UNIVERZITA KARLOVA

Právnická fakulta

Bc. Jana Havlíčková

Prevence kriminality

Specifika prevence kyberkriminality na sociálních sítích

Diplomová práce

Vedoucí diplomové práce: doc. JUDr. Jana Tlapák Navrátilová, Ph.D.

Katedra trestního práva

Datum uzavření rukopisu: 15. prosince 2017

Prohlašuji, že jsem předkládanou diplomovou práci vypracovala samostatně, že všechny použité zdroje byly řádně uvedeny a že práce nebyla využita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této práce včetně mezer a včetně poznámek pod čarou má 186 982 znaků.

V Praze dne 15. prosince 2017

autorka diplomové práce

Obsah

Úvod

Kriminalita je nejzávažnějším negativním společenským jevem, protože porušování zákona ve formě útoků na chráněné společenské hodnoty, způsobuje těžko nahraditelné či nenahraditelné újmy. Proto je třeba jít za hranice represivního působení, kriminalitě předcházet a nikoli ji pouze trestat. Prevence kriminality je systémem aktivit směřujících k eliminaci nežádoucích jevů ve společnosti a k vytvoření lepšího standardu lidského života ve všech jeho aspektech.

Kriminalita se přizpůsobuje vývoji společnosti. Za současné míry globalizace a úrovně technologií musíme pracovat s novými a vyvíjejícími se formami kriminality. Tyto nové formy je nutné analyzovat, včas a efektivně na ně reagovat a prognózovat jejich vývoj. Nejdynamičtěji se rozvíjející kriminalitou je kybernetická trestná činnost.

Cílem této práce je sestavit aktuální obraz prevence kriminality s důrazem na kyberkriminalitu. Diplomovou práci jsem pomyslně rozdělila na dvě části, přičemž první z nich řeší kriminalitu a její prevenci obecně, zatímco druhá se věnuje právě specifikům kyberkriminality. Metodologicky práce vychází z klasifikační, kauzální, a vztahové analýzy, kompilace, komparace a syntézy jednotlivých zdrojů, indukčně-dedukčního logického vyvozování, analogie a modelování.

V první části práce nejdříve stručně vymezím základní pojmy, jako kriminalita, kriminalizace a dekriminalizace, kriminogenní faktory, recidiva, kriminologie, penologie, viktimologie, kontrola kriminality, represe a prevence. Dále systematizuji prevenci kriminality, a především se věnuji jejímu členění dle obsahu či cílového objektu na sociální, situační a viktimologickou, a také dle okruhu adresátů na primární, sekundární a terciární. Značný prostor budu věnovat současnému zaměření prevence kriminality, kdy se odkazuji zejména na Deklaraci z Dauhá a další výstupy z 13. Kongresu OSN pro prevenci kriminality a trestní justici, dále na aktuální Víceletou strategii EUCPN a, v neposlední řadě, na Strategii prevence kriminality v České republice na léta 2016 až 2020 a na ní navazující Akční plán prevence kriminality na léta 2016 až 2020. Poté přiblížím systém prevence kriminality v České republice, jeho subjekty na jednotlivých úrovních a jejich aktuální specifické cíle.

Druhá část práce se věnuje kyberkriminalitě se zaměřením na její projevy na sociálních sítích. Po vymezení pojmů souvisejících s kyberkriminalitou, nastíním legislativní rámec kyberprostoru a kyberkriminality ve vnitrostátním i mezinárodním kontextu, se zaměřením na trestné činy spadající pod pojem kybernetická trestná činnost. Následně zmíním strategie v oblasti prevence kyberkriminality. Dále se pokusím vymezit konkrétní projevy kyberkriminality na sociálních sítích, které označujeme jako kybergrooming, kyberstalking, kyberšikana, sexting a související dětská pornografie. U těchto forem kyberkriminality uvedu pravidla pro jejich předcházení a vhodné reakce a způsoby řešení případů rizikové komunikace, vycházející z metodik prevence kyberkriminality. V závěru práce uvedu několik českých i mezinárodních iniciativ a projektů prevence kyberkriminality, zejména se budu věnovat projektu Safer Internet CZ a jeho dílčím projektům a aktivitám.

Zaměření diplomové práce vyplývá nejen z aktuálních cílů preventivních strategií, ale i z mého dlouhodobého zájmu o kyberkriminalitu. Ve své bakalářské práci na téma Krádež virtuálního majetku, jsem se zaměřovala na věci ve virtuálních světech, respektive herních virtuálních světech, a trestné činy proti nim. Zároveň jsem letos působila jako lektorka prevence kyberkriminality pro základní školy v rámci projektu Praha bezpečně online 2017. Toto zohledňuji především při popisu a hodnocení preventivních přístupů ke konkrétním projevům kyberkriminality.

1 Prevence kriminality a související pojmy

Kriminalita

Kriminalita čili zločinnost je nejzávažnějším sociálně patologickým jevem,[1] tedy závažnou poruchou v chování jedince nebo skupiny projevující se porušováním sociálních a trestněprávních norem.[2] Kriminologie[3] rozlišuje dvě rozsahem odlišná pojetí kriminality, a to užší juristické pojetí kriminality a širší sociologické pojetí. Juristické, nebo také legální, pojetí vnímá kriminalitu shodně s pojetím trestněprávním, a tedy jako souhrn jednání, které zákon *de lege lata* označuje jako trestné. Jde tak o pojem určitý, avšak relativní, jelikož záleží, která jednání jsou v daném čase a v daném právním řádu kriminalizována.[4] Sociologické pojetí pracuje nezávisle na trestním právu, a tedy zahrnuje i jednání, která nejsou ze zákona trestná, ale přesto jsou společensky nežádoucí, či naopak. Tímto může zároveň kriminologie působit na trestní právo *de lege ferenda* návrhem kriminalizace nebo dekriminalizace určitého konání či opomenutí.[5]

Kriminalizace a dekriminalizace

Kriminalizace[6] je prohlášení určitého jednání zákonem za trestné, naopak dekriminalizace[7] je vynětí určitého jednání z kodexu trestných činů. Příčinou těchto legislativních úprav bývá změna názoru na společenskou škodlivost daného jednání, tedy jestli je snížena či zvýšena tolerance porušování určitých společenských a právních norem. Zároveň tento proces souvisí se státní kriminální politikou.

Kriminalita skutečná

Skutečný objem kriminality na určitém území v určitém čase je součtem kriminality registrované a kriminality latentní.

---

[1] ZOUBKOVÁ, Ivana a kol. *Kriminologický slovník*. Plzeň: Aleš Čeněk, 2011. s. 81. ISBN 978-80-7380-312-4.
[2] Tamtéž. s. 164.
[3] Viz níže v této kapitole.
[4] Viz níže v této kapitole.
[5] ZOUBKOVÁ, Ivana a Marcela MOULISOVÁ. Kriminologie pro studenty doktorského studijního programu. Praha: PA ČR, 2014. s. 13. ISBN 978-80-7251-409-0.
[6] ZOUBKOVÁ, Ivana a kol. *Kriminologický slovník*. Plzeň: Aleš Čeněk, 2011. s. 88. ISBN 978-80-7380-312-4.
[7] Tamtéž. s. 38.

Kriminalita registrovaná

Registrovaná kriminalita je evidována orgány činnými v trestním řízení a zaznamenávána v rámci statistik

Kriminalita latentní

Latentní kriminalita, je ta kriminalita, o které se orgány činné v trestním řízení nedozvěděly, respektive jim nebyla oznámena. Jedná se o temná čísla kriminality. V širším smyslu sem můžeme zařadit i šedá čísla kriminality, která odpovídají registrované kriminalitě, u které se nepodařilo najít pachatele. Poslední složkou je latence umělá, a tedy kriminalita, o které se orgány činné v trestním řízení dozvěděly, ale neregistrovaly ji.[8]

Kriminogenní faktory

Kriminogenní faktory, zjednodušeně příčiny kriminality, jsou okolnosti usnadňující vznik, rozšiřování nebo trvání kriminality a sociální jevy vytvářející vhodné prostředí a podmínky pro kriminalitu. Rizikové faktory obvykle souvisejí s individuálními dispozicemi jednotlivců i s funkčností normativního, tedy nejen legislativního, systému.[9]

Recidiva

Recidivou zpravidla myslíme opakování trestného činu stejným pachatelem.

- recidiva kriminologická – opětovně spáchal TČ (i latentní)
- recidiva trestněprávní – opětovně spáchal TČ poté, co byl pachatel odsouzen
- recidiva penologická – opětovně spáchal TČ poté, co vykonal trest odnětí svobody
- recidiva viktimologická – opětovné spáchání TČ na stejné oběti (i jiným pachatelem)

Kriminologie

Kriminologie je multidisciplinární naukou, která zkoumá kriminalitu jako sociálně patologický fenomén. V rámci kriminálních věd je nejobecnější a své poznatky čerpá například ze sociologie, psychologie, psychiatrie, kriminalistiky, pedagogiky, trestního práva, statistiky

[8] ZOUBKOVÁ, Ivana a kol. *Kriminologický slovník*. Plzeň: Aleš Čeněk, 2011. s. 83. ISBN 978-80-7380-312-4.
[9] Tamtéž. s. 92-93.

a dalších oborů. Výstupy kriminologických výzkumů mají sloužit především zákonodárným a justičním orgánům, případně orgánům sociální kontroly.[10]

Viktimologie

Viktimologie je kriminologickou vědou, zabývající se obětí trestného činu, jejími vlastnostmi a její rolí v průběhu trestného činu i v průběhu následného trestního řízení.

Penologie

Penologie je kriminologickou vědou, zabývající se pachatelem trestného činu ve výkonu trestu, účinností jednotlivých druhů trestu, možnostmi alternativních trestů a mimo jiné penitenciárním a postpenitenciárním působením na pachatele.

Kontrola kriminality

Kontrolou kriminality znamená ovlivňování kriminality, a tedy snižování kvantity kriminality, respektive zastavení růstu kriminality nebo podpora jejího klesání, a snižování kvality ve smyslu škodlivosti kriminality se zaměřením na eliminaci závažných forem kriminality, zejména násilné, mravnostní a hospodářské.[11] Složkami kontroly kriminality jsou represivní strategie, založené na odstrašujícím účinku hrozby sankcí, a preventivní strategie plnící cíle preventivní politiky.

Preventivní politika

Preventivní politika patří vedle trestní politiky do kriminální politiky, která je dílčí součástí politiky bezpečnostní. Preventivní politika směřuje do budoucnosti a představuje ofenzivní strategii kontroly kriminality, tedy spoléhá především na nerepresivní prostředky. Zabývá se systematický snižováním výskytů kriminality.[12]

[10] ZOUBKOVÁ, Ivana a Marcela MOULISOVÁ. Kriminologie pro studenty doktorského studijního programu. Praha: PA ČR, 2014. ISBN 978-80-7251-409-0.
[11] Tamtéž. s. 31.
[12] GJURIČOVÁ, Jitka. O prevenci kriminality. Prevence kriminality [online]. [cit. 12.12.2017]. Dostupné z: http://www.prevencekriminality.cz/prevence-kriminality/teoreticky-uvod/

2 Teoretická systematizace prevence kriminality

Z hlediska strategie dělíme prevenci kriminality na přímou, cílící bezprostředně proti kriminalitě, a nepřímou, zaměřenou na zkvalitnění životních podmínek. Podle obsahu rozlišujeme prevenci sociální, situační a viktimologickou. Podle adresátů stupňujeme prevenci primární, sekundární a terciární. Z hlediska preventivního působení represe rozlišujeme prevenci individuální a generální. V souvislosti s předchozí klasifikací dělíme prevenci na pozitivní, upravenou pravidly a normami, a negativní, spoléhající na hrozbu sankcí. Z časového hlediska či vývojového stadia trestné činnosti rozlišujeme prevenci predeliktní a postdeliktní, bránící recidivě. Preventivní opatření rozeznáváme organizační (institucionální), technická, personální, výchovná a dle použitých prostředků je dělíme na právní a mimoprávní.[13]

2.1 Struktura prevence kriminality

Struktura prevence kriminality je klasifikací podle obsahu, respektive podle cílového objektu – pachatel, situace, oběť. Podle těchto kritérií se prevence dělí na sociální, situační a viktimologickou.[14]

2.1.1 Sociální prevence kriminality

Sociální prevence se zaměřuje na sociální příčiny kriminality, zahrnuje aktivity ovlivňující proces socializace a sociální integrace jedince a projekty zaměřené na změnu nepříznivých společenských podmínek.[15] Sociální prevence je tedy orientovaná na osobu pachatele, z hlediska jeho začlenění do společnosti, a na změnu negativních jevů ve společnosti, které jsou příčinami kriminality. Mezi sociální kriminogenní faktory řadíme prostituci, alkoholismus a jiné toxikomanie a závislosti, nezaměstnanost, chudobu, záškoláctví a negramotnost, extremismus, bezdomovectví, deformaci hodnot a morálky, působení médií ve vztahu k agresivitě a

[13] Srov. ZAPLETAL, Josef. *Prevence kriminality*. 3., přeprac. vyd. Praha: PA ČR, 2008. s. 9-11. ISBN 978-80-7251-270-6.
SVATOŠ, Roman. *Prevence kriminality*. 2., aktualiz. vyd. České Budějovice: Vysoká škola evropských a regionálních studií, z.ú., 2016. s. 31-32. ISBN 978-80-7556-009-4.

[14] Viz Příloha č. 1 – Trojúhelník analýzy kriminality.

[15] GJURIČOVÁ, Jitka. O prevenci kriminality. Prevence kriminality [online]. [cit. 12.12.2017]. Dostupné z: http://www.prevencekriminality.cz/prevence-kriminality/teoreticky-uvod/

negativním hrdinům, nedostatečné sociální služby nebo nevyhovující preventivní a výchovné působení na mladistvé.

Z hlediska sociální prevence má klíčový význam zaměření na rodinu, jelikož právě s ní souvisí další faktory jako životní styl, bydlení a zaměstnanost. Přestože je těžké do tak intimního prostředí proniknout, je nutné najít vhodná opatření v oblasti poradenství, rodičovství a manželství, aby rodina dokázala plnit výchovnou, emocionální, ochrannou a ekonomickou funkci. Dalším krokem je prevence v rámci školství, kde by měly být zaznamenány a řešeny případné nedostatky výchovného působení v rodině, a zároveň by mělo být předcházeno negativním jevům typickým pro školní kolektiv, jako šikana nebo záškoláctví. U dětí a mladistvých by také neměl být opomíjen význam vhodných volnočasových aktivit.[16]

Primární sociální prevence by tedy měla být realizována v působnosti rodiny, obce a škol. S ohledem na odbornou náročnost aktivit náleží sekundární a terciární prevence do působnosti odborných pracovníků resortu Ministerstva práce a sociálních věcí a v některých souvislostech i Ministerstva spravedlnosti a Ministerstva zdravotnictví.[17] Opatření sociální prevence z významné části spadají do sociální politiky, a tedy omezení kriminality není jejich výslovným cílem, proto se jedná o nepřímou strategii prevence kriminality.[18]

2.1.2 Situační prevence kriminality

Situační prevence vychází ze zkušenosti, že se určité druhy kriminality objevují v určité době, na určitých místech a za určitých okolností.[19] Strategie situační prevence se proto zaměřují na zvyšování námahy a rizika spojených s páchání trestné činnosti a na snižování užitků plynoucích z trestné činnosti.[20]

---

[16] Srov. SVATOŠ, Roman. *Prevence kriminality*. 2., aktualiz. vyd. České Budějovice: Vysoká škola evropských a regionálních studií, z.ú., 2016. s. 23-24. ISBN 978-80-7556-009-4.

[17] GJURIČOVÁ, Jitka. O prevenci kriminality. Prevence kriminality [online]. [cit. 12.12.2017]. Dostupné z: http://www.prevencekriminality.cz/prevence-kriminality/teoreticky-uvod/

[18] ZAPLETAL, Josef. *Prevence kriminality*. 3., přeprac. vyd. Praha: PA ČR, 2008. s. 13. ISBN 978-80-7251-270-6.

[19] GJURIČOVÁ, Jitka. O prevenci kriminality. Prevence kriminality [online]. [cit. 12.12.2017]. Dostupné z: http://www.prevencekriminality.cz/prevence-kriminality/teoreticky-uvod/

[20] GRAHAM, John a Trevor BENNETT. Strategie prevence kriminality v Evropě a Severní Americe. Praha : Institut pro kriminologii a sociální prevenci, 1996. ISBN 80-86008-23-1. Převzato z: ZAPLETAL, Josef. *Prevence kriminality*. 3., přeprac. vyd. Praha: PA ČR, 2008. s. 18 an. ISBN 978-80-7251-270-6.

Zvýšení námahy spojené s pácháním trestné činnosti lze dosáhnout ztížením dosažení cíle, a to zajištěním či zvýšením bezpečnosti jednotlivých objektů, vypracováním statistických přehledů o bezpečnosti a identifikací nedostatků, vydáváním projekčních a stavebních bezpečnostních standardů, nebo formou veřejných propagačních kampaní a pojišťovacích stimulů. Dále lze potřebnou námahu zvýšit kontrolou přístupů do určitých oblastí, respektive s tím souvisejícím odkloněním pachatelů, a konečně omezením a kontrolou prostředků, které mohou sloužit k trestné činnosti. Zvýšení rizika, kterému se pachatel vystavuje pří páchání trestného činu, souvisí s dohledem. Ať již jde o dohled formální, prováděný policií nebo soukromými bezpečnostními službami, dohled prováděný zaměstnanci, či přirozený dohled občany při každodenních činnostech. Snížení užitku plynoucího z trestné činnosti je možno dosáhnout odstraněním cíle či jeho přemístěním do bezpečnější lokality, označením věcí pro snazší identifikaci, odstraněním lákadel z viditelných míst a stanovením přísnějších pravidel chování na dotčených místech.[21]

Nástrojem zvyšujícím efektivitu situační prevence kriminality mohou být mapy kriminality. Příkladem mohou být Mapy budoucnosti – moderní nástroj ke zvýšení efektivity a kvality výkonu veřejné správy v oblasti prevence kriminality založený na analýze a predikci kriminality[22] nebo, pro veřejnost určená, Mapa kriminality.[23] Vzhledem k tomu, že se situační prevence zaměřuje na konkrétní okolnosti kriminality, jedná se o přímou strategii prevence kriminality.[24] Sociální a situační přístupy se na jednotlivých úrovních prevence vzájemně doplňují.

2.1.3 Viktimologická prevence kriminality

Viktimologická prevence je založena na konceptech bezpečného chování, přizpůsobeného na různé kriminální situace, a na psychické připravenosti ohrožených osob na jednotlivá rizika.

---

[21] ZAPLETAL, Josef. *Prevence kriminality*. 3., přeprac. vyd. Praha: PA ČR, 2008. s. 18-22. ISBN 978-80-7251-270-6.

[22] Mapy budoucnosti. *Prevence kriminality* [online]. [cit. 12.12.2017]. Dostupné z: http://www.prevencekriminality.cz/projekty/mapy-budoucnosti/

[23] Mapa kriminality [online]. [cit. 12.12.2017]. Dostupné z: http://www.mapakriminality.cz/ a http://www.czechcrime.org

[24] ZAPLETAL, Josef. *Prevence kriminality*. 3., přeprac. vyd. Praha: PA ČR, 2008. s. 17. ISBN 978-80-7251-270-6.

Tento přístup využívá poznatků viktimologie k sestavení strategií a metodik prevence. Viktimologická prevence se potom zaměřuje především na informační, osvětovou a poradenskou činnost směřovanou na jedince i skupiny. V praxi se setkáme se zdravotním, psychologickým a právním poradenstvím, tréninky v obranných strategiích, například i kurzy sebeobrany, a propagací technických možností ochrany.[25]

Specifické aktivity a metodiky cílí na osoby s vysokou mírou viktimnosti. Rizikovými skupinami jsou například senioři, děti, osoby s postižením, bezdomovci, cizinci, příslušníci menšiny, v závislosti na situaci ženy nebo naopak muži, a s ohledem na profesi například policisté, sociální pracovníci, lékaři, prodavači, bankovní úředníci, hlídači, dopravci, taxikáři, prostitutky.[26] Viktimologická prevence používá metody sociální i situační prevence, a navíc zahrnuje oblast pomoci obětem trestných činů.

2.2 Úrovně prevence kriminality

Prevence kriminality se z hlediska šíře a specializace okruhu adresátů příslušných opatření dělí na primární, sekundární a terciární. Méně výstižným a také méně používaným označením této klasifikace je dělení podle vývojového stádia kriminálního problému.[27] Společně s klasifikací podle obsahu vytvářejí kostru systému preventivních opatřeních.[28]

2.2.1 Primární prevence kriminality

Primární prevence se věnuje veškerému obyvatelstvu, respektive geograficky nebo demograficky skupinám. Působí plošně v dané skupině bez ohledu na míru viktimnosti či rizikovosti jedince.[29] Zvláštní pozornost věnuje pozitivnímu ovlivňování příslušných hodnotových měřítek zejména dětí a mládeže. Primární prevence zahrnuje především výchovné,

[25] GJURIČOVÁ, Jitka. O prevenci kriminality. Prevence kriminality [online]. [cit. 12.12.2017]. Dostupné z: http://www.prevencekriminality.cz/prevence-kriminality/teoreticky-uvod/

[26] Srov. GŘIVNA, Tomáš, Miroslav SCHEINOST a Ivana ZOUBKOVÁ. *Kriminologie*. 4., aktualiz. vyd. Praha: Wolters Kluwer, 2014. s. 115. ISBN 978-80-7478-614-3.

[27] ZAPLETAL, Josef. *Prevence kriminality*. 3., přeprac. vyd. Praha: PA ČR, 2008. s. 25. ISBN 978-80-7251-270-6.

[28] Viz Příloha č. 2 – Schéma prevence kriminality.

[29] GŘIVNA, Tomáš, Miroslav SCHEINOST a Ivana ZOUBKOVÁ. *Kriminologie*. 4., aktualiz. vyd. Praha: Wolters Kluwer, 2014. s. 160. ISBN 978-80-7478-614-3.

vzdělávací, volnočasové, osvětové a poradenské aktivity.[30] Respektive mívá charakter nepřímé strategie ovlivňující hospodářskou, sociální, kulturní a právní politiku.[31]

Z toho vyplývá, že primární prevence má nejširší uplatnění v prevenci sociální, kdy se zaměřuje na osvětu, výchovu, vzdělání nebo zaměstnanost. Primární situační prevence se zaměřuje především na fyzické faktory bezpečnosti, jedná se tedy například o architektonické plánování, pouliční osvětlení, střežení objektů nebo limity hotovostních plateb. Viktimologická prevence na primární úrovni spočívá v systematické informační kampani určené pro veřejnost na celém území státu. K takové kampani by se mohla využít masmédia, a to zvláště pokud jde o obecná témata jako zajištění osobní bezpečnosti nebo ochrana majetku.[32]

Současnými tuzemskými koncepcemi primární strategie jsou například Národní strategii primární prevence rizikového chování dětí a mládeže na období 2013–2018,[33] Metodika pro poskytování dotací ze státního rozpočtu na realizaci aktivit v oblasti prevence rizikového chování v období 2013–2018,[34] Zdraví 2020 – Národní strategie ochrany a podpory zdraví a prevence nemocí,[35] a také jsou vypracovány standardy specifické primární prevence pro jednotlivé oblasti rizikového chování.[36]

2.2.2 Sekundární prevence kriminality

Sekundární prevence se zabývá rizikovými jedinci a skupinami osob, úžeji vymezenými podle věku, druhu ohrožení nebo lokality, u nichž je zvýšená pravděpodobnost, že se stanou pachateli nebo oběťmi trestné činnosti, dále sociálně patologickými jevy, jako jsou drogové a

[30] GJURIČOVÁ, Jitka. O prevenci kriminality. Prevence kriminality [online]. [cit. 12.12.2017]. Dostupné z: http://www.prevencekriminality.cz/prevence-kriminality/teoreticky-uvod/

[31] GŘIVNA, Tomáš, Miroslav SCHEINOST a Ivana ZOUBKOVÁ. *Kriminologie*. 4., aktualiz. vyd. Praha: Wolters Kluwer, 2014. s. 160. ISBN 978-80-7478-614-3.

[32] ZAPLETAL, Josef. *Prevence kriminality*. 3., přeprac. vyd. Praha: PA ČR, 2008. s. 25-26. ISBN 978-80-7251-270-6.

[33] *Národní strategii primární prevence rizikového chování dětí a mládeže na období 2013–2018* [online]. [cit. 12.12.2017]. Dostupné z: http://www.msmt.cz/file/28077

[34] *Metodika pro poskytování dotací ze státního rozpočtu na realizaci aktivit v oblasti prevence rizikového chování v období 2013–2018* [online]. [cit. 12.12.2017]. Dostupné z: http://www.msmt.cz/vzdelavani/socialni-programy/dotacni-program-pro-oblast-prevence-2013-2018

[35] *Zdraví 2020 – Národní strategie ochrany a podpory zdraví a prevence nemocí* [online]. [cit. 12.12.2017]. Dostupné z: https://www.mzcr.cz/Verejne/dokumenty/zdravi-2020-narodni-strategie-ochrany-a-podpory-zdravi-a-prevence-nemoci_8690_3016_5.html

[36] strategie s. 38

alkoholové závislosti, šikana, sprejerství, gamblerství, výtržnictví, vandalismus, rasismus či xenofobie.[37] Jedná se tedy o přímou strategii cílící na potenciální pachatele, potenciální oběti a kriminogenní situace. Předpokladem pro efektivní působení sekundární prevence je včasné rozpoznání a prognózování problémů, jelikož samotnému výkonu prevence zpravidla předchází metodika školení pracovníků, kteří budou s rizikovými skupinami v kontaktu.

Sekundární sociální prevence spočívá ve specializovaných aktivitách sociální péče, vykonávaných prostřednictvím výchovných poradců ve školách, sociálních pracovníků, protidrogových koordinátorů, linek důvěry a poraden. Sekundární situační prevence vyhledává rizikové lokality, a snaží se na ně reagovat rozšiřováním bezpečnostních nástrojů. Sekundární viktimologická prevence zkoumá míry viktimizace jednotlivých skupin společnosti, a zaměřuje se na ty nejrizikovější skupiny a jednotlivce tak, že je informuje, která rizika jsou pro ně relevantní a jak je zmírnit.[38]

2.2.3 Terciární prevence kriminality

Terciární prevence je prevencí přímou postdeliktní, jedná se totiž o prevenci recidivy u konkrétních osob nebo prevenci opakovaného výskytu trestné činnosti v konkrétních lokalitách. Orientuje se na předcházení kriminální recidivě u pachatele a viktimologické recidivě oběti.[39] Terciární prevence kriminality čerpá poznatky ze statistik, a především ze závěrů penologie a viktimologie.

Sociální prevence na terciární úrovni spočívá především v resocializaci kriminálně narušených osob v rámci penitenciární a postpenitenciární péče nebo prostřednictvím sociálního a rodinného poradenství a pomoci při získávání sociální, sociologické a ekonomické samostatnosti.[40] U viktimologické prevence jde i o předcházení sekundární viktimizaci v rámci

[37] GJURIČOVÁ, Jitka. O prevenci kriminality. Prevence kriminality [online]. [cit. 12.12.2017]. Dostupné z: http://www.prevencekriminality.cz/prevence-kriminality/teoreticky-uvod/

[38] ZAPLETAL, Josef. *Prevence kriminality*. 3., přeprac. vyd. Praha: PA ČR, 2008. s. 26. ISBN 978-80-7251-270-6.

[39] GŘIVNA, Tomáš, Miroslav SCHEINOST a Ivana ZOUBKOVÁ. *Kriminologie*. 4., aktualiz. vyd. Praha: Wolters Kluwer, 2014. s. 162. ISBN 978-80-7478-614-3.

[40] GJURIČOVÁ, Jitka. O prevenci kriminality. Prevence kriminality [online]. [cit. 12.12.2017]. Dostupné z: http://www.prevencekriminality.cz/prevence-kriminality/teoreticky-uvod/

vyšetřování, o napravení následků trestného činu a o poskytnutí potřebné pomoci.[41] Terciární situační prevence se specializuje na lokality a případně komunity, které jsou zasaženy vysokou kriminalitou určitého druhu.[42]

[41] GŘIVNA, Tomáš, Miroslav SCHEINOST a Ivana ZOUBKOVÁ. *Kriminologie*. 4., aktualiz. vyd. Praha: Wolters Kluwer, 2014. s. 162. ISBN 978-80-7478-614-3.

[42] ZAPLETAL, Josef. *Prevence kriminality*. 3., přeprac. vyd. Praha: PA ČR, 2008. s. 27. ISBN 978-80-7251-270-6.

3 Současné zaměření prevence kriminality

Tato kapitola se bude věnovat strategickým a metodickým materiálům zakotvujícím současné cíle a zájmové oblasti prevence kriminality.

3.1 Kongres OSN v Dauhá

Deklarace z Dauhá, o začlenění prevence kriminality a trestní justice do širší agendy OSN s cílem zaměřit se na sociální a ekonomické výzvy a prosazovat zákonnost na národní i mezinárodní úrovni a participaci veřejnosti, byla schválena aklamací 13. Kongresem OSN o prevenci kriminality a trestní justici, který se konal v katarském Dauhá 12.–19. dubna 2015.

3.1.1 Deklarace z Dauhá

Deklarace připomíná, že OSN uznalo závazky členských států hájit lidská práva a základní svobody, a zdůrazňuje zaručení těchto práv a svobod především pro ty, jenž byli postiženi kriminalitou, nebo jsou zranitelnými členy společnosti, kteří mohou být vystaveni závažným formám diskriminace, a tedy dovozuje nutnost zamezovat kriminalitě, včetně té vyplývající z netolerance.[43] Přijetím deklarace se členové OSN zavázali mimo jiné:

- usilovat o přijetí komplexních a inkluzivních národních programů a projektů v oblasti prevence kriminality a trestní justice, zohledňujících prvotní příčiny kriminality i podmínky umožňující nebo usnadňující její vznik a rozvoj;[44]
- zaměřit se na problematiku dětí a mládeže, a to především na význam ochrany dětí před všemi formami násilí, vykořisťování a zneužívání, v souladu s relevantními mezinárodními dokumenty včetně Úmluvy o právech dítěte, či Modelových strategií a praktických opatření OSN pro odstranění násilí na dětech v oblasti prevence kriminality a trestní justice;
- posilovat rovnost před zákonem vedoucí k potlačení diskriminace a nesnášenlivosti, a zároveň respektovat genderová specifika zejména v oblasti prevence kriminality a zacházení s pachatelem;[45]

[43] Deklarace z Dauhá. čl. 5.
[44] Tamtéž. čl. 5. písm. a.
[45] Tamtéž. čl. 5. písm. f, g, p, q, r.

- rozvíjet programy pro vězněné související s prevencí recidivy, a tedy se zaměřením na resocializaci, reintegraci, vzdělání a práci. Zároveň přezkoumat trestní politiku s ohledem na řešení otázky přeplněnosti věznic a podpory využívání alternativních trestů.[46]

Deklarace zdůrazňuje významný podíl vzdělání mládeže, včetně vymýcení negramotnosti, na prevenci kriminality. Za cíl si klade vytvářet ve školách bezpečné výukové prostředí, a to ochranou dětí před obtěžováním, šikanou, sexuálním zneužíváním, zneužíváním drog, či jinými formami násilí. Dále začlenit prevenci kriminality nejen do vzdělávacího systému, ale i do ekonomických a sociálních strategií, s čímž souvisí rozšiřování vzdělávacích a pracovních příležitostí pro děti a mladé dospělé i podpora celoživotního vzdělávání.[47]

Deklarací byla uznána zodpovědnost za adekvátní reakci na vznikající a vyvíjející se hrozby a nové formy trestné činnosti, vyplývající z technologického, sociálního a ekonomického pokroku. Deklarace považuje za nutné realizovat komplexní postupy v oblasti prevence kriminality a trestní justice, případně přijmout legislativní a administrativní opatření na národní a mezinárodní úrovni reagující na nové formy kriminality. S tím souvisí vytvoření bezpečného a odolného kyberprostředí, a tedy:

- bránění kriminálním aktivitám realizovaným v kyberprostoru (se zaměřením na krádeže identit, obchodování s lidmi a ochranu dětí před zneužíváním online);
- posílení spolupráce na národní a mezinárodní úrovni (s cílem identifikovat a chránit oběti, například i odstraňováním materiálu zobrazujícího sexuální zneužívání dětí);
- vylepšení zabezpečení počítačových sítí;
- poskytování technické pomoci a rozvíjení schopností státních úřadů postupovat proti kyberkriminalitě (zajištění odbornosti, technické kapacity, vzájemné spolupráce a součinnosti, finanční podpory).

Zároveň deklarace vyzývá Komisi pro prevenci kriminality a trestní justici, aby pověřila otevřenou mezivládní expertní skupinu výměnou informací o národních legislativách,

[46] Deklarace z Dauhá. čl. 5. písm. j, h.
[47] Tamtéž. čl. 7.

osvědčených postupech, technické pomoci a mezinárodní spolupráci, za posílení současných postupů a návrhu nových národních a mezinárodních strategií pro potírání kyberkriminality.[48]

Deklarace se dále zaměřuje na konzultativní a participativní procesy v prevenci, s cílem zapojit všechny členy společnosti včetně těch, kteří jsou vystaveni riziku viktimizace. Na vývoji i realizaci strategií by se měla podílet občanská společnost, soukromý sektor, akademická sféra i média. Mělo by se zacílit na zhodnocení potenciálu informačních a komunikačních technologií, zlepšování systémů e-government, prosazování nových technologií v rámci community policing,[49] posilování spolupráce se soukromou sférou, zajištění veřejné dostupnosti legislativy. Také by se měla rozvíjet opatření, která povedou veřejnost a zvláště oběti, k nahlašování trestné činnosti, vytvářet postupy na ochranu oznamovatelů a svědků trestné činnosti, podporovat komunitní iniciativy, vybízet soukromý sektor k aktivnímu zapojení do programů sociálního začleňování a vytvářet kapacity pro výzkumy v oblasti kriminologie i forenzních a penologických věd.[50]

3.1.2 Nové formy nadnárodního zločinu

Podpůrný dokument pro Kongres OSN v Dauhá na téma komplexní a vyvážené přístupy k prevenci a adekvátnímu řešení nových a vznikajících forem nadnárodního zločinu se věnuje těmto formám kriminality: pirátství, kyberkriminalita, sexuální zneužívání dětí, trestná činnost proti životnímu prostředí a obchodování s kulturními statky. Přičemž prevence a potírání nových a vznikajících forem trestné činnosti i předvídání vývoje kriminality je poměrně náročný úkol. Hnací faktory, jako tempo technologického vývoje a postupující globalizace, vytvořily nové hodnoty, umožnily vznik nových vazeb mezi potenciálními oběťmi a pachateli, a prostředky anonymizace snížily riziko odhalení. Výsledkem není pouze zrod nových forem trestné činnosti, ale i renesance historických forem kriminality, například moderní pirátství.[51]

[48] Deklarace z Dauhá. čl. 9.
[49] Blíže viz kap. 4.4.
[50] Deklarace z Dauhá. čl. 10.
[51] Komplexní a vyvážené přístupy k prevenci a adekvátnímu řešení nových a vznikajících forem nadnárodního zločinu. čl. 1-2.

V tomto kontextu se v materiálech OSN setkáme s následujícími termíny, přičemž tento dokument pracuje právě s posledním z nich:

- *new dimensions of criminality* – nové dimenze kriminality,
- *emerging policy issues* – vznikající strategická témata,
- *new forms and dimensions of transnational organized crime* – nové formy a dimenze nadnárodního organizovaného zločinu,
- *new and emerging forms of crime* – nové a vznikající formy trestné činnosti.[52]

Nové typy kriminality jsou často zastřešujícími pojmy pro řadu specifických trestných činů, jako je tomu typicky v případě kyberkriminality.[53] Navíc se tyto typy kriminality nemusejí projevovat ve více státech homogenně a mohou zpočátku vzbuzovat dojem, že jde pouze o vnitrostátní problém, kdy teprve následně nabydou nadnárodního významu, typicky obchodování s kulturními statky. A konečně, nové formy kriminality se zaměřují na nové typy obětí, s čímž přichází nové výzvy tyto skupiny obětí identifikovat.[54]

Kořeny a hnací faktory

I když jsou výše zmíněné vyvíjející se formy kriminality navzájem odlišné, lze identifikovat řadu společných vývojových trendů, respektive socioekonomických faktorů, které jsou kořeny a hnacími faktory rozvíjející se kriminality. Jedná se o globalizaci, blízkost chudoby, násilné konflikty, slabou legislativu v oblasti cenných trhů, a zejména pokrok na poli technologie a globální konektivity.[55]

Globalizace s moderními technologiemi propojuje nejen národní ekonomiky, ale umožňuje integraci poznatků, včetně informačních, kulturních, ideologických a technologických toků. Existence kyberprostoru[56] s sebou přináší nové možnosti seberealizace, a to i v negativním kontextu. Jménem své kyberidentity, podníceni anonymitou a nedostatečným odstrašením,

[52] Komplexní a vyvážené přístupy k prevenci a adekvátnímu řešení nových a vznikajících forem nadnárodního zločinu. čl. 8.
[53] Viz kap. 5.
[54] Komplexní a vyvážené přístupy k prevenci a adekvátnímu řešení nových a vznikajících forem nadnárodního zločinu. čl. 8-11.
[55] Tamtéž. čl. 12.
[56] Viz kap. 5.

mohou lidé páchat trestné činy, kterých by se v reálném světě nedopustili s ohledem na svůj společenský status a postavení. Zároveň globální konektivita zjednodušuje vznik kriminálních spojenectví, od nelegálních tržišť, přes verbování teroristických skupin a podněcování k násilí, po pedofilní online komunity. A například vysoká míra anonymity na darknetu[57] a jeho tržištích s nelegálním zbožím, platba virtuální měnou a dodání zboží do úschovné schránky, značně ztěžuje orgánům činným v trestním řízení identifikaci pachatele.[58]

Nové způsoby fungování

Vyvíjející se trestnou činnost lze charakterizovat specifickými způsoby fungování. Setkáváme se se změnami ve struktuře organizovaných zločineckých skupin, posilováním vazeb mezi kriminálními operacemi, či využitím korupce pro usnadnění trestné činnosti. Současné technické prostředky, zejména tedy internet, umožňují rozšíření spolupráce bez geografického omezení. Většinou se nejedná o kompletně organizovanou zločineckou skupinu, častěji jde o sociální síť zprostředkovávající kooperaci uživatelů s různým profesionálně kriminálním zaměřením (programátoři, hackeři, účetní, kurýři). Zároveň není neobvyklé, že si klasická zločinecká skupina najme na specializovanou činnost, často technického rázu, odborníka přes internetová tržiště služeb.[59]

Při zachování současného trendu můžeme předpokládat, že v budoucnu bude klasická kriminalita čím dál tím víc propojena s technologiemi a provázána s kyberprostorem. Příkladem může být fyzické pašování drog zastírané technologiemi, kdy za pomocí mallwaru[60] infiltrovaného do počítačového systému jednoho evropského přístavu byly zastírány nezákonné aktivity zločinecké skupiny.[61]

[57] Viz kap. 5.

[58] Komplexní a vyvážené přístupy k prevenci a adekvátnímu řešení nových a vznikajících forem nadnárodního zločinu. čl. 22-29.

[59] Tamtéž. čl. 30, 32-34.

[60] Viz kap. 5.1.

[61] Komplexní a vyvážené přístupy k prevenci a adekvátnímu řešení nových a vznikajících forem nadnárodního zločinu. čl. 35.

Komplexní a vyvážené reakce

Mají-li metodiky adekvátně reagovat a předcházet vznikajícím formám trestné činnosti, musejí být komplexní, tedy se mají zaměřovat na všechny formy nové kriminality a vycházet z výše uvedených kořenů, hnacích faktorů a způsobů fungování, i vyvážené, tak že se prevence kriminality a vyšetřovací a trestní opatření budou uplatňovat současně, se souběžnou mobilizací úsilí a zdrojů širší skupiny aktérů, včetně soukromých podniků, občanské společnosti, akademické sféry a obětí. Zároveň se tyto požadavky netýkají jen reakcí na národní úrovni, ale také mezinárodních reakcí a budování kapacit.[62]

Přeměna hnacích faktorů vznikajících forem trestné činnosti na nové reakce

Kořeny a hnací faktory nových forem kriminality, mohou být zároveň využity k prevenci a potírání těchto trestných činů. Například globalizace nabízí příležitosti pro posílení nadnárodních reakcí v oblasti vymáhání práva a trestní justice. Rychlejší doprava a komunikace by měla vést k usnadnění rozvoje sítí mezinárodní spolupráce orgánů činných v trestním řízení, kdy příkladem mohou být Středoamerická síť státních zástupců proti organizovanému zločinu a Síť západoafrických ústředních orgánů a státních zástupců proti organizovanému zločinu. Podobně nástup nových trhů a posílená tržní konektivita může zároveň vytvářet specifické příležitosti pro intervence, například zavedení či zlepšení statistik o dovozu a vývozu kulturních statků, zavedení mechanismů umožňujících nahlašování podezřelého obchodování nebo prodejů na internetu.[63]

Zároveň pokroky v technologii nabízejí i nové metody vyšetřovatelům. Množství informací sdílených na sociálních sítích a diskuzních fórech, či uložených v koncových zařízeních, které lze při policejních operacích zabavit, vytváří nový zdroj pro kriminální vyšetřování. Nástroje umožňující skrývání identit v kyberprostoru jsou účinná pouze natolik, nakolik je uvědomělý lidský faktor za nimi, a kolik za sebou nechá nevědomých digitálních stop vedoucích k jejich osobě (IP adresa, e-mailová adresa). Orgány činné v trestním řízení také mohou využívat

[62] Komplexní a vyvážené přístupy k prevenci a adekvátnímu řešení nových a vznikajících forem nadnárodního zločinu. čl. 39-42.
[63] Tamtéž. čl, 43-45.

moderní technologie pro zabezpečení sdílení informací, vyspělé techniky zachycování dat včetně například nasazení dronů jako operativně pátracích prostředků.[64]

Inovativní metodologie sběru dat

Účinnost prostředků proti trestné činnosti mimo jiné závisí na důkazech, které jsme schopni shromáždit. Komplexní povaha nových forem trestné činnosti není příliš kompatibilní s tradičními zdroji dat, jakými jsou policejní statistiky. Zároveň vysoká latence nové kriminality vede k tomu, že statistická data nereflektují současné trendy. K získání objektivnějšího náhledu, je tedy nutno kombinovat více různých zdrojů, provádět průzkumy trhu a využívat nové technologie včetně geografických informačních systémů a počítačových zabezpečovacích produktů. Nové informační zdroje budou zahrnovat koncepty monitorování informačních vzorců chování typu velkých dat nebo informačních zplodin. Bezpečnostní software bude moci předpovědět kyberútok, včetně jeho povahy a geografického zdroje. Zároveň je třeba respektovat nadnárodní dosah těchto forem trestné činnosti a vybudovat kapacity sběru dat na mezinárodní úrovni.[65]

Posilování národní legislativy, mezinárodní spolupráce a kapacity orgánů vymáhání práva

Jedním z klíčových bodů při potlačování nových forem kriminality je kriminalizace takového jednání a související legislativní úpravy procesního práva s ohledem na nové technologie, například i jejich využití v rámci vyšetřování, a harmonizace právních systému vzhledem k mezinárodnímu charakteru trestné činnosti. Je tedy nutno buď vytvořit nové trestné činy, nebo výklad či znění těch dosavadních rozšířit o nové formy páchání. Pokud jde o kriminalizaci kyberkriminality, používají se oba přístupy současně, a to formulací nových specifických trestných činů i akceptací možnosti páchat obecnou kriminalitu v rámci kyberprostoru.[66]

[64] Komplexní a vyvážené přístupy k prevenci a adekvátnímu řešení nových a vznikajících forem nadnárodního zločinu. čl, 46.
[65] Tamtéž. čl. 47-50
[66] Blíže viz kap. 5.

Na globální úrovni lze harmonizace ve specifických oblastech dosáhnout mezinárodními smlouvami. Ty však nemusejí vždy zavazovat k výslovné legislativní úpravě všech aspektů daného jevu. Proto při posuzování oboustranné trestnosti vycházíme z podstaty daného jednání, a ne z konkrétních národních termínů či definic. I pokud dosáhneme mezinárodní harmonizace, může se dostat před další překážku. Tak je tomu v oblasti kyberkriminality, například při využívání peer-to-peer systému,[67] kdy nejsme schopni identifkovat konkrétní státy, které by měly v daném případě realizovat mezinárodní spolupráci. Zřejmě tedy bude potřeba inovace konceptu teritoriální suverenity a vzájemné uznávání procesních a zejména vyšetřovacích postupů. Orgány činné v trestním řízení by se pak měly zaměřit na zvyšování forenzní odbornosti v oblasti moderních technologií.[68]

Prevence

Pro prevenci nově vznikajících forem kriminality je klíčová informovanost, nejen mezi potenciálními obětmi, ale i dalšími subjekty jako jsou odborní a pedagogičtí pracovníci. Proto vlády i instituce ze soukromého sektoru informují o indikátorech jednotlivých typů kriminality. U kyberkriminality se setkáváme s doporučeními ohledně uvědomělého chování v kyberprostoru, včetně prostředků ochrany, jakými jsou například silná hesla. Informační kampaň je také vedena vůči potenciálním pachatelům, zejména se jedná o sdělení ohledně kriminalizace určitého jednání se snahou odradit především mladistvé od zapojení se do skupin páchajících trestnou činnost. Jak již bylo zmíněno výše, moderní technologie nejsou pouze hrozbou a prostředkem páchání kriminality, ale mohou a měli by být využívány i u preventivních přístupů, jako je zabezpečování nebo sledování potenciálních cílů trestné činnosti (střežení archeologických nalezišť drony, či identifikační označení a katalogizace rizikových výrobků, jakými jsou například léky).[69]

Další generace vznikajících forem trestné činnosti a globální rozvojová agenda

Lze předpokládat, že procesy globalizace a technologického rozvoje se budou nadále zrychlovat a, v kombinaci s dalšími hnacími faktory, jakými jsou klimatické změny, nedostatek

[67] Viz kap. 5.1.

[68] Komplexní a vyvážené přístupy k prevenci a adekvátnímu řešení nových a vznikajících forem nadnárodního zločinu. čl. 51-59.

[69] Tamtéž. čl. 60-65.

vody, decentralizace hodnot a služeb, nové formy získávání energie, vývoj biotechnologií a bioinženýrství, virtuální měny nebo pokroky v robotice, autonomních systémech a umělé inteligenci, s sebou přinesou další vlnu nových forem kriminality. Zřejmě bude třeba aplikovat regulatorní opatření v souvislosti s prevencí úpravou prostředí[70] s cílem omezit možnosti potenciálního kriminálního zneužití socioekonomických inovací.[71]

Závěry a doporučení

V závěru dokumentu byla shrnuta následující doporučení:

- zajistit tvorbu, realizaci, monitorování strategií;
- zrevidovat zákony s ohledem na nové formy kriminality tak, aby byly dostatečně specifické a umožňovaly flexibilitu;
- zvyšovat národní kapacity pro vymáhání práva;
- optimalizovat a posilovat mezinárodní a regionální spolupráci;
- podporovat prevenci nových forem kriminality, zejména informačními kampaněmi, rozvojem partnerství se soukromým sektorem, sdílením informací a specifickými intervencemi;
- rozvinout výzkumné metody a monitorovací kapacity pro identifikaci možných kořenů, hnacích faktorů a způsobů fungování vznikajících forem trestné činnosti;
- realizovat další výzkumy, analýzy a poskytování technické pomoci;
- využívat odborných poznatků a zajistit spolupráci mezi různými aktéry zapojenými do prevence. [72]

[70] prevention by design

[71] Komplexní a vyvážené přístupy k prevenci a adekvátnímu řešení nových a vznikajících forem nadnárodního zločinu. čl. 69-70.

[72] Tamtéž. čl. 71.

3.1.3 Workshop: prevence kyberkriminality

Výchozí dokument pro workshop č. 3 při kongresu OSN v Dauhá se věnuje posilování reakcí v oblastech prevence kriminality a trestní justice na vznikající formy trestné činnosti, jako je kyberkriminalita a obchodování s kulturními statky, včetně získaných poučení a mezinárodní spolupráce. Cílem tohoto dokumentu je ilustrovat získané poznatky a možné přístupy týkající se mezinárodní spolupráce při prevenci proti obchodování s kulturními statky a při prevenci kyberkriminality.[73] V této kapitole budou shrnuty poznatky tohoto workshopu, které jsou relevantní pro prevenci kyberkriminality.

Kyberkriminalita – identifikace výzvy

Pojem kyberkriminalita zastřešuje kriminální jednání proti počítačovým systémům, nebo s jejich využitím.[74] S rozvojem moderních technologií a rozpínající se globalizací se hranice mezi kyberkriminalitou a klasickou kriminalitou značně rozostřuje. Používání internetu je každodenní rutinou a informace, jako historie prohlížení a vyhledávání, e-mailové a jiné zprávy, i jiný sdílený obsah, se stávají objemným zdrojem elektronických důkazů.[75]

Moderní technologie a rozšíření internetového pokrytí s sebou přináší možnosti ekonomického růstu, vznik nových profesí, přístup k základním službám, jako je vzdělání, zdravotnictví nebo elektronizace veřejné správy. Paralelně s užitečným rozvojem ale došlo i k rozvoji kriminálnímu. Například sociální sítě, které vznikly jako platforma pro virtuální komunity, lze jednoduše zneužívat k obtěžování, šíření nenávistných projevů, výhrůžky, vydírání a jiným kriminálním aktivitám, a to v globálním měřítku a během několika sekund. Zároveň s rozmachem internetu věcí je stále více předmětů, které se mohou stát terčem kyberútoku a případně součástí botnetu.[76]

[73] Workshop 3: Posilování reakcí v oblastech prevence kriminality a trestní justice na vznikající formy trestné činnosti, jako je kyberkriminalita a obchodování s kulturními statky, včetně získaných poučení a mezinárodní spolupráce. čl. 1, 12.

[74] Blíže ke kyberkriminalitě a souvisejícím pojmům viz kap. 5.1.

[75] Workshop 3: Posilování reakcí v oblastech prevence kriminality a trestní justice na vznikající formy trestné činnosti, jako je kyberkriminalita a obchodování s kulturními statky, včetně získaných poučení a mezinárodní spolupráce. čl. 13-16.

[76] Tamtéž. čl. 17-18

V současné době už také neplatí, že internet poskytuje naprostou anonymitu. Uživatelé i orgány činné v trestním řízení si jsou vědomi technických aspektů přenosu dat, a tedy toho, že činností v kyberprostoru vytváříme digitální stopu. S pokrokem digitálních forenzních nástrojů jsou elektronické stopy pro vyšetřovatele stále dostupnější. Ti však musí čelit dalším výzvám v oblasti prostředků zabezpečení dat formou šifrování, nebo anonymizace prostřednictvím přesměrování připojení či decentralizovaného ukládání dat. Typickým příkladem je využívání prostoru darknetu, ideálně prostřednictví služby Tor.[77]

Měření kyberkriminality

Zjišťování počtu případů kyberkriminality nemůžeme přenechat pouze policejním statistikám, zejména pro vysokou latenci mírnějších forem kyberkriminality. Obecně statistiky orgánů činných v trestním řízení nelze beze všeho mezinárodně srovnávat s ohledem na různé statistické metodiky, či odlišné rozčlenění trestných činů. Je tedy nasnadě realizovat průzkumy mezi veřejností, čerpat informace ze zpráv od společností poskytujících zabezpečení, či společností spravujících online hlášení kyberkriminality. Jedním ze zdrojů informací o některých formách kyberkriminality mohou být analýzy kyberkriminálních trhů, fór a sociálních sítí. Nové technologie umožňují sledování i skrytých služeb Tor,[78] což může usnadnit monitorování činností na darknetu. Dalším ztížením určité systematizace je absence jednotného profilu kyberpachatele. Ani nepředpokládáme, že každý kyberútočník je nutně hacker,[79] protože na spoustu forem kyberkriminality postačují uživatelské znalosti.[80]

[77] Workshop 3: Posilování reakcí v oblastech prevence kriminality a trestní justice na vznikající formy trestné činnosti, jako je kyberkriminalita a obchodování s kulturními statky, včetně získaných poučení a mezinárodní spolupráce. čl. 19-20.

[78] SPITTERS, Martijn, Stefan VERBRUGGEN a Mark VAN STAALDUINEN. Towards a comprehensive insight into the thematic organization of the ToR hidden services. Intelligence and Security Informatics Conference (JISIC), 2014. s. 220-223. [online]. ISBN978-1-4799-6364-5. [cit. 5.12.2017]. Dostupné z: http://ieeexplore.ieee.org/document/6975577/

[79] Blíže viz např. TURGEMAN-GOLDSCHMIDT, Orly. Meanings that Hackers Assign to their Being a Hacker. International Journal of Cyber Criminology (IJCC) [online]. 2008, 2(2), 382–396. [cit. 5.12.2017]. ISSN: 0974-2891. Dostupné z: https://pdfs.semanticscholar.org/f40f/32d6b63f9c55460938312946348b977f7f45.pdf

[80] Workshop 3: Posilování reakcí v oblastech prevence kriminality a trestní justice na vznikající formy trestné činnosti, jako je kyberkriminalita a obchodování s kulturními statky, včetně získaných poučení a mezinárodní spolupráce. čl. 21-27.

Prevence a potírání kyberkriminality

Výchozím předpokladem pro přípravu účinných strategií jsou informace o povaze a rozsahu kyberkriminality. Při přípravě preventivních materiálů je třeba dbát na specifika jednotlivých forem kriminality, a tedy informační kampaň o bezpečném internetovém bankovnictví bude obsahovat jiný pohled na rizika internetu než osvětová kampaň v oblasti ochrany dětí v kyberprostoru. Informace o nových formách kriminality jsou podstatné také při přípravě vhodných a účelných vyšetřovacích reakcí.[81]

Jak již bylo zmíněno, je nutné zakotvit legislativní rámec kriminalizace kyberkriminality, včetně procesních pravomocí orgánů činných v trestním řízení, a vytvořit a využívat kapacity forenzní informatiky. Dále je vhodné posilovat mechanismy mezinárodní spolupráce na poli trestního práva a prevence kriminality. Jedním z nástrojů pro usnadnění nadnárodní spolupráce je online UNODC repozitář pro kyberkriminalitu který obsahuje relevantní strategické materiály jednotlivých zemí.[82] Současnými výzvami mezinárodní spolupráce jsou cloudcomputing a peer-to-peer sdílení.[83] Tyto metody sdílení a ukládání dat jsou specifické tím, že data obvykle existují v mnoha kopiích a mohou se nacházet na mnoha místech v mnoha státech současně a zároveň se mohou během prakticky nepatrného časového intervalu přesunout na místa jiná. Provozovatelé datových úložišť mají obvykle zákonem uloženou povinnost po určitou dobu archivovat kopie dat a spolupracovat s orgány činnými v trestním řízení např. při podání vysvětlení. Problém nastává, když se takový provozovatel nachází mimo jurisdikci, ve které řízení probíhá, a administrativní lhůty pro mezinárodní spolupráci jsou delší než povinné archivační doby. U fyzických osob je možno postupovat v režimu zajištění věci.[84]

Nejen proto by se do i mezinárodní spolupráce měl zapojit soukromý sektor, tedy poskytovatelé internetových služeb. Ti mohou preventivně působit na své koncové uživatele, zabezpečit přístupy, blokovat škodlivý obsah a zároveň mohou uchovávat záznamy relevantní

[81] Workshop 3: Posilování reakcí v oblastech prevence kriminality a trestní justice na vznikající formy trestné činnosti, jako je kyberkriminalita a obchodování s kulturními statky, včetně získaných poučení a mezinárodní spolupráce. čl. 28

[82] Blíže viz kap. 5.2.4.

[83] Viz kap. 5.1.

[84] Workshop 3: Posilování reakcí v oblastech prevence kriminality a trestní justice na vznikající formy trestné činnosti, jako je kyberkriminalita a obchodování s kulturními statky, včetně získaných poučení a mezinárodní spolupráce. čl. 29-33.

pro trestní řízení. Samozřejmostí je potom podpora zvyšování úrovně forenzních metod a nástrojů pro vyhodnocování například takto získaných digitálních důkazů, a systematické rozšiřování personálních kapacit v oblasti moderních technologií.[85]

Závěry a doporučení

Pro formulaci účinných reakcí je nezbytné předjímat budoucí vývoj kyberkriminality, a tedy začít systematickým výzkumem a sestavením aktuálních statistik a dodržovat globální konsenzus.[86] Tento dokument k oblasti kyberkriminality shrnuje následující opatření:

- posílit národní kapacity pro zaznamenávání trestné činnosti a vyměňovat si relevantní informace na regionální i mezinárodní úrovni;
- spolupracovat se soukromým sektorem;
- revidovat legislativní rámec kyberkriminality i s ohledem na skutky tradiční kriminality páchané obdobnými prostředky;
- posílit mezinárodní spolupráci v trestních věcech, zrychlit procesy vzájemné právní pomoci a vymáhání práva;
- posílit sdílení nových přístupů k vyšetřování komplexních kybernetických trestných činů (finanční podvody, obchod s drogami, virtuálních měny, praní peněz) a poskytovat si vzájemnou technickou podporu;
- přijmout holistický přístup zohledňující možný budoucí vývoj trestné činnosti, reagovat s oporou mezinárodní spolupráce, využít technologie (databází, zabezpečené komunikační platformy).[87]

3.2 Víceletá strategie EUCPN

Evropská síť prevence kriminality (EUCPN)[88] je primárním zdrojem rozvoje prevence kriminality a osvědčených postupů v rámci EU. Strategickým cílem EUCPN je být referenčním

[85] Workshop 3: Posilování reakcí v oblastech prevence kriminality a trestní justice na vznikající formy trestné činnosti, jako je kyberkriminalita a obchodování s kulturními statky, včetně získaných poučení a mezinárodní spolupráce. čl. 36-38.
[86] Tamtéž. čl. 53-54.
[87] Tamtéž. čl. 55.
[88] European Crime Prevention Network viz *EUCPN* [online]. [cit. 13.12.2017]. Dostupné z: http://eucpn.org/

bodem pro cílové skupiny, šířit kvalitativní poznatky o prevenci kriminality, podporovat aktivity prevence kriminality na národní a lokální úrovni, přispívat k preventivní politice EU v různých aspektech prevence kriminality na úrovni EU, pokud jde o strategické priority EU.

Cílovými skupinami sítě jsou:[89] vykonavatelé a tvůrci strategií na místní úrovni, vykonavatelé a tvůrci strategií na národní úrovni a relevantní evropské a mezinárodní agentury, organizace a pracovní skupiny. Aktuálním dokumentem je Víceletá strategie Evropské sítě prevence kriminality na léta 2016 až 2020.[90]

Cíl: Být referenčním bodem pro cílové skupiny sítě

Síť se zaměří na identifikaci informačních potřeb každé cílové skupiny a příslušných prostředků komunikace s cílovými skupinami, a na informovanosti každé cílové skupiny ohledně důležitosti prevence kriminality. Specifické cíle pro tento bod jsou:

- pokračování ve vytváření databáze kontaktů členů cílové skupiny v souladu s prioritami politického cyklu;
- zlepšení komunikační strategie sítě;
- rozvíjení funkce sítě jako širší platformy EU v oblasti prevence kriminality;
- zajištění dynamického a interaktivního informačního bulletinu EUCPN;
- zachování standardu webových stránek EUCPN, co se týče obsah, designu a uživatelské přívětivosti;
- aktualizace nástrojů jednotné zpětné vazby pro EUCPN;
- zachování zásady rotace předsednictví a předsednictví správní rady EUCPN;
- posílení sekretariát EUCPN, pokud budou k dispozici finanční prostředky.[91]

Cíl: Rozšiřovat kvalitativní poznatky o prevenci kriminality

Úkolem sítě je zpracovávat koncepce prevence kriminality, shromažďovat přesné informace o příslušných kriminálních problémech, informace o účinných zákrocích a informace o účinných způsobech provádění intervencí. Specifické cíle v oblasti kvality informací jsou:

[89] Viz Příloha č. 3 – Organizace a vztahy EUCPN.

[90] *Multiannual Strategy for the European Crime Prevention Network* [online]. [cit. 13.12.2017]. Dostupné z: http://eucpn.org/sites/default/files/content/download/files/mas_2016-2020_final_version.pdf

[91] Tamtéž. s.4.

- intenzivní výměna informací prostřednictvím sítí, výzkum a hodnocení nejlepších postupů a vypracování doporučení v konkrétních tématech;
- analýza a rozvoj koncepce sítě v prevenci kriminality;
- šíření informací o příslušných kriminálních problémech a přiměřených reakcích na ně;
- posuzování dopadu práce v oblasti prevence kriminality;
- rozvíjení spektra výstupů s cílem zvýšit kapacitu pro reakce na klíčové potřeby zúčastněných stran.[92]

Cíl: Podporovat aktivity prevence kriminality na národní a místní úrovni

EUCPN by mělo zkoumat otázky a řešení financování projektů prevence kriminality, programů a iniciativ, otázky komunikace a význam kontextu při zavádění osvědčených postupů. V tomto ohledu se bude věnovat následujícím specifickým cílům:

- přehled zdrojů financování EU a vnitrostátních mechanismů financování trestné činnosti
- preventivní činnosti;
- publikace klíčových dokumentů v národních jazycích;
- vypracování doporučení o dopadu kontextu prevence na trestnou činnost;
- implementace nejlepších postupů členskými státy;
- transparentnější financování činností podporovaných EUCPN;
- zlepšení vazeb mezi EUCPN a institucemi vnitrostátní prevence kriminality.[93]

Cíl: Přispívat k preventivní politice EU v různých aspektech prevence kriminality na úrovni EU, pokud jde o strategické priority EU

Síť zintenzivní komunikaci s Komisí a dalšími příslušnými orgány a agenturami EU, bude využívat přístupu k informacím z jiných zdrojů v EU a zároveň bude poskytovat konkrétní možnosti iniciativy v prevenci kriminality na úrovni EU. S tím souvisí specifické cíle:

- zajištění užší spolupráce s příslušnými orgány, agenturami a organizacemi;
- zvýšení viditelnosti EUCPN;

[92] *Multiannual Strategy for the European Crime Prevention Network* [online]. [cit. 13.12.2017]. s. 4-5. Dostupné z: http://eucpn.org/sites/default/files/content/download/files/mas_2016-2020_final_version.pdf
[93] Tamtéž. s. 5.

- systematické sladění priorit s dohodnutými prioritami EU ohledně boje proti trestné činnosti;
- rozvíjení úlohy EUCPN při vytváření politik v oblasti prevence kriminality;
- strategičtější přístup k určování činností EUCPN;
- snaha o vytvoření širší evropské platformy pro prevenci kriminality na bázi spolupráce s jednotlivými subjekty.[94]

3.3 Strategie prevence kriminality v ČR

Prevence kriminality se v České republice začala formovat v rámci vládní politiky prakticky již od jejího vzniku v roce 1993. První Strategie prevence kriminality byla přijata v roce 1996, současné strategii tak předcházely strategie prevence kriminality na léta 1997 až 2000, 2001 až 2003, 2004 až 2007, 2008 až 2011 a 2012 až 2015.

Strategie prevence kriminality v České republice na léta 2016 až 2020 byla schválena Usnesením vlády České republiky ze dne 25. ledna 2016 č. 66 o Strategii prevence kriminality v České republice na léta 2016 až 2020. Tato strategie navazuje na obecnější strategické dokumenty s především bezpečnostní problematikou, zejména Bezpečnostní strategie České republiky, Strategický rámec udržitelného rozvoje České republiky, Strategie vnitřní bezpečnosti a ochrany obyvatelstva České republiky. Strategie prevence kriminality se zároveň nevěnuje souvisejícím oblastem, které jsou upraveny samostatnými strategickými materiály, například Strategie České republiky pro boj proti terorismu, Koncepce rozvoje českého vězeňství, Akční plán prevence domácího a genderově podmíněného násilí, Národní strategie boje proti obchodování s lidmi, Národní strategie primární prevence rizikového chování dětí a mládeže, Národní strategie bezpečnosti silničního provozu, či Národní strategie kybernetické bezpečnosti České republiky.[95] Koordinace prevence kriminality v těchto oblastech probíhá zejména prostřednictvím Republikového výboru pro prevenci kriminality.[96]

[94] *Multiannual Strategy for the European Crime Prevention Network* [online]. [cit. 13.12.2017]. s. 6. Dostupné z: http://eucpn.org/sites/default/files/content/download/files/mas_2016-2020_final_version.pdf
[95] Strategie prevence kriminality v České republice na léta 2016 až 2020. s. 3-4
[96] Blíže viz kap. 4.1.

3.3.1 Globální cíl

V České republice stabilně funguje rozvinutý systém prevence kriminality,[97] který plně odpovídá doporučením mezinárodních orgánů zabývajících se prevencí kriminality. Funkční systém a strategie prevence kriminality přispívají k tomu, že je tuzemský trend kriminality dlouhodobě klesající a že se daří aktivně a relativně včasně reagovat na nově vznikající formy kriminality. Na současné poměry navazuje globální cíl současné strategie, který deklaruje závazek České republiky udržovat a posilovat systém prevence kriminality, zajistit vhodné systémové, organizační a systémové předpoklady a podporovat preventivní přístupy v režimu moderního demokratického státu.[98]

3.3.2 Strategické cíle

Strategie prevence kriminality v České republice na léta 2016 až 2020 definuje pět strategických cílů, které rozvádí do celkem devadesáti osmi specifických cílů,[99] na které konkrétními úkoly navazuje Akční plán prevence kriminality na léta 2016 až 2020. Tyto strategické a navazující specifické cíle jsou v souladu s aktuálními prioritami prevence kriminality na mezinárodní úrovni, respektive reflektují Deklaraci z Dauhá.[100] Česká republika by se tedy podle současné strategie měla zaměřit na:

- rozvoj vybudovaného systému prevence kriminality, posílení spolupráce, kompetencí a kapacity relevantních partnerů, rozšíření prostoru pro dobrovolné aktivity při zajišťování bezpečnosti a veřejného pořádku, a to za opory mezinárodní spolupráci a vědeckých poznatků;
- poskytování a zkvalitnění pomoci a poradenství obětem trestné činnosti se zvláštním zaměřením na skupiny zvlášť zranitelných obětí;
- problém kriminální recidivy, účinnější resocializaci pachatelů a prevenci kriminality dětí a mládeže;

[97] Blíže viz kap. 4.
[98] Usnesení vlády ČR ze dne 25. ledna 2016 č. 66, o Strategii prevence kriminality v České republice na léta 2016 až 2020. s. 6-7.
[99] Blíže viz kap. 5
[100] Blíže viz kap. 3.1.1

- uplatnění komplexního přístupu k řešení zvýšené kriminality v rizikových lokalitách s vícezdrojovými příčinami (typicky sociálně vyloučené lokality);
- reakci na nové hrozby a trendy v oblasti bezpečnosti a veřejného pořádku a aplikaci nových efektivních přístupů k jejich předcházení.[101]

3.3.3 Základní principy preventivní politiky

Základní principy preventivní politiky prostupují celou strategií prevence kriminality a odrážejí se ve vymezených cílech a uložených úkolech. Současná strategie zdůrazňuje tyto principy:

- ***Prevence kriminality jako předpoklad pro udržitelný rozvoj a růst společnosti*** – Účinné strategie prevence kriminality pomáhají nejen snižovat trestnou činnost a tím i počet obětí, ale zároveň přispívají k celkové bezpečnosti ve společnosti. S tím přichází udržitelný rozvoj státu, zlepšující se kvalita života a dlouhodobé snižování nákladů na trestní politiku.
- ***Sdílení kompetencí a odpovědnosti*** – V oblasti zajišťování bezpečnosti a veřejného pořádku je nutná spolupráce jednotlivých subjektů (ministerstva a další státní orgány, Policie ČR, krajské a obecní samosprávy, obecní policie, neziskové organizace, fyzické i právnické osoby), které mají v systému vymezenou působnost. Současně je třeba srovnávat lokální a státní pohledy na hodnocení bezpečnostních problémů.
- ***Spolupráce a koordinovaný přístup*** – Vzhledem k tomu, že příčiny konkrétního kriminálního jednání vychází z více faktorů, je k zajištění předchozího principu nezbytná úzká spolupráce a koordinace vzájemných postupů.
- ***Sdílení dat a jejich analýza*** – Prevence kriminality může efektivně naplňovat vlastní cíle pouze v případě, kdy vychází z pečlivě zjištěných a analyzovaných dat.[102] Proces prevence tedy zahrnuje sběr informací, analýzu, reakce a vyhodnocení. Je také nutné nepodceňovat přípravu, plánování a řízení realizovaných projektů.

[101] Usnesení vlády ČR ze dne 25. ledna 2016 č. 66, o Strategii prevence kriminality v České republice na léta 2016 až 2020. s. 9-10.

[102] Model SARA: Scanning, Analysis, Response, Assesment. Blíže viz např. ECK, John E., Ronald V. CLARKE. *Analýza kriminality v 60 krocích* [online]. Praha: Otevřená společnost, 2010. [cit. 10.12.2017]. ISBN: 978-80-87110-22-5. Dostupné z: http://www.popcenter.org/library/reading/PDFs/60steps_czech.pdf

- ***Diferenciace a komplexnost preventivních opatření*** – Každé kriminálně rizikové chování má svůj motiv, své faktory, své příčiny a své prostředí. Tato kombinace vnějších a vnitřních vlivů může vyvěrat v jednorázový exces, nebo se může stát obecnější hrozbu opakování kriminality v dané lokalitě, daným pachatelem, či na dané oběti. Je tedy logické, že neexistuje žádné univerzální preventivní opatření, a proto je také třeba volit v různých případech rozdílné nástroje a přístupy.
- ***Přebírání pozitivních příkladů a zkušeností*** – Jedním ze zdrojů metodiky mohou být příklady dobré praxe a pozitivních zkušeností. Tyto lze čerpat jak ze zkušeností tuzemských, tak i na základě mezinárodních vztahů, či z odborné literatury. Tato řešení však nelze beze všeho aplikovat na nové případy a je třeba jednotlivé případy zanalyzovat a vyhodnotit, zda můžeme daný model převzít.[103]

3.3.4 Metody a nástroje preventivní politiky

Program prevence kriminality

Současná strategie ukládá Ministerstvu vnitra každoročně uvolňovat prostředky na prevenci kriminality tak, aby v celkovém objemu dosáhly v letech 2016 až 2020 výše minimálně 300 mil. Kč, přičemž minimálně 285 mil. Kč bude vyčleněno na nadresortní Program prevence kriminality.[104] Dotační Program prevence kriminality je proto nejvýraznějším nástrojem podpory prevence kriminality v České republice. Program vyhlašuje každoročně Ministerstvo vnitra tak, aby reflektoval aktuální Strategii prevence kriminality a Akční plán prevence kriminality. Specifické cíle Programu prevence kriminality podle současné strategie jsou:

- pokračovat v realizaci programu a dle možností posilovat jeho finanční rámec;
- převést dosavadní proces podávání písemných žádostí krajů a obcí do elektronické podoby a vytvořit novou databázi preventivních projektů a nástroj pro sdílení příkladů dobré praxe;
- usnadnit menším obcím zapojení do Programu prevence kriminality, pokud to jejich bezpečnostní situace vyžaduje;

[103] Usnesení vlády ČR ze dne 25. ledna 2016 č. 66, o Strategii prevence kriminality v České republice na léta 2016 až 2020. s. 10-12.
[104] Tamtéž. s. 58-59.

- klást důraz na vyhodnocování podpořených preventivních projektů dle metodik, analyzovat efektivitu a na základě příkladů dobré praxe vytvářet další metodické materiály a doporučení.[105]

Priority aktuálního programu se vždy přizpůsobují bezpečnostní situaci. Pro rok 2017 měly prioritu projekty se zaměřením na systém prevence kriminality, pomoc obětem trestné činnosti, boj proti recidivě, účinnější resocializace pachatelů, prevence kriminality dětí a mládeže, komplexní přístup k bezpečí v sociálně vyloučených a jiných rizikových lokalitách, nové hrozby a přístupy.[106] Jednotlivé projekty, na které budou uvolňovány finanční prostředky v roce 2018, musí být zaměřeny k podpoře a rozvíjení aktivit zaměřených na pouliční kriminalitu a prevenci majetkové trestné činnosti (hlavní priorita pro rok 2018), nové hrozby a nové přístupy v oblasti prevence kriminality (kriminalita ve virtuálním prostředí, ochrana měkkých cílů, zadlužení, extremismus, hatecrime a další), zvlášť zranitelné oběti trestných činů, kriminalitu dětí a mladistvých, trestné činy na úseku dopravy pod vlivem alkoholu a jiných návykových látek. Vítané jsou také inovativní přístupy k řešení uvedených oblastí preventivního působení.[107]

Další nástroje prevence kriminality

Strategie kromě Programu prevence kriminality uvádí další preventivní metody a nástroje, včetně specifických cílů v jejich oblasti:

- ***Analytický přístup a sdílení dat*** – Pro analýzu by se měly využívat moderní analytické nástroje. Dále má být vytvořen a realizován pilotní projekt pro využití nástrojů v oblasti mapování, analýz a predikce kriminality a dle výsledku se implementují tyto nástroje pro potřeby Policie ČR s případným využitím pro obce a obecní policii. Také je nutné posílit kvantitativní i kvalitativní personální kapacity, zlepšovat kvalitu shromažďovaných dat,

[105] Usnesení vlády ČR ze dne 25. ledna 2016 č. 66, o Strategii prevence kriminality v České republice na léta 2016 až 2020. s. 24-26.

[106] Vyhlášení Programu prevence kriminality na rok 2017 [online]. [cit. 5.12.2017]. Dostupné z: http://www.mvcr.cz/clanek/vyhlaseni-programu-prevence-kriminality-na-rok-2017.aspx

[107] Vyhlášení Programu Ministerstva vnitra v oblasti prevence kriminality na rok 2018 [online]. [cit. 5.12.2017]. Dostupné z: http://www.mvcr.cz/clanek/prevence-kriminality-v-resortu-ministerstva-vnitra.aspx

sdílet data s relevantními partnery a vytvořit pravidla a podmínky pro takovou spolupráci, (včetně zajištění ochrany sdílených dat).[108]

- ***Odborné vzdělávání*** – V návaznosti na projekt Efektivní rozvoj a posilování kompetencí lidských zdrojů se vytvoří vzdělávací kurzy, jejich obsah a rozsah se přizpůsobí dle potřeb různých cílových skupin a bude se zajišťovat průběžné odborné vzdělávání pracovníků v oblasti prevence kriminality a sociálně patologických jevů.[109]
- ***Osvěta a informační aktivity*** – V oblasti informovanosti veřejnosti je třeba posilovat důvěru prostřednictvím větší otevřenosti a sdílení, rozvíjet stávající prostředky osvětových a informačních aktivit (včetně využití nových informačních kanálů), pokračovat v provozování portálu prevencekriminality.cz[110] a rozšířit poskytované informace o klíčové dokumenty a aktivity dalších členů Republikového výboru. Také by bylo vhodné posílit význam národní soutěže o nejlepší preventivní projekt,[111] zakotvit pravidla hodnocení a otevřít jej i dalším subjektům.[112]
- ***Legislativa*** – V případě vhodnosti a širšího konsenzu by bylo na místě posílit systém prevence kriminality legislativní cestou s cílem vytvořit stabilnější a efektivnější podmínky pro prevenci kriminality.[113]
- ***Mezinárodní spolupráce*** – Jelikož je mezinárodní spolupráce dobrým zdrojem pozitivních zkušeností a osvědčených řešení, je nutné ji neustále rozvíjet a činnosti v rámci mezinárodních organizací věnovat mimořádnou pozornost. Česká republika bude v této oblasti pokračovat v aktivním zapojení na mezinárodní úrovni, zejména v rámci Evropské unie, sdílet zkušenosti v oblasti prevence kriminality, zapojovat se do aktivit mezinárodních neziskových uskupení, zejména v rámci situační prevence ve městech, podílet se na tvorbě evropských norem v oblasti prevence kriminality, využívat zahraniční finanční k realizaci

[108] Usnesení vlády ČR ze dne 25. ledna 2016 č. 66, o Strategii prevence kriminality v České republice na léta 2016 až 2020. s. 29.
[109] Tamtéž. s. 30.
[110] *Prevence kriminality* [online]. [cit. 11.12.2017]. Dostupné z: http://www.prevencekriminality.cz/
[111] Viz např. Soutěž o Nejlepší projekt prevence kriminality na místní úrovni za rok 2017 [online]. [cit. 5.12.2017]. Dostupné z: http://www.mvcr.cz/clanek/zname-nejlepsi-projekty-prevence-kriminality.aspx
[112] Usnesení vlády ČR ze dne 25. ledna 2016 č. 66, o Strategii prevence kriminality v České republice na léta 2016 až 2020. s. 32.
[113] Tamtéž. s. 33.

preventivních projektů a aktivit, posilovat bilaterální spolupráci v oblasti prevence kriminality.[114]

- ***Věda, výzkum, inovace*** – Cílem na poli vědy, výzkumu a inovací je realizace společensko-vědných výzkumů, konkrétně celospolečenský výzkum zaměřený na prevenci kriminality a zjišťování pocitu bezpečí obyvatel, národní viktimologický výzkum a výzkumy v oblasti prevence kriminality, trestní a bezpečnostní politiky státu zaměřené na aktuální dílčí problematiky. Zároveň je třeba implementovat nejnovější technologie a trendy do praxe subjektů podílejících se na řešení prevence kriminality.[115]

3.3.5 Nové hrozby a přístupy k prevenci kriminality

Kriminalita a její formy se v čase vyvíjí a je tedy nutné nové trendy identifikovat, zhodnotit a připravit adekvátní reakci. Na vývoj mají vliv především demografické i legislativní změny a rozvoj nových technologií. Současná strategie uvádí mezi aktuálními tématy kriminalitu ve virtuálním prostředí,[116] zadlužení jako významný kriminogenní faktor, stárnutí populace, bezpečnost měkkých cílů, kriminalitu páchanou cizinci a na cizincích, nové přístupy v boji proti majetkové kriminalitě. A v těchto oblastech si klade následující specifické cíle:

- podporovat a realizovat projekty zaměřené na boj proti kyberkriminalitě, informovat o existujících rizicích a možnostech ochrany a technických opatření, poskytovat pomoc a podporu obětem kyberkriminality;
- podporovat aktivity dluhového poradenství a v oblasti finanční gramotnosti, a to vůči cílové skupině ohrožených osob i vůči pracovníkům odpovědných orgánů a organizací;
- reflektovat demografický vývoj a zaměřit preventivní aktivity a poskytování pomoci na cílovou skupinu seniorů;
- budovat systém ochrany měkkých cílů s cílem zvyšovat míru zabezpečení proti závažným útokům, zaměřit se na vzájemnou spolupráci soukromého, nevládního a veřejně správního sektoru;

[114] Usnesení vlády ČR ze dne 25. ledna 2016 č. 66, o Strategii prevence kriminality v České republice na léta 2016 až 2020. s. 34.
[115] Tamtéž. s. 35-36.
[116] Blíže viz kap. 6.

- sledovat a analyzovat vývoj v oblasti migrace a jeho vliv na kriminalitu, v případě potřeby reagovat vhodnými preventivními aktivitami a projekty;
- uplatňovat nové přístupy a technologie zejména v situační prevenci s ohledem na majetkovou kriminalitu.[117]

[117] Usnesení vlády ČR ze dne 25. ledna 2016 č. 66, o Strategii prevence kriminality v České republice na léta 2016 až 2020. s. 55-57.

4 Systém prevence kriminality v ČR

Česká republika má zakotvený stabilní systém prevence kriminality, vybudovaný systém rozvíjí, posiluje spolupráci, kompetence a kapacity relevantních partnerů, rozšiřuje prostor pro působení dobrovolníků při zajišťování bezpečnosti a veřejného pořádku, přičemž se opírá rovněž o mezinárodní spolupráci a vědecké poznatky.

Prevence kriminality je v České republice organizována na třech úrovních:

- ***meziresortní úroveň*** – vytváření preventivní politiky vlády ve vztahu k tradiční kriminalitě a koordinace, případně vytváření nových, preventivních činností jednotlivých resortů zastoupených v Republikovém výboru pro prevenci kriminality;[118]
- ***resortní úroveň*** – programy prevence kriminality v rámci věcné působnosti jednotlivých ministerstev, obohacují jejich běžné činnosti o nové prvky a přístupy a ovlivňují tvorbu příslušné legislativy;
- ***místní úroveň*** – orgány veřejné správy, policie, nevládní organizace a další instituce působící v obcích, případně instituce na krajské úrovni.[119]

Zároveň subjekty prevence kriminality řadíme do následujících úrovní:[120]

- ***republiková úroveň*** – vláda ČR, Republikový výbor pro prevenci kriminality, ministerstva a další státní instituce;
- ***krajská úroveň*** – krajské úřady;
- ***lokální úroveň*** – samosprávy měst a obcí.[121]

4.1 Republiková a resortní prevence kriminality

Nejdůležitější úlohu v prevenci kriminality má vláda ČR, která zakotvuje strategický rámec, navrhuje legislativu a rozdělení finančních prostředků. Koordinační úlohu na celorepublikové

[118] Viz níže v této kapitole.

[119] Viz např. SVATOŠ, Roman. *Prevence kriminality*. 2., aktualiz. vyd. České Budějovice: Vysoká škola evropských a regionálních studií, z.ú., 2016. s. 18. ISBN 978-80-7556-009-4.

[120] Celý systém prevence kriminality a roli jednotlivých subjektů v něm znázorňuje schéma Systém prevence kriminality v ČR. Viz Příloha č. 4 – Systém prevence kriminality v ČR.

[121] Usnesení vlády ČR ze dne 25. ledna 2016 č. 66, o Strategii prevence kriminality v České republice na léta 2016 až 2020. s. 13.

úrovni zastává Republikový výbor pro prevenci kriminality, který funguje jako meziresortní orgán, odpovědný je však Ministerstvu vnitra. Ministerstva a jim podřízené organizace následně zajišťují naplňování strategie prevence kriminality v rámci resortních koncepcí a programů.

Republikový výbor pro prevenci kriminality

Republikový výbor pro prevenci kriminality (RVPPK) je meziresortní iniciační, koordinační a metodický orgán zřízený při Ministerstvu vnitra.[122] Výbor vytváří a sjednocuje koncepci preventivní politiky vlády ČR na meziresortní úrovni a metodicky napomáhá při její realizaci na všech úrovních veřejné správy. Za tímto účelem plní zejména tyto úkoly:

- koordinuje činnost ústředních orgánů státní správy v oblasti prevence kriminality v rámci bezpečnostní politiky;
- předkládá Strategii prevence kriminality ke schválení vládě České republiky;
- vládě České republiky předkládá výroční zprávu o plnění Strategie prevence kriminality;
- schvaluje žádosti o dotace, výši dotací a vyhodnocuje účinnost v rámci Programu prevence kriminality pro územní samosprávné celky;
- projednává další dotační programy v rámci Výboru v oblasti prevence kriminality,
- metodicky spolupracuje s vyššími územně samosprávnými celky při posuzování, zpracování a realizaci místních projektů prevence kriminality;
- doporučuje relevantní normy v oblasti prevence kriminality;
- podílí se na vzdělávání pracovníků, např. manažerů prevence kriminality krajů a obcí;
- spolupracuje s nevládními sektory, především neziskovými organizacemi, profesními sdruženími, akademickými a výzkumnými institucemi;
- posiluje mezinárodní spolupráci v oblasti prevence kriminality.[123]

Specifický cíl Výboru, a to posílení spolupráce subjektů v oblasti prevence kriminality, za tím účelem rozšíření zastoupení na úrovni členství o zástupce krajských a obecních samospráv a Agentury pro sociální začleňování,[124] byl z velké části naplněn usnesením vlády ČR ze dne

[122] Usnesení vlády ČR ze dne 3. listopadu 1993 č. 617, o projednání koncepce a programu prevence kriminality. Usnesení vlády ČR ze dne 16. listopadu 2016 č. 1007, Statut a Jednací řád RVPPK. čl. 1.
[123] Tamtéž. čl. 2.
[124] Usnesení vlády ČR ze dne 25. ledna 2016 č. 66, o Strategii prevence kriminality v České republice na léta 2016 až 2020. s. 14.

16. listopadu 2016 č. 1007, kterým byl s účinností od 1. ledna 2017 aktualizován statut a jednací řád Republikového výboru pro prevenci kriminality. Přetrvávající částí úkolu[125] je potom aktivní zapojení těchto nových členů.

Dle aktualizovaného statutu má Republikový výbor pro prevenci kriminality dvacet pět členů. Jeho předsedou je ministr vnitra a výkonným místopředsedou je náměstek ministra vnitra v oblasti prevence kriminality.[126] 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, – oblast sociálních služeb a sociální práce; Ministerstva spravedlnosti – oblast trestní politiky, – oblast trestní legislativy; Ministerstva školství, mládeže a tělovýchovy, Ministerstva vnitra – ředitel odboru, do jehož gesce spadá oblast prevence kriminality, – vedoucí oddělení, do jehož gesce spadá oblast prevence kriminality; Ministerstva zdravotnictví, Nejvyššího státního zastupitelství, Policejního prezidia České republiky – oblast vnější služby, – oblast služby kriminální policie a vyšetřování, – republikový koordinátor prevence kriminality Policie České republiky; Probační a mediační služby České republiky, Soudcovské unie České republiky, Svazu měst a obcí České republiky, Úřadu vlády České republiky – Odboru sociálního začleňování (Agentura), – Rady vlády pro koordinaci protidrogové politiky, – Rady vlády pro záležitosti romské menšiny; kteří jsou jmenováni osobami stojícími v čele vysílajících subjektů.[127]

Ministerstva a jim podřízené státní organizace

Podle cílů aktuální strategie a úkolů akčního plánu vytvářejí jednotlivá ministerstva a jim podřízené instituce, zejména pak členové Republikového výboru, vlastní resortní strategie a zajišťují jejich realizaci, a k tomu také často disponují vlastními dotačními tituly. Dále se zaměřují na specifické projekty prevence kriminality v rámci svých věcných působností. Aby tyto aktivity byly kontinuálně zajišťovány, tak musí být udržovány a zkvalitňovány kompetence

[125] Akční plán prevence kriminality na léta 2016 až 2020. s. 7.
[126] Usnesení vlády ČR ze dne 16. listopadu 2016 č. 1007, Statut a Jednací řád RVPPK. čl. 3 odst. 1, 2.
[127] Tamtéž. čl. 3 odst. 3.

a kapacity těchto orgánů.[128] Pro ministerstva a jim podřízené státní organizace stanovila strategie tyto specifické cíle:

- promítat preventivní politiku do svých působností a vhodně implementovat prevenci kriminality do svých vlastních strategií a koncepcí;
- disponovat odpovídajícími dotačními programy na podporu aktivit prevence kriminality dle své působnosti;
- realizovat vlastní preventivní projekty a aktivity dle své působnosti;
- posilovat vlastní kapacity a kompetence v oblasti prevence kriminality dle své působnosti.[129]

Jednotlivé specifické úkoly a aktivity v oblasti prevence kriminality jsou mezi jednotlivé resorty rozděleny následovně:[130]

- ***Ministerstvo vnitra*** – Ministerstvo vnitra se zaměřuje zejména na snižování míry a závažnosti kriminality a zvyšování pocitu bezpečí občanů, snížení delikvence u cílových rizikových skupin potenciálních pachatelů a zvýšení ochrany u cílových ohrožených skupin potenciálních obětí, efektivní, koordinovaný a komplexní a spolupracující systém prevence a vytvoření efektivního systému sběru a předávání informací v oblasti prevence kriminality. Ministerstvu vnitra je podřízena i v oblasti prevence kriminality Policie České republiky.[131] Dalším resortním subjektem je Poradní sbor ministra vnitra pro situační prevenci kriminality, který je koordinačním a iniciačním orgánem pro koncepční otázky a pro meziresortní spolupráci v rámci Programu prevence kriminality.[132]
- ***Ministerstvo práce a zahraničních věcí*** – Do specializace Ministerstva práce a zahraničních věcí spadají sociální služby, zejména služby sociální prevence, sociálně-právní ochrana dětí, politika zaměstnanosti a sociální dávky.

[128] Usnesení vlády ČR ze dne 25. ledna 2016 č. 66, o Strategii prevence kriminality v České republice na léta 2016 až 2020. s. 15.
[129] Tamtéž.
[130] SVATOŠ, Roman. *Prevence kriminality*. 2., aktualiz. vyd. České Budějovice: Vysoká škola evropských a regionálních studií, z.ú., 2016. s. 57-62. ISBN 978-80-7556-009-4.
Akční plán prevence kriminality na léta 2016 až 2020.
[131] Blíže k policejní prevenci viz kap. 4.4.
[132] Blíže k Programu prevence kriminality viz kap. 3.3.4.

- ***Ministerstvo spravedlnosti*** – Ministerstvo spravedlnosti je ústředním orgánem, jemuž jsou podřízeny Probační a mediační služba ČR, Nejvyšší státní zastupitelství, Institut pro kriminologii a sociální prevenci a Vězeňská služba ČR. Aktivity těchto institucí směřují k efektivnímu výkonu trestu, ať již odnětí svobody, či alternativnímu, a tím k prevenci recidivy. Především potom Institut pro kriminologii a sociální prevenci zkoumá projevy a příčiny kriminality a zabývá se otázkami trestní a bezpečnostní politiky a kontroly kriminality z pohledu represe i prevence.
- ***Ministerstvo školství, mládeže a tělovýchovy*** – Ministerstvo školství, mládeže a tělovýchovy zajišťuje především koncepci a koordinaci primární prevence rizikového chování dětí a mládeže, dále také přípravu, administraci, kontrolu a vyhodnocování dotačních programů.
- ***Ministerstvo zdravotnictví*** – Úkolem Ministerstvo zdravotnictví je vyhlašovat a administrovat dotační programy na podporu projektů zaměřených na prevenci rizikového chování a prevenci kriminality v souladu se schválenými akčními plány v rámci strategie Zdraví 2020. Jedněmi z nejpodstatnějších zaměření jsou péče o děti a zacházení s návykovými látkami a jejich prekursory.
- ***Ministerstvo pro místní rozvoj*** – Ministerstvo pro místní rozvoj je ústředním orgánem státní správy v oblasti prevence kriminality zejména pro regionální strategie a politiku bydlení.
- ***Ministerstvo obrany*** – Úkolem Ministerstva obrany je především vyčlenit finanční prostředky a kapacity na proškolení svých zaměstnanců, u nichž se zvyšuje míra rizikového chování vzhledem k povaze služebního poměru, či odloučení od rodiny.

Dalšími vládními orgány s vlastními aktivitami v oblasti prevence kriminality jsou Úřad vlády, Rada vlády pro koordinaci protidrogové politiky, Rada vlády pro záležitosti romské menšiny, Zmocněnec vlády pro lidská práva nebo Odbor pro začleňování v romských lokalitách.[133]

[133] SVATOŠ, Roman. *Prevence kriminality*. 2., aktualiz. vyd. České Budějovice: Vysoká škola evropských a regionálních studií, z.ú., 2016. s. 62-63. ISBN 978-80-7556-009-4.

4.2 Krajská prevence kriminality

Kraje realizují preventivní politiku v rámci samostatné působnosti,[134] a to zejména prostřednictvím manažerů kriminality, koordinace aktivit a předávání informací v rámci systému prevence kriminality, čerpáním dotací a realizací dotačních aktivit, a především naplňování vlastních bezpečnostních strategií a cílů. V praxi je přínosná dobrovolná spolupráce orgánů samosprávy a státní správy, zejména pak Policie ČR a justičních orgánů. Metodická, koordinační a finanční podpora je poskytována na základě strategie prevence kriminality, která zároveň nastavuje pravidla krajské prevence kriminality a stanovuje její specifické cíle:

- prostřednictvím Asociace krajů ČR se aktivně podlet na činnosti Republikového výboru pro prevenci kriminality;
- zpracovávat krajské koncepce prevence kriminality, bezpečnostní analýzy na krajské úrovni, stanovit rizikovost jednotlivých území pro plánování preventivních opatření;
- zajišťovat krajského manažera prevence kriminality včetně potřebného zázemí a specializované vzdělávání, vytvářet Pracovní skupiny prevence kriminality a zajišťovat a koordinovat jejich činnost;
- prostřednictvím manažerů prevence kriminality poskytovat konzultace a metodickou podporu pro preventivní aktivity obcí na svém území, zajišťovat informovanost v oblasti prevence kriminality z krajské a republikové úrovně směrem k obcím;
- podílet se na hodnocení a výběru projektů prevence kriminality obcí v rámci Programu prevence kriminality, zpracovávat a realizovat vlastní preventivní programy a projekty v rámci Programu prevence kriminality;
- podporovat preventivní aktivity a projekty kraje a obcí na svém území rovněž z vlastních zdrojů;
- vyhodnocovat plnění přijatých preventivních koncepcí a realizovaných preventivních projektů a opatření.[135]

[134] Srov. § 1 odst. 4 zákona č. 129/2000 Sb., o krajích (krajské zřízení).

[135] Usnesení vlády ČR ze dne 25. ledna 2016 č. 66, o Strategii prevence kriminality v České republice na léta 2016 až 2020. s. 19-20.

4.3 Lokální prevence kriminality

Obce jsou základním článkem v místní prevenci kriminality, kterou obdobně jako kraje realizují v samostatné působnosti.[136] Zároveň obec může k zabezpečení místních záležitostí veřejného pořádku ukládat povinnosti obecně závaznou vyhláškou[137] nebo k tomuto účelu zřídit obecní policii.[138] Klíčová je dobrovolná spolupráce samosprávných orgánů obce, orgánů vykonávajících přenesenou působnost, obecní policie, Policie ČR, neziskového sektoru, občanů i podnikatelských subjektů. Obce musejí reagovat na současný trend přesunu kriminality do menších obcí, znatelný především v sociálně vyloučených lokalitách. Strategie pro prevenci na obecní úrovni stanovuje specifické cíle:

- prostřednictvím Svazu měst a obcí ČR se aktivně podílet na činnosti Republikového výboru pro prevenci kriminality;
- zpracovávat obecní koncepce či plány prevence kriminality a bezpečnostní analýzy na lokální úrovni;
- zajišťovat činnost manažera prevence kriminalita obce včetně potřebného zázemí a specializovaného vzdělávání, vytvářet Pracovní skupiny prevence kriminality a zajišťovat a koordinovat jejich činnost (se zvláštním zaměřením na spolupráci, výměnu dat a informací a příkladů dobré praxe s Policií ČR na svém území);
- zřizovat obecní policii;
- zpracovávat a realizovat vlastní preventivní aktivity a programy či projekty v rámci Programu prevence kriminality;
- podporovat preventivní aktivity a projekty na svém území rovněž z vlastních zdrojů;
- vyhodnocovat plnění přijatých preventivních koncepcí a realizovaných preventivních projektů a opatření.[139]

[136] Srov. § 35 odst. 2 zákona č. 128/2000 Sb., o obcích (obecní zřízení).
[137] Srov. § 10 zákona č. 128/2000 Sb., o obcích (obecní zřízení).
[138] Srov. § 35a ?? a zákon č. 553/1991 Sb., o obecní policii, ve znění pozdějších předpisů.
[139] Usnesení vlády ČR ze dne 25. ledna 2016 č. 66, o Strategii prevence kriminality v České republice na léta 2016 až 2020. s. 20-22.

4.4 Policejní prevence kriminality

Úkolem Policie ČR je chránit bezpečnost osob a majetku a veřejný pořádek, plnit úkoly podle trestního řádu a další úkoly na úseku vnitřního pořádku a bezpečnosti svěřené jí zákony, a ve smyslu prevence kriminality předcházet trestné činnosti. [140] Prevence kriminality je v rámci Policie ČR oficiálně svěřena do působnosti specializovaných pracovišť, a to oddělení tisku a prevence (na úrovni krajských ředitelství a policejního prezidia) a skupina tisku a prevence (na územních odborech). Zatížení jediného pracoviště, či při nedostatku personálních zdrojů dokonce jediného pracovníka, dvěma zcela různými agendami, jejichž problematika vyžaduje odborné znalosti, které však nejsou definovány v rámci kvalifikačních předpokladů, tak nutně ovlivňuje kvalitu i kvantitu výsledků v obou činnostech.[141] Prevence kriminality je přitom průřezovou oblastí týkající se většiny policejních činností. V rámci policie narůstá agenda preventivních činností a zvyšuje se časová náročnost zajišťovaných úkolů a policie se zaměřuje na posílení role prevence kriminality v rámci svých činností, tak aby prevenci integrovala do policejní práce na všech úrovních.[142]

Analytická a metodická východiska policejní prevence kriminality jsou zakotvena ve strategických materiálech, zejména v Koncepci prevence kriminality policie na léta 2014 až 2016,[143] Strategii prevence kriminality v České republice na léta 2016 až 2020, Akčním plánu prevence kriminality na léta 2016 až 2020 a aktualizované Koncepci rozvoje Policie České republiky do roku 2020.[144] Cílem gestora prevence kriminality, kterým je ředitel kanceláře policejního prezidenta a oddělení tisku a prevence policejního prezidia, je personální posílení a integrace prevence tak, aby měli občané přehled o bezpečnostní situaci v okolí, dostupné programy a projekty pro snižování rizika ohrožení kriminalitou.[145] Konkrétními cíli Koncepce rozvoje Policie České republiky do roku 2020 jsou:

[140] Srov. zákon č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.
[141] Usnesení vlády ČR ze dne 25. ledna 2016 č. 66, o Strategii prevence kriminality v České republice na léta 2016 až 2020. s. 16-17.
[142] Koncepce rozvoje Policie České republiky do roku 2020 (aktualizace 2017). s. 49.
[143] Zde zakotvené cíle trvají a měly by být přeneseny při přijetí Koncepce prevence kriminality policie na léta 2017 až 2019.
[144] Aktualizace z února 2017.
[145] Koncepce rozvoje Policie České republiky do roku 2020 (aktualizace 2017). s. 104.

- rozvoj systému prevence kriminality pro efektivnější předcházení trestné činnosti;
- zlepšení efektivní komunikace policie a policistů s veřejností;
- posílení nerepresivní role policie v souladu s ustanovením § 2 zákona č. 273/2008 Sb., o Policii České republiky;
- budování pozitivní moderní bezpečnostní organizace státu;
- posilování pocitu spoluodpovědnosti občanů ČR za bezpečnost v zemi.[146]

Podmínky dosažení cílů předpokládají průběžné posilování lidských zdrojů již od roku 2017 a provedení organizačních změn ve smyslu oddělení preventivní a tiskové činnosti, a tedy zamezení kumulace více druhů činností vykonávaných jedním policistou. Koncepce rozvoje Policie České republiky do roku 2020 uvádí následující opatření:

- personální posílení pro oblast prevence kriminality;
- technické vybavení organizačních článků zabývajících se prevencí kriminality;
- realizace projektů zaměřených na komunikaci policistů s občany;
- naplňování Koncepce prevence kriminality policie na léta 2014 až 2016 a přijetí nové Koncepce prevence kriminality policie na léta 2017 až 2019;
- nastavení spolupráce policie se státní správou a samosprávou na detekci a eliminaci problémů v oblasti kriminality;
- v rámci přenášení dobré praxe se bude vycházet ze stávajících funkčních projektů spolupráce s občany a na základě evaluace jejich přínosů se vytvoří návrhy legislativní a systémové úpravy činností zainteresovaných subjektů tak, aby byly tyto činnosti celorepublikově aplikovatelné;
- posilování role prevence a určení služebních systemizovaných míst zaměřených na oblast prevence na všech úrovních policie.[147]

Community policing

Community policing je způsob výkonu policejní práce, v rámci prevence kriminality tedy analýzy, prognózování, spolupráce a vzdělávání, s orientací na občanskou komunitu a veřejnou službu. Tento přístup si zakládá na spolupráci policie s veřejností při zajišťování bezpečnosti a

[146] Koncepce rozvoje Policie České republiky do roku 2020 (aktualizace 2017). 62, 103.
[147] Tamtéž.

předcházení trestné činnosti a předpokládá, že profesionální, vstřícný a osobní přístup policistů povede k větší důvěře veřejnosti a ke zvýšení její důvěru se zapojovat do bezpečnostních opatření. Na základě vzájemné komunikace policie identifikuje rizikové faktory, navrhne jejich řešení a společně s občany realizuje opatření na odstranění příčin těchto problémů. Kvůli efektivitě je tento koncept uplatňován na lokální úrovni. Základní východiska community policing jsou:

- Standardní policejní práce není community policing nahrazena, jedná se pouze o metodický koncept doplnění, zkvalitnění a usnadnění policejních činností v dané lokalitě.
- Za bezpečnost a veřejný pořádek a celkovou kvalitu života přebírají část odpovědnosti místní instituce a občané. V občanech se rozvíjí motivace se zapojit do věcí veřejných v místě svého bydliště.
- Policie vede své partnery k společnému řešení trestné činnosti a současně usiluje o eliminaci příčin jejího výskytu.
- Policie pravidelně informuje veřejnost o bezpečnostní situaci a při plánování své činnosti bere v úvahu zpětnou vazbu, např. pravidelnými průzkumy spokojenosti.
- Preventivní aktivity jsou stejnoměrně delegovány na každého policistu v rámci jeho běžných služebních povinností.
- V lokalitě působí dlouhodobě stejní policisté, aby měli dostatek času získat dobrou místní znalost a možnost osobního přístupu k občanům, a zároveň, aby občané poznali svého policistu.
- Policisté jsou motivováni k proaktivní činnosti částečným přenesením zodpovědnosti za přidělenou oblast.[148]

4.5 Mezinárodní prevence kriminality

S mírou globalizace světa, kdy kriminalita ani její příčiny prakticky nemají hranice, je existence nadnárodní bilaterální nebo multilaterální spolupráce opravdu nezbytná. S tím souvisí

[148] *Community Policing* [online]. [cit. 3.12.2017]. Dostupné z: http://www.mvcr.cz/clanek/community-policing.aspx
Co je to Community policing [online]. [cit. 13.12.2017]. Dostupné z: http://www.policie.cz/clanek/co-je-to-community-policing.aspx

i zapojení mezinárodních organizací po metodické, koordinační, a zejména finanční stránce. Proto je nutné mezinárodní spolupráci věnovat mimořádnou pozornost a neustále pracovat na jejím rozvoji. Česká republika se v rámci mezinárodní prevence kriminality soustředí na zapojení se v nejdůležitějších světových a evropských organizacích a jejich specializovaných orgánech. Zároveň Česká republika spolupracuje na resortních projektech se zahraničními partnery, a inspiruje se příklady zahraniční dobré praxe.[149]

V rámci Organizace spojených národů (OSN)[150] je Česká republika zastoupena Ministerstvem vnitra mimo jiné v Úřadu pro drogy a kriminalitu (UNODC),[151] Komisi OSN pro prevenci kriminality a trestní justici (CCPCJ),[152] ve Výboru OSN pro lidská práva,[153] Výboru pro odstranění rasové diskriminace (CERD),[154] nebo Výboru pro odstranění diskriminace žen (CEDAW).[155] Vzhledem k členství v Evropské unii,[156] je pro Českou republiku podstatná činnost Evropské sítě prevence kriminality (EUCPN),[157] která úkoluje členské státy na základě víceleté strategie prevence kriminality.[158] V rámci Rady Evropy[159] má Česká republika zastupitelskou delegaci v Kongresu místních a regionálních orgánů Rady Evropy (CLRAE).[160]

[149] Usnesení vlády ČR ze dne 25. ledna 2016 č. 66, o Strategii prevence kriminality v České republice na léta 2016 až 2020. s.33-34.

[150] United Nations viz *UN* [online]. [cit. 13.12.2017]. Dostupné z: http://www.un.org/

OSN [online]. [cit. 13.12.2017]. Dostupné z: http://www.osn.cz/

[151] United Nations Office on Drugs and Crime viz *UNODC* [online]. [cit. 13.12.2017]. Dostupné z: http://www.unodc.org/unodc/index.html

[152] Commission on Crime Prevention and Criminal Justice viz *CCPCJ* [online]. [cit. 13.12.2017]. Dostupné z: http://www.unodc.org/unodc/en/commissions/CCPCJ/index.html

[153] Human Rights Council a Office of the UN High Commissioner for Human Rights viz *OHCHR* [online]. [cit. 13.12.2017]. Dostupné z: http://www.ohchr.org/EN/pages/home.aspx

[154] Committee on the Elimination of Racial Discrimination viz *CERD* [online]. [cit. 13.12.2017]. Dostupné z: http://www.ohchr.org/EN/HRBodies/CERD/Pages/CERDIntro.aspx

[155] Committee on the Elimination of Discrimination against Women viz *CEDAW* [online]. [cit. 13.12.2017]. Dostupné z: http://www.ohchr.org/EN/HRBodies/CEDAW/Pages/Introduction.aspx

[156] European Union viz *EU* [online]. [cit. 13.12.2017]. Dostupné z: http://europa.eu/

[157] European Crime Prevention Network viz *EUCPN* [online]. [cit. 13.12.2017]. Dostupné z: http://eucpn.org/

[158] Viz kap. 3.2.

[159] Council of Europe viz *COE* [online]. [cit. 13.12.2017]. Dostupné z: https://www.coe.int/en/web/portal/home

[160] Congress of Local and Regional Authorities of the Council of Europe viz *CLRAE* [online]. [cit. 13.12.2017]. Dostupné z: https://www.coe.int/en/web/congress/home

5 Prevence kyberkriminality a související pojmy

5.1 Kyberkriminalita a související pojmy

Kyberkriminalita

Kyberkriminalita není nutně odborným právním termínem, ale jde spíš souhrnné označení pro soubor skutků páchaných v kyberprostoru, respektive páchanou s využitím počítačových systémů nebo proti nim. Rozlišujeme kyberkriminalitu vlastní, tedy trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat či systémů, jako je trestný čin neoprávněný přístup k počítačovému systému a nosiči informací (§230 TZ), a obecnou kriminality páchanou prostřednictvím informačních a komunikačních technologií či služeb nabízených v kyberprostoru. Nutno připomenout, že se kyberkriminality dopouštějí i děti, i ty mladší patnácti let, tudíž bychom mohli mluvit o kyberproviněních, nebo kyberčinech jinak trestných. Některé formy kriminality mohou mít i povahu přestupku, či jiného správního deliktu.

Pod pojem kybernetická kriminalita lze tedy zařadit trestné činy následujících tří kategorií:

- trestné činy, jejichž individuálním objektem je ochrana počítačového systému, jeho vybavení a součástí před specifickými druhy útoku, respektive zájem na nerušeném užívání počítačového systému,
- trestné činy, u kterých je jedním ze znaků skutkové podstaty spáchání prostřednictvím informačních nebo komunikačních technologií,
- ostatní trestné činy, které mohou být v konkrétním případě také spáchány prostřednictvím informačních nebo komunikačních technologií.[161]

Kyberprostor

Kyber prostor je digitálním prostředím umožňujícím vznik, zpracování a výměnu informací, které je tvořené informačními systémy, a službami a sítěmi elektronických komunikací.[162]

---

[161] KOLOUCH, Jan. *Cybercrime* [online]. Praha: CZ.NIC, 2016. [cit. 2.3.2017] ISBN 978-80-88168-18-8. s. 37. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf

[162] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „zákon o kybernetické bezpečnosti“)

Kyberprostor je také možno definovat jako *„prostor kybernetických aktivit či jako prostor vytvořený informačními a komunikačními technologiemi, který vytváří virtuální svět (či prostor) jako paralelu k prostoru reálnému.“*[163]

Termín kyberprostor poprvé použil americko-kanadský spisovatel William Gibson v roce 1982 v příběhu pro časopis Omni, a poté ve svém sci-fi románu Neuromancer, kde kyberprostor popsal jako počítačovou síť ve světě plném bytostí s umělou inteligencí. V devadesátých letech bylo kyberprostor označováno „místo“, kde se lidé navzájem střetávali při používání Internetu.[164] V současnosti kyberprostor vnímáme jako vylepšený, větší a rychlejší odraz reálného světa, se všemi jeho nástrahami i nástrahami vlastními umocněnými menší uživatelskou intuicí.

Informační a komunikační technologie

Informační a komunikační technologie (ICT) zahrnují technologie, které poskytují přístup k informacím prostřednictvím telekomunikací, tedy internet, bezdrátové sítě, mobilní telefony a další komunikační média.[165]

Počítačový systém

Počítačový systém je souhrnem technických a programových prostředků.[166] Klasickým příkladem počítačového systému je osobní počítač, bankomat, mobilní telefon, tablet nebo herní konzole. Mezi počítačové systémy je však možné zařadit i televize a další chytré domácí spotřebiče, či palubní počítače a jiné systémy v automobilech, poskytující obdobné funkce.[167]

---

[163] KOLOUCH, Jan. *Cybercrime* [online]. Praha: CZ.NIC, 2016. [cit. 2.3.2017] ISBN 978-80-88168-18-8. s. 43. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf

[164] *Cyberspace*. [online]. [cit. 9.3.2017]. Dostupné z: https://www.britannica.com/topic/cyberspace

[165] ICT. *Tech terms* [online]. [cit. 14.12.2017]. Dostupné z: https://techterms.com/definition/ict

[166] Neboli hardware (technické prostředky) a software (programové prostředky).

[167] KOLOUCH, Jan. *Cybercrime* [online]. Praha: CZ.NIC, 2016. [cit. 2.3.2017]. ISBN 978-80-88168-18-8. s. 57-59. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf

Sociální sítě

Sociální sítě jsou webové služby a portály, které svým uživatelům umožňují vzájemnou komunikaci a interakci (diskutovat, chatovat, psát si blogy, sdílet fotografie).168 Při registraci si uživatel založí profil, tedy svou kyberidentitu. Nejoblíbenějšími sociálními sítěmi jsou Facebook, YouTube, Instagram, Twitter, Reddit, Pinterest, Vine, Ask.fm, Tumblr, Flickr, Google+, LinkedIn, VK, ClassMates a Meetup.[169] Na základě podobnosti, můžeme sociální sítě rozdělit na jednotlivé podkategorie:

- ***instant messaging*** – internetová služba, umožňující svým uživatelům sledovat, kteří jejich přátelé jsou právě připojeni, posílat zprávy, přeposílat soubory, a i jinak komunikovat, která funguje na principu odesílání zpráv v reálném čase (Facebook Messanger, Whatsapp, Hangouts, Skype)
- ***e-mail*** – elektronická pošta, jejíž provozovatelé nabízejí rozšířené služby, včetně propojení s instant messagingem nebo cloudovým úložištěm (Seznam Email, Gmail, Yahoo Mail, Windows Live Hotmail)
- ***online hry*** – hry zpravidla pro více hráčů připojených přes internet (WOW, WOT, LOL)
- ***profesní sociální sítě*** – v dnešní době slouží místo životopisu (LinkedIn)
- ***seznamky*** – seznamovací portály a aplikace (Tinder, Badoo)

Další související pojmy

- ***botnet*** – Síť infikovaných počítačů, které ovládá jediný cracker, který tak má přístup k výpočetnímu výkonu mnoha tisíců strojů současně. Umožňuje provádět nezákonnou činnost ve velkém měřítku, zejména útoky DDoS a distribuci spamu.
- ***cloudcomputing*** – Způsob využití výpočetní techniky, kde jsou škálovatelné a pružné IT funkce zpřístupněné uživatelům jako služba. Výhody cloudů: snadný upgrade softwaru, nenáročné klientské stanice a software, levný přístup k mohutnému výpočetnímu výkonu bez nutnosti investic do HW, garantovaná dostupnost.

---

168 Slovník. *Bezpečně online* [online]. [cit. 14.12.2017]. Dostupné z: https://bezpecne-online.saferinternet.cz/slovnik

169 *Top 15 Most Popular Social Networking Sites and Apps* [online]. November 2017. [cit. 13.12.2017]. Dostupné z: https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/

- ***darknet (darkweb)*** – Temná část internetu, respektive neprohledávaná klasickými vyhledávači, dostupná prohlížeči typu Tor.
- ***hoax*** – Poplašná zpráva, která se snaží svým obsahem vyvolat dojem důvěryhodnosti. Informuje např. o šíření virů nebo útočí na sociální cítění adresáta. Může obsahovat škodlivý kód nebo odkaz na internetové stránky se škodlivým obsahem
- ***malware*** – škodlivý software
- ***peer-to-peer*** – Např. BitTorrent je nástrojem pro peer-to-peer (P2P) distribuci souborů, který rozkládá zátěž datových přenosů mezi všechny klienty, kteří si data stahují.
- ***sociální inženýrství*** – Způsob manipulace lidí za účelem provedení určité akce nebo získání určité informace. Formami jsou například phishing (Podvodná metoda, usilující o zcizování digitální identity uživatele, jeho přihlašovacích jmen, hesel, čísel bankovních karet a účtu apod. za účelem jejich následného zneužití (výběr hotovosti z konta, neoprávněný přístup k datům atd.). Vytvoření podvodné zprávy, šířené většinou elektronickou poštou, jež se snaží zmíněné údaje z uživatele vylákat. Zprávy mohou být maskovány tak, aby co nejvíce imitovaly důvěryhodného odesílatele.), nebo pharming (Podvodná metoda používaná na internetu k získávání citlivých údajů od obětí útoku. Principem je napadení DNS a přepsání IP adresy, což způsobí přesměrování klienta na falešné stránky internetbankingu, e-mailu, sociální sítě atd. po zadání URL do prohlížeče.)
- ***spam*** – Nevyžádaná reklamní pošta, nebo jiné nevyžádané sdělení, zpravidla komerčního charakteru, které je šířeno Internetem. Nejčastěji se jedná o nabídky afrodisiak, léčiv nebo pornografie. Není-li systém dostatečně zabezpečen, může nevyžádaná pošta tvořit značnou část elektronické korespondence.
- ***Tor (The Onionin Browser)*** – Anonymizovaný prohlížeč fungující na bázi cibulového směrování, respektive postupného přesměrování IP adresy.[170]

5.2 Právní úprava kyberkriminality a její prevence

Kybernetická trestná činnost je z legislativního hlediska těžce uchopitelná. Její dvojí pojetí, respektive pravá kyberkriminalita a obecná kriminalita páchaná prostředky moderních

[170] *Výkladový slovník kybernetické bezpečnosti* [online]. [cit. 13.12.2017]. Dostupné z: https://www.govcert.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf

technologií, bylo nejen v našem právním systému vyřešeno vytvořením nových trestných činů a zároveň rozšířením výkladu či znění dosavadních trestných činů o nové formy páchání.

Vzhledem k možnosti dynamického vývoje a okamžité změny kyberkriminality není možné kyberkriminalitu kodifikovat, proto je legislativa v otázkách kyberkriminality a kyberprostoru roztříštěná v jednotlivých právních předpisech napříč veřejným i soukromým právem. Nadnárodní organizace se v této oblasti snaží docílit harmonizace.

Mimo právní předpisy je typickou soukromoprávní právní regulací kyberprostoru uživatelská smlouva neboli End-User Licence Agreement (EULA) anebo podmínky používání služby čili Terms of Use případně Terms of Service. Jedná se o smlouvu uzavřenou adhezním způsobem (§ 1798 - § 1801 OZ), kdy provozovatel dané aplikace, serveru, sociální sítě nebo webových stránek stanovuje podmínky koncovému uživateli, který ji přijímá click-wrap metodou[171] před registrací či udělením přístupu.

5.2.1 Mezinárodní a evropská právní úprava kyberprostoru a kyberkriminality

Jedním z prvních dokumentů věnujících se problematice kyberkriminality, přijatých na mezinárodní úrovni, byl v roce 1994 Manuál OSN o prevenci a kontrole trestných činů spojených s počítači.[172] Nejpodstatnějším dokumentem nadnárodního významu současnosti je Úmluva o kyberkriminalitě a dodatkový protokol k ní, stanovující základní rámec trestných kybernetických činů a prostředky pro odhalování a vyšetřování této kriminality.

Úmluva o kyberkriminalitě

Úmluva o kyberkriminalitě[173] byla schválena Výborem ministrů Rady Evropy v listopadu 2001 a v platnost vstoupila 1. července 2004. Českou republikou byla podepsána v únoru 2005, ratifikována v srpnu 2013 a v platnost vstoupila 1. prosince 2013. Podstatou Úmluvy je sjednotit národní legislativní zakotvení kyberkriminality, a zavázat smluvní strany k národní

[171] Viz např. Clickwrap Agreement. *Techopedia* [online]. [cit. 13.12.2017]. Dostupné z: https://www.techopedia.com/definition/4243/clickwrap-agreement

[172] *United Nations Manual on the prevention and control of computer-related crime* [online]. [cit. 9.3.2017]. Dostupné z: http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Guide.pdf

[173] *ETS No. 185 Convention on Cybercrime* [online]. [cit. 9.3.2017]. Dostupné z: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

implementaci takových nástrojů, které umožní postih definovaných kybernetických trestných činů. Úmluva tedy vytváří právní rámec pro jednotný a společný postup proti kyberkriminalitě a jejím pachatelům bez ohledu na místo spáchání trestného činu. Úmluva o kyberkriminalitě přináší definice kybernetických útoků a rozřazuje je do následujících skupin:

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

Dodatkový protokol k Úmluvě o kyberkriminalitě

Dodatkový protokol k Úmluvě o kyberkriminalitě[174] byl Radou Evropy přijat v lednu 2003. Jeho úlohou je definovat trestné činy, které neobsáhla Úmluva, a to ty, jež spočívají v šíření materiálů obsahujících nebo podporujících nenávist, diskriminaci nebo násilí na základě rasy, barvy pleti, rodové, národní, etnické nebo náboženské příslušnosti. Konkrétně se jedná o:

- Šíření rasistického a xenofobního materiálu skrze počítačový systém;
- Rasisticky a xenofobně motivovaná výhrůžka;
- Rasisticky a xenofobně motivovaná urážka;
- Popírání, hrubé zlehčování, schvalování nebo ospravedlňování genocidy nebo zločinů proti lidskosti.

Evropská úprava kyberprostoru a kyberkriminality

Z právních norem EU nebo ES jsou z pohledu boje s kyberkriminalitou nejvýznamnější následující dokumenty:

- Směrnice Rady 91/250/EHS o právní ochraně počítačových programů
- Rozhodnutí Rady 92/242/EHS o bezpečnosti informačních systémů
- Rámcové rozhodnutí Rady 2000/375/JHA o boji proti dětské pornografii na internetu

[174] *ETS No. 189 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems* [online]. [cit. 9.3.2017]. Dostupné z: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168008160f

- Rámcové rozhodnutí Rady 2001/413/SVV o potírání podvodů a padělání bezhotovostních platebních prostředků
- Směrnice Evropského parlamentu a Rady č. 2002/21/EC o společném regulačním rámci pro sítě a služby elektronických komunikací (rámcová směrnice)
- Směrnice Evropského parlamentu a Rady č. 2002/19/EC o přístupu k sítím elektronických komunikací a přidruženým zařízením a o jejich propojení (přístupová směrnice)
- Směrnice Evropského parlamentu a Rady č. 2002/20/EC o oprávnění pro sítě a služby elektronických komunikací (autorizační směrnice)
- Směrnice Evropského parlamentu a Rady č. 2002/22/EC o universální službě a uživatelských právech týkajících se sítí a služeb elektronických komunikací
- Směrnice Evropského parlamentu a Rady 2002/58/EC o ochraně údajů v elektronických komunikacích
- Rámcové rozhodnutí Rady EU č. 2002/584/JHA o evropském zatýkacím rozkazu a postupech předávání mezi členskými státy
- Směrnice Evropského parlamentu a Rady 2013/40/EU, o útocích na informační systémy, ze dne 12. srpna 2013
- Sdělení Komise Evropskému parlamentu, Radě, Hospodářskému a sociálnímu výboru a Výboru regionů – Boj proti spamu a špionážnímu („spyware“) a škodlivému softwaru („malicious software“), ze dne 15. 11. 2006
- Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů k obecné politice v boji proti počítačové kriminalitě, ze dne 22. 5. 2007
- Závěry Rady o společné pracovní strategii a konkrétních opatřeních v oblasti boje proti počítačové trestné činnosti, ze dne 27. listopadu 2008
- Sdělení komise Radě a Evropskému parlamentu, Řešení trestné činnosti v digitálním věku: zřízení Evropského centra pro boj proti kyberkriminalitě, 2012
- Nařízení Evropského parlamentu a Rady (EU) č. 526/2013, o Agentuře Evropské unie pro bezpečnost sítí a informací (ENISA), ze dne 21. května 2013
- Nařízení Evropského parlamentu a Rady (EU) č. 513/2014, kterým se jako součást Fondu pro vnitřní bezpečnost zřizuje nástroj pro finanční podporu policejní spolupráce,

předcházení trestné činnosti, boje proti trestné činnosti a řešení krizí a zrušuje rozhodnutí Rady 2007/125/SVV, ze dne 16. dubna 2014

- Nařízení Evropského parlamentu a Rady (EU) 2016/794, o Agentuře Evropské unie pro spolupráci v oblasti prosazování práva (Europol), ze dne 11. května 2016
- Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, ze dne 27. dubna 2016
- Směrnice Evropského parlamentu a Rady (EU) 2016/1148, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii, ze dne 6. července 2016[175]

5.2.2 Česká právní úprava kyberprostoru a kyberkriminality

V českém právní řádu mají vztah ke kyberprostoru a kyberkriminalitě především:

- Zákon č. 40/2009 Sb., trestní zákoník
- Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim
- Zákon č. 141/1961 Sb., o trestním řízení soudním
- Zákon č. 218/2003 Sb., zákon o soudnictví ve věcech mládeže
- Zákon č. 121/2000 Sb., autorský zákon
- Zákon č. 127/2005 Sb., o elektronických komunikacích
- Zákon č. 480/2004 Sb., o některých službách informační společnosti
- Zákon č. 273/2008 Sb., o Policii České republiky
- Zákon č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich
- Zákon č. 250/2016 Sb., o některých přestupcích
- Zákon č. 89/2012 Sb., občanský zákoník
- Zákon č. 101/2000 Sb., o ochraně osobních údajů
- Zákon č. 14/1993 Sb., o opatřeních na ochranu průmyslového vlastnictví
- Zákon č. 441/2003 Sb., o ochranných známkách
- Zákon č. 527/1990 Sb., o vynálezech, průmyslových vzorech a zlepšovacích návrzích
- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů

[175] Celý výčet viz KOLOUCH, Jan. *Cybercrime* [online]. Praha: CZ.NIC, 2016. [cit. 13.12.2017] s. 335-337. ISBN 978-80-88168-18-8. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf

- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce
- Zákon č. 160/1999 Sb., o svobodném přístupu k informacím
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti[176]

5.2.3 Trestná činnost spojená s kyberkriminalitou

Mezi kybernetické trestné činy, tedy trestné činy, u nichž je počítačový systém objektem, resp. hmotný předmětem útoku, nebo nástrojem umožňující jejich spáchání, ať již stanoven jako znak skutkové podstaty trestného činu nebo nikoli, je v českém právu možné zařadit: neoprávněné nakládání s osobními údaji (§ 180 TZ), poškození cizích práv (§ 181 TZ), porušení tajemství dopravovaných zpráv (§ 182 TZ), porušení tajemství listin a jiných dokumentů uchovávaných v soukromí (§ 183 TZ), pomluva (§ 184 TZ), šíření pornografie (§ 191 TZ), výroba a jiné nakládání s dětskou pornografií (§ 192 TZ), zneužití dítěte k výrobě pornografie (§ 193 TZ), navazování nedovolených kontaktů s dítětem (§ 193b TZ), krádež (§ 205 TZ), neoprávněné užívání cizí věci (§ 206 TZ), podvod (§ 209 TZ), provozování nepoctivých her a sázek (§ 213 TZ), podílnictví (§ 214 TZ), legalizace výnosů z trestné činnosti (§ 216 TZ), poškození cizí věci (§ 228 TZ), neoprávněný přístup k počítačovému systému a nosiči informací (§ 230 TZ), opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 TZ), poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232 TZ), neoprávněné opatření, padělání a pozměnění platebního prostředku (§ 234 TZ), výroba a držení padělatelského náčiní (§ 236 TZ), zkreslení údajů a nevedení podkladů ohledně vývozu zboží a technologií dvojího užití (§ 264 TZ), porušení práv k ochranné známce a jiným označením (§ 268 TZ), zkreslení údajů a nevedení podkladů ohledně zahraničního obchodu s vojenským materiálem (§ 267 TZ), porušení chráněných průmyslových práv (§ 269 TZ), porušení autorského práva, práv souvisejících s právem autorským a práv k databázi (§ 270 TZ), obecné ohrožení (§ 272 TZ), poškození a ohrožení provozu obecně prospěšného zařízení (§ 276 TZ), šíření toxikomanie (§ 287 TZ), získání kontroly nad vzdušným dopravním prostředkem, civilním plavidlem a

[176] KOLOUCH, Jan. *Cybercrime* [online]. Praha: CZ.NIC, 2016. [cit. 13.12.2017] s. 338. ISBN 978-80-88168-18-8. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf

pevnou plošinou (§ 290 TZ), ohrožení bezpečnosti vzdušného dopravního prostředku a civilního plavidla (§ 291 TZ), teroristický útok (§ 311 TZ), vyzvědačství (§ 316 TZ).[177]

5.2.4 UNODC repozitář pro kyberkriminalitu

Úřad pro drogy a kriminalitu OSN vypracoval online UNODC repozitář pro kyberkriminalitu[178] jako centrální databázi zákonů o počítačové kriminalitě a získaných zkušeností, za účelem usnadnění dalšího hodnocení potřeb a schopností trestního soudnictví, poskytování a koordinace technické pomoci. Úložiště se skládá ze tří databází:

- ***Case Law Database*** – soubor judikatury a záznamů o úspěšných operací vymáhání práva v oblasti kyberkriminality a trestných činnů souvisejících s elektronickými důkazy;
- ***Database of Legislation*** – soubor právních předpisů, týkajících se kyberkriminality a procesního práva, ve kterém lze vyhledávat podle země, trestného činu a procedurálních aspektů;
- ***Lessons Learned*** – národní postupy a strategie v oblasti prevence a boje proti kyberkriminalitě.[179]

[177] KOLOUCH, Jan. *Cybercrime* [online]. Praha: CZ.NIC, 2016. [cit. 2.3.2017] s. 338-340. ISBN 978-80-88168-18-8. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf

[178] *UNODC Cybercrime Repository* [online]. [cit. 11.12.2017]. Dostupné z: https://www.unodc.org/cld/v3/cybrepo/

[179] About Us. *UNODC Cybercrime Repository* [online]. [cit. 11.12.2017]. Dostupné z: https://www.unodc.org/cld/about-us/index-cybrepo.html?lng=en

6 Kyberkriminalita na sociálních sítích a její prevence

V prostředí sociálních sítí lze spáchat většinu forem kyberútoků. Prevence kyberkriminality na sociálních sítích vychází z informovanosti veřejnosti o rizicích a nástrahách neuvědomělého používání informačních technologií. Významným opatřením primární prevence kyberkriminality je také začlenění témat spojených s rizikovou virtuální komunikací do školních osnov. Velmi důležitým nástrojem ochrany dětí v kyberprostoru je fungující komunikace mezi dítětem a rodičem.[180] Prevence kyberkriminality se zaměřuje na zvyšování kybergramostnosti společnosti. Preventivní opatření jsou tedy především osvětová a informační. V rámci programů prevence kyberkriminality vznikají přehledné infografiky,[181] které mohou být umístěny na vývěsná místa v prostorách veřejných budov a na nástěnkách ve školách.

6.1 Kybergrooming

Kybergrooming je druhem psychické manipulace realizované v kyberprostoru, tedy prostřednictvím internetu, případně informačních a komunikačních technologií.[182] Jednání útočníka má v oběti vyvolat důvěru, respektive nevzbudit podezření, a přimět oběť něco vykonat či se s útočníkem osobně setkat. Medializovaná podoba kybergroomera často představuje staršího muže s pedofilní preferencí, který se snaží zlákat dítě k osobní schůzce, aby jej mohl sexuálně zneužít. Kybergrooming ovšem zahrnuje větší rozsah útočníků, obětí i způsobu jednání a motivace. Například se vše může odehrávat mezi vrstevníky, kdy jeden z druhého vyloudí informace nebo fotografie, které použije pro kyberšikanu. Nebo může jít pouze o způsob získávání pornografického materiálu.

Rizikové skupiny obětí

Obětí kybergroomingu se může stát prakticky kdokoli, mezi zvýšeně ohrožené ale patří oběti ve věku 11-17 let, ženského pohlaví, trávící mnoho volného času v on-line komunikačních prostředích, se sklony k závislostnímu chování, se sníženou sebeúctou a sebedůvěrou, strádající

[180] *Příručka pro rodiče: jak zajistit bezpečnost dětí na internetu* [online]. [cit. 11.12.2017]. Dostupné z: http://www.ncbi.cz/category/6-metodiky-ucebni-materialy

[181] Viz Příloha č. 5 – Infografika Sociální sítě.

[182] Srov. např. ZOUBKOVÁ, Ivana a kol. *Kriminologický slovník*. Plzeň: Aleš Čeněk, 2011. s. 88. ISBN 978-80-7380-312-4.

nedostatkem pozornosti, s nedostatkem kritického myšlení, zvýšeně sugestibilní, a především digitálně negramotné.[183] Mezi nejčastější oběti patří:

- ***děti s nízkou sebeúctou nebo nedostatkem sebedůvěry*** – lze je snadno izolovat;
- ***děti s emocionálními problémy, oběti v nouzi*** – potřebují pomocnou ruku;
- ***děti naivní a přehnaně důvěřivé*** – komunikují s neznámými lidmi, nerozpoznávají rizika;
- ***adolescenti*** – zajímá je sexualita, chtějí experimentovat.[184]

Etapy a způsob komunikace

Kybergroomer bývá uvědomělým pokročilým uživatelem moderních technologií a zároveň zkušeným lhářem, respektive hercem schopným improvizace, a laickým psychologem. Své schopnosti s každou další obětí zdokonaluje a buduje si strategii kontaktu s obětí. Tyto postupy lze zobecnit a rozdělit do čtyř základních etap: příprava kontaktu, kontakt s obětí, příprava na osobní schůzku a osobní schůzka,[185] kdy je každá etapa specifická použitými technikami komunikace. Fáze komunikace bychom mohli rozlišovat i následovně:

- vyhlédnutí oběti na sociální síti;
- oslovení, navázání komunikace;
- budování důvěry a přátelského vztahu;
- vytváření emocionální závislosti;
- izolace oběti od okolí, utajování vztahu;
- erotické směřování komunikace;
- požadování sexuálně explicitního materiálu (fotografie, videa);
- uplácení oběti (dárky, nabízení peněz);
- přitvrzování komunikace, vydírání, vyhrožování;
- osobní schůzka (první a nezřídka zároveň poslední);

[183] *Kybergrooming a kyberstalking: metodický materiál pro pedagogické pracovníky* [online]. Národní centrum bezpečnějšího internetu, 2012. [cit. 13.12.2017]. s. 9. Dostupné z: http://www.ncbi.cz/category/6-metodiky-ucebni-materialy

[184] KOPECKÝ, Kamil. *Kybergrooming: nebezpečí kyberprostoru.* [online]. Olomouc: NET UNIVERSITY, 2010. [cit. 3.12.2017]. s. 4. ISBN 978-80-254-7573-7. Dostupné z: https://www.e-bezpeci.cz/index.php/component/content/article/7-o-projektu/925-materialy

[185] KOPECKÝ, Kamil. *Kybergrooming: nebezpečí kyberprostoru.* [online]. Olomouc: NET UNIVERSITY, 2010. [cit. 3.12.2017]. ISBN 978-80-254-7573-7. Dostupné z: https://www.e-bezpeci.cz/index.php/component/content/article/7-o-projektu/925-materialy

- násilí, útok, napadení (sexuální nátlak, pohlavní zneužití, znásilnění, zneužití dítěte k výrobě pornografie, kuplířství)
- případné další schůzky.[186]

Příprava kontaktu

Jelikož si je kybergroomer často vědom, že svým jednáním porušuje normy, tak použije to, co mu sociální sítě nabízejí – vytvoření kyberidentity. Většinou se jedná o identitu upravenou či zcela falešnou, tedy uvádění nepravdivých osobních údajů či používání cizích fotografií. Někteří útočníci dávají přednost statické identitě, tedy tomu, že si vytvoří a používá pouze jeden profil na dané sociální síti. Flexibilnější je užívání dynamické identity, kdy útočník podle potřeby identitu upravuje nebo rovnou používá více profilů (někdy i několik desítek profilů),[187] takový útočník zpravidla komunikuje s několika obětmi současně. Někteří útočníci dokonce vytvoří falešnou autoritu, tedy nevystupují jako konkrétní fyzická osoba, ale vydávají se za zástupce firem,[188] nebo v současné době jednodušeji – vytvoří facebookovou stránku s populární tématikou a s obětmi komunikují jako správce takové stránky.

Kontakt s obětí, navázání a prohlubování vztahu

Útočník si zpravidla potenciální oběť pečlivě vybírá. Kritéria takového výběru mohou být různá od preferenční skupiny, přes lokalitu pobytu oběti, po rozsah a typ sdílených informací. Jedna z typických činností pro tuto etapu komunikace je sběr informací[189] a na jejich základě profilování oběti. Útočník se zaměřuje nejen na informace, které oběť veřejně sdílí na svých

---

[186] *Kybergrooming a kyberstalking: metodický materiál pro pedagogické pracovníky* [online]. Národní centrum bezpečnějšího internetu, 2012. [cit. 13.12.2017]. s. 7. Dostupné z: http://www.ncbi.cz/category/6-metodiky-ucebni-materialy

[187] Aydin Coban (mimo jiné případ Amandy Todd) využíval ke kybergroomingu, respektive ke kyberšikaně, 96 facebookových profilů. Viz např. PERRIE, Robin. 'I WILL DRIVE YOU TO KILL YOURSELF' Sick internet paedophile gets 10-year sentence for blackmailing children into performing explicit webcam shows after at least one of his victims commits suicide. *The Sun* [online]. 2017. [cit. 11.12.2017]. Dostupné z: https://www.thesun.co.uk/news/3109867/sick-internet-paedophile-gets-10-year-sentence-for-blackmailing-children-into-performing-explicit-webcam-shows-after-at-least-one-of-his-victims-commits-suicide/

[188] Případ Pavla Hovorky viz např. Soud poslal muže za zneužívání chlapců na osm let do vězení. *ČT24* [online]. [cit. 11.12.2017]. Dostupné z: http://www.ceskatelevize.cz/ct24/domaci/1422179-soud-poslal-muze-za-zneuzivani-chlapcu-na-osm-let-do-vezeni

[189] Cílené sbírání informací neboli fishing. Srov. *Methods of Online Predators.* [online]. [cit. 5.12.2017]. Dostupné z: https://www.webroot.com/us/en/home/resources/tips/cyberbullying-online-predators/safety-methods-of-online-predators

profilech na sociálních sítích, ale v systematickém sběru pokračuje i v průběhu komunikace. Ze získaných informací se snaží utvořit osobnostní profil oběti, který využívá k dotvoření své kyberidentity a podle kterého volí způsob a témata komunikace. Pokud je informací dostatek, nebo jsou v daném smyslu užitečné, nebývá pro útočníka obtížné oběť najít a identifikovat v reálném světě.

Při komunikaci se útočník snaží oběť zaujmout, proto kopíruje její zájmy a přizpůsobuje se jejímu způsobu vyjadřování i použité slovní zásobě.[190] Cílem útočníka v této fázi je vlichotit se oběti, aby mu věnovala čas, a tím získal prostor pro utváření vzájemného vztahu, ideálně vztahu závislosti. Komunikace ze strany útočníka je tedy milá až úlisná, zaměřuje se na oblasti, ve kterých je oběť nedoceněna, případně oběť přímo uplácí. Takové dárky mohou být drobnostmi, jako je značkové tričko nebo nákup online hry, může se ovšem jednat i o přislíbení nového telefonu nebo společné dovolené. Vztah také může být vytvořen na základě pocitu sounáležitosti či soucitu, kdy pachatel může předstírat smutek ze ztráty štěněte, nebo bezradnost při rozvodu rodičů.[191] Úplatky také mohou být silnou motivací oběti k osobnímu setkání, a to i opakovaně. Pokud jsou tato setkání za účelem sexuálního kontaktu, pak se prakticky jedná o prostituci, respektive dětskou prostituci.[192]

Svěřit se někomu koho vůbec neznáme, a navíc přes internet bez osobního kontaktu, je mnohdy jednodušší, než s problémem jít za kamarádem nebo rodiči. Kybergroomer toto umí využít ve svůj prospěch, a při utvrzování oběti v tom, že on se také dokáže svěřit jenom jí, a že jenom ona mu rozumí, buduje u oběti stav závislosti. Čím více důvěrných informací o oběti získá, tím větší má prostor pro následnou manipulaci. Útočník zpravidla prosí, či přímo zakazuje, aby se o něm oběť s někým bavila, a pokud by mu nebylo vyhověno, hrozí rozšířením citlivých informací o oběti. Zpočátku tedy oběť vyhledává kybergroomera dobrovolně, jako svého internetového kamaráda, později však může setrvávat v komunikaci z donucení.

---

[190] Zrcadlení neboli mirroring. Srov. *Methods of Online Predators.* [online]. [cit. 5.12.2017]. Dostupné z: https://www.webroot.com/us/en/home/resources/tips/cyberbullying-online-predators/safety-methods-of-online-predators

[191] Lákání neboli luring. Srov. např. *The 17 Lures Predators May Use to Exploit Children.* [online]. [cit. 5.12.2017]. Dostupné z: http://www.ortv.org/Charter/17_lures_predators_may_use.htm

[192] Viz kap. 6.5.

Také není neobvyklé, že virtuální komunikace postupně přejde do sextingu.[193] Pokud se útočníkovi podaří zlákat oběť k zaslání sexuálně explicitních materiálů, tak se můžeme setkat s následujícími jevy. První možností je sdílení získaných materiálů jako pornografického obsahu, a když uvážíme obvyklé oběti, tak se často jedná o dětskou pornografii.[194] V druhém případě může útočník využít získané materiály k získání dalších, a to vydáváním se za osobu na fotografii k vylákání obdobných materiálů na další oběti, nebo prostým vyhrožování zveřejněním, pokud oběť neposkytne další materiál, či nepřijde na osobní schůzku. Je také možné, že se útočník například k fotografii se sexuálním obsahem dostane náhodou a zároveň získá i kontakt na osobu na fotografii (nebo se k těmto údajům dostane cíleně, když obdobné materiály systematicky vyhledává), tak se zpravidla nejedná o klasický kybergrooming, ale začíná rovnou ve fázi vyhrožování zveřejněním, pokud oběť nebude spolupracovat.

Kybergroomer může také vyhrožovat nejen sdílením informací o oběti, ale právě využít těchto informací k přenesení hrozby do reálného světa a oběti vyhrožovat například fyzickým napadením v místě bydliště. Avšak ani reálné důsledky v případě, kdy není útočník s chováním oběti spokojen a citlivé informace týkající se oběti nebo právě materiál se sexuálním obsahem nasdílí nebo rozpošle, nejsou zanedbatelné. A není neobvyklé, že se tyto materiály stanou podnětem pro kyberšikanu.[195]

Příprava na osobní schůzku

Útočník, který zpočátku nesměřuje k osobní schůzce, ale jeho zájmem byly například fotografie se sexuálním obsahem, zpravidla zůstává u virtuální komunikace. Pokud však útočník cílí komunikaci s obětí k osobnímu setkání, použije různé prostředky manipulace, aby ke schůzce došlo. Je možné, že se oběť chce s útočníkem setkat, i když zná (třeba i od začátku) jeho pravou identitu. Buďto se jedná o výše zmíněné případy vydírání a vyhrožování, anebo může být dobrovolné setkání podmíněno nabídnutým úplatkem.

---

[193] Viz kap. 6.4.

[194] viz kap. 6.5

[195] viz kap. 6.3

Případ Amandy Todd viz *Amanda Todd Legacy* [online]. [cit. 11.12.2017]. Dostupné z: http://www.amandatoddlegacy.org/

Pokud se dospělý útočník vydává při komunikaci za vrstevníka své dětské oběti, pak musí pro osobní setkání vyřešit nesoulad kyberidentity se svou identitou. Jednou z komunikačních taktik je technika překonávání věkového rozdílu mezi útočníkem a oběti.[196] Příkladem může být situace, kdy se útočník vydává za vrstevníka oběti, tedy dítě. Po určitém čase pak sdělí oběti, že mu rodiče zakázali počítač, ale že si s ní může dál psát jeho starší bratr. Časem se oběť adaptuje na skutečnost, že komunikuje s dospělým.[197] Jednodušší taktikou potom může být udržování kyberidentity až do osobní schůzky, kdy ovšem útočník při setkání sehraje úlohu například otce, který má oběť vyzvednout.[198]

Osobní schůzka

Osobní setkání je vyvrcholením někdy i několika měsíčního působení kybergroomera na oběť. Výsledkem této schůzky může být mimo jiné sexuální zneužití oběti, fyzické násilí na oběti, zneužití oběti pro dětskou prostituci nebo k výrobě dětské pornografie. Je možné, že počátek schůzky, a někdy i celá první schůzka či několik prvních schůzek, bude sloužit pouze k ověření identity oběti a prohloubení vztahu oběti s útočníkem. K útoku tedy může dojít až po několika schůzkách. Zároveň může mít útočník dostatek prostředků, jak finančních na úplatky nebo materiálních jako předmětu vydírání, aby se s ním oběť scházela opakovaně, i když už k útoku došlo.[199]

---

[196] KOPECKÝ, Kamil. *Kybergrooming: nebezpečí kyberprostoru.* [online]. Olomouc: NET UNIVERSITY, 2010. [cit. 3.12.2017]. s. 7. ISBN 978-80-254-7573-7. Dostupné z: https://www.e-bezpeci.cz/index.php/component/content/article/7-o-projektu/925-materialy

[197] BROWN, Duncan. Developing strategies for collecting and presenting grooming evidence in a high tech world. *National Center for Prosecution of Child Abuse Update*. 2001, 14(11). Převzato z: BERSON, Ilene R. *Grooming Cybervictims: The Psychosocial Effects of Online Exploitation for Youth.* [online]. [cit. 11.12.2017]. Dostupné z: https://www.cs.auckland.ac.nz/~john/NetSafe/I.Berson.pdf

[198] Případ Ashleigh Hall viz např. CARTER, Helen. Facebook murderer who posed as teenager to lure victim jailed for life. *The Guardian* [online]. 2010. [cit. 11.12.2017]. Dostupné z: https://www.theguardian.com/uk/2010/mar/08/peter-chapman-facebook-ashleigh-hall

[199] KOPECKÝ, Kamil. *Kybergrooming: nebezpečí kyberprostoru.* [online]. Olomouc: NET UNIVERSITY, 2010. [cit. 3.12.2017]. s. 8. ISBN 978-80-254-7573-7. Dostupné z: https://www.e-bezpeci.cz/index.php/component/content/article/7-o-projektu/925-materialy

Prevence kybergroomingu

Velmi důležitým nástrojem ochrany dětí v kyberprostoru je fungující komunikace mezi dítětem a rodičem. Rodiče by se měli zajímat o moderní technologie, se kterými jejich děti přichází do styku, a o rizika, která s tím souvisí.

Pravidla pro rodiče:

- Komunikujte se svými dětmi o tom, co dělají na internetu. V kyberprostoru neexistuje pojem doma v bezpečí.
- Počítač dítěte by měl být tam, kde ho můžete namátkou kontrolovat.
- Pokud to zařízení dovoluje nastavte prvky rodičovské kontroly.
- Vysvětlete dětem, jaká rizika může internet představovat.
- Zákaz používat počítač rizikovou komunikací nevyřeší. V případě, že se vaše dítě dostane do problémů spojených s kybergroomingem, kyberšikanou či dalšími nebezpečnými komunikačními jevy, řešte je s příslušnými institucemi a nebojte informovat policii.[200]

Základní pravidla pro děti a mládež:

- Lidé lžou a na internetu je to ještě mnohem snazší. Nenechte se zlákat sliby virtuálních útočníků.
- Všímejte si nesrovnalostí v projevu útočníka.
- Uvědomte si, proč by někdo chtěl za každou cenu udržet internetový vztah nebo obsah komunikace v tajnosti.
- Nenechte se manipulovat a vytyčte si své osobní hranice. Nepřijímejte ani neodesílejte jiným uživatelům materiály se sexuálním obsahem.
- Ve virtuálním prostředí nikomu nesdělujte své osobní údaje, tedy ani své fotografie.
- Nikdy nechoďte na osobní schůzku, aniž by o ní někdo věděl. Uvědomte si, co všechno se vám na schůzce může stát.

---

[200] KOPECKÝ, Kamil. *Kybergrooming: nebezpečí kyberprostoru.* [online]. Olomouc: NET UNIVERSITY, 2010. [cit. 3.12.2017]. s. 14. ISBN 978-80-254-7573-7. Dostupné z: https://www.e-bezpeci.cz/index.php/component/content/article/7-o-projektu/925-materialy

Srov. Několik tipů na ochranu před kybergroomingem. *Bezpečně online* [online]. [cit. 11.12.2017]. Dostupné z: https://bezpecne-online.saferinternet.cz/pro-rodice-a-ucitele/teenageri-a-komunikace/item/36-jak-muzete-prispet-k-tomu-aby-se-vase-dite-nestalo-obeti-kybergroomingu

- Internetová komunikace vypadá jako anonymní, ale není. Nechcete přece, aby vás někdo vystopoval v reálném světě, nebo aby vás nutil dělat něco, co dělat nechcete.[201]

Modelový příklad

Pro přednášky na základních školách[202] na téma kybergrooming se mi osvědčil tento model. Před třídou přednesu následující příklad komunikace ze strany neznámé osoby, a poté pokládám dotazy směřující k rizikovým faktorům komunikace, společně hodnotíme odpovědi a snažíme se sestavit ideální postup při osobním setkání s někým, koho známe jen z internetu.

Do přátel na Facebooku ti pošle žádost o přátelství Petr Novák. Podle údajů na profilu je z Prahy a je mu 13 let. Na profilové fotografii má obrázek mopse. Zároveň ti od něj přijde zpráva a následná komunikace vypadá takto:

(Petr, 13) ahoj, jak je?
(x) …
(Petr, 13) já taky fajn
(Petr, 13) hele, kam že to chodíš na školu?
(x) …
(Petr, 13) no tak já jsem z druhý strany prahy.
(Petr, 13) ale koukal sem, že hraješ fotbal. je to tak?
(x) …
(Petr, 13) ty jo, a nemohl bych se někdy přijít podívat na trénink?
(Petr, 13) já totiž taky hraju, ale ten náš tým, to je samá lama
(x) …
(Petr, 13) jo, v úterý ve tři můžu. třeba za tím skladem vedle stadionu?
(x) …
(Petr, 13) super. tak čau v úterý

[201] KOPECKÝ, Kamil. *Kybergrooming: nebezpečí kyberprostoru.* [online]. Olomouc: NET UNIVERSITY, 2010. [cit. 3.12.2017]. s. 14. ISBN 978-80-254-7573-7. Dostupné z: https://www.e-bezpeci.cz/index.php/component/content/article/7-o-projektu/925-materialy
Srov. Bezpečnostní pravidla. *Bezpečně online* [online]. [cit. 11.12.2017]. Dostupné z: https://bezpecne-online.saferinternet.cz/k2-information/surfuj-bezpecne/komunikace-se-svetem/item/46-bezpecnostni-pravidla
[202] V rámci projektu Praha bezpečně online 2017.

- *S kým sis právě domluvil schůzku?* (kybergroomer nebo třináctiletý fotbalista)
- *Jak poznáš, že jde o falešnou kyberidentitu?* (rozpory v uváděných informacích, změny ve způsobu vyjadřování, hodně se ptá a málo mluví)
- *Jak si můžeš kyberidentitu ověřit?* (obrácené profilování, vyhledání fotografie, videohovor)
- *Jak si můžeš domluvit bezpečnou schůzku?* (na veřejném místě, říct to dospělému nebo alespoň kamarádům, vzít kamaráda s sebou, vzít si mobilní telefon)

6.2 Kyberstalking

Stalking je projevem obsesivní fixace známého či neznámého pachatele na určitou osobu, kterou systematicky obtěžuje nevyžádanou a nechtěnou pozorností. Pronásledování, slídění a obtěžování může být motivováno pozitivně obdivem či negativně zlobou. Útočník pronásleduje oběť na dálku nebo naopak fyzicky, vtíráním se do její blízkosti.[203] Právě formou distálního stalkingu je kyberstalking, tedy stalking prostřednictvím komunikačních, respektive informačních, technologií. Zpravidla považujeme za stalking jednání, které je intenzivní, například více než deset pokusů o navázání kontaktu, dlouhodobé, zpravidla minimálně měsíc, respektive čtyři až šest týdnů, obsahuje nátlak či výhružky, je pro oběť obtěžující, vyvolává u ní pocity strachu a omezuje ji.[204]

Základními projevy kyberstalkingu jsou opakované kontakty formou zpráv přes služby instant messaging,[205] či SMS zpráv a telefonátů. Zprávy mohou být příjemné, pochvalné, líbivé až úlisné, nebo naopak nechutné, urážející či vyhrožující. Není neobvyklé také střídání těchto protipólů. Zároveň dochází k působení na okolí, například snahou o převrácení rolí, kdy se stalker staví do role oběti, a tím se snaží získat mínění okolí na svoji stranu, nebo šířením nepravdivých informací s cílem očernit oběť.[206] Dalším z projevů je demonstrování síly útočníka, většinou vyhrožováním fyzickým ublížením oběti, či jejím blízkým. Krajním projevem je potom uskutečňování výhružek, či demonstrace síly formou ničení věcí patřících

[203] ČÍRTKOVÁ, Ludmila. *Forenzní psychologie*. 3., upr. vyd. Plzeň: Aleš Čeněk, 2013. s. 225. ISBN 978-80-7380-461-9.
[204] Srov. např. ČÍRTKOVÁ, Ludmila. *Moderní psychologie pro právníky: [domácí násilí, stalking, predikce násilí]*. Praha: Grada, 2008. ISBN 978-80-247-2207-8.
[205] Viz kap. 5.1.
[206] V takovém případě se již jedná o projev kyberšikany. Blíže viz kap. 6.3.

oběti.[207] Kyberstalker se zpravidla neuchyluje k fyzickému útoku, avšak nesmíme opomínat, že kyberstalking je v současné době spíše nástrojem stalkera než samostatným typem stalkingu.

Typologie stalkerů

Vzhledem ke vztahu oběti k útočníkovi může být stalkerem:

- osoba, kterou oběť osobně zná a ví, že ji pronásleduje;
- osoba, kterou oběť osobně zná, ale neví, že ji pronásleduje;
- osoba, kterou oběť osobně nezná.[208]

Obecně jsou útočníci většinou muži a oběti častěji ženy. Stalkeři reagují na běžné životní změny nápadným chováním, avšak svým jednáním nereflektují pouze momentální emoce, jelikož se za jejich projevy skrývá promyšlený záměr, umanutý úmysl nebo i blud.[209] Z pohledu vztahu útočníka k oběti rozlišujeme následující typy stalkerů:

- ***bývalý partner*** *(rejected stalker)* – Stalker není schopen přijmout ukončení vztahu s jinou osobou, přičemž se nemusí jednat pouze o partnerský či intimní vztah, ale může jít například o vztah pracovní, obchodní nebo terapeutický. Cílem stalkera je obnova vztahu, nebo naopak odplata za odmítnutí. Typickými průvodními pocity jsou hněv, žárlivost, pomstychtivost, zármutek, ponížení. Útočník často oběť zastrašuje, vyhrožuje jí.
- ***uctívač*** *(intimacy seeker)* – Stalker touží po vztahu s osobou, která jej zaujala, a předpokládá, že vyhlédnutý cíl bude jeho city opětovat. Cílem je být přijat uctívanou osobou. Jakákoli reakce oběti, mnohdy neuvědomělá nebo nemířená k útočníkovi, stalkera povzbuzuje a motivuje k dalšímu jednání. Oběti píše dopisy, kupuje dárky, telefonuje jí, a tak má pocit, že mu oběť dluží opětování jeho citů. Uctívač má zvýšené citové nároky, pokud

[207] KOPECKÝ, Kamil. *Stalking a kyberstalking: nebezpečné pronásledování.* [online]. Olomouc: NET UNIVERSITY, 2010. [cit. 3.12.2017]. s. 3. ISBN 978-80-254-7573-7. Dostupné z: https://www.e-bezpeci.cz/index.php/component/content/article/7-o-projektu/925-materialy

[208] KOPECKÝ, Kamil. *Stalking a kyberstalking: nebezpečné pronásledování.* [online]. Olomouc: NET UNIVERSITY, 2010. [cit. 3.12.2017]. s. 4. ISBN 978-80-254-7573-7. Dostupné z: https://www.e-bezpeci.cz/index.php/component/content/article/7-o-projektu/925-materialy

[209] *Kybergrooming a kyberstalking: metodický materiál pro pedagogické pracovníky* [online]. Národní centrum bezpečnějšího internetu, 2012. [cit. 13.12.2017]. s. 15. Dostupné z: http://www.ncbi.cz/category/6-metodiky-ucebni-materialy

je odmítnut, začne oběti vyhrožovat, snaží se ji poškodit, někdy užívá i násilí. Mezi tento typ patří stalkeři celebrit (celebrity stalkers).

- ***neobratný nápadník*** *(incompetent suitor)* – Sociálně neobratný stalker s malou schopností seznámit se touží po romantickém nebo intimním vztahu, ale nedokáže jej navázat. Tento typ stalkera je často narcistní, domnívá se, že je neodolatelně přitažlivý, má nedostatek empatie a nedokáže vnímat city oběti. Neobratní nápadníci se pokoušejí o fyzický kontakt s obětí, zpravidla se však neuchylují k násilí, také nebývají ve svých aktivitách příliš vytrvalí.
- ***ublížený pronásledovatel*** *(resentful stalker)* – Tento stalker usiluje o pomstu z důvodu skutečného nebo domnělého zranění nebo újmy, kterou mu podle něj oběť způsobila. Většinou se neuchyluje k přímému násilí, bývá však velmi vytrvalý a vynalézavý. Oběť zastrašuje, demonstruje sílu rozbitými předměty či zabitými domácími mazlíčky. Jeho chování bývá iracionální až paranoidní.
- ***sexuální útočník*** *(predatory stalker)* – Stalker usiluje o fyzický nebo přímo sexuální kontakt s obětí. Motivací bývá sexuální pud a pocit moci, jelikož se často jedná o útočníka se slabými sociálními dovednostmi. Související chování stalkera bývá obscénní.[210]
- ***poblouzněný milovník*** *(erotomaniac and morbidly infatuated stalker)* – Stalker věří, že je oběť do něj zamilovaná. Jakékoli jednání oběti interpretuje tak, aby to podporovalo jeho iluzi.[211] Jde o obdobu uctívače, jen je zde zdůrazněn vysoký sociální status oběti (např. také celebrita).
- ***kyberstalker*** *(cyberstalker)* – Kyberstalking je virtuální podoba stalkingu zahrnující použití informačních a komunikačních technologií se všemi možnostmi, které přináší, jako falešná kyberidentita, kybergrooming, psaní nevyžádaných soukromých zpráv formou e-mailu, SMS, chatu, psaní blogu, šíření pomluv, zasílání spamů nebo útoky malwarem.[212]

[210] MULLEN, Paul E., Michele PATHÉ a Rosemary PURCELL. The management of stalkers. *Advances in Psychiatric Treatment* [online]. 2001. 7(5). [cit. 11.12.2017]. ISSN 335-342. Dostupné z: http://apt.rcpsych.org/cgi/content/full/7/5/335

[211] Viz např. *Erotomaniac Morbidly Infatuated* [online]. [cit. 11.12.2017]. Dostupné z: https://www.asianfanfics.com/story/view/552377/6/stalker-series-newer-ver-stalker-you-psycho-obsession

[212] SMEJKAL, Vladimír. Kybernetická kriminalita. Plzeň: Aleš Čeněk, 2015. s. 273. ISBN 978-80-7380-501-2.

Prevence kyberstalkingu

Základní poučkou při prevenci kyberstalkingu, i ostatních typů kyberútoku, by mohlo být – Nesdílejte osobní a citlivé údaje s neznámými lidmi a nepodceňujte příznaky rizikové komunikace. Jak již bylo zmíněno, kyberstalker zpravidla zůstává v kyberprostoru, avšak kyberstalking je v současné době spíše nástrojem stalkera než samostatným typem stalkingu. Preventivně působit na veřejnost, ve smyslu uvědomění si rizik a možných dopadů stalkingu, můžeme například v médiích zpracováním reálných případů stalkingu formou dokumentu či osvětového videa.[213]

Privátní možnosti obrany:

- Přerušte veškeré kontakty s pronásledovatelem (neodpovídat na telefonáty, nereagovat na SMS, nescházet se). Jakýkoli kontakt s útočníkem může vést k prohloubení zájmu o oběť.
- Zprávy nemažte a nevyhazujte. Snažte se projevy pronásledování evidovat, zdokumentovat a uschovat důkazy pro následné řízení.
- Svěřte se. Informujte své blízké o pronásledování a totožnosti útočníka.
- Vyhledejte pomoc.
- Udělejte maximum pro svou bezpečnost a vypracujte bezpečností plán.
- Vyhýbejte se místům možného setkání, i kdyby to znamenalo změnit své návyky.
- Neodmítejte doprovod. Mimo domov se pohybujte ideálně s dospělým členem rodiny či jinou důvěryhodnou osobou.
- Pokud máte děti nebo bylo vyhrožováno někomu z rodiny, pak připravte přiměřený bezpečnostní plán i pro ně.
- Noste u sebe legální prostředky pro svou obranu (pepřový sprej, alarm). Mějte u sebe mobilní telefon pro případ přivolání pomoci.
- Nezveřejňujte své osobní údaje (telefonní číslo, adresu). Případně kontaktní údaje změňte a poskytněte je pouze důvěryhodným osobám.

[213] Například případy stalkingu v ČR viz Stalking. *Česká televize* [online]. [cit. 5.12.2017]. Dostupné z: http://www.ceskatelevize.cz/porady/10303355531-stalking/
Virtuální nápadník – preventivní film o stalkingu. *E-Bezpečí* [online]. [cit. 5.12.2017]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/stalking-a-kyberstalking/928-virtualni-napadnik-preventivni-film-o-stalkingu

- Věřte své intuici. Nepodceňujte situace, kdy se vám něco nezdá být v pořádku. Volejte o pomoc, běžte k lidem, hledejte jejich ochranu. Volejte policii.
- Ve všech bezpečnostních opatřeních vytrvejte tak dlouho, dokud projevy pronásledování neskončí. Pronásledování může trvat měsíce i roky.

Institucionální možnosti obrany:

- Kontaktujte formální autoritu.
- Kontaktujte odborné instituce: Bílý kruh bezpečí, intervenční centrum nebo jiné organizace pro pomoc obětem trestných činů.
- Kontaktujte policii a podejte trestní oznámení.[214]

6.3 Kyberšikana

Šikanu v reálném světě vnímáme jako déletrvající, soustavné, cílené zlomyslné týrání, obtěžování, sužování či pronásledován druhé osoby, která takové chování vnímá jako ohrožující a stresující. Typické jsou projevy agrese verbální i fyzické, krádeže, ničení věcí, stalking, ale může mít i formu sexuálního obtěžování nebo zneužívání. Šikana se týká všech věkových kategorií a různých kolektivů, obecně se posuzuje jako porucha vztahů ve skupině.[215]

Kyberšikana se odehrává ve virtuálním světě za použití informační a komunikační technologie či služby nabízené v kyberprostoru. Klasická a virtuální šikana se mohou vzájemně prolínat. Natočením reálné šikany na videozáznam a jeho sdílením na sociálních sítích přeneseme klasickou šikanu do kyberprostoru. Naopak by tomu bylo, kdyby se útočník kyberšikany rozhodl oběť vyhledat i v reálném světě. Od klasické šikany se kyberšikana nejvíce liší v následujících aspektech:

---

[214] KOPECKÝ, Kamil. *Stalking a kyberstalking: nebezpečné pronásledování.* [online]. Olomouc: NET UNIVERSITY, 2010. [cit. 3.12.2017]. s. 12. ISBN 978-80-254-7573-7. Dostupné z: https://www.e-bezpeci.cz/index.php/component/content/article/7-o-projektu/925-materialy
Nebezpečné pronásledování. *Bílý kruh bezpečí* [online]. [cit. 5.12.2017]. Dostupné z: https://www.bkb.cz/pomoc-obetem/trestne-ciny/nebezpecne-pronasledovani/
MERRITT, Marian. Straight Talk About Cyberstalking. *Norton* [online]. [cit. 5.12.2017]. Dostupné z: https://us.norton.com/cyberstalking/article

[215] ZOUBKOVÁ, Ivana a kol. *Kriminologický slovník*. Plzeň: Aleš Čeněk, 2011. s. 177-179. ISBN 978-80-7380-312-4.

- ***útočník*** – Zatímco v reálném světě se setkáváme s tím, že má útočník fyzickou převahu (ať již sám, nebo jeho zastánci), v kyberprostoru stačí místo svalů silné řeči, digitální gramotnost a ideálně sledovatelská či fanouškovská základna. Útočník kyberkriminality je mnohdy částečně nebo zcela anonymní, tedy buďto se jedná o někoho, koho vůbec neznáme, nebo ke komunikaci používá falešnou kyberidentitu.
- ***kontakt*** – Kyberkriminalita je zpravidla páchána distančně, takzvaně z bezpečí domova. I tak ji můžeme dělit na přímou (psaní soukromých zpráv) a nepřímou (šíření pomluv).
- ***publikum*** – Klasická šikana se často děje uvnitř kolektivu, je tedy zpravidla poloveřejná, přičemž kyberkriminalita může být soukromá (SMS), poloveřejná (verbální útoky ve virtuální komunitě) i veřejná (založení dehonestujících webových stránek). Publikum se u kyberšikany častěji zapojí, zatímco publikum v reálném světě častěji pasivně přihlíží. V kyberprostoru se šikana velmi rychle šíří, prakticky se sdílený obsah nedá odstranit a může se kdykoli objevit znovu.
- ***ohraničení*** – Kyberkriminalita není časově ani prostorově ohraničená. Na rozdíl od klasické kriminality například ve škole, která končí s poslední vyučovací hodinou a odchodem ze školy.
- ***motiv*** – Motivy jsou i u klasické šikany velmi subjektivní a často postačují nesympatie, či nějaká záminka. U kyberšikany se setkáme i s motivy jako nuda, snaha zabavit se, demonstrace síly, která útočníkovi chybí v reálném světě. Kyberútočník mohl být také obětí klasické šikany.
- ***důsledky*** – Oběť kyberšikany lze hůře rozeznat, jelikož neprojevuje žádné fyzické známky násilí (modřiny, roztrhané sešity, politá košile). Důsledky jsou obtížněji rozeznatelné i pro útočníka, obzvláště pokud je jím dítě. Může se tedy stát, že jde o kyberšikanu neúmyslnou, kdy pachatele nenapadne, že oběti svým jednáním ubližuje. [216]

Formy kyberšikany

Způsobů provedení kyberšikany je nepřeberné množství (soukromé zprávy na sociálních sítích / SMS / e-maily / telefonáty, sdílení informací / fotografií / videí mezi přáteli na sociálních

[216] Srov. např. BERAN, Tanya a Qing LI. The Relationship between Cyberbullying and School Bullying. *Journal of Student Wellbeing.* [online]. December 2007, 1(2). s. 15-33. [cit. 11.12.2017]. Dostupné z: https://www.ojs.unisa.edu.au/index.php/JSW/article/view/172

sítích, sdílení zmiňovaného obsahu veřejně, přetváření fotografií / videí, sdílení společné konverzace, šíření smyšlených zpráv a pomluv, zveřejnění telefonního čísla, vytváření falešných profilů na sociálních sítích, vytváření pomlouvačných a očerňujících webových stránek, krádeže identity, …) Každý útočník může být veden jiným motivem a každá oběť může reagovat jinak. Mezi časté formy kyberšikany patří:

- ***online válka*** *(flaming)* – agresivní slovní přestřelka plná nadávek a vulgarismů;
- ***online obtěžování*** *(harassment)* – opakované a urputné zasílání urážlivých, útočných, obscénních a nechutných zpráv;
- ***zostuzování*** *(denigration)* – rozesílání a sdílení nepravdivých zpráv, za účelem zničit někomu reputaci nebo přátelství;
- ***přetvářka*** *(impersonation)* – vydávání se za jinou osobu (krádež kyberidentity) a sílení škodlivého obsahu, za účelem způsobit dané osobě problémy, poškodit její reputaci nebo vztahy;
- ***odhalování*** *(outing)* – sdílení citlivých informací, tajemství, či zesměšňujících fotografií, za účelem danou osobu zostudit;
- ***manipulace*** *(trickery)* – manipulace k tomu, aby nám daná osoba sdělila něco soukromého nebo ztrapňujícího, za účelem tuto informaci nasdílet;
- ***vyloučení*** *(exclusion)* – záměrně hrubé vyloučení oběti z online komunity;[217]
- ***zveřejnění porna*** *(revenge porn)* – zveřejnění intimních fotografií či videa po rozchodu;
- ***fackování kolemjdoucích*** *(happy slapping)* – natáčení fyzického napadení náhodné osoby.[218]

Prevence kyberšikany

I kyberšikaně se dá do jisté míry předcházet.

[217] Willard, Nancy. Educator's Guide to Cyberbullying and Cyberthreats [online]. 2004. [cit. 11.12.2017]. Dostupné z: https://education.ohio.gov/getattachment/Topics/Other-Resources/School-Safety/Safe-and-Supportive-Learning/Anti-Harassment-Intimidation-and-Bullying-Resource/Educator-s-Guide-Cyber-Safety.pdf.aspx

[218] *Kyberšikana ve školním prostředí: metodický materiál pro pedagogické pracovníky* [online]. Národní centrum bezpečnějšího internetu, 2012. [cit. 13.12.2017]. s. 7. Dostupné z: http://www.ncbi.cz/category/6-metodiky-ucebni-materialy

Pravidla pro rodiče:

- Naučte děti chránit si soukromí a respektovat soukromí druhých.
- Naučte děti nereagovat na urážlivé zprávy.
- Mluvte s dětmi o tom, co přesně může být někomu druhému nepříjemné.
- Naučte děti blokovat konkrétní uživatele v komunikačních aplikacích.
- Vysvětlete dětem, ať urážlivé zprávy ukládají jako důkaz.
- Poznejte kamarády svých dětí.
- Mluvte se svými dětmi o všem, co na internetu dělají.
- Budujte důvěru svých dětí, aby se vám svěřily v případě, že se dostanou do problémů.
- Ujistěte děti, že není jejich vina, když je někdo obtěžuje.
- Vysvětlete dětem, jak důležité je chránit si heslo.[219]

Pravidla pro děti:

- Chraň si své soukromí. Rozmysli, co o sobě budeš na internetu říkat. Čím více informací ostatním poskytneš, tím větší mají možnost zaútočit. Se soukromými informacemi zacházej opatrně a nikdy nikomu nedávej svá přístupová hesla.
- Nejdřív mysli, potom piš. Už to nikdy nebudeš moct smazat a všechno, co pošleš, se dá kopírovat a rozesílat dál.
- Informuj se. Vygoogli sám sebe. Pokud narazíš na něco, co se ti nelíbí, požádej o smazání provozovatele webových stránek nebo obsah na sociálních sítích nahlas pro porušování práv.
- Na útoky nereaguj. Když odpovíš, jenom tím agresory povzbudíš a celý konflikt se ještě zvětší. Spousta stránek a služeb nabízí možnost někoho zablokovat.
- Vyhni se kontaktům. Změň přístupové údaje jako přihlašovací jména a přezdívky na sociálních sítích. Pokud nepomůže blokování, změň i telefonní číslo.
- Sbírej důkazy. Ukládej si maily, SMS, zálohuj si komunikaci na chatu, používej screenshot. Když podáš trestní oznámení na policii, mobilní operátoři i internetoví poskytovatelé mohou odhalit identitu pachatele.

[219] 10 tipů, jak předcházet kyberšikaně. *Bezpečně online* [online]. [cit. 13.12.2017]. Dostupné z: https://bezpecne-online.saferinternet.cz/pro-rodice-a-ucitele/teenageri-a-komunikace/item/33-jak-predchazet-kybersikane-10-tipu-pro-rodice-a-ucitele-deti

- Obraťte se na dospělého, kterému důvěřuješ. O kyberšikaně, se vyplatí mluvit s rodiči a učiteli. Možností je i policie, která může celou záležitost řešit právní cestou.
- Pomáhej ostatním, kteří trpí šikanou. Zakroč, pomoz oběti kyberšikany, a ideálně k tomu vyzvi i další lidi, ať je vás víc. Ti, kdo trpí šikanou, si většinou neumí sami pomoct, neumí se bránit a potřebují podporu.[220]

Kyberšikana ve školách

V rámci prevence kyberšikany může škola do školního řádu zařadit pravidla používání informačních technologií a mobilních telefonů během vyučování. Zároveň by měla zvyšovat podvědomí o bezpečném a etickém využívání internetu, začlenit toto téma do výuky a podporovat pozitivní využívání technologií. Školy by měly školit své pedagogy ohledně moderních technologií, včetně rizik a jejich řešení. Pedagog by měl ve třídě vytvářet dobré vztahy, posilovat empatii žáků a vést je k respektování druhých.

Postup školy při kyberšikaně:

- Zajistěte ochranu oběti a oběť poučte.
- Zajistěte dostupné důkazy. Kontaktujte operátora mobilní sítě, zřizovatele webových stránek, provozovatele sociální sítě.
- Důkladně vyšetřete všechny souvislosti se zjištěným incidentem a zajistěte si podporu a pomoc odborného pracovníka.
- Zvolte takové opatření a řešení, které je odpovídající závažnosti prohřešku a důsledkům, které agresor způsobil.
- Informujte a poučte rodiče oběti i rodiče kyberútočníky. Poučte rodiče o tom, koho mohou kontaktovat.
- Žádejte konečné stanovisko všech zainteresovaných subjektů.
- Při postizích útočníků postupujte v souladu se školním řádem a již vypracovaným krizovým plánem.[221]

---

[220] Kyberšikaně můžeš aktivně předcházet *Bezpečně online* [online]. [cit. 13.12.2017]. Dostupné z: https://bezpecne-online.saferinternet.cz/k2-information/surfuj-bezpecne/komunikace-se-svetem/item/49-kybersikane-muzes-aktivne-predchazet

[221] Kyberšikana. *CO DĚLAT, KDYŽ – INTERVENCE PEDAGOGA: Rizikové chování ve školním prostředí – rámcový koncept* [online]. [cit. 13.12.2017]. Dostupné z: www.msmt.cz/uploads/Priloha_7_Kybersikana.doc

6.4 Sexting

Pod pojem sexting řadíme elektronické rozesílání textových zpráv, fotografií či videí se sexuálním obsahem. Nejčastěji je osoba na fotografii zároveň jejím autorem. Motivací k zaslání takové fotografie může být snaha o zaujmout a navázat kontakt, zpestření partnerského vztahu, snaha zviditelnit se, případně tlak okolí, respektive partnera, nebo špatné vzory ve společnosti (celebrity i kamarádi).[222]

Už samotný vznik sexuálně explicitního obsahu může být problematický, protože sexting formou zasílání fotografií provozuje přes patnáct procent českých dětí,[223] a tyto fotografie jsou prakticky dětskou pornografií. Dále potom neexistuje záruka, že zaslané materiály nebudou dále šířeny kyberprostorem. Takto citlivé materiály mohou být také zneužity kyberútočníky jako předmět vydírání,[224] nebo dokonce cíleně za účelem vydírání či jiného zpeněžení od oběti vylouděny. Pokud jsou kybergrooming nebo kyberšikana spojeny právě se sextingem a intimními fotografiemi, pak jsou jejich dopady mnohem vážnější.[225]

Fotografie a videa se sexuálním obsahem mohou být zveřejněny různými způsoby. Osoba na fotografii, která je zároveň jejím autorem, může fotografii přímo zveřejnit, nebo takovou fotografii odešle a zveřejní ji příjemce, klasicky bývalý partner po rozchodu, nebo někdo další, komu se příjemce svěřil / fotografii přeposlal / někomu půjčil mobilní telefon. Další variantou je získávání materiálu se sexuálním obsahem bez vědomí zobrazované osoby. Ať již neoprávněným přístupem k datům, respektive fotografiím oběti, nebo nalákáním oběti na webcamsex, buď skutečný, nebo za využití webcam trollingu.[226]

---

[222] *Sexting.cz* [online]. [cit. 13.12.2017]. Dostupné z: www.sexting.cz
Teenageři a sexting – brožura pro náctileté. *Bezpečně online* https://bezpecne-online.saferinternet.cz/vyukove-materialy/ke-stazeni/send/4-brozury-a-letaky/78-teenageri-a-sexting-brozura-pro-nactilete

[223] Sexting a rizikové seznamování českých dětí v kyberprostoru (výzkumná zpráva) [online]. 2017. [cit. 13.12.2017]. Dostupné z: https://www.e-bezpeci.cz/index.php/tiskove-zpravy/1246-vyzkum-sexting-2017

[224] Viz kap. 6.1.

[225] Případ Amandy Todd viz *Amanda Todd Legacy* [online]. [cit. 11.12.2017]. Dostupné z: http://www.amandatoddlegacy.org/

[226] Oklamání oběti za použití podvrženého předem nahraného záznamu. Viz např. Webcam trolling. *E-Bezpečí* [online]. [cit. 13.12.2017]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/sociotechnika/1010-webcam-trolling

Prevence sextingu

Jedinou účinnou prevencí sextingu je intimní materiály vůbec nepořizovat. Pokud si někdo sexting nemůže odpustit, tak by měl dodržovat alespoň základní opatření proti zneužití:

- Počítejte s tím, že každá zaslaná fotografie je potenciálně zveřejněnou fotografií.
- Na fotografiích nemějte obličej, ani tetování, ani pro vás specifické šperky.
- Dávejte si pozor na pozadí fotografie, ať o vás nic neprozrazuje. Zrádný může být například monitor počítače, kde jste přihlášeni na sociální síti, nebo i výhled z okna či vaše nástěnka a jiné vybavení pokoje.
- Nesextujte, pokud jste přihlášeni přes firemní, školní, nebo jakoukoli nezabezpečenou wi-fi síť.
- Pokud si fotografie ukládáte, uzamkněte dané soubory heslem.

Dětská pornografie

Sexting provozovaný dítětem je prakticky výrobou dětské pornografie. Dětská pornografie zahrnuje snímky obnažených dětí v polohách vyzývavě předvádějících pohlavní orgány za účelem sexuálního uspokojení, snímky dětí zachycující polohy skutečného či předstíraného sexuálního styku nebo jiné obdobně sexuálně dráždivé snímky dětí.[227]

Fotografie a videa v rámci dětská pornografie nemusí vždy vznikat za tímto účelem. Může jít o pouhou nezodpovědnost rodičů, vůči obsahu, který sdílí na internetu.[228] Do této kategorie řadíme fotografie, z nichž je patrné, že jejich zobrazení může vést k ohrožení zdravého citového, rozumového a mravního vývoje dítěte. a fotografie, které obsahují genitálie, obnažené hýždě nebo prsa s bradavkami.[229]

[227] Viz Příloha č. 6 – Příklady nevhodného vyobrazení dětí na fotkách.
[228] VOKROUHLÍKOVÁ Kateřina a Zuzana PRŮCHOVÁ. *Naháči a prdeláči – fotky jen pro rodinu!* [online]. [cit. 5.12.2017]. Dostupné z: https://blog.nic.cz/2016/08/16/nahaci-a-prdelaci-fotky-jen-pro-rodinu/
[229] Co hlásit. *Stoponline.cz* [online]. [cit. 11.12.2017]. Dostupné z: https://www.stoponline.cz/page/3625/co-hlasit/

7 Vybrané projekty prevence kyberkriminality

V této kapitole uvedu několik českých i mezinárodních iniciativ na poli prevence kyberkriminality, zejména se budu věnovat projektu Safer Internet CZ, jeho dílčím projektům a aktivitám, které na něj navazují, a v závěru kapitoly podrobněji popíši zaměření aktuálního projektu Praha bezpečně online 2017.

E-Bezpečí

Projekt E-Bezpečí[230] je ve spolupráci s dalšími organizacemi realizován Centrem prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého.[231] Zaměření projektu je specializováno zejména na kyberšikanu a sexting, kybergrooming, kyberstalking a stalking, rizika sociálních sítí, hoax a spam, zneužití osobních údajů v prostředí elektronických médií. E-Bezpečí se partnersky podílí na projektech Google Centra pro bezpečnost,[232] Seznam se bezpečně[233] a Bezpečně na internetu.[234] Součástí E-Bezpečí je zároveň projekt E-Nebezpečí pro učitele,[235] který je zaměřený na vzdělávací aktivity pro učitele orientované na rozvoj znalostí a dovedností v oblasti informačních technologií.

Better Internet for Kids

Better Internet for Kids[236] je projektem Evropské komise, který navazuje na původní projekt Safer Internet.[237] Stěžejním materiálem tohoto projektu je Evropská strategie pro internet lépe uzpůsobený dětem.[238] Cílem této strategie je poskytnout dětem nástroje a uživatelské znalosti

---

[230] *E-Bezpečí* [online]. [cit. 9.12.2017]. Dostupné z: https://www.e-bezpeci.cz/

[231] *Centrum prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého* [online]. [cit. 9.12.2017]. Dostupné z: http://www.prvok.upol.cz/index.php/cz/

[232] *Google Centrum pro bezpečnost* [online]. [cit. 9.12.2017]. Dostupné z: https://www.google.cz/intl/cs/safetycenter/

[233] *Seznam se bezpečně* [online]. [cit. 9.12.2017]. Dostupné z: https://www.seznamsebezpecne.cz/

[234] *Bezpečně na internetu* [online]. [cit. 9.12.2017]. Dostupné z: http://o2.e-bezpeci.cz/

[235] *E-Nebezpečí pro učitele* [online]. [cit. 9.12.2017]. Dostupné z: http://www.e-nebezpeci.cz/

[236] *Better Internet for Kids* [online]. [cit. 2.12.2017]. Dostupné z: https://www.betterinternetforkids.eu/ *Better Internet for Kids – youth* [online]. [cit. 2.12.2017]. Dostupné z: https://www.betterinternetforkids.eu/web/youth/home

[237] *From a Safer Internet to a Better Internet for Kids* [online]. [cit. 9.12.2017]. Dostupné z: https://ec.europa.eu/digital-single-market/en/content/safer-internet-better-internet-kids

[238] *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Strategy for a Better Internet for Children.*

pro bezpečné využívání internetu, podněcovat tvorbu pozitivního, tvůrčího a vzdělávacího online obsahu, podporovat výuku digitální gramotnosti na školách, rozšířit možnosti nastavení ochrany soukromí a rodičovské kontroly a jejich rozlišení podle věku a přístupného obsahu, a v neposlední řadě, bojovat proti online sexuálnímu zneužívání dětí.[239]

eSafety Label

Projekt eSafety Label[240] je akreditační a podpůrnou službou pro evropské školy. Pokud škola předloží své postupy v oblasti online bezpečnosti, projde sebehodnotícím dotazníkem a plní personalizovaný akční plán, pak může získat certifikát, respektive etiketu online bezpečnosti. Etiketa může být bronzová, stříbrná, či zlatá, podle naplnění požadovaných kritérií a samostatných aktivit školy. Registrované školy mají na webových stránkách přístup k návodům, šablonám, radám a kontrolním listům.[241] V České republice realizuje tento projekt Národní centrum bezpečnějšího internetu.

Sheeplive – OVCE.sk

Projekt Sheeplive vznikl pod původním názvem OVCE.sk z iniciativy eSlovensko o.z. jako součást projektů Zodpovedne.sk, Pomoc.sk a Stopline.sk.[242] Projektovými partnery jsou Ministerstvo vnitra Slovenské republiky a Slovenský výbor pro Unicef. Projekt byl realizován s finanční podporou EU programu Bezpečný internet. Hlavním výstupem projektu je mezinárodní internetový portál Sheeplive.eu,[243] kde je umístěn animovaný seriál pro děti, který vznikal v letech 2009-2012.[244] Tento seriál se zaměřuje na bezpečnost dětí a mládeže na internetu a rizika mobilních telefonů a moderních technologií. Nalezneme zde témata jako sexting, kybergrooming, kyberšikana, happy slapping, kyberstalking, digitální stopa, anorexie,

COM(2012) 196 final [online]. [cit. 9.12.2017]. Dostupné z: http://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/european-strategy-making-internet-better-place-children

[239] *A European Strategy to deliver a Better Internet for our Children* [online]. [cit. 9.12.2017]. Dostupné z: https://ec.europa.eu/digital-single-market/node/286

[240] *eSafety Label* [online]. [cit. 9.12.2017]. Dostupné z: http://www.esafetylabel.eu/web/guest

eSafety Label (CZ) [online]. [cit. 9.12.2017]. Dostupné z: https://esafetylabel.saferinternet.cz/

[241] O eSafety Label. *eSafety Label* [online]. [cit. 9.12.2017]. Dostupné z: http://www.esafetylabel.eu/web/guest/about

[242] Obdobná struktura projektů jako u českého Národního centra bezpečnějšího internetu. Viz kap. 7.1.

[243] *Sheeplive.* [online]. [cit. 2.12.2017]. Dostupné z: http://www.sheeplive.eu/

[244] *Sheeplive – Základné informácie.* [online]. [cit. 3.12.2017]. Dostupné z: http://sk.sheeplive.eu/o-projekte/zakladne-informacie

diskriminace a rasismus, vulgarity, ochrana soukromí, online nakupování, phishing, či závislost na počítačových hrách.[245] Ve slovenské verzi jsou k dispozici i plakáty s jednotlivými tématy, či příručky pro pedagogy. K seriálu jsou postupně dotvářeny multijazyčné verze, v současné době je dostupný s českými titulky.[246] Dle mého názoru jde o velmi zdařilou výukovou pomůcku, vhodnou pro názornou ilustraci rizikového chování v prostředí kyberprostoru zejména při výuce na nižším stupni základních škol.

7.1 Safer Internet CZ

Safer Internet CZ neboli Centrum bezpečnějšího internetu (Safer Internet Center, SIC CZ) je český projekt realizovaný neziskovými organizacemi CZ.NIC[247] a Národním centrem bezpečnějšího internetu.[248] V rámci projektu spolupracovali i společnost CZI[249] a sdružení Linka bezpečí.[250] Projekt je spolufinancován Evropskou komisí[251] a svoji činnost koordinuje s evropskými Safer Internet projekty, respektive s projektem Better Internet for Kids.[252] Safer Internet CZ je také partnerem Google Centra pro bezpečnost[253] a eSafety Label.

Safer Internet CZ se zaměřuje zejména na děti a mladé lidi, cílí ovšem i na další specifické skupiny, jakými jsou odborní sociální a pedagogičtí pracovníci, či senioři. Vlajkovou lodí projektu je provoz národní platformy saferinternet.cz, na jejíž webových stránkách[254] nalezneme výukové a metodické materiály, informace ohledně ochrany soukromí v kyberprostoru. Tyto webové stránky mimo jiné slouží i jako rozcestník pro jednotlivé dílčí projekty.[255]

---

[245] Viz kap. 5.1 a kap. 6.
[246] *Sheeplive (CZ)* [online]. [cit. 3.12.2017]. Dostupné z: http://cz.sheeplive.eu/
[247] Viz níže v této kapitole.
[248] Viz níže v této kapitole.
[249] *CZI* [online]. [cit. 6.12.2017]. Dostupné z: https://www.czi.cz/
[250] *Linka bezpečí* [online]. [cit. 6.12.2017]. Dostupné z: https://www.linkabezpeci.cz/
[251] Safer Internet CZ: Safer Internet CZ – stručný popis projektu. *NCBI* [online]. [cit. 2.12.2017]. Dostupné z: http://www.ncbi.cz/evropska-komise/safer-internet-cz.html
[252] Viz výše v kap. 7.
[253] *Google Centrum pro bezpečnost* [online]. [cit. 9.12.2017]. Dostupné z: https://www.google.cz/intl/cs/safetycenter/
[254] *Saferinternet.cz* [online]. [cit. 2.12.2017]. Dostupné z: https://www.saferinternet.cz/
[255] O projektu – Centrum bezpečnějšího internetu (SIC CZ). *Saferinternet.cz* [online]. [cit. 2.12.2017]. Dostupné z: https://www.saferinternet.cz/info-o-nás/o-nás.html

Národní centrum bezpečnějšího internetu, z. s.

Národní centrum bezpečnějšího internetu (NCBI) bylo v roce 2007 založeno jako neziskové nevládní sdružení. Je členem evropské sítě center bezpečnějšího internetu Insafe[256] a spolupracuje s mezinárodní sítí horkých linek INHOPE.[257] NCBI provozuje odborné pracoviště, sdružuje lektory pro prevenci kyberkriminality, vytváří a publikuje metodické a výukové materiály k problematice bezpečnějšího kyberprostoru, ve spolupráci se svými partnery pořádá konference, semináře, přednášky a školení, na webových stránkách a prostřednictvím sociálních sítí informuje o aktualitách kyberprostoru. NCBI realizuje v rámci Saferinternet.cz řadu dílčích projektů souvisejících s bezpečnějším užíváním internetu,[258] podporuje vzdělávání, poskytuje pomoc, zasahuje při šíření nevhodného obsahu.[259]

CZ.NIC, z. s. p. o.

CZ.NIC je zájmovým sdružení právnických osob, které bylo založeno v roce 1998, nyní má 115 členů[260] a je členem INHOPE.[261] CZ.NIC provozuje webový portál nic.cz,[262] registruje doménová jména pod CZ doménou, zabezpečuje provoz domény nejvyšší úrovně .CZ, věnuje se rozšiřování technologie DNSSEC a služby mojeID a obecně podporuje rozvoj internetové infrastruktury v České republice.[263] Sdružení také provozuje interní bezpečnostní tým CZ.NIC-CSIRT[264] a Národní CSIRT tým České republiky – CSIRT.CZ.[265]

---

[256] Centra bezpečnějšího internetu se sdružují v rámci evropského projektu Better Internet for Kids. Viz Insafe and INHOPE. *Better Internet for Kids* [online]. [cit. 3.12.2017]. Dostupné z: https://www.betterinternetforkids.eu/web/portal/policy/insafe-inhope

[257] International Association of Internet Hotlines INHOPE je aktivní a spolupracující globální síť horkých linek, která se zabývá nezákonným online obsahem a je zaměřena na potlačení sexuálního zneužívání dětí na internetu. Viz *INHOPE* [online]. [cit. 3.12.2017]. Dostupné z: http://www.inhope.org/gns/home.aspx

[258] Viz níže v této kapitole.

[259] *NCBI* [online]. [cit. 6.12.2017]. Dostupné z: http://www.ncbi.cz/

[260] O sdružení. *CZ.NIC* [online]. [cit. 6.12.2017]. Dostupné z: https://www.nic.cz/page/351/

[261] Partneři. *STOPonline.cz* [online]. [cit. 6.12.2017]. Dostupné z: https://www.stoponline.cz/page/3571/partneri/

[262] *CZ.NIC* [online]. [cit. 6.12.2017]. Dostupné z: https://www.nic.cz/

[263] Tamtéž.

[264] CZ.NIC-CSIRT. *CZ.NIC* [online]. [cit. 6.12.2017]. Dostupné z: https://www.nic.cz/csirt/

[265] *Národní CSIRT České republiky* [online]. [cit. 6.12.2017]. Dostupné z: https://csirt.cz/

Computer Security Incident Response Team [online]. [cit. 6.12.2017]. Dostupné z: http://www.csirt.org/

Online Hotline #ProtiKyberzločinu

Horkou linku STOPonline.cz[266] provozuje sdružení CZ.NIC. Jednotlivé incidenty potom zpracovává a analyzuje Národní bezpečnostní tým CSIRT.CZ. STOPonline.cz je nástrojem pro ohlašování nezákonného obsahu, zejména dětské pornografie či nepatřičné dětské nahoty, šíření pornografie a kybergroomingu.[267] Podstatná je spolupráce s Policií České republiky, zapojení do mezinárodní sítě INHOPE i spolupráce s členy sdružení, díky kterým je možné v závažných případech zamezit šíření škodlivého obsahu v krátké době od oznámení incidentu.[268] Nezákonný obsah může být nahlášen prostřednictvím formuláře na domovské stránce webu STOPonline.cz,[269] pomocí e-mailu hotline@saferinternet.cz,[270] telefonicky na telefonním čísle +420 910 101 010,[271] nebo nově pomocí mobilní aplikace STOPonline.cz.[272] STOPonline.cz je v rámci sociálních sítích aktivní na Facebooku.[273]

Online Helpline #ProtiKybernásilí

Linka pomoci POMOConline.cz[274] je provozována Národním centrem bezpečnějšího internetu a specializuje se na problematiku zneužívání informačních technologií. Paralelní STOPonline.cz na ni odkazuje s tématy kyberšikana, revange porn, sexting a stalking.[275] POMOConline.cz se věnuje dětem a mladistvým i v případech kybergroomingu či sexuálního zneužívání, dále řeší rizika sociálních sítí a poskytuje pomoc dospělým a seniorům, kteří se ocitli v nepříznivé životní situaci z důvodu užívání informačních technologií.[276] Nevhodný

[266] *STOPonline.cz* [online]. [cit. 6.12.2017]. Dostupné z: https://www.stoponline.cz/stoponline/

[267] Co hlásit. *STOPonline.cz* [online]. [cit. 6.12.2017]. Dostupné z: https://www.stoponline.cz/page/3625/co-hlasit/

[268] O nás. *STOPonline.cz* [online]. [cit. 6.12.2017]. Dostupné z: https://www.stoponline.cz/page/3619/o-nas/

[269] *STOPonline.cz* [online]. [cit. 6.12.2017]. Dostupné z: https://www.stoponline.cz/stoponline/

[270] O projektu – Centrum bezpečnějšího internetu (SIC CZ). *Saferinternet.cz* [online]. [cit. 2.12.2017]. Dostupné z: https://www.saferinternet.cz/info-o-nás/o-nás.html

[271] Kontakt. *STOPonline.cz* [online]. [cit. 6.12.2017]. Dostupné z: https://www.stoponline.cz/page/3634/kontakt/

[272] Aplikace vyvinutá sdružení CZ.NIC je nyní dostupná pro mobilní operační systém Android. STOPonline.cz. *Google Play* [online]. [cit. 9.12.2017]. Dostupné z: https://play.google.com/store/apps/details?id=cz.nic.saferinternet

[273] *@stoponlinecz* [online]. [cit. 9.12.2017]. Dostupné z: https://www.facebook.com/stoponlinecz/

@horkalinkacz [online]. [cit. 9.12.2017]. Dostupné z: https://www.facebook.com/horkalinkacz/

[274] *POMOConline.cz* [online]. [cit. 9.12.2017]. Dostupné z: https://pomoconline.saferinternet.cz/

[275] Co neřešíme. *STOPonline.cz* [online]. [cit. 6.12.2017]. Dostupné z: https://www.stoponline.cz/page/3623/co-neresime/

[276] *POMOConline.cz* [online]. [cit. 9.12.2017]. Dostupné z: https://pomoconline.saferinternet.cz/

obsah a aktivity mohou být nahlášeny prostřednictvím webového formuláře,[277] pomocí e-mailu helpline@saferinternet.cz, nebo na telefonním čísle +420 252 548 438 (v pondělí a ve středu od 14:00 do 16:00).[278] Pro sdílení relevantní obsahu na sociálních sítích je pro helpline provozován facebookový profil.[279]

Bezpečně online

Dílčí činností v projektu Safer Internet CZ je provoz mládežnického panelu Bezpečně online,[280] který mimo jiné slouží k získávání zpětné vazby a námětů pro další činnost projektu od mladých lidí, zpravidla ve věku dvanácti až osmnácti let. Na webových stránkách tohoto panelu nalezneme slovník základních výrazů online bezpečnosti,[281] informace pro rodiče a učitele a výukové materiály. Vzhledem k cílové skupině tohoto panelu je samozřejmostí jeho aktivita na sociálních sítích, respektive na Facebooku.[282]

Mladí proti nenávisti online

Mezinárodní kampaň Mladí proti nenávisti online – žít, učit se a jednat pro lidská práva[283] je v České republice realizována Národní centrem bezpečnějšího internetu ve spolupráci s odborem pro mládež Ministerstva školství, mládeže a tělovýchovy ČR. Jedná se o osvětovou a vzdělávací kampaň zaměřující se na oblast lidských práv a mediální výchovu. Tato kampaň se staví proti šíření nenávisti na internetu, a to zejména proti rasové nesnášenlivosti, utlačování menšin, šíření agresivního nacionalismu či extremismu.[284] Mladí proti nenávisti online je součástí mládežnické kampaně Rady Evropy No Hate Speech Movement.[285]

---

[277] Kontaktní formulář. *POMOConline.cz* [online]. [cit. 6.12.2017]. Dostupné z: https://pomoconline.saferinternet.cz/component/visforms/?view=visforms&id=1

[278] O nás. *POMOConline.cz* [online]. [cit. 6.12.2017]. Dostupné z: https://pomoconline.saferinternet.cz/o-online-helpline.html

[279] @PomocOnline.cz. [online]. [cit. 9.12.2017]. Dostupné z: https://www.facebook.com/PomocOnline.cz/

[280] *Bezpečně online* [online]. [cit. 9.12.2017]. Dostupné z: https://bezpecne-online.saferinternet.cz/

[281] Slovník základních výrazů online bezpečnosti. *Bezpečně online* [online]. [cit. 9.12.2017]. Dostupné z: https://bezpecne-online.saferinternet.cz/slovnik

[282] @bezpecneonline. [online]. [cit. 9.12.2017]. Dostupné z: https://www.facebook.com/bezpecneonline/
@internetova.ambasada. [online]. [cit. 9.12.2017]. Dostupné z: https://www.facebook.com/internetova.ambasada

[283] *Mladí proti nenávisti online* [online]. [cit. 9.12.2017]. Dostupné z: https://protinenavisti.saferinternet.cz/

[284] O projektu. *Mladí proti nenávisti online.* [online]. [cit. 9.12.2017]. Dostupné z: https://protinenavisti.saferinternet.cz/o-projektu.html

[285] *No Hate Speech Movement* [online]. [cit. 9.12.2017]. Dostupné z: http://www.nohatespeechmovement.org/

Senioři bezpečně online

Další rizikovou skupinou v kyberprostoru jsou senioři. Projekt Senioři bezpečně online[286] se zaměřuje na aplikace a nástroje, které senioři nejvíce používají, jako je e-mail, Skype, Facebook, internetové bankovnictví a online obchody, a pomáhá jim užívat tyto nástroje bezpečně a rozeznávat například podvodné jednání protistrany.

7.2 Praha bezpečně online

Praha bezpečně online je několikaletým společným projektem Národního centra bezpečnějšího internetu, z. s., a městských částí hlavního města Prahy s podporou Ministerstva vnitra ČR. Projekt má informační a vzdělávací charakter, se zaměřením na zvýšení povědomí o pravidlech a postupech bezpečného užívání moderních technologií především dětmi a mládeží, rodiči, profesionály v oblasti školství a práce s mládeží, zástupci policie a sociálních a odborných pracovníků, a seniory.[287]

Praha bezpečně online 2017

Do projektu Praha bezpečně online 2017 jsou zapojeny městské části Praha 6, Praha 7 a Praha 14. Projekt navazuje na předchozí úspěšné ročníky a snaží se rozšiřovat cílové skupiny a u všech těchto skupin zvyšovat uživatelskou internetovou gramotnost. V rámci projektu Praha bezpečně online 2017 proběhne na základních školách spravovaných danými městskými částmi celkem sto devadesát dva kurzů primární prevence.[288] Témata seminářů pro základní školy jsou následující:

- ***Počítač nejen na počítání***
- ***Letem světem internetem***
- ***Co nám může hrozit na internetu*** – ochrana soukromí, nastavení mobilního telefonu a jednotlivých aplikací, techniky blokování komunikace
- ***Co je to, když se řekne kyberšikana*** – typy a příčiny kyberšikany, dopady kyberšikany, prožívání oběti, právní souvislosti, prevence, obrana a pomoc

[286] *Senioři bezpečně online* [online]. [cit. 9.12.2017]. Dostupné z: https://seniori.saferinternet.cz/
[287] *Praha bezpečně online.* [online]. [cit. 2.12.2017]. Dostupné z: https://praha.saferinternet.cz/index.php
[288] Tamtéž.

- ***Facebook a jiné sítě*** – sociální sítě, specifická rizika, možnosti profilu, nastavení soukromí, reklama, hry, virtuální přátelství, kybergrooming, prevence, obrana a pomoc
- ***Nebuď naháč na internetu*** – sexting, jiný škodlivý, potenciálně ohrožující, či nezákonný obsah, vytváření, publikace a sdílení, prevence, obrana a pomoc
- ***(Ne)Bezpečný mobil*** – ochrana soukromí, nastavení mobilního telefonu a jednotlivých aplikací, rizika lokačních služeb a služeb připojení, antivir, bezpečná hesla
- ***Když je selfie trestným činem (Sexting)*** – sexting, webcamsex, dětská pornografie, jiný škodlivý obsah, kyberšikana, prevence, obrana a pomoc

Praha 6 bezpečně online 2017: komunitní prevence kybernetické kriminality

Městská část Prahy 6 realizuje v roce 2017 šestý ročník komunitního vzdělávacího projektu zaměřeného na prevenci kyberkriminality. Cílovými skupinami jsou: nejmladší žáci základních škol, a to z prvních až třetích tříd; rodiče, jelikož právě ti by měli ovlivňovat chování svých dětí v kyberprostoru; pedagogičtí pracovníci a další odborníci pracující s dětmi a mládeží; a senioři. Tři nosné aktivity projektu byly stanoveny následovně:

- ***Preventivně vzdělávací semináře pro žáky prvního stupně základních škol*** – Cílem seminářů pro žáky základních škol je zvýšit povědomí o bezpečném a etickém užívání internetu a možnostech pomoci v krizových situacích. Z praxe vyplývá, že s prevencí rizik kyberprostoru by se mělo začít ve stejnou dobu, kdy děti začínají technologie užívat, proto je projekt v roce 2017 zaměřen především na děti z prvních až třetích tříd. Na téma online bezpečnosti proběhne na základních školách provozovaných městskou částí Praha 6 celkem sedmdesát dva seminářů s jednohodinovou dotací.
- ***Osvětové semináře pro seniory „Bezpečný internet pro seniory“*** – Semináře pro seniory jsou zaměřeny na osvětu v oblasti ochrany osobnosti a ochrany osobních údajů, elektronického bankovnictví a online nakupování se zaměřením na znaky podvodného jednání. Semináře jsou realizovány ve čtyř turnusech po třech lektorských hodinách ve spolupráci se Senior akademií Prahy 6.

- ***Informační a kazuistické semináře pro odborníky*** – Odborné semináře pro sociální pracovníky a preventisty z řad veřejné správy, policistů a školních metodiků jsou zaměřeny na nejnovější trendy kybernetické bezpečnosti.[289]

Praha 7 bezpečně online 2017: prevence kybernetické kriminality

Městská část Prahy 7 realizuje v roce 2017 pátý ročník projektu prevence kyberkriminality. Cílovými skupinami jsou nejen žáci všech ročníků základních škol a senioři, ale nově i živnostníci a podnikatelé a malých až středních firem. Aktivity projektu Praha 7 stanovila následovně:

- ***Preventivně vzdělávací semináře pro žáky základních škol*** – Projekt je určen pro žáky všech ročníků základních škol zřizovaných městskou částí Praha 7. Celkem se jedná o třicet pět seminářů s jednohodinovou dotací se zaměřením na rizika a hrozby, které lze potkat v online světě, účinné předcházení těmto rizikům, chování v ohrožujících situacích a možnosti pomoci dospělých.
- ***Preventivně vzdělávací semináře pro poslední ročník mateřské školy*** – Cílem této aktivity je vytvořit výukový a metodický materiál v oblasti užívání a chápání technologií dětmi v mateřských školách, a tím poskytnout mateřské škole pomůcky pro vzdělávání pedagogů i rodičů svých žáků.
- ***Implementace standardů bezpečné online komunikace eSafety Label do škol***[290]
- ***Osvětové semináře pro seniory „Bezpečný internet pro seniory“ -*** Semináře pro seniory a veřejnost jsou zaměřeny na osvětu v oblasti ochrany osobnosti a ochrany osobních údajů, elektronického bankovnictví a online nakupování se zaměřením na znaky podvodného jednání. Semináře jsou realizovány ve čtyř turnusech po třech lektorských hodinách ve spolupráci se Senior akademií Prahy 7.
- ***Příprava výukových pomůcek a publicita*** – využívání materiálů na webu projektu bezpečně online.[291]

[289] *Praha 6 bezpečně online.* [online]. [cit. 2.12.2017]. Dostupné z: https://praha.saferinternet.cz/index.php/praha-6-bol

[290] Viz výše v kap. 7.

[291] *Praha 7 bezpečně online.* [online]. [cit. 2.12.2017]. Dostupné z: https://praha.saferinternet.cz/index.php/praha-7-bol

Praha 14 bezpečně online 2017: komunitní prevence kybernetické kriminality

Projekt se na Praze 14 zaměřuje na žáky základních škol, pracovníky s mládeží a sociální pracovníky, a seniory. Cílem je zvýšit povědomí o rizicích internetu a moderních technologií. Aktivity byly stanoveny následovně:

- ***Primární prevence pro žáky základních škol*** – Projekt je určen pro žáky třetích až devátých tříd na všech šesti základních školách městské části Praha 14. Celkem se jedná o osmdesát pět seminářů s dvouhodinovou dotací se zaměřením na rizika internetu, ochranu osobnosti, právní povědomí a internetovou gramotnost. Žáci se dozvědí, jaké hrozby lze potkat v online světě, jak jim účinně předcházet, jak se chovat v ohrožujících situacích a jak požádat o pomoc.
- ***Odborný seminář pro pracovníky s mládeží a sociální pracovníky*** – Odborným seminářem je osmihodinový akreditovaný program prevence kyberkriminality a řešení internetového násilí se zaměřením na nejnovější hrozby v kyberprostoru. Projekt zahrnuje prezenční školení, metodické a výukové materiály.
- ***Odborný seminář pro seniory*** – Projekt je realizován jako jeden podvečerní informační seminář pro seniory a veřejnost se zaměřením na využívání bezpečnostních nástrojů a uvědomělé jednání v kyberprostoru.[292]

[292] *Praha 14 bezpečně online.* [online]. [cit. 2.12.2017]. Dostupné z: https://praha.saferinternet.cz/index.php/praha-14-bol

Závěr

Kriminalita je nejzávažnějším negativním společenským jevem, a proto je třeba jí věnovat dostatečnou pozornost včetně personální kapacity a finanční podpory. Vzhledem k tomu, že je kriminalita dynamickým jevem v čase i místě, pak je třeba brát v úvahu vývoj kriminogenních faktorů. A ani teoretická systematizace prevence kriminality není pouhým seznamem pojmů, nýbrž určuje osnovu preventivním opatřením, určeným danému okruhu adresátů a cílovým objektům.

Současné mezinárodní zaměření prevence kriminality spočívá v usilování o přijetí komplexních a inkluzivních národních programů a projektů v oblasti prevence kriminality a trestní justice, zohledňujících prvotní příčiny kriminality i podmínky umožňující nebo usnadňující její vznik a rozvoj; zaměření se na problematiku dětí a mládeže, a to především na význam ochrany dětí před všemi formami násilí, vykořisťování a zneužívání, v souladu s relevantními mezinárodními dokumenty včetně Úmluvy o právech dítěte, či Modelových strategií a praktických opatření OSN pro odstranění násilí na dětech v oblasti prevence kriminality a trestní justice; posilování rovnosti před zákonem vedoucí k potlačení diskriminace a nesnášenlivosti, a zároveň respektování genderových specifik zejména v oblasti prevence kriminality a zacházení s pachatelem; rozvíjení programů pro vězněné související s prevencí recidivy, a tedy se zaměřením na resocializaci, reintegraci, vzdělání a práci; a přezkoumání trestní politiky s ohledem na řešení otázky přeplněnosti věznic a podpory využívání alternativních trestů.

Zároveň prevence kriminality na evropské úrovni upřednostňuje preventivní projekty vycházející z lokálních či regionálních bezpečnostních auditů, úzkou spolupráci státní správy a samosprávy a neziskového sektoru, podporu kamerových dohlížecích systémů a efektivního bezpečnostního managementu ve městech, podporu výzkumu v oblasti prevence kriminality, intenzivní spolupráci evropských institucí zabývajících se prevencí kriminality, spolupráci a podporu národních a lokálních autorit v oblasti prevence kriminality a pořádání odborných konferencí na téma účinné prevence kriminality.

Za posledních několik let se rozvíjí těchto pět forem kriminality: pirátství, kyberkriminalita, sexuální zneužívání dětí, trestná činnost proti životnímu prostředí a obchodování s kulturními

statky. Přičemž prevence a potírání nových a vznikajících forem trestné činnosti i předvídání vývoje kriminality je poměrně náročný úkol. Hnací faktory, jako tempo technologického vývoje a postupující globalizace, vytvořily nové hodnoty, umožnily vznik nových vazeb mezi potenciálními oběťmi a pachateli, a prostředky anonymizace snížily riziko odhalení. Výsledkem není pouze zrod nových forem trestné činnosti, ale i renesance historických forem kriminality, například moderní pirátství.

Pro prevenci nově vznikajících forem kriminality je klíčová informovanost, nejen mezi potenciálními obětmi, ale i dalšími subjekty jako jsou odborní a pedagogičtí pracovníci. Proto vlády i instituce ze soukromého sektoru informují o indikátorech jednotlivých typů kriminality. U kyberkriminality se setkáváme s doporučeními ohledně uvědomělého chování v kyberprostoru, včetně prostředků ochrany, jakými jsou například silná hesla. Informační kampaň je také vedena vůči potenciálním pachatelům, zejména se jedná o sdělení ohledně kriminalizace určitého jednání se snahou odradit především mladistvé od zapojení se do skupin páchajících trestnou činnost. Jak již bylo zmíněno výše, moderní technologie nejsou pouze hrozbou a prostředkem páchání kriminality, ale mohou a měli by být využívány i u preventivních přístupů, jako je zabezpečování nebo sledování potenciálních cílů trestné činnosti, nebo jednoduše přenesením informačních a osvětových kampaní na sociální sítě.

Česká republika má zakotvený stabilní systém prevence kriminality. Vybudovaný systém rozvíjí, posiluje spolupráci, kompetence a kapacity relevantních partnerů, rozšiřuje prostor pro působení dobrovolníků při zajišťování bezpečnosti a veřejného pořádku, přičemž se opírá rovněž o mezinárodní spolupráci a vědecké poznatky. Prevence kriminality je v České republice organizována na meziresortní, resortní a místní úrovni a subjekty prevence kriminality řadíme podle působení na republikové, krajské a lokální úrovni. Policejní prevence kriminality a zapojení České republiky do mezinárodní spolupráce na poli prevence kriminality jsou nedílnou součástí tohoto systému.

Nejdynamičtěji se rozvíjející nová forma kriminality je kybernetické trestná činnost. Kyberkriminalita není nutně odborným právním termínem, ale jde spíš o souhrnné označení pro soubor skutků páchaných v kyberprostoru, respektive páchaných s využitím počítačových systémů nebo proti nim. Rozlišujeme kyberkriminalitu vlastní, tedy trestné činy proti

důvěrnosti, integritě a dostupnosti počítačových dat či systémů, jako je trestný čin neoprávněný přístup k počítačovému systému a nosiči informací (§230 TZ), a obecnou kriminalitu páchanou prostředky moderních technologií.

V prostředí sociálních sítí lze spáchat většinu forem kyberútoků. Nejrizikovějšími formami komunikace na sociálních sítích jsou kybergrooming, kyberstalking, kyberšikana a sexting, který může mimo jiné vést k výrobě a distribuci dětské pornografie. Základní poučkou při prevenci kyberútoku na sociálních sítích by mohlo být – Nesdílejte osobní a citlivé údaje s neznámými lidmi a nepodceňujte příznaky rizikové komunikace. Pokud to rozvedeme, tak se dostaneme k možnostem nastavení soukromí na sociálních sítích, k zabezpečí zařízení, ze kterých na sociální sítě přistupujeme, nastavení systému vlastních bariér při virtuální komunikaci, a uvědomování si rizik spojených se sdílením informací. Prevence kyberkriminality na sociálních sítích vychází z informovanosti veřejnosti o rizicích a nástrahách neuvědomělého používání informačních technologií. Významným opatřením primární prevence kyberkriminality je také začlenění témat spojených s rizikovou virtuální komunikací do školních osnov. Velmi důležitým nástrojem ochrany dětí v kyberprostoru je fungující komunikace mezi dítětem a rodičem.

Jedním z celorepublikových programů prevence kyberkriminality s významným dosahem je Safer Internet CZ, který se zaměřuje zejména na děti a mladé lidi, cílí ovšem i na další specifické skupiny, jakými jsou odborní sociální a pedagogičtí pracovníci, či senioři. Vlajkovou lodí projektu je provoz národní platformy saferinternet.cz, na jejíž webových stránkách nalezneme výukové a metodické materiály, informace ohledně ochrany soukromí v kyberprostoru. Tyto webové stránky mimo jiné slouží i jako rozcestník pro jednotlivé dílčí projekty, kterými jsou online hotline STOPonline.cz, online helpline POMOConline.cz, Bezpečně online, Mladí proti nenávisti online, Senioři bezpečně online. Jedním z dílčích projektů je také lokálně zaměřený projekt Praha bezpečně online, respektive letošní Praha bezpečně online 2017.

Seznam použitých zdrojů

1. Seznam použité literatury

BERAN, Tanya a Qing LI. The Relationship between Cyberbullying and School Bullying. *Journal of Student Wellbeing.* [online]. December 2007, 1(2). s. 15-33. [cit. 11.12.2017]. Dostupné z: https://www.ojs.unisa.edu.au/index.php/JSW/article/view/172

ČÍRTKOVÁ, Ludmila. *Forenzní psychologie*. 3., upr. vyd. Plzeň: Aleš Čeněk, 2013. ISBN 978-80-7380-461-9.

ČÍRTKOVÁ, Ludmila. *Moderní psychologie pro právníky: [domácí násilí, stalking, predikce násilí]*. Praha: Grada, 2008. ISBN 978-80-247-2207-8.

ECK, John E., Ronald V. CLARKE. *Analýza kriminality v 60 krocích* [online]. Praha: Otevřená společnost, 2010. [cit. 10.12.2017]. ISBN: 978-80-87110-22-5. Dostupné z: http://www.popcenter.org/library/reading/PDFs/60steps_czech.pdf

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

GŘIVNA, Tomáš, Miroslav SCHEINOST a Ivana ZOUBKOVÁ. *Kriminologie*. 4., aktualiz. vyd. Praha: Wolters Kluwer, 2014. ISBN 978-80-7478-614-3.

HAVLÍČKOVÁ, Jana. *Krádež virtuálního majetku*. Praha, 2017. Bakalářská práce. Policejní akademie České republiky v Praze. Fakulta bezpečnostně právní. Katedra trestního práva.

CHOO, Kim-Kwang Raymond. *Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences.* [online]. Canberra: Australian Institute of Criminology, c2009. [cit. 5.12.2017]. ISBN 978-1-921532-33-7. Dostupné z: http://www.aic.gov.au/media_library/publications/rpp/103/rpp103.pdf

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti. [online]. 2. aktualiz. vyd. Praha: AFCEA, 2015, s. 29. ISBN 978-80-7251-397-0. [cit. 5.12.2017]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/akce-udalosti/2193-vykladovy-slovnik-kyberneticke-bezpecnosti-druhe-vydani/

JIROVSKÝ, V. *Kybernetická kriminalita*. Nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. ISBN 978-80-247-1561-2.

KOLOUCH, Jan. *Cybercrime* [online]. Praha: CZ.NIC, 2016. [cit. 2.3.2017] ISBN 978-80-88168-18-8. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf

KOLOUCH, Jan a Petr VOLEVECKÝ. *Trestněprávní ochrana před kybernetickou kriminalitou.* Praha: Policejní akademie České republiky v Praze, 2013. ISBN 978-80-7251-402-1.

KOPECKÝ, Kamil. *Kybergrooming: nebezpečí kyberprostoru.* [online]. Olomouc: NET UNIVERSITY, 2010. [cit. 3.12.2017]. ISBN 978-80-254-7573-7. Dostupné z: https://www.e-bezpeci.cz/index.php/component/content/article/7-o-projektu/925-materialy

KOPECKÝ, Kamil. *Stalking a kyberstalking: nebezpečné pronásledování.* [online]. Olomouc: NET UNIVERSITY, 2010. [cit. 3.12.2017]. ISBN 978-80-254-7573-7. Dostupné z: https://www.e-bezpeci.cz/index.php/component/content/article/7-o-projektu/925-materialy

KREJČÍ, Veronika. *Kyberšikana: kybernetická šikana.* [online]. Olomouc: NET UNIVERSITY, 2010. ISBN 978-80-254-7791-5. [cit. 3.12.2017]. Dostupné z: https://www.e-bezpeci.cz/index.php/component/content/article/7-o-projektu/925-materialy

MELOY, Reid J. Stalking (Obsessional Following): A Review Of Some Preliminary Studies. *Aggression and Violent Behavior* [online]. 1996. 1(2), 147-162 [cit. 5.12.2017]. Dostupné z: http://drreidmeloy.com/wp-content/uploads/2015/12/1996_StalkingObsessi.pdf

MULLEN, Paul E., Michele PATHÉ a Rosemary PURCELL. The management of stalkers. *Advances in Psychiatric Treatment* [online]. 2001. 7(5). [cit. 11.12.2017]. ISSN 335-342. Dostupné z: http://apt.rcpsych.org/cgi/content/full/7/5/335

NOVOTNÝ, František; SOUČEK, Josef et al. Trestní právo hmotné. 3 vyd. Plzeň: Aleš Čeněk, 2010. 393 s. ISBN 978-80-7380-291-2.

NOVOTNÝ, Oto, Adolf DOLENSKÝ, Tomáš GŘIVNA, Jiří HERCZEG, Pavel ŠÁMAL, Michal TOMÁŠEK, Marie VANDUCHOVÁ a Rudolf VOKOUN. *Trestní právo hmotné*. 6., přeprac. vyd. Praha: Wolters Kluwer ČR, 2010. ISBN 978-80-7357-509-0.

SMEJKAL, Vladimír. *Kybernetická kriminalita.* Plzeň: Aleš Čeněk, 2015. ISBN 978-80-7380-501-2.

SPITTERS, Martijn, Stefan VERBRUGGEN a Mark VAN STAALDUINEN. Towards a comprehensive insight into the thematic organization of the ToR hidden services. *Intelligence and Security Informatics Conference (JISIC)* [online]. 2014. s. 220-223. [cit. 5.12.2017]. ISBN978-1-4799-6364-5. Dostupné z: http://ieeexplore.ieee.org/document/6975577/

SVATOŠ, Roman. *Prevence kriminality*. 2., aktualiz. vyd. České Budějovice: Vysoká škola evropských a regionálních studií, z.ú., 2016. ISBN 978-80-7556-009-4.

TURGEMAN-GOLDSCHMIDT, Orly. Meanings that Hackers Assign to their Being a Hacker. International Journal of Cyber Criminology (IJCC) [online]. 2008, 2(2), 382–396. [cit. 5.12.2017]. ISSN: 0974-2891. Dostupné z: https://pdfs.semanticscholar.org/f40f/32d6b63f9c55460938312946348b977f7f45.pdf

Willard, N. E. *Cyber Savvy: Embracing Digital Safety and Civility*. [ebook] Corwin Press, 2011. ISBN 9781452269672.

WINTERS, Georgia M., JEGLIC, Elizabeth L. Stages of Sexual Grooming: Recognizing Potentially Predatory Behaviors of Child Molesters. Deviant Behavior [online]. 2017,

38(6) [cit. 5.12.2017]. Dostupné z: http://www.tandfonline.com/doi/full/10.1080/01639625.2016.1197656

WOLAK, Janis, David FINKELHOR, a Kimberly J. MITCHELL. Online "Predators" and Their Victims: Myths, Realities, and Implications for Prevention and Treatment. American Psychologist [online]. February–March 2008 [cit. 5.12.2017]. Dostupné z: https://www.apa.org/pubs/journals/releases/amp-632111.pdf

ZAPLETAL, Josef. *Prevence kriminality*. 3., přeprac. vyd. Praha: PA ČR, 2008. ISBN 978-80-7251-270-6.

ZOUBKOVÁ, Ivana a kol. *Kriminologický slovník*. Plzeň: Aleš Čeněk, 2011. ISBN 978-80-7380-312-4.

ZOUBKOVÁ, Ivana a Marcela MOULISOVÁ. Kriminologie pro studenty doktorského studijního programu. Praha: PA ČR, 2014. ISBN 978-80-7251-409-0.

2. Seznam použitých internetových zdrojů

10 tipů, jak předcházet kyberšikaně. Bezpečně online [online]. [cit. 13.12.2017]. Dostupné z: https://bezpecne-online.saferinternet.cz/pro-rodice-a-ucitele/teenageri-a-komunikace/item/33-jak-predchazet-kybersikane-10-tipu-pro-rodice-a-ucitele-deti

@bezpecneonline. [online]. [cit. 9.12.2017]. Dostupné z: https://www.facebook.com/bezpecneonline/

@horkalinkacz [online]. [cit. 9.12.2017]. Dostupné z: https://www.facebook.com/horkalinkacz/

@internetova.ambasada. [online]. [cit. 9.12.2017]. Dostupné z: https://www.facebook.com/internetova.ambasada

@PomocOnline.cz. [online]. [cit. 9.12.2017]. Dostupné z: https://www.facebook.com/PomocOnline.cz/

@stoponlinecz [online]. [cit. 9.12.2017]. Dostupné z: https://www.facebook.com/stoponlinecz/

A European Strategy to deliver a Better Internet for our Children [online]. [cit. 9.12.2017]. Dostupné z: https://ec.europa.eu/digital-single-market/node/286

Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems ETS No. 189 [online]. [cit. 9.3.2017]. Dostupné z: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168008160f

Amanda Todd Legacy [online]. [cit. 11.12.2017]. Dostupné z: http://www.amandatoddlegacy.org/

BERSON, Ilene R. *Grooming Cybervictims: The Psychosocial Effects of Online Exploitation for Youth.* [online]. [cit. 11.12.2017]. Dostupné z: https://www.cs.auckland.ac.nz/~john/NetSafe/I.Berson.pdf

Better Internet for Kids [online]. [cit. 2.12.2017]. Dostupné z: https://www.betterinternetforkids.eu/

Better Internet for Kids – youth [online]. [cit. 2.12.2017]. Dostupné z: https://www.betterinternetforkids.eu/web/youth/home

Bezpečně na internetu [online]. [cit. 9.12.2017]. Dostupné z: http://o2.e-bezpeci.cz/

Bezpečně online [online]. [cit. 9.12.2017]. Dostupné z: https://bezpecne-online.saferinternet.cz/

CCPCJ [online]. [cit. 13.12.2017]. Dostupné z: http://www.unodc.org/unodc/en/commissions/CCPCJ/index.html

Centrum prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého [online]. [cit. 9.12.2017]. Dostupné z: http://www.prvok.upol.cz/index.php/cz/

CERD [online]. [cit. 13.12.2017]. Dostupné z: http://www.ohchr.org/EN/HRBodies/CERD/Pages/CERDIntro.aspx

CEDAW [online]. [cit. 13.12.2017]. Dostupné z: http://www.ohchr.org/EN/HRBodies/CEDAW/Pages/Introduction.aspx

Clickwrap Agreement. *Techopedia* [online]. [cit. 13.12.2017]. Dostupné z: https://www.techopedia.com/definition/4243/clickwrap-agreement

CLRAE [online]. [cit. 13.12.2017]. Dostupné z: https://www.coe.int/en/web/congress/home

Co je to Community policing [online]. [cit. 13.12.2017]. Dostupné z: http://www.policie.cz/clanek/co-je-to-community-policing.aspx

COE [online]. [cit. 13.12.2017]. Dostupné z: https://www.coe.int/en/web/portal/home

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Strategy for a Better Internet for Children. COM(2012) 196 final [online]. [cit. 9.12.2017]. Dostupné z: http://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/european-strategy-making-internet-better-place-children

Community Policing [online]. [cit. 3.12.2017]. Dostupné z: http://www.mvcr.cz/clanek/community-policing.aspx

Computer Security Incident Response Team [online]. [cit. 6.12.2017]. Dostupné z: http://www.csirt.org/

Convention on Cybercrime ETS No. 185 [online]. [cit. 9.3.2017]. Dostupné z: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

Creating a Better Internet for Kids. [online]. [cit. 2.12.2017]. Dostupné z: https://ec.europa.eu/digital-single-market/en/policies/better-internet-kids

Cyberbullying Research Center. [online]. [cit. 5.12.2017]. Dostupné z: https://cyberbullying.org/

Cyberbullying: What Is Cyberbullying? [online]. [cit. 5.12.2017]. Dostupné z: https://www.pacerteensagainstbullying.org/experiencing-bullying/cyber-bullying/

Cybercrime. [online]. [cit. 9.3.2017]. Dostupné z: https://www.techopedia.com/definition/2387/cybercrime

Cyberspace. [online]. [cit. 9.3.2017]. Dostupné z: https://www.britannica.com/topic/cyberspace

CZI [online]. [cit. 6.12.2017]. Dostupné z: https://www.czi.cz/

CZ.NIC [online]. [cit. 6.12.2017]. Dostupné z: https://www.nic.cz/

E-Bezpečí [online]. [cit. 9.12.2017]. Dostupné z: https://www.e-bezpeci.cz/

E-nebezpečí. [online]. [cit. 5.12.2017]. Dostupné z: http://www.e-nebezpeci.cz/

E-Nebezpečí pro učitele [online]. [cit. 9.12.2017]. Dostupné z: http://www.e-nebezpeci.cz/

Erotomaniac Morbidly Infatuated [online]. [cit. 11.12.2017]. Dostupné z: https://www.asianfanfics.com/story/view/552377/6/stalker-series-newer-ver-stalker-you-psycho-obsession

eSafety Label [online]. [cit. 9.12.2017]. Dostupné z: http://www.esafetylabel.eu/web/guest

eSafety Label (CZ) [online]. [cit. 9.12.2017]. Dostupné z: https://esafetylabel.saferinternet.cz/

EU [online]. [cit. 13.12.2017]. Dostupné z: http://europa.eu/

EUCPN [online]. [cit. 13.12.2017]. Dostupné z: http://eucpn.org/

Facebook murderer who posed as teenager to lure victim jailed for life. *The Guardian* [online]. 2010. [cit. 11.12.2017]. Dostupné z: https://www.theguardian.com/uk/2010/mar/08/peter-chapman-facebook-ashleigh-hall

From a Safer Internet to a Better Internet for Kids [online]. [cit. 9.12.2017]. Dostupné z: https://ec.europa.eu/digital-single-market/en/content/safer-internet-better-internet-kids

GJURIČOVÁ, Jitka. O prevenci kriminality. Prevence kriminality [online]. [cit. 12.12.2017]. Dostupné z: http://www.prevencekriminality.cz/prevence-kriminality/teoreticky-uvod/

Google Centrum pro bezpečnost [online]. [cit. 9.12.2017]. Dostupné z: https://www.google.cz/intl/cs/safetycenter/

'I WILL DRIVE YOU TO KILL YOURSELF' Sick internet paedophile gets 10-year sentence for blackmailing children into performing explicit webcam shows after at least one of his victims commits suicide. *The Sun* [online]. 2017. [cit. 11.12.2017]. Dostupné z: https://www.thesun.co.uk/news/3109867/sick-internet-paedophile-gets-10-year-sentence-for-blackmailing-children-into-performing-explicit-webcam-shows-after-at-least-one-of-his-victims-commits-suicide/

ICT. *Tech terms* [online]. [cit. 14.12.2017]. Dostupné z: https://techterms.com/definition/ict

INHOPE [online]. [cit. 3.12.2017]. Dostupné z: http://www.inhope.org/gns/home.aspx

KOPECKÝ, Kamil. *Nebezpečí zvané kybergrooming I.* In: Metodický portál inspirace a zkušenosti učitelů [online]. 2010. [cit. 2.12.2017]. Dostupné z: https://clanky.rvp.cz/clanek/s/Z/9741/NEBEZPECI-ZVANE-KYBERGROOMING-I.html/#6a

Kybergrooming a kyberstalking: metodický materiál pro pedagogické pracovníky [online]. Národní centrum bezpečnějšího internetu, 2012. [cit. 13.12.2017]. Dostupné z: http://www.ncbi.cz/category/6-metodiky-ucebni-materialy

Kyberšikana. *CO DĚLAT, KDYŽ – INTERVENCE PEDAGOGA: Rizikové chování ve školním prostředí – rámcový koncept* [online]. [cit. 13.12.2017]. Dostupné z: www.msmt.cz/uploads/Priloha_7_Kybersikana.doc

Kyberšikana ve školním prostředí: metodický materiál pro pedagogické pracovníky [online]. Národní centrum bezpečnějšího internetu, 2012. [cit. 13.12.2017]. Dostupné z: http://www.ncbi.cz/category/6-metodiky-ucebni-materialy

Linka bezpečí [online]. [cit. 6.12.2017]. Dostupné z: https://www.linkabezpeci.cz/

Mapy budoucnosti. *Prevence kriminality* [online]. [cit. 12.12.2017]. Dostupné z: http://www.prevencekriminality.cz/projekty/mapy-budoucnosti/

Mapa kriminality [online]. [cit. 12.12.2017]. Dostupné z: http://www.mapakriminality.cz/ a http://www.czechcrime.org

Materiály pro podporu výuky. *E-Bezpečí* [online]. [cit. 14.12.2017]. Dostupné z: https://www.e-bezpeci.cz/index.php/component/content/article/7-o-projektu/925-materialy

MERRITT, Marian. Straight Talk About Cyberstalking. *Norton* [online]. [cit. 5.12.2017]. Dostupné z: https://us.norton.com/cyberstalking/article

Methods of Online Predators. [online]. [cit. 5.12.2017]. Dostupné z: https://www.webroot.com/us/en/home/resources/tips/cyberbullying-online-predators/safety-methods-of-online-predators

Metodika pro poskytování dotací ze státního rozpočtu na realizaci aktivit v oblasti prevence rizikového chování v období 2013–2018 [online]. [cit. 12.12.2017]. Dostupné z: http://www.msmt.cz/vzdelavani/socialni-programy/dotacni-program-pro-oblast-prevence-2013-2018

Metodické dokumenty (doporučení a pokyny). [online]. [cit. 2.12.2017]. Dostupné z: http://www.msmt.cz/vzdelavani/socialni-programy/metodicke-dokumenty-doporuceni-a-pokyny

Mladí proti nenávisti online [online]. [cit. 9.12.2017]. Dostupné z: https://protinenavisti.saferinternet.cz/

Multiannual Strategy for the European Crime Prevention Network [online]. [cit. 13.12.2017]. Dostupné z: http://eucpn.org/sites/default/files/content/download/files/mas_2016-2020_final_version.pdf

Národní CSIRT České republiky [online]. [cit. 6.12.2017]. Dostupné z: https://csirt.cz/

Národní strategii primární prevence rizikového chování dětí a mládeže na období 2013–2018 [online]. [cit. 12.12.2017]. Dostupné z: http://www.msmt.cz/file/28077

NCBI [online]. [cit. 6.12.2017]. Dostupné z: http://www.ncbi.cz/

Nebezpečné pronásledování. *Bílý kruh bezpečí* [online]. [cit. 5.12.2017]. Dostupné z: https://www.bkb.cz/pomoc-obetem/trestne-ciny/nebezpecne-pronasledovani/

Několik tipů na ochranu před kybergroomingem. *Bezpečně online* [online]. [cit. 11.12.2017]. Dostupné z: https://bezpecne-online.saferinternet.cz/pro-rodice-a-ucitele/teenageri-a-komunikace/item/36-jak-muzete-prispet-k-tomu-aby-se-vase-dite-nestalo-obeti-kybergroomingu

No Hate Speech Movement [online]. [cit. 9.12.2017]. Dostupné z: http://www.nohatespeechmovement.org/

NoBullying.com. [online]. [cit. 5.12.2017]. Dostupné z: https://nobullying.com/

Norton Cybercrime Report 2012. [online]. [cit. 5.12.2017]. Dostupné z: http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

Norton Cybersecurity Insights Report 2016. [online]. [cit. 5.12.2017]. Dostupné z: https://us.norton.com/norton-cybersecurity-insights-report-global

O projektu – Centrum bezpečnějšího internetu (SIC CZ). [online]. [cit. 2.12.2017]. Dostupné z: https://www.saferinternet.cz/info-o-nás/o-nás.html

OHCHR [online]. [cit. 13.12.2017]. Dostupné z: http://www.ohchr.org/EN/pages/home.aspx

OSN [online]. [cit. 13.12.2017]. Dostupné z: http://www.osn.cz/

PACER's National Bullying Prevention Center. [online]. [cit. 5.12.2017]. Dostupné z: https://www.pacerteensagainstbullying.org/

POMOConline.cz [online]. [cit. 9.12.2017]. Dostupné z: https://pomoconline.saferinternet.cz/

Praha bezpečně online. [online]. [cit. 2.12.2017]. Dostupné z: https://praha.saferinternet.cz/index.php

Praha 6 bezpečně online. [online]. [cit. 2.12.2017]. Dostupné z: https://praha.saferinternet.cz/index.php/praha-6-bol

Praha 7 bezpečně online. [online]. [cit. 2.12.2017]. Dostupné z: https://praha.saferinternet.cz/index.php/praha-7-bol

Praha 14 bezpečně online. [online]. [cit. 2.12.2017]. Dostupné z: https://praha.saferinternet.cz/index.php/praha-14-bol

Prevence kriminality [online]. [cit. 11.12.2017]. Dostupné z: http://www.prevencekriminality.cz/

Příručka pro rodiče: jak zajistit bezpečnost dětí na internetu [online]. [cit. 11.12.2017]. Dostupné z: http://www.ncbi.cz/category/6-metodiky-ucebni-materialy

Republikový výbor pro prevenci kriminality. [online]. [cit. 2.12.2017]. Dostupné z: http://www.mvcr.cz/clanek/rvppk-republikovy-vybor-pro-prevenci-kriminality.aspx

Safer Internet CZ: Safer Internet CZ – stručný popis projektu. [online]. [cit. 2.12.2017]. Dostupné z: http://www.ncbi.cz/evropska-komise/safer-internet-cz.html

Saferinternet.cz [online]. [cit. 2.12.2017]. Dostupné z: https://www.saferinternet.cz/

Senioři bezpečně online [online]. [cit. 9.12.2017]. Dostupné z: https://seniori.saferinternet.cz/

Sexting a rizikové seznamování českých dětí v kyberprostoru (výzkumná zpráva) [online]. 2017. [cit. 13.12.2017]. Dostupné z: https://www.e-bezpeci.cz/index.php/tiskove-zpravy/1246-vyzkum-sexting-2017

Sexting.cz [online]. [cit. 13.12.2017]. Dostupné z: www.sexting.cz

Seznam se bezpečně [online]. [cit. 9.12.2017]. Dostupné z: https://www.seznamsebezpecne.cz/

Sheeplive. [online]. [cit. 2.12.2017]. Dostupné z: http://www.sheeplive.eu/

Sheeplive – CZ. [online]. [cit. 3.12.2017]. Dostupné z: http://cz.sheeplive.eu/

Sheeplive – Základné informácie. [online]. [cit. 3.12.2017]. Dostupné z: http://sk.sheeplive.eu/o-projekte/zakladne-informacie

Slovník. *Bezpečně online* [online]. [cit. 14.12.2017]. Dostupné z: https://bezpecne-online.saferinternet.cz/slovnik

Slovník základních výrazů online bezpečnosti. [online]. [cit. 2.12.2017]. Dostupné z: https://bezpecne-online.saferinternet.cz/slovnik

Soud poslal muže za zneužívání chlapců na osm let do vězení. *ČT24* [online]. [cit. 11.12.2017]. Dostupné z: http://www.ceskatelevize.cz/ct24/domaci/1422179-soud-poslal-muze-za-zneuzivani-chlapcu-na-osm-let-do-vezeni

Soutěž o Nejlepší projekt prevence kriminality na místní úrovni za rok 2017 [online]. [cit. 5.12.2017]. Dostupné z: http://www.mvcr.cz/clanek/zname-nejlepsi-projekty-prevence-kriminality.aspx

Stalking. *Česká televize* [online]. [cit. 5.12.2017]. Dostupné z: http://www.ceskatelevize.cz/porady/10303355531-stalking/

stopbullying.gov. [online]. [cit. 5.12.2017]. Dostupné z: https://www.stopbullying.gov/

STOPonline.cz [online]. [cit. 6.12.2017]. Dostupné z: https://www.stoponline.cz/stoponline/

STOPonline.cz. *Google Play* [online]. [cit. 9.12.2017]. Dostupné z: https://play.google.com/store/apps/details?id=cz.nic.saferinternet

The 17 Lures Predators May Use to Exploit Children. [online]. [cit. 5.12.2017]. Dostupné z: http://www.ortv.org/Charter/17_lures_predators_may_use.htm

The Digital Skills and Jobs Coalition. [online]. [cit. 2.12.2017]. Dostupné z: https://ec.europa.eu/digital-single-market/en/digital-skills-jobs-coalition

Top 15 Most Popular Social Networking Sites and Apps [online]. November 2017. [cit. 13.12.2017]. Dostupné z: https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/

TŮMOVÁ, Štěpánka. Stalking – Stolkérství – Nová forma psychického teroru. *Asociace forenzních psychologů* [online]. [cit. 12.12.2017]. Dostupné z: http://afp.wz.cz/clanky.doc/Stalking.doc

UN [online]. [cit. 13.12.2017]. Dostupné z: http://www.un.org/

United Nations Manual on the prevention and control of computer-related crime. [online]. [cit. 9.3.2017]. Dostupné z: http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Guide.pdf

UNODC [online]. [cit. 13.12.2017]. Dostupné z: http://www.unodc.org/unodc/index.html

UNODC Cybercrime Repository [online]. [cit. 11.12.2017]. Dostupné z: https://www.unodc.org/cld/v3/cybrepo/

Virtuální nápadník – preventivní film o stalkingu. *E-Bezpečí* [online]. [cit. 5.12.2017]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/stalking-a-kyberstalking/928-virtualni-napadnik-preventivni-film-o-stalkingu

VLACHOVÁ, Marta. *E-Bezpeci: Trestná činnost spojená s internetovou kriminalitou.* [online]. [cit. 5.12.2017]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/dali-rizika/148-226

VOKROUHLÍKOVÁ Kateřina a Zuzana PRŮCHOVÁ. *Naháči a prdeláči – fotky jen pro rodinu!* [online]. [cit. 5.12.2017]. Dostupné z: https://blog.nic.cz/2016/08/16/nahaci-a-prdelaci-fotky-jen-pro-rodinu/

Vyhlášení Programu prevence kriminality na rok 2017 [online]. [cit. 5.12.2017]. Dostupné z: http://www.mvcr.cz/clanek/vyhlaseni-programu-prevence-kriminality-na-rok-2017.aspx

Vyhlášení Programu Ministerstva vnitra v oblasti prevence kriminality na rok 2018 [online]. [cit. 5.12.2017]. Dostupné z: http://www.mvcr.cz/clanek/prevence-kriminality-v-resortu-ministerstva-vnitra.aspx

Výkladový slovník kybernetické bezpečnosti [online]. [cit. 13.12.2017]. Dostupné z: https://www.govcert.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf

What is a click wrap agreement? [online]. [cit. 9.3.2017]. Dostupné z: https://www.techopedia.com/definition/4243/clickwrap-agreement

Willard, Nancy. Educator's Guide to Cyberbullying and Cyberthreats [online]. 2004. [cit. 11.12.2017]. Dostupné z: https://education.ohio.gov/getattachment/Topics/Other-Resources/School-Safety/Safe-and-Supportive-Learning/Anti-Harassment-Intimidation-and-Bullying-Resource/Educator-s-Guide-Cyber-Safety.pdf.aspx

Zdraví 2020 – Národní strategie ochrany a podpory zdraví a prevence nemocí [online]. [cit. 12.12.2017]. Dostupné z: https://www.mzcr.cz/Verejne/dokumenty/zdravi-2020-narodni-strategie-ochrany-a-podpory-zdravi-a-prevence-nemoci_8690_3016_5.html

3. Seznam použitých právních předpisů

Usnesení vlády ČR ze dne 16.11.2016 č. 1007, Statut a Jednací řád Republikového výboru pro prevenci kriminality

Usnesení vlády ČR ze dne 3. listopadu 1993 č. 617, o projednání koncepce a programu prevence kriminality

Usnesení vlády ČR ze dne 25. ledna 2016 č. 66, o Strategii prevence kriminality v České republice na léta 2016 až 2020

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

Zákon č. 251/2016 Sb., o některých přestupcích, ve znění pozdějších předpisů

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

Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů

Zákon č. 128/2000 Sb., o obcích, ve znění pozdějších předpisů

Zákon č. 553/1991 Sb., o obecní policii, ve znění pozdějších předpisů

4. Seznam ostatních zdrojů

Osobní konzultace s Jiřím Palyzou, ředitelem NCBI, dne 1. 9. 2017

Zpětná vazba od žáků základních škol v rámci projektu Praha bezpečně online 2017

Seznam příloh