprovokováno samotným poškozeným, který k ní měl, dle slov obviněné, velmi negativní vztah. Její výsledné jednání tudíž bylo výsledkem vzájemně vyhrocené komunikace. Pochyby o vyvolání pocitu obavy o život a zdraví poškozeného podkládá tvrzením, že poškozený navštívil psychiatra pouze třikrát, a to pouze za účelem opatření si důkazního materiálu proti její osobě.

Závěry soudu obviněná zpochybňuje tím, že nebyla naplněna subjektivní stránka trestného činu, kdy obviněná nechtěla v poškozeném vzbudit obavy ve výše uvedeném smyslu a ani nechtěla poškozenému jiným způsobem ublížit Nesouhlasí ani s právní kvalifikací způsobení újmy na zdraví naplňující znaky ublížení na zdraví.

6.3 Právní rámec

V této části práce se zaměřím na trestněhmotněprávní následky vyplývající z tohoto rozhodnutí, nikoliv trestněprocesněprávní úpravu, která upravuje postup orgánů činných v trestním řízení.

Rozhodnutím Obvodního soudu pro Prahu 4 bylo jednání obviněné kvalifikováno jako dvojnásobný přečin nebezpečného pronásledování dle §354 odst. 1, písm. c) zákona č. 40/2009 Sb., trestního zákoníku (dále jen „TZ“), a rovněž jako přečin ublížení na zdraví dle §146 odst. 1 TZ.

Za takto kvalifikované jednání byla dle §146 odst. 1 TZ za použití §43 odst. 1 TZ odsouzena k úhrnnému trestu odnětí svobody v trvání deseti měsíců, jehož výkon byl dle §85 odst. 2 TZ a §48 odst. 4, písm. f) TZ podmíněně odložen na zkušební dobu v trvání čtyř let za současného vyslovení dohledu. Současně bylo obviněné dle §85 odst. 2 TZ a §48 odst. 4, písm. f) TZ uloženo omezení a přiměřená povinnost, aby se zdržela neoprávněných zásahů do práv poškozeného, a to, aby se zdržela jakéhokoliv osobního, písemného, elektronického, telefonického nebo jiného kontaktu s poškozeným. Dále jí byla dle §86 odst. 1, písm. c) TZ a §48 odst.4, písm. c) TZ uložena povinnost podrobit se

programu psychologického poradenství za účelem zdržení se jakýchkoliv projevů vůči poškozenému a jeho kontaktování.

Na základě odvolání podaného obviněnou Městský soud v Praze rozsudkem napadaný rozsudek zrušil ve výroku o uložení přiměřených omezení a povinností dle §86 odst. 1, písm. c) TZ, a to tak, že tutéž povinnost podrobit se programu psychologického poradenství za účelem zdržení se jakýchkoliv projevů vůči poškozenému a jeho kontaktování uložil dle §85 odst. 2 TZ a §48 odst. 4, písm. d) TZ.

Dovolání proti tomuto rozhodnutí bylo usnesením Nejvyššího soudu České republiky odmítnuto.

6.4 Význam z hlediska kyberstalkingu

I přes to, že v českém právním prostředí není judikatura soudů obecně závazná, slouží jako podklad pro rozhodnutí soudních orgánů v dalších případech, kdy judikaturou je výklad jednotlivých ustanovení právního řádu sjednocován a výklad těchto ustanovení je tak více konzistentní, což vede k větší právní jistotě subjektů práva. To však neznamená naprostou nezměnitelnost a nemožnost odchýlit se od takovýchto judikaturních závěrů. [81]

Ve výše uvedeném usnesení se Nejvyšší soud zabývá §354 odst. 1, písm. c) TZ a [82]jeho subjektivní a objektivní stránkou a objektem trestného činu, kdy subjekt je v tomto případě řešen již výše a nikoliv pouze v souvislosti s tímto ustanovením, které stanoví, že přečinu nebezpečného pronásledování dle tohoto ustanovení se dopustí ten, kdo jiného dlouhodobě pronásleduje tím, že jej vytrvale prostřednictvím prostředků elektronických komunikací, písemně nebo jinak kontaktuje a toto jednání je způsobilé vzbudit v něm důvodnou obavu o jeho život nebo zdraví nebo o život a zdraví osob jemu blízkých.

Usnesení rozebírá dopady skutkové podstaty výše uvedeného ustanovení, kterým má být postihnut stalking a také kyberstalking. Nejvyšší soud uvádí, že kyberstalking je pouze jednou z forem stalkingu, mimo forem jiných, jako například psaní dopisů, zastavování na ulici a dalších nebezpečnějších forem, jako fyzické napadení, aniž by došlo k ublížení na zdraví, poškození věcí a další.

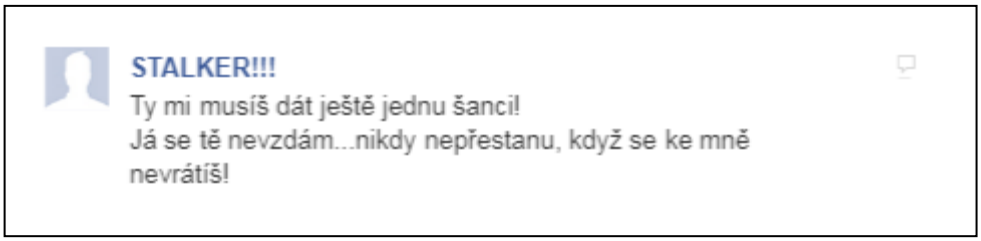
Sociální sítě dávají kyberstalkerům do rukou mnoho nástrojů, kterými mohou útočit na své oběti, zejména z důvodu, že útočník na uživatelském profilu oběti může snadno najít veškeré informace vztahující se k životu oběti. Jméno, město, ve kterém žije,

[81] Nález Ústavního soudu sp. zn. I. ÚS 3324/15 a nález Ústavního soudu sp. zn. II. ÚS 2588/16, ze dne 24. 11. 2016. [online] [cit. 2019-12-17]. In: NALUS: Vyhledávání rozhodnutí Ústavního soudu České republiky. Dostupné z: https://nalus.usoud.cz/Search/Search.aspx.

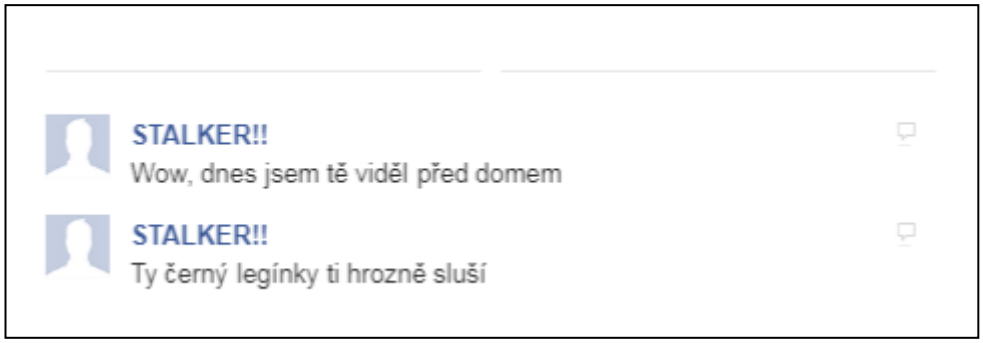
[82] Rozhodnutí Nejvyššího soudu České republiky ze dne 30. 11. 2011, sp. zn. 8 Tdo 1503/2011 [online]. [cit. 2019-12-17]. Dostupné z: https://iudictum.cz/185846/8-tdo-1503-2011.

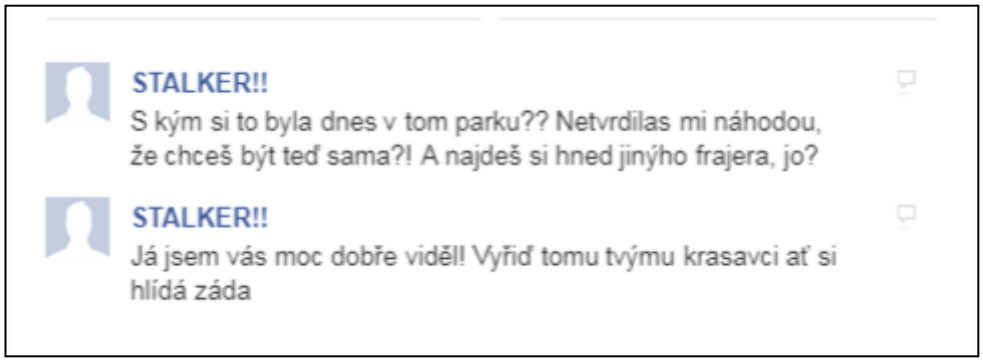
školu/zaměstnání, které navštěvuje, zájmy a koníčky, přátele a členy rodiny. Všechny tyto informace mohou být v rámci kyberstalkingu zneužity. V tomto konkrétním případě nedocházelo k obtěžování a pronásledování tváří v tvář, tudíž je možné domnívat se, že informační a komunikační technologie útočníkům umožňují schovat se za svou virtuální identitu a činit, co by v reálném světě nedokázali.

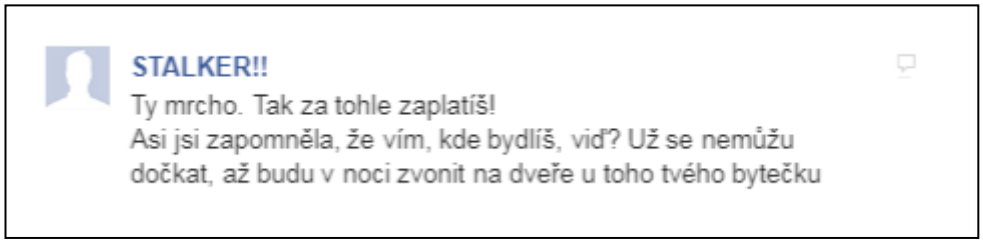
Pro stručnou ukázku, jak kontaktování oběti útočníkem může v některých případech vypadat, jsem v programu, který je dostupný na *http://fake-chat.cz/?facebook_full_chat* [83], vytvořila smyšlené zprávy z Facebook messengeru, ze kterých je evidentní, že útočník se oběť snaží zastrašovat, pokouší se obnovit jejich vztah a dále vnutit pocity viny a strachu. Tyto zprávy jsou na sobě nezávislé ani nijak nesouvisí s výše uvedeným případem.

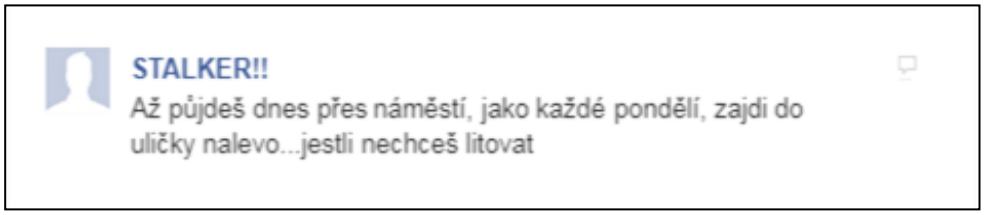


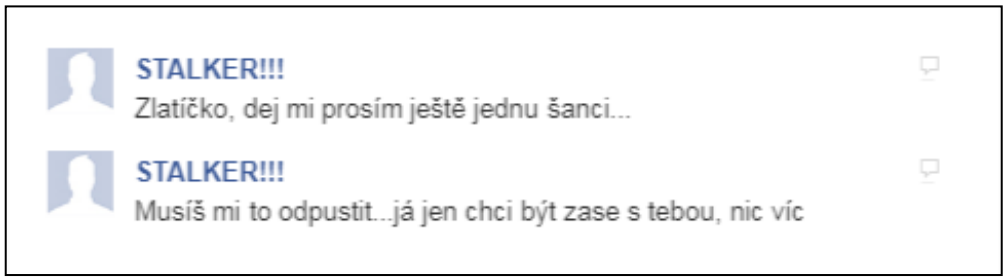
[83] Fake Chat: Facebook Chat generátor.[online]. [cit. 2020-01-07]. Dostupné z: http://fake-chat.cz/?facebook_full_chat.


STALKER!!
Wow, dnes jsem tě viděl před domem
STALKER!!
Ty černý legínky ti hrozně sluší


STALKER!!
S kým si to byla dnes v tom parku?? Netvrdilas mi náhodou, že chceš být teď sama?! A najdeš si hned jinýho frajera, jo?
STALKER!!
Já jsem vás moc dobře viděl! Vyřiď tomu tvýmu krasavci ať si hlídá záda


STALKER!!
Ty mrcho. Tak za tohle zaplatíš!
Asi jsi zapomněla, že vím, kde bydlíš, viď? Už se nemůžu dočkat, až budu v noci zvonit na dveře u toho tvého bytečku


STALKER!!
Až půjdeš dnes přes náměstí, jako každé pondělí, zajdi do uličky nalevo...jestli nechceš litovat


STALKER!!!
Zlatíčko, dej mi prosím ještě jednu šanci...
STALKER!!!
Musíš mi to odpustit...já jen chci být zase s tebou, nic víc

7 BEZPEČNĚ NA SOCIÁLNÍCH SÍTÍCH

V návaznosti na teoretickou část věnující se prevenci před kyberkriminalitou je tato kapitola druhým výstupem zvláštní části této bakalářské práce. Konkrétně se jedná o preventivní program zaměřující se na bezpečné chování na internetu, zejména na sociálních sítí a informující o nejčastějších rizicích, se kterými se na sociálních sítích může jejich uživatel setkat. Prevence kyberkriminality by se měla dle mého názoru stát součástí výchovy a vzdělávání každého od nejútlejšího věku, neboť rizikům kyberkriminality v rámci sociálních sítí může být předcházeno pouze za předpokladu, že jsou uživatelům těchto online služeb známá. Z výše uvedených důvodů jsem se při vytváření tohoto preventivního programu zaměřila na viktimologickou prevenci kriminality, neboť se tímto materiálem snažím cílit zejména na uživatele sociálních sítí, kteří by se v budoucnu jejich užívání mohli stát obětmi kybernetických útoků, v některých případech tedy i trestných činů. Jelikož se jedná o viktimologickou prevenci, soustředila jsem se zejména na to, aby potenciální oběti byly seznámeny s riziky, informovány o průběhu konkrétního útoku či způsobu, jak konkrétním útokům předcházet. Skutečná oběť, která se již v minulosti stala terčem některých z výše uvedených útoků na sociálních sítích zde může najít základní informace o bezpečném chování, o způsobech řešení či oznámení takového útoku a informacích k zabránění viktimologické recidivě, tedy k zabránění, aby se obětí takového útoku stala opakovaně. Dle okruhu osob, pro které je tento preventivní program určen, lze tento označit zejména jako sekundární prevenci, neboť oslovuje omezenější, konkrétnější okruh osob, tedy hlavně uživatele sociálních sítí. Není to ovšem jediná cílová skupina, neboť bych ráda osvětu v problematice negativní stránky sociálních sítí započala též mezi osobami, které sociální sítě zatím nevyužívají, ovšem mají zájem v tom, aby se např. jejich potomci dokázali na internetu chovat bezpečně či chtějí bezpečí na internetu svým potomkům zajistit.

Hlavním cílem tohoto preventivního programu, který je dále označován jako *„letáky“*, je tedy pomocí základních informací stručně, avšak výrazně, upozornit na některá nebezpečí a rizika komunikace na sociálních sítích, zejména na kyberšikanu, kyberstalking, kybergrooming a sexting, o kterých je pojednáváno v teoretické části této bakalářské práce. Po seznámení se s letáky by měl čtenář získat základní informace o tom, jaká rizika jsou před ním skryta na sociálních sítích, jak se chovat bezpečně při používání těchto služeb, jak předcházet protiprávnímu jednání a v případě, že se osoba sama nebo

někdo z blízkých stal obětí některého internetového útoku, seznam kontaktních pracovišť, na která se v případě potřeby lze obrátit.

Jako první byl vytvořen leták určený pro učitele a jiné pedagogické pracovníky tvořen čtyřmi stranami, v němž lze naleznout základní informace – za jakým účelem byl tento leták vytvořen a jaké problematice se věnuje. Na dalších stranách letáku je možné se dozvědět podrobnější informace o rizikovém chování na sociálních sítích, odkaz na vzdělávací videa či jiné preventivní programy a přehled kontaktních míst pro případ, že je nutné případ ohlásit.

Stejný koncept byl použit pro tvorbu letáku určenému všem rodičům, kteří chtějí dbát na bezpečnost svých dětí při používání sociálních sítí.

Dvoustránkový koncept byl použit pro tvorbu letáku určenému pro děti a studenty, který se skládá z deseti pokynů, kterými by se každé dítě, které používá sociální sítě, mělo řídit. Na straně druhé tohoto letáku je taktéž seznam kontaktních linek, na které se může dítě, v případě, že se setkalo na sociální síti s kyberútokem, s nevhodným, urážejícím či jinak nebezpečným obsahem, neprodleně obrátit.

Letáky byly vytvořeny v programu Publisher 2013 ze sady Microsoft Office 2013, jejichž stránky byly jednotlivě vloženy do souboru této bakalářské práce.

BEZPEČNĚ NA SOCIÁLNÍCH SÍTÍCH

PRO UČITELE

Na úvod

Tento materiál byl vytvořen s cílem preventivně působit primámě na děti a mládež, kteří se se sociálními sítěmi setkávají denně, avšak ne vždy si plně uvědomují rizika spojená s užíváním těchto služeb. Hlavním tématem je rizikové chování, kterého se může každý uživatel Internetu a sociálních sítí dopustit. Úkolem tohoto letáku je seznámit Vás, jako pedagogy, s riziky spojenými s užíváním sociálních sítí, abyste mohli informace předat dál, zejména Vašim žákům.

K ZAMYŠLENÍ...

Jste si vědomi rizik, která se pojí s používáním sociálních sítí?

Myslíte, že informovanost žáků o těchto rizicích je dostačující?

Víte, kam se obrátit v případě, že Vás nebo některého z Vašich žáků někdo obtěžuje na Internetu?

Sociální sítě mohou v některých případech ubližovat. A pokud tímto letákem přispěji k tomu, že Vaše děti a děti ve Vaší škole budou znát rizika spojená s užíváním sociálních sítí a budou schopny zabránit tomu, aby se staly obětmi kyberútočníků, můj cíl bude splněn.

Kateřina Pilíková, DiS.
autorka

Zdroj: https://www.memisto.cz/2017/07/09/socialni-site-muj-pohled/

Rizikové formy chování na sociálních sítích

- Kyberšikana
- Kyberstalking
- Kybergrooming
- Sexting

Více o tomto chování na další straně.

S čím se mohou na sociálních sítích setkat?

Kyberšikana, kyberstalking, kybergrooming, sexting, vydírání a další.

Víte, co je KYBERŠIKANA?

Tento pojem pod sebou skrývá mnoho podob chování útočníka, avšak cíl je jediný. Opakovaně fyzicky (nahrávání fyzického útoku) a zejména pak psychicky (vydírání, urážení, ponižování) ubližovat oběti za použití informačních a komunikačních technologií (počítače, mobilního telefonu), v kyberprostoru (na Internetu, na sociálních sítích). Pro prevenci ve škole je důležité hovořit s dětmi o kyberšikaně, jaké chování pod sebou může skrývat a že všechny způsoby takového chování jsou nepřijatelné, určete srozumitelná pravidla pro používání mobilních telefonů a jiných technologií ve škole/při výuce, seznamte je s tzv. „NETIKETOU" (etiketou na Internetu), s možnostmi obrany, pokud k útoku dojde. Snažte se kyberšikaně zcela předejít - instalací softwaru, který bude blokovat nevhodné stránky (i stránky, které nejsou nutné pro studium), vytvořením plánů postupu při řešení kyberšikany pro různé formy kyberšikany, abyste Vy i Vaši kolegové byli schopni jednat ihned. Jako pedagog můžete odhalit kyberšikanu přímým pozorováním. Zbystřit byste měli v případech, kdy dítě (oběť) začne často měnit své nálady nebo chování, při používání mobilu je nervózní, chodí za školu, uzavře se do sebe a vyhýbá se kontaktu s přáteli, je smutné či ustrašené, špatně se soustředí.

Víte, co je KYBERSTALKING?

Odvození od slova *stalking (pronásledování, lovení)* - zneužití informačních a komunikačních technologií k dlouhodobému pronásledování oběti (skrze sociální sítě, messengery,..). Pachatel svou oběť obtěžuje převážně nevyžádanými zprávami či jinou pozorností, která u oběti může vyvolat dokonce i strach o svůj život/zdraví. Rizikovou skupinou jsou celebrity, bývalý přítel/přítelkyně nebo osoby, kterým nebyla opětována láska. Pro prevenci před kyberstalkingem můžete promítnout dětem krátký film s komentářem, s názvem *„Virtuální nápadník"*, ve kterém lze vidět stupňování chování útočníka. Video je dostupné na webu www.e-bezpeci.cz nebo na YouTube*. Účinnou prevencí proti kyberstalkingu je nezveřejňovat na sociálních sítích své osobní údaje (adresa bydliště nebo školy, datum narození, telefonní číslo,..) a nepřidávat si do přátel (nekomunikovat) s cizími osobami.

Naznačte, že právě za Vámi mohou přijít, pokud mají problém..

* video dostupné zde: https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/kyberstalking/928-virtualni-napadnik-preventivni-film-o-stalkingu NEBO https://www.youtube.com/watch?v=d2VuImHIqYU

Seznamte žáky s riziky v rámci výuky IT

Jejich každodenní komunikace skrze sociální sítě se v dnešní době stává nedílnou součástí života každého z nich. Ale uvědomují si všichni rizika spojená s komunikací právě přes tyto služby? Jsou si vědomi, že jejich chování může být velmi rizikové a může mít fatální následky? Výuka IT je pro preventivní působení na žáky coby uživatele sociálních sítí ideální. Můžete je seznámit a naučit používat technické prostředky ochrany, jako je např. blokace uživatelů či nevyžádaných zpráv a jak mohou ochránit svou identitu.

SEZNAM SE BEZPEČNĚ

Tato kampaň portálu www.seznam.cz je zaměřena na rizika spojená s Internetem obecně. Na webové stránce **www.stream.cz/porady/seznam-se-bezpecne** můžete shlédnout krátká videa zobrazující ty největší rizika Internetu.

ČSOB

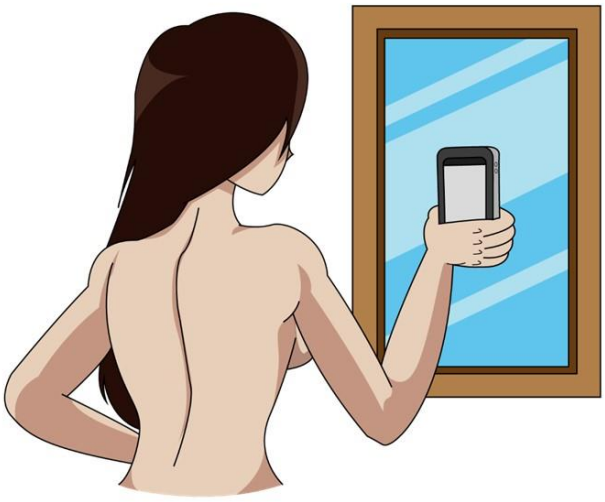
„TVOJE CESTA #ONLINEM"

Na nárůst kyberkriminality na sociálních sítích reaguje též společnost ČSOB doplněna preventisty Policie ČR, kteří pro žáky 2. stupně základních škol realizují výukové bloky v podobě debaty o nástrahách sociálních sítí a základních bezpečnostních principech online světa, které je nutné dodržovat. Více informací na **www.csob.cz/vbezpeci.**

Víte, co je SEXTING?

Spojení slov *sex* a *texting*, tedy sextování představuje jednu z nejnebezpečnějších forem chování na sociálních sítích. Zasílání zpráv sexuálního charakteru (fotografie, videa, SMS zprávy) je velmi rizikové, neboť autor tohoto materiálu nemá nikdy jistotu, ke komu se jeho fotografie nakonec dostanou. Navíc se může díky takovým fotografiím stát terčem vydírání, kyberšikany, kybergroomingu, v případě dětských autorů dokonce pachatelem trestných činů výroby, přechovávání a šíření dětské pornografie. Uživatelé sociálních sítí si často neuvědomují, že pokud svou intimní fotografii zveřejní (odešlou), ztrácí tak nad ní absolutní kontrolu a nikdo nemůže zaručit, že fotka bude trvale odstraněna a nebude tak navždy kolovat Internetem. V případě, že se někdo dostane k takovému materiálu neoprávněně či ho zneužije nebo rozšíří sociálními sítěmi, je nejlepší ihned kontaktovat Policii ČR či anonymně poradnám, které poskytují pomoc obětem sextingu.

Zdroj: http://rdomenica17.blogspot.com/2018/04/



Zdroj: https://sites.google.com/site/say17eme01/como-identificarlo

Víte, co je KYBERGROOMING?

Kybergroomingem označujeme útok osoby, jejíž cílem je vytvořit (nejčastěji u dětí) falešnou důvěru a její pomocí tak vylákat dítě k osobní schůzce, při které na něj útočník fyzicky či sexuálně zaútočí nebo ho donutí k výrobě dětské pornografie. Útokům kybergroomera lze předejít zejména tím, že dítěti budou známa rizika komunikace s cizími osobami na sociálních sítích. Mezi základní zásady patří nepřidávat si cizí osoby do seznamu přátel (i v případě, že některý z jejich dosavadních přátel se s touto osobou na sociální síti přátelí), nepořizovat a s nikým nesdílet materiály (fotografie, videa, zprávy) se sexuálním obsahem, neboť na jejich základě může být dříve nebo později oběť k osobní schůzce donucena vydíráním. Stejně tak nesvěřovat se cizím osobám s problémy a tajemstvími a celkově nebýt přehnaně důvěřivý k informacím, které získají na sociálních sítích, protože nikdy nemohou vědět, kdo se za druhou obrazovkou skrývá a zda daná osoba nelže. Dítě by se zároveň nemělo nechat podplácet dárky a žádost, aby přátelství zůstalo v úplné tajnosti, raději odmítnout.

KAM SE OBRÁTIT V PŘÍPADĚ PROBLÉMŮ?

Včasným odhalením a řešením problému můžete i Vy zamezit negativním a trvalým následkům, které hrozí obětem kyberkriminality.

ADMINISTRÁTOR SOCIÁLNÍ SÍTĚ Každá sociální síť (Facebook, Instagram, YouTube, WhatsApp a další) nabízí možnost **nahlásit nevhodný obsah** (příspěvky, komentáře) či **blokovat** uživatelské účty a zasílání zpráv
https://www.facebook.com/safety
https://help.instagram.com/667810236572057
https://www.youtube.com/yt/policyandsafety/safety.html
https://www.snapchat.com/safety
https://faq.whatsapp.com/en/android/21197244/?category=5245250

POLICIE ČR Nemusíte se bát kontaktovat Policii ČR přímo na **bezplatné lince 158**

STOP ONLINE Na webové stránce **www.stoponline.cz** naleznete formulář, kterým můžete ohlásit nezákonný obsah, zejména materiály související se zneužíváním dětí, kybergroomingem nebo šířením pornografie

DĚTSKÉ KRIZOVÉ CENTRUM - rizika kyberprostoru Na telefonním čísle **778 510 510** se děti mohou kdykoliv obrátit na psychology, se kterými si mohou promluvit o všem nepříjemném či ohrožujícím, s čím se setkaly v kyberprostoru (na sociálních sítích)

LINKA BEZPEČÍ V případě, že se dítě/dospívající z jakéhokoliv důvodu nemůže či bojí svěřit pedagogům nebo rodičům, může se bezplatně a v jakoukoliv dobu obrátit na linku **116 111**

RODIČOVSKÁ LINKA Na telefonní číslo **606 021 021** nebo e-mailovou adresu **pomoc@rodicovskalinka.cz** se mohou obrátit nejen rodiče a prarodiče, ale i další rodinní příslušníci a pedagogové, kterým není osud dětí lhostejný

PORADNA E-BEZPEČÍ Na webové stránce **www.poradna.e-bezpeci.cz** naleznete formulář, jehož vyplněním můžete oznámit problém týkající se mobilních telefonů, sociálních sítí (Internetu), pokud by jejich pomocí někdo oběť např. vydíral nebo nutil k osobní schůzce a oběť by z nějakého důvodu nechtěla kontaktovat přímo Policii ČR (chtěla by zůstat anonymní).

Vytvořila:

Kateřina PILÍKOVÁ, DiS.

v rámci bakalářské práce
SOCIÁLNÍ SÍTĚ - PROSTŘEDÍ PRO TRESTNOU ČINNOST

Vysoká škola evropských a regionálních studií, z. ú.,

České Budějovice

2020

BEZPEČNĚ NA SOCIÁLNÍCH SÍTÍCH

PRO RODIČE

Na úvod

Tento materiál byl vytvořen s cílem preventivně působit primárně na děti a mládež, které se se sociálními sítěmi setkávají denně, avšak ne vždy si plně uvědomují rizika spojená s užíváním těchto služeb. Hlavním tématem je rizikové chování, kterého se může každý uživatel Internetu a sociálních sítí, dopustit. Úkolem tohoto letáku je seznámit Vás, jako rodiče, s riziky spojenými s užíváním sociálních sítí, abyste na základě získaných informací mohli preventivně působit na své děti a naučit je tak bezpečnému chování zejména na sociálních sítích. Jedině tak můžete minimalizovat riziko, že se právě Váš syn nebo Vaše dcera stanou obětí kyberútočníka.

K ZAMYŠLENÍ...

Jste si vědomi rizik, která se pojí s používáním sociálních sítí?

Je Vaše informovanost o rizicích dostatečná?

Víte, kolik času tráví Vaše dítě na sociálních sítích?

Víte, kam se obrátit v případě, že Vás nebo Vaše dítě někdo obtěžuje na Internetu?

Sociální sítě mohou v některých případech ubližovat. A pokud tímto letákem přispěji k tomu, že Vaše děti budou znát rizika spojená s užíváním sociálních sítí a budou schopny zabránit tomu, aby se staly obětmi kyberútočníků, můj cíl bude splněn.

Kateřina Pilíková, DiS.
autorka

Zdroj: https://www.memisto.cz/2017/07/09/socialni-site-muj-pohled/

Rizikové formy chování na sociálních sítích

- Kyberšikana
- Kyberstalking
- Kybergrooming
- Sexting

Více o tomto chování na další straně.

S čím se Vaše děti mohou na sociálních sítích setkat?

Kyberšikana, kyberstalking, kybergrooming, sexting, vydírání a další.

Víte, co je KYBERŠIKANA?

Tento pojem pod sebou skrývá mnoho podob chování útočníka, avšak cíl je jediný. Opakovaně fyzicky (nahrávání fyzického útoku) a zejména pak psychicky (vydírání, urážení, ponižování) ubližovat oběti za použití informačních a komunikačních technologií (počítače, mobilního telefonu), v kyberprostoru (na Internetu, na sociálních sítích). Pro prevenci a včasné odhalení kyberšikany je důležité hovořit s dětmi o kyberšikaně, jaké chování pod sebou může skrývat a že všechny způsoby takového chování jsou nepřijatelné. Kyberšikana nebere ohledy na místo, kde se útočník nebo oběť právě nachází, je tedy možné, že se školní kyberšikana může prolínat do osobního života oběti. Proto byste měli dbát na vzájemnou důvěru mezi Vámi a Vašimi dětmi, aby se v případě potíží mohli obrátit právě na Vás. Stejně tak je pro prevenci důležité správné zabezpečení počítače či mobilního telefonu a zásady správného chování na sociálních sítích. Dítě by mělo vědět, jak se na sociálních sítích chovat tak, aby se samo nestalo obětí nebo dokonce agresorem kyberšikany. Při nastalých problémech byste měli reagovat přiměřeně situaci tak, abyste neztratili důvěru dítěte.

Víte, co je KYBERSTALKING?

Odvození od slova *stalking (pronásledování, lovení)* - zneužití informačních a komunikačních technologií k dlouhodobému pronásledování oběti (skrze sociální sítě, messengery,..). Pachatel svou oběť obtěžuje převážně nevyžádanými zprávami či jinou pozorností, která u oběti může vyvolat dokonce i strach o svůj život/zdraví. Rizikovou skupinou jsou celebrity, bývalý přítel/přítelkyně nebo osoby, kterým nebyla opětována láska. Pro prevenci před kyberstalkingem můžete promítnout dětem krátký film s komentářem, s názvem *„Virtuální nápadník“*, ve kterém lze vidět stupňování chování útočníka. Video je dostupné na webu www.e-bezpeci.cz nebo na YouTube*. Účinnou prevencí proti kyberstalkingu je nezveřejňovat na sociálních sítích své osobní údaje (adresa bydliště nebo školy, datum narození, telefonní číslo,..) a nepřidávat si do přátel (nekomunikovat) s cizími osobami. V případě, že je dítě dlouhodobě obtěžováno ze strany útočníka, mělo by s ním okamžitě přestat komunikovat a hlavně se s ním nestýkat, pokud je to možné.

* video dostupné zde: https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/kyberstalking/928-virtualni-napadnik-preventivni-film-o-stalkingu NEBO https://www.youtube.com/watch?v=d2VuImHIqYU

Kde můžete najít více informací?

Více informací o nejrůznějších preventivních opatřeních, mj. o způsobech ochrany soukromí či jak fungují rodičovské zámky, včetně výukových materiálů, můžete naleznout na mnoha webových stránkách, které se věnují prevenci před hrozbami sociálních sítí (Internetu).

www.nebudobet.cz
www.bezpecne-online.saferinternet.cz
www.vimkamklikam.cz
www.e-bezpeci.cz
www.bezpecnyinternet.cz
www.minimalizacesikany.cz
www.budsafeonline.cz
www.nasedite.cz/kampan/bezpecny-internet-detem-67/
www.sexting.cz

SEZNAM SE BEZPEČNĚ

Tato kampaň portálu www.seznam.cz je zaměřena na rizika spojená s Internetem obecně. Na webové stránce **www.stream.cz/porady/seznam-se-bezpecne** můžete shlédnout krátká videa zobrazující ty největší rizika Internetu.

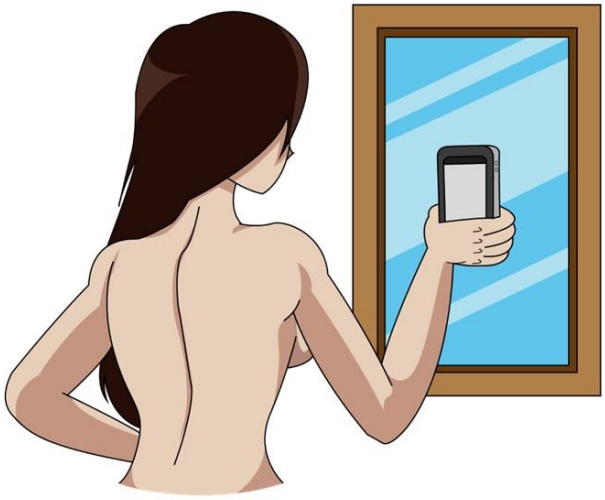
ČSOB „TVOJE CESTA #ONLINEM“

Na nárůst kyberkriminality na sociálních sítích reaguje též společnost ČSOB doplněna preventisty Policie ČR, kteří pro žáky 2. stupně základních škol realizují výukové bloky v podobě debaty o nástrahách sociálních sítí a základních bezpečnostních principech online světa, které je nutné dodržovat. Více informací na **www.csob.cz/vbezpeci.**

Víte, co je SEXTING?

Spojení slov *sex* a *texting*, tedy sextování představuje jednu z nejnebezpečnějších forem chování na sociálních sítích. Zasílání zpráv sexuálního charakteru (fotografie, videa, SMS zprávy) je velmi rizikové, neboť autor tohoto materiálu nemá nikdy jistotu, ke komu se jeho fotografie nakonec dostanou. Navíc se může díky takovým fotografiím stát terčem vydírání, kyberšikany, kybergroomingu, v případě dětských autorů dokonce pachatelem trestných činů výroby, přechovávání a šíření dětské pornografie. Uživatelé sociálních sítí si často neuvědomují, že pokud svou intimní fotografii zveřejní (odešlou), ztrácí tak nad ní absolutní kontrolu a nikdo nemůže zaručit, že fotka bude trvale odstraněna a nebude tak navždy kolovat Internetem. V případě, že se někdo dostane k takovému materiálu neoprávněně či ho zneužije nebo rozšíří sociálními sítěmi, je nejlepší ihned kontaktovat Policii ČR či anonymně poradnám, které poskytují pomoc obětem sextingu.

Zdroj: http://rdomenica117.blogspot.com/2018/04/



Zdroj: https://sites.google.com/site/say17eme01/como-identificarlo

Víte, co je KYBERGROOMING?

Kybergroomingem označujeme útok osoby, jejíž cílem je vytvořit (nejčastěji u dětí) falešnou důvěru a její pomocí tak vylákat dítě k osobní schůzce, při které na něj útočník fyzicky či sexuálně zaútočí nebo ho donutí k výrobě dětské pornografie. Útokům při osobní schůzce lze předejít zejména tím, že dítěti budou známa rizika komunikace s cizími osobami na sociálních sítích - do seznamu přátel si nepřidávat cizí osoby (i v případě, že některý z jejich dosavadních přátel se s touto osobou na sociální síti přátelí), nepořizovat a s nikým nesdílet materiály (fotografie, videa, zprávy) se sexuálním obsahem, neboť na jejich základě může být dříve nebo později oběť k osobní schůzce vydírána, stejně jako skrze svěřená tajemství či problémy a celkově nebýt přehnaně důvěřivý k informacím, které získají na sociálních sítích, protože nikdy nemohou vědět, kdo se za druhou obrazovkou skrývá a zda daná osoba nelže. Dítě by se zároveň nemělo nenechat podplácet dárky a žádost, aby přátelství zůstalo v úplné tajnosti, raději odmítnout. Zbystři byste měli hlavně v případech, kdy Vaše dítě začne trávit nezvykle mnoho času u počítače/mobilního telefonu na úkor setkání se skutečnými kamarády, zajímejte se o to, s kým na sociálních sítích komunikuje.

KAM SE OBRÁTIT V PŘÍPADĚ PROBLÉMŮ?

Včasným odhalením a řešením problému můžete i Vy zamezit negativním a trvalým následkům, které hrozí obětem kyberkriminality.

ADMINISTRÁTOR SOCIÁLNÍ SÍTĚ Každá sociální síť (Facebook, Instagram, YouTube, WhatsApp a další) nabízí možnost **nahlásit nevhodný obsah** (příspěvky, komentáře) či **blokovat** uživatelské účty a zasílání zpráv
https://www.facebook.com/safety
https://help.instagram.com/667810236572057
https://www.youtube.com/yt/policyandsafety/safety.html
https://www.snapchat.com/safety
https://faq.whatsapp.com/en/android/21197244/?category=5245250

POLICIE ČR Nemusíte se bát kontaktovat Policii ČR přímo na **bezplatné lince 158**

STOP ONLINE Na webové stránce **www.stoponline.cz** naleznete formulář, kterým můžete ohlásit nezákonný obsah, zejména materiály související se zneužíváním dětí, kybergroomingem nebo šířením pornografie

DĚTSKÉ KRIZOVÉ CENTRUM - rizika kyberprostoru Na telefonním čísle **778 510 510** se děti mohou kdykoliv obrátit na psychology, se kterými si mohou promluvit o všem nepříjemném či ohrožujícím, s čím se setkaly v kyberprostoru (na sociálních sítích)

LINKA BEZPEČÍ V případě, že se dítě/dospívající z jakéhokoliv důvodu nemůže či bojí svěřit pedagogům nebo rodičům, může se bezplatně a v jakoukoliv dobu obrátit na linku **116 111**

RODIČOVSKÁ LINKA Na telefonní číslo **606 021 021** nebo e-mailovou adresu **pomoc@rodicovskalinka.cz** se mohou obrátit nejen rodiče a prarodiče, ale i další rodinní příslušníci a pedagogové, kterým není osud dětí lhostejný

PORADNA E-BEZPEČÍ Na webové stránce **www.poradna.e-bezpeci.cz** naleznete formulář, jehož vyplněním můžete oznámit problém týkající se mobilních telefonů, sociálních sítí (Internetu), pokud by jejich pomocí někdo oběť např. vydíral nebo nutil k osobní schůzce a oběť by z nějakého důvodu nechtěla kontaktovat přímo Policii ČR (chtěla by zůstat anonymní).

Vytvořila:

Kateřina PILÍKOVÁ, DiS.

v rámci bakalářské práce
SOCIÁLNÍ SÍTĚ - PROSTŘEDÍ PRO TRESTNOU ČINNOST

Vysoká škola evropských a regionálních studií, z. ú.,

České Budějovice

2020

BEZPEČNĚ NA SOCIÁLNÍCH SÍTÍCH

PRO ŽÁKY A STUDENTY

DŮLEŽITÉ ZÁSADY A PRAVIDLA PRO BEZPEČNÉ POUŽÍVÁNÍ SOCIÁLNÍCH SÍTÍ

- **Každý má právo, abys ho na sociálních sítích respektoval/a. Nechovej se k ostatním tak, jak nechceš, aby se oni chovali k Tobě.**
- **Buď opatrný a příliš nedůvěřuj cizím osobám, se kterými se znáš jen ze sociálních sítí. Nikdy nevíš, kdo se doopravdy skrývá za druhou obrazovkou.**
- **Cizím osobám, které znáš jen ze sociálních sítí, nesděluj svůj věk, adresu, telefonní číslo ani kam chodíš do školy. Pokud tyto informace na sociální síti máš, nastav u nich, aby nebyly veřejné a mohly je vidět pouze osoby, které máš v seznamu přátel.**
- **Zvol si silné heslo a udržuj ho v tajnosti i před kamarády a při opouštění sociální sítě se vždy odhlašuj, zejména když se přihlašuješ z veřejného počítače.**
- **Nikomu neposílej a nikdy nezveřejňuj své vyzývavé fotografie či videa. Nikdy nevíš, zda je druhá osoba nezneužije nebo nerozešle. Mohl bys být vydírán nebo se stát terčem posměchu a taková fotka může kolovat internetem napořád.**
- **Nedomlouvej si osobní schůzku s někým koho znáš jen ze sociálních sítí, aniž bys to neřekl rodičům, i kdyby Tě druhá osoba přemlouvala, aby to zůstalo tajemstvím a slibovala Ti dárky.**
- **Pokud Tě někdo na internetu dlouhodobě obtěžuje, ponižuje, uráží nebo Ti vyhrožuje, přestaň s touto osobou ihned komunikovat. V případě, že bys měl strach, oznam to Policii ČR a uschovej důkazní materiál (zprávy, fotografie,..).**
- **Každé kliknutí si promysli, zejména na oznámení, že jsi se stal výhercem nějaké soutěže, do které jsi se nepřihlásil.**
- **Všímej si svého okolí. Možná se obětí některého útočníka stal Tvůj kamarád nebo kamarádka. Není ostuda svěřit se rodičům nebo učitelům ve škole.**
- **Neboj se s problémy, se kterými se na sociálních sítích setkáš, svěřit svým rodičům, učitelům, kamarádům.**

Obrázek dostupný z: https://www.memisto.cz/2017/07/09/socialni-site-muj-pohled/

KAM SE OBRÁTIT V PŘÍPADĚ PROBLÉMŮ?

Včasným oznámením problému můžeš i Ty zabránit škodlivým a trvalým následkům těchto útoků. Neboj se jednat!

ADMINISTRÁTOR SOCIÁLNÍ SÍTĚ Každá sociální síť (Facebook, Instagram, YouTube, WhatsApp a další) nabízí možnost **nahlásit nevhodný obsah** (příspěvky, komentáře) či **blokovat** uživatelské účty a zasílání zpráv
https://www.facebook.com/safety
https://help.instagram.com/667810236572057
https://www.youtube.com/yt/policyandsafety/safety.html
https://www.snapchat.com/safety
https://faq.whatsapp.com/en/android/21197244/?category=5245250

POLICIE ČR Nemusíte se bát ve vážných případech kontaktovat Policii ČR přímo na **bezplatné lince 158**

STOP ONLINE Na webové stránce **www.stoponline.cz** naleznete formulář, kterým můžete ohlásit nezákonný obsah, zejména materiály související se zneužíváním dětí, kybergroomingem nebo šířením pornografie

DĚTSKÉ KRIZOVÉ CENTRUM - rizika kyberprostoru Na telefonním čísle **778 510 510** se děti mohou kdykoliv obrátit na psychology, se kterými si mohou promluvit o všem nepříjemném či ohrožujícím, s čím se setkaly v kyberprostoru (na sociálních sítích)

LINKA BEZPEČÍ V případě, že se dítě/dospívající z jakéhokoliv důvodu nemůže či bojí svěřit pedagogům nebo rodičům, může se bezplatně a v jakoukoliv dobu obrátit na linku **116 111**

PORADNA E-BEZPEČÍ Na webové stránce **www.poradna.e-bezpeci.cz** naleznete formulář, jehož vyplněním můžete oznámit problém týkající se mobilních telefonů, sociálních sítí (Internetu), pokud by jejich pomocí někdo oběť např. vydíral nebo nutil k osobní schůzce a oběť by z nějakého důvodu nechtěla kontaktovat přímo Policii ČR (chtěla by zůstat anonymní)

Vytvořila:

Kateřina PILÍKOVÁ, DiS.

v rámci bakalářské práce
SOCIÁLNÍ SÍTĚ - PROSTŘEDÍ PRO TRESTNOU ČINNOST

Vysoká škola evropských a regionálních studií, z. ú.,

České Budějovice

2020

Závěr

Bakalářská práce svým obsahem aktuálně reaguje na prostředí sociálních sítí, které jsou v některých případech využívány k páchání trestné činnosti a stávají se tak prostředím nebezpečným, neboť ne všichni uživatelé si tato rizika spojená s užíváním sociálních sítí uvědomují. Cílem této práce bylo co nejaktuálněji zanalyzovat a popsat podstatu užívání sociálních sítí, charakterizovat kyberkriminalitu a pojmy s ní spojené pro snadnější porozumění kontextu psaného textu v bakalářské práci.

Zpracováním vlastních poznatků s poznatky z tuzemských i zahraničních zdrojů lze dospět k závěru, že uživatelé sociálních sítí, kteří neznají rizika s užíváním sociálních sítí spojená, se mohou snadno stát obětmi kyberútočníka, nicméně též pachateli, např. v případech rozesílání intimních fotografií dítěti.

Výstupem bakalářské práce je nejen případová studie kyberstalkingu, ve které je nejdříve popsán obecný rámec případu, dále rámec právní a poté je popsán význam z hlediska kyberstalkingu, tedy trestného činu, který je v jednání útočníka spatřován, ale také, jako další výstup, vytvoření preventivního programu, který má za cíl minimalizovat rizika, aby se nejen děti a mladiství stali obětmi, popř. dokonce pachateli trestných činů, ke kterým na sociálních sítích dochází. Preventivní program je tvořen třemi letáky, které jsou jak informačního, tak preventivního charakteru. Cílovou skupinou těchto letáků jsou děti a mladiství, tedy studenti a žáci, dále rodiče a učitelé. Originálním a poutavým způsobem jsou na letácích informace o nejčastějších útocích, ke kterým na sociálních sítích dochází a zároveň tipy, jak takovýmto útokům čelit či dokonce předcházet, kdy na poslední straně každého z nich je seznam kontaktních míst, kam se mohou v případě potíží uživatelé sociálních sítí obrátit.

Seznam použitých zdrojů

Literární zdroje

Děti a online rizika: sborník studií. Praha: Sdružení Linka bezpečí, 2012, 178 s. ISBN 978-80-9049202-8.

DOČEKAL, Daniel, Jan MÜLLER, Anastázie HARRIS a Luboš HEGER. *Dítě v síti: manuál pro rodiče a učitele, kteří chtějí rozumět digitálnímu světu mladé generace.* Praha: Mladá fronta, 2019, 208 s. Flowee. ISBN 978-80-204-5145-3.

ECKERTOVÁ, Lenka, Daniel DOČEKAL, Anastázie HARRIS a Luboš HEGER. *Bezpečnost dětí na internetu: rádce zodpovědného rodiče.* Brno: Computer Press, 2013, 224 s. Flowee. ISBN 978-80-251-3804-5.

JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007, 288 s. ISBN 978-80-247-1561-2.

KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016, 524 s. ISBN 978-80-88168-15-7.

KOPECKÝ, Kamil. *Rizikové formy chování českých a slovenských dětí v prostředí internetu.* Olomouc: Univerzita Palackého v Olomouci, 2015, 170 s. ISBN 9788024448619.

KOŽÍŠEK, Martin a Václav PÍSECKÝ. Bezpečně na internetu: Průvodce chováním ve světě online. 2016. Praha: Grada Publishing, 2016, 176 s. ISBN 978-80-271-9074-4.

MARTÍNEK, Zdeněk. *Agresivita a kriminalita školní mládeže.* 2., aktualizované a rozšířené vydání. Praha: Grada, 2015, 192 s. Pedagogika. ISBN 978-80-247-5309-6.

MINTON, Eric. *Cyberbullies*. The Rosen Publishing Group, 2014, 32 s. ISBN 978-1-4777-3022-5.

MINTON, Eric. *Stay Safe Online: Social Networking And Social Media Safety.* PowerKids Press, 2014, 32 s. ISBN 978-1-4777-3019-5.

SMEJKAL, Vladimír. *Kybernetická kriminalita.* 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018, 936 s. ISBN 9788073807207.

ZAVRŠNIK, Aleš. Kyberkriminalita. Praha: Wolters Kluwer, 2017, 148 s. Právní monografie. ISBN 978-80-7552-758-5.

Elektronické zdroje

BENEDIKT, Michael. Cyberspace: First Steps [online]. 1991 [cit. 2019-12-12]. Dostupné z: https://archive.org/details/CyberspaceFirstSteps.

BURÝŠKOVÁ, Lenka. Policie České republiky: Víte co je KYBERŠIKANA? [online]. [cit. 2019-12-12]. Dostupné z: https://www.policie.cz/clanek/vite-co-je-kybersikana.aspx.

Centrum nápovědy: Vytvoření účtu [online]. [cit. 2019-10-20]. Dostupné z: https://www.facebook.com/help/?helpref=hc_global_nav.

Co je kyberšikana a jak se projevuje? [online]. [cit. 2019-12-12]. Dostupné z: https://bezpecneonline.saferinternet.cz/pro-rodice-a-ucitele/teenageri-a-komunikace/item/34-co-je-to-kybersikana-a-jakse-projevuje.

DU, Jun, JIANG, Chunxiao, et. Al. Community-Structured Evolutionary Game for Privacy Protection in Social Networks. In: IEEE Transactions on Information Forensics and Security, Volume: 13; Issue: 3.[online] 2018. str. 2 [cit. 2019-10-13]. Dostupné z: http://www.eng.usf.edu/chen/pdf/Community-Structured%20Evolutionary%20Game%20for%20Privacy%20Protection%20in%20Social%20Networks.pdf.

Facebook: Centrum nápovědy [online]. [cit. 2019-10-10]. Dostupné z: https://www.facebook.com/help/570785306433644?helpref=hc_global_nav.

Facebook: Centrum nápovědy: Odebrání uživatele z přátel nebo zablokování [online]. [cit. 2019-12-12]. Dostupné z: https://www.facebook.com/help/1000976436606344?helpref=hc_global_nav.

HAPPY SLAPPING [online]. [cit. 2019-12-12]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/happyslapping/.

HOAX: Jak hoax poznáme [online]. [cit. 2020-02-12]. Dostupné z: https://www.hoax.cz/hoax/co-je-to-hoax.

InNovinky.cz: Student z Bruntálska vydíral dívky prostřednictvím intimních fotek [online]. 2019 [cit. 2020-08-18]. Dostupné z: https://www.novinky.cz/krimi/clanek/student-z-bruntalska-vydiral-divky-prostrednictvim-intimnich-fotek-40269741.

Instagram [online]. 2017 [cit. 2019-11-05]. Dostupné z: https://searchcio.techtarget.com/definition/Instagram.

Instant Messaging [online]. [cit. 2019-11-05]. Dostupné z: https://it-slovnik.cz/pojem/instantmessaging.

Internet World Stats. INTERNET USAGE STATISTICS. The Big Picture World Internet Users and 2018 Population Stats[online]. 2018. [cit. 2019-12-12]. Dostupné z: https://internetworldstats.com/stats.htm.

IROZHLAS: Po internetu koluje nahrávka o zákazu vycházení v Česku, autorce poplašné zprávy hrozí až 8 let vězení [online]. [cit. 2020-04-04]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/nahravka-zakaz-vychazeni-poplasna-zprava_2003210956_ada.

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti [online]. [cit. 2019-12-12]. Dostupné z: https://www.govcert.cz/download/aktuality/container-nodeid548/slovnikv231nbuwebcolor.pdf.

JUDr. VICHLENDA, Milan a Ph.D. Ing. Ivan KŘEČEK. Kriminologie: Studijní opora Střední školy ochrany osob a majetku s.r.o. [online]. 2011. [cit. 2020-08-20]. Dostupné z: https://www.sosoom-zlin.cz/media/skripta/kriminologie.pdf.

KOPECKÝ, Kamil. Metodický portál inspirace a zkušeností učitelů: Nebezpečí zvané kybergrooming I.[online]. 2010 [cit. 2019-12-12]. Dostupné z: https://clanky.rvp.cz/clanek/s/Z/9741/NEBEZPECIZVANE-KYBERGROOMING-I.html/.

KUCHTA, Josef. Časopis pro právní vědu a praxi: Aktuální problémy počítačové kriminality včetně její prevence [online]. Brno, 2016, XXIV (1/2016) [cit. 2019-12-12]. ISSN 1805-2789. Dostupné z: https://journals.muni.cz/cpvp/article/view/5260/4344.

LEXICO: UK Dictionary [online]. [cit.2019-10-10]. Dostupné z: https://www.lexico.com/definition/social_network.

MÁČELOVÁ, Karolína. Učení v pohodě: Fáze kybergroomingu: Podezřelé chování virtuálních přátel[online]. [cit. 2019-12-15]. Dostupné z: http://www.uceni-v-pohode.cz/faze-kybergroomingupodezrele-chovani-virtualnich-pratel/.

Ministerstvo vnitra České republiky: Prevence kriminality. Republikový výbor pro prevenci kriminality [online]. [cit. 2020-08-20]. Dostupné z: https://www.mvcr.cz/clanek/rvppk-republikovy-vybor-pro-prevenci-kriminality.aspx.

Ministerstvo vnitra České republiky: Systém prevence kriminality v ČR [online]. [cit. 2020-08-20]. Dostupné z: mvcr.cz/clanek/web-o-nas-prevence-prevence-kriminality.aspx?q=Y2hudW09NA%3d%3d.

Ministerstvo vnitra České republiky: Systém prevence kriminality v ČR [online]. [cit. 2020-08-20]. Dostupné z: mvcr.cz/clanek/web-o-nas-prevence-prevence-kriminality.aspx?q=Y2hudW09NA%3d%3d.

NEBUĎ OBĚŤ: KYBERGROOMING - Jak se bránit kybergroomerovi? [online]. [cit. 2019-12-15]. Dostupné z: http://www.nebudobet.cz/?cat=kybergrooming.

NEBUĎ OBĚŤ: SEXTING - Co je to sexting? [online]. [cit. 2019-12-15]. Dostupné z: www.nebudobet.cz/?cat=sexting.

NISSENBAUM, Helen. The Meaning of Anonymity in an Information Age. The Information Society [online]. University Center for Human Values, Princeton University, Princeton, New Jersey, USA, 1999, s. 141-144 [cit. 2019-10-20]. Dostupné z: http://crazyjamiejo.pbworks.com/w/file/fetch/69786921/Anonymity%20in%20an%20Information%20Ag e.pdf.

Our History [online]. [cit. 2019-10-20]. Dostupné z: https://newsroom.fb.com/company-info/.

PAPEŽOVÁ, Zdeňka. Policie České republiky: PREVENCE - Kyberšikana [online]. [cit. 2019-12-12]. Dostupné z: https://www.policie.cz/clanek/prevence-kybersikana.aspx.

PAPEŽOVÁ, Zdeňka. Policie České republiky: PREVENCE - Stalking [online]. [cit. 2019-12-12]. Dostupné z: https://www.policie.cz/clanek/prevence-stalking.aspx.

plk. JUDr. MAZÁNEK, Jiří. Policie ČR: Nabídka práce u NCOZ pro policistky a policisty [online]. [cit. 2020-08-20]. Dostupné z: https://www.policie.cz/clanek/nabidka-prace-u-ncoz-pro-policistky-a-policisty.aspx?fbclid=IwAR22fXe-hOtXlANswXK8vtjCVjBWWFKCmNmuiKSAPvr5C2-xaVQuGKDCLh8.

Policie ČR: Kyberkriminalita [online]. [cit. 2020-08-20]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx?fbclid=IwAR0obuwnxkkyIToVj7NwtBIfgC-ay_1SE1Cs98RFroyFXeKhmgomjvSJzF8.

Policie ČR: Preventivně informační skupina [online]. [cit. 2020-08-20]. Dostupné z: https://www.policie.cz/clanek/sprava-stredoceskeho-kraje-odkazy-akce-a-projekty-preventivne-informacni-skupina.aspx?fbclid=IwAR1NH7QtgZq7I_nJRlyzOdYZLlJ6_OEEjPzjXbYQE8lnkfqR4i31H-oZUwA.

Prevence kriminality: Prevence se musí vyplatit [online]. 2019 [cit. 2020-08-20]. Dostupné z: https://prevencekriminality.cz/prevence-kriminality/.

Sexting.cz: Co je vlastně sexting? [online]. [cit. 2019-12-15]. Dostupné z: http://www.sexting.cz/.

SULER, John. Identity Management in Cyberspace, 2002. [online]. [cit. 2019-10-13]. DOI: 10.1023/A:1020392231924. Dostupné z: https://www.researchgate.net/publication/263498490_Identity_Management_in_Cyberspace.

The threats [online]. [cit. 2019-12-12]. Dostupné z: https://www.interpol.int/Crimeareas/Cybercrime/The-threats.

TN.CZ:Hackeři ukradli intimní fotky pacientů kliniky. Vydírají tisíce lidí! [online]. 2017 [cit. 2020-08-18]. Dostupné z: https://tn.nova.cz/clanek/hackeri-ukradli-intimni-fotky-pacientu-kliniky-vydiraji-tisice-lidi.html.

Twitter [online]. 2015 [cit. 2019-11-05]. Dostupné z: https://whatis.techtarget.com/definition/Twitter.

VAN SCHAIK, Paul, JANSEN, Jurjen, et. Al. Scurity and privacy in online social networking: risk perceptions and precautionary behaviour. In: Computers in Human Behaviour. [online]. 2017. [cit. 2019-10-13]. str. 7-8. Dostupné z: https://www.researchgate.net/publication/320288475_Security_and_privacy_in_online_social_networking_Risk_perceptions_and_precautionary_behaviour.pdf. ISSN: 0747-5632.

VÝROST, Jozef a Ivan SLAMĚNÍK. Sociální psychologie. 2. přepracované a rozšířené vydání. Praha 7: Grada Publishing, 2008, str. 113. ISBN 978-80-247-1428-8. Dostupné také z: https://books.google.cz/books?id=czijlGDrBJsC&pg=PA3&dq=v%C3%BDrost+jozef&hl=cs&sa=X&ved=0ahUKEwii9OqDn4noAhUQ-qQKHaFPDMcQ6AEIQDAD#v=onepage&q=v%C3%BDrost%20jozef&f=false.

WALLACE, Kathleen A. Ethics and Information Technology [online]. Department of Philosophy, Hofstra University, NY, USA, 1999, s. 23-24 [cit. 2019-10-20]. DOI: 10.1023/A:1010066509278. Dostupné z: https://link.springer.com/article/10.1023/A:1010066509278.

WhatsApp Messenger [online]. [cit. 2019-11-05]. Dostupné z: https://play.google.com/store/apps/details?id=com.whatsapp.

Legislativní dokumenty

ČESKÁ REPUBLIKA. Usnesení č. 2/1993 Sb., předsednictva České národní rady o vyhlášení *LISTINY ZÁKLADNÍCH PRÁV A* SVOBOD jako součástí ústavního pořádku České republiky.

ČESKÁ REPUBLIKA. Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

ČESKÁ REPUBLIKA. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

ČESKÁ REPUBLIKA. Zákon č. 273/2008 Sb., o Policii ČR.

ČESKÁ REPUBLIKA. Zákon č. 40/2009 Sb., trestní zákoník.

ČESKÁ REPUBLIKA. Zákon č. 89/2012 Sb., občanský zákoník.

EVROPSKÝ PARLAMENT A RADA EU. Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: EUR-Lex [právní informační systém]. Úřad pro publikace Evropské unie. [cit. 2019-10-14]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex%3A32016R0679.

UNITED NATIONS: Všeobecná deklarace lidských práv [online]. 2015 [cit. 2019-10-13]. Dostupné z: https://www.osn.cz/wp-content/uploads/2015/12/UDHR_2015_11x11_CZ2.pdf.

Judikatura:

Nález Ústavního soudu sp. zn. I. ÚS 3324/15 a nález Ústavního soudu sp. zn. II. ÚS 2588/16, ze dne 24. 11. 2016. [online] [cit. 2019-12-17]. In: NALUS: Vyhledávání rozhodnutí Ústavního soudu České republiky. Dostupné z: https://nalus.usoud.cz/Search/Search.aspx.

Rozhodnutí Nejvyššího soudu České republiky ze dne 30. 11. 2011, sp. zn. 8 Tdo 1503/2011 [online]. [cit. 2019-12-17]. Dostupné z: https://iudictum.cz/185846/8-tdo-1503-2011.

Rozsudek Soudního dvora ze dne 19. října 2016, Patrick Breyer proti Bundesrepublik Deutschland, C-582/14, EU:C:2016:779, bod49. Dostupné z:

http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=CS.

Ostatní zdroje:

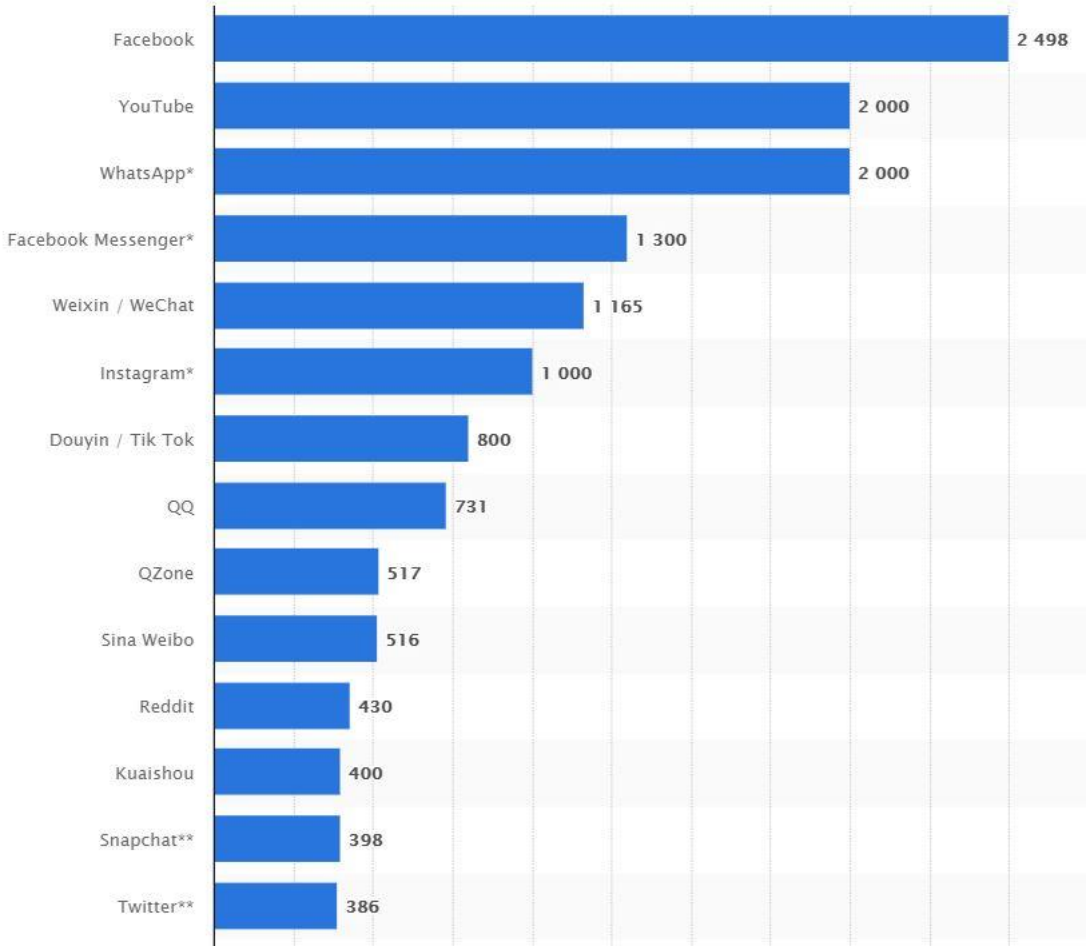
Fake Chat: Facebook Chat generátor. [online]. [cit. 2020-01-07]. Dostupné z:

http://fake-chat.cz/?facebook_full_chat.

Seznam zkratek

ZOOU	zákon o ochraně osobních údajů
NOZ	„Nový“ občanský zákoník
GDPR	Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů
TZ	trestní zákoník
ZKB	zákon o kybernetické bezpečnosti
VS	veřejná správa

Přílohy



Příloha č. 1: Most popular social networks worldwide as of April 2020, ranked by number of active users(in millions)

Zdroj: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

Příloha č. 2: The „Deep Web“ is Not All Dark

Zdroj: https://www.deepwebtech.com/deepweb-not-darkweb/

Seznam členů Republikového výboru pro prevenci kriminality

Předseda Jan HAMÁČEK (ministr vnitra)

Výkonný místopředseda JUDr. Ing. Jiří NOVÁČEK (první náměstek ministra vnitra pro řízení sekce vnitřní bezpečnosti a policejního vzdělávání)

Dalšími členy jsou zástupci:

Asociace krajů České republiky

Generálního ředitelství Vězeňské služby České republiky

Institutu pro kriminologii a sociální prevenci

Ministerstva financí

Ministerstva obrany

Ministerstva práce a sociálních věcí – oblast rodinné politiky a ochrany práv dětí

Ministerstva práce a sociálních věcí – oblast sociálních služeb a sociální práce

Ministerstva spravedlnosti – oblast trestní politiky

Ministerstva spravedlnosti – oblast trestní legislativy

Ministerstva školství, mládeže a tělovýchovy

Ministerstva vnitra – ředitel odboru, do jehož gesce spadá oblast prevence kriminality

Ministerstva vnitra – vedoucí oddělení, do jehož gesce spadá oblast prevence kriminality

Ministerstva vnitra – oblast bezpečnostní politiky

Ministerstva zdravotnictví

Nejvyššího státního zastupitelství

Policejního prezidia České republiky – oblast vnější služby

Policejního prezidia České republiky – oblast služby kriminální policie a vyšetřování

Policejního prezidia České republiky – republikový koordinátor prevence kriminality Policie ČR

Probační a mediační služby České republiky

Soudcovské unie České republiky

Svazu měst a obcí České republiky

Úřadu vlády České republiky – Odboru sociálního začleňování (Agentura)

Úřadu vlády České republiky – Rady vlády pro koordinaci protidrogové politiky

Úřadu vlády České republiky – Rady vlády pro záležitosti romské menšiny

Příloha č. 3: Seznam členů Republikového výboru pro prevenci kriminality

Zdroj: https://www.mvcr.cz/clanek/rvppk-republikovy-vybor-pro-prevenci-kriminality.aspx?q=Y2hudW09NA%3d%3d