UNIVERZITA KARLOVA

Právnická fakulta

Mgr. et Mgr. Kateřina Kudrlová

Kriminalita spojená s využíváním nových médií dětmi

Disertační práce

Školitel: doc. JUDr. Tomáš Gřivna, Ph.D.

Studijní program: Teoretické právní vědy

Datum vypracování práce (uzavření rukopisu): 31.1.2019

Prohlašuji, že jsem předkládanou disertační práci vypracoval/a 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 poznámek pod čarou má 561 330 znaků včetně mezer.

disertant/disertantka

V Praze dne 31.1.2019

Na tomto místě bych ráda poděkovala panu docentu JUDr. Tomáši Gřivnovi, Ph.D., za jeho odborné vedení, cenné rady a vstřícný přístup v průběhu celého mého studia.

Obsah

ÚVOD

V posledních desetiletích došlo k výrazným změnám ve společnosti v souvislosti s rychlým rozvojem ICT. Tak jako zavedení telegrafu a telefonu zásadně relativizovalo časoprostorové komunikační bariéry, o současných moderních ICT lze říci totéž. Představit si pod nimi lze celou řadu zařízení a způsobů komunikace, jejichž potenciál využití dynamicky roste. Slouží především k uživatelským účelům, zejm. komunikaci mezi rozličnými subjekty: komunikaci mezi jednotlivými uživateli či skupinami uživatelů, ale také mezi uživatelem a zařízením i zařízeními mezi sebou navzájem. Slouží ovšem i k dalším účelům: sledování osob, věcí a komunikace, sběru osobních údajů a jiných dat atp. Vynechat samozřejmě nelze ani zvyšování uživatelského komfortu (např. prostřednictvím různých drobných technických zařízení zjednodušujících nebo zpříjemňujících běžné činnosti) a možností využití v řadě oblastí (zdravotnictví, školství, vojenství, výzkum vesmíru a další, napříč humanitními i přírodními vědami). Rychlý rozvoj a nástup každodenního samozřejmého využívání urychlilo postupné zpřístupnění moderních informačních a telekomunikačních technologií pro většinu obyvatel moderní společnosti jejich zlevněním a masovou výrobou.

ICT zahrnují především svět internetu[1] a mobilních technologií, souhrnně označovaný jako kyberprostor. Ten zahrnuje veškeré digitální technologie, resp. digitální zařízení pracující ve vzájemném propojení. Týká se proto např. problematiky webových kamer, bezdrátových zařízení, veřejných rejstříků, on-line uživatelských systémů (např. e-konto v knihovně), elektronického obchodování, bezpečnosti (od zabezpečení osobního počítače po národní bezpečnost), zdravotnictví (např. elektronická zdravotní karta pacienta nebo digitální léčebné prostředky), managementu, logistiky, výzkumu a vývoje a dalších.

Především ovšem kyberprostor slouží ke komunikaci, a to v soukromém či pracovním životě. Každodenní samozřejmostí je využívání emailu, instant messagingu (odesílání a přijímání zpráv v reálném čase) a SNS.[2] Běžné je využívání videohovorů (např. Skype) a videokonferencí, trendem jsou rozšiřující se jednosměrná videoposelství a sebepropagace (zejm. prostřednictvím nahrávání vlastních videí na Youtube).[3] Uvedených komunikačních kanálů pochopitelně hojně využívají také média a politické subjekty, a to pro přenos zpráv, veřejné diskuse, vlastní propagace atp. V neposlední řadě slouží virtuální realita jako

[1] Kromě internetu i dalších, lokálních sítí – firemní, univerzitní atp.
[2] SNS je „virtuální propojení skupiny lidí, umožňující mezi nimi sdílet různé typy informací“ (2011).
[3] Viz např. videoklip PSY – Gangnam style se svými 3.155.778.758 shlédnutími (k 30. květnu 2018), viz YOUTUBE (officialpsy, 2012).

platforma pro reklamu: běžnou, cílenou a virální marketing (využívá princip živelného šíření zpráv především prostřednictvím SNS). Vzhledem k tomu, že s využíváním moderních ICT doznaly tradiční komunikační způsoby značných změn, hovoří se v souvislosti s nimi o tzv. nových médiích, která umožňují propojení a vzájemnou komunikaci širokého spektra osob, kdy se stírá hranice mezi producentem a konzumentem, resp. autorem a publikem, neboť autoři sami jsou si navzájem zároveň publikem.

Kyberprostor vytváří určitou formu virtuálního světa, který je však zcela reálný ve svých důsledcích. Na první pohled se zdá jako vhodné přirovnání Mertonovo pravidlo sebenaplňujícího se proroctví, kdy se určitý neexistující jev v okamžiku, kdy jej dostatečné množství osob považuje za reálně existující, stává skutečným ve svých důsledcích.[4] Virtuální realita v tomto pojetí tvoří určitý paralelní svět ke skutečné, fyzicky existující realitě, který je skutečný ve svých důsledcích. Rozlišení mezi virtuálním a reálným světem se postupně stírá, kyberprostor se prolíná s realitou a stává se jí.[5]

Kyberprostor tak představuje nejen komunikační platformu, ale specifický svět s postupně se rozvíjejícími vlastními vztahy v rovině sociální, technologické, mocenské (regulace v oblasti kyberprostoru) i ekonomické. Nabízí široké možnosti využití, a zároveň skýtá prostor pro řadu protiprávních či jiným způsobem nežádoucích či škodlivých jednání.[6] Protože kyberprostor má svá specifika, odpovídá tomu i charakter kriminality s ním spojené[7] – kyberkriminality. Předně se jedná o časoprostorové rozpojení kyberprostoru existujícího a „žijícího“ vlastním životem nezávisle na vůli jednotlivce, „informace jsou dostupné kdykoliv a kdekoliv pouze v závislosti na připojení k síti“ (Gřivna, 2015 str. 336). Mnohdy také stačí jen velmi malé náklady k získání velkého vlivu, způsobení vysoké škody atp.[8]

Kyberkriminalita ve spojení s dětmi je pak zvláště aktuálním tématem, a to hned z několika důvodů. Tím nejmarkantnějším je soustavně stoupající počet uživatelů internetu nepochybně

[4] Principem sebenaplňujícího se proroctví se zabývali již antičtí Řekové a další (typickým příkladem je příběh o Oidipovi), byl to však právě R. K. Merton, kdo koncept rozpracoval podrobněji na základě konkrétní společenské situace (Merton, 1948).

[5] Výstižným příkladem takového fungování je virtuální svět Second Life, ve kterém uživatelé / hráči prostřednictvím svých tzv. avatarů spolupracují s ostatními uživateli v de facto paralelním virtuálním světě, kde mohou takto např. obchodovat a získaný obnos následně směnit za reálné zboží.

[6] Zároveň je však třeba doplnit, že ne každé protiprávní jednání je ze společenského hlediska a priori nežádoucí. Deviantní porušování norem na jednu stranu podrývá jejich autoritu, na druhou stranu může vést ke vzniku jiných, neformálních pravidel a nakonec může být předzvěstí změněné sociální situace vyžadující odpovídající zákonné změny (Giddens, 2000 str. 184).

[7] K tomu blíže viz kapitola Kyberkriminalita, jíž je autorka spoluautorkou v učebnici Kriminologie (Gřivna, 2015).

[8] Vč. „nákladů“ v podobě technologických znalostí útočníka, kterému může stačit i běžná uživatelská zdatnost.

jdoucí ruku v ruce s rostoucím počtem uživatelských míst.[9] Např. oproti roku 2008, kdy bylo v České republice zhruba 54 % uživatelů internetu (starších šestnácti let), v roce 2010 činil jejich podíl již téměř 62 % a čísla stále stoupají až po 79 % v roce 2017.[10] Lze předpokládat, že jejich množství dále poroste - na jedné straně stále roste počet prvouživatelů starších šestnácti let,[11] na straně druhé se přes hranici šestnácti let dostávají ti, kdo používají internet již od útlého věku (jejichž procentuální zastoupení taktéž roste).

Dalším významným fenoménem je rostoucí počet dětských uživatelů spolu s tím, jak se počítač stává běžným vybavením domácnosti, resp. spíše lze říci, že naopak děti patří k příčinám růstu počtu domácností s připojením k internetu. Tento trend dokumentuje fakt, že v roce 2010 při celkovém množství 56 % domácností s přístupem k internetu je poměr takových domácností bez dětí 47,2 %, zatímco domácností s dětmi majícími přístup k internetu je téměř 80 %.“[12] V roce 2013 pak již bylo domácností s připojením k internetu 67 %, resp. 57,4 % domácností bez dětí a celých 91,5 % domácností s dětmi v uplynulém roce 2017 pak plných 77 % domácností s internetem, vč. 71 % bezdětných domácností a téměř 100 % (96 %) domácností s alespoň jedním dítětem.

Tab. č. 1: podíl uživatelů internetu starších 16 let[13]

Rok	Množství uživatelů internetu starších 16 let v ČR v procentech	Celkový počet domácností s přístupem k internetu v procentech	Počet bezdětných domácností s přístupem k internetu v procentech	Počet domácností s dětmi s přístupem k internetu v procentech
2008	54	42	27	67
2009	56	49	39	76
2010	62	56	47	80
2011	66	62	53	84
2012	70	65	57	90
2013	70	67	57	92

[9] Uživatelskými místy míním např. vytváření různých internetových kaváren a dalších míst, která zpřístupňují internet blíže neurčenému počtu uživatelů, a zároveň stále dostupnější možnost přístupu na internet, zejm. prostřednictvím mobilního telefonu a využití Wi-Fi.
[10] K uvedeným statistickým údajům viz informace uvedené na webu Českého statistického úřadu pod heslem Informační společnost v číslech (Český statistický úřad).
[11] Tedy osob, které se učí vůbec s počítači zacházet, zejm. ze starších generací.
[12] Viz též (Lukášová, 2012 str. 8).
[13] Zdrojem informací Český statistický úřad – Informační společnost v číslech (Český statistický úřad)

2014	74	72	65	93
2015	76	73	65	94
2016	77	76	69	95
2017	79	77	71	96

Naléhavost problematiky pak vyvstává zejm. s ohledem na specifika a vývojové potřeby dětské psychiky, neboť v průběhu dětství i dospívání jsou dotyční „nezkušení, důvěřiví a otevření. Vývoj jejich možností bezprostřední komunikace se světem se rozvíjí v současné době rychleji než jejich psychická připravenost na setkání s možnými nebezpečími. Chybí jim vlastní zkušenost, zkušenost starších je nejen nepřenosná, ale z principu vzpoury proti starším ji často odmítají.“[14]

Zvláště ostře se jeví potřeba pozornosti věnované dětem v souvislosti s jejich pohybem v kyberprostoru ve světle tzv. digitální propasti (či digitálního rozdělení), tj. propastným rozdílem mezi uživateli a neuživateli moderních ICT. Záleží přitom na technologické dostupnosti kyberprostoru i na vlastních schopnostech dotyčného (vč. schopnosti, ochotě a možnosti osvojit si uživatelské dovednosti).[15] Zejm. stojí proti sobě mladší generace dětí a dospívajících, narodivše se již do světa digitálních technologií, jenž je jim díky tomu zcela vlastní, oproti generacím starším. Ty se s ním mnohdy sžívají poměrně nesnadno, a tudíž jim není vlastní ani přirozená obezřetnost a mnohdy nejsou schopni detekovat a předcházet hrozbám ve virtuálním prostředí a tuto schopnost předávat dalším generacím. Snaha o zmenšení digitální propasti je proto zcela na místě.[16]

Problematiku kyberkriminality lze nahlížet z mnoha různých úhlů pohledu a perspektivou několika různých oborů, z nichž každý přispívá k jejímu poznání odlišným způsobem. Z hlediska technologie informačních a komunikačních zařízení lze sledovat jejich vývoj a případné budoucí trendy, tedy především jakým způsobem vůbec fungují zařízení vzájemně

[14] Viz metodické materiály Národního centra bezpečnějšího internetu, z.s., pro projekt Škola bezpečného internetu, jehož byla autorka spoluřešitelkou, především kapitola Bezpečné a etické užívání internetu (k dispozici pouze pro Pardubický kraj, nepublikováno).

[15] Překážky mohou být různorodé: fyzický přístup k připojenému zařízení, finanční, sociodemografické (zejm. vzdělání, příjem a věk), kognitivní (úroveň informační gramotnosti), designové (dotýká se především osob se zdravotním postižením), institucionální, politické, kulturní - např. specifické jazykové prostředky kyberprostoru (2003).

[16] Mimoto jsou zde i jiné důvody hovořící ve prospěch zmenšování digitální propasti: ekonomická rovnost (např. informace o zaměstnání), sociální mobilita (digitální gramotnost jako předpoklad úspěšné kariéry), demokracie (ve smyslu participace mas obyvatel na rozhodování) a ekonomický růst, zejm. v rozvojových zemích (Internet World Stats).

spojená v kyberprostoru, jak spolu vzájemně komunikují, jak probíhá přenos dat a jaké jsou naopak jeho překážky, jakým způsobem je lze sledovat či o nich pořizovat záznam, jaké jsou aktuální trendy a pravděpodobný budoucí vývoj. Ze sociologického hlediska (resp. v kombinaci s psychosociálním prizmatem) lze pozornost upnout na vliv moderních ICT na společnost jako takovou a na dílčí skupiny osob. K možným zaměřením patří především komunikace, a to mezi jednotlivci navzájem, skupinami a jejich kombinacemi (skupiny mezi sebou, skupina vůči jednotlivci, jednotlivec vůči skupině), ale také se zohledněním proměny veřejného diskursu a možností být jeho aktivním účastníkem s reálným vlivem, vč. prostoru pro to „být slyšen“. Bez zajímavosti není ani tvorba různých skupin a jejich působení, bez zajímavosti pochopitelně nejsou ani sociodemografické údaje. Kriminologický pohled pak sleduje především kriminalitu spojenou s kyberprostorem. Zaměřuje se na samotná jednání, jejich podobu, prevalenci, příčiny, prevenci, pachatele a oběti. Dílčí problematikou je pak závislostní jednání ve spojení s internetem jakožto kriminologický faktor. Trestněprávní nauka sleduje právní postih příslušných společensky škodlivých jevů de lege lata i de lege ferenda a jeho vývoj na poli národním i mezinárodním.

Výčet by mohl pokračovat, nicméně výše uvedené považuji za stěžejní pro předkládanou práci.[17] Kromě samozřejmého studia odborné literatury si vypůjčím za tím účelem ze škály metod kriminologického výzkumu metodu historickou (technologický vývoj a s tím spojené některé typy útoků), analýzu statistických dat, případovou studii a typologickou metodu. [18] K získání dat využiji především studium a analýzu dokumentů: právních předpisů, výzkumných zpráv, ale i informací z médií a internetu aj. Dále pak vlastní výstupy z projektu IKSP a data získaná v jeho rámci.[19] Mimoto čerpám též z poznatků načerpaných účastí na řadě odborných konferencí věnovaných problematice kyberprostoru a kyberkriminality, vč. přípravy vlastních vystoupení.

Jako určité vodítko mi budou též do jisté míry vlastní zkušenosti a vzdělání. Spolu se studiem práva jsem absolvovala navazující magisterské studium sociologie na Fakultě sociálních věd a předtím bakalářské studium základů humanitní vzdělanosti na Fakultě humanitních studií Univerzity Karlovy v Praze. Coby dlouholetá lektorka a metodička Národního centra

[17] V průběhu magisterského studia práva na Právnické fakultě jsem úspěšně dokončila navazující magisterské studium sociologie na Fakultě sociálních věd (po předchozím bakalářském studiu základů humanitní vzdělanosti na Fakultě humanitních studií), vše na Univerzitě Karlově v Praze.

[18] Viz kapitola Kriminologický výzkum (spoluautoři Cejp. M. a Kudrlová, K.) v učebnici Kriminologie, viz (Gřivna, 2015).

[19] Především justiční a policejní statistiky dostupné prostřednictvím informačního systému CSLAV a na webu Policie ČR.

bezpečnějšího internetu, z.s., jsem lektorsky vedla mnoho odborných seminářů a besed zaměřených na chování dětí v kyberprostoru, zejm. pro učitele a sociální pracovníky, čerpám tedy i z jejich vyjádření (úhrnem stovky osob z různých regionů). Takové informace sice zdaleka nepředstavují reprezentativní data, nicméně to ani není jejich smyslem, tím je naopak získat představu o aktuálních trendech a přístupech různých skupin, o tom, co dotyční pociťují jako vyřčení hodné a jaké jsou jejich vlastní zkušenosti s kyberkriminalitou, ať už z pozice aktérů[20] či přihlížejících (např. spolužáci), a to alespoň v hrubých rysech bez aspirace na objektivní danost. Jakoukoliv případnou generalizaci je proto třeba vždy brát s výhradou této poznámky. Od roku 2016 úzce spolupracuji s IKSP v rámci dvoučlenného řešitelského týmu věnujícího se výzkumnému projektu Identifikace a posouzení druhů a trendů kriminality páchané prostřednictvím Internetu (výzkum IKSP). Pohybuji se v prostředí počítačů od útlého věku, vč. využívání internetu téměř od samých jeho počátků v rámci ČR. Sleduji tak postupnou proměnu způsobů komunikace v návaznosti na stále masovější využívání moderních ICT z pozice přelomové generace, která ještě pamatuje svět bez nich, a zároveň jí pohyb v kyberprostoru není cizí tak, jako je tomu u generací starších.

Práce si klade za cíl ověření dvou hypotéz. 1. mládež, tj. děti a mladiství jsou v online prostředí ohroženy kriminalitou; 2. mládež se v online prostředí dopouští provinění a činů jinak trestných.

Jak je uvedeno výše, hlavním obsahem práce je kyberkriminalita spojená s využíváním nových médií dětmi pojatá z různých úhlů pohledu. Pro pochopení některých specifik kyberkriminality jako takové se jeví nezbytným uvést několik slov k technologickému vývoji kyberprostoru, a to zejm. k fungování internetu, neboť právě Internet[21] je nejobvyklejší platformou kyberkriminality a některé jevy si lze bez jeho pochopení jen stěží představit či jim porozumět. Naopak se v duchu digitálních technologií zaměřených na „tady a teď" (jakkoliv je výraz „tady" v souvislosti s kyberprostorem zavádějícím) věnuje jen minimálně historickým souvislostem samotného vzniku internetu.[22] Nejprve se tedy věnuji v kapitole

[20] Útočník, oběť, „soudce" (např. ředitel školy rozhodující o kárném opatření), „vyšetřovatel" (např. pedagog zjišťující původce kyberšikany), „nápravce" (např. školní výchovný poradce pomáhající oběti kyberšikany) atd.

[21] Používám zde a dále v práci výraz „Internet" s velkým počátečním písmenem pro označení právě této sítě oproti jiným, více či méně lokálním sítím, které s Internetem mohou, ale také nemusí být propojeny. Při používání pojmu „internet" s malým počátečním písmenem označuje tento výraz Internet a k němu připojené další sítě a zařízení, vč. mobilních telefonů.

[22] Velmi zjednodušeně řečeno, jedním z popudů pro vznik Arpanetu, předchůdce Internetu, byly obavy o znemožnění komunikace v důsledku raketového útoku v rámci studené války mezi USA a SSSR vedoucí k vývoji principu decentralizovaného propojení komunikačních bodů; sdílení vědění a výzkumných poznatků mezi výzkumnými institucemi i jednotlivými výzkumníky pak sloužilo jako druhý hnací motor. Od prvního propojení několika počítačů v 60. letech 20. st. se vývoj rozběhl raketovým tempem přes používání DNS

Technická stránka kyberprostoru především internetu, a to pro nastínění fungování přenosu dat, potažmo digitalizovaného obsahu (relevantní zejm. pro sexting, kyberšikanu a sběr osobních údajů), a možná zneužití. Následuje převážně sociologický pohled na **Kyberprostor a nová média**, jejichž spojení proměňuje veřejný diskurs a rozděluje digitální domorodce a imigranty (relevantní např. pro sdílení obsahu a přístup mládeže k virtuálnímu prostředí, potažmo zejm. pro sexting a kyberšikanu). V podobném duchu pokračuje kapitola **Komunikace a identita** věnující se specifikům komunikace a utváření identity dětí a dospívajících ve vztahu k těm druhým v rámci kyberprostoru (relevantní zejm. pro zranitelnost online, potažmo kyberšikanu a kybergrooming). Kapitola **Digitální otisk a SNS** propojuje technickou stránku internetu se sebeprezentací, potažmo identitou (relevantní zejm. pro SNS coby zdroj zneužitelného obsahu). **Další kriminogenní a viktimogenní faktory** poukazují na možná rizika závislostí spojených s internetem (relevantní pro zranitelnost vůbec a např. kybergrooming) a specifickou roli avatara coby reprezentace uživatele ve virtuálním prostředí (relevantní zejm. pro zneužití avatara při kyberšikaně a napadení herního účtu). Právní pohled pokračuje kapitolou **Právní rámec kyberprostoru**, se zohledněním (zde i dále) trestněprávní oblasti.[23] **BTC a typy kyberkriminality** vysvětlují princip fungování BTC a nabízí vlastní členění kyberkriminality (relevantní zejm. pro anonymitu protiprávních transakcí online, vč. spojení s dětskou pornografií, a rámec kyberkriminality, v němž je zasazena i oblast ve vztahu k dětem). **Výzkum a publikace v rámci IKSP** představuje aktuální dílčí výsledky probíhajícího výzkumu IKSP, z nichž část se dotýká i mládeže coby pachatelů (relevantní pro počítačové trestné činy). **Děti v online prostředí jako oběti i pachatelé** uvádí některé další dosud nezmíněné aspekty vlastní pro pohyb dětí online relevantní coby kriminogenní/viktimogenní faktory. **Sexuální vykořisťování dětí** podává výklad o pornografii, vč. dětské, ve spojení s mládeží, o hojně praktikovaném sextingu a o kybergroomingu, které jdou obvykle ruku v ruce. Kyberšikana představuje nejpalčivěji vnímané téma samotnými dětmi a dospívajícími, naproti tomu **Násilí a hate crime** se jich tolik nedotýká, avšak radikalizace online je zřejmá. Na závěr zbývá několik slov pro oblast **Prevence** a její aktéry a vývojové trendy kyberkriminality vůbec.

---

v 80. letech a www v 90. letech až po první spuštění FB v roce 2004 a současný tzv. internet věcí.

[23] Věnuji se převážně hmotnému právu, procesněprávní úprava zahrnuje sama o sobě obsáhlou oblast, zejm. v souvislosti s vyhledáváním a zajišťováním důkazů (např. problematika domovní prohlídky ve vztahu k datům uloženým v cloudu nebo včasné a řádné zajištění důkazního prostředku v online prostředí), přeshraniční spoluprací v průběhu trestního řízení aj.

1. Technická stránka kyberprostoru[24]

Internet spočívá ve vzájemné komunikaci připojených zařízení prostřednictvím odesílání, přeposílání a přijímání informací v podobě dat rozdělených do tzv. packetů, s nejčastějším využitím tzv. TCP/IP.[25] Tzn. jakýkoliv datový přenos je rozdělen do řady samostatných a na sobě zcela nezávislých packetů, z nichž každý nese kromě vlastního částečného obsahu zprávy také další vrstvu dat, jejíž součástí je informace o odesílateli, adresátovi a o postavení daného packetu v rámci celého celku tak, aby mohl být v zařízení adresáta následně složen do původní podoby. Každý z packetů putuje zcela samostatně až do místa určení, přičemž rozložení zprávy do samostatných packetů umožňuje efektivní využití sítě díky rychlému posílání jednotlivých packetů vždy tou nejrychlejší cestou (Rouse).

Samotná komunikace jednotlivých zařízení probíhá prostřednictvím uzlových bodů (hub, switch, router). Tzv. hub plní funkci hvězdicovitého rozbočovače, který přijatou informaci rozesílá bez rozlišení na všechny jemu známé tzv. porty, což si lze představit jako brány vstupu určující, o jaký typ informace se jedná.[26] Naproti tomu switch již dokáže rozlišit tzv. MAC adresy[27] všech nejbližších zařízení a přiřadit je k jednotlivým portům, a tudíž předávanou informací nezatěžuje ostatní porty, k nimž informace nesměřuje (Webopedia, 2006). S ohledem na značný nárůst množství přenášených dat se v současnosti využívají převážně routery, které obvykle stojí mezi dvěma a více lokálními sítěmi, mezi lokální sítí či sítěmi a internetem a mezi jednotlivými segmenty internetu vůbec. Má přehled o veškeré komunikaci procházející přes něj a u každého packetu vidí, kam směřuje. V závislosti na tom ho poté nasměruje do žádoucích míst. V prvé řadě tak rozlišuje, zda packet přicházející např. z lokální sítě směřuje zpět do této sítě či dále prostřednictvím internetu.[28] Protože router slouží zároveň jako kontaktní bod mezi lokální sítí a internetem, bývá vybaven i firewallem a

[24] Část kapitoly textu byla zpracována jako součást soutěžní práce pro VIII. ročník SVOČ s názvem Kyberkriminalita a dokazování, autorka v rámci doktorandské trestněprávní sekce získala druhé místo (Kudrlová, 2015).

[25] Transmission Control Protocol / Internet Protocol.

[26] Např. příchozí email vstupuje prostřednictvím jiného portu než požadavek na poskytnutí služby (např. zobrazení webových stránek). Porty č. 0-1023 patří nejznámějším společnostem a službám jako Apple, MSN aj. (WhatIsMyIPAddress).

[27] Připojení k internetu vyžaduje síťové zařízení, přičemž jedinečnou MAC adresu přiděluje každému konkrétnímu síťovému zařízení výrobce již při výrobě. První část MAC adresy tvoří registrované číslo výrobce, druhou část sériové číslo konkrétního kusu. MAC adresa má relativně trvalý ráz, na rozdíl od IP adresy, nicméně i ji může uživatel změnit (wikiHow) aj.

[28] Představme si firmu zaměstnávající několik animátorů a další zaměstnance. Pro lepší zajištění ochrany dat a rychlejší vnitřní komunikaci firma využívá vlastní lokální síť, propojenou zároveň s internetem. Animátoři si mezi sebou zasílají velké množství dat, což celou lokální síť zpomaluje, neboť bez použití routeru každý ze zapojených počítačů zkoumá každou posílanou informaci. Pro zefektivnění komunikace stačí v takovém případě rozdělit síť na podsíť animátorů a podsíť ostatních a přidat router s příslušnými pokyny k rozdělování komunikace (Franklin, 2000).

případně další ochranou.[29] Router tedy nejprve rozliší, do jaké sítě packet zaslat, a následně jej zašle na cílovou adresu, ať už na konkrétní cílovou adresu nebo dalšímu routeru. Routery si zároveň vzájemně předávají informace o prostupnosti vlastní části sítě a zasílají každý jednotlivý packet vždy nejrychlejší cestou. Proto hlásí-li nějaký router větší zatížení a v důsledku toho nižší prostupnost jeho části sítě,[30] odesílající router zvolí cestu jinou. Takto může dojít i k situaci, kdy každý jednotlivý packet prochází jinou cestou, resp. přes jiné routery.

Aby mohly packety dorazit do cíle, potřebuje odesílající zařízení znát svoji a cílovou IP adresu.[31] Některé IP adresy jsou statické, a tedy stabilní, což může zajistit např. jejich lepší ochranu před vnějšími útoky (např. router dostane pokyn vpustit do své lokální sítě pouze komunikaci pocházející z konkrétních IP adres trvale přiřazených firemním počítačům). Dynamická IP adresa může naopak značně zkomplikovat snahu zpětně dohledat, k jakému konkrétnímu zařízení byla přiřazena v určitý čas.[32] Aby pak jakékoliv zařízení dokázalo určit cílovou IP adresu adresáta i svoji vlastní, využívá tzv. ARP a RARP protokoly, které mu (zjednodušeně řečeno) sdělují, k jakému fyzickému zařízení patří která IP adresa (Peterka, 1996). Uživatel sám může zjistit danou informaci jejím vyhledáním ve svém zařízení nebo jednoduše pomocí některé z řady internetových aplikací (ip-adress.com). Aby bylo možné k internetu se vůbec připojit, je nutné použít síťové zařízení (např. síťová karta v počítači). Každé takové zařízení má již při výrobě přidělenu tzv. MAC adresu, která je jedinečná a za normálních okolností se nemění (uživatel ji s použitím určitého softwaru může změnit, resp. maskovat za jinou adresu).

[29] Firewall reguluje prostupnost dat oběma směry. Zpravidla slouží jako kontrolní brána mezi různými sítěmi, ale může být i součástí antiviru. Vzhledem k častým malwarovým útokům v prostředí internetu např. sdružení CZ.NIC, správce domény cz a provozovatel národního CSIRT (Computer Security Incident Response Team), nabízí router Turris vybavený speciálním softwarem, který ve spolupráci s ostatními takovými routery blokuje dosud známé hrozby a zároveň detekuje nové (CZ.NIC).

[30] Např. z důvodu velkého datového přenosu v důsledku sledování Olympijských her online v konkrétním městě či státě.

[31] Každé zařízení přistupující k internetu má IP adresu, kterou mu přiděluje poskytovatel internetu jako veřejnou (neměnná, jednoznačně identifikuje koncového uživatele) nebo neveřejnou (tzv. dynamická neboli plovoucí). Je vždy jedinečná, může se však v různých časových intervalech (např. po týdnu, při ukončení připojení atp.) měnit. Jedno zařízení může mít současně přiřazeno více IP adres, ale žádná IP adresa se nevyskytuje současně u více zařízení.

[32] Dynamické IP adresy přiřazuje ISP ze souboru svých právě dostupných adres. Představme si společnost mající k dispozici 100 aut s různými SPZ, ale stejné značky i barvy a opatřených logem společnosti. Kdykoliv může za společností přijít její klient s žádostí o užití auta (žádost o přístup na internet). Společnost (ISP) mu obratem zapůjčí některé ze svých právě dostupných vozidel (přiřadí jeho zařízení IP adresu) a klient odjede (používá internet). Po tento čas ostatní lidé (uživatelé internetu) sice vidí daný vůz (vidí, kdo je poskytovatelem služby), ale již nerozpoznají, který klient právě vůz užívá (vidí IP adresu zařízení, ale tato je pouze dočasná). Jakmile auto vrátí (odpojí se od internetu), společnost má vůz opět k dispozici pro ostatní své klienty a je jen na ní, zda příště přidělí dotyčnému opět zcela identický nebo jiný vůz (Brandejsová, a další, 2012 str. 28).

V zájmu vytvoření uživatelsky vstřícného prostředí v rámci internetu vznikla služba / aplikace WWW (World Wide Web) fungující na bázi spolupráce internetových prohlížečů a serverů, přičemž výraz „server“ má několik významů. Může se jednat o software poskytující službu jiným programům ve stejném či dalších zařízeních. Zároveň se „server“ používá jako označení zařízení, které je určeno převážně k provozování serveru-softwaru (např. firemní server). V neposlední řadě pak jde o „webový server“ spočívající v softwaru poskytujícím na základě žádosti danou službu či informace tzv. klientovi, tj. internetovému prohlížeči, který ji dále zprostředkovává samotnému uživateli prostřednictvím zobrazení požadované informace (Rouse). Uživatel tedy nejprve zašle prostřednictvím internetového prohlížeče dotaz / požadavek směřovaný na danou IP adresu (např. zadání URL adresy), tento putuje přes routery až do cílové destinace, kde jej server rozpozná a odpoví na IP adresu, ze které požadavek vzešel.

Drtivá většina uživatelů internetu a www služeb nezná cílové IP adresy, zato však znají název serveru poskytujícího danou službu (např. www.seznam.cz). Aby bylo možné využívat webové servery v této jazykově přijatelné podobě, fungují v rámci internetu tzv. DNS překladače (Domain Name System) – systém doménových jmen (Gargasz, 2009). Ty hledají na základě hierarchického uspořádání konkrétní adresu. Po zadání URL adresy se dožadující zařízení obrátí nejprve na nejbližší DNS server, který buď zná odpověď, tj. konkrétní IP adresu přiřazenou dané webové adrese, nebo vznese dotaz v hierarchii výše, až dojde např. k doméně „.cz“ nebo „.com“. Odtud je nasměrován na nižší úroveň, např. „seznam.cz“, odtud pak dále, např. „pocasi.seznam.cz“. Jakmile nalezne dožadující zařízení DNS server, který zná konkrétní cílovou URL adresu, dostane od něj zpět konkrétní IP adresu, na kterou se vzápětí obrátí. To vše v řádech milisekund (Shuler, 2002).

Část komunikace na internetu probíhá prostřednictvím webových stránek, a tedy centralizovaně na bázi klient-server, kdy server poskytuje službu všem dožadujícím klientům. Mimo ně lze využít spojení konkrétních zařízení přímo v rámci P2P (PCWorld, 2009). V takovém případě se při použití k tomu určeného softwaru připojí zařízení do společné sítě (zajišťované internetem) přímo k cílovému zařízení. Uživatel pak obvykle vyhradí pro tuto službu určitý adresář, kam umístí veškerá data, k nimž chce umožnit přístup ostatním uživatelům (TechTerms). De facto tak každé připojené zařízení slouží jako server per se.[33]

[33] Jinou podstatnou technologii představují cloudové služby (Griffith, 2016). Společnost provozující cloud umožňuje přístup k poskytovaným službám odkudkoliv prostřednictvím internetu, zpravidla ve spojení s internetovým prohlížečem a tzv. middlewarem (Strickland). Nejčastěji se takto využívají cloudy jako úložiště

Internetové vyhledávače (Google, Seznam, Bing aj.) soustavně prochází internetovou sítí a tzv. indexují veškerý obsah tak, aby po zadání požadavku ze strany uživatele poskytly co nejrelevantnější informace, resp. odkazy. Konkrétní způsob indexace patří do know-how té které společnosti, nicméně vychází z četnosti použitého výrazu, blízkosti hledaných slov, návštěvnosti odkazované adresy atp. Výsledek by pak měl obsahově zhruba odpovídat zadání, resp. nejčastější uspokojivé odpovědi na dané zadání (Hubbard, 1999).

Výsledek hledání ovšem nelze v žádném případě považovat za objektivní, neboť vychází právě ze způsobu indexace daným vyhledávačem.[34] Kromě toho bývají zobrazené výsledky zpravidla zároveň přizpůsobeny uživateli samotnému, např. na základě jeho předchozí historie vyhledávání a tzv. cookies, tj. informací sbíraných o uživateli řadou aplikací, které shromažďují o uživateli množství údajů, zpravidla za účelem personalizace obsahu a reklamy. Vzhledem k tomu, že cookies mohou být osobními údaji (viz bod 30 preambule a čl. 4 GDPR), vztahují se na jejich byť i jen částečně automatické zpracování (a na neautomatizované zpracování těch, které jsou obsaženy v evidenci nebo do ní mají být zařazeny) pravidla GDPR (čl. 2).[35]

Mimoto vyhledávače mnohdy upřednostňují určité domény, např. domény nějakým způsobem provázané s provozovatelem daného vyhledávače. Zobrazené vyhledané výsledky tak jednak do jisté míry odpovídají uživateli samotnému, jednak se z nich obvykle vytrácí ty méně často využívané, nemluvě o těch, které indexaci neumožňují, a tudíž jsou pro vyhledávače neviditelné.

Značná část obsahu internetu je tak běžnému uživateli skryta, ba zůstává skryta vůči všem, kdo neznají konkrétní cílovou adresu. Např. proto, že stránky nikam neodkazují a není na ně odkazováno, zobrazí obsah až po registraci a zadání hesla, zakazují indexaci vůbec, dovolují

---

dat a služeb spojených s jejich zobrazením a zpracováváním (např. emailová schránka). Hojně se využívá např. kancelářský software typu MS Office, ale i specializované aplikace jako např. účetní software (Beal, 2013) aj. Mimoto lze cloud využít i jako platformu pro vývoj aplikací dle vlastních potřeb, aniž by musel vývojář investovat do svého softwarového vybavení (Krill, 2010). V neposlední řadě pak cloudy slouží jako podpůrná infrastruktura, např. výzkumná laboratoř zadá cloudové infrastruktuře složitý výpočet, který by jinak zabral veškerou výpočetní sílu dané laboratoře.

[34] Z toho důvodu např. po zadání hesla „neoprávněný přístup k počítačovému systému a nosiči informací“ nabídne Seznam.cz jako první odkaz stránky s vybranými judikáty, zatímco Google.cz odkaz na znění § 230 TZ (zobrazeno k 10.12.2018). Výsledek se dále může lišit v závislosti na datu vyhledávání (např. probíhá-li právě mediální kauza shrnutelná pod vyhledávaný výraz).

[35] De lege ferenda má dopadat na oblast ochrany osobních údajů vedle GDPR v rámci národní legislativy zákon o zpracování osobních údajů (spolu s příslušným navazujícím změnovým zákonem), toho času vrácený Poslanecké sněmovně Senátem s pozměňovacími návrhy, který má nahradit stávající zák. č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Blíže k tomu viz sněmovní tisky 138 (Vláda ČR. Poslanecká sněmovna Parlamentu ČR. VIII volební období, 2019) a 139 (Vláda ČR. Poslanecká sněmovna Parlamentu ČR. VIII volební období, 2019).

přístup jen předem vybraným IP adresám nebo třeba umožňují přístup pouze za předpokladu využití anonymizujícího softwaru typu Tor, viz dále. Tato část internetu se označuje jako Deep Web, Deep Net, Deep Internet, Darknet, Hidden Web atp. Veškerý obsah internetu si lze představit jako velký ledovec, jehož jen nepatrná část je viditelná nad hladinou vody prostřednictvím internetových vyhledávačů (tzv. surface web). Ještě menší část jeho obsahu lze prozkoumat de facto pouze s použitím softwaru Tor – anonymizovaného prohlížeče (či jeho doplňku), který původní adresu dožadujícího zařízení úspěšně skryje v rámci anonymizované sítě tvořené Tor prohlížeči, jejichž prostřednictvím jednotlivé packety putují (Bhardwaj, 2012), (Kovar, 2012). Takto (ne)dostupné adresy pak nabízí řadu služeb, vč. nelegálních aktivit souvisejících s prodejem drog, distribucí dětské pornografie atp. (DeepWebSitesLinks). Specifickou problematikou je potom platba za takové služby. Předpokládá se, že se tak děje velmi často prostřednictvím kryptografické měny zvané BTC (Kasík, 2013).

1.1. Zneužití technické stránky internetu

Vzhledem ke značně sofistikované podobě internetu, který jako takový velmi důmyslně využívá řadu ve své podstatě relativně jednoduchých principů, lze nalézt množství míst, na která může zaútočit či je zneužít kdokoliv s alespoň základní znalostí v oblasti IT technologií.[36]

Odesílání a přijímání jakýchkoliv dat je spojeno s rizikem „odposlechu“, a to mj. v závislosti na síle případného šifrování. Router se může stát terčem útoku cíleného na ochromení části systému nebo i sítě v určité oblasti vůbec.[37] Pachatelé mnohdy mění svou MAC a IP adresu. Na jedné straně tak ztěžují odhalení, na straně druhé si úpravou IP a MAC adresy např. zjednají přístup k jinak pro ně (resp. jejich IP/MAC adresy) nedostupné službě. Řada útoků cílí z podobného důvodu na DNS servery: pachatel přeprogramuje DNS server tak, aby jeho IP adresu vydával za jinou, která má oprávnění ke vstupu do jemu jinak uzavřené sítě. V jiném případě přeprogramuje DNS server např. k přesměrování uživatelů přistupujících

[36] Resp. jakákoliv osoba natolik znalá, aby byla např. schopna dle jednoduchých pokynů použít tzv. exploit, tj. malware určený k hackingu - průniku do systému.
[37] Pravděpodobnost úspěšnosti takového útoku postupně klesá úměrně růstu hustoty sítě a její decentralizací, blíže k historii zavádění internetu v ČR viz (Chlad, 2000). Navíc už současná síť zasahuje i mimo jednotlivé kontinenty (Kučera, 2009).

k elektronickému bankovnictví na podvrženou stránku, která pro pachatele zaznamenává zadané přihlašovací údaje.

Cíl útoků typu DDoS spočívá ve znepřístupnění služby poskytované serverem, docilují toho ovšem různými způsoby: např. prostřednictvím malwaru určeného přímo serveru jako takovému (např. smazání dat), zahlcením řadou dotazů (tzn. zasílaných packetů s dotazy, žádostmi o přístup atp.) natolik, že zaměstnají veškerou odpovídací kapacitu serveru atp. Samotný server však nemusí být zasažen vůbec, a přesto v důsledku jednání pachatele neposkytuje své služby – pokud se např. s útočícím zařízením vypořádává samotný router rozhodující o tom, zda danou IP adresu vpustí v komunikaci dále či nikoliv.[38] Protože DDoS vyžaduje koordinovaný postup řady simultánně jednajících zařízení, pachatel si obvykle nejprve prostřednictvím malwaru podřídí řadu zařízení, která na základě jeho pokynu či v předem určený čas začnou naráz vznášet na server / router požadavky. Zařízení (tzv. zombie) mohou být podřízena s vědomím i bez vědomí vlastních uživatelů.[39]

Další nejčastější protiprávní jednání spojená s internetem pak již využívají více či méně sociální inženýrství a nepozornosti či neopatrnosti samotných uživatelů, případně jejich kombinaci: phishing, pharming, nigerijské dopisy, cross-site scripting, viry, trojské koně, červy, keyloggery, tzv. APT atp. Spíše jen minimálně pak využívají technickou stránku internetu jednání jako kyberšikana, porušování autorských práv, podvodná jednání nebo sexuální zneužívání dětí online. Nicméně ani jednání související převážně s dětmi se technické stránce zcela nevyhýbají: např. odposlech zařízení dětské oběti, jehož prostřednictvím pachatel získá přístup k množství osobních údajů, vč. fotografií a videí, kontaktních údajů, denního režimu a mnohdy i přihlašovacích údajů. Výjimkou není ani zaznamenání videohovoru při sexuálním zneužívání dítěte.

Ačkoliv děti se mohou setkat s jakýmkoliv z výše uvedených jevů, nejčastější obavy ve spojení s dětskými uživateli internetu se pojí v tomto směru s možnou škodlivostí obsahu, na který mohou narazit, a to zejm. v raném věku. Vychází z vědomí, že děti dokáží používat

[38] Při trestněprávní kvalifikaci útočníkova jednání pak nelze ani vzdáleně uvažovat o poškození cizí věci – serveru podle ust. § 228 TZ, které by mohlo připadat v úvahu při trvalém alespoň částečném znefunkčnění serveru.

[39] Budeme-li uvažovat o trestněprávní kvalifikaci DDoS útoků jako o neoprávněném přístupu k počítačovému systému a nosiči informací dle ust. § 230 odst. 1 TZ, vyvstává pak problematická otázka (ne)oprávněnosti požadavků ze strany dožadujících zařízení, neboť např. každý může být oprávněn vznést požadavek na zobrazení nějakého webu. V takovém případě lze ovšem stále považovat jednání pachatele za nedovolený výkon oprávnění, a tudíž jednání neoprávněné, k němuž jsou prostředkem využitá zombie zařízení, nemluvě o případné protiprávnosti jejich podřízení si; „za oprávněné ... nelze označit jednání, jestliže by bylo použito sice prostředku dovoleného, nikoli však dovoleného ve vztahu k účelu sledovanému pachatelem“ (Šámal, 2012 str. 1753).

různé aplikace a internetové vyhledávače od útlého dětství, počínaje přeskakováním mezi videi na Youtube již ve dvou letech po cílené vyhledávání obsahu gramotnými dětmi. Snadno tak narazí na obsah nepřiměřený jejich věku, a tudíž nevhodný. Typickým příkladem budiž pornografie, ale také násilný obsah, obscénnosti, vulgarita atd. Možný objektivně traumatizující dopad shlédnutí takového obsahu na dětskou psychiku je zřejmý, nicméně i děti samy ve větší míře vyjadřují nepříjemné pocity s ním spojené: oproti 13 % evropských dětí ve věku 11-16 let v roce 2010 to bylo již 17 % v roce 2014 (eukidsonline.net str. 3), přičemž s ohledem na všeobecné rozšiřování využívání digitálních technologií co do škály i věku lze očekávat další nárůst negativních zkušeností. Děti na internetu cíleně vyhledávají zkušenosti, které by za jiných okolností v běžném životě nezískaly a vědomě překračují bezpečné hranice: sledují pornografii, nenávistný obsah atp. S věkem a mírou užívání internetu roste pravděpodobnost setkání se s takovým obsahem, přesto by děti měli být v tomto směru nahlíženy spíše jako vynalézavé bytosti schopné ochránit sebe samé před nebezpečenstvími online, než jako na oběti kyberprostoru (Răcătău, 2013).

V řadě případů se jedná o obsah zcela v souladu s právem, zejm. pak na stránkách určených dospělým (blíže k tomu viz zejm. kapitola **Pornografie a děti online**). Významnou roli v prevenci takových setkání hrají rodiče a starší sourozenci dětí, kteří zpravidla patří mezi první osoby seznamující je s prostředím internetu (Bárta, a další, 2018),[40] a kterým v tomto směru vychází vstříc velké společnosti podnikající v oblasti digitálních technologií, jež běžně nabízí vlastní technické nástroje pro správu souvisejícího obsahu a aktivit, filtrování obsahu a kontrolu činnosti (zpětně i v reálném čase), obvykle označované jako rodičovská ochrana. Po obvyklém nastavení uživatelského účtu pro dítě umožňuje úprava prostřednictvím rodičovské ochrany např. nastavit čas využívání zařízení (v konkrétním čase nebo časovou dotací), zakázané a povolené programy (např. počítačovou hru), filtraci obsahu online (seznam zakázaných nebo povolených adres, tzv. black list a white list) nebo filtraci na základě vyskytujících se slov atp.

Pokud se už jedná o obsah protiprávní, může za něj odpovídat kromě samotné osoby, která jej umístila online, i poskytovatel dané služby. Poskytovatelů služeb online je celá řada a základní rámec jejich působení v České republice dává zák. č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách

[40] Dílčí výsledky výzkumu Digitální technologie v každodenním životě a učení studentů (Ústav pedagogických věd FF MU, 2017), mezi něž patří i uvedené zjištění, byly předneseny v prosinci 2018 na konferenci Cyberspace 2018 pořádané Masarykovou univerzitou v Brně s předpokládaným zveřejněním na jaře roku 2019, příspěvek Ambivalence in ICT-related learning od autorů Bárta, O., Juhaňák, L., Záleská, K. a Zounek, J.

informační společnosti). Ten v § 2 písm. d) definuje jako poskytovatele služeb každou fyzickou nebo právnickou osobu, která poskytuje některou ze služeb informační společnosti, tj. zjednodušeně jakákoliv služba poskytovaná elektronickými prostředky na individuální žádost uživatele podanou elektronickými prostředky [§ 2 písm. a)]. Ve vztahu k dětem se jedná především o provozovatele SNS, chatů, videokanálů, počítačových her, kteří poskytují svou infrastrukturu a softwarové zázemí k ukládání dat ze strany uživatelů [každá fyzická nebo právnická osoba, která využívá službu informační společnosti, § 2 písm. e)] (Maisner, 2016 str. 63).

Poskytovatelé služeb odpovídají za obsah informací poskytnutých uživatelem (na jeho žádost) zjednodušeně řečeno jen tehdy, pokud mohli vědět, že takový obsah je protiprávní, nebo dozvěděli-li se prokazatelně o protiprávní povaze takového obsahu[41] a neprodleně neučinili veškeré kroky, které lze po nich požadovat, k odstranění nebo znepřístupnění takového obsahu (§ 5 zák. o některých službách informační společnosti).[42] Zároveň tito poskytovatelé nejsou povinni dohlížet na takový obsah, ani aktivně vyhledávat skutečnosti a okolnosti poukazující na protiprávnost obsahu (§ 6 zák. o některých službách informační společnosti)

V tomto směru jdou mnozí, zejm. velcí poskytovatelé služeb o krok dále ve vztahu k dětem, když poměrně běžně využívají nástroje umožňující snadno označit a nahlásit provozovateli služby protiprávní obsah, případně i s rozlišením formy porušení zpravidla interních pravidel (např. vulgarita, nevyžádaný kontakt, pornografie, násilí atp.), obvykle v podobě ohlašovacího „tlačítka“, jednoduché volby hned v základním menu atp. Jiné nástroje umožňují filtrování obsahu tak, aby odpovídal příslušné cílové skupině, resp. odfiltrují nežádoucí obsah (typicky pornografii nebo násilí). Stále více se také objevují snahy alespoň minimálně korigovat nebo reagovat na samotný obsah ukládaný uživateli (nad rámec jeho využití k marketingovým účelům) – např. FB předesílá vývoj nástroje pro detekci sebevražedných sklonů na základě analýzy příspěvků uživatele spolu s následnou intervencí vhodné osoby (Kluska, 2017), Youtube se chystá blokovat a vyhledávat nevhodná videa - např. týrání dětí (Balucha, 2017).

V neposlední řadě pak nutno uvést ještě zmíněné cookies a obecně zpracovávání osobních údajů ve vztahu k dětem (nejde sice obvykle o trestněprávní oblast, přesto však zasluhuje určitou pozornost). Základní povinnosti v souvislosti s cookies coby osobními údaji vyplývají

[41] Všeobecné povědomí o možném protiprávním obsahu nestačí, taková vědomost musí být prokazatelná a jednoznačná. Původcem takového oznámení může být kdokoli a mělo by vymezit onen protiprávní obsah a jeho umístění a doložit jeho protiprávnost, a to alespoň v hrubých rysech (Maisner, 2016 str. 71).
[42] Nevztahuje se na obsah ukládaný např. ze strany zaměstnanců na základě pokynu zaměstnavatele – poskytovatele služby.

z GDPR, a to především požadavek na kvalitu zpracovávaných osobních údajů (čl. 5 odst. 1) a zákonnost jejich zpracování (čl. 6). Ochrana dětí je posílena již deklarací zvláštní ochrany, zejm. v oblasti marketingu, profilování a shromažďování osobních údajů (bod 38 preambule), zvýšenými požadavky na zásadu transparentnosti co do obsahu určeného dětem [bod 58 preambule, čl. 5 odst. 1 písm. a) a čl. 12 odst. 1], zdůrazněním práva na opravu zpracovávaných osobních údajů a práva „být zapomenut" ve vztahu k subjektům údajů, jež daly svůj souhlas s jejich zpracováním v dětském věku (bod 65 preambule a čl. 16 a 17), výslovným uvedením dětí coby subjektu údajů jako důvodu pro případné omezení zákonnosti nezbytného zpracování osobních údajů pro účely oprávněných zájmů příslušného správce či třetí strany [čl. 6 odst. 1 písm. f)] a nakonec podmínkou zákonnosti zpracování osobních údajů na základě souhlasu jejich dětského subjektu pouze v případě, je-li ve věku nejméně 16 let, přičemž tato hranice může být snížena členským státem až na 13 let [čl. 6 odst. 1 písm. a) a čl. 8].[43] Poslední jmenovanou povinnost pak upravuje vládní návrh zákona o zpracování osobních údajů (viz pozn. č. 35), který zakotvuje pro způsobilost udělit souhlas se zpracováním vlastních osobních údajů podmínku dovršení 15 let (§ 7).

1.2. Shrnutí k technické stránce kyberprostoru

Pochopení technické stránky internetu je zásadní pro porozumění některým hrozbám a rizikům. Kapitola se proto věnuje technologii zajišťující propojení jednotlivých zařízení a jejich komunikaci. Zahrnuje tak mj. technologii packetů, internetové protokoly, IP a MAC adresy, routery, servery, DNS překladače. Obsahuje také stručný nástin relevantních škodlivých jednání spojených s technologií internetu jako takovou.

Internet představuje celosvětovou síť tvořenou decentralizovaným množstvím uzlových bodů, mezi nimiž putují data. Ta jsou v místě odeslání rozložena na tzv. packety nesoucí zároveň informaci mj. o své cílové adrese a místě konkrétního packetu v rámci celku pro jeho budoucí opětovné složení do původní podoby. Každý packet putuje nezávisle na ostatních právě nejrychlejší cestou, přičemž se přesouvá mezi jednotlivými uzlovými body, především routery. Ty případně také určují, zda packet vpustí do své lokální sítě či naopak z vlastní sítě ven. Cílové místo má podobu IP adresy, která se sice může v čase měnit, v daný okamžik je

[43] Volitelnost věkové hranice však znamená komplikaci pro poskytovatele služeb, který by tak měl zohledňovat zemi uživatele, typicky např. FB (Vejvodová, 2018). Poskytovatelé služeb se zřejmě vydají cestou geolokace IP adresy.

však vždy jedinečná. Tzv. DNS překladač pak převádí její číselnou podobu na slovní URL adresu (např. seznam.cz) a slouží zároveň jako rozcestník při vyhledávání jejího konkrétního umístění v hierarchickém uspořádání: např. doména.cz, dále seznam.cz, dále seznam.cz/jizdnirady/ atd. Velkou část služeb internetu zajišťují servery, a to v podobě softwaru, spojení softwaru s hardwarem a specifického webového serveru spolupracujícího s internetovým prohlížečem. Mimo servery lze pak využít P2P. K vyhledání obsahu či služby slouží především internetové vyhledávače, které indexují veškerý jim dostupný obsah (tzv. surface web, cca 4 %) a pořadí nabídnutých odkazů obvykle upraví s ohledem na jejich návštěvnost a personalizují s ohledem na dotazujícího uživatele, zejm. s využitím tzv. cookies. Zbývající část internetu (deep web) je dostupná pouze po autorizaci nebo s využitím speciálního softwaru, její zlomek pak pouze prostřednictvím softwaru Tor (dark web, zřejmě cca 0,5-1 %). Zneužít technickou stránku internetu lze mnoha způsoby: např. odposlech dat, úprava IP a MAC adresy s cílem zpřístupnění jinak nedostupné služby či obsahu, zásah do činnosti DNS překladače (zpravidla zavádějící přesměrování nebo získání neoprávněného přístupu), DDoS a s využitím sociálního inženýrství i další: phishing, pharming, nigerijské dopisy, cross-site scripting, viry, trojské koně, červi, keyloggery, tzv. APT atp.

Ovšem ani protiprávní jednání častěji spojovaná s dětmi jako sexuální zneužívání online nebo kyberšikana se technické stránce internetu nevyhýbají, za zmínku stojí především odposlech zařízení užívaného dítětem. Mimoto se děti v online prostředí snadno setkají s pro ně nevhodným obsahem, přičemž téměř pětina z nich to pociťuje negativně. Jako prevence takových setkání slouží na technické úrovni především rodičovská ochrana, jde-li o obsah souladný s právem, u protiprávního pak nastupují zákonné povinnosti poskytovatelů služeb informační společnosti, kteří za něj mohou za určitých okolností odpovídat spolu s osobou, která jej umístila online. Stejně jako u ostatních, o dětských uživatelích internetu sbírá řada aplikací osobní údaje v podobě tzv. cookies. Jejich zpracování upravuje především GDPR, de lege ferenda doplněné zákonem o zpracování osobních údajů.

Mládež se s online kriminalitou zneužívající technickou stránku internetu setkává coby poškození v závislosti na míře vlastního využívání digitálních technologií, převážně půjde ovšem spíše pouze o protiprávní než trestný obsah. S ohledem na určitou míru potřebných znalostí k páchání provinění či činů jinak trestných v této oblasti (přinejmenším v podobě schopnosti vyhledat a využít tzv. exploit, tj. malware vytvořený jinou osobou) lze uvažovat o pachatelích de facto výlučně z řad mladistvých osob.

2. Kyberprostor a nová média[44]

Kyberprostor je všudypřítomný. Je vtělen do nespočetného množství více či méně propojených systémů tvořených na jedné straně internetem, lokálními sítěmi, sítí mobilních telefonů a připojenými zařízeními, na straně druhé pak samotnými uživateli.

Mobilní telefony patří již k běžnému vybavení domácnosti, řada osob disponuje i více zařízeními či telefonními čísly. Jako součást kyberprostředí nabývají na významu především ve spojení s přístupem na internet a s tím spojenými službami: správou emailové komunikace (prostřednictvím tzv. emailového klienta - softwaru umožňujícího práci s jednou a více emailovými adresami), prohlížením webových stránek (a odvozenými službami: nakupování v e-shopu, stahování, sdílení,[45] sledování on-line vysílání TV či poslech internetového rádia atp.), komunikací s jinými uživateli, stahováním a využíváním různých aplikací atp.[46] Kromě komunikace a přístupu na internet v sobě mobilní telefony obvykle integrují mnohé další funkce (nyní již lze hovořit spíše o „počítači“ než „telefonu“): z těch nejpoužívanějších GPS,[47] digitální fotoaparát a videokameru (vč. případného záznamu GPS), datové úložiště, čtečku a přehrávač záznamů (audio i video), v neposlední řadě též různé pomocné funkce pro osoby se zdravotním postižením a seniory.[48] Za zmínku stojí také propojení s dalšími zařízeními, např. tzv. chytrou domácností (především ovládání na dálku).[49]

Především je zde však internet[50] s řadou služeb a funkcí, do jisté míry propojující vše výše uvedené. Slouží jako informační zdroj, počínaje zprávami o aktuálním dění přes informace zveřejněné na wikipedii,[51] vč. obdobných encyklopedií více méně kopírujících její princip –

[44] Kapitola zahrnuje i text vytvořený kolektivem autorů coby výukový materiál pro pedagogy v rámci projektu Škola bezpečně online: Zvýšení kvality vzděláván v oblasti bezpečného užívání internetu v Pardubickém kraji, CZ.1.07/1.3.12/04.0016, na jehož přípravě se autorka podílela, a tam uvedených zdrojů (Národní centrum bezpečnějšího internetu), (Brandejsová, a další, 2012).

[45] Sdílením je umožnění přístupu k datům umístěným ve vlastním zařízení, aniž by to mělo vliv na data samotná, která zůstávají na svém místě.

[46] Např. aplikace pro cesty MHD upozorňující s pomocí GPS uživatele, že se blíží cílová stanice, detektor souhvězdí ve formě tzv. rozšířené reality poskytující informace o jednotlivých hvězdách při namíření mobilního telefonu s danou aplikací na noční oblohu a nespočetné množství dalších aplikací.

[47] Určení polohy GPS souřadnicemi a ve spojení se softwarovou aplikací zobrazující mapy i navigace.

[48] Např. čtení obsahu pro zrakově postižené nebo asistenční služba pro seniory pod speciálním tlačítkem (InspectLife), (iSenior, 2010).

[49] Např. lednice sledující dobu spotřeby potravin, trouba nabízející recepty v návaznosti na obsah lednice atp., viz např. (Chroust, 2013) nebo též (Redakce Chip, 2013).

[50] Řada firem a institucí využívá též lokální sítě, jež mají oproti internetu některé podstatné výhody: nejsou tolik ohroženy útoky zvenčí, přenosová kapacita může být výrazně rychlejší, umožňují snazší regulaci obsahu a detekci činností uživatelů, usnadňují utajení dat atd.

[51] Používám „wikipedie“ s malým počátečním písmenem na zdůraznění již zobecnělého výrazu označujícího Wikipedii ve zhruba 300 jazykových mutacích, ať už s původním nebo vzájemně okopírovaným obsahem. Prvotní Wikipedia.org vznikla 15. ledna 2001 a v současnosti obsahuje přes 5,7 milionů článků, resp. hesel (Wikipedia). Česká mutace Wikipedie byla spuštěna 3. května 2002 a v srpnu 2018 měla 410 tisíc hesel

např. iuridictum (Pecina), a přes informace publikované na jednotlivých webových stránkách k tomu či onomu tématu[52] až po jednotlivé tzv. blogy[53] a informace obsažené v příspěvcích samotných uživatelů (informace na SNS, příspěvky v diskusích atp.). Specifickou formu kombinace služby a informací představují e-learningové kurzy a učební platformy.[54]

K zásadním funkcím internetu patří komunikace. Na technické úrovni komunikace mezi zařízeními umožňující jejich ovládání na dálku, případně v kombinaci s mobilním telefonem (Křešnička, 2015). A tak zatímco dříve se o internetu hovořilo jako o „internetu myšlenek,“[55] v současnosti je to „internet věcí,“[56] co nabývá na významu.[57] Uvažovat lze v tomto směru o relativně drobných „věcech“, jako jsou např. chytré hodinky sledující zdravotní stav nositele a odesílající data v reálném čase příslušnému zdravotnickému zařízení (Chen, a další, 2015), chytrý dudlík (Novotný, 2015), (Blue Maestro, 2015) atp. IoT se ovšem neomezuje na jednotlivce a zahrnuje např. chytré budovy integrující v sobě požární systém komunikující s výtahy, klimatizaci reagující na aktuální stav počasí, automatickou kontrolu bezpečnosti atp. (Kranenburg), ale také celá města využívající IoT, např. v podobě regulace dopravy reakcí světelných semaforů na aktuální dopravní data získávaná přímo z projíždějících automobilů (Burrus, 2014).

Z hlediska sociálních vztahů hraje ovšem mnohem větší roli mezilidská komunikace v prostředí internetu.[58] V posledních přibližně 30 letech to byl nejprve mobilní telefon jako stále běžnější součást vybavení domácnosti, umožňující mj. i relativně nový formát přenosu zprávy v podobě sms, tedy textového vzkazu, na který lze posléze reagovat. Vedle mobilního telefonu přišel internet a s ním emailová komunikace, do jisté míry nahrazující jiné formy

---

(Wikipedie).

[52] Nepřeberné množství témat nabízí odpovědi na stejně nepřeberné množství rozličných otázek, viz např. (Houbaření - Atlas hub).

[53] „Webová aplikace obsahující příspěvky většinou jednoho editora na jedné webové stránce“ (Wikipedie). Blogy slouží ke glosování aktuálních událostí, autorské tvorbě, publikaci informací, sebeprezentaci atp.

[54] V českém prostředí patří v tomto směru k nejvyužívanějším tzv. Moodle, vč. desítek kurzů provozovaných Univerzitou Karlovou (Univerzita Karlova, 2015). Moodle funguje jako tzv. open-source software (volně přístupný, k open-source softwaru viz dále), tedy volně dostupná platforma pro tvorbu a použití online kurzů ze strany pedagoga či lektora i studentů či účastníků kurzu (moodle), (Wikipedie).

[55] „Internet of Thoughts“, internet coby prostor svobodného sdílení myšlenek aj. obsahu (Barlow, 1996).

[56] Blíže k některým aspektům „internetu věcí“ viz např. (Freyssinet, 2013 str. 6) nebo též (Dardayrol, 2013 str. 85).

[57] V současnosti se odhaduje cca 4.9 miliard „věcí“ připojených k internetu s předpokládaným rostoucím počtem až k 25 miliardám v roce 2020 (2015).

[58] V některých případech může jít i o komunikaci s tzv. botem, tj. softwarem naprogramovaným v tomto případě k simulaci komunikace fyzické osoby (často marketingově orientované), zejm. na SNS. V současnosti se lze setkat s několika úrovněmi “virtuálních bytostí”: avatary jakožto reprezentacemi uživatelů, ale také AI různého stupně – od uvedených botů po “společníka” astronautů na dálkových vesmírných letech (Lauria & Robinson, 2013). Boti v jiných oblastech např. píší zpravodajství (Čížek, 2012), (narrative science).

písemného styku.[59] K emailu se poté přidružil tzv. instant messaging, tj. možnost zobrazení kontaktů aktuálně on-line a odeslání zprávy na jejich adresu. Emailový klient i instant messangery obvykle umožňují i přechod do chatovacího režimu, tj. písemné komunikace probíhající prakticky v reálném čase (adresát vidí buď obsah po jeho odeslání pisatelem, anebo přímo každý pisatelův úhoz do klávesnice). Za tím účelem existuje řada aplikací (např. ICQ) a chatovacích místností, ať už volně využitelných nebo dedikovaných určitému tématu či osobám.[60] K nejmladším, leč nejoblíbenějším aplikacím patří videohovory a videokonference (současné zapojení více osob např. prostřednictvím Skype), tedy přenos zvuku i obrazu prakticky v reálném čase (v závislosti na rychlosti připojení), dále pak sdílení obsahu (typicky pořízení záznamu a jeho odeslání vybraným uživatelům nebo upload na vlastní profil na SNS).

Internet slouží zároveň jako platforma pro celou řadu dalších služeb a aplikací, často ve spojení s mobilním telefonem. Zvlášť velkou oblast představují hry, od bezduchého trávení volného času bezmyšlenkovým pobíjením nepřátel přes příběhově sofistikované a literárně dobře zpracované příběhy nebo hry založené na komunikaci a kooperaci řady hráčů až po vzdělávací hry.[61] K hojně využívaným službám pak patří ještě cloud, tedy zpravidla prostřednictvím internetu dostupný software poskytující klientům infrastrukturu, platformu nebo službu např. v podobě kancelářského softwaru nebo emailového klienta. Mezi podstatné výhody využívání cloudu se řadí dostupnost uložených dat či přístupnost softwaru nebo obslužnost hardwarového vybavení na dálku (např. ze strany zaměstnance mimo firemní prostory).

Mládež bývá v kontaktu s digitálními technologiemi od útlého věku, počínaje prohlížením videí na Youtube již v několika letech přes aplikace určené dětem po již běžnou uživatelskou schopnost v období dospívání. Jsou však nezkušení, důvěřiví a otevření, možnosti bezprostřední online komunikace se světem se rozvíjejí rychleji než jejich psychická připravenost na setkání s možnými nebezpečími. Chybí jim vlastní zkušenost, a zkušenost starších je nejen obtížně přenosná, ale také u mnoha současných dospělých prakticky chybí, byť se tato tzv. digitální propast postupně vyrovnává. Současní mladiství představují jedny z prvních generací, které se již narodily do světa internetu a neumí si svůj život bez něj

[59] Zejm. s pozdějším nástupem možnosti elektronického podpisu a zřízením datových schránek.
[60] Správce dané místnosti může nastavit pravidla – např. zabezpečit místnost heslem, umožnit vstup pouze registrovaným uživatelům, omezit nejvyšší možný počet aktuálně připojených uživatelů atp., viz např. (chatib).
[61] Např. hra Evropa 2045 vyvinutá ve spolupráci Filosofické a Matematicko-fyzikální fakulty Univerzity Karlovy simulující Evropský parlament, určená na podporu výuky na středních školách (Evropa 2045).

představit, vyrostli obklopeni digitálními zařízeními, počínaje stolními počítači přes mobilní telefony po IoT. M. Prensky pojmenoval tyto generace jako „digitální domorodce“ (Prensky, 2001 str. 1). Jde o přiléhavé označení, byť jsou jejich „domorodé“ užívací schopnosti limitovány kognitivním vývojem a ve věku do 8 let jsou spíše jen pasivními příjemci, byť si základní uživatelské schopnosti osvojí poměrně rychle (Chaudron, 2015 str. 7). Ve věku 15 let již užívají digitální technologie zcela běžně a samozřejmě, bylo by však mylné považovat je obecně za „digitální guru“, jak mnohdy činí zejm. učitelé základních a středních škol, neboť ICT jim slouží k usnadnění, nikoliv nahrazení běžných činností (Bárta, a další, 2018).[62]

Komunikace v kyberprostoru se vyznačuje do jisté míry také svébytným jazykem s řadou novotvarů a ustálených shluků písmen jako omg, btw, pls, np a dalšími.[63] Na vině je především snaha zestručnit a zrychlit komunikaci používanou v rámci sms (Pospíšil, 2008)[64] a v prostředí počítačových her založených na kooperaci (vyžadují zpravidla rychlé vyjadřování). České novotvary často kopírují anglické výrazy a sobě vlastním způsobem je skloňují – typicky výraz „(vy)googlit“.[65] Jazyk virtuální komunikace je pro digitální domorodce „mateřským“ jazykem, naopak starší generace se mu učí až v dospělosti, a jsou proto spíše „digitálními imigranty“.[66] Prensky vychází z poznatku, že současní žáci zacházejí s informacemi a zpracovávají je zcela jinak než generace předchozí. Stimulace mozku má vliv na jeho fyzickou restrukturalizaci po celý lidský život, a proto mají zřejmě dnešní žáci a studenti vzhledem k významně odlišné zkušenosti a podnětům v rozhodném vývojovém období fyziologicky odlišný mozek. Jsou zvyklí získat hledanou informaci velmi rychle, pracují s více úkoly souběžně, upřednostňují práci s obrazy a grafikou před textem a hry před „skutečnou“ prací, nejlépe fungují ve skupinách a neustále „propojení“ a „připojení“ (Prensky, 2001 str. 2).

[62] Dílčí dosud písemně nepublikované výsledky výzkumu, viz pozn. č. 40.
[63] Oh, my God - Bože můj, by the way - mimochodem, please - prosím, no problem - žádný problém (Nývlt, 2008).
[64] V současnosti ztrácí tento důvod na významu vzhledem k rozšířenosti tarifů mobilních operátorů nabízejících jednak za určitý paušál neomezené množství sms, jednak s využíváním aplikací sloužících k zasílání zpráv aj. obsahu prostřednictvím internetu, zejm. pak ve spojení s Wi-Fi signálem dostupným mnohdy bez poplatku (např. připojení v restaurací).
[65] Česká wikipedie vychází z běžně hovorově používaného výrazu „googlit“ ve smyslu vyhledávat na internetu (wikipedie), naproti tomu anglickojazyčné zdroje odkazují na vyhledávání obsahu na internetu s použitím vyhledávače Google (wikipedia), (Choney, 2013).
[66] Vžilo se i označení „generace Z“, tj. osoby, které se v období masového využívání nových médií, na rozdíl od generace X, jejich rodičů, a generace Y, osob narozených zhruba v 80. letech 20. st., kteří již dospívali v éře internetu, ale pamatují ještě dobu před ním.

Komunikace v digitálním prostředí svým způsobem rozpojuje čas a prostor (Giddens, 2000 str. 103), které představovaly relativně donedávna neoddělitelnou jednotu,[67] ba jednotky času a prostoru byly do jisté míry vzájemně převoditelné, byť s výhradou časoprostorové konvergence - „zkracováním" vzdáleností v důsledku rozvoje dopravních prostředků.[68] K tomu se přidaly telegraf, telefon, rádio a TV, které zásadně zkrátily čas potřebný k přenosu zprávy. Ovšem s digitálním věkem a masovým rozšířením zařízení spojených v kyberprostoru a neustále rostoucí přenosovou kapacitou jsou nyní veškerá data dostupná s minimální časovou prodlevou a prakticky zcela bez závislosti na prostoru (jen s ohledem na sílu přenosového signálu). Jakýkoliv obsah se tak může rozšířit prakticky okamžitě a všude.

Časoprostor ovlivňuje i lidskou činnost jako takovou, neboť každý musí věnovat určitý čas odpočinku a příjmu potravy, což obvykle vede k zónování činností do určitého času a prostoru. Tzv. kolonizace času s nástupem a rozšířením digitálních technologií časově i prostorově rozšířila činnosti jednotlivce nad rámec těchto tradičních zón - např. rozšíření bdělých činností do nočních hodin, tradičně věnovaných především spánku (Giddens, 2000 str. 104), tzv. home office atp. Lze také předpokládat, že určitých změn dozná např. i „tradiční" časoprostorové mapování kriminality.[69] Např. tradičně geograficky určené „hot spots" a „harm spots"[70] nadále i jako místa lokalizovatelná „v síti": např. konkrétní web, jehož prostřednictvím se šíří protiprávní obsah, nebo aplikace se skrytým malwarem atp.

Časoprostorové rozpojení, potažmo rychlost a masovost šíření obsahu má ovšem i negativní stránku, a to zejm. v případě šíření nepravdivých nebo zavádějících informací a zraňujícího obsahu. Mezi nejčastější „zpravodajské" manipulativní techniky patří apel na strach, výmysl, obviňování, démonizace, nálepkování a relativizace, přičemž uživatelé nejenže ve většině případů nerozpoznají manipulativní informace, ale naopak mnohé informace považují mylně za manipulativní (Vejvodová, 2018).[71] Tím spíše, postrádají-li vzhledem k věku dostatek vlastních zkušeností a nadhled. Specifickým fenoménem ohrožujícím zejm. dětské a mladistvé

[67] Např. je podstatné, zda hovořím o určitém údolí v období původního osídlení nebo v době jeho zatopení coby přehrady, o jakém časovém pásmu hovořím při domluvě schůzky atp., přičemž čas i prostor bývají zřejmé z ostatních okolností (např. určení „tady").
[68] Např. z východního na západní pobřeží Spojených států se lze dostat na koni za několik měsíců, autem za několik dní, letecky za několik hodin (Giddens, 2000 str. 101).
[69] Blíže k mapování kriminality viz např. (Gřivna, 2015 str. 71).
[70] Místa s výrazně vyšší koncentrací kriminální činnosti a způsobené škody, zejm. k harm spots viz (Weinborn, a další, 2018).
[71] Dílčí výsledky projektu Zvol si info (Zvol si info), mezi něž patří i uvedené zjištění, byly předneseny v prosinci 2018 na konferenci Cyberspace 2018 pořádané Masarykovou univerzitou v Brně v příspěvku P. Vejvodové How to manipulate: the techniques of online disinformation media. Blíže k problematice tzv. fake news viz (Gregor, 2018).

uživatele jsou nebezpečné návody (byť obvykle nepůjde o trestněprávní rovinu),[72] které se šíří virálně (sdílením mezi uživateli zejm. na SNS), případně i jinými kanály, jako tomu bylo např. u hry Modrá velryba, o níž informovala svého času většina médií.[73]

Zatímco tzv. fake news a nebezpečné návody se šíří zpravidla neadresně, zraňující obsah bývá naopak cílen na konkrétní jedince.[74] Obvykle jde o dehonestující informace, fotografie či videa (skutečné, upravené i zcela smyšlené), která šíří nebo jejichž šířením hrozí původce. Nejčastěji jde o součást kyberšikany, jednání zhrzeného expartnera nebo vydírání (u mládeže zpravidla s cílem dosáhnout osobního setkání či zaslání sexuálně laděného materiálu spíše než finančního obohacení). Zvlášť u expartnerů bývá původcem obsahu samotná oběť, která ho zašle v té době stávajícímu partnerovi, přičemž zraňující dopad se přidává až posléze následným zveřejněním již bez přičinění oběti. Zveřejnění takového obsahu a jeho prakticky neomezené šíření může mít zejm. na psychiku oběti zdrcující dopad, samotná hrozba zveřejnění může představovat v závislosti na obsahu značný psychický nátlak.[75]

Ještě jeden prvek považuji za vhodné zmínit v souvislosti s časoprostorovým rozpojením, a to globalizaci, tedy celosvětovou provázanost, která zahrnuje pohyb zboží, služeb a osob, provázání mocenských struktur různého charakteru (podnikatelské, mediální, politické, kulturní aj.), šíření a sdílení informací (zvláště k posledně jmenovanému přispívá internet značnou měrou). S globalizací internetu je nerozlučně spojena i decentralizace, ba jedno bez druhého by bylo jen obtížně představitelné. Absence hlavního centra má svůj původ v samotných počátcích vývoje internetu (resp. sítí předcházejících internetu) v období studené války, kdy panovaly obavy nad zneprovozněním sítě (sloužící i k vojenským účelům) v důsledku raketového útoku zasáhnuvšího případný centrální počítač (picolsigns, 2009). Díky tomu a díky síťové povaze internetu, kdy vyřazení jednoho zařízení vede pouze k putování packetů jinou cestou a znepřístupnění dat fyzicky umístěných na daném znepřístupněném serveru, de facto nelze vypnout, zrušit, zničit atp. internet jako takový, nanejvýš je možné částečně omezit zobrazení určitého obsahu.

[72] Např. tzv. Ice &Salt Challenge, při které si dotyčný přiloží na část těla posypanou solí led s cílem vydržet následnou spalující bolest a s častým výsledkem popálení a zjizvení kůže.
[73] Údajně reálná hra spočívající v plnění pokynů k různým aktivitám vč. sebepoškozování, vedoucí v závěru až k sebevraždě, ve skutečnosti však více méně pouhá marketingová snaha zvýšit návštěvnost určitého webu, které medializace spolu s virálním šířením propůjčila sílu sebenaplněného proroctví, neboť se posléze objevila řada jejích variací a skutečně hrající osoby (Holušová, 2017). V České republice získala pozornost zejm. v dubnu 2017 po varování Policie ČR a odvysílání reportáže v hlavní zpravodajské relaci ČT (ČTK, 2017).
[74] Může zahrnovat i fake news a nebezpečný návod – např. podrobný pokyn k dalšímu zraňování.
[75] Blíže viz kapitola **Kyberšikana**.

Obdobně de facto nelze spolehlivě získat zpět již zveřejněný materiál, resp. digitalizovaný obsah daný k dispozici jinému člověku. Odesílající osoba nad ním zcela ztrácí kontrolu, neboť nemá žádnou možnost zajistit, jakým způsobem s obsahem naloží sám adresát, případně jiná osoba, která získá přístup k zařízení, na němž je uložen. Digitalizovaný obsah je prakticky věčný (pouze při výlučném uložení na jediném místě podléhá případné zkáze hmotného nosiče), neomezeně kopírovatelný (s kvalitou originálu), globální (přístupný odkudkoliv) a dohledatelný (především v surface webu): je-li obsah zveřejněn (např. na SNS), nelze spolehlivě zaručit omezení jeho dalšího sdílení a i v případě, že ho provozovatel dané služby odstraní, zůstává zde možnost jeho archivace a následného obnovení.[76]

Ke kyberprostoru neodmyslitelně patří tzv. nová média, odlišná od tradičních médií jako jsou tisk, rozhlas a TV. Média lze členit na primární: přirozený jazyk a nonverbální komunikace; sekundární: technické prostředky překonávající časové a prostorové bariéry – telefon aj.; terciární: masmédia, hromadné sdělovací prostředky schopné oslovit značné množství recipientů – např. TV; a kvartární: síťová digitální média kombinující všechny předchozí typy (Volek, a další, 2006 str. 10). Média vyššího řádu v sobě zahrnují vždy i média nižšího řádu.

Tradiční média charakterizuje adresnost aktérů – typicky v rámci hovoru dvou a více osob, případně v rámci proslovu vůči fyzicky přítomné, a tudíž početně omezené skupině osob, vždy v reálném čase. Masová média již umožňují jednotlivci oslovit nepoměrně více osob, adresně neurčených a bez nutnosti fyzické přítomnosti (při využití sekundárních médií), typicky článek v novinách, projev v rozhlase, TV vysílání. Komunikace může, a nemusí probíhat v reálném čase, ba naopak bývá obsažen prvek určitého časového odstupu a periodicity – např. denní tištěné noviny, předtočené TV vysílání atp. Recipienti zpravidla nemají na obsah sdělovaných informací žádný vliv.[77]

Naproti tomu nová média nemusí podléhat omezení množství adresátů a recipientů, ale ani sdělujících osob, stejně jako časovým a prostorovým omezením předávání informací a komunikace – jsou dostupná kdykoliv a odkudkoliv a neomezená délkou obsahu. Spojení s digitálními technologiemi umožňuje interaktivitu (z konzumenta se stává uživatel), hypertextualitu (obsah je propojen s dalšími informacemi prostřednictvím odkazů a je to uživatel, kdo si ho vybírá), disperzi (rozptýlenost obsahu a jeho tvůrců - např. poslech hudby

[76] Existuje tzv. Wayback Machine, archiv internetu zálohující množství jinak již nedostupného obsahu prostřednictvím ukládání URL adres spolu s daným obsahem ke konkrétnímu okamžiku (Internet Archive).
[77] Až na sporadické výjimky usilující o jejich větší zapojení např. prostřednictvím hlasování diváků v divadle v průběhu představení o směrování příběhu.

není vázaný na předem daný program rádia) a v neposlední řadě virtualitu jakožto určitý svět bez fyzického substrátu, v němž jsme přítomni svým vědomím a některými smysly (Lister, a další, 2003). Digitální obsah je převoditelný na data v podobě binárního kódu – tzv. komputerizace kultury (Manovich, 2001). Lze ho proto rozdělit, upravit, zrychlit atp. Může existovat v nekonečném množství kopií zcela identických s originálem, resp. nerozpoznatelných od původní kopírované verze. Obsah je možné zobrazit prostřednictvím řady zařízení (stolní počítač, tablet, mobilní telefon atp.), data mohou být přístupna velmi rychle a snáze manipulována - např. přenášena (Lister, a další, 2003 str. 16). Nakládání s daty, resp. interakce s obsahem se často očekává, od pouhého vyhledávání informací přes jejich šíření a sdílení po tvorbu vlastního obsahu, vč. interakce s ostatními uživateli (např. diskuse).

Ovšem i tradiční média se v prostředí digitálních technologií transformují v média nová, a to především umožněním interakce (např. reakce v reálném čase na online dotazy diváků v TV pořadu), dostupností online (např. TV vysílání online) a dostupností obsahu na vyžádání (např. archiv předchozích vydání časopisu). Původní tradiční média sice stále zaujímají v kulturním prostředí moderní společnosti významné postavení, nová média však jejich roli do jisté míry upozaďují a proměňují, zejm. neustále se proměňujícím obsahem v reálném čase, interaktivitou a dostupností.[78] A stejně jako tradiční média znamenala skok co do šíření informací i dezinformací masovým tempem, nová média posouvají tyto hranice ještě dále, resp. rychleji,[79] vč. ovlivňování veřejného mínění a nálady ve společnosti vůbec.[80] Tradiční média se běžně prezentují i na SNS, pro něž je zvlášť typické šíření obsahu a komunikace ve vztahu mnoha aktérů navzájem. Nestojí již v pozici adresátů ani recipientů, ale aktivních tvůrců a šiřitelů obsahu. Většina dětí ve věku 15 let sice představuje spíše konzumenty (a

[78] Typicky internetové zpravodajství, soustavně doplňované a aktualizované (zejm. u rychle se vyvíjejících událostí), navíc s možností okamžitého vyhledání dalších informací prostřednictvím odkazů a vyhledávání obsahu online vůbec. Na druhou stranu přehršle informačních zdrojů zavalujících uživatele množstvím (mnohdy nedůležitých, neodpovídajících, případně i lživých) informací může být snadno zavádějící. Namísto schopnosti vyhledat informaci se tak stává klíčovou schopnost rozpoznat, která z nabízených informací je pravdivá či podstatná.

[79] Mimoto nejde o pouhé šíření (des)informací, ale o možnost působit na společnost vůbec, a to prostřednictvím ovlivňování veřejného mínění a nálady ve společnosti vůbec. Nedávným příkladem budiž zprávy upozorňující na působení tzv. trollů [tj. osob zveřejňujících provokativní prohlášení v diskusích atp. s cílem vyprodukovat množství jinak zbytečných reakcí, zpravidla rozhořčených či jinak emotivních, viz (UITS, 2018)] ve snaze vyhrotit veřejnou debatu o vakcinaci a rozdělit společnost, resp. vzbudit zdání rozdělené společnosti (což by znamenalo s ohledem na sebenaplňující se proroctví prakticky totéž, viz dále), viz např. (McNeil, 2018) nebo (Broniatowski, a další, 2018).

[80] V loňském roce se např. hojně hovořilo o tzv. trollech, tj. osobách zveřejňujících provokativní prohlášení v diskusích atp. s cílem vyprodukovat množství jinak zbytečných reakcí, zpravidla rozhořčených či jinak emotivních (UITS, 2018). Mnozí z nich usilovali o vyhrocení veřejné debaty o vakcinaci a rozdělení společnosti, resp. vzbuzení zdání rozdělené společnosti, což by znamenalo s ohledem na princip sebenaplňujícího se proroctví prakticky totéž (McNeil, 2018), (Broniatowski, a další, 2018). Pravidelně se též poukazuje na trollování v předvolebním období.

šiřitele) obsahu než původce, přesto se velmi aktivně podílí alespoň na jeho hodnocení, případně doplňování činností (Bárta, a další, 2018).[81]

2.1. Shrnutí ke kyberprostoru a novým médiím

Dovolím si tvrdit, že není na místě hovořit o kyberprostoru jako o virtuální, či snad paralelní realitě, ale že jde o kyberprostor JAKOŽTO realitu, resp. součást reality. Všudypřítomná rozmanitá zařízení (IoT) propojená pomocí internetu a mobilních telefonů zasahují mnoha (nejen) každodenních činností, které usnadňují, slouží jako informační zdroj a především nabízí již těžko odmyslitelný komunikační prostředek. Zajišťují komunikaci psanou (sms, chat, email, instant messaging), mluvenou (VoIP) i videohovory, přičemž obvykle umožňují plynulé přecházení mezi jednotlivými formami.

Děti se setkávají s kyberprostorem od útlého věku, a lze je proto považovat za tzv. digitální domorodce, neboť de facto „vrůstají“ do digitální kultury, která je jim vlastní a tvoří pro ně prakticky stejně přirozený a samozřejmý svět jako ten reálný pro starší generace. Ty lze označit naopak za tzv. digitální imigranty, neboť se s digitálním prostředím seznamují až v pozdějším věku a více či méně se s tím teprve sžívají (učí se pracovat s jeho symbolikou, principy i specifickým jazykem, který ho charakterizuje).

Kyberprostor výrazně ovlivnil i podobu tradičních médií (tisk, rozhlas, TV), která přebírají některé formy tzv. nových médií: dostupnost prakticky kdykoliv a odkudkoliv, interaktivitu, hypertextualitu, disperzi a virtualitu. Nejrychleji se ovšem šíří obsah virálně na SNS, a to vzhledem k tzv. komputerizaci kultury v podstatě jakýkoliv obsah. K tomu se přidává ještě časoprostorové rozpojení, které prakticky odstraňuje prostorová omezení komunikace a mění tradiční zónování času (spánek, zaměstnání atd.).

Rychle a masově se však může rozšířit i obsah, který je nepravdivý, zavádějící, zraňující, ať už jde o cílenou manipulaci či útok nebo nikoliv. Značně problematické může být rozpoznání takových informací i pro dospělého člověka, natož pak ze strany dětí a mladistvých postrádajících zatím životní zkušenosti a nadhled. Zvlášť ohroženi jsou na jedné straně nebezpečnými návody typu Modrá velryba, zejm. ve spojení se SNS, s jejichž pomocí sdílí své „úspěchy“ a výzvy pro ostatní. Na druhé straně je to zraňující obsah, jehož původci bývají samy děti a dospívající, a který už může zasahovat do trestněprávní roviny. Může jít o pomstu

[81] Dílčí dosud písemně nepublikované výsledky výzkumu, viz pozn. č. 40.

bývalému partnerovi nebo vydírání (v kategorii mládeže však obvykle bez majetkového zájmu), nicméně nejčastějším důvodem bývá zveřejnění a sdílení zraňujícího obsahu v rámci kyberšikany. ať už v podobě textu, fotografie či videa, skutečných či upravených. Rychlost a masovost šíření prostřednictvím nových médií a faktická nemožnost trvalého odstranění digitalizovaného obsahu pak vytváří na oběť značný psychický tlak.

Není proto pochyb o tom, že mládež je v kyberprostoru jako takovém ohrožena kriminalitou, a to především takovou, kde pachatelé jsou samy děti a mladiství. Blíže k tomu viz zejm. kapitoly **Kyberšikana** a **Sexting**.

3. Komunikace a identita[82]

Ke komunikaci v kyberprostoru patří řada specifik, předně v rámci ICT neprobíhá tváří v tvář (mimo videohovor). Vyplývá z toho několik důsledků, zejm. omezení nonverbálních signálů a s tím spojená rizika, specifický jazyk a absence některých komunikačních bariér. Zvláštní pozornost pak zasluhuje i vytváření vlastní identity a vztahu ke společnosti ve spojení s komunikací v online prostředí.

3.1. Komunikace

Při běžné komunikaci dvou osob[83] hovořící aktér nejprve formuluje zhruba svou myšlenku v mysli a následně ji kóduje, tj. převede do konkrétní podoby (slova a věty). Už při samotném kódování řeči se ztrácí část kódovaného obsahu v podobě nevyřčených či zamlčených předpokladů – např. sociální kontext (Giddens, 2000 str. 91), a v důsledku používaného jazykového kódu řečníka.[84] Takto kódované sdělení musí řečník sdělit druhému aktérovi, přičemž část obsahu sdělení předává i nonverbální komunikací. Příjemce sdělení je následně naopak dekóduje, přičemž část obsahu může být ztracena samotným sdělením (např. pro hluk v okolí příjemce neslyší vše). Další část obsahu pak může být změněna v důsledku dekódování příjemcem, který si „překládá“ obsah sdělení v rámci svých životních zkušeností, povědomí o tématu, znalostech hovořícího aktéra atp. Značnou roli hraje v tomto směru vědomostní zázemí obou aktérů (např. rozdílná představa „berana“ u řezníka a astrologa) a jejich symbolická imaginace ve smyslu přikládání obsahového významu tomu či onomu symbolu. Mimoto do komunikace vstupuje i osobnost obou aktérů, jejich aktuální emoce, stereotypy, předchozí sociální i jiné zkušenosti, předjímání (vnímaný obsah do jisté míry v mysli uzpůsobujeme tak, aby odpovídal tomu, co očekáváme).

Při komunikaci v digitálním prostředí nikoliv tváří v tvář se dost dobře nedá vůbec uvažovat o čtení řeči těla co do vzdálenosti komunikujících, hmatových kontaktů, pohybu těla a rukou a samozřejmě o výrazech obličeje (proxemika, haptika, kinezika a gestika, mimika). Přitom obsah komunikace dedukují za jiných okolností účastníci zřejmě nejméně z poloviny na

[82] Kapitola zahrnuje i text vytvořený kolektivem autorů coby výukový materiál pro pedagogy v rámci projektu Škola bezpečně online: Zvýšení kvality vzděláván v oblasti bezpečného užívání internetu v Pardubickém kraji, CZ.1.07/1.3.12/04.0016, na jehož přípravě se autorka podílela, a tam uvedených zdrojů, viz (Lukášová, Pacák, Mašková, & Brandejsová, 2012), k ostatním metodickým materiálům v rámci tohoto projektu viz (Národní centrum bezpečnějšího internetu). Mezi zde využité zdroje patří především (Nakonečný, 1999),(Coveey, 1998), (Slaměník & Výrost, 2001) a (Glasser, 2001).

[83] K základnímu nástinu struktury komunikace obecně viz např. (wikisofia).

[84] Zda se jedná o tzv. uzavřený (omezený) nebo otevřený (rozvinutý) jazykový kód, které se liší množstvím nevyřčených předpokladů, abstraktností, délkou vět a složitostí slovních spojení, bohatostí výrazů atp. (Bernstein, 1971).

základě neverbálních signálů (Vymětal, 2008 str. 54), (Gibbs, 2012). Aktéři se ochuzují kromě neverbálních projevů také o paralingvistické projevy (mimo VoIP a videohovor): informace skrytě obsažené v tónu a dynamice řeči (emoce, zaujetí aj.), v mimoslovních složkách (koktání plynoucí z napětí, zrychlený dech atp.) i v časovém aspektu řeči (pomlky značící váhání aj.) (Křivohlavý, 1988). Mnohem snáze tak vznikají konflikty plynoucí ze vzájemného nedorozumění aktérů, kdy např. každý přiřazuje vyřčené větě jiný emoční náboj (typicky rozpoznání sarkasmu či ironie).

Ke konfliktům z nedorozumění se přidává obtížnější odhalení případného nesouladu verbálně a neverbálně sdíleného obsahu – typicky v situaci, kdy mluvčí neříká pravdu, něco zamlčuje, vystupuje pod cizí identitou atd. A tak zatímco při osobním kontaktu tváří v tvář by např. zákazník vzhledem k chování prodejce záhy pojal podezření, že nabízené zboží nemá tvrzené kvality, při navštívení e-shopu se mu může jevit nabídka zcela v pořádku, viz např. (2014). Obdobně je např. jednodušší přesvědčit příjemce (resp. příjemce se snáze nechá přesvědčit) k poskytnutí finanční částky v důsledku pocitu sounáležitosti vyvolané falešným dojmem nezasloužené tíživé životní situaci žadatele atd.

Kyberprostor lze proto snadno využít k vyvolání falešného dojmu (identita, pravdivost, upřímnost atp.). Navíc komunikace pouze písemnou formou funguje do jisté míry jako „černá hodinka“: bez viditelné reakce druhého účastníka (či ostatních účastníků) a při skrytí fyzických projevů hovořící osoby (např. červenání se ze studu) je pro ni mnohem snazší vyjevit niterné pocity a přání a více se druhému otevřít než při komunikaci tváří v tvář. Šikovný tazatel se za pomoci několika podpůrných projevů (vyjádření zájmu, empatie atp.) dozví od tázaného množství osobních údajů a intimních informací.

Digitální forma komunikace díky omezení fyzických i psychických bariér usnadňuje např. navazování a udržování kontaktů. Zároveň však hrozí přesunutím takových kontaktů právě téměř výlučně jen do „virtuální“ podoby, s upřednostněním snazší, digitálními prostředky zprostředkované komunikace před setkáním obsahově bohatšího, leč náročnějšího tváří v tvář.[85] Navíc při vyjadřování bez fyzické přítomnosti ostatních účastníků nemůže mluvčí bezprostředně sledovat jejich reakce a adekvátně na ně reagovat, zejm. při písemné formě. Výrazně se také zvětšuje odchylka při dekódování obsahu sdělení a úměrně tomu roste i pravděpodobnost neadekvátní reakce (typicky ironická poznámka, kterou ostatní účastníci

[85]Jestliže se nedostatky sociální komunikace jedince týkají i virtuálního prostředí, o to větší pak může být jeho frustrace při srovnání s osobami sociálně úspěšnými v reálném světě a úměrně tomu i ve virtuálním prostředí.

komunikace dekódují jako vážně míněnou a neadekvátní kritiku, zareagují proto obranou, kterou ovšem původní mluvčí dekóduje jako ofensivní prohlášení vůči sobě samému atd. až po vzájemné konfliktní jednání). K tomu se přidává psychická zranitelnost, neboť v online prostředí jsme přítomni svou myslí, a chybí tudíž fyzická bariéra, která v reálném prostředí alespoň zmírní případný útočný projev,[86] a kritika tak snáze pronikne do samotného nitra kritizované osoby a zraní ji.

Děti a mladiství jsou zvýšeně ohrožení komunikačními konflikty už jen z titulu svého věku. Pozornost věnují situaci tady a teď, budoucí dopady svého jednání příliš neřeší. Ke komunikaci přistupují nenuceně a neohroženě, s důvěrou. Ochotně poskytují osobní údaje, soukromé informace, fotografie. Experimentují se sexualitou, ve zdánlivě anonymním prostředí internetu snadněji než v kontaktu osobním. Jsou kritičtí, neváhají zveřejňovat nekonformní názory, mají tendenci k radikálnímu hodnocení a řešení, které ovšem s vytracením se stávajícího kontextu dostává jiný rozměr (typicky usmířivší se kamarádky, jejichž předchozí vzájemné napadání se na SNS však zůstává stále přítomno). To dohromady vytváří značný konfliktní potenciál, zejm. s ohledem na rychlost a potenciální masovost šíření obsahu na SNS a jen limitovanou možnost jeho následného odstranění. Může jít i o relativně banální jednání, např. kritiku selfie zveřejněné na FB, po které následuje vlna odsuzujících komentářů vůči kritikovi ze strany ostatních společných „přátel“ kritizující a zveřejněné osoby, kteří nesouhlasí. Jiným typickým příkladem budiž nepochopená ironie nebo žertem míněná urážka vzatá vážně. Snadno se též vyhrotí zpočátku neškodné pošťuchování, kdy některý z aktérů začne překračovat únosnou mez, aniž by ho na to upozornil jinak neverbálně zřejmý nesouhlas „přihlížejících“.[87] Na rozdíl od dnešních dospělých navíc digitální domorodci nerozlišují komunikaci a vztahy na virtuální a skutečné (Eckertová, a další, 2013 str. 21) – ty virtuální jsou pro ně stejně reálné a důležité, jako ty tváří v tvář.

Předchozí generace vyrůstaly v mnohem užším vzájemném fyzickém kontaktu s vrstevníky (pobyt venku, sportovní akce atp.), vzájemná komunikace i komunikace s dospělými byla rozvinutější, bohatší, košatější. Současná mládež se takto stýká méně, bývá (dobrovolně) uzavřena v bytech a rodinných domech, do školy a na kroužky (často individuálně zaměřené) je často dopravují rodiče samotné autem namísto společné cesty v MHD s vrstevníky, mnohé

[86] Zmírní i takovým „banálním“ aktem jako založení rukou na hrudi, odmítavé kroucení hlavou atp. Samozřejmě, že tak lze činit i při jednání online, nicméně bez přítomného druhého postrádá do jisté míry jinak potenciálně uspokojivý efekt.

[87] Bez včasného zakročení pak může útočné jednání přejít i v kyberšikanu, ke které se postupně začnou se slovními útoky přidávat i ostatní.

hromadné akce jsou pro ně finančně nedostupné. Potřebu vzájemné komunikace a zpětné vazby ale mají stejnou jako předchozí generace, což je vede k využívání dostupných komunikačních kanálů – především internetu. Zároveň lehkost komunikace online vede k jejímu nadužívání oproti reálnému prostředí, kdy mládež sama od sebe preferuje využití SNS namísto osobního kontaktu. Psychické potřeby dítěte jsou uspokojovány každodenním stykem s co nejširším a nejrůznorodějším sociálním prostředím, kde se může prezentovat a přirozeně interagovat, což SNS nabízí v prakticky neomezeném měřítku. V extrémních případech internetové společenství a aktivity zcela nahradí přirozenou podporu rodiny a přátel.[88]

3.2. Identita

V životě každého člověka hraje významnou roli jeho sociální okolí, společnost. Zvlášť v období dospívání, kdy dítě stále více interaguje se svým okolím, učí se vzorce chování, vytváří a upevňuje představy o světě a sobě, testuje a nastavuje své hranice, vč. práv svých i ostatních, přijatelného a nepřijatelného, dovedností vlastních i těch druhých. Internet k tomu představuje časté a vítané cvičiště. Mládež tak činí hraním her, vyhledáváním obsahu pro starší, sledováním, vytvářením a úpravami videí a fotografií, sdílením, šířením provokativních názorů, experimentováním se vztahy a sexualitou. Internet jim umožňuje zkoušet různé varianty sebeprezentace, potažmo identity (vč. fiktivní identity). Sociální vazby a zejm. tzv. referenční skupiny a skrze ně sociální nátlak[89] patří k podstatným vlivům na případnou kriminální kariéru jedince. Jejich prostřednictvím si jedinec osobuje morální hodnoty a vnímá míru spravedlnosti[90] panující v dané společnosti, což posílí nebo naopak oslabí jeho identifikaci s ní.[91]

Podle J. Rawlse (Rawls, 1995) patří ke stěžejním prvkům spravedlnosti otázka „pravidel hry“, vč. např. procedurální spravedlnosti - zacházení s obdobnými případy obdobně (Rawls, 1995

[88] Zhruba pětina uživatelů (zejm. mužů) preferuje online kontakty před offline (Zaheer, a další, 2008 str. 47).
[89] S vlivem okolí pracuje např. Hirschiho teorie sociálních vazeb, teorie kontroly, teorie sociálně-kognitivního učení aj., viz např. „Vývoj názorů na příčiny kriminality, jednotlivé kriminologické směry a trendy“ (Válková, a další, 2012).
[90] Existuje několik pojetí spravedlnosti. Nominalismus ji chápe jako označení de facto libovolného souhrnu jevů v dané době a místě obecně považovaných za spravedlnost. Naproti tomu pro realismus je spravedlnost paralelou hmotného mnohostranného předmětu, konkrétní čas a místo má vliv jen na to, z jakého úhlu pohledu ji nahlížíme. Na pomezí mezi nimi se pak pohybuje přístup považující spravedlnost sice za koncept vykonstruovaný člověkem, avšak s vlastním základem zakořeněným v lidské přirozenosti (Elders, a další, 2005).
[91] Principům spravedlnosti a uznání se podrobněji věnuje diplomová práce a studentská odborná činnost autorky, z nichž tato část textu vychází (Lukášová, 2009), (Lukášová, 2010).

str. 18). Koncept „hry“ se vyskytuje v humanitních oborech v řadě podob a pojetí: např. L. Wittgenstein používá výraz „jazykové hry“ k vyjádření taktického prvku řeči (Wittgenstein, 1922), nebo přirovnání fungování společnosti a sociálních vztahů k instituci divadla a hraní divadelní hry (Goffman, 1999). Paralelu lze nalézt i v online prostředí, zvlášť patrně na SNS, kde vytváření vlastního profilu představuje ono jeviště s často pečlivě připravenými kulisami, zatímco příprava těchto kulis a soukromá neveřejná komunikace s vybranými osobami zákulisí.

Vnímání (ne)spravedlivého přístupu vůči jednotlivci vychází kromě objektivních vnějších okolností z identity jedince, postavení ve společnosti a vnímání vlastního postavení. Společnost potřebuje socializované jedince, kterým jsou vlastní uznávané vzorce jednání a kteří jsou uspokojovaní a odměňovaní, jednají-li s nimi v souladu (Parsons, 1971). Sebeidentifikace se společností je nerozlučně spojena s její legitimizací a symbolickým světem a významně ovlivňuje dodržování norem, sociálních i právních aj. (Berger, a další, 1999 str. 172). Společnost sestává z mnoha sociálních skupin a sociálních vztahů, jejichž prostřednictvím jedinec zakouší (zne)uznání. Prakticky vždy lze nalézt dichotomii „my“ a „oni“, párové kategorie jsou nevyhnutelné a zpravidla usnadňují sociální kooperaci (Tilly, 1998). Mohou být zakotveny biologicky - např. muž/žena, i existovat jako sociální konstrukt (Berger, a další, 1999). V prostředí internetu nalezneme prakticky neomezené množství zejm. sociálně konstruovaných párových kategorií, a to i takových, které by mimo online prostředí jen těžko nacházely dostatek obdobně smýšlejících osob k utvoření skupiny (např. neobvyklý koníček jako spojující prvek).[92]

Identita je nerozlučně spojena se seberealizací a sebenaplněním, k nimž dochází zpravidla v rámci určité společnosti a kultury prostřednictvím vztahu s druhými: „svou identitu určujeme neustále v dialogu a někdy dokonce v zápase s tím, co v nás chtějí vidět naši signifikantní druzí” (Taylor, 2001 str. 49).[93] Přílišná roztříštěnost společnosti vede k pocitům odcizení a vyloučenosti, potažmo nedostatku uznání. Dotyčný pak stále více nahlíží společnost instrumentálně, jako pouhý prostředek k dosažení svých individuálních cílů, a lne k sociálním hnutím či skupinám, které o ně usilují bez ohledu na důsledky pro společnost jako takovou. Nicméně i takové kategorie mohou přispět k opětovné identifikaci se společností, a

[92] Např. „zájemci“ o sebevraždu vyhledávající podobně smýšlející osoby a skupiny, odkud pak mohou získat i partnera pro tzv. sebevražedný pakt – dohodu dvou a více osob o společném spáchání sebevraždy (Auxéméry, a další, 2010).
[93] Identitu samozřejmě utváří i biologické a psychologické aspekty, které zde nechávám stranou.

to když nastolí určité „sporné otázky, za nimiž se rýsují společné cíle“ (Liberální společnost, 1994 str. 47).

Identifikace osob s většinovou společností představuje významný kriminogenní faktor: není-li dostatečná, ve společnosti se začne stále více projevovat stav anomie,[94] tedy situace, v níž se jedinec přestává přizpůsobovat sociálním normám (Giddens, 2000 str. 555). S nárůstem porušování sociálních norem samy postupně ztrácí svou závaznost, resp. vytrácí se sociální tlak na jejich dodržování, což opět v kruhu vede k jejich korozi a dalšímu porušování. Jedná-li se o normy vtělené do trestněprávní podoby, stoupá kriminalita. Roli hraje především identifikace s kulturními cíli společnosti a s dostupností legitimních prostředků k jejich dosažení.[95] Pokud těchto cílů nelze dosáhnout společností uznávanými legitimními prostředky (nebo jen se značnými obtížemi), vzniká napětí, které dotyčný ventiluje tak, že přizpůsobí své jednání některým ze způsobů v následující tabulce. V trestněprávní rovině stojí za pozornost především „inovace“: dosahování uznávaných cílů nelegitimními prostředky, typicky např. obstarání majetku krádeží. S rostoucím množstvím „vzpoury“ (vytvoření alternativního žebříčku hodnot a cílů i způsobů jejich dosažení) se pak postupně rozmělňují sociálně uznávaná „pravidla hry“ a stoupá hrozba anomie.

Tab. č. 2: Přehled reakcí na anomický tlak podle R. Mertona[96]

Druh reakce	Kulturní cíle	Legitimní prostředky	Anomický tlak je redukován
Konformita	uznávány (+)	akceptovány (+)	úspěšně legitimními prostředky
Inovace	uznávány (+)	odmítnuty (-)	použitím nezákonných prostředků
Ritualismus	odmítnuty (-)	akceptovány (+)	snížením nároků
Únik	odmítnuty (-)	odmítnuty (-)	únikem ze společnosti
vzpoura	nahrazeny (-/+)	nahrazeny (-/+)	předefinováním cílů a norem

K významným hodnotám moderní západní společnosti patří sociální a ekonomický status, přičemž lze diskutovat o primátu toho kterého a jejich vzájemné převoditelnosti.[97] S uznáním

[94] Blíže k anomii viz dílo E. Durkheima.
[95] Původní Durkheimovu teorii anomie dopracoval přidáním teorie napětí R. K. Merton zejm. ve své publikaci Social Theory and Social Structure.
[96] Převzato z Bock, M. Kriminologie. 2. vyd. Mnichov: Verlag Vahlen, 2000, str. 79 prostřednictvím (Válková, a další, 2012 str. 93).
[97] Např. podle N Fraserové jsou zejm. sociální a ekonomický kapitál jen omezeně vzájemně prostupné (Fraser, 2007 str. 10), K. Günther (Günther, 1997 str. 35) nebo Ch. Tilly (Tilly, 1998) kladou důraz na distributivní spravedlnost. Naproti tomu A. Honneth hovoří o distributivní a sociální spravedlnosti jako pouze rozdílných perspektivách a ekonomické nerovnosti pokládá za důsledek kulturního řádu (Fraser, a další, 2004 str. 221).

je spojen především symbolický kapitál (úcta, prestiž, moc), který se odvíjí od statutu jedince v rámci společnosti. Umožňuje získání ekonomického (např. majetek), kulturního (např. vzdělání) i sociálního kapitálu (např. síť sociálních kontaktů) a naopak jejich prostřednictvím lze zase získat symbolický kapitál (např. získat uznávaný post díky majetku, vědomostem či známému).[98] Kapitály nachází své uplatnění i v online prostředí: např. kulturní kapitál začínajícího youtubera (způsob vyjadřování, vybraná témata a názory, znalosti a schopnosti atp.) povede záhy k jeho značné sledovanosti, potažmo ekonomickému kapitálu ve formě příjmů z reklamy, sociálního kapitálu skrze sociální síť přívrženců a především symbolického kapitálu v podobě kulturního vlivu na ně. Párové kategorie pak mají tendenci vyvažovat pocity (zne)uznání, potažmo (ne)spravedlnosti. Např. nedostatek ekonomického kapitálu v dané kategorii je vyrovnán jejím silným sociálním kapitálem, který vychází ze sdíleného kulturního kapitálu (např. i postoje, tradice atp.). Kapitál slouží jako určitý ukazatel „úspěšnosti" jedincova začlenění do společnosti, resp. měřítko jeho uznání společností. Ne vždy se však dotyčný orientuje na většinovou společnost, naopak podstatnější bývá přístup referenčních skupin, tj. takových, s jejichž hodnotami, postoji a názory se jedinec identifikuje a jejichž je nebo se chce stát členem.[99] Může se jednat i o skupinu zastávající zcela odlišné hodnoty[100] oproti většinové společnosti – např. organizovaná zločinecká skupina uznávající sice obecně sdílené cíle (např. ekonomický profit), leč využívající k jejich získání nelegitimních prostředků (korupce, prodej drog atp.).

Uznání ze strany společnost sestává mimo kapitálů ze sociálního a právního ocenění. Sociální se týká schopností, jimiž se individua odlišují (vědomí, že vlastní schopnosti a výkony jsou pro společnost významné, a proto si člověk váží sebe samého), právní ocenění se týká schopností vlastních každému, a je proto spojeno s principem rovnosti. Právní uznání se proto „má normativně orientovat na rozšiřování své obecnosti a kontextuální citlivosti vůči zvláštnímu postavení jednotlivců" (Honneth, 1996 str. 20). Předpokladem obojího je existence společně sdílených hodnot jako neustálého symbolického boje různých skupin o uznání. Každý jedinec potřebuje vědomí, že ostatní jej uznávají, a že stejně tak, jako jsou oni potřební pro něj, je i on potřebný pro ně.[101] Aby se tak společnost vyhnula rostoucí anomii a s tím

[98] Blíže ke konceptu různých forem kapitálu a jejich převoditelnosti viz dílo P. Bourdieu.

[99] Ať už jde o otevřenou referenční skupinu (např. vyznavači určitého módního stylu) nebo uzavřenou s podmíněným členstvím (Bauman, 2000).

[100] Zatímco např. v roce 2009 bylo 78 % respondentů přesvědčeno o správnosti trestání veřejných projevů sympatií k rasismu (Zeman, a další, 2010 str. 63), přívrženci některých hnutí potlačujících práva a svobody člověka by zajisté tento postoj nesdíleli.

[101] Slovy J. Rawlse: „za prvé je zřejmé, že blaho každého jednotlivce závisí na způsobu společenské kooperace, bez níž by nikdo nemohl vést uspokojivý život. Za druhé, o dobrovolnou kooperaci můžeme někoho požádat

spojenými dopady na kriminalitu, potřebuje zapojit převážnou většinu svých členů do funkčního celku, obecně považovaného za vyvážený a spravedlivý. Je proto pro ni žádoucí rozšiřovat své uznání: "... na jedné straně se jedná o proces individualizace, tedy o posílení šancí na legitimní vyjádření osobních podílů, na druhé straně o proces sociální inkluze, tedy o rostoucí zahrnování subjektů do okruhu plnohodnotných členů společnosti" (Fraser, a další, 2004 str. 238).

Trvání na právním a sociálním uznání ovšem nemusí být dostačující, neboť nemohou-li dotyční hovořit při prosazování svých požadavků za sebe samé (jedná se pak "o nich bez nich"), výsledné řešení zůstává výrazem vůle hegemonní kultury (byť může být pro dotyčné výhodné a žádoucí). Podle nominalisticky orientovaného J. Habermase je proto podstatné, čemu dávají přednost sami ti, kdo se cítí zneuznáni, ať už ekonomicky nebo sociálně. K institucionálnímu pojetí se tak přidává komunikativní paradigma ve spojení s normativitou společnosti, kterou lze „chápat jako systém sociálních institucí, jejichž rámec je komunikací stanoven, ale zároveň každou komunikaci podmiňuje a teprve umožňuje" (Přibáň, 1996 str. 62). Podmínkou vůle k vyjádření svých potřeb je důvěra ve vlastní schopnosti – sebeúcta, jejíž podmínkou a předpokladem je veřejné kladné hodnocení ze strany jiných lidí. Alespoň v minimální míře toto obvykle zajistí už jen samotný „zájem komunity, k níž náleží a kde nachází své snahy potvrzeny svými druhy" (Rawls, 1995 str. 261).

Internet ve spojení s globalizací přispívá mj. k seskupování osob na základě společných zájmů. Díky tomu mohou mnozí jedinci, kteří by sami o sobě neměli možnost náležitě zřetelně vyjádřit své potřeby, získat hlas, potažmo uznání. Podle J. Habermase (Habermas, 2000), (Habermas, 2001) je třeba přistupovat ke každému stejně bez ohledu na jeho kulturní či ekonomická specifika a měl by mít možnost svobodně hovořit ve prospěch svých zájmů, přičemž svoboda musí být vnitřní i vnější.[102] Podstatnou roli zde hrají média a postavení veřejnosti. Tradiční média prakticky soustavně vyvíjí na své konzumenty určitý tlak a ovlivňují je, ať už prostřednictvím zpravodajství, zábavy, ale třeba i reklamy.[103] Jedinec je proto do jisté míry svobodný pouze zdánlivě, nicméně je třeba usilovat o to, aby tato svoboda

jenom tehdy, jsou-li podmínky spolupráce rozumné." A jinde: „je společným cílem příslušníků dobře uspořádané společnosti kooperovat spolu tak, aby se realizovala jejich vlastní povaha i povaha ostatních, jak to dovolují principy spravedlnosti" (Rawls, 1995 str. 71 a 310).

[102] J. Sokol charakterizuje svobodu tak, že člověk „jedná s rozvahou, po zralé úvaze … jednání je víc než jen reakce. Je víc především proto, že sleduje nějaký cíl – cíl, který je můj, nikoli jen vynucený okolnostmi. Na rozdíl od reakce jako odpovědi na něco, co tu teď právě je nebo bylo, je pravé jednání přípravou na něco, co teprve přijde, případně cestou, vedoucí k nějakému žádoucímu cíli" (Sokol, 1998 str. 75).

[103] Výběr konkrétních událostí, o nichž zpravodajství referuje, čas vysílání, způsob podání informace , obsah, poselství, emoční náboj, vzorce chování, paradigma každodennosti i výjimečných událostí atd.

byla co nejširší. Vnější svoboda zahrnuje faktickou možnost zapojit se do veřejné debaty a vnést do ní i svůj diskurs dle svého uvážení – tedy např. vystupovat jako člen svébytné menšinové kultury, anebo naopak svou příslušnost k ní odmítnout.[104] Záleží potom do jisté míry na každém jednotlivci, resp. na každé skupině, zda se rozhodne udržovat konkrétní párovou kategorii, spojenou zpravidla s určitou nerovností, neboť vliv na udržování (jakékoliv) kategorie má i samotné její rozlišování (Bourdieu, 2000). K odstranění rozlišování určité kategorie (např. „trestanec“) pak vede jedině úsilí o to, aby na ni společnost „zapomněla“, a to paradoxně v rozporu s převládajícím názorem, že předpokladem řešení nežádoucích nerovností je upozorňování na ně (resp. výsledkem veřejné diskuse může být zlepšení postavení dosud znevýhodněné skupiny, nikoliv však odstranění jejího znevýhodnění vůbec). Skutečnost, že poukazování na faktickou existenci určitých nerovností slouží do jisté míry jako jejich potvrzení, potvrzuje i princip sebenaplňujícího se proroctví: spolu s přesvědčením o existenci určitého sociálního faktu se pak tento stává zcela reálným ve svých důsledcích bez ohledu na to, zda reálně skutečně existuje či nikoliv (Merton, 1948), (Merton, 2007).[105]

Každá strana párové kategorie proto potřebuje mít svůj hlas, slyšitelný ostatními. I v případě, kdy se za práva menšin postaví většinová společnost a učiní taková opatření, aby samotný fakt menšinovosti nevedl příslušníky dané skupiny k zakoušení diskriminace, stále půjde o projev mocenské nadvlády a autoritářského postavení většiny. Menšina, resp. znevýhodněná strana párové kategorie by proto měla mít možnost hovořit v dialogu s většinou za sebe samu – jen tak se může stát součástí občanské společnosti, která představuje „prostor neomezeného a nezávislého lidského spolčování, jenž ve své nezávislosti vytváří ochranný val proti možné rozpínavosti státní moci, byť by byla mocí demokratickou“ (Müller, 2002 str. 28). Občanská společnost představuje protiváhu přirozené mocenské rozpínavosti státního aparátu, dává prostor pro soupeření různých společenských hodnot, zájmů a priorit a jejich prosazováním.

[104] Uvedené pojetí je vtěleno mj. i do § 3 odst. 1 NOZ, podle kterého soukromé právo chrání důstojnost a svobodu člověka i jeho přirozené právo brát se o vlastní štěstí a štěstí jeho rodiny nebo lidí jemu blízkých takovým způsobem, jenž nepůsobí bezdůvodně újmu druhým. „Zákonodárce si sebeméně nenárokuje právo určovat, co je oním štěstím, o něž se soukromá osoba bere; zavazuje se ale poskytnout mu nástroje pro to, aby se o ně brát mohl, ať je spatřuje v čemkoliv, pokud tím nebude působit újmu druhým“ (Švestka, 2014 str. 41).

[105] Může jít např. o dojem vysoké míry korupce, který sám o sobě snižuje odrazující sociální tlak, ba může k ní i nepřímo přispívat úměrně hloubce zakořenění přesvědčení, že ostatní jednají korupčně, a tudíž při vyhnutí se takovému jednání se dotyčný (více méně) dobrovolně staví do nevýhodné pozice. O to větší napětí pak v takové situaci zakouší, neboť pociťuje nesoulad mezi obecně uznávanými cíli (např. získání obchodní zakázky) a nelegitimními prostředky k jejich dosažení – v tomto případě trestněprávním korupčním jednáním (§ 331-334 TZ). Napětí plynoucí z využití nelegitimních prostředků bude ovšem redukováno úměrně míře obecného přijímání korupčního jednání, kdy právní norma zakazující uvedené jednání nenajde dostatečnou odezvu v obecném společenském postoji, a tudíž bude moci působit pouze silou autority vyplývající jen a pouze ze závaznosti právní normy jako takové.

Jakmile se lidé identifikují se společností, mohou jejím prostřednictvím pociťovat uznání, potažmo sebeúctu a úspěšnou seberealizaci.

Zajímavým příkladem přínosu internetu může být v tomto směru jeho pravděpodobný pozitivní vliv při „démonizaci" určité skupiny, kdy na jednu stranu sice může štvavá kampaň nabrat enormních rozměrů (zejm. co do rychlosti a rozsahu šíření zpráv), na druhou stranu umožňuje opovrhované skupině nechat zaznít i svůj hlas a argumenty, diskutovat se svými odpůrci a vzájemně si poskytovat podporu. Názorný příklad lze nalézt v „úspěšné" kampani vedené proti příznivcům heavy metalu v 80. letech 20. st. v USA a jejímu „neúspěšnému" opakování ve Velké Británii v roce 2008 (Brown, a další, 2012).

Požadavek na menšinu hovořící za sebe samu předpokládá (veřejný) prostor, ve kterém může být vyslyšena – obdobu antické agory.[106] Zde musí být dalším aktérem i většina (resp. alespoň část ostatních skupin v opozičním postavení), neboť samotné hlásání vlastních požadavků bez odpovídajícího publika znamená pouze prázdné deklarace. K agoře se přidal knihtisk, poté masmédia, avšak nová média ji přivádí k novým rozměrům. Internet pak nabízí téměř ideální prostor pro to „být slyšen". Zaručit rovnocenný prostor nebo pravidla napříč internetem sice nelze (i kvůli přeshraničnímu charakteru internetu ztěžujícímu jakékoliv právně závazné ujednání zahrnující celý internet), ať už jde o upload vlastního obsahu nebo změnu stávajícího, lze však aktivně vytvářet nový obsah, pro který internet coby platforma nabízí řadu míst a forem: SNS, web, osobní blog, upload videa na Youtube atp. Jakým způsobem pak skupina uchopí vlastní prezentaci, záleží na ní samotné (zda poukáže na vlastní jedinečnost, nebo ji naopak relativizuje, či o sobě zcela pomlčí), omezena je pouze vlastní kreativitou a vybavením (např. webkamera).[107] Výjimku zde tvoří pochopitelně osoby zcela bez přístupu k internetu.

Tradičně se mezi znevýhodněné osoby (přinejmenším co do možnosti hovořit za sebe samé) řadí kromě národnostních menšin, handicapovaných osob, seniorů aj. řadí i mládež a osoby blízké věku mladistvých, potažmo tzv. mladí dospělí. Doba, ve které začínají děti aktivně, pravidelně a samostatně používat internet a mobilní technologie se překrývá s obdobím, kdy pro ně začínají být zásadně významné vztahy s vrstevníky a kdy se vytváří a upevňují sociální dovednosti ve vztahu k širší společnosti. Jedním z nejdůležitějších vývojových úkolů v období

[106] Shromaždiště (obvykle spojeno i s tržištěm), kde se stýkali svobodní občané, aby diskutovali o filosofických otázkách a probírali věci veřejné (Otto, 1888 str. 457).
[107] Z formálního hlediska pochopitelně vyjma zákonných norem svého státu, místa své fyzické přítomnosti a místa fyzické přítomnosti serveru, na němž má být obsah umístěn.

dospívání je budování vlastní identity, kterou si vytváří mj. na základě zpětné vazby okolí, především vrstevníků. SNS aj. komunikační nástroje umožňují rozmanitou sebeprezentaci a masivní zpětnou vazbu.

S věkem a pokračující vlastní vyspělostí děti postupně nabývají svéprávnost až po zletilost, případně do přiznání svéprávnosti nebo uzavření manželství (§ 30 a 31 NOZ) a „má se ... za to, že nezletilý, který nenabyl plné svéprávnosti, je způsobilý právě k těm právním jednáním, která jsou co do povahy přiměřená rozumové a volní vyspělosti nezletilých jeho věku ...“[108] Zároveň se i tradiční média snaží je alespoň minimálně zapojit do aktivního působení ve veřejném prostoru prostřednictvím jim vyhrazených pořadů.[109] I přes tyto snahy však hlas dětí samých ve veřejném prostoru zůstával jen velmi slabý. Naproti tomu v digitálním prostředí internetu dostal zcela nový rozměr, ať už proto, že věkové složení uživatelů internetu je nižší oproti rozložení v rámci ČR,[110] nebo proto, že pohyb v digitálním prostředí je pro ně samozřejmý a přirozený, ale i proto, že jsou díky tomu schopny rychlou nápodobou, adaptací a hromaděním příležitostí (viz dále) virtuální prostředí téměř opanovat, přinejmenším ve vztahu ke svým vrstevníkům.[111] Věku oněch aktivně hovořících vesměs odpovídají i vybraná témata,[112] nicméně kromě předpokládané pozornosti upřené na hraní počítačových her, radosti a strasti dospívání, líčení atp., se lze setkat i s relativně vážnými tématy z oblasti politiky, světonázorů, zdraví, ekologie atp.[113] Občanská společnost jakožto protiváha moci státu tak nyní zahrnuje už i diskurs[114] dětí. Mají díky tomu možnost získat a uvědomit si svoje postavení v rámci společnosti, se kterou se o to snáze identifikují, oč snáze je ona přijímá.

V souvislosti s veřejným prostorem zasluhuje pozornost cenzura, vždy v nějaké míře v médiích přítomná. Lze ji rozlišit na vnitřní (autocenzura) a vnější. Autocenzura probíhá neustále v každém jako výsledek určitého morálního kompasu a vlastního sociálního cítění, které nám velí, zda a jak něco vyjádřit. Vnější cenzura pak neznamená pouze negativní zásah

[108] Viz komentář O. Frinty k § 31 občanského zákoníku (Švestka, 2014).
[109] Např. svého času (v letech 1997-2002) diskusní pořad Áčko na TV Nova, kam byly zvány i děti a jejich témata, nebo téměř každodenní hodinové vysílání s dětmi a pro děti na rozhlasové stanici Českého rozhlasu Dvojka v roce 2012 a později atp.
[110] Větší procento uživatelů-dětí a naopak menší uživatelů-seniorů. Velmi orientačně lze říci, že počínaje 16 lety (nejnižší sledovaný věk Českým statistickým úřadem co do užívání ICT) s rostoucím věkem klesá užívání ICT, viz tab. č. 1 v rámci statistického listu Českého statistického úřadu Využívání ICT jednotlivci 2016 (Český statistický úřad).
[111] Typicky tzv. Youtubeři (tj. osoby pravidelně zveřejňující tematicky prakticky neomezená videa prostřednictvím Youtube.com) se sledovanost jdoucí jen na České scéně do statisíců až milionů tzv. odběratelů (tj. osob sledujících daného Youtubera) a počtů shlédnutí, viz např. (Youtuberi.tv).
[112] Viz např. rozhovor s jedním z mladých (9 let) českých youtuberů (Sláma, 2016).
[113] Např. prezidentské volby (KOVY, 2018).
[114] Diskurs ve foucaultovském smyslu, tj. jakožto určitá forma vědění a specifický způsob rozumění světu, způsob, jakým se o něčem mluví (Foucault, 1994).

do svobody vyjadřování, nýbrž nastavuje určitá pravidla a omezení, která mohou být pro danou společnost i žádoucí.[115] Zároveň prakticky jakákoliv vnější cenzura s sebou vždy nese riziko přílišného omezení veřejného prostoru, potažmo občanské společnosti.[116] K podobné regulaci dochází i ze strany šiřitelů obsahu. Přesto je riziko mocenského uzurpátorství „pravdy" přímo úměrné možnosti koncentrace moci a rozhodovacích pravomocí co do určování obsahu médií. „Pravda" nemusí být objektivní, ale pouze zdánlivá v důsledku reálného dopadu sebenaplňujícího se proroctví,[117] což se ovšem nevztahuje pouze na tradiční média.[118] Protiváha moci byla vždy nějak přítomna (opozice, samizdat atp.), s nástupem internetu a zejm. SNS však nabývá na síle.

Internet tak na jednu stranu přispívá k rozmanitosti a občanské společnosti, na druhou zároveň utvrzuje stávající párové kategorie. Ekonomické nerovnosti spojené s párovými kategoriemi vznikají a reprodukují se prostřednictvím mechanismů vykořisťování, exkluze/hromadění příležitostí, nápodoby a adaptace (Tilly, 1998).[119] Vykořisťování probíhá formou odměňování a zavazování si osob, které zajišťují udržování této praxe, v online prostředí ovšem není tak snadné umlčet hlas kritiků poukazujících na mocenské postavení „elit" v důsledku vykořisťování, a nikoliv jejich vlastních schopností. Hromadění příležitostí nabývá na intenzitě v návaznosti na udržitelnou sociální síť. A tak zatímco v reálném prostředí je jedinec schopen udržovat svou sociální síť (ve smyslu skupiny osob, které mohou být aktivizovány, požádány o pomoc, sdílení atp.) o velikosti cca 150 osob, SNS umožňují udržení až několika

[115] Např. zákaz reklamy zboží, služeb nebo jiných výkonů či hodnot, jejichž prodej, poskytování nebo šíření je v rozporu s právními předpisy [§ 2 odst. 1 písm. a) zák. č. 40/1995, o regulaci reklamy a o změně a doplnění zákona č. 468/1991 Sb., o provozování rozhlasového a televizního vysílání], zákaz zveřejnit jakýmkoliv způsobem výsledky předvolebních nebo volebních průzkumů vztahujících se k volbě prezidenta republiky v určitém období (§ 35 odst. 8 zák. č. 275/2012 Sb., o volbě prezidenta republiky a o změně některých zákonů), nebo naopak zákonem zaručený vysílací čas pro volební kandidáty před konáním voleb (např. § 35 odst. 7 zák. č. 275/2012 Sb., nebo § 16 odst. 8 zák. č. 247/1995 Sb., o volbách do Parlamentu České republiky a o změně a doplnění některých dalších zákonů).

[116] Např. Hlavní správa tiskového dohledu / Ústřední publikační správa / Úřad pro tisk a informace vykonávající předběžnou cenzuru periodického tisku od 50. do konce 80. let 20. st. (Navara, a další, 2010 str. 33) nebo § 1 odst. 1 zák. č. 184/1950 Sb., o vydávání časopisů a o Svazu československých novinářů, podle něhož je posláním tisku mj. spolupráce na výchově československého lidu k socialismu.

[117] Viz výše. Hledání „pravdy" může být až trapně úsměvné, jako např. spor o existenci údajného článku F. Peroutky Hitler je gentleman, o němž hovořil toho času prezident republiky Miloš Zeman. Důsledky však mohou být i mnohem závažnější, jako např. přesvědčení o nadřazenosti jedné rasy nad ostatními. Mohou být i plíživé, jako např. přesvědčení o korupčním jednání úředníků vedoucí fakticky k jejich korumpovatelnosti (viz výše).

[118] Z dlouhodobého hlediska hrají významnou roli např. školní osnovy (Novinky, 2014), (2017). Obdobné snahy jsou patrné pochopitelně i v online prostředí (Procházková, 2016). Velmi rozporuplně se v tomto smyslu jeví návrh skupiny poslanců k zavedení nové skutkové podstaty trestného činu (a odpovídajícího přestupku) „porušování svobody projevu" (§ 179a TZ), který má kriminalizovat mazání příspěvků uživatelů ze strany provozovatelů velkých sociálních sítí (Skupina poslanců. Poslanecká sněmovna Parlamentu ČR. VIII volební období, 2019). Na jednu stranu sice rozšiřuje prostor svobody projevu, zároveň ale výrazně ztíží účinný boj SNS proti škodlivému obsahu a dezinformacím (kromě samotného omezení svobody provozovatele stanovit pravidla jím poskytované služby, tedy např. vymezit tolerovaný obsah příspěvků).

[119] Blíže ke vztahu kriminality a párových kategorií viz (Lukášová, 2010).

tisíc osob. Jednak zastupují paměť (ke každému kontaktu podávají snadno dostupné informace a archivují vzájemnou komunikaci), jednak šetří množství času možností oslovit v jediném okamžiku všechny nebo libovolný počet kontaktů naráz a hromadně s nimi komunikovat. Představují tak enormní potenciální sociální kapitál. Nápodoba se v online prostředí internetu přímo nabízí, vzhledem k rychlému a potenciálně masovému šíření jakéhokoliv obsahu. Pouze u adaptace (udržování známých sociálních zvyklostí de facto jen z toho důvodu, že jde právě o známé sociální zvyklosti, které lze změnit jen se značnými náklady) slouží internet v obou směrech: jednak utvrzuje stávající zvyklosti jako samozřejmé, jednak může naopak značně urychlit jejich změnu rychlým rozšířením jiného modelu.

Je všeobecně přijímáno, že internet je (přinejmenším v ČR) doménou převážně mladších generací,[120] které jsou si vědomy svých obvykle lepších uživatelských schopností i přístupu oproti starším generacím. Ve spojení s virtualitou a možnou eliminací dohledu ze strany dospělých (např. uzavřená chatovací místnost, anonymizovaný prohlížeč atp.) se tak může internet v pojetí dětí zdát jako prostor bez pravidel, nicméně i zde postupně vznikají mantinely a „pravidla hry“ spolu s dohlížiteli na ně, a to morální, uživatelské i právní. Morální pravidla postupně vytváří tzv. netiketu,[121] tj. soubor pravidel slušného chování online (gramaticky správné psaní vč. diakritiky, respekt k soukromí a osobním údajům druhých, neurážení, dbaní autorských práv atp.). To, co nazývám uživatelskými pravidly, se prolíná s morálními i právními. Na jedné straně stojí obvyklé zvyklosti v komunikaci vymezené technologickými standardy,[122] na straně druhé pak pravidla vymezená provozovateli služby (typicky SNS), s nimiž obvykle uživatel vyjadřuje souhlas samotným užíváním, případně výslovně. Mezi uživatelská a právní pravidla lze zařadit i určitou formu vnější cenzury: poskytovatelé služeb mnohdy deklarují regulaci obsahu[123] a obvykle zakazují využívání služeb v rozporu s právem.[124] Nakonec jsou zde právní pravidla stanovující základní rámec používání internetu, počínaje základními lidskými právy a svobodami přes regulaci online

[120] Viz (Livingstone, 2016) nebo Tab. č. 1: podíl uživatelů internetu starších 16 let.
[121] Viz např. (Chování.eu), (Satrapa, 2005) nebo zřejmě první významnější dokument vztahující se k netiketě v podobě RFC (Request For Comments, tj. určité doporučení v oblasti informatiky) z dílny IETF (The Internet Engineering Task Force, otevřená organizace věnující se standardizaci v oblasti internetu) z roku 1995 (IETF, 1995).
[122] Např. respektování časové prodlevy způsobené slabým signálem jednoho z účastníků VoIP, soukromý rozhovor na SNS vedený neveřejnou formou zpráv atp.
[123] Např. zákaz příspěvků mimo téma v bodě 8. Pravidel pro diskutující na serveru Slunečnice.cz (Slunečnice.cz).
[124] Např. zákaz podpory nebo propagace hnutí prokazatelně směřujícího k potlačení práv a svobod člověka v bodu 2.2.3 Zásad Uživatelského obsahu serveru Uložto.cz (Ulož.to).

prostředí po trestní zákony, pochopitelně vč. mezinárodních dokumentů (viz kapitola **Právní rámec kyberprostoru**).

Pokud uživatelé překročí vymezený rámec, kromě právních kroků (trestní stíhání, žaloba na ochranu osobnosti aj.) lze přistoupit i k zásahu po technické stránce a daný obsah blokovat. Může se tak dít ze strany koncových uživatelů (např. blokace obsahu či uživatele), formou rodičovské kontroly, nebo i ze strany provozovatele zařízení (např. zaměstnavatel blokující určitý obsah na svých pracovních počítačích). Do jisté míry lze obsah blokovat na úrovni samého státu prostřednictvím celoplošného blokování obsahu, vyhledávaných hesel, konkrétních adres atp. K těm nejpropracovanějším patří zřejmě činnosti států jako KLDR, Čínská lidová republika, Kuba, ale zřejmě i Rusko aj. (Wikipedie). I blokovaný obsah však může být dostupný, od přeshraniční Wi-Fi po anonymizované prohlížeče, zejm. nejpoužívanější Tor.[125]

Většina států moderní společnosti se ovšem snaží přístup k internetu podporovat a naopak zpřístupnit samotnou státní správy online. V ČR tak od roku 2007 (Ministerstvo vnitra ČR, 2010) funguje tzv. Czech POINT, jehož prostřednictvím lze v rámci jednoho univerzálního místa získat data z informačních systémů veřejné správy, úředně ověřit dokumenty, získat informace o průběhu správních řízení atd. (CzechPOINT). Digitalizace státní správy bývá již tradičně i součástí programového prohlášení vlády, naposledy tak učinila vláda Andreje Babiše dne 27.6.2018, která se zavázala mj. zajistit „...úplné pokrytí cenově dostupným vysokorychlostním internetem, propojení všech státních databází a elektronickou identitu pro každého občana.... vytvořit prostředí podporující českou společnost v digitální transformaci, tzv. Společnost 4.0[126] ...učinit klíčová opatření zejm. v oblastech uživatelsky přívětivých online služeb, digitálně přívětivé legislativy a centrální koordinaci ICT“ (Vláda České republiky, 2018). Hovoří se i o digitalizaci voleb, viz např. (Kubátová, 2018), základní předpoklad byl naplněn v podobě přijetí zákona č. 250/2017 Sb., o elektronické identifikaci (platný od 18.8.2017, účinný od 1.7.2018).

[125] Ať už jde o obsah považovaný za nelegální jen daným státem nebo napříč mezinárodním společenstvím (torservers.net), (Othman, 2013), (Reporters Without Borders, 2014), (Europol, 2014).

[126] Pozn. aut.: Společnost 4.0 nebo také čtvrtá průmyslová revoluce odkazuje na řadu technologických a v jejich důsledku i sociálních změn, jež se udály v posledních letech: vývoj umělé inteligence, kryptoměny, IoT, 3D tisk atp. Koncept „chytré továrny“ zřejmě zásadně promění trh práce, a tedy i ekonomické vztahy, požadavky na vzdělání atd. (wikipedie), (Fidrmuc, 2017). V rámci ČR byla vládou v roce 2017 ustanovena Aliance Společnost 4.0 jakožto platforma pro spolupráci subjektů z veřejného i soukromého sektoru a akademické sféry v zájmu přípravy ČR na probíhající a nadcházející změny spojené s digitalizací 4.0 (digiczech, 2016) a Strategie digitálního vzdělávání do roku 2020, viz (Ministerstvo školství, mládeže a tělovýchovy ČR), (Ministerstvo školství, mládeže a tělovýchovy ČR, 2014). Pro bližší zamyšlení nad Společností 4.0 viz např. (Haupt, 2018).

Elektronická identifikace má do budoucna umožnit rozšířit spektrum online využitelných služeb nabízených veřejným sektorem a vyžadujících ověřenou identitu. Místa, kde tak bude možné učinit, se proto zařadí mezi tzv. přístupové body expertních systémů. Expertní systémy (technické systémy organizující velké oblasti fyzického a sociálního prostředí) spolu se symbolickými znaky představují abstraktní systémy spojené s vyvazujícími mechanismy, které vytlačují sociální vztahy z jejich bezprostředního kontextu a spočívají na důvěře v abstraktní formy namísto jedinců je představujících (Giddens, 2003 stránky 27, 32 a 76). Internet lze považovat za takový abstraktní systém per se, patří k nejvýznamnějším institucím modernity, svázaných coby abstraktní systémy s mechanismy důvěry v důsledku vyvázání bezprostředních sociálních vztahů. Zvlášť důležité jsou proto kontakty s experty, resp. představiteli expertních / abstraktních systémů v tzv. přístupových bodech, jež zakládají (ne)důvěryhodnost představitelů, potažmo daného systému vůbec. V nich se tzv. beztvářný sociální vztah, založený na důvěře v abstraktní systém, znovu připoutává k lokálním podmínkám času a místa spojeným s důvěryhodností konkrétních osob (Giddens, 2003 str. 75). Na jedné straně tak stojí internet jakožto abstraktní systém reprezentovaný technickými parametry (dostupnost, zabezpečení, rychlost atp.), na straně druhé jako systém přístupný prostřednictvím představitelů – konkrétních osob více či méně zakládajících jeho důvěryhodnost: v případě služeb poskytovaných veřejným sektorem typicky úředníci zpracovávající požadavky občanů za přepážkami Czech POINT, jejichž profesionalita více či méně podtrhuje spolehlivost systému, tj. internetu ve spojení se státní správou. Naproti tomu stojí SNS (aj. aplikace) coby zosobnění internetu ve spojení se systémem mezilidské komunikace. V tomto směru jsou to v mnohem větší míře tvářné závazky, které jej reprezentují, a to tvářné od samého počátku, nikoliv znovunavázané přístupovými body po předchozím vyvázání. Kromě přenesení sociálních kontaktů z reálného světa na SNS zde dochází k vytváření mnoha dalších kontaktů a vazeb s osobami poznanými pouze virtuálně. Ty pak představují naopak beztvářné závazky spoléhající se na specifický abstraktní systém SNS s jejími symbolickými znaky (diskurs, pravidla atp.) i expertním systémem (technické parametry) a paradoxními přístupovými body, které lze spojit s konkrétními osobami jen velmi vzdáleně (typicky u nejpoužívanějších SNS hojně využívajících pro komunikaci s uživateli tzv. boty, tj. softwarovou AI).

3.3. Shrnutí ke komunikaci a identitě

Mezilidská komunikace skýtá mnohá úskalí, z nichž některá kyberprostor umocňuje, jiná naopak potlačuje. Část obsahu se vždy ztrácí v procesu kódování a dekódování a mění

v závislosti na aktérech. Při komunikaci v kyberprostoru (nejde-li o videohovor) se navíc vytrácí i neverbální řeč těla tvořící jinak tváří v tvář až polovinu předávané informace, mimo VoIP také paralingvistické projevy (např. napětí v hlase). Aktéři tak obsahu snadno přisoudí jiný emoční (např. sarkasmus), ale i věcný význam (vyplývající např. z nepochopeného kontextu). Ztížené je též odhalení nepravdy, zamlčování, manipulace, a naopak snazší podlehnout mylnému dojmu vzájemných sympatií, otevřít se a sdílet osobní a intimní obsah.

Omezení fyzických a psychických bariér sice usnadňuje komunikaci a navazování kontaktů, svádí však k preferenci virtuálních vztahů, které jsou pro digitální domorodce srovnatelné s těmi reálnými. Případná kritika a odmítnutí pak vzhledem k absenci fyzické bariéry snáze pronikne do nitra a zraní adresáta. To ohrožuje zejm. mládež, která zároveň patří mezi nejčastější „útočníky“, neboť zcela nedomýšlí důsledky svého jednání, je kritická a radikální a především sdílející, ať už jde o veřejnou prezentaci svých postojů, vzájemné pošťuchování nebo výslovné odsouzení.

V období dospívání děti a mladiství vytváří vlastní identitu, sociální vazby a vztah ke společnosti, a to z velké části skrze vnímání zpětné vazby, na jedné straně v podobě hodnocení vrstevníků, na druhé pak uznáním ze strany společnosti a vlastních tzv. referenčních skupin. Učí se „pravidla hry“, jejichž rovnocennost je předpokladem spravedlivého uspořádání společnosti. Člověk potřebuje zakoušet spravedlivé i nespravedlivé aspekty, aby se socializoval. Sociální vztahy dávají zakoušet pocity uznání i zneuznání konkrétním jedincům, ale i celým skupinám, párovým kategoriím v dichotomii „my“ a „oni“. V prostředí internetu je takových kategorií nepřeberné množství, neboť dává možnost sdružovat se bez ohledu na vzdálenosti, ekonomické rozdíly, kulturní odlišnosti atd. A tak zatímco do jisté míry rozmělňuje hodnotový rámec, potažmo socializaci jedince v rámci většinové společnosti, a tím přispívá k celkové anomii (a představuje tak určitý kriminogenní faktor), umožňuje zároveň redukci anomického tlaku předefinováním cílů a norem.

Aby to bylo možné, členové dané společnosti musí zakoušet uznání, od společnosti jako takové nebo od jejích částí (referenční skupiny, párové kategorie). V tomto směru představuje online prostředí pouze další platformu pro vzájemné převádění různých forem kapitálu (symbolický, ekonomický, sociální, kulturní), byť v některých směrech značně amplifikované. Výrazněji však vystupuje do popředí fakt, že klíčovou roli hrají oproti většinové společnosti především jednotlivé referenční skupiny, jejichž výběr je v kyberprostoru výrazně rozmanitější. Díky tomu může být i zakoušená nespravedlnost vůči

jedné straně párové kategorie vyvážená o to větším uznáním (potažmo nějakou formou kapitálu) v rámci této kategorie a zároveň má každý k dispozici mnoho potenciálních skupin / kategorií, jejichž prostřednictvím může zmírnit napětí vyplývající ze zneuznání v rámci jedné kategorie uznáním v jiné.

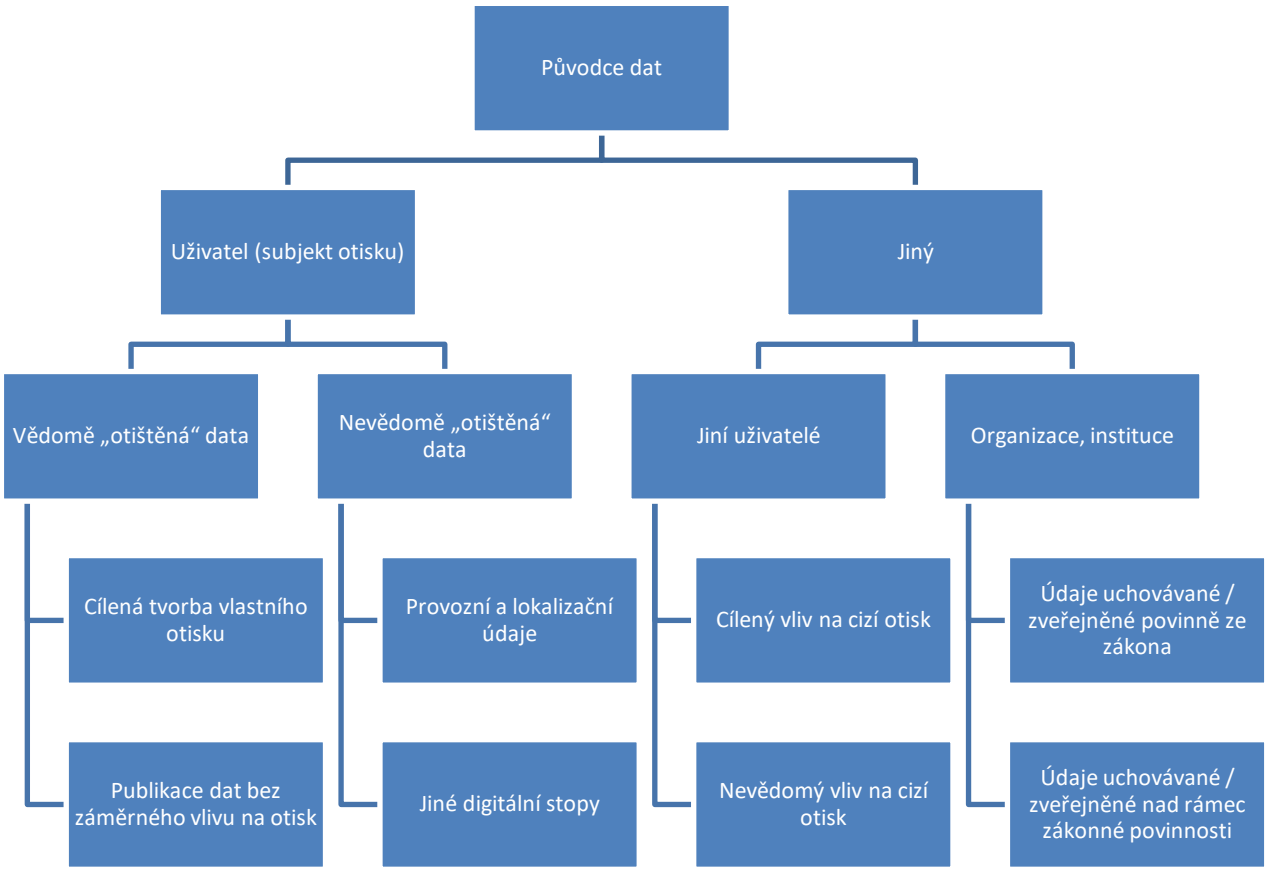
Sociální uznání vychází z jedinečnosti člověka oproti ostatním, právní je naopak založeno na rovném přístupu a zajištění individuální autonomie. Klíčové je proto zajistit, aby nikdo (jedinec ani skupina) nebyl znevýhodněn či přímo vyloučen z politického společenství. K tomu ovšem nestačí, aby většina dbala práv a svobod menšin, o nichž rozhoduje, nýbrž musí jim zajistit možnost vlastního vyjádření, a to vč. rozhodnutí hovořit o sobě coby členu té které skupiny či naopak. I s ohledem na určité potvrzování stávajícího postavení skupiny snahou o jeho výslovnou změnu a princip sebenaplňujícího se proroctví, podle něhož se jakýkoliv jev stává faktickým ve svých důsledcích, je-li o něm přesvědčeno dostatečné množství lidí. Menšiny / skupiny / párové kategorie proto musí mít svůj hlas slyšitelný ostatními, i kdyby se jeho prostřednictvím rozhodly o sobě mlčet.

Předpokladem k tomu je vnitřní i vnější svoboda a možnost její realizace. Tu nabízí internet coby veřejný prostor dostupný i pro jinak méně „slyšitelné“ osoby – děti a mladistvé – kteří se ho chápou více než jakýchkoliv jiných platforem pro sebeprezentaci (typicky youtubeři a jejich interaktivní publikum). Zpětná vazba od vrstevníků a společnosti představuje významný faktor ovlivňující utváření vlastní identity a vztahu ke společnosti. Ačkoliv podléhají vnitřní (autocenzura) i vnější cenzuře (např. pravidla provozovatele služby), dokáží využít potenciál párových kategorií a jejich reprodukce (zejm. hromadění příležitostí v podobě sociálního kapitálu na SNS) i takové kategorie bořit adaptací na změněné poměry a jejich rychlou a masovou nápodobou. Většinou tak činí v souladu s uživatelskými, morálními i právními pravidly, případně i tzv. netiketou. Většina států moderní společnosti (vč. ČR) proto podporuje dostupnost internetu a usiluje i o určitou digitalizaci státní správy.

Děti i mladiství v online prostředí hojně komunikují, a to mezi sebou navzájem i vůči většinové společnosti. Zejm. při komunikaci mezi vrstevníky však dochází ke vzájemnému napadání (záměrně i z nedorozumění), které může překročit i trestněprávní mez, zejm. při kyberšikaně a sextingu. A to ve zvlášť zranitelném období vytváření vlastní identity odvíjející se z velké části od zpětné vazby ze strany vrstevníků a referenčních skupin, potažmo společnosti vůbec.

4. Digitální otisk a SNS

Ať už využíváme digitální technologie více či méně, zanecháváme v kyberprostoru svůj „digitální otisk“. Původcem digitálního otisku je na jedné straně jeho subjekt, na straně druhé pak ostatní uživatelé a různé instituce a organizace, jež spoluvytváří jeho konkrétní podobu, a to i bez vůle či vědomí subjektu otisku.



Většina osob má alespoň určité povědomí o svém digitálním otisku, zejm. pokud vytváří svůj digitální odraz cíleně – např. zveřejňování vybraných fotografií aj. obsahu na SNS, vlastní blog atp. Již méně vědomé je potom zanechávání digitálních stop v podobě např. vlastních komentářů zveřejněných v rámci diskuse pod článkem, aniž by je autor sepisoval se záměrem ovlivnění vlastního otisku, nebo třeba samotný způsob psaní vlastního blogu, kdy lze např. z použitých výrazů, větné skladby atp. usuzovat na psychické rozpoložení či vzdělanostní zázemí autora (Čírtková, 2010).

Mimoto jsou zde ovšem i nevědomě „otištěná“ data, resp. otištěná v důsledku jednání subjektu, ovšem bez ohledu na jeho vůli. Jejich velkou část tvoří tzv. provozní a lokalizační údaje, tj. údaje zpracovávané pro potřeby přenosu zprávy sítí elektronických komunikací nebo

pro její účtování[127] a údaje zpracovávané v síti elektronických komunikací nebo službou elektronických komunikací, které určují zeměpisnou polohu telekomunikačního koncového zařízení uživatele veřejně dostupné služby elektronických komunikací.[128] K provozním a lokalizačním údajům se řadí typicky např. datum a čas odeslání textové zprávy sms, identifikátor mobilního přístroje volajícího a volaného, datum a čas zahájení a ukončení připojení k internetu a další.[129] Typickou digitální stopou uživatele je pak jeho IP a MAC adresa. Dále patří mezi více či méně nevědomě vytvářená data o uživateli i další údaje jako je souhrn navštívených webových stránek, cookies, vyhledávaná hesla atp. Ve svém souhrnu pak dávají takové údaje poměrně přesný obrázek daného uživatele. Slovy skupiny poslanců zastoupených poslancem Markem Bendou: s jejich pomocí lze „sestavit komunikační a pohybový profil jednotlivce, z kterého lze získat nejen údaje o jeho minulých aktivitách, ale s vysokou mírou pravděpodobnosti i správně předvídat jeho aktivity v budoucnosti (...).“[130] Nicméně do jisté míry může být takový komunikační a pohybový profil jednotlivce zavádějící, a to zejm. ve dvou případech. První překážka rozdělující digitální profil na základě zde uvedených údajů od faktické reality nastává při sdílení zařízení více uživateli, kdy nelze jednoho od druhého (či ostatních) dost dobře rozlišit. Druhý případ nastává v okamžiku cíleného maskování vlastní IP a případně i MAC adresy, zpravidla za účelem anonymizace pohybu po síti (blíže k IP a MAC adresám a cookies viz kapitola **Technická stránka kyberprostoru**).

Nejen uživatel je však původcem dat o něm samém, případně ne vždy má možnost jejich formální či neformální autorizace. Množství takových dat se vyskytuje zejm. na SNS, od fotografií o textových informací o uživateli po celé profily či stránky představující sebeprezentaci, o jejichž existenci dotyčný vůbec netuší. Nakonec zde zbývá řada institucí, v jejichž datových souborech a databázích bude subjekt otisku zachycen. Předně se nevyhne uchovávání a v některých případech i zveřejnění osobních údajů ze strany institucí, které tak činní ze zákona povinně,[131] bez závislosti na vůli subjektu údajů. Naopak údaje zveřejněné organizacemi a institucemi nad rámec zákonné povinnosti (např. zveřejnění jmenného

[127] Provozní údaje, viz § 90 odst. 1 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích).
[128] Lokalizační údaje, viz § 91 odst. 1 zákon č. 127/2005 Sb., o elektronických komunikacích.
[129] Viz § 2 vyhlášky č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů.
[130] Viz nález Ústavního soudu Pl. ÚS 24/10 ze dne 22. 3. 2011, vyhlášený pod č. 94/2011 Sb.
[131] Typicky např. datum narození živnostníka zveřejněné v živnostenském rejstříku, viz § 60 odst. 2 písm. a), odst. 3 zákona č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon).

seznamu členů) už zpravidla vyžadují nějakou formu souhlasu dotčené osoby (či jejího zákonného zástupce).[132]

Vlastní digitální otisk se začíná rýsovat již před narozením, počínaje zanesením potvrzení těhotenství do zdravotnické databáze,[133] případně biometrickými daty matky využívající IoT. Informační systémy veřejné správy začnou provádět příslušné zápisy způsobem umožňujícím dálkový přístup [§ 2 písm. o) zák. č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů]: těhotenství matky, narození, základní registry atp., vč. případného Rejstříku trestů.[134] Někteří rodiče podrobně informují o potomkovi na SNS, příp. vytvoří jeho vlastní profil (zejm. FB)[135] ((Ne)uživatelé internetu – malý průvodce kybernástrah, 2015).

Mládež běžně využívá řadu aplikací určených ke komunikaci, přičemž některé z nich představují potenciálně rizikové prostředí vzhledem k množství vlastních digitálních stop vč. osobních údajů a ostatním uživatelům daných služeb.[136] Veřejné chatovací místnosti patří k nejrizikovějším vzhledem k časté anonymitě (postupně je ovšem nahrazují SNS). Chatující většinou nemá možnost ovlivnit, kdo všechno se v chatovací místnosti objeví, ani případně zablokovat obtěžujícího uživatele. Chatovací aplikace jsou běžně integrované i v SNS nebo emailech. U nás se nejvíce chatuje na: xchat.cz, Lidé.cz, Líbímseti.cz a online seznamkách. U instant messengerů/komunikátorů má sice uživatel už větší vliv na to, s kým komunikuje (může též jiného uživatele zablokovat), ale v rámci těchto aplikací často komunikují lidé, kteří se v reálném životě neznají, a je zde vysoká hrozba rozvinutí rizikové komunikace s potencionálním agresorem. Komunikace prostřednictvím emailu a ještě více mobilního telefonu se snadno stane důležitým prostředkem navazování intimního vztahu, sexuálně laděné komunikace, lákání na schůzku nebo posílání nevyžádaných zpráv a dalšího obtěžování. Seznamování ovšem probíhá ponejvíce na SNS, přičemž uživatelé na svých

[132] Forma odvíjející se od toho, zde jde či nejde o tzv. systematicky / automatizovaně zpracovávané osobní údaje, s nimiž nakládání podléhá režimu nařízení GDPR, zákona o ochraně osobních údajů a de lege ferenda zákona o zpracování osobních údajů (viz pozn. č. 35).
[133] V současnosti ve vývoji (Národní strategie elektronického zdravotnictví).
[134] Viz např. § 32 zák. č. 187/2006 Sb., o nemocenském pojištění, § 1 odst. 4 zák. č. 301/2000 Sb., o matrikách, jménu a příjmení a o změně některých souvisejících zákonů, § 3 zák. č. 111/2009 Sb., o základních registrech, zák. č. 133/2000 Sb., o evidenci obyvatel, § 27 zák. č. 592/1992 Sb., o pojistném na všeobecné zdravotní pojištění, § 28 odst. 1 písm. b) zák. č. 561/2004 Sb., školský zákon, § 60 zák. č. 455/1991 Sb., živnostenský zákon, zák. č. 269/1994 Sb., o Rejstříku trestů (zahrnující vedle trestných činů od 1.10.2016 i přestupky).
[135] Vč. případného následného (i nevědomého) přispívání k dětské pornografii (Policie ČR, 2014).
[136] Následující výčet vychází z textu vytvořeného kolektivem autorů coby výukový materiál pro pedagogy v rámci projektu Škola bezpečně online: Zvýšení kvality vzděláván v oblasti bezpečného užívání internetu v Pardubickém kraji, CZ.1.07/1.3.12/04.0016, na jehož přípravě se autorka podílela, a tam uvedených zdrojů, viz (Brandejsová, a další, 2012), k ostatním metodickým materiálům v rámci tohoto projektu viz (Národní centrum bezpečnějšího internetu). Informace zde uvedené odpovídají stavu v roce 2012, kdy byl projekt dokončen.

profilech často zcela veřejně poskytují kontaktní údaje, osobní fotografie a informace o svých zvyklostech. Na SNS je také jednoduché vytvořit falešný profil, pomocí něhož agresor naváže důvěrný vztah se svou obětí. U nás je nejpoužívanější SNS FB.com, mezi dospívajícími dále např. i Lidé.cz nebo Líbímseti.cz.

V současnosti patří k nejvyužívanějším aplikace kombinující instant messengery, mobilní telefony a SNS jako WhatsApp, Instagram, Messenger[137] aj. Zde již otázka anonymita do jisté míry postrádá smysl, neboť uživatelé vystupují pod svým vlastním jménem a telefonním číslem a jejich prostřednictvím využívají relativně stabilní profil a na něj navázané kontakty – profily dalších osob. Tyto aplikace umožňují svým uživatelům sledovat, který z jejich kontaktů je právě online, komunikovat s jednotlivci i celými skupinami v reálném čase nebo zanechávat zprávy k pozdějšímu přečtení, sdílet data (vč. fotografií a videí, případně i v podobě upravené danou aplikací). Zpravidla tak činí v rozhraní přístupném z různých zařízení: mobilního telefonu, stolního počítače, tabletu atd., některé z nich mezi nimi dokážou přepínat prakticky okamžitě.[138] Obvykle využívají kombinaci webové verze na počítači a vlastní aplikace na mobilním telefonu. Uživatelé tak mohou být prakticky neustále online (některé aplikace se navíc spouští automaticky s daným zařízením), čemuž odpovídá i potenciální rychlost a masovost šíření sdíleného obsahu.

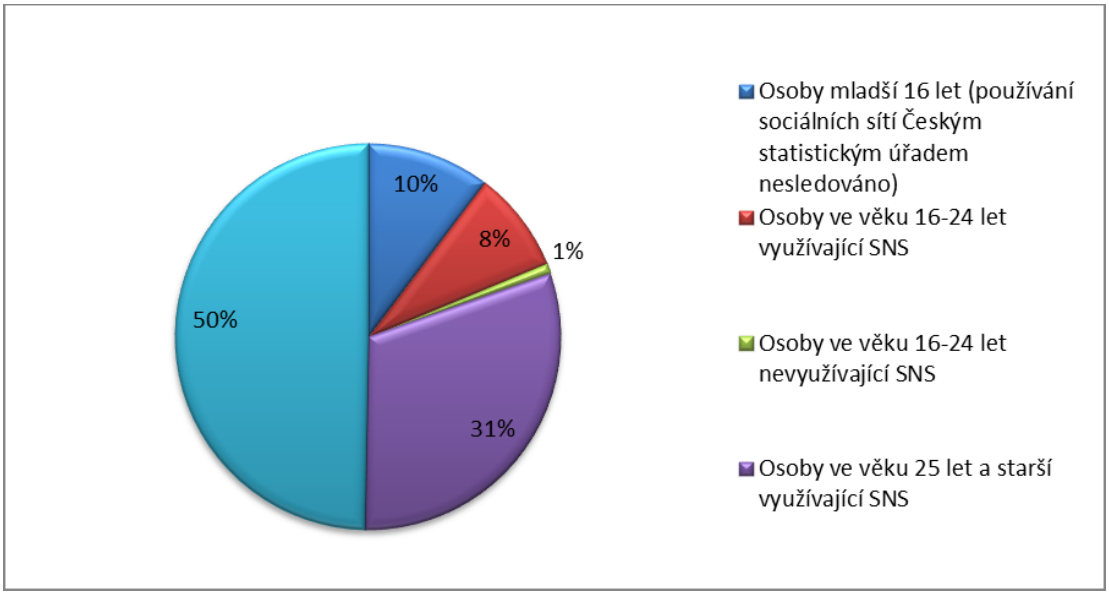
Uživatelé SNS sdílí velice pestrý obsah, od útržkovitých zpráv, fotografií atp. po podrobné komentáře a detaily z intimního života. Informace, které o sobě lidé na internetu sdělují, se samy o sobě nemusejí zdát ohrožující, při troše úsilí ale bývá snadné z údajů poskládat celou mozaiku o soukromí jednotlivce. Zneužitelné údaje lze velmi zhruba roztřídit do dvou skupin, přičemž se obě mohou doplňovat a v obou zaujímají zvláštní místo majetkové údaje. První sestává z údajů identifikujících dotyčného v reálném prostředí, které mohou vést k jeho fyzickému ohrožení (např. adresa bydliště). Druhá zahrnuje údaje vztahující se k osobě a projevům dotyčného ve virtuálním prostředí, které mohou vést k předstírání jeho identity.

Tak jako děti vedou domácnosti k využívání internetu (viz tab. č. 1 a komentář k ní), hrají prim i v přístupu k SNS: oproti cca 44 % osob starších 16 let využívajících internet v roce

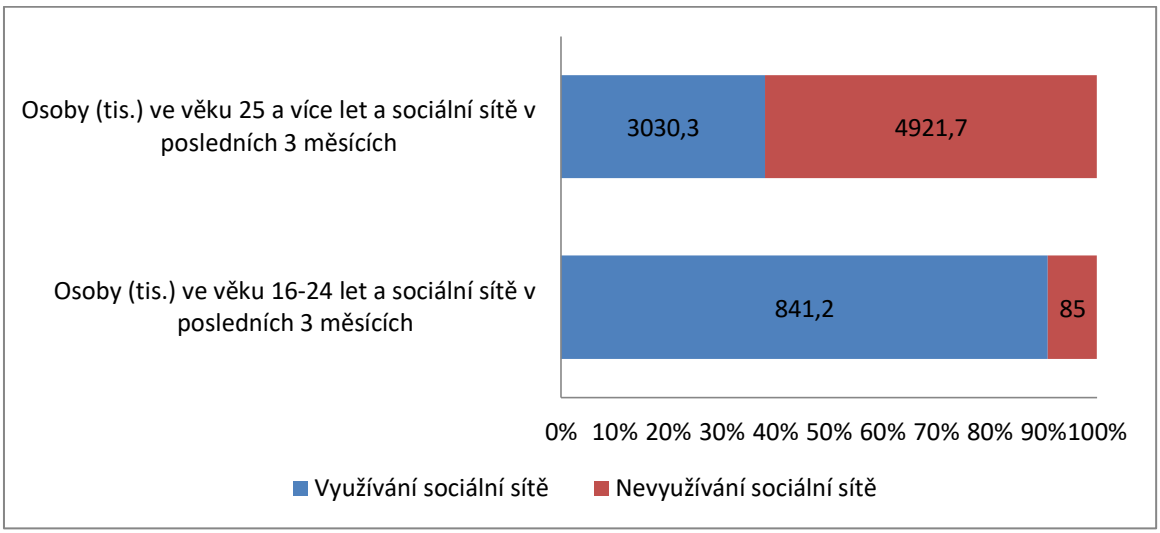
[137] Messenger a WhatsApp patří do vlastnictví FB (Wikipedie).
[138] Interoperabilita („schopnost vzájemně si vyměňovat informace a vzájemně vyměněné informace užívat," viz směrnice Evropského parlamentu a Rady 2009/24/ES ze dne 23. dubna 2009 o právní ochraně počítačových programů) mezi počítačem, mobilním telefonem a obdobnými zařízeními patří k současným trendům. Uživatelé mohou díky ní snadno a automaticky zálohovat a synchronizovat data a v řadě případů též plynule a prakticky v reálném čase přecházet od rozdělané činnosti na jednom zařízení k pokračování v ní na zařízení jiném.

stojí plných 93 % osob ve věku 16-24 let, oba podíly pak přinejmenším od roku 2012 více méně vytrvale stoupají.[139]

Graf č. 1: Věkové rozložení obyvatel (ne)využívajících SNS[140] v souhrnu v roce 2017[141]



Graf č. 2: Využívání SNS u vybraných skupin[142]



[139] Počínaje např. 31 % osob ve věku 16 a více let a 83 % osob ve věku 16-24 let v roce 2012, viz data Českého statistického úřadu pod záložkou Využívání ICT v domácnostech a mezi jednotlivci – 2017, tab. č. 54 (Český statistický úřad, 2017 str. 70).
[140] Bez zohlednění pracovních sítí jako LinkedIn, tzn. FB, Instagram, Twitter atp.
[141] Data vychází z údajů Českého statistického úřadu pod záložkami Využívání ICT v domácnostech a mezi jednotlivci – 2017, tab. č. 50 (Český statistický úřad, 2017 str. 67) a Věkové složení obyvatelstva – Věkové složení obyvatel k 31.12.2017 (Český statistický úřad, 2018) a vztahují se k využití SNS v uplynulých 3 měsících.
[142] Výběr dat z obdobných zdrojů jako u předchozího grafu.

Zatímco Český statistický úřad se soustředí na sledování používání ICT ze strany osob od 16 let, jiné studie cílí i na mladší uživatele, vč. nejvýznamnějšího projektu EU Kids Online.[143] Ten opakovaně ukazuje, že čeští dětští uživatelé internetu jsou aktivní již od poměrně raného věku 8 let. V 9-16 letech již má 72 % českých dětských uživatelů internetu vlastní profil na SNS, resp. 52 % dětí ve věku do 12 let a 90 % dětí ve věku 13-16 let. Nejčastěji (91 %) využívají dětští uživatelé FB, a to ve 46 % i děti mladší 13 let (ve 13-16 letech je to již 84 %), navzdory pravidlu užívání FB od 13 let (Livingstone, a další, 2011 str. 24 a 37), (Livingstone, a další, 2010 stránky 1, 3 a 4), (Facebook, 2018).

Uvedený trend potvrzuje v českém prostředí i výzkum České děti a FB, který probíhal v roce 2015 formou dotazníkového šetření dětí ve věku 8-17 let. Podle něj má vlastní profil téměř 60 % dětí mladších 13 let, přičemž jejich podíl s věkem převážně stoupá.[144] Děti na FB dle uvedeného výzkumu především vzájemně komunikují (vč. komentování příspěvků ostatních), udržují svou sociální síť, sdružují se, hrají hry, seznamují se, sdílí všemožný obsah, „drží krok“ s vrstevníky, sebeprezentují se (Univerzita Palackého v Olomouci, Pedagogická fakulta, 2015 stránky 7-9 a 11).

Kromě FB využívají děti a dospívající samozřejmě i další SNS, od nichž se pak odvíjí převažující aktivity. Zjednodušeně řečeno: na Youtube sdílí a sledují videa, zejm. tzv. [letspleje][145] a youtubery. Přes WhatsApp, Messenger a Viber dětští uživatelé především komunikují, ale také sdílí (fotografie, videa). Přes Instagram primárně sdílí (mnohdy upravené) fotografie a videa a komentáře k nim. Na Ask.fm se ptají (a odpovídají), na LinkedIn ty starší profesně prezentují a na Twitteru sledují vybrané osoby. Oblibě se těší také Snapchat umožňující zaslat fotografii na zvolená telefonní čísla s pokynem k automatickému sebesmazání po určené době. Řada z těchto aplikací nahrazuje tradiční sms a volání mobilním telefonem, neboť namísto paušálu či předplacené karty telefonního operátora využívají internet, resp. především dostupné bezplatné Wi-Fi.

[143] Mnohonárodnostní výzkumná síť založená v rámci programu Evropské komise Safer Internet, později Better Internet for Kids, věnující se od roku 2007 tematice dětí online ve většině evropských zemí, nově též i v několika státech mimo Evropskou Unii, vč. USA a Ruska. Publikované zprávy vychází pod standardním označením ISSN 2045 256X a dostupné jsou všechny na www.eukidsonline.net. Data použitá v této kapitola pochází převážně z druhé a třetí výzkumné série probíhající v letech 2009-2011 a 2011-2014.

[144] Ve zveřejněných datech můžeme zaregistrovat výrazný odklon od FB mezi 15. a 16. rokem, kdy užívání začne opět následně nabývat na intenzitě. Lze se domnívat, že v tomto věku děti a dospívající objevují a více využívají i jiné SNS jako Twitter nebo profesní LinkedIn. Zároveň někdy v tomto věku prochází určitou módní vlnou, kdy „je in NEBÝT na Fejsu,“ která však posléze obvykle utichne a většina uživatelů se k FB vrátí – soudě dle opakovaného vyjádření řady učitelů co do jejich zkušeností s žáky a jejich vztahu k FB.

[145] „Let´s play“ coby označení pro videa věnovaná hraní her: obvykle autentické záběry ze hry doplněná komentářem hráče.

Od typu SNS se odvíjí i s ní spojená rizika a hrozby: přílišná otevřenost a sdílení intimních informací, podvodná jednání, ponižující nebo zesměšňující jednání, vydírání a vyhrožování, šikana, sexuální zneužívání, závislost aj. Generace Z (digitální domorodci) běžně sdílí množství informací ze svého každodenního života, od náhlých myšlenek přes fotografie a videa po faktické a osobní údaje. Případný útočník proto zpravidla bez větších potíží nalezne velmi rychle množství zneužitelných dat. Zvlášť bohatý digitální otisk zanechávají uživatelé nejpoužívanějšího FB, který (zjednodušeně řečeno) rozlišuje sdílení obsahu především na „veřejně" nebo „pro přátele", přičemž počty „přátel" (tj. ostatních kontaktů na FB) dětských a mladistvých uživatelů dosahují stovek až tisíců osob, počínaje 24 % nejmladších dětských uživatelů do 16 let se sto a více navázanými kontakty (Livingstone, a další, 2011 str. 38). Dle výzkumu České děti a FB 2015 byl průměrný počet „přátel" na FB dětí ve věku 11-17 let v roce 2015 téměř 200 (Univerzita Palackého v Olomouci, Pedagogická fakulta, 2015 str. 13).[146] Útočníkovi proto obvykle postačuje dotyčného „požádat o přátelství", po akceptaci již získá přístup do „omezené" skupiny přátel a ke zdánlivě soukromému obsahu. K závažným jednáním využívajícím FB patří především sexuální zneužívání dětí (online i potažmo offline) a kyberšikana, ať už s využitím stávajícího profilu oběti nebo naopak vytvoření falešného. Zapojení mládeže na straně pachatelů (vč. pachatelek se dotýká především tzv. sextingu a kyberšikany).

4.1. Shrnutí k digitálnímu otisku a SNS

Ve většině zemí světa má každý jedinec svůj určitý „otisk" v digitálním světě, větší či menší, výstižnější či méně výstižnou stopu vlastní osobnosti, a to vč. osob, které samy o sobě digitální prostředí využívají jen minimálně, případně vůbec. Původcem digitálního otisku je na jedné straně samotný otištěný subjekt, na straně druhé pak ostatní uživatelé a různé instituce a organizace. Vzniká cíleně, nevědomky i bez vlastního přičinění subjektu. Cílený otisk zahrnuje vlastní profil na SNS, blog atp., necílený pak především provozní a lokalizační údaje (vč. IP adresy) a cookies. Otisk dále spoluutváří instituce a organizace, které zveřejňují údaje na základě zákona nebo souhlasu subjektu údajů, a nakonec ostatní osoby zejm. na SNS (typicky fotografie subjektu na profilu jiné osoby).

[146] Motivací k „přijímání přátelství", tj. akceptování daného kontaktu do skupiny „přátel" je z velké části vnímání počtu přátel jako ukazatele sociálního statusu.

Otisk z vlastního přičinění subjektu vzniká především na SNS (zejm. FB), ale i v dalších aplikacích. Uživatelé sdílí pestrý obsah, z něhož lze mnohdy poskládat celou mozaiku o jejich soukromí. Zneužitelné data zahrnují především identifikační údaje, které mohou vést k fyzickému ohrožení, a dále údaje vztahující se k osobě a projevům dotyčného ve virtuálním prostředí, které mohou vést k předstírání jeho identity a/nebo kyberšikaně. Děti hojně využívají SNS již od 8 let (polovina dětí mladších 12 let), v 16-24 letech je užívá přes 90 % osob. Jde především o FB, kde komunikují, hrají hry, seznamují se, sebeprezentují, sdílí obsah atp., dále pak Youtube (sdílení videí, vč. youtuberů), WhatsApp, Messenger a Viber (komunikace a sdílení), Instagram (sdílení fotografií a krátkých videí).

Rizika spojená s digitálním otiskem se pojí s přílišnou otevřeností a sdílením, zejm. v případě zneužití dat k sexuálnímu zneužívání dětí a kyberšikaně. Zvlášť při kyberšikaně a sextingu bývají aktéři z řad mládeže na obou stranách.

5. Další kriminogenní a viktimogenní faktory

Hojné využívání ICT, rychlost a potenciální masovost sdíleného obsahu, komunikace online, potřeba uznání i obsáhlost digitálního otisku a hojné využívání SNS, to vše představuje významné potenciální kriminogenní/viktimogenní faktory. Za zmínku však stojí i dva další, které nemusí být tak zřejmé.

5.1. Netholismus

Jakákoliv závislost představuje potenciálně významný kriminogenní/viktimogenní faktor, závislost ve spojení s ICT není výjimkou. O závislosti lze hovořit tehdy, když začíná zasahovat prakticky do všech sfér života člověka, od fyziologických potřeb (např. stravovací návyky) po destrukci sociálního života a více či méně i sebe samého.[147] V mnoha případech jde ovšem spíše o excesívní užívání (Masarykova univerzita, 2016). V souvislosti s mládeží a ICT lze hovořit zejm. o závislosti/excesivním užívání počítačové hry (zpravidla konkrétní) a SNS, v menší míře též hazardu[148] a sebepoškozování.

Přístupy, domněnky a fakta o vlivu počítačových her (a do jisté míry i SNS) v dětství a dospívání se různí, viz např. (Loukota, 2011), (Dohnal, 2017), (Granic, a další, 2014), (Gray, 2014). Na jedné straně stojí obavy ze vzdalování se od reality, snižování sociability, vytěsnění ostatních aktivit, růstu agresivity, závislosti, fyziologických změn.[149] Na straně druhé pak možný pozitivní vliv na soustředěnost (zejm. lepší krátkodobou koncentraci) a koordinaci oka a ruky (žádoucí např. pro chirurgy), vyzkoušení různých sociálních rolí (vč. opačného pohlaví), „prožití“ jinak nedostupných zkušeností, jazykovou vybavenost (zejm. angličtina),

[147] Slovy Mezinárodní statistické klasifikace nemocí a přidružených zdravotních problémů MKN-10 je závislost „soubor behaviorálních, kognitivních a fyziologických stavů, který se vyvíjí po opakovaném užití substance a který typicky zahrnuje silné přání užít drogu, porušené ovládání při jejím užívání, přetrvávající užívání této drogy i přes škodlivé následky, priorita v užívání drogy před ostatními aktivitami a závazky, zvýšená tolerance pro drogu a někdy somatický odvykací stav“ (ÚZIS, 2018 str. 200). Závislost spojená s internetem zde sice výslovně uvedena není, nicméně příznaky mohou být obdobné (s potlačením fyziologických a zdůrazněním psychických aspektů). V připravované MKN-11 již figuruje i závislost na hraní on-line a off-line her (Mohr, 2017). K problematice závislosti ve spojení s internetem viz zejm. publikaci Psychology of Cyberspace J. Sulera (Suler).

[148] Dle výzkumu IKSP 3 pachatelé počítačového trestného činu odsouzeného v roce 2015 spáchaného ve věku blízkém věku mladistvých usilovali svým jednáním o platby na vlastní účty pokerových online her (dosud nepublikované výsledky probíhajícího výzkumu, blíže k tomu viz kapitola **Výzkum** a publikace v rámci IKSP).

[149] Vývoj příslušných částí mozku a nedostatek fyzické aktivity. Naproti tomu stojí ale i pozitivní fyziologický vliv – např. lepší pozornost při řízení auta (Handwerk, 2009), rovnováha, krátkodobá paměť, zmírnění chronické bolesti a depresivity aj. (Bennington-Castro, 2015), (Primack, a další, 2012). Obavy (i naděje) se ovšem týkají i používání ICT vůbec, nejen počítačových her (Cooper, 2018), (Paton, 2014).

relaxaci a odlehčení od reality (např. v tíživé životní situaci), prožití úspěchu. Záleží na dané hře a konkrétním přístupu a predispozic hráče.[150]

Příznivci SNS oceňují přínos pro sociabilitu a snadnou komunikaci, sdílení všeho a neustále, prožívání radostí (ale i strastí) ostatních a s ostatními, okamžitou a širokou zpětnou vazbu na vlastní sebeprezentaci. V tom ovšem spočívá i stinná stránka, a to potenciální síla negativního dopadu na (mnohdy nečekané) odsouzení ze strany ostatních. Objevuje se také tzv. syndrom FOMO, tj. úzkostný pocit, že zajímavé a vzrušující události se odehrávají jinde, často vyvolaný zprávami zveřejňovanými na SNS (Oxford Dictionaries), vedoucí k permanentnímu bažení po vlastní přítomnosti na SNS, soustavné kontrole nových zpráv, pocitům opomíjení, depresi nad vlastním nezajímavým životem oproti ostatním atp. (2015). I když nemusí jít přímo o FOMO (Čermák, 2015), přidává se ještě omezení vlastního soukromí, odloučení od přátel a rodiny, osamělost a nespokojenost s vlastním životem. Od toho se pak odvíjí nespravedlivé odsuzování ostatních, změny osobnosti, paranoia, žárlivost na ostatní a snížení koncentrace (Hogan, 2015).

Sebepoškozování[151] nabývá mnoha různých podob, počínaje psychickou nepohodou přes fyzické působení na vlastní tělo až po sebevraždu, přičemž psychická nepohoda (např. pocit nezáživnosti vlastního života v porovnání se životem druhých) začíná už u relativně běžného užívání SNS (Subjective well-being prediction from social networks: A review, 2016), (Sabatini, a další, 2017). Fyzické poškozování vlastního těla zahrnuje škrábání se, štípání, pálení, bití atd. Odlišnou formou sebepoškozování představují poruchy příjmu potravy, vč. mentální anorexie, bulimie a ortorexie. Příznivci webů zaměřených na sebepoškozování (např. tzv. Pro-Ana) je vnímají jako bezpečné prostředí, kde si mohou osoby trpící danou poruchou na jednu stranu vzájemně dodávat síly k vytrvání a posilovat vlastní patologické prožívání a životní styl, na druhou stranu ale i diskutovat o své nemoci a jejích negativních důsledcích a podporovat tak ty, kdo se snaží uzdravit (Brandejsová, a další, 2012). I sebevražedné jednání a diskuse o něm mají své místo v online prostředí, od černého humoru po bolestné výpovědi „neúspěšných“ sebevrahů a trýzněných osob zvažujících odchod ze života. Velká část obsahu zahrnuje varování, psychickou podporu a rady, kde hledat pomoc (Freeman, 2018), najdou se ale i „kybersebevraždy“: v prvním významu ústup dotyčného z online prostředí, v druhém

[150] Hráčská komunita zahrnuje ovšem převážně dospělé osoby (častěji muže), zejm. ve věku 16-34 let (ISFE), (ISFE, 2012).

[151] Sebepoškozování přináší fyzickou bolestí úlevu od psychického trápení: akt sebepoškození mu dá na chvíli zapomenout na vlastní bezmoc nad prožívanými emocemi, do těla se vyplaví endorfiny, které sníží stres a uvolní napětí, mysl se zabývá praktickými otázkami (zastavit a zakrýt krvácení) atp. (Jarolímková, 2014).

významu sebevražedný pakt uzavřený mezi osobami znajícími se pouze virtuálně vzájemně je zavazující k sebevraždě v daný čas a daným způsobem, případně společně (Auxéméry, a další, 2010). Sebepoškozující se mládež často využívá internet. Obyčejně z důvodů hledání podpory a rad pro zvládnutí svého problému,[152] ale může se setkat i s negativním vlivem: pokládáním sebepoškozování za normální (snižuje odrazující sociální tlak a následné pocity studu) a odrazováním od vyhledávání (profesionální) pomoci a svěření se se svým problémem (Daine, a další, 2013), (Rodham, a další, 2013). Internet navíc bývá nástrojem kyberšikany, jejíž zakoušení patří mezi podstatné faktory vedoucích k sebepoškozování - sociální napětí vede k negativním emocím a ty posléze k sebepoškozování.[153] Mimoto se právě v prostředí internetu mohou virálně šířit „hry" jako Modrá velryba nebo zprávy o sebevraždách celebrit, po nichž obvykle následuje sebevražedná vlna (Sedláček, 2018), (Honzák, 2009).

Jakákoliv závislost bývá spojena s neúspěchem, bezmocí, problémy s okolím, emoční deprivací. Internet a především SNS mohou sloužit jako spouštěč a katalyzátor psychické poruchy, ale také nabízí pomocnou ruku a podporující komunitu. Podstatné je proto všimnout si varovných signálů (např. rodič, kamarád, učitel) a upozornit na ně, případně vyhledat odbornou pomoc, jde-li o závislost nebo sebevražedné tendence. (Nejen) při excesivním užívání pak může pomoci vymezení času určeného konkrétní aplikaci,[154] zažití úspěchu i jinde, přesun aktivit do offline prostředí.

5.2. Avatar[155]

Ať už jde o hraní her nebo přítomnost na SNS, dotyčný mnohdy vystupuje prostřednictvím svého avatara či avatarů, s nimiž se více či méně identifikuje. Zejm. počítačové hry doznaly s vývojem ICT značných změn: nejprve se jednalo o čistě textové hry, časem přibylo grafické rozhraní reagující na textové pokyny hráče. Dalším krokem bylo ovládání klávesnicí a posléze

[152] Doporučuje se proto věnovat pozornost „volání o pomoc", úvahám o sebevraždě, vyhledávání informací o sebepoškozování atp. ve svém okolí, neboť se SNS to může být prakticky kdokoliv, kdo zachytí takové volání a může nabídnout pomocnou ruku, třeba i formou možnosti snadného oznámení administrátorovi dané sociální sítě, který následně kontaktuje vhodné osoby, viz např. (Luxton, a další, 2012).

[153] Tento dopad snad může být zmírněn autoritativním rodičovským přístupem a vysokou sebekontrolou (Hay, a další, 2010).

[154] Minimalizuje nutkavé myšlenky na danou hru či SNS mimo tento vymezený čas a tzv. flow efekt - „duševní stav, při kterém je osoba ponořena do určité činnosti tak, že nic jiného se jí nezdá důležité" (Wikipedie).

[155] Kapitola vznikla za podpory programu rozvoje vědních oblastí na Univerzitě Karlově (PRVOUK) P06 "Veřejné právo v kontextu europeizace a globalizace". Původní publikovaný text odpovídal právnímu stavu v roce 2014 (Avatar jako kriminogenní faktor, 2014), zde uvedené znění je upraveno a reflektuje novelizaci § 134 z roku 2015.

za použití počítačové myši (v běžném užívání cca od 80. let 20. st.). Díky tomu stále více umocňují prožitek ze hry a dávají hráči pocit přímého působení na herní prostředí,[156] což je i zřejmou úlohou avatarů. Díky rozvoji ICT se tzv. telepresence[157] stále více přibližuje reálným pocitům až do té míry, že prožitek z virtuálního prostředí se stává zcela reálným v myšlenkách a vzpomínkách.[158]Avatar však není jen jedním z prvků her jako ostatní virtuální "věci", neboť reprezentuje přímo uživatele a ve větší či menší míře je jeho projekcí.[159] Jeho prostřednictvím uživatel komunikuje s ostatními a opomenout nelze ani ekonomický faktor, totiž hodnotu avatara pro hráče a samu o sobě. Pro digitální domorodce, kteří staví reálný a virtuální svět a vztahy prakticky na roveň, se i vlastní vystupování prostřednictvím avatara blíží hraní rolí mimo kyberprostor.[160]

Jak vlastně avatar vzniká? Pro vstup do mnoha virtuálních prostředí[161] je třeba nejprve zvolit svou reprezentaci, nejčastěji ve formě zosobnění člověka nebo humanoidní bytosti, přičemž se stále rozšiřují možnosti úprav dané bytosti dle vlastní představy (barva pleti, tvar obličeje, postava, účes atp., od hrou stanovené podoby po prakticky 3D zobrazení uživatele). Zpravidla bývá nezbytnou součástí též výběr jména. Z hlediska uživatele může být avatar jednorázový (např. náhodně generovaná postava určená pro jedinou bitvu), krátkodobý (určený k jedinému odehrání hry) nebo dlouhodobý, se kterým tráví i roky života.[162] Může být v rámci hry

[156]Např. dálkový ovladač wii remote přenášející pohyby hráče (např. jako by držel meč), kinect, který za použití kamery a projektoru přímo snímá pohyby hráče bez zprostředkujícího zařízení, nebo software schopný přenést webkamerou mimický výraz uživatele na virtuální osobu (vč. avatara) v reálném čase (Capin, a další, 1999).

[157]Více či méně dokonalá iluze reálné přítomnosti docilovaná použitím ICT, od videohovorů po virtuální realitu. Využívá se přenos obrazu, zvuku i fyzického kontaktu (např. dálkově ovládaný chirurgický robot).

[158] Např. vzpomínka na „rozhovor" s jiným uživatelem ve virtuálním prostředí – pamatuji si, kde v daném prostředí rozhovor proběhl, jak vypadali oba avataři atp., ovšem už si nevybavím, kde jsem zrovna seděla se svým notebookem nebo co jsem měla v tu chvíli na sobě v reálném světě. Budu-li o rozhovoru říkat další osobě (zejm. digitálnímu domorodci), zřejmě se nepozastaví nad vyjádřením, že jsem se s danou osobou "viděla" ve virtuálním prostředí, byť se vzájemně "setkali" pouze naši avataři.

[159]Jak z hlediska přenesení fyzického chování do virtuálního prostředí (úhozy do klávesnice, ovládáním myši, wii atp.), tak co do připisování vlastností hráče samého jeho avatarovi či avatarům jiných hráčů.

[160] Proběhly a probíhají sice výzkumy zabývající se mj. vztahem mezi uživatelem a jeho avatarem, viz např. (Ikegami, 2011) nebo (Williams, 2007), avšak vzhledem k relativně nové a specifické oblasti kyberprostoru se potýkají s "porodními problémy" (reprezentativnost vzorku, specifika zkoumaného jevu – např. přepínání uživatele mezi jednotlivými avatary, přístup do konkrétní virtuální oblasti pouze s náležitě vybaveným avatarem atp.). S ohledem na rostoucí význam kyberprostoru lze očekávat postupný rozvoj antropologie a sociologie kyberprostoru, s podoblastí virtuálních prostředí.

[161]Nikoliv internet nebo kyberprostor jako takový, ale jednotlivé virtuální světy (Second life, World of Warcraft, GTA, Battlefield, Habbo Hotel atp.). Nemusí se vždy jednat o hru – např. Second life slouží jako platforma pro setkávání a komunikaci uživatelů prostřednictvím jejich avatarů, prostor kreativity uživatelů i místo ekonomického zisku (v rámci Second life se např. pořádají koncerty, obchoduje se, prezentují se zde reálné společnosti, vzdělává se atp.) – de facto zde chybí základní účel hry, a to hraní samotné.

[162]Např. avatar ve hře typu World of Warcraft, kde cílem je hru hrát, nikoliv dohrát, nebo ve virtuálním prostředí typu Second life.

jediným avatarem nebo naopak jedním z mnoha.[163] Předmětem zde je především dlouhodobý hlavní avatar, neboť právě s ním se lze v průběhu času nejvíce sebeidentifikovat.

Rozšířený žánr MMO her a virtuálních prostředí per se tvoří specifické sociální prostředí, kde se skrze své avatary setkává množství uživatelů, kteří jejich prostřednictvím vzájemně komunikují, ba někdy je avatar vnímán dokonce jako pravdivější prezentace osobnosti než vystupování v reálném světě (Wolfendale, 2007 str. 111). Relativně bez rizika tak může uživatel experimentovat s vlastní sebeprezentací (Lindsay, a další, 2010) a zkoušením různých rolí, vč. opačného pohlaví, což činí zhruba polovina hráčů (Zaheer & Griffiths, 2008, str. 47). Avatar tak dává svému uživateli do jisté míry nahlédnout na sebe samého, neboť "skrze Tebe vidím sebe".[164] A protože pro virtuální prostředí je typické formování různých skupin, řada uživatelů prostřednictvím svých avatarů "někam patří", má své místo a úlohu. Nelze ovšem vynechat ani ekonomický prvek. Avatar má vždy nějakou hodnotu sám o sobě. Na jedné straně pro svého uživatele, který do něj zpravidla investoval v určité míře čas i peníze.[165] Zároveň má pro svého uživatele citovou hodnotu (jeho prostřednictvím např. navázal citový vztah, našel v kyberprostoru přátele, prožil herní úspěch, uzavřel dobrý obchod, „navštívil zajímavé místo" atp.). Avatar může být i prostředkem výdělku – např. vytvoření avatara určité úrovně za účelem jeho následného prodeje. Avataři se proto stávají i předmětem obchodování, ať už v souladu či rozporu s pravidly daného virtuálního prostředí.

Jednou z podstatných otázek po lidském bytí je sebevnímání ve spojení s vlastním tělem: "mám tělo", nebo "jsem svým tělem?" Na jedné straně stojí mé duševno v opozici vůči tělesnému světu, který mne omezuje, ale ve kterém a jehož prostřednictvím jedině se může mé duševno projevit tak, aby to mohl zachytit i někdo jiný mimo mne (neberu v potaz ontologický solipsismus, podle něhož svět ani druzí mimo mou mysl neexistují). Na straně druhé nejde o opozici, když právě jedině prostřednictvím tělesna může duševno existovat, a nikoliv mimo ně.[166] Ať už je odpověď jakákoliv, podobnou otázku lze do jisté míry položit i ve vztahu k avatarovi (hlavnímu, dlouhodobému): "mám avatara," nebo "jsem svým

[163]Rozlišuje se pak tzv. alt (vedlejší) a main, hlavní avatar, kterému dává hráč do jisté míry přednost, tráví ve spojení s ním většinou nejvíce času, bývá jeho prostřednictvím v kontaktu s více ostatními hráči, nejvíce si dává záležet na jeho vybavení, „reputaci" atd.

[164] S určitým nadnesením v buberovském pojetí osoby poznávající sebe samu nahlédnutím do tváře druhého (Buber, 1996). Prostřednictvím avatara jednak vidím vystupování ostatním vůči mně, jednak „vidím" vystupování svého vlastního avatara vůči ostatním.

[165]U většiny herních avatarů uživatel vylepšuje jejich „schopnosti" postupem ve hře, případně lze zakoupit doplňkové vybavení, ať už za reálné peníze nebo virtuální (herní peníze nebo virtuální měnu per se typu BTC).

[166]Nepřijmu-li představu čehosi jako duše „oblékající se" do těla, jakákoliv má existence je vázána na tělo, počínaje buněčnou látkovou výměnou a abstraktním myšlením vázaným na fyziologický mozek konče, taktéž však i bytí (má již vědomá existence, o niž se starám a jíž jsem si vědoma, tedy vím, že „jsem").

avatarem?" Jestliže jsou mé odpovědi takové, že "jsem svým tělem", ale "mám svého avatara", pak ho lze těžko odlišit od jakékoliv jiné věci, se kterou disponuji. Na opačné straně stojí "mám své tělo", ale "jsem svým avatarem" – takový přístup by značil radikální upřednostnění kyberprostoru na úkor reálného světa. Na pomezí stojí relativně neproblematické "mám své tělo" a "mám svého avatara", oproti "jsem své tělo" a zároveň "jsem svým avatarem." V posledně jmenovaném případě (stejně jako u "mám své tělo", ale "jsem svým avatarem") lze usuzovat, že sebeidentifikace uživatele s avatarem pokročila do té míry, že ho považuje za součást své osobnosti, a tudíž i útok na avatara by v takovém případě mohl znamenat porušení osobnostních práv uživatele.[167] Podotýkám, že avatar jakožto součást osobnosti by pak už nemusel být věcí v občanskoprávním smyslu, neboť by nebyl rozdílný od osoby (§ 489 NOZ, viz dále).

Avatar může sloužit jako předmět i prostředek útoku, a to jakožto reprezentace pachatele i reprezentace poškozeného. Může tak dojít k neoprávněnému nakládání s avatarem v reálném světě i k virtuálnímu útoku v daném prostředí. Důvodem může být ekonomický faktor, neboť avatar má jako jakákoliv věc určitou hodnotu, motivem může být též např. snaha odstranit obchodní konkurenci nebo i projev tzv. tradiční kriminality v novém kabátě (např. podvodné jednání prostřednictvím avatara). Útok na avatara může být veden s úmyslem poškodit jeho uživatele (s vědomím sepětí uživatele s avatarem). V abstraktnější rovině může být útok sycen i symbolicky, kdy prostřednictvím útoku na avatara pachatel např. vyjadřuje svůj nesouhlas s tím či oním, zasahuje dané virtuální prostředí jako takové nebo provozující společnost. Velmi diskutabilní jsou pak možné formy podněcování k nenávisti různých skupin prostřednictvím avatarů či útoků na avatary. Prostřednictvím avatara pachatel např. vydírá poškozeného, vyhrožuje mu atp. (přičemž své jednání směřuje k poškozenému coby osobě reprezentované „ohroženým" avatarem) - v takových případech je pak role avatara alternativou telefonního hovoru, výhružného emailu atp., ovšem probíhá v reálném čase. Při silné citové vazbě poškozeného na svého avatara a v závislosti na míře telepresence může poškozený vnímat útok na něj i jako útok na sebe samého a výhrůžky jako hrozbu zcela bezprostřední. Variant je mnoho, přičemž jejich kvalifikace se bude lišit i v závislosti na postavení avatara z hlediska práva.

[167]Pakliže by avatar byl považován alespoň v některých případech za součást osobnosti, v úvahu by pak musel připadat i např. útok na avatara jako na nezpůsobilý předmět útoku – pachatel by se např. mylně domníval, že poškozeného nutí něco konat pod pohrůžkou vážné újmy, poškozený by se však se svým avatarem neidentifikoval natolik, aby hrozící útok vůči avatarovi vůbec mohl dosáhnout intenzity vážné újmy. Nemluvě o nelehké úloze orgánů činných v trestním řízení posoudit, zda se jedná v daném případě o součást osobnosti či nikoliv.

5.2.1. Avatar z hlediska práva

Avatar vzniká na základě pokynu hráče v herním prostředí[168] k jeho vzniku a úpravě, tj. zadáním příkazů počítačovému programu (hře) k jeho vytvoření v konkrétní podobě. Spočívá pouze v příslušném datovém souboru a nemá žádný vlastní zdrojový kód, pouze strojový.[169] Data[170] lze charakterizovat např. jako „označení jakýchkoliv údajů zpracovávaných programem“ (Krištoufek, 1982 str. 34), počítačová data jako „jakékoli vyjádření faktů, informací nebo pojmů ve formě vhodné pro zpracování v počítačovém systému, vč. programu způsobilého zapříčinit provedení funkce počítačovým systémem“ (čl. 1 bod 2 sdělení Ministerstva zahraničních věcí ČR č. 104/2013 Sb. m. s.), soubor jako „posloupnost bajtů uložená na záznamovém médiu pod označením, které jí přiřadil uživatel nebo systém. Soubor je v jistém smyslu základní datovou jednotkou: uživatel se na něj odkazuje jeho jménem, pracuje s ním navenek jako s celkem“ (Hlavenka, 1997 str. 381).

Nabízí se otázka, “co” je vlastně avatar z hlediska práva, a to i s ohledem na relevantní trestněprávní ustanovení. Lze se již setkat s judikaturou v rámci ČR i na poli mezinárodním, která se zabývá virtuálním prostředím.[171] Jedná se však zpravidla o virtuální “věci” typu virtuální meč, nikoliv však o avatary, a proto je její využitelnost v tomto směru jen omezená.

Nejprve se nabízí pojetí avatara jako věci. Z hlediska NOZ avatar zřejmě splňuje daná kritéria, totiž je rozdílný od osoby a slouží potřebě lidí (§ 489 NOZ), je ovladatelný. Nemá hmotný substrát, resp. ne víc než např. počítačový program.[172] Ke své existenci a případné manifestaci (ve spojení s příslušným programem a zobrazovací periferií) ve „vnějším“, byť virtuálním prostředí vyžaduje své uchování prostřednictvím paměťového média (např. disku), tj. fyzickém nosiči, který však slouží pouze jako médium uchovávající jeho podstatu a je zaměnitelné s jakýmkoliv jiným médiem podobného typu, aniž by výměna jakkoliv ovlivnila

[168] Stejně tomu bude u uživatele SNS, diskusního fóra atp., bude-li reprezentován prostřednictvím avatara, zde pro zjednodušení hovořím o avatarovi v herním prostředí.
[169] Spočívá v určitém konkrétním shluku bitů - binárního kódu (souhrn jedniček a nul), který tvoří určitý počet bytů, potažmo datový soubor o velikosti několik kB-MB.
[170] Blíže k tomu viz (Smejkal, 2018 str. 36).
[171] Viz např. rozsudek odvolacího soudu v Leeuwardenu z roku 2009 (LJN no. BQ9251), kde došel nizozemský soud k závěru, že virtuální předměty (zde amulet a maska) jsou věcí z hlediska nizozemského trestního zákoníku, především proto, že mají pro svého vlastníka určitou hodnotu (Fialová, 2010 str. 23), (tVPN Admin, 2012).
[172] Viz např. vymezení uvedené v rozhodnutí Nejvyššího soudu 5 Tdo 1271/2016 ze dne 19.10.2016: „za počítačový program se považuje nehmotný výsledek autorovy tvůrčí činnosti, tedy určitá struktura daná organizací dat, posloupností instrukcí, volbou algoritmů a způsobem komunikace s uživatelem, který je většinou zapsán ve zdrojovém textu nebo strojovém (binárním) kódu. Tento zápis má již určitou hmotnou povahu a podobu a schopnost zobrazení.“

data samotná.[173] Coby datový soubor[174] není avatar pouhým právem, nýbrž v souladu s § 496 NOZ jinou věcí bez hmotné podstaty – věcí nehmotnou.[175]

Nepochybně není pozemkem, podzemní stavbou se samostatným účelovým určením, ani věcným právem k nim, a ani právem prohlášeným za nemovitou věc zákonem, a tudíž jde o věc movitou (§ 498 NOZ).

Podle konkrétní hry může být avatar ve více méně předem určené podobě, bez možnosti okamžitých či následných úprav v průběhu hry (zejm. hry spočívající v krátkodobých jednorázových bitvách, soubojích atp., např. Soldier of Fortune). V takovém případě bude jakožto movitá věc nahraditelná jinou věcí téhož druhu věcí zastupitelnou (§ 499 NOZ). Naproti tomu v řadě her se využívají avataři upravovaní jak v samém úvodu hry, tak v jejím průběhu (měnitelní co do schopností i vzhledu, např. MMO World of Warcraft), se kterými hráč tráví i dlouhé měsíce až roky. V takovém případě už půjde spíše o věc nezastupitelnou, byť nikoliv bezvýhradně.[176]

Podobně může být avatar věcí zuživatelnou i nezuživatelnou (§ 500 NOZ). Zuživatelnou tehdy, když herní systém spočívá v jednorázovém využití zpravidla zastupitelných avatarů, pročež jejich použitím (tj. odehráním hry jejich prostřednictvím) hráč avatara pozbývá, tj. přijde o něj při běžném užívání.[177] Naopak zejm. avataři coby nezastupitelné věci budou zpravidla zároveň i věcmi nezuživatelnými.

Mohlo by se zdát namístě uvažovat o avatarovi jako hromadné věci (§ 501 NOZ) ve spojení s herním účtem, avšak zpravidla tomu bude tak, že půjde spíše o součást herního účtu, neboť k němu bude podle své povahy náležet a nebude moci být oddělen, aniž se tím herní účet

[173] Paralelu lze najít v elektrické energii coby nehmotné přírodní síle, ovladatelné ve spojení s úložištěm (akumulátorová baterie aj.), přičemž v případě elektrické energie NOZ výslovně zakotvuje přístup k ní, jakoby šlo o věc hmotnou (což ovšem u počítačového programu ani datového souboru nečiní, ergo z pohledu NOZ zůstává počítačový program i datový soubor věcí nehmotnou), viz § 497 NOZ, část důvodové zprávy k § 496-498 (Poslanecká sněmovna PČR; Vláda ČR, 2012) a komentář k § 497 (Švestka, 2014). Stejně jako při přenosu elektrické energie může dojít a dochází při posílání dat internetem v jednotlivých paketech k určitým ztrátám dílčích dat, zpravidla však nikoliv takových, aby mohla jejich ztráta ovlivnit datový soubor jako celek (resp. packety, které dorazí do cílové stanice poškozené nebo nedorazí vůbec, jsou nahrazeny opakovaně odeslanými identickými packety- zde paralela s elektrickou energii končí).

[174] V literatuře se lze setkat např. se zdůrazněním „samostatné užitečnosti a alespoň virtualizované možnosti se soubory nakládat," než aby je bylo lze pojímat jako věci hmotné vzhledem k nezbytnosti fyzického nosiče (Loučka, 2016).

[175] Někteří dokonce zcela odmítají spojení dat s fyzickým nosičem - např. „elektronický dokument není vůbec svázán s materiálním nosičem" (Lechner, 2013 str. 19).

[176] Záležet bude na míře „individuality" avatara, resp. jeho jedinečnosti oproti ostatním avatarům. Při jeho úpravách více či méně předem připraveným způsobem bude naopak spíše věcí zastupitelnou (jiným avatarem, do jehož vývoje bylo investováno obdobně).

[177] Viz komentář T. Kindla k § 500 NOZ (Švestka, 2014).

(alespoň částečně) znehodnotí (§ 505 NOZ).[178] Literatura hovoří o třech kumulativních kritériích, která avatar obvykle splňuje:[179] náleží k hlavní věci podle své povahy (avatar obyčejně slouží coby avatar se všemi svými vlastnostmi pouze ve spojení s konkrétním herním prostředím), je s herním účtem relativně neoddělitelně spojen a nemůže být oddělen, aniž by byl herní účet znehodnocen. Oddělitelnost avatara od herního účtu coby práva užívat hru mohou zakotvit smluvní podmínky užívání - v takovém případě již bude možné s věcí/avatarem disponovat samostatně, byť obvykle pouze v omezené formě (např. převod mezi herními účty téhož uživatele), což ovšem jeho pojetí před oddělením coby součásti věci hlavní nevylučuje, ba naopak podtrhuje.[180]

V některých případech bude možné avatara považovat za autorské dílo. S pokročilými technologiemi už se hráči nemusí vždy spoléhat na předem připravené postavy, které případně pouze upraví, ale může de facto vytvořit zcela novou originální podobu pomocí určení i těch nejjemnějších rysů obličeje. Lze pak uvažovat o autorském dílu, neboť představuje výsledek tvůrčí činnosti hráče/autora, resp. je jedinečným výsledkem tvůrčí činnosti autora a je vyjádřeno v elektronické objektivně vnímatelné podobě (§ 2 AutZ). Na první pohled by snad mohl někdo přirovnat avatara k počítačovému programu, odlišuje je však několik podstatných vlastností, které z nich činí věci zcela rozdílné. Počítačový program představuje „ucelený souhrn instrukcí (příkazů), pomocí kterých provádí počítač určitou činnost. Program je tvořen souborem nebo více soubory, které jsou v úhrnu dostatečně schopné provádět předepsanou činnost“ (Hlavenka, 1997 str. 328). Odpovídající datový soubor vypadá na té nejnižší úrovni podobně jako datový soubor obsahující avatara: zápis binárního kódu shluknutý po osmi bitech do bytů, kB, MB atd. Podstatný rozdíl však spočívá v exekutivní funkci programu, kterou jest předávání pokynů procesoru[181] k vykonávání určitých činností. Tyto instrukce mají podobu některého z programovacích jazyků (např. C++), které využívají namísto extrémně nepřehledného zápisu v binárním kódu pro člověka srozumitelný uzavřený souhrn předem definovaných formulací („goto“, __if_exists“ atp.), tzv. zdrojový kód (převáděný

[178] Není sice vyloučeno pojetí avatara jako „samostatné a samostatně obchodovatelné věci, jejímž účelem je, aby se jí trvale užívalo společně s hlavní věcí,“ o kterém hovoří důvodová zpráva k NOZ v komentáři k § 505-509 v souvislosti s příslušenstvím věci (Poslanecká sněmovna PČR; Vláda ČR, 2012), přesto se zdá přiléhavější položit důraz na těsné spojení avatara s herním účtem.

[179] Viz komentář T. Kindla k § 505 NOZ (Švestka, 2014).

[180] Věc vedlejší lze od věci hlavní oddělit, byť k ní dle své povahy náleží a je s ní relativně neoddělitelně spojena – tj. avatar patří k danému hernímu prostředí a mimo něj prakticky nemá jiného užití (mimo rámec obchodovatelnosti jako se samostatnou věcí ze strany uživatele, které však smluvní podmínky obvykle striktně zakazují) a zároveň její oddělení vede ke znehodnocení věci hlavní – dlouho utvářený avatar může být nejcennější částí herního účtu.

[181] „Jádro hardwarového systému počítače, výkonná jednotka schopná vykonávání instrukcí programu“ (Hlavenka, 1997 str. 327).

automatickými prostředky na základě předem určeného algoritmu do binárního – strojového kódu, srozumitelného naopak pro procesor).

Právě zdrojový kód programu představuje jedinečný výsledek tvůrčí činnosti autora, vyjádřený v elektronické podobě (§ 1 odst. 1 a 2 AutZ). Nejpřiléhavější formou se zdá být dílo literární (coby souhrn příkazových instrukcí), neboť počítačový program lze sice zpětně analyzovat, tj. přečíst jeho binární kód a převést jej opětovně do některého z programovacích jazyků, výsledný zápis však bude postrádat „lidské uvažování“ a ponese zřejmý nádech automatizovaného přepisu.[182] Původní zdrojový kód je proto zcela unikátním duševním výtvorem autora a s ohledem na textovou formu dílo literární, nemluvě o výslovném zakotvení literární podoby v zákoně: původní počítačový program je coby autorův vlastní duševní výtvor pojímán jako autorské dílo literární.[183] S ohledem na výše uvedené by však měl být počítačový program chráněn coby dílo literární i bez výslovného zákonného ukotvení, splňuje-li podmínku výsledku tvůrčí činnosti autora. Naproti tomu podmínku jedinečnosti díla lze ve světě počítačových programů s ohledem na omezené množství použitelných programovacích vět zpochybnit, neboť výjimečně (zejm. u jednoduchých programů) může dojít k naprosté shodě zdrojových kódů vytvořených nezávisle na sobě různými autory.[184] Zákon proto uplatňuje „koncept původnosti (originality) díla ve smyslu vlastního duševního výtvoru“ a přiznává autorskoprávní ochranu počítačovým programům jako autorským dílům formou fikce (Telec, a další, 2007 str. 43).

Na rozdíl od počítačového programu v sobě nenese avatar žádné exekutivní instrukce a bez příslušného programu, pro který je určen, nelze vyvolat žádné jeho funkce a pravděpodobně jej ani zobrazit v jiné podobě než binárním kódu. Přesto může jít ve výjimečných případech o autorské dílo, v závislosti na míře hráčovy/autorovy vlastní kreativní činnosti. Zdánlivá tautologie (o autorské dílo coby výsledek tvůrčí činnosti jde tehdy, když do něj autor vloží dostatečně výrazný tvůrčí prvek) není tak jednoznačná, neboť ve většině případů avatar vznikne zejm. jako výsledek výběru hráče z omezeného (byť i značného) množství možných

[182] Počítač sice technickými prostředky převede zdrojový kód do binárního, nicméně při zpětném „překladu“ do původního programovacího jazyka v řadě případů pravděpodobně vzhledem k odlišnému „uvažování“ a strojové logice zvolí jiné řešení.
[183] Viz § 2 odst. 2 a § 65 odst. 1 AutZ a čl. 1 odst. 1 Směrnice Evropského parlamentu a Rady 2009/24/ES ze dne 23. dubna 2009 o právní ochraně počítačových programů.
[184] V takovém případě bude každý z nich identickým originálem, navzdory oxymóronu „identické originály“: „na světě mohou existovat tisíce či dokonce miliardy stejných originálů, u kterých nikdo nebude sto rozhodnout, který byl první, který je originálem v materiálním přístupu. ... nelze využívat principu jedinečnosti svázaného s materiálním nosičem, protože ten v elektronickém světě prostě neexistuje“ (Lechner, 2013 str. 19).

variant.[185] Pokud ovšem hráč/autor vybírá nikoliv z variant, ale ze škály, kterou navíc může třeba i blíže upravit (např. hustota vlasů), může tak vytvořit vlastní tvůrčí činností prakticky neomezené množství podob. Lze si pak v takovém případě představit i případnou objektivně vnímatelnou uměleckou hodnotu vytvořeného dnes již zpravidla trojrozměrného modelu.[186]

Pojetí avatara jako autorského díla[187] nebrání ani fakt jeho vytvoření prostřednictvím technického zařízení – počítače.[188] „V konkrétním případě je však nutno posoudit tvůrčí účast autora toho počítačového programu, který umožnil následný „umělý" vznik díla" (Telec, a další, 2007 str. 25). Nabízí se proto otázka, zda může jít o tzv. dílo odvozené, tj. dílo vzniklé zpracováním díla jiného,[189] v tomto případě avatara coby dílo výtvarné odvozené od hry (Burk, 2008 str. 142) - počítačového programu – díla literárního.[190] Ačkoliv si lze představit i jiný výklad (bude-li např. samotná hra spočívat v tvorbě avatara), avatar bude zřejmě představovat samostatné, nikoliv odvozené dílo, neboť využívá počítačový program de facto pouze jakožto technický prostředek umožňující jeho vznik.[191] V opačném případě by muselo jít o zpracování původního literárního díla – počítačového programu do jiné – výtvarné formy, což by ovšem znamenalo zpracování zdrojového kódu jinou formou, a to avatar zjevně nesplňuje.[192] U odvozeného díla by autor musel zpracovat původní dílo nebo jeho část (např.

[185] Např. kombinace jednoho z pěti typů postavy, obličeje, tvaru hlavy, barvy očí a barvy pleti znamená již 3125 výsledných možných podob, všech ovšem programem předurčených.

[186] Půjde zřejmě o umělecké dílo výtvarné (Telec, a další, 2007 str. 38). Jiná kritéria (přínos pro společnost, kritérium vkusu, životnost díla atp.) nejsou z hlediska AutZ relevantní (Chaloupková, a další, 2012 str. 4), (Telec, a další, 2007 str. 33).

[187] Přičemž „Autorskoprávní povahu díla ... nelze dohodou stran či jiným právním úkonem (např. prohlášením autora) určit ani vyloučit" (Telec, a další, 2007 str. 32).

[188] Při opačném výkladu by ad absurdum nebylo možné považovat za autorské dílo např. ani fotografii coby výtvarné dílo vytvořené prostřednictvím technického prostředku – fotoaparátu (a příslušné techniky k vyvolání fotografie do listinné podoby).

[189] Viz § 2 odst. 4 AutZ a komentář důvodové zprávy k § 2 AutZ (Poslanecká sněmovna PČR; Vláda ČR, 1999).

[190] Přičemž na způsobilost být předmětem autorského práva „nemá žádný vliv jeho kulturní, vědecký, historický, politický, národní nebo jiný význam. Stejně tak ani účel vytvoření, resp. účel veřejného nebo jiného užití, ani povahové určení díla (jeho vlastnosti), ani právní poměr, v němž bylo dílo vytvořeno nebo užito" (Telec, a další, 2007 str. 32).

[191] I v situaci, kdy by snad avatara bylo lze někdy v budoucnu považovat za počítačový program, pravděpodobně by nešlo o odvozené dílo, neboť by nebyl aktivně použit nebo modifikován samotný zdrojový kód hry (pouze by na jeho základě vznikl nový zdrojový kód, a tudíž by i jeho pojetí jakožto odvození mohlo být v konkrétních případech diskutabilní), navíc ani „pouhé použití knihovny [pozn. aut.: tj. „skupiny účelově zaměřených funkcí a programů, které je možno používat jako stavební prvky pro vlastní programátorskou tvorbu. Jedná se o jakési předprogramované části programu, které plní obvykle často používané funkce" (Hlavenka, 1997 str. 224)] prostřednictvím aplikačního programového rozhraní (API) nečiní z programu dílo odvozené z knihovny," což lze považovat za podstatná (byť nikoliv výlučná) kritéria pro označení programu jako odvozeného díla, viz (Rosen, 2001) prostřednictvím (Lhotka, 2005). K případné problematice následného licencování odvozeného programu viz např. (Jansa, 2017).

[192] Naopak s jeho zněním autor nemusí a v drtivé většině případů ani nepřijde do styku. Zpravidla tak půjde o využití vizuálních grafických prvků daného programu, které však nepředstavují předmět autorskoprávní ochrany, viz např. rozsudek Soudního dvora ze dne 2. 5. 2012 ve věci C-406/10, SAS Institute Inc. proti World Programming Ltd, zejm. bod 38: „Soudní dvůr ... dospěl k závěru, že zdrojový a strojový kód počítačového programu jsou formami vyjádření tohoto programu, kterým v důsledku toho přísluší autorskoprávní ochrana

vizuálně ztvárnit zdrojový kód), avšak výstižnější se zdá být využití onoho „původního“ díla – počítačového programu pouze coby nositele specifických omezených technických prostředků k vytvoření díla zcela nového. Nepřichází zde v úvahu ani koncept původnosti namísto jedinečnosti, neboť v těch případech, kdy lze uvažovat o avatarovi jako autorském díle, prakticky nemůže nastat situace identického výsledku tvůrčí duševní činnosti více na sobě nezávislých autorů.

Nyní přichází na řadu otázka využití NOZ ve vztahu k autorskému dílu a autorskoprávní ochraně zakotvené autorským zákonem.[193] Dle § 9 odst. 2 NOZ se soukromá práva a povinnosti osobní a majetkové povahy řídí občanským zákoníkem v tom rozsahu, v jakém je neupravují jiné právní předpisy. Někteří vyslovují určité pochybnosti o tom, zda lze považovat autorské dílo za věc ve smyslu NOZ, viz např. (Valeková, 2012), neboť zahrnuje soubor majetkových, ale i osobnostních práv autora (§ 10 a 11 odst. 4 AutZ, problematickým prvkem je omezené nakládání s osobnostními právy autora). Dle důvodové zprávy k AutZ je třeba umělecká díla coby nehmotné statky „odlišovat od hmotného substrátu, na němž nebo jehož prostřednictvím jsou tato díla vyjádřena. Nehmotný statek je pojmově vymezen právě skutečností, že jeho podstata má duševní (myšlenkovou) povahu, a že existuje nezávisle na hmotném podkladu, jehož prostřednictvím je tento nehmotný statek vnímán a může být kdykoli a kýmkoli současně užíván, aniž by byl spotřebován,“ viz komentář k § 10 a 11 AutZ (Poslanecká sněmovna PČR; Vláda ČR, 1999). Tato dualita spolu s dualitou osobnostních a majetkových práv autora umožňuje aplikaci ustanovení NOZ vztahující se k věcem na autorská majetková práva (v těch oblastech, které AutZ coby lex specialis neupravuje), a to při rozlišení autorských majetkových práv (např. autorskoprávní licence), hmotného nosiče díla (např. disk, na němž je uložen datový soubor s avatarem) a samotného nehmotného díla coby výsledku tvůrčí činnosti autora.[194]

Pojetí avatara coby věci podle NOZ, ať už jako autorského díla či nikoliv, podporuje ještě více méně zrovnoprávnění elektronické a listinné verze dokumentů, tzv. konverze dokumentů (listinných a elektronických).[195] Pakliže totiž lze přepisem binárního kódu převést avatara

počítačových programů podle čl. 1 odst. 2 směrnice 91/250. Naproti tomu, pokud jde o grafické uživatelské rozhraní, Soudní dvůr rozhodl, že takové rozhraní neumožňuje rozmnožení daného počítačového programu, ale představuje pouze prvek tohoto programu, jehož prostřednictvím uživatelé využívají funkce uvedeného programu ... .“

[193] Ve vztahu k majetkovým autorským právům v souvislosti s počítačovými programy viz např. (Tomíšek, 2014) nebo (2013).

[194] Objektivně vnímatelného ve spojení s hmotným substrátem – nosičem díla. K oddělení díla a věci viz např. (Beran, 2015).

[195] V rámci mnohaletého postupného vývoje směrem k uznání důvěryhodnosti elektronických dokumentů, blíže

z elektronické podoby do listinné a naopak, nastal by v případě odmítnutí jeho chápání jako věci zjevný rozpor v závislosti na nakládání s ním v elektronické anebo listinné podobě, což ovšem neodpovídá principu konverze dokumentů.[196]

Avatar nemusí sloužit pouze jako reprezentace uživatele v herním prostředí, ale může být jeho projekcí i v prostředí SNS (obvykle odlišný avatar, není-li daná SNS spojena přímo s hrou, v jejímž rámci avatar vznikl) a do budoucna nelze vyloučit ani prostupnost avatara různými platformami.[197] V tu chvíli se však nabízí ještě jiný pohled na avatara, a to jako na přesah osobnosti uživatele do virtuálního prostředí,[198] kde je jeho prostřednictvím „přítomen" a interaguje se svým okolím. Osobnost si lze představit jakou souhrn vlastností, vědomostí, zkušeností, sociálních vztahů atd. svázaných s konkrétní bytostí nadanou určitými přirozenými právy (čl. 5 Ústavy, čl. 19 odst. 1 a § 81 NOZ). „Podstatou osobnosti jsou její vztahy k vnímané skutečnosti, k druhým lidem (tzv. interpersonální vztahy) ... apod. Tyto vztahy se projevují ve styku s lidmi, v jednání a chování člověka, jeho kulturními výtvory apod.," viz komentář P. Pavlíka k § 81 NOZ (Švestka, 2014 str. 268). Avatar by tak představoval nejspíše specifický projev osobní povahy per se,[199] což by poněkud zproblematizovalo vztah mezi uživatelem - reprezentovaným subjektem a poskytovatelem služby, jejímž prostřednictvím avatar vznikl,[200] neboť kromě obvyklých smluvních ujednání by bylo nezbytné vzít v úvahu i kogentnost některých norem.[201]

---

k tomu viz např. (Lechner, 2013 str. 26), lze zmínit zejm. zák. č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, zák. č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů (§ 22), NOZ pak zrovnoprávnil elektronickou formu s listinou pouze s výhradou vyvratitelné domněnky spolehlivosti zejm. v § 562 NOZ, blíže k tomu viz např. komentář L. Tichého k § 562 (Švestka, 2014 str. 1111).

[196] Pro doplnění podotýkám, že žádný dokument nepředepisuje uchovávání datových souborů výlučně v elektronické či naopak listinné podobě.

[197] Hra, SNS, chatovací místnosti, atd. Může tomu tak být např. v podobě určitého profilu zahrnujícího kromě samotného jména (skutečného nebo přezdívky) vzhled, vybrané osobní údaje, kontakty na jiné uživatele atp., které by coby navázané na jedinečný profil uživatele reprezentovaly v online prostředí vůbec. Anebo v minimalističtější míře v podobě základních údajů v případném spojení s vizuální podobou, jimiž by se uživatel prezentoval na různých platformách, aniž by musel tyto údaje vyplňovat vždy znovu a znovu – podobně jako v současnosti funguje např. v oblasti hesel služba „Moje ID" (cz.nic), a to v návaznosti na míru interoperability na internetu vůbec.

[198] Zejm. u autorského díla lze do jisté míry hovořit o „emanaci osobnosti tvůrce" (Telec, a další, 2007 str. 26).

[199] Nelze ho zredukovat na podobiznu, písemnost, soukromí, vztahy k okolí atp., nýbrž vytváří ho právě jejich souhrn.

[200] A která případně zajišťuje možnost jeho faktické „existence" v online prostředí (např. zajišťování interoperability a schopnosti ostatních programů „rozpoznat" daného avatara a „komunikovat" s ním).

[201] Např. nepřevoditelnost osobnostních práv autora (§ 11 odst. 4 AutZ) nebo vůbec zákaz ujednání porušující právo týkající se postavení osob, vč. práva na ochranu osobnosti (§ 1 odst. 2 NOZ). Práva uživatele k vlastnímu avatarovi obvykle vyplývají z autorskoprávní licence ve spojení s pravidly virtuálního prostředí na něž obvykle uživatel přistupuje před prvním vstupem do daného prostředí, a která zahrnují na jedné straně chování uživatele „uvnitř" (vč. chování vůči ostatním uživatelům), na straně druhé pak vzájemná licenční ujednání (vč. např. i považování vizuální podoby avatara za součást původního autorského díla – hry – a nikoliv za autorské dílo

V trestněprávní oblasti se vymezení pojmu „věc“ donedávna lišilo, když vycházelo z definice uvedené v § 134 TZ, která rozlišovala věci a jiné majetkové hodnoty. Pro splnění kritéria věci v tehdejším trestněprávním smyslu (Šámal, 2012 str. 1397) by tak avatar musel být shledán jedině „jinou majetkovou hodnotou“.[202] Současná podoba trestního zákona už ovšem nahlíží věci z úhlu pohledu bližšího pojetí v NOZ, když po novelizaci provedené zákonem č. 279/2003 Sb. a účinné od 1.6.2015 bere obsah pojmu „věc“ za zřejmý s ohledem na znění NOZ, od něhož se odchyluje pouze co do pojetí ovladatelné přírodní síly, živých zvířat a zpracovaných oddělených části lidského těla (nevyplývá-li z jednotlivých ustanovení trestního zákona něco jiného),[203] které se ovšem avatara nikterak nedotýkají.

Z hlediska trestněprávně relevantního neoprávněného nakládání s avatarem tak přichází v úvahu řada skutkových podstat, a to především v závislosti na tom, zda ho pojmeme jako věc, autorské dílo nebo součást osobnosti (byť se tato pojetí vzájemně nevylučují). Ať už ale zdůrazníme v konkrétním případě kterýkoliv z těchto tří aspektů, u nezastupitelného avatara, s nímž se uživatel dostatečně identifikuje, se vždy může jednat o takovou součást jeho života, jejíž poškození by mohl vnímat jako těžkou újmu, intenzitou srovnatelnou s hrozbou spojovanou s pohrůžkou násilí, takže pohrůžka takové újmy by u něj mohla „vyvolat obavu obdobnou s ohrožením jeho života nebo zdraví. Pohrůžka jinou těžkou újmou může spočívat v hrozbě způsobení závažné majetkové újmy, vážné újmy na právech ... apod. Musí se však jako těžká újma objektivně jevit a napadený ji jako těžkou újmu musí také objektivně pociťovat (viz rozhodnutí Nejvyššího soudu publikované pod č. 10/1979-II. Sb. rozh. tr.). Za této podmínky to může být i hrozba újmou na majetku, která není násilím na věci ...,“ viz rozhodnutí Nejvyššího soudu 7 Tdo 1120/2017 ze dne 20.12.2017. Zároveň „při posuzování, zda jde o jinou těžkou újmu, je nutno přihlížet k osobním poměrům napadeného, k jeho vyspělosti, zkušenostem, psychickému stavu apod.“ (Šámal, 2012 str. 1696) a „ve vztahu k těmto okolnostem se musí z povahy věci vztahovat úmysl“ (Šámal, 2012 str. 1636). Zvlášť ve vztahu k dětem nutno zdůraznit při zvažování naplnění znaku pohrůžky jinou těžkou újmou jejich osobní poměry, vyspělost, zkušenosti a psychický stav, potažmo jejich vztah k vlastnímu avatarovi a jeho prostřednictvím navázané sociální okolí.[204]

---

uživatele, s čímž se ovšem nelze vždy ztotožnit).

[202] Živým zvířetem, zpracovanou oddělenou částí lidského těla, peněžními prostředky na účtu nebo cenným papírem, ovladatelným hmotným předmětem či přírodní silou (§ 134 TZ ve znění účinném do 31. 5. 2015) – ničím z toho pochopitelně avatar není.

[203] Viz § 134 TZ a příslušné části důvodové zprávy k zákonu č. 86/2015 Sb. (Vláda ČR; Poslanecká sněmovna PČR, 2014 str. 81).

[204] Např. tzv. guilda ve hře, tj. skupina hráčů (obvykle v počtu několika jedinců až desítek osob) vědomě

Znak pohrůžky jinou těžkou újmou obsahuje základní skutková podstata obchodování s lidmi, vydírání, porušování svobody sdružování a shromažďování, znásilnění, sexuální nátlak , pletichy při zadání veřejné zakázky a při veřejné soutěži a pletichy při veřejné dražbě [(§ 168 odst. 2, § 175 odst. 1, § 179 odst. 1, § 185 odst. 1, § 186 odst. 1, § 257 odst. 1 písm. a) a § 258 odst. 1 písm. a) TZ]. Při posledních dvou zmíněných je avatar jako předmět útoku ovšem z pochopitelných důvodů nanejvýš nepravděpodobný, podobně jakožto zvlášť přitěžující okolnost u nedovoleného přerušení těhotenství bez souhlasu těhotné ženy, neoprávněného odebrání tkání a orgánů, porušování práv a chráněných zájmů vojáků stejné hodnosti a porušování práv a chráněných zájmů vojáků podřízených nebo s nižší hodností [§ 159 odst. 2 písm. b), § 164 odst. 3 písm. b), § 382 odst. 2 písm. a) a § 383 odst. 2 písm. a) TZ].

„Pohrůžka jiné těžké újmy spočívá v ohrožení subjektivních občanských práv v majetkové nebo v osobní sféře postiženého subjektu, a to v takové míře, že svou závažností má stejný dopad jako případně použité násilí nebo hrozba násilím. Konkrétně může jít o hrozbu způsobení újmy na majetku, ... zásah do osobních vztahů ... apod.“[205] Nejčastěji proto připadá v úvahu právě zásah do majetkové sféry (při chápání avatara jako věci) nebo zásad do osobních vztahů (při zdůraznění avatara coby komunikačního prostředníka s částí sociálního okolí). Nelze však opomenout ani případný znak způsobení vážné újmy, přičemž jiná vážná újma má „nemajetkovou povahu. Jedná se o zásah do právní sféry poškozeného, který se nedotýká přímo jeho majetkových práv, ale přesto je jím oprávněně pociťován úkorně, neboť zasahuje do jeho práva na ochranu osobnosti. Může se jednat např. o zásah do nejbližšího sociálního zázemí poškozeného (rodina, zaměstnání, záliby), ohrožení kariéry (sportovní, pracovní, politické) apod.“[206] Pod sociálním zázemím si lze představit sociální „okolí“ uživatele v prostředí, kde vystupuje prostřednictvím avatara, obdobně se nabízí ohrožení zálib (hraní hry, „šlechtění“ avatara atp.). Nelze odmítnout ani ohrožení „sportovní“ a „pracovní“ kariéry, pokud půjde o nezastupitelného avatara spjatého s profesionálním hráčem.[207]

V úvahu tak připadají i další trestné činy, jejichž základní skutkové podstaty zahrnují znak způsobení nebo hrozby jinou vážnou újmou: braní rukojmí a pomluva (§ 174 odst. 1 a § 184

---

tvořících uskupení, v jehož rámci se hráči častěji „potkávají“, pomáhají si, stojí v opozici vůči jiné guildě atp. Při ztrátě avatara hráč např. pravděpodobně změní i svou pozici v guildě – může do ní sice opětovně vstoupit prostřednictvím nového avatara (pokud ho ostatní přijmou), nemusí však už mít přístup do míst podmíněných užíváním „zkušeného“ avatara, a tudíž ani hrát s ostatními v těchto mezích a zůstává poněkud stranou až do doby, kdy se mu podaří nového avatara vylepšit na úroveň obdobnou tomu předchozímu.

[205] Viz heslo „Jiná těžká újma“ v rámci přehledu společných hesel trestního zákoníku (Draštík, a další, 2015).

[206] Tamtéž.

[207] Již i v České republice se postupně vytváří týmy profesionálních hráčů, ať už jde o tzv. e-sporty, karetní hry, strategie, „střílečky“ atd. (GAMIFIQUE.cz, 2017).

odst. 1 TZ); dále se vyskytuje uvedený znak jako zvlášť přitěžující okolnost: porušení tajemství listin a jiných dokumentů uchovávaných v soukromí, zasahování do nezávislosti soudu, křivé obvinění, křivá výpověď a nepravdivý znalecký posudek a křivé tlumočení [- § 183 odst. 2, § 335 odst. 2 písm. c), § 345 odst. 3 písm. c), § 346 odst. 3 písm. b) a§ 347 odst. 3 písm. b) TZ].

Velmi snadno si lze představit poškození cizích práv (§ 181 TZ), zejm. při zneužití cizího avatara k uvedení jiného v omyl a následné způsobení vážné újmy na právech jiného.[208] Při systematickém postupu po ostatních jednotlivých skutkových podstatách uvedených ve zvláštní části TZ se dále nabízí (pravděpodobně ve spojení s neoprávněným přístupem k počítačovému systému a nosiči informací dle § 230 TZ) porušení tajemství dopravovaných zpráv [§ 182 odst. 1 písm. b) nebo c), případně odst. 5 TZ],[209] pojmeme-li avatara jako datový soubor,[210] obdobně pak i porušení tajemství listin a jiných dokumentů uchovávaných v soukromí (§ 183 TZ). Znak vážné újmy figuruje i ve skutkové podstatě trestného činu pomluvy (§ 184 TZ), jakkoliv se snad zdá být taková situace ve spojení s avatarem nepravděpodobná – jako v jiných případech, i zde patří mezi potenciální poškozené především profesionální hráči.[211]

Zřejmě nejpočetnější a potenciálně nejvyužitelnější skupinu skutkových podstat trestných činů zahrnujících avatara coby věc otevírá na prvním místě loupež a krádež (§ 173 a § 205 odst. 1 TZ) se znakem zmocnění se cizí věci.[212]K tomu dojde např. při neoprávněném

[208] Např. neoprávněné ovládnutí avatara jiného uživatele a jeho prostřednictvím lákání intimního obsahu (fotografie, tajemství atp.) od uživatele, který má s uživatelem ovládnutého avatara blízký vztah a domnívá se, že komunikuje právě s ním (obdoba využití pro pohlavní styk omylu poškozené ženy považující pachatele za svého manžela, viz rozhodnutí Najvyššieho súdu SSR 4 Tz 62/78 ze dne 14. 9. 1978).

[209] Druhou ze tří základních skutkových podstat, uvedená v odst. 2 § 182 TZ, ovšem také nelze a priori zcela vyloučit.

[210] Vzhledem ke konverzi listinných a elektronických dokumentů může výjimečně dojít i na aplikaci § 182 odst. 1 písm. a) TZ, při nakládání s avatarem v listinné podobě.

[211]Příkladem budiž osočení uživatele ze zneužití cizího herního účtu, vedoucí zpravidla k pozastavení daného účtu přinejmenším do doby prokázání oprávněného uživatele. Při „správném“ načasování (z pohledu pachatele) může uživatel takto ztratit např. možnost zúčastnit se klíčové bitvy, turnaje atp. Zde však bude jen tenká hranice mezi pomluvou a poškozením cizích práv (§ 184 a § 181 TZ).

[212] Navzdory tomu, že v původním znění TZ zákonodárce takovou aplikaci spíše nepředpokládal, jak lze vyčíst z důvodové zprávy: „zmocnění se jiné majetkové hodnoty (pozn. aut.: dle původního znění § 134 TZ by avatar byl právě jinou majetkovou hodnotou) je jen obtížně představitelné a zpravidla takové jednání bude naplňovat znaky trestného činu podvodu,“ viz komentář důvodové zprávy k § 204 (Vláda ČR, 2008). Naproti tomu „zmocnění se věci“ lze definovat jako „převzetí moci nad věcí a uplatnění k ní všech atributů vlastnického práva, tedy odnětí cizí věci (tou je z hlediska trestního zákona movitý předmět ...) z dispozice vlastníka nebo oprávněného držitele s úmyslem sám s ní moci volně a neomezeně nakládat,“ viz marg. č. 5 komentáře V. Vočky k § 173 TZ (Draštík, a další, 2015). Jinými slovy „pachatel si zjedná možnost s takovou věcí nakládat s vyloučením toho, kdo ji měl dosud ve své moci. Zmocnění se věci tudíž představuje převedení faktické moci nad ní z oprávněné osoby na pachatele. Napadený nemusí být vlastníkem věci, stačí, že ji má ve své dispozici proto, že mu věc byla půjčena, svěřena apod.“ (Šámal, 2012 str. 1726) – lze proto uvažovat i o věci/avatarovi s jeho

převedení avatara na jinou osobu.[213]V obou případech pak přichází v úvahu i souběh s trestným činem podvodu (§ 209 TZ), případně trestněprávní kvalifikace jednání jako podvodného bez dalšího (např. pokud pachatel míní vystupovat jménem poškozeného uživatele, jehož avatara se zmocnil). Ke slovu může přijít i zpronevěra.[214]

Skutkové podstaty trestného činu neoprávněného užívání cizí věci,[215] zatajení věci a poškození cizí věci (§ 207, 219 a 228 odst. 1 TZ) obsahují znak věci nikoli malé hodnoty nebo způsobení škody nikoli malé hodnoty (tj. dosahující částky nejméně 25.000 Kč, viz § 138 odst. 1 TZ), což jejich aplikaci v souvislosti s avatarem ve většině případů zřejmě vyloučí (snad až na výjimky dlouhodobě vyvíjených nebo „profesionálních" avatarů). Podobně i aplikace skutkové podstaty trestného činu porušení autorského práva, práv souvisejících s právem autorským a práv k databázi (§ 270 TZ) tam, kde avatar nabude podoby autorského díla. Nanejvýš nepravděpodobné je pak plenění v prostoru válečných operací (§ 414 TZ).[216]

Vzácně by se dalo uvažovat také o avatarovi v souvislosti s výrobou a jiným nakládáním s dětskou pornografií zejm. dle § 192 odst. 1 a/nebo 3 TZ (pokud by avatar zjevně zobrazoval dítě, tj. dle § 126 TZ osobu mladší 18 let, a bude-li zachycen na fotografiích či videu pornografického charakteru),[217] dále pak o šíření pornografie v případě tvrdé pornografie (§ 191 odst. 1 TZ) nebo prosté pornografie šířené směrem k dětem (§ 191 odst. 2 TZ).

5.3. Shrnutí k dalším kriminogenním faktorům

Netholismus představuje coby závislost významný kriminogenní a především viktimogenní faktor, ať už jde o závislost u mládeže nejčastěji spojenou se SNS nebo hraním her, případně

---

pravidly užívání stanovenými smluvními podmínkami provozovatele hry, sociální sítě atd.

[213] Pokud pachatel pouze získá datový soubor obsahující avatara (ať už v elektronické nebo listinné podobě), samo o sobě to ještě neznamená zároveň odnětí věci z dispozice vlastníka či zde spíše oprávněného držitele, neboť samotné zkopírování datového souboru původní soubor nikterak neovlivní.

[214] Pokud např. uživatel „půjčí" svého avatara jinému, a tento se rozhodne si jej ponechat (aniž by úmysl přisvojit si jej pojal ještě před zapůjčením, a tedy by nešlo ve vztahu k původnímu uživateli o podvod dle § 209 TZ).

[215] Ať už by se měl pachatel zmocnit cizího avatara dle al. 1 nebo způsobit jeho neoprávněným užíváním škodu na cizím majetku poté, co mu byl svěřen dle al. 2 § 207 TZ.

[216] I pokud by na takové jednání došlo formou sbíhajících se trestných činů, a nejednalo se o pokračování v trestném činu (§ 116 TZ), kdy se sčítají škody způsobené jednotlivými dílčími útoky, trestný čin spočívající v přisvojení si avatara v prostoru válečných operací, na bojišti, v místech postižených válečnými operacemi, ozbrojeným konfliktem nebo na obsazeném území, by byl pravděpodobně fakticky konzumován dalším jednáním pachatele.

[217] Byť lze vyslovit určité pochybnosti ohledně protiprávnosti zcela virtuální „dětské" pornografie.

sebepoškozováním. Riziko „pouhého“ excesivního užívání pak spočívá zejm. v množství času, aktivit a sociálních kontaktů v daném prostředí na úkor tomu reálném a preferenci online prostředí a vztahů až po případný netholismus.

Určitým dobrovolným sebepoškozováním je už samotné časté využívání SNS, neboť navzdory pozitivním stránkám vede mnohdy k nespokojenosti s vlastním životem v porovnání s životem těch druhých (resp. jeho prezentovanou podobou na SNS), případně až k FOMO syndromu. Jiné formy sebepoškozování nachází v online prostředí vyjádření v podobě podpůrných webů (zvlášť v případě poruch příjmů potravy), odrazujících i vybízejících k sebepoškozování, a to vč. nejzávažnějších sebevražd.

Závislostní potenciál počítačových her spočívá především v prožívání úspěchu a v návaznosti na to pak mnohdy i uznání ze strany ostatních hráčů (zejm. vlastní referenční skupiny v daném virtuálním prostředí). Zvlášť spojení telepresence s avatarem, s nímž se hráč identifikuje, může vést k fakticky zcela reálnému prožitku. Zajištění si uznání prostřednictvím avatara zároveň vede i k větší sebeidentifikaci s ním a činí hru/virtuální prostředí o to lákavější oproti reálnému světu. Na jedné straně tak nabízí možnost snížit případnou frustraci plynoucí z nedostatku uznání v reálném světě jeho nahrazením uznáním ve světě virtuálním, na stranu druhou však připoutává uživatele k virtuálnímu prostředí, kde je “úspěšnější”.

Avatar může být jednorázový, krátkodobý nebo dlouhodobý, může být jediným i jedním z mnoha (hlavní a vedlejší). Uživatel jeho prostřednictvím zakouší různé sociální role, komunikuje s jinými avatary/hráči, hraje svou úlohu v rámci skupiny, „prožívá“ (např. poznání „nového místa“). Kromě citové hodnoty obsahuje i ekonomický prvek v podobě investice herního času a reálných i virtuálních peněz. Případný útok na avatara tak může být motivován způsobením nemajetkové újmy i hmotné škody, resp. bezdůvodným obohacením. V úvahu přichází též avatar coby prostředek útoku (např. při vydírání).

Z právního hlediska přichází v úvahu pojetí avatara (datový soubor v podobě strojového kódu, na rozdíl od počítačového programu bez vlastního zdrojového kódu) jako nehmotné movité věci, dle dalších okolností zastupitelné i nezastupitelné, zuživatelné i nezuživatelné, častěji součásti uživatelského (herního aj.) účtu než samostatné věci. Také však může být samostatným výtvarným autorským dílem, neodvozeným od díla původního – počítačového programu (díla literárního). Nakonec pak i součástí osobnosti svého uživatele. Podle toho se pak odvíjí i případná trestněprávní kvalifikace neoprávněného nakládání s avatarem.

Avatar je věcí i z hlediska trestního práva, od čehož se odvíjí i relevantní skutkové podstaty (v závislosti na tom, zda ho pojmeme jako věc, autorské dílo nebo součást osobnosti), vždy se ovšem může jednat o takovou součást jeho života, jejíž poškození by mohl uživatel vnímat jako těžkou újmu, zvlášť ve spojení se vztahem digitálních domorodců k vlastnímu avatarovi a na něj navázanému sociálnímu okolí (např. ve spojení s vydíráním nebo sexuálním nátlakem). Vážná újma prostřednictvím avatara pak přichází v úvahu např. u pomluvy nebo poškození cizích práv. Avatar coby věc a předmět útoku pak může figurovat např. u loupeže, krádeže, podvodu. Může hrát roli i ve výrobě a jiném nakládání s dětskou pornografií a šíření pornografie.

Ohrožení mládeže prostřednictvím avatara pak vystupuje zvlášť naléhavě vzhledem k jejich možnému sepětí s ním, ať už na SNS nebo ve virtuálním prostředí. Avatar coby prostředek útoku vedeného dítětem či mladistvým pak přichází ke slovu např. při kyberšikaně. Nastíněné pojetí avatara (vč. otázky, zda „mám avatara“ nebo „jsem svým avatarem“) může čtenáři-neuživateli připadat nepravděpodobné, někdo jde však ve svých úvahách ještě dále – např. koncept avatara coby reprezentace uživatele v kyberprostoru vůbec.[218]

[218]Uživatel by např. nepoužíval webový vyhledávač, ale prostřednictvím avatara by “navštívil” knihovnu s odkazy v podobě knih přesměrujících ho otevřením na dané místo – např. virtuální “kamennou prodejnu”.

6. Právní rámec kyberprostoru

S ohledem na globalizaci a decentralizaci podléhá internet různým právním řádům s odlišnými pravidly a zároveň je jeho regulace jednotlivými státy poměrně neúčinná. Klíčová je proto mezinárodní spolupráce s doplněním příslušné národní legislativy. Pro ČR hrají nevýznamnější roli CoC, legislativa Evropské unie a národní předpisy: příslušné ústavní, zákonné (vč. trestních) a podzákonné normy, které regulují samotný obsah na internetu, přístup k němu, poskytování služeb, zabezpečení atd. V zájmu vyhnutí se určité bezbřehosti[219] je zde položen důraz na trestněprávní úpravu v národní legislativě a ji přímo ovlivňující relevantní mezinárodní dokumenty, výčet relevantních předpisů dotýkajících se kyberprostoru proto není z celkového hlediska ani zdaleka vyčerpávající.[220]

Základní rámec právnímu vymezení online prostředí a chování v něm dávají ústavní zákony, zejm. Listina, byť lze jít i obecnější cestou a zmínit např. zásadu legální licence nebo úctu ke svobodám člověka a občana (čl. 2 odst. 4 a čl. 1 odst. 1 Ústavy).[221] Listina zakotvuje především ochranu osobnosti a právo na soukromí (čl. 10 Listiny), dnes problematické zejm. s ohledem na stírání veřejného a soukromého prostoru[222] nebo technologický rozvoj sledovacích zařízení dostupných prakticky pro kohokoliv, blíže k tomu viz komentář E. Wagnerové k čl. 10 Listiny (Wagnerová, a další, 2011). Dále poskytuje ochranu listovního tajemství a tajemství jiných písemností (důvěrnost komunikace zahrnující i emailovou komunikaci aj.), právo na vyjadřování vlastních názorů a vyhledávání jiných spolu s nepřípustností cenzury (zákonem omezitelné s ohledem na ochranu práv a svobod druhých, mravnosti atd.) a nakonec zásadu nullum crimen sine lege (čl. 13, 17 a 39 Listiny).

Významným předpisem z hlediska zajištění ochrany kritické infrastruktury státu, potažmo infrastruktury internetu vůbec je ZoKB,[223] který zakotvuje mj. NÚKIB a pojmy jako

[219] Bylo by zcela nadbytečné uvádět předpisy dotýkající se kyberprostoru jen vzdáleně nebo v jiné než trestněprávní oblasti - např. směrnice Evropského parlamentu a Rady 2012/19/EU ze dne 4. července 2012 o odpadních elektrických a elektronických zařízeních (OEEZ) nebo rozhodnutí Evropského parlamentu a Rady č. 1152/2003/ES ze dne 16. června 2003 o zavedení elektronického systému pro přepravu a sledování výrobků podléhajících spotřební dani, zák. č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů (upravuje mj. elektronické systémy spisové služby) atd.

[220] Názorný výčet podává např. V. Smejkal (Smejkal, 2018 str. 72).

[221] Lze jít i ještě obecnější cestou - např..

[222] Např. „veřejný“ profil na SNS – viz např. diskuse nad „veřejným vs. soukromým“ vystupováním prezidentova mluvčího (Kabátová, 2017).

[223] Jeho přijetí předpokládala Strategie pro oblast kybernetické bezpečnosti ČR na období 2012 – 2015. Současná Národní strategie si klade za cíl při zajišťování kybernetické bezpečnosti mj. zajištění efektivity a posilování všech struktur, procesů a spolupráce (ve veřejném sektoru, se soukromým sektorem, s mezinárodním prvkem), podporu vzdělávání a osvětu, rozvoj schopností Policie ČR vyšetřovat a postihovat informační kriminalitu, pokračovat v tvorbě a úpravě právního rámce zajišťujícího kybernetickou bezpečnost atd. Blíže k jednotlivým

kybernetická bezpečnostní událost nebo kybernetický bezpečnostní incident, a příslušné prováděcí předpisy.[224] Dále upravuje oblast kyberprostoru řada dalších právních předpisů, vč. zák. č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, zák. č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, zák. č. 127/2005 Sb., o elektronických komunikacích, zák. č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), zák. č. 251/2016 Sb., o některých přestupcích. Jednotlivé zákony stanovují zpravidla i přestupky a jiné správní delikty a sankce za jejich spáchání, s obecnými pravidly procesního i hmotněprávního charakteru stanovenými zákonem č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich. Z hlediska kriminality ve spojení s využíváním nových médií dětmi ovšem přichází v úvahu zejm. přestupky proti občanskému soužití a proti majetku (§ 7 a 8 zák. o některých přestupcích).[225]

Zvláštní pozornost zasluhuje v souvislosti s kyberprostorem s ohledem na rozmach SNS a snadnost automatického zpracování dat ze strany osob a institucí z veřejné i soukromé sféry ochrana osobních údajů (od shromáždění přes uchování a využití po likvidaci). Zvyšuje se také kapacita a rychlost přenosu a uchovávání dat, a tak lze ve spojení s vynalézavě programovanými automatickými systémy např. získat v relativně krátkém čase velké množství osobních údajů od mnoha osob.[226] Zároveň množství osob sděluje/zveřejňuje své osobní aj. údaje zcela dobrovolně, ve velkém množství a bez zábran. Zejm. u dětí je tento jev patrný – zhruba polovina evropských dětí ochotně sděluje své osobní údaje prostřednictvím internetu (vč. intimních informací, fotografií atp.), a to i osobám známým pouze online (Livingstone, a další, 2009 str. 16 a 43), (Livingstone, a další, 2011). Jde ale také o údaje zpracovávané v souvislosti s výkonem veřejné moci, ať už se povinnost jejich zpracování týká každého člověka či občana nebo ad hoc pouze některých (např. matriční údaje oproti datům zpracovávaným v souvislosti se soudním řízením konkrétní osoby). Základní atributy upravuje GDPR dosud stále doplněné zákonem č. 101/2000 Sb., o ochraně osobních údajů a o

strategiím a příslušným akčním plánům viz (NÚKIB).

[224] V současnosti vyhl. č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), vyhl. č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby, vyhl. č. 205/2016 Sb., kterou se mění vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích a samotná vyhl. č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, jejíž další novelizace se připravuje (Úřad Vlády ČR).

[225] U přestupků proti majetku zejm. při podvodném jednání nenaplňujícím všechny znaky trestného činu podvodu např. z důvodu způsobení nižší než nikoli nepatrné škody [§ 8 odst. 1 nebo 2, písm. a) bod 3. zák. o některých přestupcích].

[226] Např. spuštěním bota na SNS, kde vyhledává dostupné osobní údaje uživatelů, případně s nimi i na základní úrovni komunikuje (Jelínek, a další, 2015 str. 286).

změně některých zákonů, který má být v nejbližší době nahrazen novým zákonem[227] reflektujícím celoevropskou úpravu a doplňujícím/konkretizujícím GDPR. K hlavním změnám a novým institutům patří mj. právo „být zapomenut“ (právo na výmaz uvedené v čl. 17 GDPR) a posílení ochrany dětí, blíže k tomu viz podkapitola Zneužití technické stránky internetu, (Vláda ČR. Poslanecká sněmovna Parlamentu ČR. VIII volební období, 2019) a (Škorničková). Proti zneužití osobních aj. údajů chrání i řada dalších předpisů upravujících např. povinnost mlčenlivosti, ale také povinnost dbát ochrany osobnosti zakotvené v Oddíle 6 Dílu 2 Hlavy II Části první NOZ: zejm. ochrany osobnosti vůbec (§ 81 NOZ), zachycení a rozšiřování podoby (§ 84 a 85 NOZ) a nedotknutelnost soukromí (§ 86 NOZ). V trestněprávní rovině může neoprávněné nakládání s osobními údaji naplnit znaky různých skutkových podstat, zejm. neoprávněného nakládání s osobními údaji (shromážděnými v souvislosti s výkonem veřejné moci nebo chráněnými státem uznanou povinností mlčenlivosti, viz § 180 odst. 1 a 2 TZ).

Značné obavy ze ztráty soukromí bývají spojovány s IoT, neboť připojená zařízení zpravidla odesílají na příslušná místa množství dat, vč. případných provozních a lokalizačních údajů. Mnohdy se může jednat o velmi citlivé osobní údaje [§ 4 písm. b) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů], např. biometrická data o zdravotním stavu nositele chytrých hodinek. Kvalita ochrany se odvíjí do jisté míry od způsobu a síly použitého šifrování dat, které však není samozřejmostí. Kromě toho nelze opomenout ani možnost neoprávněného „odposlechu“ takto odesílaných dat a jejich případné následné zneužití. Připojené „věci“ také podléhají malwarovým útokům z prostředí sítě nebo jiným formám pokusu o zneužití či znefunkčnění (např. vyřazení ochranného alarmu a jeho komunikace s pultem centrální ochrany před vloupáním se do rodinného domu). Panují také jisté obavy ohledně možného přetěžování sítí v souvislosti s rostoucím počtem připojených zařízení (BusinessIT, 2015).

[227] Příslušné návrhy projednává Parlament ČR, po schválení Poslaneckou sněmovnou ve 3. čtení jako sněmovní tisky 138 (vládní návrh zákona o zpracování osobních údajů – EU) a 139 (vládní návrh zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů) byly oba zákony doručeny 8.1.2019 Senátu, viz (Vláda ČR. Poslanecká sněmovna Parlamentu ČR. VIII volební období, 2019) a (Vláda ČR. Poslanecká sněmovna Parlamentu ČR. VIII volební období, 2019).

6.1. Trestněprávní postih kyberkriminality[228]

Nejvýznamnějším dokumentem na poli mezinárodního práva je co do postihu kyberkriminality nepochybně CoC[229] vzniknuvší na půdě Rady Evropy. Dále je to Dodatkový protokol[230] a několik směrnic EU zakotvujících postih určitých jednání (součástí bývají též pravidla procesněprávního charakteru). Z hlediska práva EU se na rozdíl od CoC soustředí právní dokumenty relevantní pro postih kyberkriminality především na boj proti sexuálnímu vykořisťování dětí a ochranu práv duševního vlastnictví. Stěžejní je v tomto směru směrnice Evropského parlamentu a Rady 2011/93/EU ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV, dále pak směrnice Evropského parlamentu a Rady 2004/48/ES ze dne 29. dubna 2004 o dodržování práv duševního vlastnictví, směrnice Evropského parlamentu a Rady 96/9/ES ze dne 11. března 1996 o právní ochraně databází a směrnice Evropského parlamentu a Rady 2001/29/ES ze dne 22. května 2001 o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti.

Za kyberkriminalitu lze v nejužším smyslu považovat jednání podřaditelná pod počítačové trestné činy (§ 230-232 TZ), jejichž objektem je „zájem na ochraně počítačových systémů a jejich částí, dále dat v nich uložených a dat uložených na nosičích informací a také na ochraně počítačů nebo jiných technických zařízeních pro zpracování dat před neoprávněnými přístupy a zásahy“ (Šámal, 2016 str. 695). Z hlediska subjektivní stránky vyžadují základní skutkové podstaty počítačových trestných činů úmyslné zavinění, pouze k naplnění skutkové podstaty trestného činu poškození záznamu v počítačovém systému a na nosiči informací a zásahu do vybavení počítače z nedbalosti (§ 232 odst. 1 TZ) postačí zavinění z hrubé nedbalosti, jak ostatně název naznačuje, tj. takové, kdy „přístup pachatele k požadavku náležité opatrnosti svědčí o zřejmé bezohlednosti pachatele k zájmům chráněných trestním zákonem“ (Šámal, 2012 str. 2323). U kvalifikovaných skutkových podstat počítačových trestných činů se úmysl vyžaduje pro naplnění skutkové podstaty trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 odst. 3 písm. a) i b) TZ, stejně tak dle § 230 odst. 4 písm. a) TZ (vyplývá z povahy věci), totéž platí pro skutkovou podstatu

[228]Kapitola vznikla za podpory programu rozvoje vědních oblastí na Univerzitě Karlově (PRVOUK) P06 "Veřejné právo v kontextu europeizace a globalizace" a byla publikována (Jelínek, a další, 2015 stránky 288-297), částečně vychází z (Kyberkriminalita dnes, 2014).
[229] Název Úmluva o počítačové kriminalitě používá český překlad prezentovaný Radou Evropy (Rada Evropy) i řada autorů, viz např. (Gřivna, a další, 2008), nicméně přiléhavější se zdá být Úmluva o kyberkriminalitě, vzhledem k rozšiřujícímu se spektru IoT. CoC vznikla v roce 2001 a vstoupila v účinnost 1. 7. 2004, ČR ji podepsala 9. února 2005 a ratifikovala 22. srpna 2013.
[230]ČR ho podepsala 17. května 2013 a ratifikovala 7. srpna 2014 s účinností od 1.12.2014.

trestného činu opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat dle § 231 odst. 2 písm. a) TZ. Ve všech ostatních případech postačí nedbalostní zavinění okolnosti zvlášť přitěžující, zde vždy v podobě těžšího následku [srov. § 17 písm. a) TZ a § 230 odst. 4 písm. b), c), d) a e), odst. 5 TZ, § 231 odst. 2 písm. b), odst. 3 TZ a § 232 odst. 2 TZ]. Všechny tři počítačové trestné činy jsou zařazeny v rámci hlavy V. TZ. Kromě kvalifikované skutkové podstaty trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 odst. 1, 5 TZ nebo dle § 230 odst., 5 TZ, kdy jde o zločin,[231] se jedná o přečiny.[232]

Zdaleka nejfrekventovanější neoprávněný přístup k počítačovému systému a nosiči informací (§ 230 TZ) obsahuje dvě základní skutkové podstaty (Šámal, 2016 str. 696). V prvním odstavci dopadá na jakýkoliv neoprávněný přístup k PS a nosiči informací, tedy na pachatele, jenž překoná bezpečnostní opatření mající za úkol přístup omezit (Šámal, 2012 str. 2305). V současnosti se jedná nejčastěji o překážku omezující přístup k fyzickému zařízení prostřednictvím internetu v podobě firewallu, obvykle též zároveň za použití antivirového programu, případně antispywaru. Bezpečnostních opatření si uživatel nemusí ani býti zcela vědom (např. má určité povědomí o tom, že používá nějaký antivirový program zabraňující průniku nevyžádaného softwaru do vlastního zařízení, netuší však již, že součástí daného antivirového programu je zároveň antispyware). A samozřejmě nelze opomenout ani základní ochranu obsahu či přístupu prostřednictvím hesla, bez ohledu na jeho snadnou prolomitelnost (např. heslo „12345“) či naopak sílu. Naplnění objektivní stránky skutkové podstaty trestného činu dle § 230 odst. 1 TZ může být samotným cílem pachatele (např. pachatel chce zjistit obsah nosiče informací - USB flash disku chráněného heslem, aniž by však měl v úmyslu s daty tam uloženými jakýmkoliv způsobem manipulovat či k nim přidat data jiná). Nebude však výjimkou, aby uvedené jednání sloužilo jako příprava k dalšímu jednání, zejm. v podobě neoprávněného nakládání s daty, tj. naplňující objektivní stránku základní skutkové podstaty uvedené v odst. 2 (§ 230 TZ). Zde již nezáleží na oprávněnosti získání přístupu k PS nebo nosiči informací. Může tedy jít o přístup oprávněný (např. přístup administrátora spravujícího firemní síť v rámci pracovněprávních povinností), stejně tak jako neoprávněný, kterým je zároveň naplněna skutková podstata dle prvního odstavce (§ 230 TZ), která však

[231] Za uvedená jednání hrozí trest odnětí svobody s horní hranicí osmi let, a tedy se nejedná o přečin, srov. § 14 odst. 2 TZ. Jelikož horní hranice trestu odnětí svobody za uvedená jednání je zároveň nižší než deset let, nepůjde o zvlášť závažný zločin, srov. § 14 odst. 2 a 3 TZ.

[232] Za uvedená jednání hrozí trest odnětí svobody s horní hranicí šest měsíců, jeden rok, dvě léta, tři léta nebo pět let – ve všech těchto případech se jedná o přečin (v případě přečinu dle § 232 TZ již vzhledem k tomu, že se jedná o nedbalostní trestný čin), srov. § 14 odst. 2 TZ.

pravděpodobně bude fakticky konzumována. Objektivní stránku § 231 TZ lze naplnit pouze v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) TZ nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2 TZ (může jít např. o počítačový program přizpůsobený k prolomení hesla). Způsobením značné škody spočívající ve znehodnocení dat nebo zásahu do technického či programového zařízení pro zpracování dat, a to porušením povinnosti vyplývající ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté lze pak spáchat trestný čin dle § 232 TZ. Vyžaduje se zde tedy speciální subjekt – tím může být „jednak osoba (fyzická nebo právnická), která vykonává zaměstnání, povolání, postavení nebo funkci, jednak i jiná osoba (fyzická nebo právnická), která porušila zákonem uloženou nebo smluvně převzatou povinnost“ (Šámal, 2012 str. 2323).

Formulace počítačových trestných činů v rámci TZ vychází především z čl. 2 CoC požadujícího kriminalizaci neoprávněného přístupu do počítačového systému nebo jeho části (§ 230 odst. 1 TZ), a to vč. přípravného jednání (s ohledem na koncipování trestní odpovědnosti za přípravu pouze zvlášť závažného zločinu obsahuje TZ i samostatnou skutkovou podstatu v § 231 TZ). Dále vychází z čl. 4 a 5 CoC požadujícího kriminalizaci neoprávněného zásahu do dat nebo systému [§ 230 odst. 2 písm. b), c) a d) TZ], zneužití zařízení v čl. 6 CoC (§ 231 TZ) a falšování údajů souvisejících s počítači v čl. 7 CoC [§ 230 odst. 2 písm. c) TZ]. Mimoto zavazovalo ČR k postihu počítačových trestných činů i Rámcové rozhodnutí Rady EU 2005/222/SVV ze dne 24. února 2005 o útocích proti informačním systémům, které požadovalo v čl. 8 kriminalizaci protiprávního přístupu k informačním systémům [čl. 1 písm. a) a čl. 2 tohoto rámcového rozhodnutí, odpovídajícím ustanovením v rámci TZ je § 230 odst. 1 a § 231] a protiprávního zásahu do systému nebo dat [čl. 3 a 4 tohoto rámcového rozhodnutí a § 230 odst. 2 písm. b), c) a d) TZ]. Uvedené rámcové rozhodnutí bylo s účinností od 3. září 2013 nahrazeno směrnicí Evropského parlamentu a Rady 2013/40/EU ze dne 12. srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV.[233] Ta požaduje kriminalizaci neoprávněného přístupu k informačním systémům v čl. 3, neoprávněného zasahování do informačních systémů v čl. 4 a neoprávněného zasahování do údajů v čl. 5 (§ 230 a též § 276 TZ). Kromě toho požaduje tato směrnice v čl. 6 kriminalizaci neoprávněného sledování údajů (§ 182 TZ) a neoprávněného nakládání s počítačovými programy, hesly, přístupovými

[233] Transpozici provedl zákon č. 165/2015 Sb., kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, který zpřísnil horní hranice trestní sazby u skutkové podstaty neoprávněného přístupu k počítačovému systému a nosiči informací (§ 230 odst. 1, 2, 3 TZ).

kódy aj. obdobnými údaji se záměrem použít je ke spáchání některého z výše uvedených trestných činů. Rovněž požadavek trestnosti pokusu a účastenství na těchto trestných činech je v rámci TZ naplněn (§ 21, 24 TZ).[234]

Kromě toho ovšem reaguje TZ na „kyberrealitu" i dalšími ustanoveními.[235] Skutková podstata trestného činu porušení tajemství dopravovaných zpráv (§ 182 TZ) se v prvním odstavci vztahuje mj. k úmyslnému porušení tajemství datových, textových, hlasových, zvukových či obrazových zpráv posílaných prostřednictvím sítě elektronických komunikací a přiřaditelných k identifikovanému účastníku nebo uživateli, který zprávu přijímá, a k neveřejnému přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, vč. elektromagnetického vyzařování z počítačového systému, přenášejícího taková počítačová data[236] [§ 182 odst. 1 písm. b) a c) TZ]. Typicky proto půjde např. o email, se kterým se dosud adresát neměl možnost seznámit.[237] Klíčový je proto okamžik, kdy poprvé vstoupí uživatel do své emailové schránky poté, co email dorazil na místo svého určení, tj. na příslušný server, jehož prostřednictvím se může adresát s obsahem emailu seznámit. Dále se dotýká kyberprostoru i druhý odstavec § 182 TZ, kde se hovoří o prozrazení nebo využití tajemství, o němž se pachatel dozvěděl z přenosu prostřednictvím sítě elektronických komunikací, který nebyl určen jemu. Obdobně též základní skutková podstata trestného činu porušení tajemství dopravovaných zpráv dle § 182 odst. 5 písm. c) TZ, kterou může naplnit pouze speciální subjekt, a to mj. zaměstnanec provozovatele počítačového systému anebo kdokoli jiný vykonávající komunikační činnosti, pokud pozmění nebo potlačí mj. zprávu podanou neveřejným přenosem počítačových dat nebo jiným podobným způsobem. Závazek k postihu porušení tajemství dopravovaných zpráv obsahuje směrnice Evropského parlamentu a Rady 2013/40/EU ze dne 12. srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV, požadující mj. ve svém čl. 6 kriminalizaci neoprávněného sledování údajů.

Obdobně jako porušení tajemství dopravovaných zpráv i skutková podstata trestného činu porušení tajemství listin a jiných dokumentů uchovávaných v soukromí (§ 183 odst. 1 TZ) dopadá na neoprávněné nakládání s emaily a dalším obsahem (např. zprávy na SNS nebo jakékoliv uložené soubory), když postihuje jednání spočívající v neoprávněném porušení

[234] Vč. trestní odpovědnosti právnických osob za poškození a ohrožení provozu obecně prospěšného zařízení (§ 276 TZ, § 7 TOPO).
[235] Odstavec vychází z (Kyberkriminalita dnes, 2014).
[236] Vztahuje se k tzv. počítačovým datům (Šámal, 2012 str. 1809).
[237] Srov. rozhodnutí Nejvyššího soudu 8 Tdo 407/2011 a 11 Tdo 349/2009.

tajemství mj. počítačových dat nebo jiného záznamu[238] uchovávaného v soukromí jiného tím, že je zveřejní, zpřístupní třetí osobě nebo je jiným způsobem použije. Z hlediska emailu se bude jednat o takové neoprávněné nakládání s ním od okamžiku, kdy se adresát mohl s jeho obsahem seznámit (viz výše) bez ohledu na to, zda tak skutečně učiní či nikoliv.

Vynechat nelze ani skutkovou podstatu trestného činu poškození a ohrožení provozu obecně prospěšného zařízení (úmyslné i nedbalostní, § 276 a 277 TZ). Dle výkladového ustanovení uvedeného v § 132 TZ je obecně prospěšným zařízením i zařízení a sítě elektronických komunikací, kdy proto takovým zařízením bude typicky např. server, ať už půjde o server firemní či využívaný širokou veřejností v rámci zapojení do sítě Internet. V úvahu proto připadá tato skutková podstata zejm. v případě DDoS.[239]

Dále jsou s kyberprostorem spjaty skutkové podstaty zohledňující spáchání činu veřejně nebo veřejně přístupnou počítačovou sítí jako zvlášť přitěžující okolnost. Trestný čin je spáchán veřejně mj. tehdy, je-li spáchán veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem [§ 117 písm. a) TZ].[240] Z hlediska spáchání činu veřejně přístupnou počítačovou sítí jakožto okolnosti podmiňující použití vyšší trestní sazby se jedná o skutkovou podstatu trestného činu neoprávněného nakládání s osobními údaji, pomluvy, šíření pornografie, výroby a jiného nakládání s dětskou pornografií, šíření toxikomanie, podpory a propagace terorismu a vyhrožování teroristickým trestným činem,[241] křivého obvinění, násilí proti skupině obyvatelů a proti jednotlivci, hanobení národa, rasy, etnické nebo jiné skupiny osob, podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod, založení, podpory a propagace hnutí směřujícího k potlačení práv a svobod

[238] Např. záznam zachycený pomocí webové kamery v počítači (Šámal, 2012 str. 1823).

[239] DDoS míří na zneprovoznění konkrétního serveru. Útočníci obvykle vytvoří nejprve tzv. botnet, tj. síť podřízených počítačů (např. předchozím zasažením malwarem), jejichž prostřednictvím následně požaduje po cíleném serveru určitou činnost. V závislosti na množství takových požadavků pak může dojít k zahlcení serveru a jeho znepřístupnění. Trestněprávní kvalifikace jednání může poměrně variovat především podle toho, zda je takový „úspěšný" útok proveden prostřednictvím podřízených počítačů bez vědomí jejich uživatelů (a tudíž zpravidla po předchozím neoprávněném přístupu k počítačovému systému a neoprávněném vložení dat/malwaru) a zda cílený server skutečně zasáhl nebo zůstal takříkajíc přede dveřmi, tj. na úrovni firewallu. Ten sice není obecně prospěšným zařízením (§ 132 TZ), avšak jeho zahlcení může vést k ohrožení využívání serveru jakožto obecně prospěšného zařízení, neboť v jeho důsledku je znemožněn přistup k serveru ostatním uživatelům.

[240] Veřejně přístupnou počítačovou sítí se rozumí „funkční propojení počítačů do sítí s cílem vytvořit informační systém pracující s tzv. dálkovým přístupem, jakým je především internet a jiné podobné informační systémy" (Šámal, 2012 str. 1300).

[241] Skutkové podstaty podpory a propagace terorismu a vyhrožování teroristickým trestným činem byly zakotveny do TZ s účinností od 1.2.2017 zákonem č. 455/2016 Sb., kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a další související zákony. Novela reagovala na rámcové rozhodnutí Rady 2008/919/SVV ze dne 28. listopadu 2008, kterým se mění rámcové rozhodnutí 2002/475/SVV o boji proti terorismu (Vláda ČR; Poslanecká sněmovna PČR, 2016), nyní neplatné v důsledku směrnice Evropského parlamentu a Rady (EU) 2017/541 ze dne 15. března 2017 o boji proti terorismu, kterou se nahrazuje rámcové rozhodnutí Rady 2002/475/SVV a mění rozhodnutí Rady 2005/671/SVV.

člověka a podněcování útočné války [§ 180 odst. 3 písm. b), § 184 odst. 2, § 191 odst. 3 písm. b), § 192 odst. 4 písm. b), § 287 odst. 2 písm. c), § 312e odst. 4 písm. a), § 312f odst. 2 písm. b), § 345 odst. 3 písm. b), § 352 odst. 3 písm. b), § 355 odst. 2 písm. b), § 356 odst. 3 písm. a), § 403 odst. 2 písm. a) a § 407 odst. 2 písm. b) TZ].

Z hlediska spáchání trestného činu veřejně jsou relevantní skutkové podstaty trestného činu podpory a propagace terorismu, hanobení národa, rasy, etnické nebo jiné skupiny osob, podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod, podněcování k trestnému činu,[242] schvalování trestného činu, genocidia, projevu sympatií k hnutí směřujícímu k potlačení práv a svobod člověka, popírání, zpochybňování, schvalování a ospravedlňování genocidia a podněcování útočné války. [§ 312 odst. 1, § 355 odst. 1 písm. a) i b), § 355 odst. 1 písm. a) i b), § 356 odst. 1, § 364, 365 odst. 1, § 400 odst. 2, § 404, 405 a § 407 odst. 1 TZ].

Do této skupiny spadá i skutková podstata trestného činu týrání zvířat, kterou naplní ten, kdo týrá zvíře surovým nebo trýznivým způsobem veřejně nebo na místě veřejnosti přístupném, a trestného činu výtržnictví, kterou naplní, kdo se dopustí veřejně nebo na místě veřejnosti přístupném hrubé neslušnosti nebo výtržnosti [§ 302 odst. 1 písm. b) a § 358 odst. 1 TZ]. Místo veřejnosti přístupné je „každé místo, kam má přístup široký okruh lidí individuálně neurčených a kde se také zpravidla více lidí zdržuje, takže týrání zvířete může vnímat více lidí, byť v době činu tam nemusí být přítomni. Takové místo však nemusí být přístupné bez omezení komukoli a kdykoli ..., nýbrž postačí, že jsou přístupné jen některým osobám určeným např. povahou jejich zaměstnání nebo jinak a v určitou dobu“ (Šámal, 2012 str. 313 a 3324). Takovým neveřejným místem proto může být z hlediska kyberprostoru např. i uzavřená firemní počítačová síť, ke které bude mít přístup široký okruh blíže neurčených osob (např. po zadání příslušných přihlašovacích údajů opravňujících uživatele-zaměstnance ke vstupu do prostoru sítě), aniž by se však jednalo o veřejně přístupnou počítačovou síť. V případě, že k takové uzavřené síti bude mít přístup jen malý okruh blíže neurčených osob, nemělo by se jednat o spáchání činu na místě veřejnosti přístupném a tím spíše ne o spáchání činu veřejně přístupnou počítačovou sítí, nicméně stále může dané jednání z hlediska okruhu možných zasažených osob (tj. těch, na koho může mít pozorované jednání vliv – typicky

[242] Požadavek kriminalizace jednání spočívajícího v podněcování k trestnému činu jako takového v mezinárodních dokumentech sice nenalezneme, avšak je ve větší či menší míře obsažen hned v několika předpisech, vždy ve spojení s kriminalizací konkrétněji vymezeného jednání.

přihlížející) dosáhnout takové intenzity, aby se jednalo o spáchání činu veřejně, a to „jiným obdobně účinným způsobem“ [§ 117 písm. a) TZ].

Další prvek kyberprostoru lze nalézt u těch skutkových podstat, které operují se zveřejněním určitého obsahu nebo jeho učiněním veřejně přístupným, kdy takovým zveřejněním bude i zveřejnění nebo zpřístupnění na veřejně přístupné počítačové síti, typicky na internetu. Ovšem zejm. v případě zveřejnění/zpřístupnění na SNS bude třeba zabývat se každým případem zvlášť z hlediska posouzení, zda je takové intenzity, jaké odpovídá spáchání činu veřejně, ať už veřejně přístupnou počítačovou sítí nebo vůbec. Již dříve bylo judikováno, že spáchání činu emailem takové intenzity bez dalšího nedosahuje.[243] V případě profilu na SNS je proto třeba nejprve rozlišit, zda je veřejný nebo naopak neveřejný. U veřejného profilu k němu má přístup zpravidla kdokoliv, případně s omezující podmínkou vlastního účtu na dané SNS. Zveřejnění/zpřístupnění obsahu na takovém profilu proto spíše bude svou intenzitou odpovídat spáchání činu veřejně přístupnou počítačovou sítí, nicméně i zde je nezbytné zabývat se počtem uživatelů, kteří mohli mít k danému obsahu přístup. U neveřejného profilu (např. „viditelný jen pro přátele“) je obvykle přístup ostatních uživatelů omezen, a je proto třeba sledovat, kolik osob mohlo nebo stále ještě může mít přístup ke zveřejněnému obsahu. Škála začíná u několika málo osob přes menší či větší skupiny (např. žáci jedné školní třídy nebo celé školy) až po tisíce uživatelů. Jsou ovšem i takové profily, kde naopak jejich obsah není viditelný nikomu kromě samotného uživatele/autora. Proto lze teprve na základě takového posouzení dojít k závěru, zda se mohlo jednat o spáchání činu s obdobnou intenzitou jako spáchání veřejně přístupnou počítačovou sítí.[244] Z hlediska relevantních skutkových podstat přichází v úvahu v tomto směru neoprávněné nakládání s osobními údaji, porušení tajemství listin a jiných dokumentů uchovávaných v soukromí a obě základní skutkové podstaty zneužití informace v obchodním styku (§ 180 odst. 1 a 2, § 183 odst. 1, § 255 odst. 1 a/nebo 2 TZ). Dále pak se znakem „činí veřejně přístupným“ šíření pornografie TZ) a výroba a jiné nakládání s dětskou pornografií (§ 191 odst. 1 a § 192 odst. 3 TZ).

Výše uvedené skutkové podstaty jsou ty, jež reagují na oblast kyberkriminality přímo, ovšem ke slovu přichází i řada dalších skutkových podstat kyberprostor výslovně nezohledňujících,

[243] Naproti tomu již rozeslání zprávy 163 adresátům již znak „spáchání činu veřejně“ naplňuje, viz rozhodnutí Nejvyššího soudu sp. zn. 8 Tdo 1467/2010 ze dne 12.1.2011.
[244] Nejen s ohledem na to, kolik kontaktů má daný profil na sebe navázaných, ale např. také podle toho, zda se jim nově zveřejněný obsah zobrazuje přednostně či nikoliv, viz nález Ústavního soudu ČR sp. zn. I. ÚS 1428/13 ze dne 20.8.2013.

typicky např. skutková podstata trestného činu podvodu (§ 209 TZ)[245] nebo porušení autorského práva, práv souvisejících s právem autorským a práv k databázi (§ 270 TZ).[246] Zejm. v konstrukci skutkové podstaty porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 270 TZ se projevil vliv práva EU, neboť transponuje směrnici Evropského parlamentu a Rady 2004/48/ES ze dne 29. dubna 2004 o dodržování práv duševního vlastnictví, směrnici Evropského parlamentu a Rady 96/9/ES ze dne 11. března 1996 o právní ochraně databází a směrnici Evropského parlamentu a Rady 2001/29/ES ze dne 22. května 2001 o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti.

Specifickou problematikou je v souvislosti s kyberkriminalitou nakládání s dětskou pornografií a sexuální zneužívání dětí prostřednictvím kyberprostoru vůbec. Již tradičně je postihováno zpřístupňování pornografie dětem a nakládání s jakoukoliv formou dětské pornografie (vč. elektronické a počítačové formy) prostřednictvím skutkové podstaty trestného činu šíření pornografie a výroby a jiného nakládání s dětskou pornografií (§ 191 a 192 TZ), v obou případech jde o zvlášť přitěžující okolnost spáchání činu veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem. Mimoto trestní právo kriminalizuje navazování nedovolených kontaktů s dítětem, účast na pornografickém představení a pro úplnost je třeba doplnit ještě trestný čin svádění k pohlavnímu styku[247] (§ 193b, 193a a 202 TZ). Výchozím dokumentem pro postih sexuálního vykořisťování dětí v souvislosti s kyberprostorem je kromě čl. 3 odst. 1 písm. a), (ii), c) Opčního protokolu k Úmluvě o právech dítěte týkajícího se prodeje dětí, dětské prostituce a dětské pornografie[248] především CoC. Ta v čl. 9 požaduje kriminalizaci výroby dětské pornografie pro účely její distribuce [odst. 1 písm. a)], nabízení nebo zpřístupňování [odst. 1 písm. b)], distribuce nebo přenášení [odst. 1 písm. c)], opatřování pro sebe nebo jinou osobu, vždy prostřednictvím počítačového systému [odst. 1 písm. d)], a jejího uchovávání v počítačovém systému nebo na médiu pro ukládání počítačových dat [odst. 1 písm. e)], vč. požadavku možnosti trestněprávního postihu právnických osob. V rámci Rady Evropy vznikla též Úmluva o ochraně dětí před sexuálním

[245] Např. podvodné jednání na aukčním serveru, kdy poškozený po uhrazení požadované částky obdrží namísto slíbeného mobilního telefonu balíček karet.
[246] Např. rozšiřování softwaru bez příslušné licence. Zásah do práva autorského ovšem musí být nikoli nepatrný, přičemž v úvahu je třeba vzít především „intenzitu takového zásahu, způsob provedení činu, jeho následky, ... v případě déletrvajících a opakovaných zásahů i počet takových případů, délku doby narušování konkrétního chráněného práva apod.“ (Šámal, 2012 str. 2753).
[247] Jestliže bude účast na pornografickém představení nebo např. sledování obnažování dítěte za úplatu sledováno pachatelem prostřednictvím sítě elektronických komunikací, tedy např. při videohovoru přes Skype.
[248] Viz sdělení Ministerstva zahraničních věcí ČR č. 74/2013 Sb. m. s., o sjednání Opčního protokolu k Úmluvě o právech dítěte týkajícího se prodeje dětí, dětské prostituce a dětské pornografie.

zneužíváním a sexuálním vykořisťováním, která požaduje kriminalizaci protiprávního úmyslného nakládání s dětskou pornografií (ETS No.: 201, Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse), vč. kriminalizace úmyslného získání přístupu k dětské pornografii prostřednictvím ICT, což bylo zakotveno v TZ až zákonem č. 141/2014 Sb., který kriminalizoval uvedené jednání v rámci skutkové podstaty trestného činu výroby a jiného nakládání s dětskou pornografií vložením nového odst. 2 k § 192 TZ. Na poli práva EU dopadá na postih sexuálního vykořisťování dětí především směrnice Evropského parlamentu a Rady 2011/93/EU ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV, která se týká mimo jiného i jednání spočívajícího v pořizování nebo držení dětské pornografie, vědomém získávání přístupu k ní prostřednictvím ICT, v její distribuci, šíření nebo předávání, v jejím nabízení, dodávání nebo zpřístupňování a ve výrobě dětské pornografie. Tato směrnice požaduje mj. kriminalizaci návrhu setkání dítěti prostřednictvím ICT s cílem účasti na sexuálních praktikách tohoto dítěte nebo výroby dětské pornografie (čl. 6 ve spojení s čl. 3 odst. 4 a čl. 5 odst. 6 této směrnice), na což reagoval český zákonodárce zavedením skutkové podstaty navazování nedovolených kontaktů s dítětem (§ 193b TZ).Článku 3 a zejm. 4 uvedené směrnice pak odpovídá skutková podstata účasti na pornografickém představení (§ 193a TZ).

Ve většině případů kyberkriminality se mohou dopouštět trestné činnosti i právnické osoby.[249] Požadavek jejich trestní odpovědnosti je zpravidla obsažen v dané směrnici či jiném dokumentu požadujícím trestněprávní postih určitého jednání, jimiž je ČR vázána nebo je neratifikovala[250] či k nim dosud nepřistoupila v důsledku dřívější absence právní úpravy trestní odpovědnosti právnických osob (Poslanecká sněmovna PČR; Vláda ČR, 2011 str. 7). Vzhledem ke stávajícímu znění § 7 TOPO[251] (ve spojení s § 110 TZ a § 1 odst. 1 a 2 TOPO) se jedná o skutkové podstaty všech výše uvedených trestných činů. [252]

Trestní odpovědnost právnických osob za počítačové trestné činy (resp. kriminalizaci protiprávního přístupu k informačním systémům)[253] požadovalo v čl. 8. již rámcové

[249] Následující odstavce vychází z autorčiny kapitoly Trestní odpovědnost právnických osob a kyberprostor (Jelínek, 2013 stránky 285-295).
[250] Příkladem budiž dlouhé období mezi podepsáním a ratifikací CoC: vznikla v roce 2001 a vstoupila v účinnost 1. 7. 2004, ČR ji podepsala 9. 2. 2005, avšak ratifikovala právě především z důvodu chybějící trestní odpovědnost právnických osob za vybraná jednání požadovaná v čl. 12 CoC až 22.8.2013.
[251] Novelizovanému zákonem č. 183/2016 Sb., kterým se mění zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, ve znění pozdějších předpisů, s účinností od 1.12.2016.
[252] K otázkám tzv. přičitatelnosti trestného činu právnické osobě viz § 8-10 TOPO a (Jelínek, 2013).
[253] Dle tohoto rozhodnutí je informačním systémem „jakýkoli přístroj nebo skupina vzájemně propojených nebo

rozhodnutí Rady EU 2005/222/SVV ze dne 24. února 2005 o útocích proti informačním systémům. CoC ani uvedené rámcové rozhodnutí ovšem nezavazovaly ke kriminalizaci neoprávněného užití dat uložených v počítačovém systému nebo na nosiči informací [§ 230 odst. 2 písm. a) TZ]. Směrnice Evropského parlamentu a Rady 2013/40/EU ze dne 12. srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV již v čl. 6 přidává kriminalizaci neoprávněného sledování údajů, neoprávněného užití dat uložených v počítačovém systému nebo na nosiči informací však nikoliv. Mimoto žádný z výše uvedených dokumentů nezahrnuje ani požadavek kriminalizace nedbalostní formy zavinění, jak učinil zákonodárce prostřednictvím skutkové podstaty poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232 TZ). Lze tedy konstatovat, že nebyl zcela striktně dodržen deklarovaný úmysl zákonodárce kriminalizovat kromě daňových trestných činů jen taková jednání právnických osob, u nichž požadují zavedení deliktní odpovědnosti právnických osob mezinárodní smlouvy a právní předpisy ES/EU (Poslanecká sněmovna PČR; Vláda ČR, 2011 str. 14). Trestní odpovědnost právnické osoby lze při splnění dalších znaků dovodit mj. i u trestného činu porušení tajemství dopravovaných zpráv (§ 7 TOPO a § 182 TZ), jak požaduje CoC v čl. 3 (protiprávní zachycení informací). I zde byla ovšem částečně překročena snaha kriminalizovat jednání právnické osoby jakožto pachatele, když se zákonodárce rozhodl zahrnout do věcné působnosti TOPO § 182 TZ jako celek, tedy vč. odst. 1 písm. a) TZ, který se vztahuje na porušení tajemství uzavřeného listu nebo jiné písemnosti při poskytování poštovní služby nebo přepravované jinou dopravní službou nebo dopravním zařízením.

Co se týče kriminalizace jednání souvisejícího s dětskou pornografií, k zavedení trestní odpovědnosti právnických osob zavazuje i Opční protokol k Úmluvě o právech dítěte o prodeji dětí, dětské prostituci a dětské pornografii [čl. 3 odst. 1 písm. c), odst. 4)], CoC (čl. 12), úmluva Rady Evropy o ochraně dětí před sexuálním zneužíváním a sexuálním vykořisťováním (čl. 26), směrnice Evropského parlamentu a Rady 2011/93/EU ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV (čl. 11). Dále požaduje trestní odpovědnost právnické osoby Dodatkový protokol (čl. 8 ve spojení s čl. 12 CoC). V podobném duchu se nese i Rámcové rozhodnutí Rady 2008/913/SVV ze dne

přidružených přístrojů, z nichž jeden nebo více provádí na základě programu automatické zpracování počítačových dat, jakož i data těmito přístroji uložená, zpracovaná, opětovně vyhledaná nebo přenesená za účelem jejich provozu, použití, ochrany a údržby“ [čl. 1 písm. a) tohoto rozhodnutí]. Protiprávnímu přístupu dle čl. 2 odpovídá § 230 odst. 1 a § 231 TZ, protiprávnímu zásahu do systému nebo dat v čl. 3 a 4 odpovídá § 230 odst. 2 písm. b), c) a d) TZ.

28. listopadu 2008 o boji proti některým formám a projevům rasismu a xenofobie prostřednictvím trestního práva (čl. 5). Požadavek kriminalizace jednání zakládajícího porušení autorských práv a práv k databázi prostřednictvím trestní odpovědnosti právnických osob není sice stanoven přímo, řada mezinárodních právních předpisů se však k porušování autorských práv vyjadřuje (Šámal, 2012 str. 2735).

6.2. Shrnutí k právnímu rámci kyberprostoru

Regulace samotného internetu, ale i jeho obsahu a protiprávního jednání v souvislosti s ním vychází z mezinárodního i národního práva. Základní národní legislativní rámec poskytuje Ústava a Listina, které jsou doplněny řadou zákonů, vč. ZoKB, zákona o elektronických komunikacích, o některých službách informační společnosti, o některých přestupcích aj. Za zmínku pak stojí evropské GDPR a příslušné doplňující zákony upravující ochranu osobních údajů.

Z hlediska mezinárodního boje proti kriminalitě online hrají pro ČR roli zejm. CoC (a Dodatkový protokol), Opční protokol k Úmluvě o právech dítěte týkajícího se prodeje dětí, dětské prostituce a dětské pornografie a Úmluva o ochraně dětí před sexuálním zneužíváním a sexuálním vykořisťováním. Dále pak legislativa EU, především směrnice Evropského parlamentu a Rady 2011/93/EU (o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii), 2004/48/ES (o dodržování práv duševního vlastnictví), 96/9/ES (o právní ochraně databází), 2001/29/ES (o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti), 2013/40/EU (o útocích na informační systémy).

Ty více či méně upravují formulaci počítačových aj. trestných činů relevantních z hlediska zneužívání kyberprostoru (vč. požadavku trestní odpovědnosti právnických osob): poškození a ohrožení provozu obecně prospěšného zařízení, porušení tajemství dopravovaných zpráv, porušení tajemství listin a jiných dokumentů uchovávaných v soukromí; dále skutkové podstaty zohledňující spáchání činu veřejně (vč. místa veřejnosti přístupném) nebo veřejně přístupnou počítačovou sítí jako zvlášť přitěžující okolnost (např. šíření pornografie); skutkové podstaty s objektivní stránkou zahrnující zveřejnění určitého obsahu nebo jeho učinění veřejně přístupným (vč. specifika „veřejnosti“ SNS, např. výroba a jiné nakládání s dětskou pornografií); za zmínku stojí i další skutkové podstaty jako podvod nebo porušení

autorského práva, práv souvisejících s právem autorským a práv k databázi. Významnou oblast představuje sexuální vykořisťování dětí online, od šíření pornografie přes výrobu a jiné nakládání s dětskou pornografií po účasti na pornografickém představení a navazování nedovolených kontaktů s dítětem.

7. BTC a typy kyberkriminality

Na pomezí mezi ochranou soukromí a protiprávním jednáním se pohybují virtuální měny, sloužící na jedné straně oprávněnému zájmu o zachování soukromí, na straně druhé pak legalizaci výnosů z trestné činnosti. Představují tak předěl mezi jednáním v souladu s právem a (kyber)kriminalitou, nastíněnou dále.

Virtuální měny[254] se zpravidla váží na internet, tou nejrozšířenější je bezesporu bitcoin.[255] BTC vznikly sice jako virtuální forma měny, v současnosti jsou však prakticky volně převoditelné na obvyklé měny (Fillner, 2014). Nepodléhají žádné centrální autoritě, decentralizaci může ohrozit pouze velká skupina tzv. těžařů nebo těžař s enormně výkonnou výpočetní silou (bitcoinwiki). Síla BTC se odvíjí od důvěry uživatelů a představuje vzhledem k velkým výkyvům kurzu značně spekulativní investici (bitcash.cz). Aktuální množství BTC v oběhu je vždy známé,[256] přičemž jejich počet zpomalujícím se tempem stále roste. Konečný počet všech uvolněných BTC do oběhu se předpokládá v roce 2140 (cca 21.000.000 BTC), s většinou v oběhu v roce 2030.

Uživatelé BTC se dělí na těžaře a koncové uživatele, přičemž kdokoliv může být jedním či druhým i oběma zároveň. Koncoví uživatelé převádějící BTC si mohou být jisti, že je nelze padělat a že jejich transakce bude ověřena prostřednictvím těžařů, jejichž role je v celém systému klíčová. V současnosti těžaři BTC tzv. dolují, tj. vytváří nové BTC. Znamená to, že věnují část výpočetní síly svého zařízení s připojením k internetu na ověřování všech nově proběhnuvších transakcí, za což je jim odměnou přidělení nově vzniklých BTC a transakčních poplatků. Každé těžící zařízení vypočítává řešení složitého matematického problému, přičemž lze ke správnému výsledku dojít různými způsoby a možných správných výsledků je více. K tomu se přidává náhodně přidělený vstupní údaj, který zajišťuje nahodilost co do rychlosti dosažení cíle, která se sice odvíjí z velké části od síly užité výpočetní techniky, nikoliv však absolutně.[257] Se správným řešením těžař vytvoří tzv. blok (nový blok vzniká každých cca 10 minut), který v sobě nese informaci o všech předchozích blocích, na které navazuje, informaci

[254] Text věnující se BTC vychází z (Kudrlová, 2015), čerpáno je mj. z (Wikipedie).
[255] Blíže k právní regulaci tzv. kryptoměn viz např. (Němec, a další, 2018) a (Němec, a další, 2018).
[256] Např. 16.4.2015 v 11:30 hod to bylo 352.349 BTC, 14.1.2019 ve 22:17 to bylo 558.552 BTC (blockexplorer.com). Jde ovšem o „vytěžené" BTC, z nichž malá část je ztracena: absolutně např. zničením disku, na němž byly uloženy, nebo relativně při ztrátě soukromého klíče (s BTC pak nelze nakládat) či zasláním na neexistující adresu.
[257] Tzn. např. těžař s běžným těžícím zařízením (např. stolním počítačem) má šanci dospět jako první ke správnému výsledku cca za 5 let, zatímco jiný těžař se silnější technikou např. cca za měsíc, nicméně přesto to neznamená, že pro prvního těžaře by získání BTC těžbou bylo nemožné, což zajišťuje motivaci i pro drobné těžaře.

o všech transakcích provedených od vzniku předchozího bloku a náhodně vygenerovanou adresu těžaře, který blok vytváří, na kterou má přijít odměna - BTC a transakční poplatky z ověřených transakcí (bitcoinwiki). Pokud dospěje ke správnému řešení více těžařů současně, síť těžících zařízení náhodně určí, čí blok bude přidán do jednotného řetězce, tzv. blockchainu (bitcoinwiki), který lze vysledovat až k prvnímu bloku vůbec. Bloky nelze žádným způsobem měnit či kopírovat, neboť informace o nich je předávána v podobě tzv. hashe, tj. algoritmu převádějícího jakékoliv množství údajů do podoby mnohamístného čísla, přičemž jakákoliv změna vstupních dat toto číslo zásadně mění a zároveň nelze na jeho základě odvodit původní vstupní data, takže spočítání hashe je matematicky značně náročné, zatímco jeho ověření extrémně rychlé a snadné (bitcoinwiki). Takto je celý řetězec (a transakce v něm zachycené) vždy znovu ověřen s tvorbou každého dalšího bloku. Protože za jediný správný řetězec se považuje vždy ten s nejvyšší náročností řešení, není možné jej padělat či zpětně upravovat ani duplikovat.

Samotné transakce pak probíhají prostřednictvím adres, na nichž jsou BTC uloženy. Ty se generují uživateli zcela náhodně, přičemž ke každé patří soukromý a veřejný klíč. Uživatel zašle požadované množství BTC ze své adresy za použití soukromého klíče na cílovou adresu v podobě hashe veřejného klíče (a tato transakce je záhy ověřena těžaři v podobě jejího zařazení do nového bloku). Protože BTC lze odeslat z jedné adresy vždy jen všechny najednou (případně na různá místa zároveň), při požadavku na odeslání pouze části BTC z dané adresy odejdou z této všechny tam dostupné BTC a zároveň se odesílateli vygeneruje nová adresa, kam se mu zbývající BTC vrátí (resp. kam směřují jako do další cílové adresy). Mj. z toho důvodu se při nakládání s BTC využívají tzv. klienti, tj. software sloužící ke správě dolování a sdružující veškeré adresy uživatele do jednotného místa.[258] Protože adresy jsou generovány zcela náhodně a každá transakce s sebou nese pouze informaci o cílové adrese, používání BTC je z velké části anonymní, nikoliv však absolutně. Pokud se podaří spárovat adresu s konkrétní osobou (např. ji uživatel uvede na veřejně přístupném fóru jako adresu pro možné zasílání příspěvků), lze od této adresy sledovat následné transakce, které jsou všechny zahrnuty v ověřeném řetězci, a stejně tak adresy, z nichž proběhly transakce na známou adresu (Reid, a další, 2013). Může se také podařit vysledovat konkrétní platbu: např. vím, že osoba A uhradila v určitém krátkém časovém rozmezí 123 BTC a v rámci ověřeného řetězce naleznu pouze jednu jedinou transakci v této výši, je tudíž zřejmé, že odesílatelem je ona

[258] Tzn. uživatel např. ví, že vlastní 357 BTC, aniž by se zabýval tím, že oněch 357 BTC je rozloženo do 16 adres, nicméně má současně možnost mít přehled o tom, kolik BTC má na jaké adrese, a ovládat je samostatně.

osoba A (Ludwin, 2015). Lze se proto setkat s řadou tipů na zvýšení anonymity. Základním doporučením je použít každou adresu pouze jednou a eliminovat tak riziko „kompromitovaných“ adres.[259] Dalším způsobem je používání tzv. ePeněženek, kdy uživatelé posílají své BTC na sdílené adresy e-Peněženky, ze kterých pak probíhají požadované platby (transakce ověřované těžaři). V rámci anonymizace se doporučuje zaslat BTC z ohrožených či již kompromitovaných adres do ePeněženky, následně je přeposlat do jiné e-Peněženky a poté zpět sobě. Takto sice jejich původ není zcela zastřen, nicméně je značně ztíženo jeho rozkrytí vzhledem k množství transakcí prováděných prostřednictvím e-Peněženek (bitcoinwiki). Dalším vylepšením je pak uchovávání těchto anonymizovaných BTC na jiné adrese tak, aby se případně nesmíchaly a tudíž nedeanonymizovaly s jinými BTC.

Největší slabina BTC z hlediska kyberkriminality a jejího dokazování spočívá nepochybně ve značné anonymitě, resp. komplikovanosti dohledávání majitelů BTC a rozkrývání jejich přesunů. Vzhledem k tomu se předpokládá značné využívání BTC jakožto měny téměř ideální pro platby spojené s nelegálními činnostmi, ať už se jedná o zbraně, drogy, obchodování s lidmi, dětskou pornografií atp., podobně jako jejich zřejmě hojné využívání při praní špinavých peněz prostřednictvím směny za reálnou měnu a naopak. Organizovaný zločin i instituce na samé hranici legality mohou využívat BTC jako „dary“ ze strany třetích osob, aniž by tyto byly dohledatelné.[260] Vzhledem k výpočetní náročnosti získávání nových BTC se lze setkat s botnetem, jehož nedobrovolní členové na pozadí běžných činností nevědomky soustavně dolují BTC. Krádež BTC či jejich padělání jsou nanejvýš nepravděpodobné, nicméně objevují se (někdy i úspěšné) pokusy neoprávněně vstoupit do zařízení majitele a např. získat jeho soukromý klíč, a tudíž i přístup k BTC umístěným v dané schránce. V posledních letech pak jsou BTC značně oblíbeny pro platby v rámci ransomwaru.

Kyberkriminalita má určitá specifika vyplývající z imanentních vlastností kyberprostoru, z nichž některá dosud nezazněla.[261] Předně je to předpokládaná vysoká latence, viz např. (Gřivna, 2015 str. 337). Poškozený mnohdy vůbec neví o probíhajícím útoku (např. při

[259] Samotná veřejnost hashe veřejného klíče anonymitu neohrožuje, neboť adresa je generována zcela náhodně, je v rámci sítě neznámá až do provedení první transakce a soukromý klíč k ní drží pouze její uživatel (uložený ve svém zařízení).

[260] Nedávný výzkum provedený v Nizozemí naznačuje, že organizovaný zločin navzdory očekávání preferuje oproti BTC hotovost, prezentace výsledků zazněla na konferencích Eurocrim 2018 v srpnu 2018 v Sarajevu a opakovaně na Human Factor in Cybercrime v říjnu 2018 v Jeruzalémě (Leukfeldt, a další, 2018). Lze však namítnout, že výzkum zachycuje převážně „známý“ organizovaný zločin, zatímco jeho velká část zůstává skryta, možná právě díky většímu využívání BTC.

[261] Odstavec vychází z kapitoly Kyberkriminalita zpracované ve spoluautorství autorky a T. Gřivny a publikované v učebnici Kriminologie (Gřivna, 2015 stránky 334-353).

odposlechu), nebo neví, že jednání je trestné (např. neoprávněný přístup do SNS po překonání hesla k cizímu profilu). Jindy poškozený nechce oznámit orgánům činným v trestním řízení napadení svých zařízení (např. z obavy ztráty důvěryhodnosti e-shopu či služby elektronického bankovnictví). V mnoha případech není podání trestního oznámení ani žádoucí, s ohledem na množství soustavných útoků, které lze v drtivé většině případů vyřešit vlastními silami (např. antivirem). K vysoké latenci přispívá též bezprostřední neviditelnost způsobených následků (oproti např. vloupání) a někdy i zpochybňovaná společenská škodlivost (např. při porušování práv duševního vlastnictví). Útok s minimem nákladů (finančních i znalostních) může způsobit rozsáhlé škody[262] a proběhnout jednorázově nebo dlouhodobě.[263] V české literatuře se lze setkat např. ještě se zmínkami o legislativě jen pomalu reagující na rychlý technologický vývoj, nedostatek právních, režimových a organizačních prostředků pro boj s kyberkriminalitou, podceňování zabezpečení ze strany uživatelů, složitost ICT a přehnanou důvěru v ně nebo enormní objem nekontrolovatelných dat.[264] Některé typy útoků vyžadují hlubší znalosti ICT (např. malware), naopak tzv. tradiční kriminalita v novém kabátě obvykle zvláštní schopnosti nevyžaduje. Lze proto dělit pachatele na amatéry a profesionály (Madliak, a další, 2008 str. 54), přičemž někdy se vyděluje ještě zvláštní skupina – teroristé (Látal, 1998 str. IX). Specifickým útočníkem je pak osoba usilující o neoprávněný přístup do počítačového systému, obvykle označovaná jako hacker nebo cracker (hacker usiluje o testování vlastních schopností, pocit všemocnosti, nalezení bezpečnostních chyb atp., cracker naopak o vlastní obohacení) s řadou podskupin (white, black a grey hats, rodents aj.).

Lze se setkat s řadou definic kyberkriminality, od využití ICT[265] (s níž se lze se zdůrazněním ICT prvku v zásadě ztotožnit) po páchání trestné činnosti, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení vč. dat, nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět této trestné činnosti nebo jako nástroj trestné činnosti (Smejkal, 2018 str. 25). Počátky kriminalizace kyberkriminality v českém prostředí lze spatřovat ve skutkové podstatě trestného činu poškození a zneužití záznamu na nosiči informací

[262] Např. napadení twitterového účtu tiskové agentury podsunutím falešné zprávy o napadení Bílého domu ovlivnivší zřejmě vývoj na americkém akciovém trhu (ČTK, 2013)
[263] Např. jako součást rozsáhlejšího jednání v podobě informační války, viz např. (Čížek, 2013), (Gřivna, a další, 2008 str. 50).
[264] Viz např. (Jirovský, 2007 str. 19), (Matějka, 2002 str. 8), (Madliak, a další, 2008 str. 47), (Válková, a další, 2012 str. 606).
[265] Sdělení Evropské komise COM(2000) 890.

(§ 257a sTZ).[266] Ta byla v rozšířené podobě přejata do nového trestního zákoníku jako skutková podstata dle § 230 TZ, kdy kromě ochrany informací obsažených na nosiči informací a technického nebo programového vybavení telekomunikačního zařízení proti jednání v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch nově kriminalizuje i samotný neoprávněný přístup k počítačovému systému nebo jeho části vůbec, konkretizuje ochranu dat v rámci počítačového systému a stanoví několikero zvlášť přitěžujících okolnosti (Kudrlová, a další, 2017).

Kyberkriminalita samotná se nejčastěji člení podle CoC.[267] Do první skupiny spadají trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů: nigerijské dopisy, phishing, pharming, malware, DNS útoky, hacking (vč. tzv. hacktivismu), útoky na elektronické bankovnictví, DDoS, APT[268] aj. Druhou skupinu tvoří trestné činy související s počítači: falšování údajů a podvod. Třetí skupina zahrnuje trestné činy související s obsahem: dětskou pornografií (vč. virtuální). Čtvrtá skupina sestává z trestných činů souvisejících s porušením autorského práva a práv příbuzných autorskému právu. Dodatkový protokol pak hovoří o trestných činech ve spojení s rasistickým a xenofobním obsahem (Kyberkriminalita dnes, 2014).

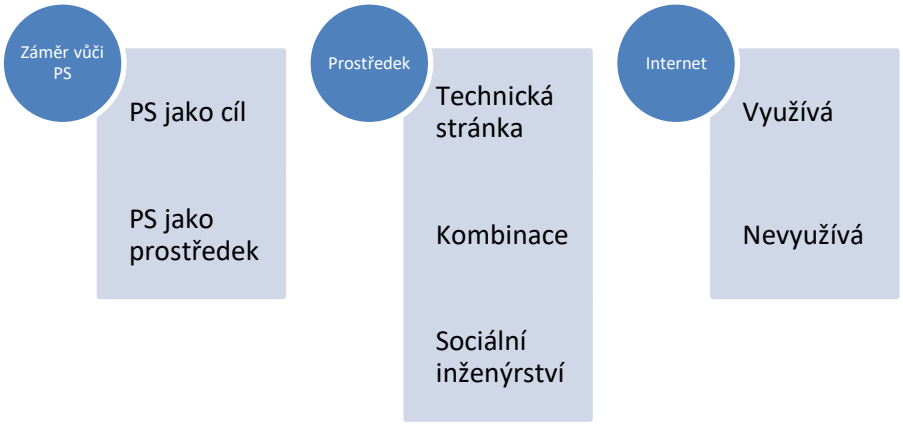
Jiné časté členění rozlišuje trestnou činnost závislou nebo pouze usnadněnou využitím ICT. Závislá činnost (cyber-dependent) může být prováděna pouze s použitím počítačů, počítačových sítí nebo jiných forem ICT: malware, hacking, DDoS aj. Naproti tomu trestná činnost usnadněná využitím ICT je prováděna online nebo offline, a „je-li prováděna online, může být uskutečňována v mimořádném měřítku a rychlostí“ (Costs of Cyber Crime Working Group, 2018 str. 11).

Členění podle CoC ovšem nedopadá na veškeré relevantní jevy (např. kybergrooming), jednak proto, že se záměrně vztahuje pouze k těm nejpalčivějším, jednak proto, že je pevně zakotvena v určitém časovém rámci, zatímco technologický a uživatelský vývoj kyberprostoru spěje nezadržitelně dále. Naproti tomu dělení na trestnou činnost závislou nebo

[266] Zavedeno zákonem č. 557/1991 Sb. s účinností od 1.1.1992, novelizováno zákonem č. 134/2002 Sb. s účinností od 1.7.2002.
[267] CoC uvádí též definice některých pojmů jako „počítačový systém“, „počítačová data“ aj.
[268] Advanced Persistent Threat - sofistikovaný a často dlouhodobý útok kombinující sociální inženýrství i technologické znalosti. APT útok mnohdy cílí na síť jako takovou, a tudíž na obecně prospěšné zařízení. Útoky výše uvedené jsou mnohdy páchány prostřednictvím organizované skupiny, případně organizované zločinecké skupiny (§ 129 TZ). Nejprve shromáždí informace k proniknutí do sítě (technické, organizační, osobní aj.), následuje samotný průnik a sběr dat (Marinos, 2016 str. 64), (Security-Portal, 2013), (Imperva, 2017).

usnadněnou ICT sice zahrnuje prakticky neomezenou škálu jevů, nicméně (právě proto) je naopak příliš obecné. Dovoluji si proto nabídnout vlastní rozdělení.[269]

Obr. č. 1: základní členění kyberkriminality



Kyberkriminalitu lze charakterizovat jako kriminalitu související s PS, které představují spojení hardwaru (fyzické zařízení) a softwaru (program zařízení) provádějící automatické zpracování dat (Šámal, 2012 str. 2306). Tradičně byl takovým PS typicky počítač, dnes zahrnuje i jiná zařízení. Dříve používaný termín „počítačová kriminalita“ již proto není tak přiléhavý zejm. s ohledem na rozmanitost IoT. V nejobecnější rovině lze rozdělit kyberkriminalitu v závislosti na záměru pachatele, který využívá PS buď jako cíl (např. pokus o průnik do systému za účelem jeho poškození), anebo jako prostředek útoku (např. neoprávněný přístup do elektronického bankovnictví za účelem odčerpání peněz z účtu poškozeného). Další dělení se odvíjí od míry využití technické stránky přenosu a automatického zpracovávání dat. Na jedné straně stojí útoky převážně technického typu [např. DDoS], i ty ovšem obvykle vyžadují alespoň minimální sociální inženýrství, zejm. co do odhadu chování uživatelů za účelem usnadnění útoku (např. skrytí malwaru do zdarma distribuované počítačové hry). Druhou stranu zaujímají jednání využívající zpravidla internet jakožto svébytnou komunikační platformu bez hlubšího zohlednění technické stránky (např. podvodné předstírání virtuálního vztahu za účelem vylákání peněž). Kombinované útoky využívají obě stránky (např. phishing). Většina kyberkriminality je spojena s internetem, jehož prostřednictvím cílí na PS a/nebo jejich uživatele. Může ovšem směřovat i vůči uzavřeným lokálním sítím (např. SCADA).

[269] Vychází z několika dříve publikovaných prací autorky, především ze studentské vědecké odborné činnosti (Kudrlová, 2016), ve stručnější podobě (Kudrlová, 2016), a z příslušné kapitoly učebnice Kriminologie (Gřivna, 2015).

Obr. č. 2: jednotlivé formy kyberkriminality

Obr. č. 3: zásah do systému

Zásah do systému zahrnuje pestrou paletu jednání, mnohdy slouží jen jako prostředek k naplnění jiného záměru pachatele (např. ransomware). Spadá sem hacking: neoprávněný přístup do systému zpravidla využitím bezpečnostní chyby/mezery v systému nebo aplikací určitého softwaru, ať už vzdáleným přístupem nebo bezprostředně fyzicky. Dále tzv. viry, červi a trojští koně, jejichž společným jmenovatelem je malware zpravidla s cílem poškodit, ovládnout či odposlouchávat systém. K instalaci obvykle dochází po neoprávněném přístupu do systému nebo vlastní aktivitou nepozorného uživatele.[270] Z časového hlediska může malware vykazovat aktivitu ihned nebo i po určité době, k určitému datu, jednorázově i dlouhodobě atp. DDoS usiluje zpravidla o znepřístupnění napadeného serveru či služby. Spočívá obvykle v koordinovaném jednání množství zařízení, která se v krátkém časovém úseku dožadují aktivity napadeného serveru, přičemž hrozí jeho zahlcení a v důsledku toho znepřístupnění.[271] DDoS vyžaduje řadu zařízení postupujících koordinovaně – tzv. botnet, tj. síť podřízených zařízení. Mnohdy se jedná o zařízení napadená dříve malwarem, který zajistí jejich alespoň částečné ovládnutí útočníky.[272] Při DNS spoofingu napadený překladač pošle dožadující se zařízení na jinou adresu, často velmi podobnou (např. falešná stránka elektronického bankovnictví sloužící ke sběru přihlašovacích údajů).[273] Naproti tomu při IP spoofingu pachatel zamění svou IP adresu tak, aby jejím prostřednictvím získal (neoprávněně) přístup k jinak nedostupnému systému nebo službě (např. určené jen pro zaměstnance). Odposlech probíhá v různých podobách, od zvukového (mikrofon) přes vizuální (zaměřený dovnitř i ven – klonování monitoru i ovládnutí webové kamery) po tzv. keylogger (odposlech úhozů do klávesnice).[274] XSS označuje neoprávněné vpisování vlastního kódu do cizích webových stránek (např. vložení odkazu). Šifrování dat zajišťuje na jedné straně ochranu soukromí, na straně druhé dává nástroj sloužící k vydírání uživatele, jehož data byla nevyžádaně zašifrována – tzv. ransomware (spojený s požadavkem platby nejčastěji v BTC

[270] Viry i červi (na rozdíl od trojského koně) se šíří rozesíláním kopií sebe sama, přičemž červ tak činí samostatně, zatímco virus pouze ve spojení s jiným souborem.

[271] Server může být zahlcen využitím veškeré své kapacity k odpovědím, a tak nezbývá žádný prostor pro odpověď jakémukoliv dalšímu uživateli. Jindy může být DDoS útok „zachycen" již ochranným softwarem, a tak se botnet k zahlcení serveru samotného nedostane, nicméně onen ochranný software zpravidla nedokáže odlišit požadavek oprávněného uživatele (tj. zařízení dožadujícího se aktivity bez souvislosti s probíhajícím útokem), kterému přístup odepře taktéž – server je tak fakticky znepřístupněn, aniž by došlo k vlastnímu kontaktu mezi ním a botnetem.

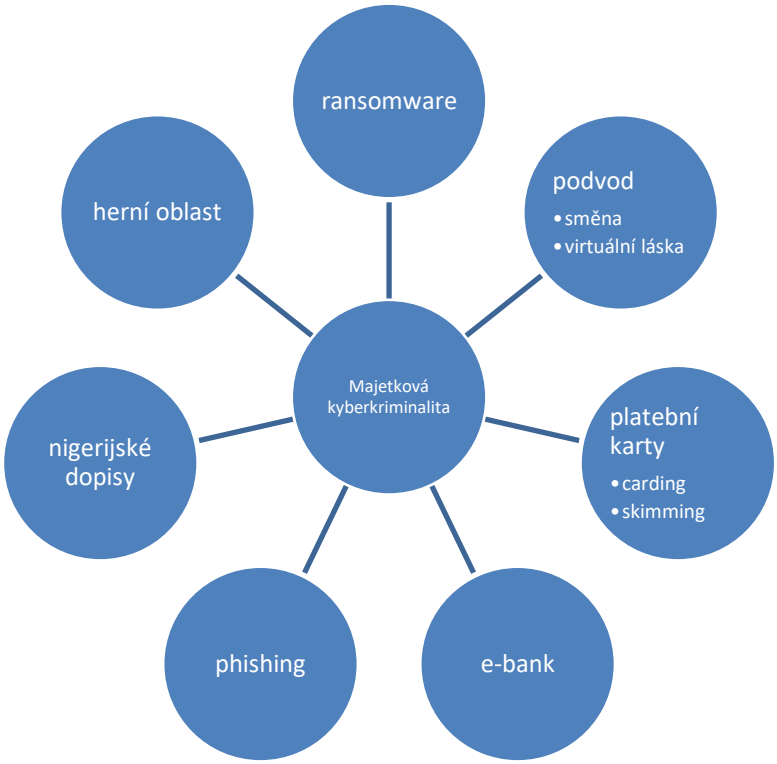
[272] U DDoS lze někdy zpochybnit protiprávnost jednání (např. „pouze" zasílání požadavků na zobrazení stránky vlada.cz), zřízení botnetu však obvykle předchází neoprávněný přístup k počítačovému systému a nosiči informací v podobě neoprávněného vložení dat (ovládací malware) do napadených zařízení, která botnet vytvoří [§ 230 odst. 1 a/nebo 2 písm. d) TZ].

[273] Alternativou je tzv. pharming, kdy je obdobně napadeno koncové zařízení uživatele nebo zařízení „na cestě" mezi koncovým zařízením uživatele, DNS serverem a serverem s požadovaným obsahem.

[274] Samotné využití odposlechu ovšem nemusí být protiprávní (např. sledování činnosti zaměstnanců na pracovních zařízeních po předchozím upozornění).

výměnou za odšifrování). Nakonec je zde ještě široká zbytková oblast neoprávněné úpravy dat, ke které dochází často po neoprávněném přístupu do systému (ten může být cílem i sám o sobě). Jedná se o smazání dat, jejich úpravu, potlačení (data samotná zůstávají sice neporušena, neplní však nadále svou funkci), falšování atp. Může jít o jakákoliv data, tedy např. i obsah profilu na SNS.

Obr. č. 4: majetková kriminalita



K ransomwaru viz výše. Podvody se v prostředí internetu vyskytují převážně ve dvou podobách: v různých formách směny (např. fiktivní e-shop nebo jiné než zaplacené zboží atp.) a předstíráním virtuální lásky (za účelem vylákání peněz). Zneužívání platebních karet online bez potřeby fyzického nosiče se nazývá carding, skimming označuje výrobu kopie platební karty ve spojení s jejími autentizačními údaji (typicky kombinace skimmovacího zařízení kopírujícího magnetický proužek karty a kamery nebo klávesnice snímající zadávaný PIN). Řada útoků míří na ovládnutí cizího elektronického bankovnictví: DNS spoofing, pharming, ale také tzv. phishing. Ten označuje email pocházející zdánlivě z důvěryhodného zdroje (např. bankovní instituce) a vyzývající zpravidla k určité aktivitě: zaslání osobních údajů, zadání přihlašovacích údajů na odkazované stránce, instalace přiložené aplikace do mobilního

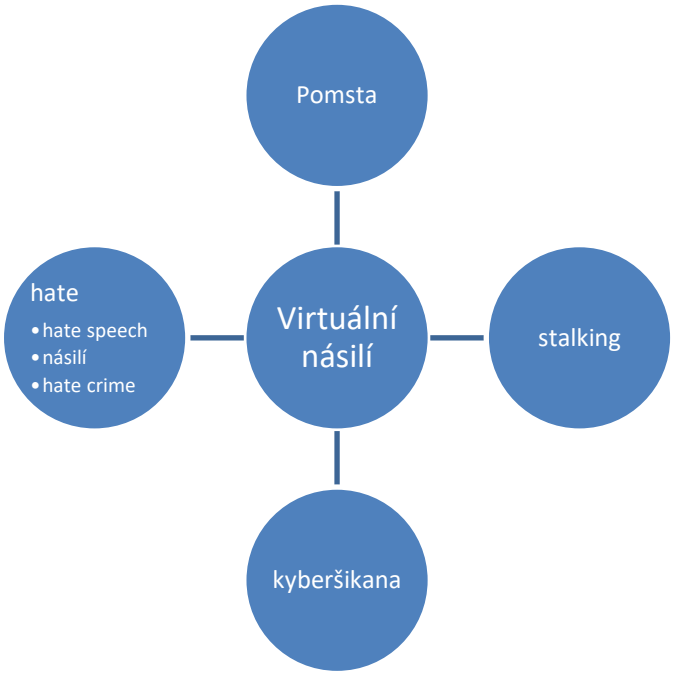
telefonu atp.[275] Phishingu se podobají nigerijské dopisy (scam419), obvykle s cílem přimět uživatele ke sdělení osobních údajů a/nebo zaplacení určité částky (typicky nabídka účasti v dědickém řízení nebo možnost převzetí výhry v obou případech po zaplacení administrativního poplatku). Nakonec je to herní oblast, která se týká především neoprávněného přístupu k herním účtům, ze kterých pachatelé vyčtou řadu osobních údajů (vč. údajů o platebních kartách), zakoupí na účet poškozeného herní čas (ve prospěch vlastního herního účtu) či přímo hru, zcizí herní „majetek" spojený s napadeným účtem atp.

Obr. č. 5: krádež identity

Jako krádež identity (nikoliv „krádež" v trestněprávním smyslu) bývá označováno jednání, kdy se pachatel díky množství získaných osobních údajů vydává za poškozeného. V kyberprostoru je výrazně snazší než v reálném prostředí: jednak lze na SNS a jinde nalézt množství osobních údajů, jednak je náročnější falešnou identitu odhalit (např. převzetí cizího profilu na SNS a oslovení navázaných kontaktů se žádostí o půjčku). Motivací bývá majetkové obohacení pachatele (např. získání zboží nebo úvěru jménem a na účet poškozeného), dále pak i virtuální násilí, kdy pachatel jedná coby poškozený s cílem poškodit jeho pověst a dobré jméno, znepřátelit okolí, difamovat veřejně činnou osobu atp. (např. zveřejňování odsouzeníhodných komentářů na SNS jménem poškozeného).

[275] K jiným úspěšnějším phishingům patří např. emaily z e-shopu vyzývající k zaplacení dlužné částky pod hrozbou exekuce nebo emaily „od Policie ČR" vyzývající k úhradě pokuty za sledování ilegální pornografie pod hrozbou zahájení trestního stíhání.

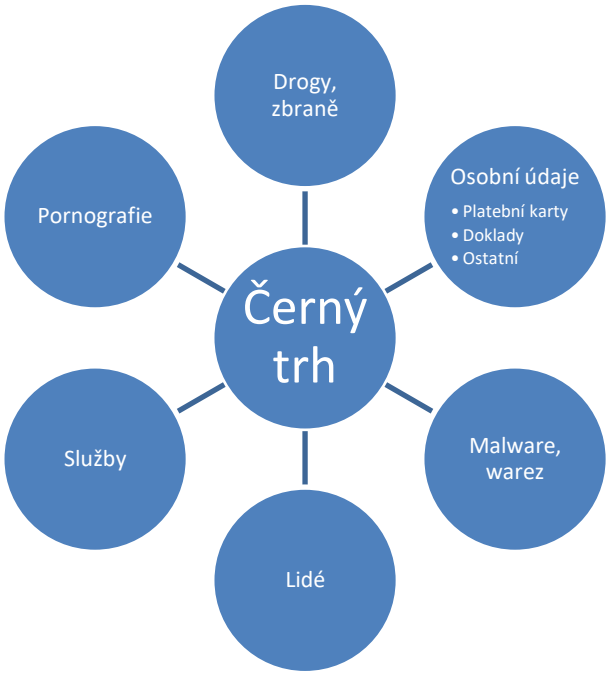
Obr. č. 6: virtuální násilí



Virtuální násilí se může zdát jako protimluv, leč s ohledem na množství přihlížejících v online prostředí má potenciál značného dopadu na psychiku oběti. I bez krádeže identity pachatel např. šíří o oběti pomluvy, zveřejňuje ponižující fotografie a videa (často zaznamenané v rozporu s ochranou osobnosti nebo montáže) atp. Mnohdy se jedná o intimní obsah zveřejněný zhrzeným ex-partnerem, který neunese rozpad vztahu (typicky sexting). Stalking narušuje soukromí oběti každodenním množství zpráv a telefonátů, doplněných o emaily a zprávy na SNS (v závislosti na sdílnosti oběti na SNS může mít stalker dobrý přehled o jejích sociálních kontaktech i aktivitách v rámci času i prostoru). Někdy pak stalker doplňuje obtěžování umístěním osobních údajů (zejm. telefonního čísla) na seznamkách, u inzerátů s prodejem zboží za extrémně nízkou cenu atp., čímž zajišťuje další nevyžádané kontakty. Zvlášť traumatizujícím jednáním je kyberšikana, která na rozdíl od tradiční šikany v reálném prostředí není prostorově ani časově omezená a často probíhá na SNS (např. založení FB skupiny „Jana smrdí“). Její součástí bývá i tzv. hate speech - nenávistná mluva s různorodými projevy: komentáře na SNS, blogy, diskuse, ale i celé weby aj. Nemusí vždy naplňovat znaky pomluvy nebo některého z trestných činů z nenávisti, naopak ve většině případů jde „jen“ o zásah do osobnosti a práva na soukromí, důstojnost a čest. Jiná podoba virtuálního násilí spočívá v zobrazování násilného obsahu (násilí vůči lidem, zvířatům i věcem). Ve spojení s počítačovými hrami pracujícími s násilným obsahem se pak někdy hovoří o obavě z násilí

jakožto ukotvující se normy pro řešení konfliktních situací. V závažnějších případech hate speech a zobrazování či vyzývání k násilí už může jít o hate crime, trestný čin z nenávisti.

Obr. č. 7: černý trh

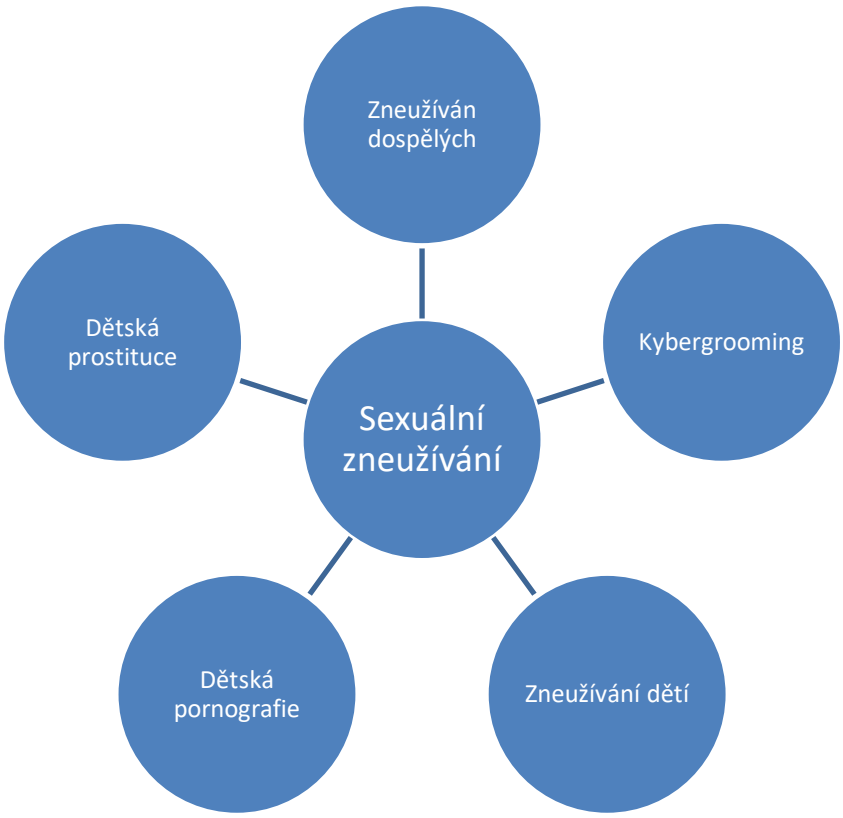


Oblast černého trhu lze nalézt v kyberprostoru převážně v darkwebu (viz kapitola **Shrnutí k technické stránce kyberprostoru**). Jedná se o šifrovaný obsah (s koncovkou .onion) dostupný pouze prostřednictvím prohlížečů Tor, které do značné míry anonymizují své uživatele a jejich pohyb po síti. Tor na jedné straně chrání uživatele při návštěvě stránek v dané zemi zakázaných např. z politických důvodů, ale zároveň anonymizuje uživatele při různorodých protiprávních aktivitách. Jako rozcestník při vyhledávání obsahu dark webu slouží nejčastěji The Hidden Wiki (Hidden Wiki), nabízející seznam některých adres dle kategorií, vč. drog aj. (např. web Islámského státu). Platby v darknetu probíhají zpravidla prostřednictvím transferu BTC. Darkweb pravděpodobně slouží jako komunikační platforma, zdroj pro získání nelegálního zboží, prostředků útoku, uplatnění neoprávněně nabytých hodnot i legalizaci výnosů z trestné činnosti v souvislosti více či méně se všemi typy kyberkriminality. Co se týče drog, darknet nabízí hned několik míst k jejich pořízení, z nichž nejznámější je Silk Road a její variace.[276] Stejně jako u většiny komodit probíhá platba s využitím tzv. escrow (forma úschovy). K obchodovaným osobním údajům patří jména,

[276]De facto e-shop/tržiště pro nepřeberné množství nelegálního zboží a služeb. Silk road byla zrušena FBI v roce 2013, posléze znovu vznikla a o rok později byla opět zrušena coby Silk Road 2.0. V současnosti by měly být v provozu Silk Road 3.0 a/nebo Silk Road Reloaded.

adresy, rodná a telefonní čísla, přihlašovací údaje, čísla účtů a samozřejmě platebních karet (vč. CVV, cena se pohybuje v závislosti n typu karty, národnosti držitele aj.). Vedle tradičního nelegálního zboží ve fyzické podobě jako jsou drogy a zbraně se pak obchoduje např. s doklady totožnosti, zejm. pasy (ceny se odvíjí především od země vydání). Další oblastí je obchodování s malwarem a warezem (autorská díla v rozporu s autorskoprávní ochranou, vč. softwaru). Lze si vybrat z předem vytvořených programů, požádat o vývoj malwaru pro konkrétní cíl nebo třeba využít kapacitu prozatím spícího botnetu. Obdobně lze např. objednat prolomení ochrany autorsky chráněného díla (např. softwaru v hodnotě desítek tisíc korun).[277] Závažnější obsah pak nabízí weby zaměřené na obchodování s lidmi (děti i dospělé).[278] Mezi nabízenými službami se nachází hacking, ale i nabídky odstranění nežádoucích osob („Hitman service“). Cena se odvíjí od významu oběti aj. okolností (např. způsob odstranění), „klient“ však podstupuje riziko vydírání namísto požadované služby. Specifickou oblast tvoří pornografie, dětská („Hard Candy“) a tvrdá.[279]

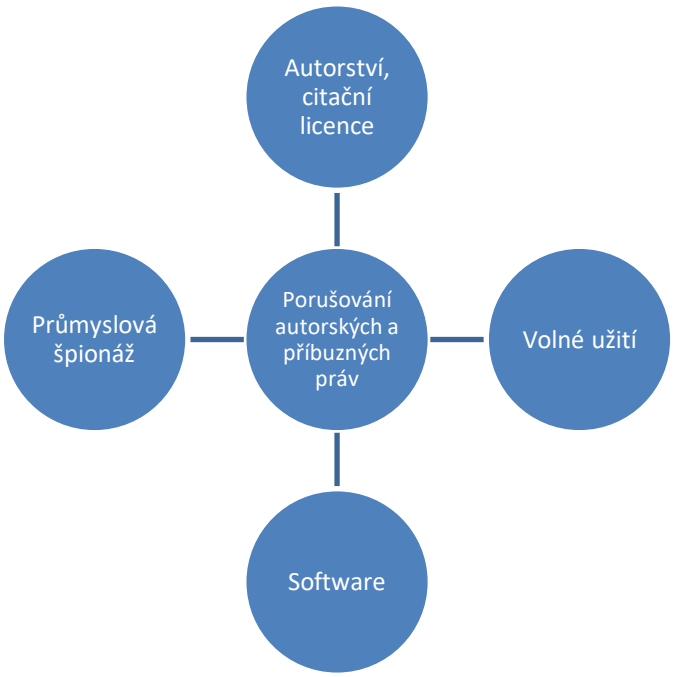
Obr. č. 8: sexuální zneužívání



[277] Warez se ovšem zdaleka neomezuje na dark web.
[278] Agentura DARPA proto vyvíjí speciální vyhledávač Memex schopný procházet deep web i část dark webu za účelem odhalování obchodování s lidmi a nalézání obětí (Shen).
[279] Samotný přístup k nelegální pornografii obvykle vyžaduje z pohledu dané komunity určité „bezpečnostní“ pojistky zpravidla v podobě poskytnutí vlastní, dosud nezveřejněné dětské či tvrdé pornografie.

Sexuální zneužívání dospělých omezené na prostředí internetu není příliš časté. Předstírání virtuální náklonnosti mívá za cíl majetkové obohacení, ale i sexuální uspokojení. Bez uvádění dotyčné/ho v omyl (např. předstírání citové vazby) lze těžko uvažovat u dospělých osob o jakémkoliv zneužití. Specifickou podobu uvádění v omyl a využití omylu (dlouhodobě udržovaného) představuje kybergrooming (psychická manipulace oběti prostřednictvím ICT s cílem jejího sexuálního zneužití) a spojené jednání, typicky sexting. Zneužívání dětí zahrnuje kromě kybergroomingu dětskou pornografii a dobrovolnou dětskou prostituci, dále nevyžádané kontaktování dětí s nabídkou a poptávkou sexuálních aktivit (typicky v chatovacích místnostech určených dětem, ale i v MMO hrách a jinde). Dětská pornografie se objevuje především v darkwebu, ale i v deep webu – k jejímu získávání slouží i zdánlivě nevinné ankety, soutěže, nabídky castingu atp. (může být na pomezí pornografického charakteru). (Dobrovolná) dětská prostituce souvisí ponejvíce s výrobou dětské pornografie, ať už s vědomím zobrazeného dítěte či bez něj, zahrnuje i pornografické představení (např. striptýz před webkamerou). K jednání dochází obvykle za úplatu nebo s domněnkou vzájemné výměny.

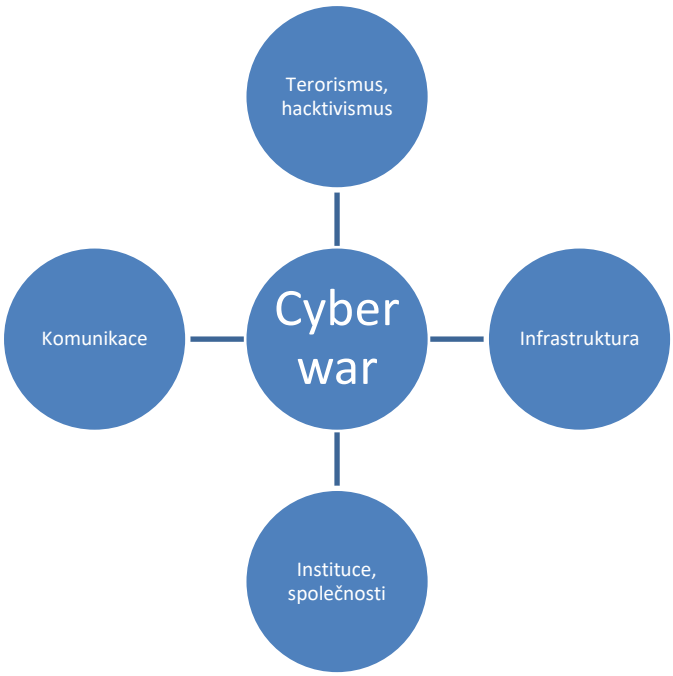
Obr. č. 9: porušování autorských a příbuzných práv



K porušování autorských práv (ať už v rovině trestněprávní, přestupkové nebo „jen“ občanskoprávní) dochází jak v darkwebu, tak deep webu a surface webu. Vzhledem ke snadné dostupnosti autorských děl v online prostředí se autoři potýkají především s plagiátorstvím (zejm. kopírování obsahu bez náležité citace zdroje) a nedodržováním podmínek licence –

typicky překročením podmínek tzv. volného užití. To se děje typicky tzv. sdělováním veřejnosti – např. zpřístupněním díla veřejnosti prostřednictvím jeho volně dostupného umístění na některém z běžně využívaných datových úložišť, případně odkazem na umístění díla nebo zpřístupněním v rámci P2P sítě. Předcházet může (protiprávní) odstranění ochrany proti kopírování. Protože softwaru se volné užití netýká, nelze jej bez příslušné licence využívat ani pro osobní potřebu fyzické osoby. K protiprávním jednáním proto dochází v souvislosti s odstraňováním ochrany proti kopírování, kopírováním, šířením, ale též vlastními úpravami, nejde-li o freeware (volně dostupný software) nebo open source software (software s otevřeným zdrojovým kódem). Průmyslová špionáž se v online prostředí přímo nabízí, vzhledem k výraznému propojení podnikatelské činnosti s kyberprostorem. Na jedné straně tak lze získat po neoprávněném vstupu např. do uzavřené firemní sítě obchodní kontakty, údaje o zakázkách atp. Na straně druhé pak využít např. hromadně rozesílaný spyware cílící na konkrétní typ souborů v napadených zařízeních a tyto odesílat pachateli.[280]

Obr. č. 10: cyber war



Zvyšující se závislost států na kyberprostoru znamená i s tím spojenou zranitelnost. Při posuzování hrozby se sleduje především zdroj útoku, jeho následek, motivace a sofistikovanost. V některých případech jde o akt státu či několika států jednajících

[280] Např. spyware vyhledávající soubory s příponou „.dwg“ využívané programy na projektování (architektura, stavitelství, ale též strojírenství aj.).

koordinovaně,[281] provést úspěšný útok ovšem může i hrstka IT specialistů (lze pak hovořit o kyberterorismu). Pro některé útoky je přiléhavější označení hacktivismus – hacking usilující o politickou či sociální změnu (např. pomocí XSS zobrazení textu hacktivistů namísto původního obsahu vládního webu). Nejzávažnější útoky mají za cíl ochromení státu (či dílčích oblastí) a/nebo přístup k jinak nedostupným informacím. Patří k nim především útoky na telekomunikační služby, rejstříky veřejné správy, řízení dopravy, energetiku, zdravotnictví, obranné systémy. Část útoků cílí na konkrétní instituce či společnosti, případně sektor: bankovní, pojišťovny aj. Daný sektor nemusí být přímo ochromen, aby již došlo k destabilizaci státu a obyvatelstva. Dalším terčem bývají např. společnosti spolupracující na armádních zakázkách (např. dlouhodobý spyware). Specifickou oblastí útoků jsou různé formy komunikace[282] a získávání utajovaných informací (a další nakládání s nimi). V případě komunikace jde především o odposlechy telefonních hovorů a emailové komunikace (není-li dostatečně šifrována a zabezpečena). K jinak nepřístupným informacím se útočníci dostávají opět prostřednictvím odposlechů, spywarem i prostřednictvím dalších prvků.[283]

Z hlediska relevantních skutkových podstat se jich nabízí celá řada více či méně přiléhavě dopadajících na pestrou škálu kyberkriminality. Demonstrativní výčet zahrnuje jen nejběžnější jednání a v úvahu vždy přichází souběh s účastí na organizované zločinecké skupině (§ 361) a samozřejmě neoprávněným přístupem k počítačovému systému a nosiči informací (§ 2320 TZ). Skutkové podstaty s větším využitím ve vztahu k mládeži coby pachatelům i poškozeným jsou blíže rozvedeny dále a v následujících kapitolách. Vzato postupně, nejprve se nabízí obchodování s lidmi, vydírání, poškození cizích práv, porušení tajemství dopravovaných zpráv a listin a jiných dokumentů uchovávaných v soukromí, pomluva (§ 168, 175, 181, 182, 183, a 184 TZ). Ještě bohatším zdrojem jsou trestné činy proti lidské důstojnosti v sexuální oblasti: sexuální nátlak, šíření pornografie, výroba a jiné nakládání s dětskou pornografií a zneužití dítěte k výrobě pornografie, případně v souběhu s účastí na pornografickém představení (v závislosti na povědomí účinkujícího dítěte o pořízení záznamu), navazování nedovolených kontaktů s dítětem a svádění k pohlavnímu styku (§ 186, 191, 192, 193, 193a, 193b a 202 TZ). Z trestných činů proti majetku je třeba zmínit zejm. krádež (vč. souběhu s § 230 při odčerpání prostředků z bankovního účtu), podvod, legalizaci výnosů z trestné činnosti, poškození cizí věci a samozřejmě neoprávněný

[281] Např. virus Flame vyvinutý údajně USA spolu s Izraelem za účelem zmapování íránské počítačové sítě.
[282] Vč. propagandy, viz např. (ČTK, 2019).
[283] Za zmínku stojí v tomto směru např. varování NÚKIB před použitím technických nebo programových prostředků společností Huawei Technologies Co., Ltd., a ZTE Corporation určené vybraným subjektům provozujícím informační systémy důležité pro chod státu (NÚKIB, 2018).

přístup k počítačovému systému a nosiči informací (§ 205, 209, 216, 228 a 230 TZ). K dalším patří poškozování spotřebitele a porušení práv k ochranné známce a jiným označením, porušení chráněných průmyslových práv, porušení autorského práva, práv souvisejících s právem autorským a práv k databázi (§ 253 a 268, 269, 270 TZ). Dále pak poškození a ohrožení provozu obecně prospěšného zařízení, nedovolené ozbrojování a nedovolená výroba a jiné nakládání s omamnými a psychotropními látkami a s jedy, týrání zvířat (§ 276, 279, 284 a 302 TZ). Ke zvlášť závažným patří teroristický útok, sabotáž a vyzvědačství (§ 311,[284] 314 a 316 TZ). Výjimkou není násilí proti skupině obyvatelů a proti jednotlivci, hanobení národa, rasy, etnické nebo jiné skupiny osob a podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod, nebezpečné vyhrožování a pronásledování, méně často pak šíření poplašné zprávy. Zmínit lze též podněcování k trestnému činu a schvalování trestného činu (§ 352, 353, 354, 355, 356, 357, 364 a 365 TZ). Nakonec založení, podporu a propagaci a projev sympatií k hnutí směřujícímu k potlačení práv a svobod člověka a popírání, zpochybňování, schvalování a ospravedlňování genocidia (§ 403, 404 a 405 TZ).

7.1. Shrnutí k BTC a typům kyberkriminality

BTC představují nejvýznamnější virtuální měnu, navíc již vzájemně převoditelnou na tradiční měny (byť značně spekulativně). Vzhledem k technickým parametrům (decentralizace, faktická nepadělatelnost, značná anonymita uživatelů díky náhodným adresám atd.) se nabízí její předpokládané (ostatně vysoká latence je kyberkriminalitě vlastní) hojné využívání k legalizaci výnosů z trestné činnosti aj. protiprávním aktivitám (např. požadované platby při ransomwaru), zejm. ve spojení s dark webem.

Kyberkriminalita se nejčastěji člení dle CoC, která však nepostihuje celou její šíři, případně se odlišuje velmi obecně kriminalita usnadněná ICT a závislá na ICT. Kapitola proto představuje vlastní dělení, počínaje záměrem vůči PS, převažujícími použitými prostředky a (ne)využitím internetu. Dále rozvádí podtypy zásahu do systému (často jen prostředek dalšího jednání), majetkové kyberkriminality, krádeže identity, virtuálního násilí, černého trhu, sexuálního zneužívání, porušování autorských a příbuzných práv a cyber war.

[284] S ohledem na novelizaci provedenou zák. č. 287/2018 Sb. (s účinností od 1.2.2019) zejm. § 311 odst. 1 písm. e) TZ.

Mládeže coby poškozených se dotýkají více či méně všechny uvedené oblasti. Ze zásahů do systému napadení malwarem v závislosti na používaných ICT zařízeních, „odposlech“ (uložené fotografie aj.), ransomware a úprava dat (např. profilu na SNS). Z majetkové kyberkriminality především útoky v herní oblasti, při krádežích identity pak zejména motivace virtuálním násilím, typicky pomsta expartnera, kyberšikana a hate speech, za zmínku pak stojí i setkávání s násilným obsahem. Na černém trhu je to zejm. nakládání s dětskou pornografií, další formy sexuálního zneužívání zahrnují kybergrooming a dětskou prostituci, vč. sextingu. Porušování autorských a příbuzných práv a cyber war se jich dotýká naopak minimálně.

Jinak je tomu u mládeže coby pachatelů, kdy porušování (zejm.) autorských práv nebude výjimkou. V závislosti na vlastních schopnostech se mohou podílet na hackingu (případně s využitím exploitu), zdaleka nejčastější však je úprava dat, často po neoprávněném přístupu do systému (typicky neoprávněný přístup a úprava cizího profilu na SNS). V majetkové oblasti přichází v úvahu opět především herní oblast a opět v závislosti na schopnostech pachatele (ať už co do technických znalostí nebo sociálního inženýrství a např. vylákání přihlašovacích údajů k hernímu účtu). Krádež identity bývá především součástí kyberšikany, jinou podobou virtuálního násilí pak pomsta expartnera a hate speech. Nakonec v oblasti sexuálního zneužívání přichází v úvahu zejm. šíření dětské pornografie ve spojení se sextingem.

8. Výzkum a publikace v rámci IKSP

Počínaje rokem 2000 vydal IKSP (výzkumná organizace zřízená Ministerstvem spravedlnosti ČR) publikaci věnující se počítačové kriminalitě (Musil, 2000), dále pak poskytl součinnost při výzkumu T. Gřivny a J. Drápala (Gřivna, a další, 2018). Do svého střednědobého plánu výzkumné činnosti na období 2016-2019 pak zařadil IKSP mj. i výzkum kybernetické kriminality zaměřený na počítačové trestné činy (řešitelem autorka spolu s Mgr. Jiřím Vlachem): Identifikace a posouzení druhů a trendů kriminality páchané prostřednictvím Internetu.

8.1. Výzkum IKSP[285]

Součástí výzkumu IKSP je mj. i analýza vybraného vzorku trestních spisů, údaje zde uvedené proto vychází převážně z kombinace justičních statistik a dat získaných z trestních spisů zahrnujících věci, ve kterých byla podána obžaloba pro naplnění skutkové podstaty § 230 TZ[286] a trestní řízení pravomocně skončilo v roce 2015.[287] Vymezení rozsahu analýzy na rok 2015 vychází z předpokladu (podpořeného justičními statistikami), že již uplynula dostatečně dlouhá doba od zavedení počítačových trestných činů na to, aby bylo možné pracovat s dostatečným množstvím spisů,[288] zároveň bylo možné zpracovat za daný rok spisy všechny a souhrnná statistická data v resortu justice byla již k dispozici v roce 2017. Určité informace o rozsahu kyberkriminality v ČR lze vyčíst kromě policejních a justičních statistik (s výhradou vysoké latence) z jiných výzkumných projektů věnovaných online prostředí, tyto se ovšem věnují počítačovým trestným činům spíše jen okrajově, pokud vůbec (zaměřují se převážně na sexuální zneužívání dětí, používání SNS a kyberšikanu).[289]

[285] Kapitola vychází ze studentské vědecké odborné činnosti autorky (Kudrlová, 2018).
[286] V roce 2015 se nevyskytl žádný jiný počítačový trestný čin samostatně – v obou jediných trestních řízeních vedených pro § 231 TZ, která pravomocně skončila v roce 2015, se pachatelé dopustili svého jednání v souběhu s § 230 TZ.
[287] Přesněji řečeno jde o ta pravomocně skončená řízení, jejichž údaje (statistické listy trestní) byly v roce 2015 odeslány do evidence statistiky Ministerstva spravedlnosti ČR. Tzn. data zahrnují i několikero věcí pravomocně skončených již v roce 2014 a naopak zřejmě neobsahují některé z roku 2015, které byly pravomocně skončeny až ke konci roku a jejich statistické listy proto odeslány do evidence až v roce následujícím. Pro zjednodušení se zde nicméně hovoří o věcech „pravomocně skončených v roce 2015“, byť s výhradou tohoto drobného „převisu“ případů z předchozího a do následujícího roku.
[288] Počet počítačových trestných činů (vč. § 257a sTZ) rok od roku stoupá, počínaje 2 odsouzenými pachateli v roce 2001 přes 17 v roce 2011 až k 73 odsouzeným v roce 2016 (Kudrlová, a další, 2017), v roce 2017 to bylo již 107 osob.
[289] Viz např. výzkum České děti a FB 2015 (Univerzita Palackého v Olomouci, Pedagogická fakulta, 2015), Výzkum rizikového chování českých dětí v prostředí internetu (Univerzita Palackého v Olomouci, Seznam.cz,

Analýza trestních spisů probíhala formou vyhledávání a zaznamenávání sledovaných proměnných do záznamových listů. V některých případech byly veškeré potřebné údaje snadno a rychle zjistitelné, v jiných si jejich zjištění vyžádalo dlouhé pročítání a hledání zejm. v protokolech o výpovědích a z hlavního líčení. Zpracováno bylo tímto způsobem 65 trestních spisů[290] z celkového počtu 71 věcí[291] pravomocně skončených v roce 2015, jednalo se o 68 obviněných.[292] Prostřednictvím záznamových listů bylo sledováno 50 položek zahrnujících především základní údaje o obviněném[293] (a okrajově též o poškozených), trestném činu samotném a o průběhu trestního řízení. Protože může jít o jednorázové i relativně dlouho trvající jednání, věk pachatele zde uváděný se vztahuje nikoliv k době spáchání trestného činu (dokončení trestněprávně relevantního jednání naplňujícího znaky dané skutkové podstaty), ale k okamžiku zahájení úkonů trestního řízení, aby tak bylo možné využít předem stanovený jednotný časový bod srovnatelný napříč sledovanými skutky vč. těch, u nichž nelze dobu spáchání trestného činu jednoznačně a přesně stanovit. Určitým oříškem operacionalizace (převedení sledovaných znaků na jednoznačné stručné proměnné, se kterými lze dále statisticky pracovat) byl skutek a jeho charakteristiky (zejm. způsob spáchání a „komunikační kanál“, tj. převažující platforma jednání), některé z indikátorů byly jen obtížně jednoznačně zařaditelných pod konkrétní znaky:[294] např. prolomení hesla a následné ovládnutí profilu poškozené na SNS dílem ze žárlivosti (snaha prohlédnout si jinak neveřejnou komunikaci poškozené) a dílem z touhy po pomstě kvůli zavržení pokračování vztahu ze strany poškozené (snaha poškodit poškozenou komunikací jejím jménem), které posléze přešlo v podvodné jednání (snaha vylákávat prostřednictvím tohoto profilu od známých poškozené a poté i dalších osob tzv. m-platby). Navzdory tomu se podařilo získat množství informací uvedených dále.

Google, 2014) nebo EU Kids Online (eukidsonline.net).

[290] Počet leží na hranici statisticky relevantních dat, takže nelze vyloučit zkreslení fenomenologie nějakou výjimečnou věcí, shodou náhod atp. Přesto jde o prakticky kompletní pravomocnou soudní agendu za rok 2015, a tudíž se s výsledky lze spokojit, byť s uvedenou výhradou.

[291] Zbývající spisy se nepodařilo získat kvůli nepřítomnosti spisu u dožádaného soudu nebo jeho dalšímu používání (např. z důvodu zaslání spisu jinému soudu pro využití v jiném trestním řízení).

[292] Blíže k tomu viz (Kudrlová, a další, 2017) (Kybernetická kriminalita - dílčí poznatky z výzkumu I, 2018) a (Kybernetická kriminalita - dílčí poznatky z výzkumu II, 2018).

[293] Většina údajů zahrnuje osoby obviněné, tj. pachatele i ty, jejichž trestní stíhání bylo skončeno jinak než odsouzením.

[294] Mezi indikátory patří např. pohlaví pachatele, mezi znaky pak „muž“ či „žena“ (Gřivna, 2015 str. 200).

8.2. Kyberkriminalita v ČR z pohledu dostupných statistických údajů[295]

Hlavním zdrojem informací alespoň o části kyberkriminality jsou online dostupné statistiky Ministerstva vnitra ČR a Policie ČR publikované ve formě Zpráv o bezpečnostní situaci na území České republiky a Statistických přehledů kriminality (Ministerstvo vnitra ČR), (Ministerstvo spravedlnosti ČR), (Policie ČR). Statistické přehledy skýtají mj. souhrnné údaje pro počítačové trestné činy (vykazovány pod jednotným takticko-statistickým kódem 865 „poškozování a zneužívání záznamu na nosiči informací“ v rámci hospodářské kriminality). Jiná z hlediska kyberkriminality relevantní jednání jsou však skryta pod celou řadou dalších skutkových podstat a nelze je ve statistických údajích odlišit od klasické kriminality, typicky online podvod kvalifikovaný jen dle § 209 TZ bez souběhu s § 230 TZ (Smejkal, 2018 str. 186).

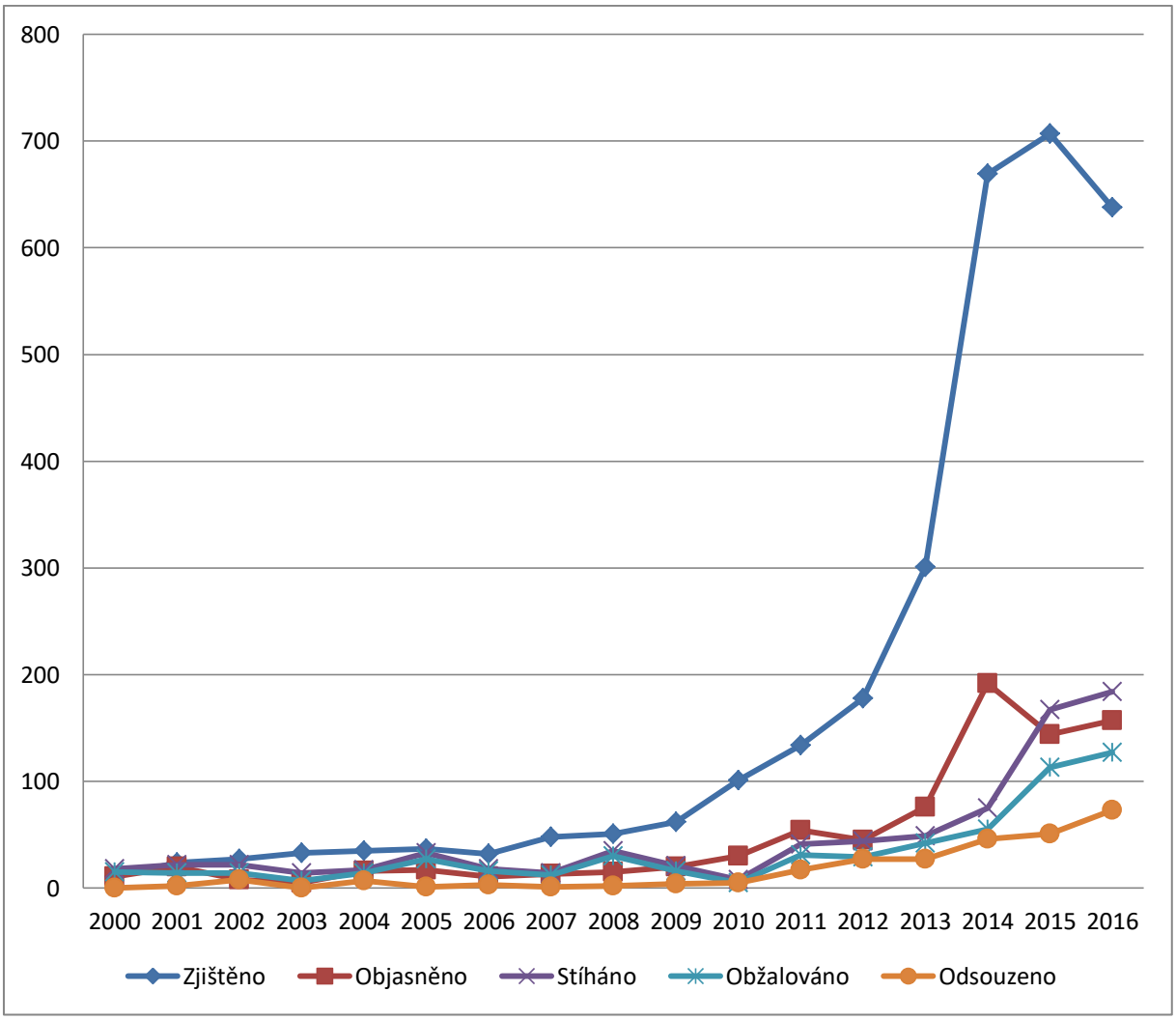
Tab. č. 3: Přehled statistických údajů o počítačových trestných činech[296]

Rok	Zjištěno	Objasněno	Míra objasněnosti	Stíháno	Obžalováno	Odsouzeno
2000	11	11	100%	18	15	0
2001	24	20	83%	22	14	2
2002	27	8	30%	22	14	8
2003	33	5	15%	14	7	0
2004	35	16	46%	17	14	7
2005	37	17	46%	33	27	1
2006	32	11	34%	18	16	3
2007	48	13	27%	14	12	1
2008	51	15	29%	35	30	2
2009	62	20	32%	21	16	4
2010	101	30	30%	8	5	5
2011	134	54	40%	41	31	17
2012	178	45	25%	44	29	27
2013	301	76	25%	49	42	27

[295] Kapitola vychází z článku vytvořeného ve spoluautorství s J. Vlachem (Kudrlová, a další, 2017).
[296] Zdroj: Statistické přehledy kriminality (Policie ČR) a Statistické ročenky kriminality a systém CSLAV (Ministerstvo spravedlnosti).

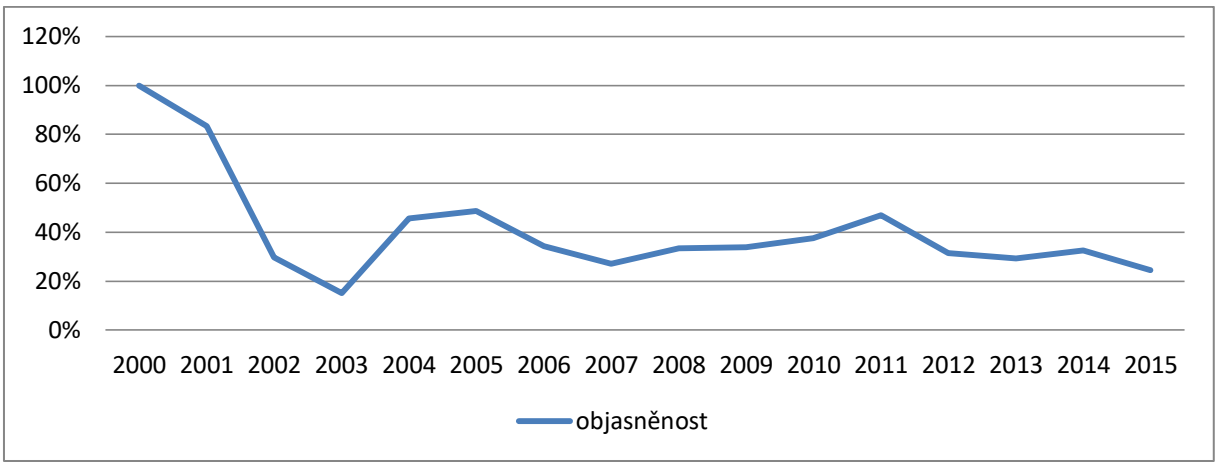
2014	669	192	29%	75	55	46
2015	707	144	20%	167	113	51
2016	638	157	25%	184	127	73

Graf č. 3:Vývoj počítačových trestných činů



V letech 2000 až 2015 se zvyšoval počet zjištěných skutků, přičemž od roku 2010 vykazuje růst o poznání větší dynamiku. Nevětší meziroční nárůst v tomto období činící 122,3% (tj. o 368 skutků více) byl zaznamenán mezi roky 2013 a 2014 (podrobněji viz tab. č. 3). Naproti tomu míra objasněnosti těchto skutků ve sledovaném období převážně klesá s nejvýraznějším propadem mezi lety 2000 až 2003 (z počáteční 100% objasněnosti až na 15 %). Po opětovném zvýšení objasněnosti v následujícím roce se v dalších letech pohybovala (byť s výkyvy) kolem průměru 35 % (podrobněji viz tab. č. 3 a graf č. 4).

Graf č. 4: Míra objasněnosti skutků dle § 230 – 232 TZ



I ve vývoji počtu stíhaných, obžalovaných a odsouzených osob pro počítačové trestné činy lze zaznamenat výrazný vzestupný trend po roce 2010. Největší, více než pětinásobné meziroční zvýšení počtu stíhaných osob v tomto období (o 33 osob) bylo zaznamenáno mezi roky 2010 a 2011. Také u počtu obžalovaných byl mezi těmito lety zaznamenán nárůst největší, více než šestinásobný (o 26 osob). Přestože se také počet odsouzených za počítačové trestné činy po roce 2010 nesl ve znamení růstu, největší nárůst zaznamenal až mezi roky 2013 a 2014, kdy činil 170 % (o 19 osob více), podrobněji viz tab. č. 3 a graf č. 3.

8.3. Dosud zjištěná data z výzkumu IKSP[297]

Drtivá většina sledovaných trestních řízení se zabývala přečinem neoprávněného přístupu k počítačovému systému a nosiči informací dle § 14 odst. 2 a § 230 odst. 1-4 TZ (67 trestních řízení),[298] v jednom případě šlo o zločin [§ 14 odst. 3 a § 230 odst. 2 písm. a), d), odst. 5 písm. a) TZ].[299] Ve dvou z těchto trestních řízení vedených o přečinech byli jeden pachatel a dva spolupachatelé stíhání zároveň pro jednočinný souběh s přečinem opatření a přechovávání

[297] Kapitola vychází ze studentské vědecké odborné činnosti autorky (Kudrlová, 2018).
[298] V jednom ze sledovaných případů soud posuzoval jednání pachatele kvalifikovaného v obžalobě jako neoprávněný přístup k počítačovému systému a nosiči informací dle § 230 odst. 2 písm. a) TZ v jednočinném souběhu se zneužitím pravomoci úřední osoby dle § 329 odst. 1 písm. a) TZ a neoprávněným nakládáním s osobními údaji dle § 180 odst. 2 TZ (příslušník Policie ČR neoprávněně vstoupil do jinak neveřejné databáze přístupné prostřednictvím služebních počítačů, z níž získal osobní údaje poškozené osoby, které předal jinému), byl pachatel bez dalšího odsouzen pouze za spáchání přečinu zneužití pravomoci úřední osoby, aniž by se soud v průběhu řízení k zúžení trestněprávní kvalifikace jakkoliv vyjádřil.
[299] Z hlediska časové působnosti trestních zákonů (§ 2 TZ) byly všechny sledované činy posuzované podle nového trestního zákoníku.

přístupového zařízení a hesla k počítačovému systému a jiných takových dat dle § 14 odst. 2, § 231 odst. 1 písm. b) TZ.

Tab. č. 4: Sledovaná trestní řízení o počítačových trestných činech

Skutkové podstaty počítačových trestných činů, jejichž naplnění shledala obžaloba	Počet trestních řízení pravomocně skončených v roce 2015
§ 230 odst. 1-4 TZ	65
§ 230 odst. 2 písm. a), d), odst. 5 písm. a) TZ	1
§ 230 odst. 1-4 TZ + § 231 odst. 1 písm. b) TZ	2
§ 232 TZ	0

Ve všech sledovaných řízeních rozhodl meritorně soud prvního stupně. Kromě jediného řízení tak učinil okresní soud, onou výjimkou bylo rozhodování krajského soudu v Brně o zločinu dle § 230 odst. 2 písm. a), d) odst. 5 písm. a) TZ, kterého se pachatel dopustil v souběhu se zvlášť závažným zločinem úvěrového podvodu a neoprávněného opatření, padělání a pozměnění platebního prostředku dle § 14 odst. 3, § 234 odst. 3, 5 písm. b) a § 211 odst. 1, 6 písm. a) TZ, a tudíž konal řízení v prvním stupni krajský soud (§ 17 odst. 1 a § 21 odst. 1 TŘ).

Tab. č. 5: Meritorně rozhodující soudy 1. stupně a počty pravomocně rozhodnutých řízení o počítačových trestných činech za rok 2015

Brno (městský soud)	6	Ostrava	1
Brno - venkov	1	Pardubice	2
Bruntál	3	Pelhřimov	1
Česká Lípa	1	Plzeň - město	1
České Budějovice	1	Praha 10	2
Frýdek-Místek	3	Praha 2	1
Havlíčkův Brod	3	Praha 3	1
Hradec Králové	1	Praha 4	2
Chomutov	1	Praha 5	1
Jablonec nad Nisou	3	Praha 6	1
Karlovy Vary	1	Praha 7	1
Karviná	2	Praha 8	3

Kolín	2	Prostějov	2
Kutná Hora	1	Přerov	2
Liberec	2	Příbram	1
Litoměřice	1	Strakonice	1
Louny	1	Šumperk	3
Most	1	Tábor	2
Nový Jičín	1	Tachov	2
Olomouc	2		

K neoprávněnému přístupu k počítačovému systému a nosiči informací docházelo většinou v souběhu s dalším či dalšími trestnými činy – pro samotný § 230 TZ byl obviněný souzen v pouhých 25 případech.[300] Ve 25 případech se pak jednalo o souběh s jedním dalším trestným činem, ve zbývajících 18 o souběh s více trestnými činy, zpravidla dalšími dvěma až třemi, v ojedinělém případě s dalšími pěti.[301] § 230 TZ jde nejčastěji ruku v ruce s útokem směřujícím proti majetku: krádež (§ 205 TZ, 8 souběhů), podvod a úvěrový podvod (§ 209 a 211 TZ, 12 souběhů).[302] Zařazení počítačových trestných činů v rámci hlavy V. zvláštní části TZ, tj. mezi trestnými činy proti majetku, je tak zcela namístě, byť nelze opominout ani ty případy, kdy se pachatel dopustí § 230 TZ nikoliv ze zištných, ale spíše z nenávistných nebo žárlivých pohnutek a usiluje především o zasažení osobnosti a způsobení nemajetkové újmy poškozenému.[303] Za zmínku pak stojí ještě zneužití pravomoci úřední osoby (§ 329 TZ, 8 souběhů, zejm. zneužití přístupu k jinak neveřejnému informačnímu systému),[304] vydírání (§ 175 TZ, 6 souběhů) a porušení tajemství dopravovaných zpráv (§ 182 TZ, 5 souběhů). Bez zajímavosti není ani bližší pohled na udílené tresty. Nutno podotknout, že jakmile se pachatel

[300] Se zohledněním pouze těch jednání, která více či méně souvisela s § 230 TZ – vícečinný souběh nestejnorodý není brán v potaz, pokud s počítačovými trestnými činy nikterak nesouvisel.

[301] Pachatel (v době zahájení trestního řízení ve věku 20 let) neoprávněně pronikal na cizí FB profily a jejich prostřednictvím či prostřednictvím zcela fiktivních profilů nebo profilů vydávajících se za pravé s využitím osobních údajů konkrétních osob vylákával tzv. m-platby, jimiž financoval své účty na několika portálech s hazardními hrami. Odsouzen byl kromě neoprávněného přístupu k počítačovému systému a nosiči informací [§ 230 odst. 2 písm. a), odst. 4 písm. b) TZ] za neoprávněné opatření, padělání a pozměnění platebního prostředku (§ 234 odst. 1 TZ), poškození cizích práv [§ 181 odst. 1 písm. a) TZ], porušení tajemství listin a jiných dokumentů uchovávaných v soukromí (§ 183 odst. 1 TZ), nebezpečné pronásledování [§ 354 odst. 1 písm. a) a c) TZ] a podvod [§ 209 odst. 1, 4 písm. d) TZ, dílem dokonaný, dílem ve stadiu pokusu].

[302] Nejednou ve spojení ještě s neoprávněným opatřením, padělaním a pozměněním platebního prostředku (§ 234 TZ, 7 souběhů) – např. zneužití cizí platební karty k výběru peněz předtím neoprávněně získaných úvěrovým podvodem.

[303] Např. neoprávněný přístup k profilu poškozené osoby na SNS a rozesílání urážlivých zpráv jejím jménem (Kybernetická kriminalita - dílčí poznatky z výzkumu II, 2018).

[304] Ze spáchání § 230 TZ v souvislosti s postavením úřední osoby bylo obviněno 10 osob.

dopustil svého jednání v souběhu, zpravidla je právě sbíhající se trestný čin tím přísněji trestným, podle něhož soud ukládá trest. To konec konců odpovídá charakteru skutkové podstaty neoprávněného přístupu k počítačovému systému a nosiči informací, která má do jisté míry charakter předčasně dokonaného trestného činu,[305] zejm. při naplnění znaků výlučně prvního odstavce, tj. při pouhém neoprávněném získání přístupu k PS nebo jeho části po překonání bezpečnostního opatření.[306]

Podřazování jednání obviněného pod skutkovou podstatu dle § 230 TZ ovšem trpí určitou nejednotností a vágností plynoucí zřejmě z faktu, že se jedná o dvě samostatné základní skutkové podstaty, které mohou, ale nemusí být naplněny zároveň. V prvním odstavci § 230 TZ je chráněna primárně důvěrnost počítačových dat a počítačového systémů, v druhém pak jejich integrita a dostupnost (Šámal, 2012 str. 2086). Pachatel tak může zasáhnout jeden, druhý, nebo i oba chráněné objekty.[307] V některých případech je nepochybně namístě uvažovat o faktické konzumpci skutkové podstaty uvedené v prvním odstavci naplněním znaků té druhé (zejm. při naplnění znaků některé z kvalifikovaných skutkových podstat), a obžaloba i soudy tak ve svých rozhodnutích činí (byť jim lze vytknout, že zpravidla mlčky), problematičtější se však zdá být nikoliv výjimečné podřazení jednání pouze pod základní skutkovou podstatu uvedenou v prvním odstavci, byť pachatel naplnil zároveň i znaky základní skutkové podstaty uvedené v druhém odstavci.[308] Problematické proto, že s ohledem na chráněné objekty může být (nikoliv však nutně a vždy) skutková podstata v prvním odstavci ve vztahu subsidiarity vůči skutkové podstatě ve druhém odstavci, neboť narušení důvěrnosti lze v některých případech považovat za určitou formu spíše ohrožovacího trestného činu, zatímco narušení integrity za určitou formu poškozovacího trestného činu

[305] K předčasně dokonanému trestnému činu viz např. (Šámal, 2012 str. 237). Rozhodnutí zařadit do nového trestního zákoníku takto formulované skutkové podstaty počítačových trestných činů (§ 231 TZ je předčasně dokonaným trestným činem sám o sobě, pouze § 232 TZ takto označit nelze) vychází z velké části z mezinárodních závazků ČR, blíže k tomu viz kapitola **Trestněprávní postih kyberkriminality** a (Jelínek, a další, 2015 str. 286).

[306] Pachatel např. neoprávněně pronikne do emailové schránky poškozené – své přítelkyně, aby zjistil, zda komunikuje s dalšími muži, aniž by s daty samotnými jakkoliv manipuloval nebo činil cokoliv nad rámec pouhého prohlédnutí příchozí a odchozí pošty.

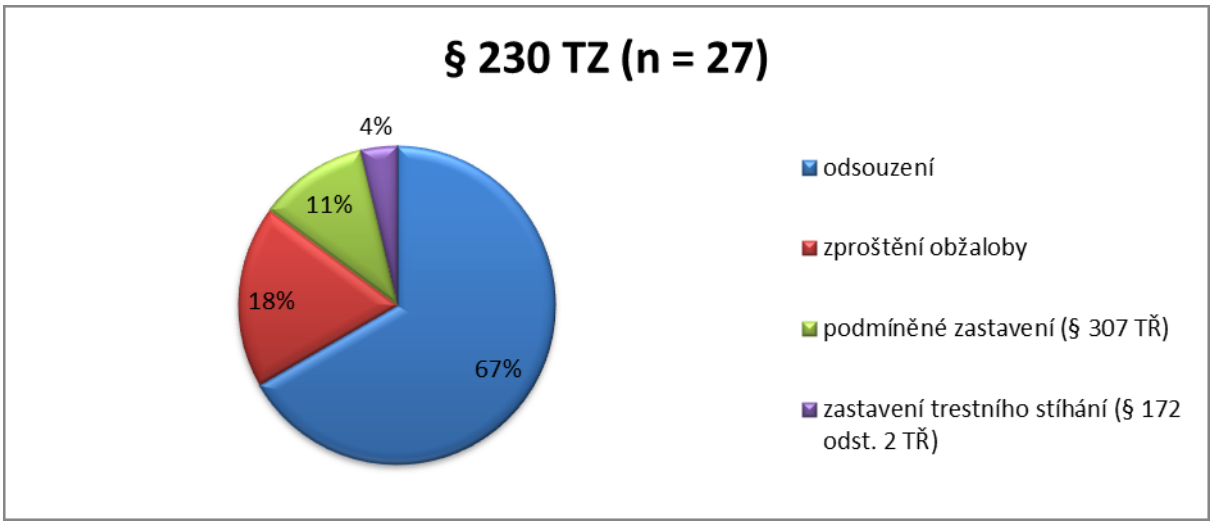
[307] Např. pachatel si pouze ze žárlivosti prohlédne po neoprávněném vniknutí do emailové schránky manželčinu poštu, nebo je manželkou požádán o kontrolu pošty a k tomu účelu mu manželka sdělí své přihlašovací údaje, ovšem on část pošty bez jejího svolení smaže, anebo naplní obě základní skutkové podstaty tím, že část pošty smaže poté, co do emailové schránky pronikl neoprávněně.

[308] Typicky pachatel neoprávněně pronikne do PS, ve kterém upraví data – např. neoprávněně vstoupí do profilu na SNS a smaže fotografie.

(Šámal, 2012 str. 133), což podtrhuje i skutečnost, že trestný čin neoprávněného přístupu k PS a nosiči informací je při naplnění znaků druhé základní skutkové podstaty přísněji trestný.[309]

Při pohledu na ukládané tresty zde proto nerozlišuji trestněprávní kvalifikaci dle prvního nebo druhého odstavce § 230 TZ a neberu zřetel na jednání v souběhu s dalšími trestnými činy vyjma ostatních počítačových trestných činů. Zůstává tak celkem 27 relevantních případů, což sice nelze považovat za statisticky významný počet, má však alespoň orientační vypovídací hodnotu. Z těchto 27 věcí v pěti případech soud obviněného zprostil obžaloby, v jednom bylo trestní stíhání zastaveno (§ 172 odst. 2 TŘ), ve třech podmíněně zastaveno (§ 307 TŘ), ve zbývajících 18 došlo k odsouzení. Z toho ve 14 případech soud uložil trest odnětí svobody, který podmíněně odložil. Průměrná délka trestu činila 6 měsíců (ukládáno 3-10 měsíců). Zkušební dobu uložil soud průměrně v délce 16 měsíců (12-30 měsíců).[310] V 5 případech soud uložil trest obecně prospěšných prací (třikrát 150 hod a jedenkrát 30 hod a 200 hod). Nedošlo k uložení žádného vedlejšího trestu, v 9 případech pak vůbec nedošlo k odsouzení. Nebylo uloženo ani žádné ochranné nebo výchovné opatření. Ve třech případech soud shledal polehčující okolnost v podobě vedení řádného života před spácháním trestného činu [§ 41 písm. o) TZ], v jednom přitěžující okolnost spáchání trestného činu ze zavrženíhodné pohnutky, zákeřně a ve větším rozsahu [§ 42 písm. b), c) a m) TZ]. Dvanáctkrát soud rozhodl rozsudkem nebo zjednodušeným rozsudkem, čtyřikrát usnesením a jedenáctkrát trestním příkazem.

Graf č. 5: Skončení trestního řízení

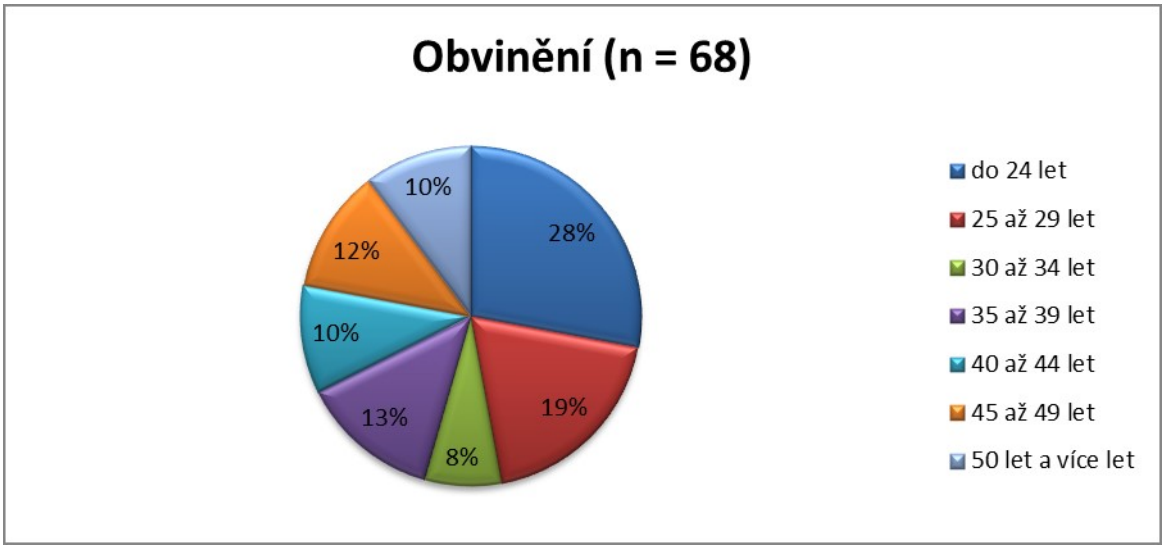


[309] Pachateli hrozí trest odnětí svobody až na tři léta oproti až dvěma rokům hrozícím za naplnění znaků pouze prvního odstavce (§ 230 odst. 1 a 2 TZ).
[310] Tresty ve dvou případech souběhu s jiným počítačovým trestným činem (§ 231 TZ) ve výši 7 a 6 měsíců se zkušební dobou 12 měsíců mezi ostatními nijak nevynikají.

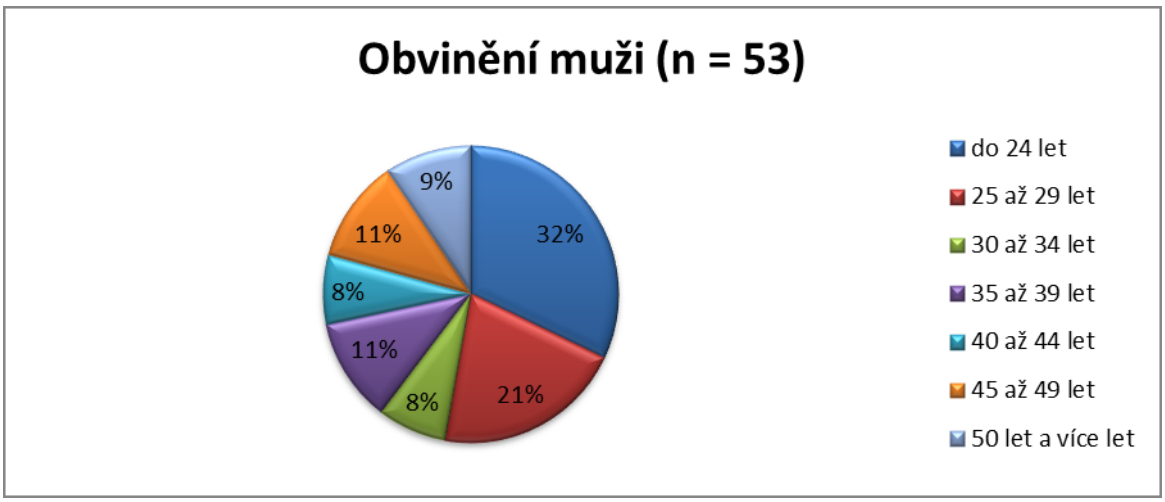
Skladba obviněných dle pohlaví, blíže k tomu viz (Kybernetická kriminalita - dílčí poznatky z výzkumu II, 2018), se v rámci kriminality jako takové poněkud vymyká, neboť ženy představují 22 % oproti běžným 12-15 % (Gřivna, 2015 str. 97). Bylo by předčasné vytvářet na základě tak malého souboru dat teorie, proč tomu tak je, jedním z faktorů však může být charakter kyberkriminality s předmětem útoku v podobě „PS nebo jeho části, nosiči informací, ... programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat“ (Šámal, 2016 str. 695). Jinými slovy obvykle jakási virtuální data, nehmatatelná a vzdálená, která představují snadnější předmět útoku než např. konkrétní osoba fyzicky přítomná, ať už z hlediska praktického provedení útoku (např. fyzické napadení oproti smazání dat na dálku) nebo psychického rozpoložení (např. fyzický stav napadené osoby vyvolávající při pohledu na ni lítost oproti poškození rádoby nepersonalizovaných dat ve virtuálním prostředí).

Věkově se obvinění muži a ženy v souhrnu pohybovali nejčastěji do 29 let, ovšem při rozlišení obou pohlaví se jejich rozložení částečně liší, neboť průměrný věk obviněných žen se oproti obviněným mužům zvyšuje, neboť se pohybují převážně ve věkové skupině 35-49 let (53 %), viz grafy č. 6-8. Vysvětlení odlišností opět spočívá s největší pravděpodobností ve specifickém charakteru kybernetické kriminality (resp. zde počítačových trestních činů), ovšem opět (a ještě výrazněji) s výhradou malého vzorku a statisticky nevýznamného počtu.

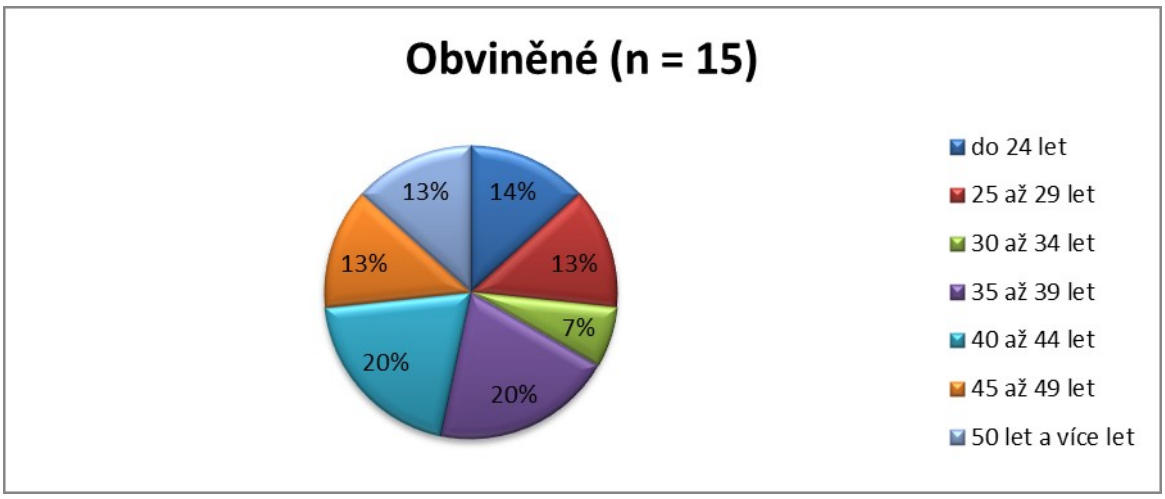
Graf č. 6: Věkové složení obviněných mužů a žen v souhrnu



Graf č. 7: Věkové složení obviněných mužů samotných



Graf. č. 8: Věkové složení obviněných žen



Většinu obviněných (42 osob, 62 %) tvořili prvopachatelé, 7 obviněných mělo za sebou již 1 pravomocné odsouzení a 18 bylo recidivisty s 2 a více dřívějšími pravomocnými odsouzeními (se 2-13 odsouzeními) u jednoho z obviněných se obžaloba ani soud jeho trestní minulostí vůbec nezabývaly. Ve spolupachatelství se svého jednání dopustilo 6 osob (vč. 1 návodce), z toho 2 ženy. Všichni až na 1 muže a 1 ženu pocházející ze Slovenské republiky byli občané ČR. Z hlediska rodinného stavu, vzdělání a socioprofesního statusu představují poměrně pestrou paletu bez výraznějšího vzorce, který by zde stál za větší pozornost, vyjma snad 10 již zmíněných osob, jejichž jednání mělo souviset s postavením úřední osoby.

Mezi poškozenými figurovaly fyzické i právnické osoby i obojí. Zdá se, že pachatelé § 230 TZ útočí na data vybraných jednotlivců, anebo se dopouštějí svého jednání ve velkém měřítku: v 59 případech byla mezi poškozenými jediná fyzická (42) nebo právnická (17) osoba, v 15 pak 2-5 osob. Ve zbývajících případech s alespoň částečně známým počtem poškozených se jejich počet vyhoupl na minimálně 75, dále 97 a dokonce 282 poškozených. Velmi často usnadnila či přímo umožnila trestné jednání neopatrnost až liknavost poškozených vůči svým přihlašovacím údajům. Pachatelé tak zneužívali zejm. nezměněná hesla svých ex-partnerů, která znali ještě z dob společného života,[311] hesla a potvrzovací sms vylákaná od poškozených pod rozličnými záminkami, příliš slabá hesla a neopatrnosti a důvěřivosti poškozených sdělivších jim přihlašovací údaje v dobré víře jejich nezneužití (např. žádost o kontrolu emailové pošty) nebo nedbajících řádného zabezpečení po fyzické stránce (např. vytištěné přihlašovací údaje k internetovému bankovnictví nalezené spolubydlícím). Namístě je přitom ochrana zejm. přístupových údajů k elektronickému bankovnictví a emailové schránce, dále pak k SNS a veškerým aplikacím spravujícím osobní údaje.

Počet dílčích útoků se mnohdy nepodařilo zjistit, ba se tím obžaloba a soudy ani podrobněji nezabývaly.[312] Výjimku tvořily případy s prokázanou škodou, kterou pachatel způsobil nebo se pokusil způsobit. Výše škod má však takový rozptyl, že nemá smysl je průměrovat bez podrobnějšího rozlišení předmětu útoku (zejm. elektronické bankovnictví, SNS, emailové schránky aj.), což by však bylo statisticky již zcela bezvýznamné: od 1.200 Kč po cca 26 mil. Kč.[313] Veškeré sledované trestné činy úzce souvisely s internetem. Pouze ve 4 případech využil pachatel technické znalosti nad rámec běžného užívání ICT: využití slabin v zabezpečení webových stránek (a následná publikace tam nalezených jinak skrytých osobních údajů), přístup k jinak neveřejným datům získaný zpětnou analýzou volně přístupného zdrojového kódu programu (a jejich využití ve vlastním konkurenčním softwaru bývalým vývojářem napadené aplikace), dvakrát vytvoření falešných přihlašovacích stránek a jejich prostřednictvím sběr osobních údajů (přihlašovací jméno a heslo) k následnému

[311] Totéž platí i pro organizace a přístupové údaje do vnitřního informačního systému bývalých zaměstnanců.

[312] S obvyklou formulací „v blíže neurčenou dobu," případně dokonce v kombinaci „s blíže neurčeným způsobem." Obžaloba i soud se spokojily s prokázáním trestněprávně relevantního následku a kauzálním spojením se zřejmým jednáním pachatele v určitém časovém období, a nelze jim to mít za zlé, vzhledem k případné nadbytečnosti a náročnosti (až nemožnosti) získání podrobnějších důkazních prostředků, nemluvě o technických znalostech potřebných pro správné vyvození samotného důkazu (Fenyk, a další, 2015 str. 330) – např. logy (tj. záznamy o činnosti a běhu některých programů a jejich funkcí).

[313] Mimoto pachatelé mnohdy způsobili kromě škody (někdy výlučně) i nemajetkovou újmu (44 případů) – např. zostuzení poškozené před spolupracovníky po rozeslání urážlivých emailů jejím jménem prostřednictvím neoprávněného přístupu do emailové schránky poškozené.

využití.[314] Dle očekávání došlo poměrně často (ve 29 případech) ke zneužití přístupu jinak oprávněnou osobou, z toho pětkrát šlo osobou ve služebním poměru, čtrnáctkrát zaměstnancem či bývalým zaměstnancem.[315]

V 58 případech měli obvinění použít při páchání trestné činnosti stolní nebo osobní počítač a v 10 mobilní telefon. V 17 případech využili email či emailovou schránku, rovněž v 17 sociální síť FB (a ve 4 jiné SNS). Ve 28 případech umožnila spáchání činu fyzická přítomnost pachatele, který buď získal nebo měl přístup k jinak nedostupnému informačnímu systému (např. interní informační systém bankovní instituce) či zařízení (např. zapůjčený notebook s uloženými přihlašovacími údaji poškozeného). V 9 případech pachatel pronikl do cizího internetového bankovnictví, odkud převedl či vybral finanční prostředky nebo si jménem poškozeného vzal úvěr ve svůj prospěch. Co se týče motivace pachatele známé orgánům činným v trestním řízení, ve 38 případech mířil útok primárně na osobnost poškozeného, z toho ve 13 případech na osobní údaje (např. sběr interních dat o klientech zaměstnavatele pro konkurenční společnost), v ostatních 25 pachatelé především kontrolovali poštu a zasílali nebo zveřejňovali zprávy dehonestující poškozeného, a to zejm. ze žárlivosti nebo z pomstychtivých důvodů (14 případů). Ve 22 případech pachatelé útočili na majetek, zpravidla primárně ve snaze získat pro sebe z různých důvodů finanční prostředky.

Při bližším pohledu na skutky pravomocně odsouzené v roce 2015 se ukázalo, že řadu z nich lze označit za skoro až banální jednání (např. nahlédnutí do manželova mobilu a přeposlání si několika jeho sms ze žárlivosti). Co na tom, že na takové situace pamatuje trestní řád zásadou oportunity a možností odklonu,[316] když už není možné využít zásady subsidiarity trestní represe.[317] Samotný fakt trestního řízení ovlivňuje život obviněného a odčerpává z justice finanční i časové prostředky. Zároveň není možné zmírnit formulaci samotných základních skutkových podstat § 230 TZ vyplývajících z mezinárodních závazků ČR (včetně kriminalizace přípravy neoprávněného přístupu k PS a nosiči informací, v rámci TZ v podobě opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat, viz § 231 TZ). Pakliže by se tato situace měla změnit, bylo by zde namístě uvažovat o rozvolnění trestní represe (nikoliv však o dekriminalizaci vůbec): např. přidáním

[314] 1 z pachatelů vytvořil sofistikovaný automatizovaný systém přeposílání a filtrování zájmové pošty v napadených emailových schránkách, který mu umožnil sledování cizí komunikace v masovém měřítku.
[315] Mezi podezřelými a pachateli se zaměstnanci a bývalí zaměstnanci poškozené společnosti ocitají běžně (Smejkal, 2018 str. 689).
[316] Zde bylo trestní stíhání soudem zastaveno dle § 172 odst. 2 písm. c) TŘ.
[317] Chybí jiný právní předpis, podle něhož by bylo možné odpovědnost uplatnit, jak předpokládá § 12 odst. 2 TZ, pouze v některých případech je možné využít zák. o některých přestupcích (zejm. § 7 nebo 8 – přestupky proti občanskému soužití nebo majetku).

dalších znaků k základním skutkovým podstatám, jako spáchání činu zvlášť zavrženíhodným způsobem, vůči zvlášť ohroženým osobám,[318] v úmyslu získat pro sebe nebo pro jiného neoprávněný prospěch nebo z jiné zavrženíhodné pohnutky atp. Za úvahu by též stála určitá privatizace bezpečnosti ve smyslu sebeochrany,[319] a to z toho prostého důvodu, že vyšetřování a prokazování kyberkriminality je nanejvýš obtížné a náročné (časově, finančně, znalostně), naproti tomu velké části úspěšných útoků lze předejít či se jim bránit relativně jednoduchými kroky: silnými a různými hesly, ověřenými zdroji softwaru, ověřováním identity komunikující osoby atp. Zvlášť apel[320] na pozornost a péči věnovanou vlastní heslům o ochraně osobních údajů v online prostředí se zdá být na místě, neboť velká část sledovaného jednání byla spojena se zneužitím osobních údajů, ať už v podobě slabého hesla, fyzicky nezabezpečeného či vyzrazeného hesla nebo údajů potřebných k vytvoření důvěryhodného falešného profilu.

8.4. Případová studie – email jako vstupní brána[321]

Ač byla paleta jednání sledovaných v rámci výzkumu IKSP poměrně pestrá, ukázalo se několikero opakujících se jevů. Uvedená studie názorně ilustruje napadání emailových schránek a jejich zranitelnost v podobě slabě zabezpečeného hesla. Pachatelovo jednání lze stručně shrnout jako neoprávněné pronikání do cizích emailů za účelem prohlídky nebo stažení jejich obsahu. V jeho případě se jednalo o fotografie a videa s erotickou nebo přímo pornografickou tematikou,[322] která využíval pro vlastní sexuální uspokojení: „...nikde jsem je dále nešířil. Při prohlížení těchto fotografií jsem masturboval.“ Dle znaleckého posudku z oboru zdravotnictví, odvětví psychiatrie a sexuologie, byl pachatel v době jednání závislý na konzumaci internetové erotiky k autoerotickým aktivitám, na alkoholu a drogách, jeho ovládací schopnosti byly v důsledku toho podstatnou měrou sníženy. „Ve většině případů ... jsem často byl pod vlivem alkoholu, kdy jsem za večer vypil asi 5 12stupňových piv a

[318] V online prostředí zejm. osoby snáze manipulovatelné: důvěřivé, naivní, neznalé digitálního prostředí, zranitelné i v reálném prostředí - typicky děti a senioři, postižené osoby postižené (mentálně i jinak).
[319] Ačkoliv tato bývá ve své vyhraněné podobě obecně vnímána spíše negativně, neboť má tendence vést k vysokým zdem znemožňujícím sousedské soužití, tvorbě ghett, diskutabilnímu zbrojení obyvatelstva atp.
[320] Např. formou vzdělávacích TV nebo spíše internetových spotů, jaké vytváří např. CZ.NIC (CZ.NIC, 2012).
[321] Kapitola byla přednesena na konferenci pořádané Českou kriminologickou společností ve spolupráci s Právnickou fakultou Univerzity Palackého v Olomouci VI. kriminologické dny a publikována (Kybernetická kriminalita - dílčí poznatky z výzkumu II, 2018).
[322] Spojení neoprávněného přístupu k počítačovému systému a nosiči informací se získáváním pornografického materiálu touto cestou bylo v roce 2015 ojedinělé, a to navzdory úzkému propojení mezi internetem a pornografií (vč. dětské pornografie) jako takovou.

pravděpodobně vždy jsem byl pod vlivem marihuany.“ Pachatel neměl dosud žádný záznam v trestním rejstříku a svého jednání se dopouštěl po dobu zhruba pěti let ve svých 32 až 37 letech, skončil po absolvování prvního výslechu v této věci. Trestné činnosti pak dle svého tvrzení dobrovolně zanechal: „...pokračoval jsem v tom až do prvního výslechu... Potom jsem už nic takového nedělal. V současné době ... trestnou činnost již neprovádím. Přišel jsem na to sám, ale kdy a za jakých okolností si již nevybavuji.“ Své vzdělání dovršil na střední škole s maturitou, ještě v době trestního řízení byl svobodný a žil ve společné domácnosti se svou matkou. Jeho průměrný měsíční výdělek jakožto instalatéra činil zhruba 8.000 Kč (z toho splácel úvěr 100.000 Kč vždy částkou 5.000 Kč měsíčně).

Modus operandi byl po celou dobu jednání poměrně neměnný. Nejprve si pachatel vyhlédl osobu na SNS Lidé.cz nebo Najdise.cz. Mezi jeho objekty zájmu patřily především mladé dívky, a to výhradně ty, které uvedly jako kontaktní email adresu v doméně seznam.cz. Následně se pokusil zjistit, zda existuje s jejich příjmením profil na SNS Spolužáci.cz, který by mohl patřit jejich matce,[323] neboť právě zde se zpravidla nachází vedle stávajícího příjmení dané osoby i její jméno za svobodna.[324] Vyzbrojen těmito údaji se následně pokusil proniknout do emailové schránky prostřednictvím tzv. obnovy zapomenutého hesla. V předchozích letech poskytovatel emailových služeb Seznam.cz umožňoval uživatelům zajistit svůj účet pro případ zapomenutí hesla prostřednictvím odpovědi na kontrolní otázku vybranou z krátkého seznamu, kde byla na prvním místě otázka po rodném příjmení matky.[325] Podle pachatele většina vybraných majitelek používala právě tuto otázku: „Protože volba kontrolní otázky je velmi omezená, naprostá většina žen tam měla rodné příjmení své matky za svobodna. Také je to první z možností v nabídce na kontrolní otázku a většina lidí si to právě proto vybere.“ Tento zdánlivě jednoduchý způsob byl podle pachatele zdlouhavý a nepochybně vyžadoval určitou dávku trpělivosti: „Byla to mravenčí práce, uspět se a najít potřebnou odpověď se mi podařilo jen asi v 5 % případů, kdy jsem hledal odpověď na kontrolní otázku ke vstupu.“ Nutno podotknout, že oněch 5 % znamenalo přinejmenším 97 emailových schránek, do nichž se pachateli prokazatelně podařilo proniknout. Jakmile se pachatel octl v emailové schránce, pokusil se vyhledat zejm. v rámci odchozí pošty přílohy v

[323] Vodítkem mu bylo např. místo narození, bydliště nebo navštěvovaná škola (zpravidla informace dostupná na některé SNS, nejčastěji FB), křestní jméno odhadoval.
[324] SNS Spolužáci.cz vznikla a je hojně využívána k vyhledávání bývalých spolužáků (a udržování komunikace s nimi), a proto si ji lze jen těžko představit jako úspěšně fungující bez tohoto atributu.
[325] V současnosti již Seznam.cz upřednostnil obnovu zapomenutého hesla prostřednictvím tzv. ověřeného telefonu nebo emailu, na který v případě zapomenutého hesla zašle heslo nové. Možnost obnovy hesla prostřednictvím kontrolní otázky zůstává pouze u dříve založených emailových schránek, jejichž uživatelé dosud žádný mobilní telefon ani email neověřili.

podobě fotografií a videí erotického až pornografického charakteru, v některých případech objevil i samostatné složky, jejichž názvy vypovídaly o takovém obsahu. Pokud byl ve svém hledání úspěšný, emailovou adresu a přihlašovací údaje k ní si poznamenal pro opakované pozdější použití: „Emailovou adresu a přístupové heslo jsem si uložil pro případné budoucí využití, kdy jsem do těchto schránek vstupoval i opakovaně a pátral, zda se zde neobjevily nějaké nové fotografie.“ Motivem pachatelova jednání bylo sexuální uspokojení jednak formou masturbace, jednak plynoucí ze samotného vědomí, že majitelky napadených emailových schránek o jeho jednání nic netuší: „Mé jednání bylo způsobeno mým zvýšeným sexuálním apetitem, který jsem si neměl kde vybít. Vzrušovalo mě, že o tom, že se jim dívám do emailů a stahuji si jejich fotky a videa poškozené nevěděly. Na text nějakého emailu jsem se podíval asi jen v jednom případě, ale to mě nijak nezajímalo, chtěl jsem pouze fotografie.“

Pachatel se nakonec neomezil "pouze" na procházení obsahu napadených emailových schránek, ale jeho sexuální apetit si vyžádal další aktivity, a to v podobě stahování dětské pornografie prostřednictvím P2P. Soud mu proto uložil úhrnný trest ve výměře dvanácti měsíců za sbíhající se přečiny neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 odst. 1 TZ (týkalo se pouze neoprávněně navštívených emailových schránek) a § 230 odst. 2 TZ (z některých navštívených schránek pachatel přeposlal část obsahu na svůj email) a dále přečin výroby a jiného nakládání s dětskou pornografií dle § 192 odst. 1 TZ, který podmíněně odložil na zkušební dobu 36 měsíců. Vedle toho pak trest propadnutí věci (mj. tří počítačů vč. netbooku) a ochranné léčení sexuologické ambulantní formou [viz § 43 odst. 1, § 81 odst. 1, § 82 odst. 1 a § 70 odst. 2 písm. a) TZ a § 99 odst. 3 a § 99 odst. 4 TŘ).[326] Poškozené byly se svým nárokem na náhradu škody odkázány na řízení ve věcech občanskoprávních.

Ač si to mnozí neuvědomují, email představuje do jisté míry vstupní bránu do virtuálního světa jeho majitele. V prvé řadě zahrnuje vlastní aktivity spojené s emailovou komunikací jako takovou, zejm. samotný obsah komunikace (vč. příloh) a emailové adresy osob, s nimiž dotyčný udržuje nebo byl někdy v kontaktu. Z využívání emailové schránky lze do jisté míry vyčíst např. i dobu aktivity a spánku, stav offline i online. Mimoto velmi často obsahuje i přihlašovací údaje k SNS a dalším aplikacím.[327] V neposlední řadě pak mnohdy slouží i pro

[326] Trestní řízení bylo zahájeno na základě podaného trestního oznámení na neznámého pachatele od jedné z poškozených, která při náhodné kontrole odeslané pošty objevila několik odešlých emailů, které však sama neposlala).

[327] Náš pachatel díky tomu ve dvou případech „navštívil“ i profily poškozených na SNS FB, když vyhledal přihlašovací údaje právě v jejich napadených emailových schránkách.

obnovu hesla pro tyto aplikace, tj. jako adresa, na kterou je v případě zapomenutí odesláno stávající heslo nebo odkaz pro jeho změnu.

Ve sledovaných spisech hrál email významnou roli zhruba ve čtvrtině případů. Útok byl cílený na obsah emailové schránky jako takové v 9 případech, přičemž v 5 byl blízký vztah mezi pachatelem a poškozeným (ať už šlo o muže či ženy na obou stranách) – manželé či partneři, stávající i bývalí. Pachatelé zejm. pátrali po nevěře (v 5 případech), ale také např. hledali informace použitelné v rozvodovém řízení, 1 z pachatelů si neoprávněně zálohoval „svou" firemní poštu po ukončení pracovního vztahu. Napadení emailové schránky ovšem sloužilo ve zbývajících 8 případech i jako prostředek k dalšímu jednání, převážně šlo o zištnou motivaci nebo nějakou formu virtuálního násilí. Ve 2 případech virtuálního násilí pachatele motivovala touha po odplatě (bývalé přítelkyni po rozchodu a vůči sestře pro rodinné neshody) a usiloval o poškození dobré pověsti poškozené (rozesíláním jejích intimních fotografií a zveřejněním jinak neveřejné komunikace na FB). Zištná motivace vedla jednoho z pachatelů k přeposílání dat o klientech zaměstnavatele konkurenční společnosti. Další prostřednictvím napadených emailových schránek získával přístup mj. k FB všude tam, kde se mu podařilo dohledat uschované přihlašovací údaje. Ty poté změnil, aby s nimi jejich oprávněný uživatel nemohl nakládat, a jménem tohoto uživatele oslovoval další osoby s žádostí o přeposlání potvrzovacích sms, v nichž se skrývaly platby prostřednictvím tarifu mobilního operátora v různé výši, které využíval pro dobití kreditu na několika pokerových portálech, na nichž hrál.[328] Poslední vybraný pachatel zachytával emailovou komunikaci obsahující výrazy jako „platba", „faktura" atp., aby v takových emailech následně pozměnil čísla účtů ve svůj prospěch.[329]

Všechny útoky na emailové schránky měly až na jedinou výjimku společné nedostatečné zabezpečení hesla, které nabývá několika základních podob: jednoduchost, fyzické nezabezpečení, neměnnost, zranitelnost obnovy. Příliš jednoduché heslo pachatel ve třech případech uhodl (např. heslo v podobě jména poškozené instituce). Fyzicky nezabezpečené heslo využili pachatelé ve dvou případech (nalezené v diáři spolubydlící a uložené v zapůjčeném počítači). Dlouho neměnné heslo se stalo kamenem úrazu pro bývalého zaměstnavatele vůči zaměstnanci po rozvázání pracovního poměru a pro poškozenou, jejíž

[328] Počet poškozených zde dosáhl téměř 300, způsobená škoda téměř 470 tisíc Kč (pachatel se pokusil způsobit škodu přesahující 1 milion Kč).
[329] Někdy své jednání doplnil emailovou komunikací jménem poškozených – např. zrušil objednaný zájezd u cestovní kanceláře poté, co změnil ve svůj prospěch číslo účtu v emailu potvrzujícím rezervaci zájezdu adresovaném poškozené, aby tak oddálil okamžik zjištění podvodu.

partner ho znal ještě z časů bezproblémového soužití.[330] Nakonec je zde ona zranitelnost obnovy hesla, s jejíž pomocí pachatel snadno obejde i jinak neprolomitelné a bedlivě střežené heslo, a která byla při neoprávněném pronikání do emailových schránek využita ve čtyřech případech (z toho ve 3 šlo o kontrolní otázku zjišťující rodné jméno matky za svobodna, ve čtvrtém o oblíbenou filmovou postavu).[331] Za zmínku stojí ještě 3 případy sofistikovanějšího získání hesla, a to prostřednictvím phishingu: šlo o email zdánlivě pocházející od administrátorů SNS požadující pro kontrolu sdělení přihlašovacích údajů pod hrozbou ztráty přístupu k vlastnímu profilu, dále pak o dvoje falešné přihlašovací stránky, na něž pachatelé zaslali poškozeným odkaz s cílem získat jejich přihlašovací údaje vyplněné na těchto stránkách.[332]

Samotné jednání uvnitř napadené emailové schránky obvykle spočívalo ve čtení zpráv a prohlížení příloh, případně jejich přeposlání na jinou adresu, ve vyhledání a změně přihlašovacích údajů k dané schránce a dalším aplikacím. Pouze jeden z pachatelů vytvořil prakticky plně automatizovaný systém, který v napadených schránkách zachytával pro něho zajímavou poštu (obsahující výrazy jako „platba“, „faktura“ atp.), kterou z napadené schránky dočasně odstranil. Z této dále vyfiltroval emaily sdělující adresátům čísla účtů pro provedení plateb převyšujících určitou částku, se kterými dále pracoval: změnil platební údaje ve svůj prospěch a pozměněný email „vrátil“ původnímu adresátovi (pouze s určitým časovým odstupem), stejně jako pro pachatele jinak nezajímavé emaily, které takto zachytil. Dle své výpovědi tak činil díky softwarové automatizaci prakticky v masovém měřítku, výslovně se zmínil o 20 tis. napadených emailových schránkách, nicméně odsouzen byl za 5 dílčích útoků se způsobenou škodou necelých 700 tis. Kč.

8.5. Některá další data z výzkumu IKSP relevantní pro mládež a mladé dospělé

Nyní podrobnější pohled na některé údaje z výzkumu IKSP. Vzhledem k možnému odstupu mezi zahájením trestné činnosti, dobou spáchání činu a zahájením trestního řízení nelze přesně určit rozhodnou věkovou hranici, neboť sebraná data pracují jednotně s okamžikem zahájení trestního řízení. Proto v této podkapitole uvádím data relevantní pro věkovou

[330] Zaměřeno na zneužití hesla v souvislosti s neoprávněným proniknutím do emailové schránky.
[331] Obojí lze často nalézt na SNS, či se jednoduše zeptat pod smyšlenou záminkou samotného budoucího poškozeného (jeden z pachatelů tak úspěšně učinil).
[332] V jednom z těchto případů pachatel oslovoval náhodně vybrané osoby, jejichž emailové adresy vyhledával na serverech jako bezrealitky.cz atp., způsobená škoda dosáhla téměř 700 tis. Kč.

skupinu až do období mladých dospělých (případně s výslovnou zmínkou k obviněným do 30 let) s vědomím, že zřejmě zahrnují i osoby překročivší kategorii mládeže, nikoliv však výrazně. Jedná se o 1 mladistvého pachatele, 7 pachatelů ve věku blízkém věku mladistvých[333] a 14 mladých dospělých,[334] celkem tedy 22 osob vč. 2 žen (9 %),[335] tzn. zhruba třetinu všech obviněných.

Tab. č. 6: Vybraní obvinění sledovaní při výzkumu IKSP

Věk obviněných	Počet obviněných	Z toho žen
17	1	
18	1	
19	6	1
20	2	
21	3	
22	3	1
23	0	
24	3	
25	3	
26	2	
27	2	1
28	5	1
29	1	
30	1	

Ve všech případech šlo o § 230 TZ, ve 12 pachatelé naplnili i znaky kvalifikované skutkové podstaty – především jednali v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch [11x § 230 odst. 3 písm. a) TZ]. V 10 případech jednali v souběhu (46 %): § 171, 175, 181, 183 (2x), 205 (2x), 209 (3x), 216, 234 (2x), 354, 357 TZ. Dva obvinění byli zproštěni (spolupachatelé), jedno trestní stíhání podmíněně

[333] Tj. osoby zhruba do věku 19 let: „lze v souladu s ustálenou judikaturou a odkazem na § 73 odst. 1 písm. b) a odst. 2 zák. č. 218/2003 Sb., o soudnictví ve věcech mládeže, vycházet z toho, že hranicí, do níž lze hovořit o věku pachatele blízkém věku mladistvých, je devatenáct let, byť v konkrétním případě s ohledem na rozumovou a mravní vyzrálost pachatele není ani tato hranice nepřekonatelná," viz komentář V. Krále k § 41 TZ (Draštík, a další, 2015).
[334] Tj. osoby ve věku zhruba do 25 let (Musilová, 2018), (McDonagh, 2018).
[335] Zastoupení mladých pachatelek se zdá být výrazně nižší než u počítačových trestných činů vůbec, opět však upozorňuji na výhradu statistické významnosti.

zastaveno (§ 307 TŘ). Ze 14 odsouzených pachatelů soud uložil sankci za spáchání výlučně počítačového trestného činu 10 odsouzeným, a to 6x podmíněně odložené odnětí svobody v průměrné délce 6 měsíců (3-10 měsíců) se zkušební dobou průměrně 15 měsíců (12-20 měsíců) a 4x trest obecně prospěšných prací (150 nebo 200 hod bez zkušební doby), ochranné ani výchovné opatření uloženo nebylo. V dané věkové kategorii bylo překvapivě již 9 obviněných (41 %) recidivisty ponejvíce s 1 předchozím pravomocným odsouzením.[336]

Většinou útok směřoval proti fyzické osobě, 6x proti právnické a 2x proti oběma. Pachatelé shodně v 8 případech útočili na majetkovou sféru (z toho 3x za účelem získání prostředků k hazardní hře online) a na osobnost poškozeného (virtuální násilí, z toho 5x byl pachatelem bývalý partner). Nejčastěji znemožnili poškozeným přístup na jejich FB (5x) a email (3x), kde jejich jménem komunikovali a mazali údaje (3x), případně zde poškozené dehonestovali (text a fotografie). Umožnila jim to především důvěra či neopatrnost samotných poškozených vůči vlastním přihlašovacím údajům (9x). Pachatelé využívali nejčastěji FB (8x) a email (7x), jejichž prostřednictvím se majetkově obohacovali (např. vylákávání m-plateb) a jinak komunikovali jménem poškozených, mazali jejich data, manipulovali s intimními fotografiemi poškozených a samotné profily a emailové schránky znepřístupňovali změnou přihlašovacích údajů.

8.6. Shrnutí k výzkumu a publikacím v rámci IKSP

Kapitola uvádí některé dílčí výsledky výzkumu IKSP vztahující se k trestním řízením o počítačových trestných činech, v nichž byla podána obžaloba a došlo k pravomocnému skončení řízení v roce 2015. Vychází z justičních a policejních statistik a analýzy 65 trestních spisů (tj. 92 %), zahrnuje 68 obviněných.

Počet skutků vytrvale stoupá, podobně počet stíhaných, obžalovaných a odsouzených. Zpravidla meritorně rozhoduje okresní soud, a to o přečinu neoprávněného přístupu k počítačovému systému a nosiči informací (§ 14 odst. 2, § 230 TZ). 43 obviněných se mělo jednání dopustit v souběhu s dalším alespoň 1 trestným činem, a to zejména majetkovým nebo ve formě virtuálního násilí. Výlučně za spáchání počítačových trestných činů (27 případů, 18 odsouzení) soudy ukládaly nejčastěji trest odnětí svobody v průměrné délce 6 měsíců, podmíněně odložený se zkušební dobou průměrně 16 měsíců, případně trest obecně

[336] 1 pachatel ve věku 25 let byl pravomocně odsouzen již 5x a 1 pachatel ve věku 19 let dokonce 6x.

prospěšných prací. Pachatelé (z 62 % prvopachatelé) byli ponejvíce ve věku do 29 let (vztaženo k okamžiku zahájení trestního řízení), ženy (22 %) spíše starší. Poškozeny byly fyzické i právnické osoby, nejčastěji jedna, případně 2-5, výjimečně desítky až stovky. Hojně byly zneužívány přihlašovací údaje, k nimž získal pachatel přístup díky neopatrnosti či důvěře poškozeného, naopak minimálně vyžadovalo jednání pachatele větší než běžné uživatelské znalosti ICT. Kromě fyzického přístupu k určitému zařízení pachatelé nejčastěji napadali a zneužívali FB a emailové schránky poškozených. Útočili primárně na osobnost a osobní údaje poškozeného (38x, zejm. kontrola pošty a dehonestace), dále na majetek (22x). Řada souzených jednání byla až na hranici banality, s ohledem na mezinárodní závazky však nelze zmírnit kriminalizaci počítačových trestných činů. V opačném případě by bylo žádoucí rozvolnit trestní represi např. dalším znakem základní skutkové podstaty § 230 TZ (např. v úmyslu získat pro sebe nebo pro jiného neoprávněný prospěch).

Případová studie názorně demonstruje opakující se jev zneužití SNS (zejm. FB) a emailové schránky poškozeného, k nimž pachatel získá přístup díky neopatrnosti poškozeného vůči vlastním přihlašovacím údajům, a význam emailové schránky coby vstupní brány do virtuálního světa poškozeného.

Z výzkumu IKSP lze vyčíst i informace o mladých obviněných, zde do věku 25 let coby mladých dospělých (k okamžiku zahájení trestního řízení), tj. o 20 mužích a 2 ženách. Ti jednali zhruba v polovině případů v souběhu s alespoň 1 dalším trestným činem a 9 z nich bylo již recidivisty. Výlučně za počítačové trestné činy soudy ukládali trest odnětí svobody v průměrné délce 6 měsíců podmíněně odložený se zkušební dobou průměrně 15 měsíců nebo trest obecně prospěšných prací. Útoky směřovaly častěji na fyzické osoby, vyrovnaně na majetkovou sféru i osobnost poškozených (nejčastěji virtuální násilí ze strany expartnera), převážně prostřednictvím FB a emailové schránky.

9. Děti v online prostředí jako oběti i pachatelé

Děti disponují několika vlastnostmi a rysy, které se v průběhu dospívání mění a utváří, ať už jde o ideály, představy o světě, okolí, dospělých, vrstevnících i rodině, zkušenosti nebo postupně nabývané vědění a schopnosti: „jsou v tomto ohledu nezkušení, důvěřiví a otevření. Vývoj možností bezprostřední online komunikace se světem se rozvíjejí v současné době rychleji než jejich psychická připravenost na setkání s možnými nebezpečími. Chybí jim vlastní zkušenost, zkušenost starších je nejen obtížně přenosná, ale také mnoha současným dospělým obdobná chybí zkrátka pro to, že s internetem a mobily nevyrůstali“ (Brandejsová, a další, 2012 str. 3). Děti teprve utváří vlastní identitu, skrze vlastní prožívání a prostřednictvím druhých – rodiny, vrstevníků, okolí – v jejichž reakcích na vlastní jednání zakouší různorodé pocity: úspěch, uznání, respekt atd., ale i jejich protějšky, a jejichž prostřednictvím vytváří vlastní sebeuvědomění. Zkouší hranice toho, co si vůči svému okolí mohou dovolit, aniž by je za to společnost (resp. referenční skupina) odsoudila. Navíc žijí obyčejně „tady a teď“, a tudíž mnohdy ani nedomýšlí důsledky svého jednání nad rámec okamžiku.[337] Zkoušení, posunování a překračování hranic spolu s nezralou identitou a nedomýšlením důsledků děti předurčuje ke zvýšené viktimitě i patří mezi kriminogenní faktory.[338] Problematický prvek ve složitém období dospívání představují SNS, zejm. FB. Zvýšení požadované hranice pro jejich užívání na 15 let (viz kapitola **Zneužití technické stránky internetu**) zřejmě na jejich užívání nic nezmění.[339] Děti postupně nabývají způsobilosti k právním úkonům a deliktní způsobilosti[340] a na SNS se jim otevírá cesta k prakticky neomezenému množství „přátel“, příspěvků a publiku pro vlastní příspěvky, nevyžádaným kontaktům (od náhodných žádostí o přátelství přes spamovací boty po záměrný kontakt a obtěžování) a všudypřítomné reklamě. I když nedojde naplnění závislostní potenciál

[337] Např. budoucí trauma oběti založené chvilkovým pobavením útočníka, který však nezamýšlel nic než právě ono chvilkové pobavení.

[338] Např. podle L. Kohlberga prochází člověk několika stupni morálního vývoje od prvotního vyvarování se trestu v důsledku podřízení se moci až po finální vázanost principy spravedlnosti, rovnosti a respektu k lidskému životu, přičemž pachatelé trestných činů zůstávají na nižších stupních (Válková, a další, 2012 str. 80). Děti v tomto kontextu zatím neměly šanci projít všemi stádii, resp. zvnitřnit a začít se řídit principy vyšších stupňů morálního vývoje.

[339] Daniel Bradbury Dočekal (internetový publicista věnující se mj. SNS) na jednom ze společných školení před několika lety vyslovil tezi, že děti mladší 13 let za sebe nevyplňují onen minimální požadovaný věk, ale „pro jistotu“ se udělají ještě o něco staršími, nejlépe 18 či 19letými.

[340] „Nezletilí nabývají svéprávnosti postupně, a to v rozsahu, jaký odpovídá jejich rozumové a volní vyspělosti“ (Lavický, 2014 str. 197). Určité vodítko lze nalézt v souvislosti s deliktní způsobilostí k náhradě škody dle § 2920 odst. 1 NOZ, podle něhož „nezletilý, který nenabyl plné svéprávnosti, ... nahradí způsobenou škodu, pokud byl způsobilý ovládnout své jednání a posoudit jeho následky,“ přičemž deliktní způsobilost je individuální: „bere se zřetel k individualitě konkrétního člověka (jeho rozumová vyspělost, chápavost, zkušenost, vzdělání, vliv prostředí i rodiny apod.). U nezletilých tak nerozhoduje jejich věk, není stanovena žádná pevná hranice (Hulmák, 2014 str. 1592).

SNS, působí jako Damoklův meč a zároveň zbraň nebývalé síly, jakou neměly k dispozici žádné z předchozích generací (typicky ke kyberšikaně).

Děti jsou nezkušené, naivní, důvěřivé, a tudíž snadno manipulovatelné a zranitelné. Virtuální prostředí se dotýká člověka přímo, bez fyzické bariéry působí bezprostředně na mysl, emoce, sebepojetí. Jejich zranitelnost je zneužitelná zejm. ve spojení se SNS. Bezbřehé přidávání „přátel" na FB relativizuje sebelepší nastavení soukromí na úroveň de facto veřejného profilu s množstvím osobních informací[341] a zároveň označení „přítel" vyvolává mylný dojem blízkého vztahu, umocněný chybějící neverbální komunikací. Komunikace s „přítelem" pak evokuje dojem skutečně blízké a důvěryhodné osoby, která se postupně dozvěděla příliš mnoho intimních podrobností, než aby si dítě připustilo, že by mohlo být dotyčným manipulováno a zneužito. I pokud však dítě obezřetně komunikuje pouze s vrstevníky známými i z reálného prostředí, snadno se splete ve svém úsudku a zveřejní obsah, za nějž se na něj snese vlna odsuzující kritiky.

Vytrvalé využívání nových médií, resp. odklon od fyzických aktivit v reálném prostředí může vést k viktimitě spojené s netholismem, která nabývá na intenzitě zvlášť tehdy, když se k ní připojí citová deprivace (zejm. problémy v rodině nebo s vrstevníky, od kterých hledá dítě únik v kyberprostoru) a ve spojení s naivitou, důvěřivostí a absencí neverbální komunikace téměř předurčuje dotyčného k podlehnutí manipulátorovi. Děti oslabené v reálném prostředí budou zřejmě oslabeny i v online prostředí. Typicky se např. osoba s nízkými sociálními schopnostmi potýkající se s nedostatkem přátel přesune o to více do prostředí SNS doufaje, že se tím její sociální status zlepší. Získá sice zřejmě nové přátele, ale v porovnání s jinak sociálně úspěšnými vrstevníky jich bude zřejmě nepoměrně méně, a tak bude onen rozdíl ještě markantnější. Přílišné přebývání v kyberprostoru vede i k nedostatku racionálního odstupu a realistického pohledu na fyzickou bolest. Dítě tak mnohem snáze podlehne záměrně zákeřným návodům na ublížení sobě či ostatním.

Přirozeně také mnohem častěji přijde do styku s potenciálně ohrožujícím obsahem, kontakty atp., zároveň se s nimi však snáze vyrovnává, zejm. provázejí-li ho virtuálním prostředím jeho rodiče.[342] Mimoto se zdá, že úsilí řady osob a organizací napřené k varování dětí a naučení je

[341] Osobní poměry dítěte, rodinní příslušníci, vrstevníci – to vše figuruje ve zveřejňovaných příspěvcích, vč. fotografií i videí a tzv. „označení osoby", tj. rozpoznání osoby na základě dříve známé fotografie na FB (Dočekal, 2015).

[342] Zdá se, že méně újmy pociťují děti, které se aktivně brání (např. mazání nechtěných zpráv a blokace odesílatele). Naproti tomu děti, jejichž rodiče využívají internet jen sporadicky, mají tendence spíše k pasivní resistenci, která však není tak účinná (d'Haenens, a další, 2013).

pracovat bezpečně s online technologiemi snad přináší výsledky, protože ač internet využívají stále více, pociťování újmy spojené s online prostředím úměrně tomu neroste (eukidsonline.net str. 19). Děti využívají řadu strategií, které jim pomáhají vyrovnat se s případnou újmou způsobenou v online prostředí, resp. pracovat s online prostředím tak, aby skrze něj újmu nepociťovaly či ji alespoň minimalizovaly (d'Haenens, a další, 2013). Předně s někým hovoří o tom, s čím se setkaly, přičemž to bývají spíše vrstevníci než rodiče, a to z obav z kritiky a ztráty soukromí a dosavadní svobody (eukidsonline.net str. 20), a činí další kroky (blokování odesílatele nevyžádaných zpráv, mazání nevítaných komentářů atp.).

Dětem jako obětem věnuje zvláštní pozornost trestní zákon (TZ, ZSVM a TOPO, viz § 110 TZ), a to kromě příslušných základních skutkových podstat trestných činů v podobě zvlášť i obecně přitěžujících okolností spáchání trestného činu ke škodě dítěte (např. § 144 odst. 1 a 2 a § 42 písm. h) TZ]. Dále např. zák. č. 45/2013 Sb., o obětech trestných činů a o změně některých zákonů (zákon o obětech trestných činů), přiznává dětem status tzv. zvlášť zranitelné oběti (§ 2 odst. 4), což jim zaručuje oproti „běžným“ obětem určité zvýhodnění zejm. co do procesních práv.

Některé aspekty online prostředí působí nejen jako viktimizační, ale zároveň i kriminogenní faktory, zejm. nezkušenost, jen postupná socializace (vč. vytváření vlastní identity a vztahu ke společnosti), lpění na uznání ze strany ostatních, vědomé i nevědomé překračování hranic a pravidel, nedomýšlení důsledků a orientace na přítomnost, SNS s potenciálně ohromným publikem a rychle se šířícím obsahem (i bez prvotního zájmu původce). Dále anonymita (a tedy snížení sociálního tlaku na „správné“ chování), absence neverbální komunikace (útočník nevidí bezprostřední dopad svého chování i jednání).[343] Při jednání řady osob více méně v souladu i zpočátku neškodný žert snadno roztočí prohlubující se kruh napadání, protože „to dělají i ti druzí,“ podobně jako při chování v davu (Le Bon, 2016). Opomenout nelze ani určitou averzi vůči normám a autoritám v průběhu dospívání a žebříček hodnot, který se teprve utváří a současně relativizuje setkáváním s odlišnými kulturami v globálním kyberprostoru – problematické zejm. pro druhou generaci imigrantů (Kriminalita mladistvých imigrantů, 2013). Dětem je vlastní také určitá dravost,[344] k čemuž se přidávají sociální vzory chování přebírané mj. z TV pořadů zdánlivě zobrazujících reálnou každodennost, ve skutečnosti však zaměřených na konfliktní situace a vztahy (typicky reality show). To

[343] S rozlišením chování coby bezprostřední reakce bez hlubšího rozmyslu a jednání coby uváženého aktu (Sokol, 1998 str. 74).
[344] Mnohokrát opakovanými slovy různých učitelů: „děti jsou jako predátoři – jak ucítí slabost, využijí ji.“

umocňuje vliv SNS, kde uživatelé zveřejňují zpravidla příspěvky, které jim připadají zajímavé, šokující, chytlavé, zábavné atp. a kterými se chtějí prezentovat navenek. Vytrácí se proto běžná každodenní všednost a řešení „obyčejných" malých problémů a situací. S trávením stále více času online se ztrácí fyzický kontakt s realitou, resp. fyzickou bolestí a reálnými možnostmi lidského těla. I zde tak snadno přeroste zdánlivě nevinný žert v nezamýšlené důsledky (např. navedení druhého k sebepoškozujícímu jednání bez vědomí skutečných následků).[345]

Za zmínku stojí ještě pokles evidované kriminality v posledních letech na národní i celoevropské úrovni, provázený úvahami nad možnými příčinami: zejm. změnami ve statistické evidenci[346] a přesunem kriminality do online prostředí (dotýkající se i dětských pachatelů). Ti na jedné straně tráví více času online, a nikoliv ve veřejném prostoru, a dostatečně se zabaví např. hraním her nebo přítomností na SNS,[347] na druhou stranu případní pachatelé se dnes možná dopustí trestné činnosti spíše online, neboť to prostředí je jim vlastní, není zde taková kontrola jako např. nad veřejným prostorem a s vysokou latencí se nese relativně malé riziko odhalení.

Dětem jako pachatelům se věnuje zejm. ZSVM obsahující normy hmotněprávního i procesněprávního charakteru. Zahrnuje také ustanovení vztahující se k řízení ve věcech dětí mladších 15 let, kdy nelze hovořit o trestném činu,[348] resp. provinění (§ 6 odst. 1 ZSVM), a nelze tedy ani případně vyslovit vinu dítěte mladšího 15 let (Šámal, a další, 2011 str. 823).[349] Přesto přichází v úvahu uložení některého z vybraných opatření k nápravě (§ 93 ZSVM) soudem pro mládež [§ 2 odst. 2 písm. d) ZSVM] postupujícím podle občanského soudního řízení (§ 96 ZSVM), tj. podle zák. č. 292/2013 Sb., o zvláštních řízeních soudních, coby řízení ve věcech péče soudu o nezletilé dítě [§ 466 písm. m)].[350] Naopak u starších „dětí" trestní zákon pracuje i s tzv. pachateli ve věku blízkém věku mladistvých [§ 41 písm. f) TZ], kterým přičítá věk v době spáchání činu do 19, příp. až cca 21 let jako obecně polehčující okolnost

[345] Za zdařilý počin lze považovat knihu Fyzika superhrdinů přibližující reálné a „virtuální" fyzikální vlastnosti (Kakalios, 2018).
[346] Např. co se eviduje ve spojení s odměnami za dostatečnou objasněnost atp., k problémům se statistickými výkazy Ministerstva spravedlnosti ČR viz např. (Válová, 2018).
[347] Nezbývá tedy „dostatek času na hlouposti", což představuje jednu z proměnných (involvement) hrajících roli v teorii sociálních vazeb T. Hirschiho (Válková, a další, 2012 str. 96).
[348] Z důvodu nenaplnění všech znaků trestného činu – chybějící obecný znak věku (§ 25 TZ), nemluvě o nanejvýš pravděpodobně nedostatečné rozumové a mravní vyspělosti (§ 5 odst. 1 ZSVM).
[349] Spodní věková hranice, od kdy již může přicházet v úvahu řízení ve věcech trestně neodpovědných dětí, stanovena a priori není, obecně se má však za to, že by jí mělo být období zhruba od 12 let, v závislosti na konkrétním dítěti a jeho rozumovém a mravním vývoji ještě posunutelná případně až k samému počátku školní docházky (Šámal, a další, 2011 str. 701).
[350] Blíže k tomu viz komentář M. Hrušákové k § 96 ZSVM (Hrušáková, a další, 2015).

(Šámal, 2012 str. 548). Za zmínku stojí též tzv. podmíněná (relativní) příčetnost, tedy rozumová a mravní vyspělost mladistvého (§ 5 dost. 1 ZSVM), jejíž případná nedostatečnost zakládá speciální důvod nepříčetnosti (§ 26 TZ),[351] resp. nedostatečnost alespoň jedné z jejích složek, tedy „postupného individuálního nabývání schopnosti pojmového myšlení" (rozumová vyspělost) nebo „osvojení norem chování, které platí v daném období rozvoje společnosti, a jejich přeměna na osobní a morální kvality, tedy vytváření vlastního hodnotového systému, který je v určitém vztahu k hodnotám společnosti, v níž žije" (Šámal, 2012 str. 42).

Co se týče deliktní odpovědnosti za přestupek, viz zák. o odpovědnosti za přestupky a řízení o nich, pachatelem může být pouze osoba dovršivší věk 15 let (§ 18). Řízení o přestupku mladistvého, tj. osoby dovršivší věk 15 let a nepřekročivší 18 let (§ 55) se koná podle Hlavy IX., která mj. snižuje horní hranici sazby pokuty na polovinu, nejvýše 5.000. Kč (§ 57).

Při způsobení škody nezletilým, který nenabyl plné svéprávnosti, mohou nastat v zásadě 4 různé situace co do osoby odpovědné za její náhradu v závislosti na deliktní způsobilosti škůdce a (ne)zanedbání povinného dohledu[352] nad ním (§ 2920 § 2921 NOZ): 1. škůdce je s ohledem na konkrétní situaci deliktně způsobilý a dohled nad ním byl zanedbán → odpovídají škůdce a zanedbavší osoba za škodu společně a nerozdílně; 2. škůdce je deliktně způsobilý a dohled zanedbán nebyl → za škodu odpovídá sám škůdce; 3. škůdce není deliktně způsobilý a dohled byl zanedbán → za škodu odpovídá sama zanedbavší osoba; 4. škůdce není deliktně způsobilý a dohled nebyl zanedbán → škoda jde k tíži poškozeného. Výjimka z posledního případu může nastat pouze v případě výraznějšího majetkového nepoměru mezi škůdcem a poškozeným ve prospěch škůdce, kdy soud může uložit povinnost k náhradě škody i deliktně nezpůsobilému škůdci, viz § 2920 odst. 2 NOZ (Hulmák, 2014, str. 1593).

V roce 2017[353] bylo pravomocně odsouzeno za spáchání počítačového trestného činu, resp. provinění 6 mladistvých, tj. cca 5 % pachatelů fyzických osob (oproti cca 2,2% podílu mladistvých pachatelů na kriminalitě vůbec). Uloženo bylo 4x trestní opatření odnětí svobody podmíněně odložené na zkušební dobu, 1x bylo podmíněně upuštěno od uložení trestního opatření (§ 14 ZSVM) a 1x uloženo výchovné opatření v podobě povinnosti podrobit se probačnímu programu (§ 17 ZSVM). Mezi oběťmi počítačových trestných činů byly 4 osoby

[351] Blíže k tomu viz (Šámal, 2012 str. 38). Odlišný názor zaujímá např. J. Jelínek považující ji za „samostatný obligatorní znak subjektu provinění, který stojí vedle příčetnosti a věku" (Jelínek, 2017 str. 214).
[352] Osobou povinovanou dohledem jsou v prvé řadě rodiče (§ 858 NOZ), v době vyučování pak škola (§ 881 NOZ), viz (Hrušáková, a další, 2014 str. 917).
[353] V roce 2016 nebyl z hlediska počítačových trestných činů pravomocně odsouzen žádný mladistvý a statistická data za rok 2018 dosud (leden 2019) nejsou k dispozici, viz CSLAV (Ministerstvo spravedlnosti ČR).

mladší 18 let, tj. cca 12 % (oproti jejich cca 30% podílu mezi oběťmi vůbec).[354] Lze tedy konstatovat, že mládež se stává obětí počítačových trestných činů méně často než zbytek populace, ovšem s výhradou pravděpodobně vysoké latence: spíše vlastní řešení namísto podání trestního oznámení (např. blokace útočníka), nevědomost oběti (neví např. o zneužití profilu na SNS), chybná kvalifikace jednání bez souběhu s počítačovým trestným činem.

9.1. Shrnutí k dětem v online prostředí coby obětem i pachatelům

Mládež je nezkušená, naivní, důvěřivá, a tudíž snadno manipulovatelná a zranitelná. Nedostatek vlastních a nepřenositelnost zkušeností starších osob, jen postupná socializace, potřeba uznání od sociálního okolí, zkoušení a posunování hranic jednání, nedomýšlení důsledků, omezení neverbální komunikace, hojné využívání SNS a nadměrné trávení času online představují hlavní viktimizační i kriminogenní faktory. Coby potenciální oběti jsou ohrožené zejm. osoby ohrožené i v reálném prostředí (závislost, citová deprivace, nedostatek sociálních dovedností atp.). Nejen ony se však postupně učí s újmami způsobenými v online prostředí vypořádat a eliminovat je. Na děti jako oběti a poškozené myslí trestní zákon některými skutkovými podstatami i obecně a zvlášť přitěžujícími okolnostmi, dále pak zákon o obětech trestných činů (status zvlášť zranitelné oběti).

K mládeži coby pachatelům v online prostředí přispívá ještě dostupná anonymita a vysoká latence kriminality online, averze vůči normám a autoritám v období dospívání, relativizovaný žebříček hodnot, pochybné vzorce chování a nereálná představa každodennosti umocněná SNS, zároveň se ale snáze zabaví. Mládeži coby pachatelům se věnuje zejm. ZSVM (vč. podmíněné příčetnosti), dětem mladším 15 let pak ještě zák. o zvláštních řízeních soudních a pachatelům ve věku blízkém věku mladistvých TZ. I osoby mladší 18 let pak mohou navzdory nenabytí plné svéprávnosti odpovídat za přestupek (zák. o odpovědnosti za přestupky a řízení o nich) a způsobenou škodu (NOZ), případně spolu s osobou zanedbavší povinný dohled nad nezletilým. Na samotných počítačových trestných činech se mladiství pachatelé podílejí více než na kriminalitě vůbec, naopak mezi oběťmi figuruje mládež méně často.

[354] V roce 2015, který sledoval výzkum IKSP, byla data podobná, resp. podíl mladistvých obětí počítačových trestných činů ve výši cca 19 % oproti cca 30% podílu na obětech vůbec.

10. Sexuální vykořisťování dětí

Sexuální vykořisťování dětí nabývá v kyberprostoru rozmanitých podob, včetně dětské pornografie, sextingu (vč. dětské prostituce) a kybergroomingu. Společným jmenovatelem je internet coby umožňující/usnadňující komunikační platforma a SNS coby zdroj intimního obsahu a nevyžádaných kontaktů.

10.1. Pornografie a děti online[355]

S přirozeným psychickým vývojem dochází i k sexuální identifikaci a zrání. Pokud je sex při fyzickém i psychickém dospívání konzumován přiměřeně, přispívá ke vzniku a rozvoji zdravé osobnosti, online je však dostupný i v nejdrsnějších podobách. Nutno poukázat na rozdílné vnímání pornografie ze strany práva (prostá, dětská a tvrdá) a psychologie (soft, hard a deviantní). Soft pornografie (měkká – vše erotické mimo hard a deviantní pornografii), neškodná v jakémkoliv věku, podněcuje představivost, rozvíjí fantazii a přispívá ke zdravému sexuálnímu vývoji. Naopak nevhodná pornografie (hard a často i deviantní)[356] a konzumování pornografie v nevhodném věku nebo nevhodném prostředí mohou vést k rizikovému sexuálnímu chování mládeže,[357] vč. frustrace z vlastních aktivit v důsledku zcela nerealistických představ, hledání náhradních sexuálních objektů (např. dětí) nebo rozvoje sexuálních deviací aj.

Výskyt pornografie je bohatý a pestrý, dostupný i zdarma a v různých podobách (foto, video, text, animace). Pornografický web bývá zřejmý na první pohled – obvykle na jeho obsah upozorňuje vstupní stránka, v některém případě se rovnou zobrazí i pornografické obrázky. Obvykle se považuje za dostačující ochranu a označení, umístí-li provozovatel na web před zobrazením samotného obsahu varování (tzv. disclaimer) o umístění obsah přístupného až od 18 let, případně např. přidá nutnost uvedení věku uživatele a v situaci, kdy se tento ohlásí jako osoba mladší 18 let, obsah stránky se nezobrazí. Takto zabezpečený web lze pak z hlediska práva považovat za „dětem nepřístupný“, byť na něj děti de facto vstoupit mohou.[358]

[355] Kapitola vychází z publikovaných textů (Brandejsová, a další, 2012), (Lukášová, 2012) a (Vybrané navrhované změny trestního zákoníku - § 192, 193b TZ, 2013).
[356] Hard coby tvrdá pornografie (nikoliv z hlediska práva), přímé zobrazení sexuálního aktu vč. detailů, a deviantní - přímé zobrazení sexuálních úchylek běžně se nevyskytujících, např. dětská pornografie.
[357] Nevhodný věk se odvíjí od sexuálního zrání jedince a tomu přiměřeným praktikám (např. dotyky vlasů - „francouzské“ líbání - masturbace a vlastní sexualita jako součást osobní identity). Nevhodné prostředí postrádá intimitu (např. párty, přítomnost a komentáře „zkušenějších“).
[358] Obdobně jako mohou např. vstoupit do obchodu s erotickými pomůckami navzdory nápisu zakazujícímu

V opačném případě by se provozovatel webu mohl dopustit přečinu šíření pornografie, neboť na místě, které je dětem přístupné (web bez zakázaného přístupu dětem), jinak zpřístupňuje elektronické pornografické dílo [§ 14 odst. 1, § 191 odst. 2 písm. b) TZ].[359] Nabídka pornografie online je široká i mimo weby na ni zaměřené – např. s použitím vyhledávače.[360] Na vzniku, šíření a zveřejňování (dětské) pornografie se hojně podílejí i samotné děti, především teenageři v prostředí SNS. Naopak pornografie v dark webu je dostupná zpravidla pouze uzavřenému okruhu osob, do něhož lez vstoupit teprve po zaslání dosud nezveřejněné pornografie dané kategorie, což značně ztěžuje jakoukoliv infiltraci (Bartlett, 2015).

Děti se s pornografií setkávají poměrně hojně,[361] četnost roste s věkem. S online zdroji pornografie se v roce předcházejícím výzkumu setkalo necelých 30 % českých dětí (s pornografií vůbec se setkalo cca 45 % dětí), chlapci jen o málo častěji než dívky. Z toho v důsledku setkání se se sexuálním obsahem online pociťuje újmu pouze necelá čtvrtina českých dětí (oproti celoevropské třetině), tzn. méně než 10 % českých dětí. Nejčastěji narazí na sexuální obsah v podobě tzv. pop-up oken, dále pak na videokanálech jako Youtube a SNS a většinou jde o obrázky nahých osob, v méně případech potom zobrazení sexu nebo intimních partií (o tvrdou pornografii jen minimálně). Není proto třeba se kontaktu dětí s pornografií přehnaně obávat, ale zároveň situaci nebagatelizovat a věnovat jí náležitou pozornost (Tsaliki, a další, 2014).

Pornografické dílo[362] není v současnosti v trestním zákoně definováno, lze tedy pouze dovozovat, co jím je a co není, a to i s ohledem na určitou hladinu morálního vývoje uznávanou společností a na to, co ještě společnost považuje za přijatelné - odvíjí se od stávajícího převažujícího morálního cítění. Posuzujeme ovšem dílo jako takové, nikoliv ve vztahu k jeho „uživatelům“ či adresátům.[363] Odborná veřejnost se shoduje na tom, že „pornografické dílo lze charakterizovat tím, že vtíravým způsobem podněcuje sexuální pud,

---

vstup osob mladších 18 let umístěnému na dveřích. Zpřístupňování je definováno jako „jednání, kterým je umožněno, aby se s pornografickým dílem mohly seznámit děti“ (Šámal, 2012 str. 1885), je proto klíčové, zda úmysl případného pachatele kryje i tuto skutečnost, tedy zda případný pachatel chtěl, aby bylo pornografické dílo zpřístupňováno dětem, nebo věděl, že se tak může stát, a pro ten případ s tím byl srozuměn (§ 15 TZ).

[359] K místu dětem přístupnému a jinému zpřístupňování viz (Šámal, 2012 str. 1885).

[360] Obsah se liší v závislosti na použitém vyhledávači: např. Google.com nabídne po zadání hesla „kreslená pornografie“ pestrou paletu obrázků, naproti tomu Seznam.cz jen několik málo výsledků (navíc s apriorním nastavením „Skrýt hanbaté“).

[361] Údaje zde uvedené se vztahují zpravidla k dětem ve věku 9-16 let a jejich setkáním s pornografií v roce předcházejícím výzkumnému šetření a vychází z kapitoly 5. Seeing Sexual Images (Livingstone, a další, 2011), kde lze nalézt i další informace.

[362] Výraz „dílo“ je z hlediska trestního zákona širší než přesně vymezené dílo autorské dle autorského zákona.

[363] K pojmu (dětská) pornografie srov. usnesení Nejvyššího soudu ze dne 28. 12. 2004 sp. zn. 7 Tdo 1077/2004-I nebo usnesení Ústavního soudu ČR ze dne 19. 4. 2004, sp. zn. IV. ÚS 606/03 a viz bod 2. komentáře R. Fremra k § 192 TZ (Draštík, a další, 2015).

překračuje podle převládajících názorů ve společnosti uznávané hranice sexuální slušnosti, uráží neakceptovatelným způsobem cit pro sexuální slušnost“ (Šámal, 2016 str. 629).[364] Zjednodušeně řečeno: „za pornografické dílo se považuje takové dílo, jehož jediným účelem je vyvolat (zvyšovat) sexuální vzrušení“ (Jelínek, 2008 str. 249).

Dětská pornografie je pak taková, která zobrazuje nebo jinak využívá dítě (tj. dle § 126 TZ osobu mladší 18 let) nebo osobu, jež se jeví být dítětem. Půjde o „snímky obnažených dětí v polohách vyzývavě předvádějících pohlavní orgány za účelem sexuálního uspokojení, dále pak snímky dětí zachycující polohy skutečného či předstíraného sexuálního styku s nimi ... závěr o pornografickém charakteru díla nelze bez dalšího dovozovat jen z toho, že jsou za účelem uspokojení osob trpících sexuální deviací (tj. v tomto případě osob, pro které jsou sexuálně atraktivní nedospělé osoby) zpřístupňovány takovými prostředky, které tyto osoby vyhledávají.“[365] Až do 30. listopadu 2011 dětská pornografie odkazovala pouze na takovou pornografii, která zobrazuje nebo jinak využívá dítě, ale nikoliv již osobu jako dítě pouze vypadající, avšak s ohledem na evropské právo[366] trestní zákon považuje nyní za dětskou pornografii i takovou, která zobrazuje „osobu, jež se jeví být dítětem.“ Zahrnuje proto i případy neexistujícího, ale realisticky znázorněného dítěte – „vyobrazení, které vzniklo zcela pomocí počítače. S ohledem na použití slova ´osoba´ může být sporné, zdali i pouhé fantazijní vyobrazení neexistujícího dítěte je vyobrazením ´osoby´“ (Šámal, 2012 str. 1892).[367] Navíc není ani zřejmé, o jak moc realistické znázornění by mělo jít, počínaje animacemi téměř k nerozeznání od skutečné nafilmované osoby přes kreslené a zjevně animované postavy až po humanoidní bytosti s rysy „dítěte“.[368] Takové pojetí chápe jako objekt trestného činu výroby a jiného nakládání s dětskou pornografií nejen zájem společnosti na ochraně mravního vývoje dětí a jejich ochraně před sexuálním zneužíváním, ale také zájem na mravních hodnotách společnosti, která dětskou pornografii považuje za škodlivou.

[364] Důvodová zpráva hovoří o díle, které „zvláště intenzivním a vtíravým způsobem zasahuje a podněcuje samotný sexuální pud. Současně takové dílo hrubě porušuje uznávané morální normy společnosti a vyvolává pocit studu,“ viz komentář k § 188-190 (Vláda ČR, 2008).

[365] Srov. usnesení Nejvyššího soudu ze dne 28. 12. 2004, sp. zn. 7 Tdo 1077/2004.

[366] Zákonem č. 330/2011 Sb. provedená implementace rámcového rozhodnutí Rady EU 2004/68/SVV ze dne 22. prosince 2003 o boji proti pohlavnímu vykořisťování dětí a dětské pornografii, která požaduje kriminalizaci pornografie zobrazující mj. „skutečnou osobu se vzhledem dítěte“ nebo „realistické znázornění osoby se vzhledem dítěte“ [čl. 1 písm. a) bod ii) a iii)]. Rámcové rozhodnutí tak jde ještě dále než CoC požadující kriminalizaci (mimo jiné) kromě pornografie zobrazující „osobu, jež se zdá být nezletilou“ i „realistické zobrazení představující nezletilou osobu“ [čl. 9 odst. 2 písm. b) a c)].

[367] Právní řád ČR rozlišuje osoby fyzické a právnické, dále se lze setkat s osobami veřejného práva a soukromého práva, avšak nikdy s osobou coby pouhým vyobrazením.

[368] Zůstává zde navíc stále určitý prostor pro případné použití takové „quasi dětské“ pornografie zejm. ve vztahu k léčbě pedofilů, nebo spíše ve vztahu k tlumení jejich sexuálních potřeb (Jílková, 2007), (Herczeg, 2008).

Kromě dětské pornografie trestní zákon zná ještě tvrdou pornografii, tj. takové „pornografické dílo, v němž se projevuje násilí či neúcta k člověku, nebo které popisuje, zobrazuje nebo jinak znázorňuje pohlavní styk se zvířetem“ (§ 191 odst. 1 TZ). Veškerá ostatní pornografie je tzv. prostá a lze s ní libovolně nakládat vyjma zpřístupňování dítěti (§ 191 odst. 2 TZ) a zapojení dítěte do její výroby (§ 193 TZ).

Dne 1.8.2014 nabyl účinnosti zák. č. 141/2014 Sb., který mj. vložil do § 192 TZ nový odst. 2 a zavedl nový § 193a a 193b,[369] čímž implementoval směrnici Evropského parlamentu a Rady 2011/36/EU ze dne 5. dubna 2011 o prevenci obchodování s lidmi, boji proti němu a o ochraně obětí a směrnici Evropského parlamentu a Rady 2011/93/EU ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii. Kromě zavedení nové skutkové podstaty novela zároveň snížila výši horní hranice trestu odnětí svobody u § 192 odst. 1 TZ ze 2 let na 1 rok, a to z důvodu vzájemné proporcionality trestních sazeb u § 192 odst. 2, § 193a odst. 1 a § 193b TZ, jejichž společenskou škodlivost lze pokládat za obdobnou. § 192 odst. 2 TZ nyní zní „stejně bude potrestán ten, kdo prostřednictvím informační nebo komunikační technologie získá přístup k dětské pornografii.“ Důvodová zpráva uvádí pouze nezbytnost implementace čl. 5 odst. 3 směrnice Evropského parlamentu a Rady 2011/93/EU. Podle něho se „vědomé získávání přístupu k dětské pornografii prostřednictvím ICT trestá odnětím svobody s horní hranicí trestní sazby nejméně jeden rok.“ Novelizované znění jde tak částečně nad rámec pouhé implementace, když namísto „vědomého získávání přístupu“ k dětské pornografii prostřednictvím ICT postihuje již osamocené „získání přístupu k dětské pornografii“ použitím ICT. Z faktického hlediska tak může jít o ojedinělý přístup k dětské pornografii, avšak s ohledem na svou společenskou škodlivost lze považovat dokonavý vid zcela na místě, a to bez ohledu na to, zda pachatel k dětské pornografii přistupuje opakovaně či nikoliv.

Objektem druhého odstavce § 192 TZ je ochrana dětí před pohlavním vykořisťováním a ochrana mravních hodnot společnosti považující dětskou pornografii za škodlivou bez dalšího. Usiluje proto o zamezení či omezení šíření dětské pornografie pomocí nových technologií a internetu (s ohledem na technologický pokrok se šíří ve výrazně větší míře, k čemuž zároveň přistupují problémy se znepřístupněním takového obsahu na internetu, a proto je na místě přísnější postih jednání prostřednictvím těchto technologií). Objektivní stránka spočívá v použití ICT v úmyslu získat přístup k dětské pornografii. Orgány činné

[369] Pochopitelně s příslušnými legislativně technickými úpravami.

v trestním řízení by ji však měly vykládat spíše restriktivně, s ohledem na šíři uplatňování ICT v současném každodenním životě.[370] Pachatelem může být kdokoli, nicméně s ohledem na zásadu, že nemůže být trestným ten, k jehož ochraně je ustanovení určeno, patrně nemůže být trestně odpovědný za spáchání tohoto přečinu mladistvý v případě, že on sám je aktérem zobrazeným v dětské pornografii, k níž se snaží prostřednictvím ICT získat přístup. Z hlediska subjektivní stránky novelizované znění § 192 odst. 2 TZ vyžaduje zavinění ve formě úmyslu. Pachatel proto musí k naplnění znaků této skutkové podstaty na straně jedné úmyslně použít ICT, na straně druhé tak vědomě získat přístup k dětské pornografii. Vzhledem k tomu, že je v§ 192 odst. 2 TZ modifikována subjektivní stránka (úmysl získat přístup k dětské pornografii) i objekt (mj. snaha omezit šíření dětské pornografie prostřednictvím nových technologií a internetu) a jiným jednáním lze naplnit i znaky objektivní stránky, jedná se o druhou základní skutkovou podstatu trestného činu výroby a jiného nakládání s dětskou pornografií. Protože za takové jednání lze uložit trest odnětí svobody s horní hranicí trestní sazby jeden rok, jedná se o přečin (§ 14 odst. 2 TZ).

Skutková podstata trestného činu výroby a jiného nakládání s dětskou pornografií dle§ 192 odst. 2 TZ by mohla být vhodně použita např. i při postihu kybergroomingu, při němž pachatel požaduje po vybrané osobě ji zobrazující pornografické materiály (je-li si vědom komunikace s dítětem). V úvahu pak přichází i souběh s trestnými činy ohrožování výchovy dítěte, svádění k pohlavnímu styku, zneužití dítěte k výrobě pornografie, výroby a jiného nakládání s dětskou pornografií a zřejmě i šíření pornografie, neboť jedním ze způsobů lákání pornografického materiálu bývá předchozí zaslání jiného pornografického díla dítěti, po němž je materiál vyžadován [§ 201, 202, 193, 192 odst. 1, příp. odst. 3 a § 191 odst. 2 písm. a) TZ]. Zřejmě však nebude možný jednočinný souběh přečinu výroby a jiného nakládání s dětskou pornografií dle§ 192 odst. 2 TZ s trestným činem svádění k pohlavnímu styku (§ 202 TZ) v případě, že pachatel bude např. po dítěti požadovat za úplatu jeho obnažování se před webovou kamerou za účelem svého uspokojení a zároveň s tím, že si z takového vystoupení pořídí záznam, neboť v takovém případě lze zahrnout jeho jednání pod skutkovou podstatu trestného činu výroby a jiného nakládání s dětskou pornografií dle

[370]K naplnění znaků této skutkové podstaty mohou nastat rozličné situace. Zřejmě bude naplněna beze všech pochybností např. tehdy, když pachatel navštíví webovou stránku s dětskou pornografií za účelem stažení jejího obsahu. Sporné však může být její uplatnění v případě, kdy si např. zájemce pokusí objednat prostřednictvím e-shodu papírový časopis s dětskou pornografií nebo zavolá prostřednictvím mobilního telefonu kamarádovi s žádostí o zapůjčení videokazety s dětskou pornografií atp. Objektem skutkové podstaty výroby a jiného nakládání s dětskou pornografií dle § 192 odst. 2 TZ je mj. snaha zamezit či omezit šíření dětské pornografie pomocí nových technologií a internetu, jak je uvedeno výše, ovšem v posledních dvou naznačených případech už lze pochybovat, zda bylo dosaženo takového stupně společenské škodlivosti, jaký se váže k možnostem využití ICT.

§ 192 odst. 3 TZ v souběhu s trestným činem svádění k pohlavnímu styku (nebude-li si dítě vědomo, že se účastní výroby dětské pornografie), přičemž přečin výroby a jiného nakládání s dětskou pornografií dle§ 192 odst. 2 TZ bude zřejmě fakticky konzumován.

10.2. Sexting[371]

Při online komunikaci mládež často posílá a sdílí sexuálně laděné zprávy a vlastní intimní obrázky nebo videa. Sexting je lákavý zejm. kvůli touze po sebeprezentaci a kladné odezvě okolí (zvlášť v dospívání),[372] dále pak i snaze o přivýdělek.[373] Sexting tak může působit pozitivně na vnímání vlastní sexuality a sebepojetí, také je ale může naopak deformovat. Nelze vynechat ani vliv vrstevnické skupiny a běžné normy chování v jejím rámci (sexting jako norma či naopak deviace). Zasílání a zveřejňování vlastních intimních materiálů představuje pro mládež značné riziko, neboť nad zdigitalizovaným odeslaným obsahem zcela ztrácí kontrolu: nelze zajistit, jak s ním příjemce naloží (např. smaže nebo zveřejní), kdy tak učiní (ihned nebo i po letech) ani za jakým účelem (např. pomsta nebo vydírání). Někteří pak hovoří o následné psychologické a emoční úzkosti až sebevražedných sklonech (Kopecký, a další, 2017 str. 6).

České děti v 11-16 letech patří v rámci Evropy mezi obvyklejší aktéry sextingu: v roce předcházejícím výzkumu jich 20 % sexting obdrželo a 10 % samo odeslalo, přičemž z toho jen necelých 20 % obdrževších (tj. cca 4 % celkově) se tím cítilo obtěžováno (s minimálními rozdíly mezi chlapci a dívkami), a to zhruba v polovině případů po dobu v řádech dní až měsíců.[374] Dotyční především dostávali sexuálně laděné zprávy a sami je odesílali, již méně jich vidělo nějaký sexuální akt a výrazně méně pak bylo požádáno o hovor na takové téma nebo o zaslání vlastních intimních fotografií či videa. Nejčastěji se tak stalo v rámci instant messagingu nebo na SNS, dále pak v chatovací místnosti, v několika případech i ve spojení s počítačovou hrou. Blíže k tomu viz (Livingstone, Haddon, Görzig, & Ólafsson, 2011),

[371] kapitola vychází z (Brandejsová, a další, 2012) a (Lukášová, 2012).
[372] Původci zpravidla „posílají do světa“ jen takové, na kterých vypadají dle svého názoru skutečně dobře (zejm. z hlediska své referenční skupiny).
[373] Typicky v podobě kreditu do mobilního telefonu výměnou za zaslání vlastní fotografie či videa, a to až na úroveň dětské prostituce. Dle informací operátorů a Policie ČR, jež zazněly opakovaně na různých odborných konferencích věnovaných mj. problematice dětské pornografie, se liší jednání dle pohlaví: dívky vyžadují častěji úplatu, chlapci jednají spíše pod dojmem vzájemné výměny s (zdánlivě) opačným pohlavím.
[374] Obyčejně si pak někomu svěřily (60 %), nejčastěji některému z rodičů (téměř 40 %) nebo kamarádovi (30 %), zprávy od odesílatele smazaly a do budoucna zablokovaly (40 %), změnily vlastní kontaktní údaje (25 %) nebo dokonce přestaly na čas vůbec používat internet.

kapitola Sending / Receiving Sexual Messages. Čeští aktéři v 8-17 letech[375] nejčastěji chtějí upoutat pozornost a flirtují (60 % dívek, 50 % chlapců). Relativně často také reagují na žádost přítele/kyně (35 % dívky, 30 % chlapci) či někoho cizího (téměř 30 % dívek, 20 % chlapců). Kolem 5 % dětí své intimní materiály sdílí i na SNS. Zhruba v polovině případů aktéři zasílají sexting prostřednictvím aplikace Snapchat[376] (Kopecký & Szotkowski, Sexting a rizikové seznamování českých dětí v kyberprostoru. Výzkumná zpráva, 2017).

Pokud sextingový materiál splňuje kritéria pornografie a směřuje k adresátovi mladšímu 18 let, odesílatel může naplnit skutkovou podstatu trestného činu šíření pornografie [§ 191 odst. 2 písm. a) TZ], neboť pachatel přenechává pornografické dílo dítěti: „přenecháváním se již pornografické dílo skutečně dostává do rukou dítěte, které se tak může s pornografickým dílem seznámit“ (Šámal, 2012 str. 1885). Jestliže pachatel „pouze“ zašle osobě mladší 18 let soubor s pornografickým dílem, který je k jeho vnímání nutno nejprve otevřít (tedy vyvinout určitou aktivitu ze strany dítěte), lze takové jednání posoudit jako nabídnutí pornografického díla dítěti: „nabízením se rozumí jakékoli předložení pornografického díla, které má za cíl, aby si je dítě převzalo“ (Šámal, 2012 str. 1885). Při rozlišení znaku „přenechává“ a „nabízí“ tak u sextingu nutno rozlišit, zda se pornografické dílo adresátovi automaticky zobrazí či nikoliv (a zda je tato skutečnost kryta zaviněním pachatele ve formě úmyslu) – zda pachatel např. nabízí obrázek jako přílohu nebo přenechává v těle mailu. O trestný čin se ovšem jedná samozřejmě za předpokladu, že jednání pachatele dosáhlo natolik významného stupně společenské škodlivosti, že postih podle jiných právních předpisů není postačující, a je proto nutné použít jakožto ultima ratio prostředky trestního práva (pozornost otázce společenské škodlivosti je pochopitelně třeba věnovat vždy).

Mladistvý se může dopustit také trestného činu výroby a jiného nakládání s dětskou pornografií. Nikoliv však tím, že vyrobí dětskou pornografii, jejímž bude jediným aktérem, vzhledem k obecné právní zásadě, že „nemůže být trestná osoba, k jejíž ochraně je příslušné trestněprávní ustanovení určeno“ (Šámal, 2012 str. 1968), a k tomu, že „objektem trestného činu výroby a jiného nakládání s dětskou pornografií ... je zájem společnosti na ochraně mravního vývoje dětí a jejich ochraně před sexuálním zneužíváním“ (Šámal, 2016 str. 630). Nicméně kdokoliv vč. mladistvého se může dopustit trestného činu výroby a jiného nakládání

[375] Data zde uvedená se vztahují k českým dětem ve věku 8-17 let, blíže k tomu viz (Kopecký, a další, 2017).
[376] Snapchat umožňuje zaslat fotografii na zvolená telefonní čísla s pokynem k automatickému sebesmazání po určené době. Jen dočasná existence fotografie je ale iluzí - ignoruje možnost uložení adresátem nebo i jen prosté vyfocení displeje mobilu adresáta někým dalším v okamžiku zobrazení fotografie. Důvěra v dočasnost znamená, že dotyční jsou ochotni zaznamenat a zaslat výrazně odvážnější materiál, než s vědomím rizika jeho trvalé existence.

s dětskou pornografií podle § 192 odst. 3 al. 1 TZ tím, že rozesílá dětskou pornografii, neboť takové jednání můžeme podřadit pod nabídnutí, příp. zprostředkování dětské pornografie jinému – za předpokladu, že objektem trestného činu výroby a jiného nakládání s dětskou pornografií podle § 192 odst. 3 al. 1 TZ je kromě zájmu společnosti na ochraně mravního vývoje dětí a jejich ochraně před sexuálním zneužíváním zároveň zájem na mravních hodnotách společnosti, která dětskou pornografii považuje za škodlivou.

Trestného činu šíření pornografie i výroby a jiného nakládání s dětskou pornografií se lze dopustit v jednočinném souběhu s ohrožováním výchovy dítěte podle § 201 TZ: „objektem trestného činu ohrožování výchovy dítěte je zájem na řádné výchově dětí, která má být vedena v souladu se zásadami morálky občanské společnosti tak, aby byl zaručen jejich řádný rozumový, mravní a citový vývoj“ (Šámal, 2012 str. 1953). K ohrožení rozumového, citového nebo mravního vývoje dítěte pak dojde zejm. tehdy, jestliže jednání pachatele vede ke vzniku reálného nebezpečí např. pohlavní nevázanosti, promiskuity, osvojení si takových návyků dítětem, které vedou „k jeho morálnímu úpadku a k neschopnosti usměrňovat způsob svého života v souladu s obecnými morálními zásadami občanské společnosti“ (Šámal, 2012 str. 1954). Výjimečně by se tak mohlo stát i v případě sextingu, pokud by jeho provozování a obsah přesáhly určitou míru.[377] Trestného činu ohrožování výchovy dítěte podle § 201 odst. 1 písm. b) nebo d) TZ se mohou dopustit např. i rodiče dítěte, jestliže porušení jejich rodičovské zodpovědnosti je takové závažnosti, že umožní vést dítěti v tomto případě nemravný život nebo závažným způsobem poruší svou povinnost o ně pečovat či jinou svou důležitou povinnost vyplývající z rodičovské zodpovědnosti.

Sexting může být spojen i s trestným činem zneužití dítěte k výrobě pornografie (§ 193 TZ). O kořistění z účasti dítěte na pornografickém díle u sextingu se zřejmě jednat nebude, zato však půjde především o najmutí, a to tehdy, když se pachatel s dítětem dohodne na tom, že dítě samo vyrobí a zašle mu pornografický materiál, který ho bude zobrazovat, výměnou za kredit do mobilního telefonu či jinou úplatu (např. koupě herního času). Předpokladem je, že dítě tento materiál vyrobilo až na základě takové dohody s pachatelem. Skutková podstata trestného činu zneužití dítěte k výrobě pornografie může být ovšem naplněna i zlákáním nebo svedením zvláště v případě partnerských vztahů mládeže, v jejichž rámci jeden partner přesvědčí druhého k výrobě dětské pornografie. Souběh s přečinem svádění k pohlavnímu

[377] Ospravedlnitelnou např. touhou experimentovat s vlastní sexualitou nebo vyhledávat zážitkové podněty. Zlomový bod se pak bude nalézat někde mezi pokusem/občasnými pokusy a běžně se opakujícím jednáním.

styku (§ 14 odst. 2, § 202 TZ) bude spíše vyloučen z důvodu subsidiarity svádění k pohlavnímu styku.

Dne 22.7.2014 s účinností od 1.8.2014 se stala součástí trestního zákona i nová skutková podstata účasti na pornografickém představení (§ 193a TZ).[378] Může dojít naplnění i v souvislosti se sextingem, bude-li jeho obsah spojený nikoliv s dětskou pornografií, ale s pornografickým představením dítěte, tzn. půjde např. o striptýz před webkamerou.[379] „Pornografickým představením se rozumí živé vystoupení využívající dítě, jež v něm účinkuje, k vytvoření pornografického díla určeného určitému publiku, a to ... též osobám, jež je sledují i prostřednictvím ICT. Postihuje se samotná úmyslná účast pachatele na takovém pornografickém představení, ve kterém účinkuje dítě.“[380] Pokud se bude pachatel podílet zároveň na výrobě a jiném nakládání s dětskou pornografií nebo zneužití dítěte k výrobě pornografie, samotná jeho účast na pornografickém představení bude zřejmě konzumována z důvodu subsidiarity.

10.3. Kybergrooming[381]

Kybergrooming lze nejjednodušeji charakterizovat jako psychickou manipulaci[382] oběti prostřednictvím ICT s cílem sexuálně ji využít, které začíná zpravidla jako nevyžádané kontaktování. V roce 2009 komunikovalo s osobou známou pouze z prostředí internetu 46 % českých dětí ve věku 9-16 let a 15 % se s takovou osobou i setkalo tváří v tvář (Livingstone, a další, 2011 str. 86), v roce 2013 to bylo mezi dětmi ve věku 11-17 let již 53 %, přičemž 36 % respondentů by bylo ochotno na takovou schůzku jít (Univerzita Palackého v Olomouci, Seznam.cz, Google, 2014).

Při typickém průběhu kybergroomingu útočník pod falešnou identitou brouzdá internetovými seznamkami, chaty, dětskými weby a na SNS. Zde kontaktuje množství osob (až desítky souběžně), zejm. těch, které samy explicitně vyhledávají přítele, neboť ty snáze sklouznou do fáze manipulovatelnosti. Je-li vyhlédnutá osoba ochotna komunikovat, kybergroomer s ní

[378] Blíže k novelizaci viz kapitola **KybergroomingChyba! Nenalezen zdroj odkazů.**.
[379] K poměrně výnosné formě obživy v podobě online přenášených pornografických představení viz (Bartlett, 2015), kapitola Lights, Web-camera, Action.
[380] Viz komentář R. Fremra k § 193a TZ (Draštík, a další, 2015).
[381] Kapitola vychází ze studentské vědecké odborné činnosti autorky (Lukášová, 2012) a dále z (Vybrané navrhované změny trestního zákoníku - § 192, 193b TZ, 2013), (Brandejsová, a další, 2012) a (Kudrlová, 2017).
[382] Manipulovaná osoba jedná v souladu s vůlí manipulátora a pod jeho vlivem, aniž by si toho byla sama vědoma, resp. jedná v iluzi vlastního neovlivněného rozhodování.

nadále udržuje a prohlubuje kontakt. Nejprve pro sebe nenápadně získává praktické informace: zda a kdy má daná osoba přístup k počítači o samotě, jaké jsou její rodinné poměry atp.[383] Spolu s tím se snaží zároveň vylákat co nejvíce intimních informací, osvědčenou taktikou je v tomto směru prozrazení nějakého vlastního (jakoby) „tajemství", po jehož sdělení se cítí druhá osoba natolik zavázána, že na oplátku se svěří s vlastním tajemstvím, tentokrát už skutečným. Jak pokračuje vzájemná komunikace, vyhlédnutá oběť důvěřuje kybergroomerovi stále víc a více. Důvěra je podpořena i ochotou kybergroomera být pro dotyčnou osobu vždy k dispozici, třeba k vyslechnutí jejího trápení, pocitů, myšlenek. Kybergroomer se také obvykle orientuje v zájmech své cílové skupiny a vystupuje jako podobně orientovaný jedinec (např. stejné záliby, hudební styl atp.), což umocňuje vzrůstající pocit oběti, že v kybergroomerovi našla spřízněnou duši. V průběhu udržované komunikace (trvající i měsíce) se snaží kybergroomer oběť izolovat od jejího sociálního okolí, zejm. rodičů. Jednak si tím zajišťuje, aby nebyl odhalen a oběť nezačala být v důsledku varování okolí ostražitější, jednak tím upevňuje důvěru oběti, pro kterou se stává jejich komunikace tajemstvím skrytým i před jejími nejbližšími jako něco výjimečného, stávají se spiklenci. Oběť získává postupně pocit, že pouze před útočníkem nemusí skrývat žádné tajemství a komu může věřit, na rozdíl od okolí vč. nejbližší rodiny, které jí zdaleka tak nerozumí. Dříve či později se komunikace s kybergroomerem stočí k sexuální tematice, od textové podoby k fotografiím a videím, případně svlékání oběti před webkamerou atp. (v závislosti na míře dosud získané důvěry oběti). Kybergroomer na oplátku zasílá „vlastní" fotografie odpovídající jeho smyšlené identitě. Není ovšem vyloučeno, že útočník postupně upraví či zcela odhalí svou skutečnou identitu[384] (a odpovídající fotografie), případně např. poskytne pouze fotografie svých pohlavních orgánů. Vzhledem k již alespoň částečně vybudované důvěře ze strany vyhlédnuté osoby může tato snadno podlehnout a fotografie mu poskytnout.[385] Pokud oběť na sexuální tematiku nechce přistoupit, útočník ji pobízí i drobnými úplatky, typicky kreditem do mobilního telefonu („aby si mohli povídat"). Po určité době začne kybergroomer naléhat na osobní setkání. Při odmítnutí nebo váhání zkusí nejprve psychický nátlak, kdy hrozí např. skončením vzájemného vztahu, což samo o sobě může oběť přesvědčit, je-li už na útočníkovi psychicky závislá. Pakliže nikoliv, kybergroomer neváhá oběť k setkání nutit pod pohrůžkou zneužití dosud nabytých intimních informací a materiálů

[383] Řadu informací poskytne dotyčná osoba sama, některé i její „přátelé" na základě pouhého dotazu, případně smyšlené záminky.
[384] Např. s postupnou ztrátou ostražitosti oběti zvyšuje svůj předstíraný věk až ke skutečné hodnotě.
[385] Resp. poskytnout mu to, o co žádá, ať už se jedná o fotografie zaslané přes počítač nebo prostřednictvím MMS, svléknutí se před webkamerou aj.

(např. zveřejnění nebo zaslání rodičům jejích intimních fotografií).[386] Pokud oběť se schůzkou souhlasí, dojde zpravidla k sexuálnímu zneužití, od sexuálního nátlaku po znásilnění, výjimkou není ani výroba (zejm. dětské) pornografie, může dojít i na obchodování s lidmi.

Lze se ovšem setkat i s používáním výrazu „kybergroomer" v širším smyslu jako osoba lákající (zejm. od dětí) sexuálně ladění materiál. V této lehčí formě navštěvuje internetové seznamky, chaty či obdobná místa, kde vystupuje mnohdy i pod vlastní identitou (resp. s omezením na křestní jméno a věk). Zde naváže komunikaci s některou z přítomných osob a záhy stočí hovor explicitně k sexuální tematice (např. dotazem na spodní prádlo, masturbaci atp.). První kontakt mnohdy vypadá jako nevinná žádost o přátelství: „Ahoj, koukám, že jsi taky z Prahy a nudíš se, chceš se bavit? Dáš si mě do přátel?" Záhy stočí konverzaci sexuální směrem: „už jsi to někdy dělala? A chtěla bys? Už jsi ho viděla? Už jsi ho držela? Už jsi ho kouřila?"[387] Při odmítnutí přesune kybergroomer svou pozornost na někoho jiného. I v těchto případech obvykle dochází k jedno či oboustrannému sextingu, ať už jako „hře" s lákavým přivýdělkem nebo i bez něj.

V nemalé míře se začalo objevovat také vydírání dospělých mužů, kteří se nechali zlákat ke kybersexu domnívaje se, že komunikují s mladou slečnou, a kterým následně pachatel hrozí např. zveřejněním komunikace v médiích, zasláním manželce atp. (Europol, 2017). Zde ovšem nejde o kybergrooming v pravém slova smyslu, neboť prvotním záměrem pachatele je namísto sexuálního uspokojení zisk.

Od samého počátku kybergroomer manipuluje psychiku oběti a začíná pracovat na její závislosti na něm. Čím je v tomto směru úspěšnější, tím bolestnější je pro oběť ukončení komunikace, ať už dobrovolné nebo pod vnějším tlakem (např. na pokyn rodičů), což umocňuje fakt, že pro digitální domorodce má i zcela virtuální komunikace a vztah stejnou hodnotu jako ten v reálném světě. S pokračujícím kontaktem mezi útočníkem a obětí se proto zvyšuje riziko a závažnost její psychické újmy způsobené ukončením vztahu. Oběť trpí oběť i vzrůstající izolací od přátel a zejm. nejbližší rodiny (může dojít i ke značnému odcizení). Intimní až pornografické materiály oběť poskytuje mnohdy bez jakýchkoliv obav z možných rizik: jednak již kybergroomerovi obvykle důvěřuje a nepředpokládá jeho úmysl materiál zneužít, jednak si dovede jen těžko představit, jak by mohly být v její neprospěch zneužity

[386] Hrozbu jejich zneužití využívá mnohdy už při samotné sexuálně laděné komunikaci, kdy např. vyžaduje další a další fotografie.
[387] Autentické výňatky z proběhnuvší komunikace mezi některými z usvědčených pachatelů navazování nedovolených kontaktů s dítětem a jejich obětí.

např. sexuálně lichotivé fotografie. Pornografie od kybergroomera spolu se vzájemným sextingem pak mohou deformovat její pohled na sexualitu a ohrozit zdravý vývoj v období dospívání (např. nabytí představy o promiskuitě coby normě nebo sexuální deviace). Pokud útočník začne oběť nutit k dalším sexuálním aktivitám (sexting, masturbace před webkamerou atp.) nebo osobnímu setkání, ať už pohrůžkou ukončení vztahu nebo zneužití intimního obsahu, tato se dostává do paradoxní pozice, kdy na jednu stranu stále ještě nechce kybergroomera/"spřízněnou duši" ztratit, a zároveň pociťuje hrůzu např. z prozrazení jejího tajemství a obavy z poskytnutí dalšího obsahu či osobního setkání. Negativní dopady případného setkání jsou pak zřejmé, od újmy spojené se sexuálním zneužitím (dle jeho formy) po psychické trauma v důsledku deziluze.

Ovšem bez dopadu nemusí být ani lehčí forma kybergroomingu: např. negativní vliv sextingu vůbec, komercializace vlastního těla, deformace hodnot (zejm. morálky a mravnosti). Nedochází sice k manipulaci (nebo jen v menší míře) a osobnímu kontaktu, potažmo fyzickému ohrožení, ani k budování a následnému zničení důvěry a deziluzi oběti, zůstává však přítomen digitalizovaný obsah, který může kybergroomer kdykoliv využít.

K dokladu a názornější představě o kybergroomingu v českých podmínkách může dobře posloužit kauza P.H. odehrávající se zhruba v letech 2005–2009.[388] P. H. vyhledával a navazoval přátelství s dětmi na internetových seznamkách, přičemž se zaměřoval zejm. na chlapce z dětských domovů. S dětmi si chatoval a později i telefonoval, průběžně vylákával za drobné úplatky fotografie. Po čase pozval oběť k sobě do práce - vrátnice, kde byl zaměstnán i ubytován. Pokud chlapci odmítali, hrozil zveřejněním získaných fotografií a pověr o jejich homosexualitě. Dále např. uspořádal soutěž „Dítě VIP", kdy výherce mohl za odměnu strávit několik dní v Praze (tj. ve vrátnici u P. H.). Oklamáni byli i ti pedagogičtí pracovníci z dětských domovů, kteří se pokusili prověřit důvěryhodnost P. H. prostřednictvím internetu, neboť dotyčný cíleně upravoval svůj digitální otisk na různých webech fiktivními pozitivními ohlasy z jiných dětských domovů.[389] Na vrátnici byly oběti drženy několik dní, během nichž byly různě sexuálně zneužívány. P. H. byl obžalován ze zvlášť závažného zločinu znásilnění, zločinu pohlavního zneužití a dále přečinů vydírání, ohrožování výchovy dítěte a svádění k pohlavnímu styku spáchaných na 20 chlapcích. Soud mu v prvním stupni uložil trest odnětí svobody v délce 8 let a sexuologickou léčbu, nicméně odvolací soud

[388] Informace zde podané jsou získané vesměs z médií: (2009), (Nebuď oběť), (E-Bezpeci, 2009), (2012), (2009), (ČTK, 2009), (ČT24, 2009), (ČTK, 2009), (2009), (Kopecký, 2009), (Seznam.cz).
[389] Vystupoval pod svým skutečným jménem a věkem (36 let), nicméně jako podnikatel snažící se ulehčit úděl dětem z dětských domovů prostřednictvím sponzorských darů.

později snížil délku trestu na 6,5 let, neboť neměl za prokázané, že P. H. spáchal zvlášť závažný zločin znásilnění. K pohlavnímu styku provedenému způsobem srovnatelným se souloží nepochybně došlo, avšak nikoliv zřejmě násilím nebo pohrůžkou násilí nebo pohrůžkou jiné těžké újmy. Může se to sice zdát nepravděpodobné, avšak je třeba vzít v potaz, že se jednalo o děti z dětských domovů, a tedy pravděpodobně citově a emočně deprivované – právě ty snáze přilnou k laskavému kybergroomerovi, snad i do té míry, že jsou ochotni přistoupit dobrovolně na sexuální praktiky.

Zatím není známa žádná zvláštní charakteristika, která by poukazovala na sklony ke kybergroomingu, spíše jde o souhrn dílčích okolností vůbec umožňujících kybergrooming. Předně je to alespoň základní uživatelská znalost ICT a zdatnost v používání konkrétních komunikačních kanálů (SNS, seznamky, chaty aj.) – jaký obsah kde nalézt, jak vyhledat vhodnou osobu atp. Je schopen zajistit jiné osobě kredit do mobilního telefonu, zakoupit herní čas nebo třeba vylepšit avatara. Oplývá povědomím o možnostech a zájmech své cílové skupiny – oblíbené filmy, počítačové hry, hudba atp. Obvykle také ví, jaké sociální či psychické problémy často trápí osoby v cílové skupině (např. zhoršení vztahu s rodiči v pubertě, kyberšikana atp.) i co je právě „in“ (např. po jakém mobilním telefonu zřejmě dotyční touží). Kromě toho bývá kybergroomer inteligentní, cílevědomý a trpělivý – dokáže tak udržovat komunikaci i po mnoho měsíců a s více osobami současně. V emocionální rovině je zpravidla chladnokrevný a pro citové utrpení oběti spojené s kybergroomingem nemá žádné pochopení, nepřipouští si špatnost svého jednání. Vůči oběti vystupuje sice nanejvýš empaticky, avšak jen proto, že (racionálně předstíraná) „empatie“ znamená nejjednodušší cestu k důvěře a nitru oběti. Výjimkou nejsou pedofilní kybergroomeři, nikoliv však většinově. Spíše lze o nich říci, co o většině pachatelů mravnostní kriminality – jejich primární sexuální orientace směřuje k dospělým jedincům (resp. jedincům obdobného věku), avšak v důsledku nenaplnění vlastních sexuálních potřeb (např. pro neschopnost navázat blízký vztah) se obrací na zástupný, snazší cíl - děti (přesto bude mnohdy na místě uložit pachateli ochranné opatření v podobě uložení ochranného léčení sexuologického).

I o obětech kybergroomingu lze říci určitá obecná specifika. Předně jde nejčastěji o děti ve věku 9–17 let, zpravidla hojně využívající ICT. Ač bývají poučeny, mnohdy si nepřipouští možnost, že by právě ony narazily na kybergroomera, a stejně tak jako jsou sami otevření, upřímní a důvěřiví, předpokládají totéž u druhých. Viktimitu výrazně zvyšují emoční deprivace a problémy s okolím. Pokud kohokoliv citové potřeby nejsou naplněny (např. problémy v rodině), touží po zaplnění vnitřní prázdnoty. Velmi snadno pak dotyčný podlehne

kouzlu „přítele“, který má vždy po ruce laskavé slovo, podporu a útěchu, kterých se od jiných nedostává. Při problémech s okolím (např. šikana) pak pohyb v kyberprostoru vč. kontaktu s kybergroomerem skýtá vítaný oddech, únik z reality a falešný pocit bezpečí. Jako varovný signál může sloužit rozvoj závislostního chování (netholismus i závislost v reálném světě), které poukazuje na jiný, hlubší problém, v jehož řešení daná osoba selhává a od něhož utíká. Oběť je pak jednak psychicky oslabená (oním těžko řešitelným problémem), jednak se kybergroomer rychle dozví, co ji trápí a pro co má slabost. Dalším rizikovým faktorem je problém navázat vztah v reálném světě. Může tak být z důvodů psychických a sociálních (např. stud, tréma, introverze, nedostatek emoční či komunikační inteligence, nedostatek komunikačních příležitostí), fyzických (např. vada řeči nebo vzhledu), ale i vlivem prostředí (např. místo a okolí bydliště dané osoby, kde chybí sociální zázemí pro stýkání se s vrstevníky). Zbývá ještě dodat, že v případě lehčí formy kybergroomingu se budou potenciální oběti rekrutovat zejm. z řad neopatrných osob (ač mnohdy poučených), které si nepřipouští ohrožení, ať už v daný okamžik nebo i digitalizovaným obsahem v budoucnu. Výrazným faktorem je také chování vrstevníků a blízkých osob.

10.3.1. Právní kvalifikace kybergroomingu

V průběhu kybergroomingu se pachatel může dopouštět a pravděpodobně i dopustí trestných činů zasahujících různé druhové objekty, zdaleka nejpřiléhavější se však zdá být skutková podstata trestného činu navazování nedovolených kontaktů s dítětem (§ 193b TZ). Tu zavedl s účinností od 1.8.2014 zák. č. 141/2014 Sb. v následujícím znění: „kdo navrhne setkání dítěti mladšímu patnácti let v úmyslu spáchat trestný čin podle § 187 odst. 1, § 192, § 193, § 202 nebo jiný sexuálně motivovaný trestný čin, bude potrestán odnětím svobody až na jeden rok.“ Důvodová zpráva (Vláda ČR; Poslanecká sněmovna PČR, 2013) hovoří o nutné implementaci směrnice Evropského parlamentu a Rady 2011/93/EU ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV, zde konkrétně o čl. 6 odst. 1: „navrhne-li dospělá osoba prostřednictvím ICT setkání dítěti, které nedosáhlo věku pohlavní dospělosti, s cílem spáchat trestný čin uvedený v čl. 3 odst. 4 a čl. 5 odst. 6 a učiní-li po tomto návrhu

konkrétní kroky vedoucí k tomuto setkání, trestá se tento návrh odnětím svobody s horní hranicí trestní sazby nejméně jeden rok.“[390]

Objektem § 193b TZ je především ochrana dětí mladších 15 let před sexuálním vykořisťováním, zvláště pak s důrazem na ochranu před takovým jednáním, pokud jsou prostředkem k němu ICT, typicky před kybergroomingem. Tato ochrana se tedy vztahuje pouze na děti mladší 15 let, přičemž dovršení 15. roku je v ČR hranicí pohlavní dospělosti. Tím je naplněn požadavek čl. 6 odst. 1 směrnice č. 2011/93/EU. Pokud bychom však vyšli mimo její rámec, bylo by na místě poskytnout ochranu trestním zákonem před sexuálním vykořisťováním prostřednictvím ICT mládeži vůbec (podobně, jako je chráněna před zneužíváním k výrobě dětské pornografie). V takovém případě by pak měl být útok na dítě mladší 15 let znakem kvalifikované skutkové podstaty.[391] Objektivní stránku naplní ten, kdo navrhne setkání dítěti mladšímu 15 let v úmyslu spáchat trestný čin podle § 187 odst. 1, § 192, § 193, § 202 TZ nebo jiný sexuálně motivovaný trestný čin (přičemž jednání prostřednictvím ICT se výslovně nevyžaduje). Setkáním bude nepochybně jakákoliv forma schůzky, jíž se má osobně zúčastnit pachatel a dítě mladší 15 let. Z jazykového výkladu je zřejmé, že setkání musí navrhnout pachatel, tedy musí vyvinout aktivitu směřující k uskutečnění schůzky. Protože novelizované znění nevyžaduje výslovný návrh, dostačující by měla být při extenzivním výkladu i mlčky projevená vůle směřující k uskutečnění setkání (např. pachatel zašle dítěti mladšímu 15 let lístek na sportovní utkání, na kterém má v úmyslu se s ním osobně setkat). Při restriktivním výkladu by k naplnění znaků skutkové podstaty muselo jít o návrh setkání způsobilý vzbudit v adresátovi rozhodnutí k vědomé účasti na setkání s pachatelem, a tedy by takový návrh odpovídal požadavkům kladeným na účastenství na trestném činu ve formě návodu. Pachatelem může být kdokoli, vč. právnické osoby (§ 7 TOPO). Subjektivní stránka vyžaduje úmyslné jednání doplněné pohnutkou v podobě úmyslu spáchat trestný čin pohlavního zneužití, výroby a jiného nakládání s dětskou pornografií, zneužití dítěte k výrobě pornografie, svádění k pohlavnímu styku nebo jiný sexuálně motivovaný trestný čin (tím může být např. účast na pornografickém představení dle § 193a TZ).

[390]Trestným činem uvedeným v čl. 3 odst. 4 a čl. 5 odst. 6 je účast na sexuálních praktikách s dítětem, které nedosáhlo věku pohlavní dospělosti (v českých podmínkách dítě mladší 15 let, viz§ 187 TZ), a výroba dětské pornografie. K tomu viz čl. 6 odst. 1, čl. 3. odst. 4 a čl. 5 odst. 6 uvedené směrnice.

[391] A to navzdory paradoxu, kdy děti ve věku 15-18 let již mohou mít pohlavní styk, ale nesmí přijít do styku s žádnou pornografií, nemluvě o protiprávnosti dětské pornografie. Paradox je to však pouze zdánlivý, neboť konzumace pornografie může vést k poruchám vlastní sexuality a dětská pornografie odporuje navíc i morálním hodnotám moderní společnosti západního typu.

§ 193b TZ dopadá na jednání, která jsou z materiálního hlediska přípravným jednáním ke spáchání sexuálně motivovaného trestného činu. Trestně odpovědným bude proto i pachatel, který sice navrhne setkání dítěti mladšímu 15 let v úmyslu spáchat sexuálně motivovaný trestný čin, avšak o samotný tento čin se už ani nepokusí. Před zavedením § 193b TZ mohl být pachatel navrhnuvší setkání dítěti mladšímu 15 let v úmyslu spáchat sexuálně motivovaný trestný čin trestně odpovědný pouze v případě, kdy tak usiloval o zvlášť závažný zločin znásilnění [§ 185 odst. 1 al. 1 nebo 2, odst. 2 písm. b), odst. 3 písm. a), odst. 5 TZ], zvlášť závažný zločin sexuálního nátlaku [§ 186 odst. 1 al. 1 nebo 2, odst. 3 písm. a), odst. 5 písm. a), odst. 7 TZ] nebo zvlášť závažný zločin pohlavního zneužití (§ 187 odst. 1, 2, 5 TZ), přičemž o takový trestný čin se ani nepokusil, a zůstal tak ve stadiu přípravy (§ 20 odst. 1 TZ). Nyní případný jednočinný souběh výše uvedených zvlášť závažných zločinů s přečinem navazování nedovolených kontaktů s dítětem by měl být zřejmě vyloučen z důvodu subsidiarity navazování nedovolených kontaktů s dítětem, nicméně i v těchto případech bude pachatel trestně odpovědný dle § 193b TZ, pakliže zanikne trestnost přípravy toho kterého zde vyjmenovaného zvlášť závažného zločinu. Za spáchání trestného činu navazování nedovolených kontaktů s dítětem hrozí pachateli trest odnětí svobody až na jeden rok, a proto se jedná o přečin (§ 14 odst. 2 TZ).

V názvu skutkové podstaty trestného činu navazování nedovolených kontaktů s dítětem lze upozornit na určité gramatické a jazykové nedůslednosti. Předně jde o množné číslo co do „navazování nedovolených kontaktů“ – z jazykového a gramatického výkladu s ohledem na množné číslo vyplývá nezbytnost více takových kontaktů, což ovšem nemá oporu v samotném textu skutkové podstaty. Nejasnost doplňuje jednotné číslo „s dítětem“, což by znamenalo nezbytnost více takových kontaktů s konkrétním dítětem, zatímco však „navazování kontaktů“ by více odpovídalo navazování kontaktů „s dětmi“. Mimoto samotná skutková podstata se vztahuje k dítěti mladšímu 15 let, nikoli dítěti (tedy osobě mladší 18 let, § 126 TZ). Vhodnějším názvem by proto bylo např. „navazování nedovoleného kontaktu s dítětem“. Použití nedokonavého vidu pro „navazování“ nedovolených kontaktů s dítětem naznačuje, že k faktickému navázání kontaktu s dítětem dojít nemusí. Skutková podstata trestného činu navazování nedovolených kontaktů s dítětem dopadá zejm. na kybergrooming (v jeho závažnější formě), kdy je konkrétní dítě při následném uskutečnění setkání již fyzicky ohroženo, na rozdíl např. od „pouhé“ výroby dětské pornografie, při které se pachatel nemusí s dítětem vůbec setkat. Bylo by proto na místě zvážit přísnější postih takového jednání. Ne vždy však půjde § 193b TZ při postihu kybergroomingu vůbec aplikovat, neboť oběť může

být zmanipulována natolik, aby návrh setkání vyšel nikoliv od útočníka, leč od ní samotné. Skutková podstata trestného činu navazování nedovolených kontaktů s dítětem by proto měla být vykládána tak, aby návrh setkání nemusel vzejít výslovně od pachatele, ale aby bylo dostačujícím jednáním z hlediska trestní odpovědnosti již jednání pachatele směřující k setkání s dítětem v úmyslu spáchat sexuálně motivovaný trestný čin. Specifická situace by mohla nastat v případě, kdy kybergroomer navrhne setkání s dítětem, avšak z jiného důvodu než s úmyslem spáchat sexuálně motivovaný trestný čin, přičemž později se rozhodne čin předpokládaný ustanovením § 193b TZ spáchat v souvislosti s navrženým setkáním. V takovém případě zřejmě nebude možné jeho jednání postihnout jako navazování nedovolených kontaktů s dítětem.

Od zavedení § 193b TZ v roce 2014 se již objevilo několikero trestních řízení v této věci (viz tab. č. 7).[392] Pachatelů (všichni muži, převážně ve věku kolem 29 let) je v tuto chvíli prozatím poskrovnu, jak se ovšem dalo čekat vzhledem ke krátké účinnosti nové právní úpravy (trestní řízení pravomocně skončená v roce 2018 a probíhající nejsou v tabulce zahrnuta). Obvykle bývá v souvislosti s trestním řízení zpracovaný znalecký posudek v oboru zdravotnictví, sexuologie, který konstatuje u pachatele sklony k hebefilii. V důsledku toho není výjimkou uložení ochranného léčení sexuologického. Pachatelé si v průběhu řízení zpravidla uvědomují protiprávnost svého jednání, doznávají se a svého jednání litují (nezřídka také sami hovoří o potřebě sexuologické léčby, může však jít samozřejmě o snahu dosáhnout nižšího trestu). Poškozené byly zpravidla dívky ve věku 10-14 let, což pachatelé věděli prakticky od samého počátku (či téměř od samého počátku). Komunikace někdy probíhá převážně jednostranně: pachatel iniciuje konverzaci a v jejím průběhu je aktivnější. Může jít i o dialog, kdy oběť nezůstává v sexuálně laděné komunikaci pozadu. K prvnímu kontaktu dochází nejčastěji prostřednictvím FB, komunikace může přejít na telefonní hovor. Některé z obětí v komunikaci dobrovolně pokračují až k osobnímu setkání, jiné se ji snaží ukončit již ve fázi konverzace v „bezpečí“ SNS a setkání se vyhnout. Pokud nechtějí nebo se bojí pachatele odmítnout přímo, raději např. vymyslí historku o svém pobytu v nemocnici, pro který nemohou dorazit na místo schůzky, náhlou nevolnost, nečekané domácí povinnosti atp. Pachatelé obvykle komunikují ve stejném období s více než jednou obětí.

[392] Zde uvedené údaje vychází z analýzy několika vybraných pravomocně skončených trestních řízení v souvislosti s probíhajícím výzkumem IKSP.

Tab. č. 7: § 193b TZ

	2015	2016	2017
Počet pravomocně skončených věcí	3 odsouzení	6 odsouzených 1x zastaveno[393]	16 odsouzených
Počet prvopachatelů	2	2	10
Pachatel ve věku 15-17 let	0	1	0
Pachatel ve věku 18-19 let	0	0	1
Pachatel ve věku 20-24 let	1	2	1
„Pachatel“ ve věku 25-29 let	2	3[394]	5
Pachatel ve věku 30-39 let	0	1	7
Pachatel ve věku 40-49 let	0	0	2
Uloženo ochr. léčení sexuologické	2	4	8 (z toho 1 x ústavní)

Už v samotném počátku jednání, tedy při navázání komunikace s obětí, ale především pak v průběhu udržování komunikace se může pachatel dopouštět přečinu poškození cizích práv (§ 181 TZ), neboť uvádí svou oběť v omyl, kterého pak obvykle dále využívá, přičemž jí tím způsobí vážnou újmu na právech: snahou o izolaci oběti, nabádáním k utajování komunikace aj. narušováním zejm. rodinných vztahů mezi poškozenou a jejími blízkými. V nejzávažnějších případech tak může způsobit i újmu dosahující svou intenzitou vážné újmy na právech, přičemž pachatel bude v takových případech s největší pravděpodobností srozuměn s tím, že takový následek může svým jednáním způsobit.

Je-li vyhlédnutou obětí dítě, tj. osoba mladší 18 let (§ 126 TZ), a kybergroomer stáčí hovor k sexuální tematice, začíná již připadat v úvahu přečin ohrožování výchovy dítěte [§ 201 odst. 1 písm. a) TZ], neboť takové jednání lze nepochybně posoudit jako směřující k ohrožení mravního vývoje dítěte.[395] Při přeposílání pornografie se nabízí hned několik možných skutkových podstat. Pokud oběť-dítě, zašle dobrovolně a z vlastního popudu pachateli své vlastní pornografické fotografie či videa a pachatel si je ponechá, dopustí se tento přečinu výroby a jiného nakládání s dětskou pornografií (naplní znak „přechovává elektronické pornografické dílo, které zobrazuje nebo jinak využívá dítě“, § 192 odst. 1 TZ).

[393] Podle § 172 odst. 2 písm. a) TŘ (trest, k němuž mohlo stíhání vést, by byl zcela bez významu vedle trestu, který byl obviněnému již uložen pro jiný čin).
[394] Vč. obviněného, jehož trestní řízení bylo zastaveno.
[395] S ohledem na subsidiaritu trestní represe za předpokladu, že k takové komunikaci dochází opakovaně, resp. nikoliv jednorázově, a vůči konkrétnímu dítěti, jehož mravní vývoj tím může být narušen.

Pravděpodobnější je však situace, kdy kybergroomer svou oběť-dítě vůbec přesvědčí k výrobě takového díla, tzn. zneužije dítě k výrobě pornografie (§ 193 odst. 1 TZ), neboť dítě k výrobě pornografického díla např. přiměje svým již vybudovaným vlivem, najme za drobný úplatek (např. kredit do mobilu), zláká nabídnutím „vlastních" pornografických materiálů, svede vybízením k takové výrobě např. i pod otevřeně vyjádřenou záminkou poznat dítě „blíže". Pokud sám kybergroomer zasílá oběti-dítěti prostou pornografii, bude šířit pornografii [§ 191 odst. 2 písm. a) TZ]. Zašle-li oběti (nejen dítěti) dětskou pornografii,[396] dopustí se opět přečinu výroby a jiného nakládání s dětskou pornografií, ovšem tentokrát v základní skutkové podstatě tohoto přečinu uvedené v odst. 3 § 192 TZ, neboť jinému dětskou pornografii zprostředkuje. Ne vždy musí ovšem dojít přímo k výrobě pornografického díla, kybergroomer se může spokojit např. s požadováním obnažování se oběti před webkamerou při videohovoru. Pokud bude oběť dítětem a kybergroomer jí nabídne, slíbí nebo poskytne za takové jednání úplatu, dopustí se přečinu svádění k pohlavnímu styku [§ 202 odst. 1, příp. i odst. 2 písm. a) a příp. i písm. d) TZ].[397]

Pro kvalifikaci dalšího jednání už nehraje takovou roli, zda je obětí dítě či nikoliv. Když se kybergroomer uchýlí při naléhání na pokračování a zintenzivnění sextingu nebo na osobní setkání k hrozbám ukončením vztahu a komunikace, lze to v některých případech považovat za pohrůžku jiné těžké újmy, s ohledem na již vybudovaný vztah až závislosti oběti na kybergroomerovi. Zvláště u obětí mladších 18 let, vzhledem k psychicky náročnému vývojovému období, kdy jsou takové osoby zvláště emočně citlivé, a přikládání stejné váhy vztahům reálným i virtuálním. Přichází tak v úvahu přečin vydírání (§ 175 odst. 1 TZ), obdobně jako při vyhrožování např. zveřejněním získaných pornografických materiálů, detailů o intimním životě poškozeného atp. V méně závažných případech, kdy naléhání nepřekročí hranici jiné těžké újmy, se pachatel stále může dopustit útisku (§ 177 TZ), pakliže nutí oběť, aby něco konala, zneužívaje její emoční závislosti.[398]

Následná osobní schůzka pak obvykle směřuje k sexuálnímu zneužití: znásilnění, sexuálnímu nátlaku, pohlavnímu zneužití,[399] výrobě a jinému nakládání s dětskou pornografií (výroba

[396] Např. proto, že se sám vydává za dítě a na podtržení své důvěryhodnosti zašle oběti např. pornografické fotografie konkrétního dítěte nalezené na internetu nebo získané obdobným způsobem od jiné oběti-dítěte.
[397] Vztah mezi kybergroomerem a jeho obětí má zpravidla intimní charakter, který prakticky vylučuje, aby bylo takové jednání oběti zároveň tzv. pornografickým představením předpokládajícím určité publikum, a tudíž nepřichází v úvahu účast na pornografickém představení (§ 193a TZ).
[398] Ovšem psychická závislost oběti na kybergroomerovi patrně ještě sama o sobě neznamená trestněprávně relevantní závislost, a proto bude nutné posoudit faktický stav závislosti dle okolností konkrétního případu.
[399] Viz předchozí poznámka - psychická závislost oběti na kybergroomerovi nemusí ještě zakládat kvalifikovanou skutkovou podstatu pohlavního zneužití při zneužití závislosti dítěte (§ 187 odst. 1, 2 TZ),

dětské pornografie), zneužití dítěte k výrobě pornografie, kuplířství nebo obchodování s lidmi, zavlečení, zbavení nebo omezování osobní svobody. Pakliže se pachateli podaří prokázat zastřešující záměr směřující k sexuálnímu zneužití, bude na místě posoudit předcházející jednání i jako přípravu k danému trestnému činu, resp. případně posoudit trestní odpovědnost za přípravu daného zvlášť závažného zločinu (§ 20 TZ), neboť pachatel cílenou manipulací oběti úmyslně vytváří podmínky pro jeho spáchání. Tak tomu bude v případě přípravy ke spáchání kvalifikované skutkové podstaty zvlášť závažného zločinu znásilnění, sexuálního nátlaku, pohlavního zneužití (pakliže pachatel zamýšlí zneužít svého postavení a z něho vyplývající důvěryhodnosti nebo vlivu), obchodování s lidmi, zavlečení.

Co se týče lehčí formy kybergroomingu, situace je z trestněprávního hlediska již méně pestrá. Kybergroomer sice může uvádět vybranou osobu v omyl nebo jejího omylu využívat, nicméně jeho jednání patrně nedosáhne takové intenzity, aby mohlo způsobit vážnou újmu na právech (ani to pravděpodobně nebude pachatelovým úmyslem, neboť usiluje spíše o jednorázové potěšení, než o dlouhodobý manipulativní vztah). Bude-li však ve větší míře lákat osobu mladší 18 let k sextingu, může se i v těchto případech dopustit přečinu ohrožování výchovy dítěte [§ 201 odst. 1 písm. a) TZ]. Dojde-li v rámci takové komunikace k nakládání s pornografií, bude na místě obdobná kvalifikace jako u kybergroomingu vůbec. Častější však bude ovšem svádění k pohlavnímu styku (§ 202 TZ), bude-li kybergroomer vědomě komunikovat s dítětem.[400] Jestliže si kybergroomer např. nahrává obnažující se oběť mladší 18 let (s jejím vědomím i bez něj) a taková nahrávka dosáhne úrovně pornografie, zneužije dítě k výrobě pornografie (§ 193 TZ nebo § 192 odst. 3 TZ).[401] Případné další nakládání s takovým dílem by pak naplňovalo skutkovou podstatu přečinu výroby a jiného nakládání s dětskou pornografií (§ 192 odst. 3 TZ).

Zbývá ještě doplnit, že nejde-li o znak základní skutkové podstaty, spáchání trestného činu na dítěti bývá často zvlášť přitěžující okolností vedoucí při alespoň nedbalostním zavinění k naplnění kvalifikované skutkové podstaty [§ 17 písm. b) TZ], jinak je nutno tuto okolnost posoudit jako obecně přitěžující [§ 42 písm. h), ev. i) TZ].

---

podobně jako je třeba ji uvážit u sexuálního nátlaku (§ 186 odst. 2 TZ).

[400] Resp. kybergroomer bude s touto eventualitou alespoň srozuměn, aniž by spoléhal z nějakého konkrétního důvodu, že tomu tak není – např. osoba na druhé straně vystupuje pod přezdívkou „Anička14“.

[401] V závislosti na tom, zda tak oběť činí zcela z vlastního popudu nebo až na základě vybízení atp. pachatelem.

10.4. Shrnutí k sexuálnímu vykořisťování dětí

Sexuální vykořisťování dětí v online prostředí bývá spojeno zejm. s pornografií, sextingem a kybergroomingem. Psychologie rozlišuje soft, hard a deviantní pornografii, právo prostou, dětskou a tvrdou, přičemž obě kategorie se mohou, ale nemusí prolínat. Pornografické weby obvykle používají tzv. disclaimer, aby nemohly být považovány za místo dětem přístupné, nicméně mládež se s pornografií online setkává relativně často (v horizontu předchozího roku cca třetina dětí ve věku 9-16 let), ať už jejich prostřednictvím nebo jinak. Pornografie je definována např. jako dílo, jehož jediným účelem je vyvolat/zvyšovat sexuální vzrušení, dětská pornografie pak zobrazuje nebo jinak využívá dítě (tj. osobu mladší 18 let) nebo osobu, jež se jeví být dítětem. Zapovězena je tedy i virtuální pornografie, a to s ohledem na zájem na ochraně mravních hodnot společnosti považující dětskou pornografii za škodlivou vůbec, tj. i bez zneužití konkrétního dítěte. V tomto duchu pak bylo v roce 2014 kriminalizováno i samotné získání přístupu k dětské pornografii (jakékoliv) prostřednictvím ICT – zákonodárce tak pod vlivem legislativy EU odpověděl na potřebu postihu specifické formy šíření dětské pornografie prostřednictvím ICT, které výrazně zvyšuje rychlost i masovost šíření (z hlediska času, prostoru, množství obsahu i počtu adresátů).

Sexting označuje posílání a sdílení sexuálně laděných zpráv, fotografií a videí. Mládež tak činí v rámci vlastního sexuálního zrání a sebeprezentace, ovšem někteří (častěji dívky) praktikují sexting i jako formu přivýdělku. V horizontu předchozího roku byla mezi českými dětmi ve věku 9-16 let cca 1/5 příjemců a 1/10 odesílatelů, nejčastěji chtějí upoutat pozornost a flirtují (cca polovina dotázaných ve věku 8-17 let). V souvislosti se sextingem může dojít zejm. k trestnému činu šíření pornografie, ať už při naplnění znaku „přenechává“ nebo „nabízí“ pornografické dílo dítěti, výroby a jiného nakládání s dětskou pornografií (a to i samotný dětský aktér např. jejím rozesláním), zneužití dítěte k výrobě pornografie, účasti na pornografickém představení, ohrožování výchovy dítěte. [§ 191 odst. 2 písm. a), § 192 odst. 3 al. 1, § 193, 193a, § 201 TZ].

Pod kybergroomingem se skrývá psychická manipulace oběti prostřednictvím ICT s cílem sexuálně ji využít. Zhruba ½ českých dětí ve věku 11-17 let komunikuje s osobami známými pouze online a zhruba třetina je ochotna se s nimi i reálně setkat. Kybergroomer kontaktuje řadu osob, s vybranými pak dál komunikuje i měsíce. Vyhledává a láká od nich zejm. intimní informace, působí empaticky a jako spřízněná duše, oběť postupně izoluje od sociálního okolí a ta se na něm stává psychicky závislou. Dříve či později dojde na sexting (i vzájemný),

nejednou podpořený nějakou formou úplaty. Posléze naléhá na osobní setkání, při odmítání hrozí ponejvíce ukončením vztahu a/nebo zneužitím dosud nabytých intimností (tajemství oběti, digitalizovaný obsah). Při setkání pak dochází k fyzickému sexuálnímu zneužití. Názorný příklad podává jedna z mediálně známých kauz kybergroomingu v ČR. V širším významu se kybergrooming používá ve smyslu nevyžádaného kontaktování osob na chatech, SNS atp., kdy dotyčný záhy stočí konverzaci na sexuální tematiku a vybízí k sextingu (a praktikuje jej), případně i za úplatu. Objevuje se též vydírání dospělých mužů, kterým pachatel hrozí zveřejněním jejich předchozí intimní konverzace s ním (vedené nejčastěji v domněnce komunikace s mladou slečnou), zde jde ovšem primárně o majetkový zisk, nikoliv sexuální uspokojení pachatele. Psychické trauma oběti kybergroomingu se odvíjí od intenzity vztahu s pachatelem (míra závislosti, izolace, délka vztahu, hloubka intimity a důvěry, množství sextingového obsahu atd.) a následné deziluze. Sdílená pornografie a sexting mohou deformovat vlastní sexualitu a vývoj zejm. v citlivém období dospívání, nemluvě o negativních dopadech samotného fyzického zneužití, dojde-li k němu. I při lehčí formě kybergroomingu pak zůstává v kyberprostoru množství digitalizovaného obsahu, nad nímž oběť odesláním kybergroomerovi zcela ztratila kontrolu. Kybergroomer bývá běžným uživatelem ICT, znalý v oblasti SNS, seznamek, chatů atp. a obeznámený s běžnými zálibami i problémy cílové skupiny. Bývá inteligentní, cílevědomý, trpělivý a chladnokrevný, leč schopný předstírat empatii. Mládež coby oběti představuje spíše zástupný objekt než sexuálně preferovanou skupinu vůbec. Oběti bývají ve věku 9-17 let, emočně deprivované a s problémy v rodině, s vrstevníky či jinými (např. problematické navazování vztahů). Varovným signálem může být závislost, vždy poukazující na nějaký jiný problém.

Od roku 2014 dopadá zejm. na kybergrooming skutková podstata trestného činu navazování nedovolených kontaktů s dítětem (§ 193b TZ). Poskytuje ochranu obětem mladším 15 let a postihuje návrh setkání ze strany pachatele za účelem sexuálního zneužití (de facto příprava sexuálního trestného činu). Navzdory určité problematičnosti (např. nekonzistence jazykového a gramatického výkladu názvu a samotného obsahu skutkové podstaty) a krátké době účinnosti se před rokem 2018 vyskytlo již 25 pravomocně odsouzených pachatelů (muži zejm. ve věku kolem 29 let), jejichž oběťmi byly převážně dívky ve věku 10-14 let, k prvnímu kontaktu došlo nejčastěji prostřednictvím FB. Z hlediska postihu kybergroomingu (a přidruženého jednání) přichází v úvahu dále vydírání, útisk, poškození cizích práv, šíření pornografie, výroba a jiné nakládání s dětskou pornografií, zneužití dítěte k výrobě pornografie, ohrožování výchovy dítěte, svádění k pohlavnímu styku [§ 175 odst. 1, § 177,

181, 191 odst. 2 písm. a), § 192, 193, 201 odst. 1 písm. a), § 202 TZ]. Také příprava daného zvlášť závažného zločinu (např. znásilnění dítěte), případně samotný sexuálně motivovaný trestný čin, a to se zohledněním spáchání činu na dítěti coby případné zvlášť nebo obecně přitěžující okolnosti [§ 17 písm. b), § 42 písm. h), ev. i) TZ].

11. Kyberšikana[402]

Kyberšikana, jedna z forem psychické šikany, patří mezi sociálně-patologické jevy. Agresor oběť úmyslně opakovaně ohrožuje, pronásleduje a psychicky týrá prostřednictvím ICT. Odehrává se tedy ve virtuálním světě, zpravidla bez přímého kontaktu, prolíná se ovšem s šikanou v reálném prostředí. Agresorem se může stát kdokoli bez ohledu na fyzickou vyspělost. Na rozdíl od běžné šikany není prostorově ani časově omezená: prostřednictvím mobilních telefonů a internetu pronásleduje dítě všude a neustále,[403] neomezuje se na školní prostředí a čas vyučování. S tím, jak snadno se na internetu šíří digitální obsah, je jednoduché rozšířit i dehonestující informace (text, fotografii i video), ať už pravdivé či nikoliv. Zejm. na SNS, portálech pro sdílení videí a veřejných chatech, kam má přístup kdokoliv. U rozvinutých šikan dochází k veřejnému hlasování, peticím, masovým komentářům atp. na úkor oběti, přičemž s počtem diváků úměrně narůstá i frustrace oběti. Kyberšikana nezanechává fyzické stopy, a snadno tak zůstává před okolím dlouho skrytá. Přesto působí závažná zranění (např. úzkostné poruchy, posttraumatické poruchy, deformuje rozvoj sociálních a morálních kompetencí). Zejména je třeba uvědomit si závažnost dopadů s ohledem na teprve se rozvíjející identitu dětí a dospívajících, potřebu uznání ze strany okolí a vztah digitálních domorodců ke kyberprostoru (blíže k tomu viz kapitoly **Kyberprostor a nová média**, **Komunikace a identita** a **Digitální otisk a SNS**). Anonymita (byť zdánlivá) posiluje účinnost násilných zpráv a útoků. Přestože bývá útočník ze stejného kolektivu jako oběť,[404] často zůstane záměrně skrytý, čímž zvýší strach a utrpení oběti. Kyberútoky u školních dětí je proto třeba je posuzovat jako možný ukazatel různě rozvinuté školní šikany vůbec.

Se šikanou (resp. zraňujícím jednáním) se v horizontu předchozího roku setkala téměř čtvrtina českých dětí ve věku 9-16 let, z toho cca 8 % online, především na SNS a prostřednictvím instant messagingu. Zhruba 12 % dětí přiznalo aktivní zraňující jednání v uplynulém roce (10 % tváří v tvář, 3 % online a 2 % přes mobilní telefon). Zvlášť zajímavým zjištěním je fakt, že kyberšikanována byla jen asi 4 % osob, které samy nešikanovaly, zatímco u šikanujících dětí to bylo přes 40 %.[405] Zhruba třetina dětí šikanovaných online pociťovala

[402] Kapitola vychází ze spoluautorského publikovaného textu (Brandejsová, a další, 2012).
[403] Samotný odklon od užívání ICT může znamenat bezprostřední ochranu a úlevu, nikoliv však řešení – např. absence na SNS, kterou používají ostatní spolužáci, může vést k ostrakizaci, a zároveň nevědomost oběti o probíhajících online útocích (např. další a další zahanbující fotomontáže) nijak nezmírní paralelní útoky v reálném prostředí (např. strkání, posměšky okolí).
[404] Oběť i agresor bývají ze stejné třídy, nebo alespoň školy. Stále sice převažuje šikana v reálném prostředí, avšak poměr se s rostoucím věkem dospívajících vyrovnává (Livingstone, a další, 2011 str. 62).
[405] Nejjednodušší vysvětlení, že kyberšikana slouží jako prostředek odplaty obětí reálné šikany vůči svým agresorům, již výzkumy vyvrátily – role oběti a útočníka se v reálném a virtuálním prostředí většinou nemění.

v důsledku toho velmi rozrušeně, pouhých 15 % bylo netknuto, negativní důsledky pociťovalo 40 % dětí ještě následující dny až měsíce. Tři čtvrtiny šikanovaných online se někomu svěřily, nejčastěji kamarádovi nebo rodiči (50 a 40 %). Téměř polovina v reakci blokovala útočníka a/nebo smazala došlé zprávy, pětina přestala na čas internet vůbec používat (necelé polovině z nich to však nijak nepomohlo).[406] Vysoká čísla potvrdil i výzkum kyberšikany dětí ve věku 11-17 let v českém prostředí v roce 2013. Podle něj se s kyberšikanou setkala polovina dětí. Byly to především verbální útoky, průniky na účty a obtěžování prozváněním (25-45 %), dále vyhrožování a zastrašování, ponižování a ztrapňování (zejm. šířením fotografií, méně často videí), „krádež" identity, vydírání. Zhruba 6 % dětí přiznalo vlastní zraňující jednání v souvislosti s ponižující fotografií, 3 % s videem (Univerzita Palackého v Olomouci, Seznam.cz, Google, 2014).

Fenoménem per se je kyberšikana učitelů,[407] s jejímiž projevy se setkala cca pětina učitelů (oproti cca 6 % obětí tradiční šikany). Zhruba ve třetině případů šlo o verbální útoky (online i sms atp.), ve čtvrtině o obtěžující prozvánění. Útoky využívají nejčastěji SNS, mobilní telefon a email, případně veřejný chat. Útočí většinou (učitelovi žáci 35 % známých útočníků) a ve třetině případů o takovém jednání vědí i kolegové (v 15 % ví i ředitel, ve 13 % naopak neví nikdo). Kyberšikanovaní pociťují mj. vztek, smutek a nejistotu a potýkají se s psychosomatickými problémy jako poruchy spánku, špatná koncentrace, bolesti hlavy (Kopecký, a další, 2016).

Často dochází k projevům kyberšikany v prostředí SNS, s vědomím i bez vědomí oběti: zveřejňování fotografií a videí, jízlivé komentování profilu oběti, posílání nadávek, vytěsňování ze skupiny vrstevníků pomluvami a urážkami, vytvoření falešného profilu oběti a jejím jménem společensky nepřijatelné projevy a „sebeprezentace". Dalším prostředkem jsou mobilní telefony (většina školních dětí disponuje vlastním telefonem: zasílání výhružných a urážlivých SMS (často z neznámých telefonních čísel), opakované prozvánění, nepříjemné hovory, fotografování a natáčení oběti. Může dojít až k „zavalení" oběti zprávami a telefonáty z mnoha čísel. Zneužíván bývá i telefon oběti: uváděn jako kontakt v nejrůznějších falešných inzerátech (porno seznamka, výhodná nabídka vozu atp.) - oběť se pak musí vypořádávat s dalšími nevyžádanými kontakty. Videoportály (typicky Youtube) slouží k umísťování dehonestujících videí, rostoucí počet shlédnutí umocňuje trauma oběti z množství

Zřejmě se tím potvrzuje teze, že (kyber)šikana se šíří jako nákaza, resp. představuje snadno předávaný sociální vzorec chování (konec konců stává-li se v kolektivu normou, odpadá sociální tlak omezující ji coby deviaci).

[406] Viz (Livingstone, a další, 2011), kapitola Bullying.

[407] Data se vztahují převážně k učitelům základních a středních škol.

přihlížejících. Využívá se také email oběti: zahlcování nevyžádaným obsahem (vč. pornografie), při získání/znalosti přístupového hesla nakládání se soukromou poštou a zasílání emailů jménem oběti. Chaty slouží opět k veřejnému ponižování, urážení oběti nebo jejímu vytěsňování ze skupiny diskutujících. Objevují se i weby s ponižujícími fotkami a videi oběti, doplněné o pikantní komentáře a výzvu ostatním uživatelům, aby se vyjádřili. Obvykle se kyberšikana prolíná s tradiční šikanou. Začíná-li jednání jako tradiční šikana, útočník postupně přidá i ICT formy útoku (SNS aj.). Naopak jednání začínající jako kyberšikana obvykle získává s postupem času víc a víc přihlížejících a dehonestace oběti se přenese i do reálného prostředí (posměšky, ústrky, ostrakizace až po tradiční šikanu).

Čím déle se šikana rozvíjí, tím větší počet dětí zasahuje, pozice agresorů se upevňují, útoky jsou brutálnější, traumata obětí se prohlubují a náprava je čím dál těžší. Kyberšikana prochází několika vývojovými fázemi kolektivu, od kterých se odvíjí závažnost útoků a dopadů pro oběť a míra zapojení přihlížejících, kteří se postupně stávají aktéry. V první fázi začíná být oběť v rámci skupiny ostrakizována, ignorována, odmítána. Při určité konstelaci sociálních vztahů ve třídě se může jednání posunout do druhé fáze: přitvrzení manipulace, zejm. při potřebě ventilovat napětí nebo zabavit se. Stále mohou rozvinutí jednání zabránit přihlížející, u nichž převládne soudržnost a přesvědčení o morální špatnosti takového jednání (je-li jich dostatečné množství oproti těm na straně útočníků). Ve třetím stádiu se vytváří relativně stabilní (kyber)šikanující jádro, které si počíná systematicky a zaměřuje se na nejslabší jedince (předchozí ostrakizace, „otloukánek“ sloužící k pobavení atp.). Není-li skupina šikanu odmítajících přihlížejících dostatečně silná, přijde čtvrtá fáze, kdy většina kolektivu postupně přebírá (kyber)šikanování dotyčného jako normu a stále více se na něm také podílí. (Kyber)šikana se šíří jako virus a vede ke ztrátě zábran podobně jako při davovém chování napodobujícím sociální vůdce skupiny – původní útočníky. V páté fázi se (kyber)šikany účastní prakticky celá skupina s jednoznačně rozdělenými rolemi obětí a agresorů bez výjimek[408] (Kolář, 1997), (Kolář, 2011).

Na rozdíl od běžného škádlení probíhá (kyber)šikana dlouhodobě, zákeřně a s vymezenými rolemi. Dlouhodobost je spojena s intenzitou jednání, kdy může oproti tradiční šikaně rozvíjející se dny až měsíce propuknout i během jediného dne: např. ráno ve škole dojde k trapnému incidentu, dopoledne umístí agresor jeho videozáznam či fotografie s komentáři na SNS a večer se jím „baví“ již celá škola. Zákeřnost spočívá v systematickém a záměrně

[408] Mnozí přihlížející / aktéři pak následně při zpětném ohlédnutí pociťují stud a zahanbení nad vlastním posléze těžko pochopitelným a ospravedlnitelným chováním, kdy se přidali na stranu agresorů.

zraňujícím jednání, nejde např. o jednorázové „vyřizování si účtů“ po hádce atp. Typické je také nerovnoměrné mocenské postavení aktérů, kteří mají jednoznačně jasno v tom, kdo je podřízený a nadřízený, byť to nemusí být pro osobu „zvenčí“ na první pohled zjevné – např. agresor nutí oběť ke (kyber)šikanování další oběti.

Původcem kyberšikany se může za určitých konstelací stát v podstatě kdokoli, existují však určité predispozice k řešení vztahů násilným způsobem, některé měnící se s vývojovými etapami dítěte. Agresorem se častěji stává žák necitlivý, nadprůměrně inteligentní, s dřívější zkušeností s (kyber)šikanou (v roli útočníka, oběti nebo i jen svědka), výrazně usilující (neúspěšně) o sebeprosazení, s představou vlastní výjimečnosti (nekritické protěžování rodinou), s poruchou psychického vývoje (skrytou či projevenou). Již na prvním stupni základní školy dochází ke kyberšikanování, přičemž agresorem bývá žák sociálně a emočně nezralý, s vlastní traumatickou zkušeností (CAN syndrom), poruchou učení či pozornosti, poruchami chování, hyperaktivní, nudící se, s rodinnými problémy (nefunkční rodina, probíhající rozvod atp.), s běžnými tvrdými tresty v rodině. Na druhém stupni bývá agresorem žák bezohledný a podezíravý, fyzicky či psychicky zdatný, s potřebou předvádět se a dokazovat svou převahu, bez svědomí, manipulátor, člen věkově starší party, z výchovně nebo emocionálně chudého rodinného prostředí. Na střední škole pak mívá agresor vysoké sebevědomí, rozvíjející se disociální poruchu osobnosti nebo probíhající psychické onemocnění, nezralý nebo negativně nastavený hodnotový systém, (mylnou) představou vlastní beztrestnosti a bývá z rodiny majetné nebo významně postavené.

I obětí kyberšikany se může stát prakticky kdokoli, důvodem může být cokoli: prospěch či majetkové poměry (horší nebo naopak lepší), vzhled, ta či ona vlastnost.[409] Výrazně větší roli než samotný zpravidla zástupný důvod na straně oběti hraje sociální klima třídy a ochota se přidat na stranu agresorů, resp. nedostatek síly nebo motivace přihlížejících k tomu se jim postavit.[410] Oběť kyberšikany bývá i obětí tradiční šikany, k čemuž ji obecně predisponuje zvýšená vulnerabilita: např. děti jakýmkoli způsobem se lišící (např. výší intelektu), vzorné i „zlobivé“, hrubé nebo naopak velmi citlivé atd. Nemusí tedy jít vždy o oslabení či handicap. Protože je školní (kyber)šikana projevem poruchy vztahů ve skupině, záleží na vývoji kolektivu, kde se konkrétní dítě ocitá, a na práci pedagoga se skupinovými vztahy.

[409] Útoky bývají obhajovány slovy „zasloužil si to,“ „je prostě taková divná,“ „provokuje“ atp.
[410] Postaví-li se útočníkům pouze oběť sama (zejm. v pokročilejších stádiích), vede to většinou spíše k eskalaci útoků: čím výraznější reakce oběti, tím větší uspokojení agresorů.

(Kyber)šikana se dotýká mnoha právních oblastí, počínaje metodickými pokyny MŠMT přes ochranu osobnosti a sociálně-právní ochranu dětí až po trestní právo. K povinnostem školy se řadí mj. předcházení sociálně patologickým jevům [§ 29 odst. 1 zák. č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon)], mezi něž nepochybně patří i (kyber)šikana. Odpovídají tomu i metodické pokyny vydávané MŠMT k jejímu předcházení a strategii řešení.[411] Žáci/studenti (dále jen „žáci“) jsou mj. povinni dodržovat školní a vnitřní řád a předpisy a pokyny školy k ochraně zdraví a bezpečnosti, s nimiž byli seznámeni [§ 22 odst. 1 písm. b) školského zákona], v nichž se obvykle stanoví i nepřípustnost kyberšikany, ať už mezi žáky navzájem nebo žáky a učiteli. Pakliže tak neučiní, škola jim může udělit některé z výchovných, resp. kázeňských opatření (§ 31 odst. 1 školského zákona): (podmíněné) vyloučení žáka nebo studenta ze školy (při splnění povinné školní docházky, § 31 odst. 2 školského zákona) a další kázeňská opatření, která nemají právní důsledky pro žáka nebo studenta. Těmi jsou napomenutí třídního učitele, důtka třídního učitele a důtka ředitele školy (§ 17 odst. 3 vyhl. č. 48/2005 Sb., o základním vzdělávání a některých náležitostech plnění povinné školní docházky). Zvláště hrubé opakované slovní útoky žáka nebo studenta vůči zaměstnancům školy nebo vůči ostatním žákům se považují za zvláště závažné zaviněné porušení povinností stanovených školským zákonem (§ 31 odst. 3 školského zákona).

V souvislosti s kyberšikanou hojně dochází k narušování práva na ochranu osobnosti, tedy základních lidských práv (čl. 10 Listiny), a to zejm. zasahováním do důstojnosti, vážnosti a cti člověka, jeho soukromí i projevů osobní povahy (srov. § 81 an. NOZ). Zasahovány jsou tedy jak složky osobnosti (soukromí, čest, důstojnost), tak projevy osobní povahy: především vizuální projevy (podoba a vzhled člověka), ale i jeho zvukové projevy, písemnosti osobní povahy atd. (Lavický, 2014 str. 396). Důstojnost lze charakterizovat jako „elementární úctu k člověku jako rozumem nadané živé bytosti a k jeho jedinečné lidské osobnosti ... minimum všeobecně uznávaných a dodržovaných pravidel etiky a slušnosti“ (Lavický, 2014 str. 412). Čest jako „vlastní vnitřní náhled člověka na ocenění sebe sama a jeho postoj k vlastním elementárním životním hodnotám a představám“ (Lavický, 2014 str. 423), kterým (kyber)šikana otřásá v samotných základech, zejm. v situacích, kdy již (kyber)šikana dospěla

[411]Metodický pokyn ministryně školství, mládeže a tělovýchovy k prevenci a řešení šikany ve školách a školských zařízeních, č.j. MSMT-21149/2016, a především Metodické doporučení k primární prevenci rizikového chování u dětí a mládeže, č.j. 21291/2010-28, s v roce 2017 aktualizovanou přílohou č. 7 – Kyberšikana (MŠMT). MŠMT vytvořilo ve spolupráci s dalšími subjekty i Národní strategii primární prevence rizikového chování dětí a mládeže na období 2013-2018, kam zahrnulo vedle netholismu a sexuálního rizikového chování mj. i kyberšikanu aj. rizikové formy multimediální komunikace (Ministerstvo školství, mládeže a tělovýchovy ČR, 2013 str. 9).

do takového stádia, že kolektiv nelze snadno napravit, „vyléčit“, a rodiče oběti se rozhodnou raději změnit školu. V takových případech není výjimkou opakování stejné situace na nové škole,[412] což oběť jen utvrdí ve vsugerovaném přesvědčení o vlastní méněcennosti. O vážnosti při probíhající (kyber)šikaně pak lze hovořit jen s velkou nadsázkou: „uznání člověka v okolí, jeho postavení ve společnosti a prokazování úcty ze strany ostatních“ (Lavický, 2014 str. 423). Soukromí zahrnuje „především možnost vlastního uvážení zda, popř. v jakém rozsahu a jakým způsobem mají být skutečnosti osobního soukromí člověka zpřístupněny jiným subjektům“ (Lavický, 2014 str. 444). K relativně běžnému porušování soukromí dochází při (kyber)šikaně v podobě zveřejňování jinak soukromé komunikace (např. předstírání virtuálního vztahu agresorem a následné zveřejnění intimní konverzace), obsahu emailové schránky,[413] fotografií ze „zapůjčeného“ mobilního telefonu oběti (např. vlastní sextingové fotografie) atp. Dochází tak i k porušování práva na ochranu projevů osobní povahy (srov. § 84 an. NOZ) vč. práva k podobě člověka, neboť „významnou součástí tohoto práva je i osobnostní oprávnění člověka osobovat si svoji podobu. Tedy možnost člověka požadovat, aby k němu byla přiřazována jeho podoba a aby byl s touto podobou identifikován. To spočívá zejm. v možnosti bránit se přiřazení podoby jiného člověka nebo naopak zamezit použití vlastní podoby ve vztahu k jinému člověku“ (Lavický, 2014 str. 504). Typicky se tak děje zneužíváním účtů na SNS, tedy tvorbou falešného profilu s podobou oběti a jiným jménem anebo se jménem oběti a cizí podobou. Častým protiprávním jednáním bývá také neoprávněné zaznamenávání projevů osobní povahy, a to v podobě obrazových, audiovizuálních a zvukových záznamů, neboť NOZ poskytuje ochranu i jiným projevům osobní povahy než pouze výslovně zmíněné podobě. Typicky jde o focení a filmování oběti bez jejího souhlasu a následné zveřejnění záznamu (na SNS, videokanálu, rozeslání „vtipně“ upravených fotografií přes Instagram atp.). K soukromoprávní i veřejnoprávní deliktní odpovědnosti nezletilých viz kapitola **Děti v online prostředí jako oběti i pachatelé**.

K dopouštění se přestupků dochází při (kyber)šikaně poměrně snadno,[414] zejm. proti občanskému soužití zesměšněním nebo hrubým urážením nebo úmyslným narušením občanského soužití schválností nebo jiným hrubým chováním vůči jinému (§ 7 odst. 1

[412] Zakušení role oběti představuje viktimizační faktor – oběť se „naučí“ daný vzorec chování, „zná“ ho a snadno k němu sklouzne, což ostatní děti vycítí a při určité konstelaci opět propukne (kyber)šikana i v novém kolektivu.
[413] Na základní škole děti velmi často znají vzájemně své přístupové údaje – typicky např. jako „důkaz přátelství nejlepší kamarádky“ nebo pro jejich jednoduchost (např. bezpečnostní otázka dotazující se na jméno třídní učitelky).
[414] Pochopitelně tam, kde již připadá v úvahu deliktní odpovědnost pachatele, viz kapitola **Chyba! Nenalezen zdroj odkazů.**.

písm. a) a/nebo c) bod 3 a/nebo 4 zák. o některých přestupcích). Dle důvodové zprávy[415] je „pojmovým znakem přestupku nactiutrhání skutečnost, že se jedná o výrok urážlivý nebo zesměšňující a dále povědomost pachatele o tom, že se v dané situaci a v dané skupině obyvatel jedná o výrok hanlivý. Musí však jít o výrok, který překračuje svou intenzitou pouhou nevhodnost, výrok dehonestující a hrubě urážlivý z objektivního hlediska.“[416] V tomto směru bude proto záležet např. na běžném chování i používaných výrazech v daném třídním kolektivu, zda již např. nadávky dosahují intenzity hrubé urážky, ovšem pouze za předpokladu, že dané výroky nepřekročí rámec třídy. U tradiční šikany tak bude záležet kromě samotných aktérů na fyzicky přítomných osobách, naproti tomu u kyberšikany může být publikum prakticky neomezené.[417] V některých případech tak budou kritéria na intenzitu hrubosti u kyberšikany přísnější, jindy naopak mírnější.[418] O „schválnosti“ lze uvažovat u kyberšikany např. při soustavném mření aktivit oběti online (např. při vytváření společného projektu online třídou v rámci výuky) nebo nevhodném a obtěžujícím prozvánění, o „jiném hrubém jednání“ při vyhrožování jinou újmou než na zdraví (Jemelka, a další, 2017 str. 1061)[419] - např. zničení avatara nebo úprava profilu na SNS, nebude-li již přicházet v úvahu naplnění znaku „jiné těžké újmy“ a eventuální trestněprávní odpovědnost. V úvahu přichází též odpovědnost za přestupek proti majetku, byť to v souvislosti s kyberšikanou nebude tak časté. Mohlo by jít např. o způsobení škody na cizím majetku úmyslným podvodem nebo krádeží [např. převod účtu jménem oprávněného uživatele nebo jeho přisvojení, § 8 odst. 1 písm. a) bod 3 nebo 1 zák. o některých přestupcích] nebo neoprávněným užíváním cizího majetku při neoprávněném přístupu na herní účet oběti [§ 8 odst. 1 písm. b) zák. o některých přestupcích] a jeho užívání, případně zkonzumování (např. „spotřebování“) nastřádaných předmětů (nemluvě o případném neoprávněném přístupu k počítačovému systému a nosiči informací v takovém případě, § 230 TZ).

Při nejzávažnějších prohřešcích kyberšikany mohou agresoři naplnit řadu skutkových podstat trestných činů. Často se tak bude dít prostřednictvím neoprávněného přístupu k počítačovému systému a nosiči informací – profilu oběti na SNS. V prvé řadě už samotný průnik na cizí účet naplňuje znak překonání bezpečnostního opatření (typicky znalostí, vylákáním nebo

[415] Odkazující mj. na rozsudek Nejvyššího správního soudu sp. zn. 2 As 60/2006 ze dne 17.1.2007.
[416] Viz komentář k § 7 (Vláda ČR; Poslanecká sněmovna PČR, 2015).
[417] Nepůjde-li např. o chatovací místnost přístupnou pouze určité skupině osob – pak by v úvahu připadalo posouzení pouze z jejich hlediska.
[418] Např. v rámci „otrlého“ kolektivu běžně používajícího vzájemné nadávky konkrétní pronesený výrok nemusí působit natolik hrubě, aby již mohl zakládat přestupek, avšak při zveřejnění stejného výroku online před širokým publikem již může dotyčného dehonestovat (samozřejmě nelze opomenout alespoň nedbalostní zavinění ze strany pachatele vůči hrubě urážlivé povaze výroku).
[419] Viz.

uhádnutím hesla), a tím získání neoprávněného přístupu k PS - účtu na SNS (§ 230 odst. 1 TZ). U pouhého průniku však obyčejně nezůstane, nýbrž pachatel jde zpravidla dále a s cizím účtem neoprávněně manipuluje (§ 230 odst. 2 TZ): data (např. fotografie) si zkopíruje [písm. a)] nebo smaže [písm. b)], změní statusové aj. údaje oběti [písm. c)] a přidá vlastní, upravené fotografie [písm. d)]. Samotné předchozí vylákání přístupových údajů za tím účelem od oběti by pak naplnilo znaky opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 TZ). „Oblíbená" je také následná změna přístupových údajů nebo smazání/znepřístupnění profilu oběti vůbec,[420] což už by ve výjimečném případě mohlo naplnit i znaky trestného činu poškození cizí věci, neboť pachatel by učinil cizí věc (účet na SNS) neupotřebitelnou (§ 228 odst. 1 TZ) – pokud by se jednalo např. o marketingový účet s navázanými kontakty, jehož hodnota by dosáhla výše alespoň nikoli nepatrné (tedy nejméně 5.000 Kč, § 138 TZ).[421] Kromě poškození cizí věci může takovým „zabráním si" účtu dojít i na poškození cizích práv (§ 181 TZ), zejm. při tzv. „krádeži" identity a jednání prostřednictvím účtu oběti na SNS jejím jménem[422] – relativně běžný projev virtuálního násilí směřující k poškození nemajetkových práv v podobě narušení zejm. sociálních vztahů poškozeného, oběti kyberšikany s okolím, ale i rodinných vztahů. Obdobným způsobem, byť méně často bývají využívány i emailové účty. Kromě falešných a neoprávněně užívaných profilů na SNS bývají také vytvářeny profily, stránky, blogy atp. s cílem zesměšnit a očernit oběť. Nelze v takovém případě vyloučit natolik závažný zásah do vážnosti, cti a důstojnosti oběti, že již bude namístě postih trestněprávními prostředky (pomluva, § 184 TZ), půjde-li o nepravdivé údaje způsobilé např. vážně narušit rodinné vztahy (např. tvrzení o sexuálních praktikách oběti vůči svému sourozenci). V úvahu přichází také tzv. hate crime.

Oběti kyberšikany mnohdy hovoří o obtěžujícím prozvánění, které samo o sobě sice nemůže překročit intenzitu přestupku, avšak ve spojení s dalším jednáním (např. vyhrožováním jinou újmou - vyzrazení tajemství rodičům poškozeného atp.) již může naplnit znaky trestného činu nebezpečného pronásledování (§ 354 TZ), neboť poškozeného vytrvale kontaktuje, pokud bude takové jednání způsobilé vzbudit důvodnou obavu např. o zdraví osob jemu blízkých - např. nervové zhroucení rodiče (Šámal, 2012 str. 3298). Opomenout nelze ani nebezpečné vyhrožování (např. anonymní opakované vzkazy z různých zdrojů doplněné detailním

[420] Např. profil na FB nelze smazat, ale pouze deaktivovat, tj. znepřístupnit.
[421] Přichází v úvahu např. u úspěšného Youtubera, sportovní celebrity atp.
[422] V takovém případě nemusí jít ani o vlastní profil oběti, ale o zcela ad hoc vytvořený profil agresorem, o němž se oběť v počátku ani nemusí dozvědět. Pak by zůstala odpovědnost agresora zřejmě v rovině občanskoprávní ochrany osobnosti oběti.

itinerářem dne poškozeného, § 353 TZ) a vydírání (např. nucení oběti k šikanování 3. osoby pod pohrůžkou zveřejnění předchozí intimní konverzace s agresorem, § 175 TZ), případně útisk (při rozvinuté šikaně v podobě „otrokářské společnosti“ již agresor nemusí oběť ani fakticky „nutit“, § 177 TZ). Pro oběť spíše jen obtěžující je potom např. zahlcování emailové schránky pornografií [přenechání pornografie spíše než pouhé nabízení, § 191 odst. 2 písm. a) TZ, případně též ohrožování výchovy dítěte dle § 201 odst. 1 písm. a) TZ].[423] Zveřejnění pornografického videa zachycujícího oběť-dítě (např. vlastní sextingové fotografie nalezené v telefonu oběti) by pak již bylo výrobou a jiným nakládáním s dětskou pornografií (§ 192 odst. 3 TZ). Blíže k tomu viz kapitola **Sexting**. Z častějších projevů kyberšikany zbývá zmínit ještě porušení tajemství listin a jiných dokumentů uchovávaných v soukromí (např. zveřejnění fotografií z mobilního telefonu oběti, § 183 TZ), případně méně časté porušení tajemství dopravovaných zpráv (např. zachycení emailu určeného oběti předtím, než má reálnou možnost se s ním seznámit, § 182 TZ). K majetkové kriminalitě v souvislosti s kyberšikanou dochází oproti virtuálnímu násilí méně často, nelze ji ovšem vyloučit, a to zejm. v podobě loupeže (§ 173 TZ), krádeže (§ 205 TZ) a podvodu (§ 209 TZ) v souvislosti s herními účty (viz kapitola **Avatar**). Falešné i neoprávněně užívané profily na SNS sice bývají prostředky podvodného jednání, nicméně spíše při jednání s primárním cílem obohacení pachatele než poškození oběti, tedy nikoliv jako součást kyberšikany. Nakonec přichází v úvahu v online prostředí ještě účast na sebevraždě (např. utvrzování oběti v předsevzetí provést sebevraždu, § 144 TZ), byť bude úmyslné zavinění agresora v tomto směru jen výjimečné.[424]

Při úvahách de lege ferenda se v souvislosti s bojem proti kyberšikaně nabízí snížení trestní odpovědnosti dětí na 14 let, o čemž se konec konců diskutovalo už v souvislosti s přijetím TZ. Lze se ovšem plně ztotožnit s důvody uvedenými v důvodové zprávě k zákonu novelizujícímu TZ ještě před jeho účinností, který věkovou hranici trestní odpovědnosti opětovně zvýšil z navržených 14 na 15 let, a to i s ohledem na množství navazujících právních předpisů, které by vyžadovaly obdobnou úpravu, právní kontinuitu a celkovou změnu koncepce přístupu k dětem (Vláda ČR; Poslanecká sněmovna PČR, 2009).

[423] Blíže k tomu viz kapitola **Pornografie a děti online**.

[424] U tradiční šikany může dojít až na rituální popravu (Kolář, 1999). Ačkoliv k sebevraždám v důsledku kyberšikany dochází (Wikipedia), většinou jde o vnitřní rozhodnutí oběti, nanejvýš podpořené agresory (agresor spíše oběť k sebevraždě svým jednáním dožene, nikoliv však s úmyslem ji k ní pohnout nebo ji v učiněném rozhodnutí utvrdit). K sebevraždám a sebevražedným paktům viz kapitola **Netholismus**.

.

Český právní řád nabízí poměrně propracovaný systém sociálně-právní ochrany dětí, ať už co do práce s ohroženými dětmi nebo provinilci.[425] Velmi ovšem záleží na přístupu a jednání všech konkrétních zainteresovaných osob, počínaje rodiči přes učitele po pracovníky orgánu sociálně-právní ochrany dětí, případně i orgány činnými v trestním řízení. Při citlivém a odpovídajícím přístupu lze mnohdy jednání kolektivu usměrnit vlastními silami kolektivu a školy za pomoci výchovného poradce nebo psychologicko-pedagogické poradny. Přizvání dalších osob (orgán sociálně-právní ochrany dětí) již znamená poměrně výrazný zásah, neboť přichází osoba zvenčí, neznalá daného kolektivu a vztahů v něm, nemluvě o případném nezbytném zapojení orgánů činných v trestním řízení a hrozící sekundární viktimizaci oběti.

Školy by jistě uvítaly širší pravomoci při postihu agresorů, neboť v současnosti se velmi často potýkají s nadužíváním odvolávání se na princip enumerativnosti veřejnoprávních pretenzí ze strany rodičů agresorů bránících postihu svého potomka s tím, že k útokům online docházelo mimo čas vyučování a půdu školy, a tudíž nelze hovořit o porušování školního řádu či jiném titulu udělení kázeňského opatření. K tomu lze říci tolik, že prakticky nemůže nastat situace, kdy by rozvíjející se kyberšikana nepřešla i do školního prostředí, ale nemusí se tak stát hned – může se rozvíjet plíživě a nějaký čas bez vnější detekce. Neřešené jednání při určité sociální konstelaci však vždy nabude na intenzitě. Školy se nicméně vyrovnávají i s takovou situací mnohdy se ctí, když při podezření na kyberšikanu se jí zabývají a věnují všem zúčastněným náležitou pozornost, aniž by přistoupily ke kázeňskému opatření, neboť již mnohdy samotné (citlivé) projednání věci a upozornění na to, že nepřejde bez povšimnutí, v počátečních fázích kyberšikany stačí k uklidnění atmosféry.

V úvahu přichází také zvýšení minimálního věku požadovaného pro používání SNS, na čemž pracuje český zákonodárce v reakci na GDPR v podobě zákona o zpracování osobních údajů, který tuto hranici zvyšuje na 15 let (viz kapitola **Zneužití technické stránky internetu**). Domnívám se ovšem, že právní úprava v této věci nepřinese výrazný užitek, neboť již nyní dochází u nejužívanějšího FB k porušování hranice minimálního věku 13 let ve velkém měřítku, počínaje dětmi ve věku 9 let. Při uzákonění minimální věkové hranice by však např. orgány sociálně-právní ochrany dětí mohly zvýšit tlak na rodiče, aby věnovali aktivitám svých dětí online náležitou pozornost vzhledem k možnému porušování zákona. Negativním důsledkem by ale zároveň bylo hrozící vyloučení používání SNS v souvislosti s vyučováním

[425]S výjimkou některých procesních práv dětí v souvislosti s řízením ve věcech péče soudu o nezletilé dle Hlavy III. Části I. ZSVM a § 466 písm. b) zák. o zvláštních řízeních soudních, zejm. obsah a rozsah „obhajoby" dítěte mladšího 15 let, které mělo spáchat čin jinak trestný.

na základních školách, které by tak ztratily možnost učit děti správnému a slušnému chování v online prostředí SNS (pokud by k tomu zákonní zástupci nedali souhlas). Tzn. používání SNS dětmi by se zřejmě vrátilo o krok zpět k místu bez pravidel, a tak se jako vhodnější úprava jeví uzákonění nejnižšího možného věku, a to 13 let (čl. 8 odst. 1 GDPR).

11.1. Shrnutí ke kyberšikaně

Při kyberšikaně agresor využívá k jednání ICT, jednání se ovšem obvykle prolíná i s tradiční šikanou. Není časově ani prostorově omezená a útočník může zůstat po určitý čas i anonymní, byť je nejčastěji ze stejné školní třídy jako oběť. Se snadností, rychlostí a masovostí sdíleného obsahu online se lavinově šíří i dehonestace umocňující frustraci oběti s rostoucím počtem přihlížejících. Se zraňujícím jednáním online má zkušenost (v horizontu uplynulého roku) zkušenost cca čtvrtina až polovina českých dětí, přičemž cca 5-10 % v roli agresora. Mezi oběťmi figurují i učitelé základních a středních škol (cca 20 % učitelů). Nejčastěji se kyberšikana projevuje na SNS (zejm. FB), a to v podobě verbálních útoků a průniků na účet. Agresoři zveřejňují ponižující komentáře, fotografie i videa a vytváří falešné profily se zesměšňující „sebeprezentací“ oběti. Mobilní telefony pak používají především k obtěžujícímu prozvánění a pořizování záznamů oběti, které pak umístí na videoportál, typicky Youtube. Nevynechávají ani emaily (zahlcování pornografií atp.), chaty, ad hoc weby. Kyberšikana prochází několika vývojovými fázemi kolektivu: od ostrakizace přes manipulaci, systematicky jednající jádro a kyberšikanování jako postupně převažující normu až po účast prakticky celého kolektivu v roli agresorů. Postup do jednotlivých fází je zásadně ovlivněn sociálním klimatem třídy a reakcemi okolí (přihlížející či protestující). Kyberšikana probíhá dlouhodobě, zákeřně a s vymezenými rolemi agresorů i oběti. Původcem může být kdokoli, častěji již s vlastní dřívější zkušeností s (kyber)šikanou, toužící po sebeprosazení, nezralý, s psychickou poruchou, pocitem vlastní výjimečnosti atp. Podobně je tomu u oběti, samotný deklarovaný důvod kyberšikanování (např. lepší či naopak horší prospěch) bývá jen zástupný. Bývá to dítě od ostatních se lišící, s předchozí zkušeností v roli oběti (kyber)šikany.

Kyberšikany se dotýkají metodické pokyny MŠMT (prevence), školský zákon a prováděcí předpisy (povinnosti žáků a kázeňská opatření). Dále je zde občanskoprávní rovina vzhledem k obvyklému porušování ochrany osobnosti v mnoha podobách (důstojnost, soukromí, projevy osobní povahy atd., § 81 an. NOZ), případně odpovědnost za škodu. Dochází i

k přestupkům, zejm. proti občanskému soužití (§ 7 zák. o některých přestupcích), případně proti majetku (§ 8 zák. o některých přestupcích).

V trestněprávní rovině přichází v úvahu řada skutkových podstat, počínaje neoprávněným přístupem k počítačovému systému a nosiči informací ve všech základních variantách (§ 230 TZ), zejm. ve spojení se SNS. Předcházet může opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 TZ). „Zabráním" si cizího profilu a aktivitou na něm může dojít i k poškození cizí věci (§ 228 odst. 1 TZ) nebo poškození cizích práv (§ 181 TZ), jindy k pomluvě (§ 184 TZ). Další jednání budou při kyberšikaně již méně častá, nikoliv však zcela výjimečná: nebezpečné pronásledování (§ 354 TZ), nebezpečné vyhrožování (§ 353 TZ), vydírání (§ 175 TZ), útisk (§ 177 TZ), šíření pornografie (§ 192 TZ), ohrožování výchovy dítěte (§ 201 TZ), výroba a jiné nakládáním s dětskou pornografií (§ 192 TZ), porušení tajemství listin a jiných dokumentů uchovávaných v soukromí (§ 183 TZ), porušení tajemství dopravovaných zpráv (§ 182 TZ), loupež (§ 173 TZ), krádež (§ 205 TZ), podvod (§ 209 TZ), účast na sebevraždě (§ 144 TZ).

De lege ferenda přichází v úvahu např. snížení hranice trestní odpovědnosti na 14 let, zřejmě by to však výraznější změnu z hlediska kyberšikany nepřineslo. Školy by uvítaly širší pravomoci při postihu agresorů, zejm. co se týče vymezení „půdy školy". Nabízí se též úprava věkové hranice pro používání SNS (souhlas se zpracováním osobních údajů), kterou připravovaná národní legislativa snižuje z 16 let navržených GDPR na 15, vhodnější by však v tomto směru bylo snížení na minimálně možných 13 let, aby bylo možné výchovně pracovat se SNS i v rámci výuky na základní škole.

12. Násilí a hate crime[426]

V posledních letech se lze setkat s různými formani anti-hate kampaní, z těch největších např. evropská No Hate Speech (Council of Europe), (NCBI). Reagují na hojné nenávistné výroky v online prostředí (SNS, blogy, weby, diskuse atd.). Nesnášenlivé projevy mohou být namířeny prakticky proti jakékoliv skupině (vč. projevů menšiny vůči většinové společnosti) a byť na jednu stranu představují projev základního lidského práva na svobodu projevu, tato není bezbřehá, nýbrž vždy je třeba vážit ji i v porovnání s jinými lidskými právy a svobodami, v případě nenávistných výroků zejm. s právem na ochranu osobnosti, nemluvě o omezení svobody projevu zákonem (čl. 17 odst. 1, čl. 10 odst. 1 a 2 a čl. 17 odst. 4 Listiny ve spojení zejm. s TZ). Nenávistné výroky se zaměřují na osoby odlišující se barvou pleti, vyznáním, sexuální orientací, IQ atp., ať už s cílem vyjádřit hodnotové postoje, rozproudit emoce diskutujících (tzv. trolling) nebo vyzvat k jednání. Tzv. hate speech může být svým způsobem i projevem určitého občanského postoje. Online participace sice představuje mnohem snazší jednání (oproti např. organizování hnutí), na druhou stranu postrádá efekt fyzicky přítomného sdílení a zřejmě může poskytovat i menší uspokojení při dosažení úspěchu, úměrné vynaloženému úsilí. Zdá se, že online participace nemusí mít žádný vliv na pozdější občanskou angažovanost, tíhne však ke zpochybňování systému a autorit. Výsledný vliv na větší autonomii a individualitu jedince pak může variovat od posílení odmítání sociální nespravedlnosti a demokratických postojů po radikalizaci a nesnášenlivost (Macháčková, a další, 2017 str. 10).

Specifickým typem „hate projevu“ je i násilí zaměřené na určitou skupinu (bezdomovci, etnikum aj.), např. v podobě tzv. happy slappingu (slouží např. jako iniciační rituál přijetí do party): natáčení reálného fyzického napadení nejčastěji náhodně vybrané netušící oběti bez vztahu k útočníkovi s cílem získat maximálně šokující autentické video pro zveřejnění na některém z portálů pro sdílení videí (Brandejsová, a další, 2012 str. 7). Kromě toho koluje množství videí s násilným obsahem, počínaje násilnými animacemi[427] přes týrání zvířat až po veřejné popravy (2014). Obdobně se násilí objevuje ve zpravodajství, filmech a seriálech, počítačových hrách. Násilný obsah bývá atraktivní především pro chlapce v období dospívání. V kontextu absence realistického povědomí o fyzických možnostech lidského těla a bolesti

[426] Kapitola částečně vychází ze spoluautorského textu (Brandejsová, a další, 2012) a z (Lukášová, 2012).

[427] Nejpoužívanější Youtube již ovšem přijal opatření směřující k omezení mj. nenávistného obsahu proti jednotlivcům nebo skupinám, určitého násilného obsahu, výhrůžek a kyberšikany (Youtube), a to až pod sankcí zrušení účtu při trojnásobném porušení pravidel během uplynulých 3 měsíců (Google). Zakazuje také (vedle sexualizace nezletilých) zobrazování škodlivých nebo nebezpečných úkonů zahrnujících nezletilé (Google), de facto ve všech případech však v návaznosti na případném nahlášení nevhodného obsahu uživateli samotnými.

(viz kapitola **Děti v online prostředí jako oběti i pachatelé**) žijí v představě, že v podstatě o nic nejde, bez ostychu nebo vcítění se jsou schopni si násilí na mobil natočit a/nebo sdílet. Násilí online se zdá být normou a uspokojuje potřebu bojovnosti a soutěžení nenaplněnou v reálném prostředí.

Ve spojení s násilím i bez něj se projevuje online i extremismus: weby, blogy, profily na SNS, videoportály, sdílení emailem a P2P.[428] Extremistický obsah se často zdá na první pohled nevinný: anketa vtipů (s příslušnými komentáři), zkresleně, leč atraktivně podané historické události (např. Leopold Hilsner) vč. přidružených odkazů na další zdroje informací (dále manipulující), prezentace hudebních skupin atp. Skrývají mnohdy symboliku v logách, obrázcích, textech webů i skladeb atp.: symboly (např. číslo 88 odkazující na nacistický pozdrav Heil Hitler), font písma atp. (Eichler, a další, 2006). Pravidelná Čtvrtletní zpráva o extremismu Odboru bezpečnostní politiky MV[429] za 2. čtvrtletí roku 2018 hovoří ve spojitosti s extremismem/projevy nesnášenlivosti online o omezení se na komentování aktuálního dění v internetovém prostoru ze strany tradičních extremistických subjektů (Národní demokracie aj.), útocích na muslimy a imigranty téměř výhradně online a zpravidla na popud zahraničních incidentů nebo zkreslených či vymyšlených zpráv a o omezení se Antifašistické akce na monitorovací články online. Zmiňuje ovšem také tzv. kvazi-mediální projekty jako nejprogresivnější a nejaktivnější prvek na české scéně, a to v podobě vytváření pocitů strachu a paniky z migrantů, kritiky „zkažené“ EU (s protipólem vychvalované Ruské federace), opěvování panslovanství (Ministerstvo vnitra. Odbor bezpečnostní politiky, 2018 stránky 3-6). Zatím poslední zpráva (za 3. čtvrtletí) pak pouze sporadicky zmiňuje mediální zveličování významu domobran prezentujících se online, propagaci anarchistického hnutí: propagace násilných akcí a vybízení k nim (Ministerstvo vnitra ČR, 2018 str. 5 a 6). Extremismus souvisí s komplexem méněcennosti, který často pramení z vědomí závislosti na druhých lidech v moderní společnosti, a snahou tento stav překonat získáním určité sociální pozice a s ní i moci. Sociální bezmoc (neschopnost řešit náročné a konfliktní situace jinak než násilně) přivádí dospívající mezi typologicky obdobné jedince. Svět považují za “nebezpečné místo”, kde je násilí prostředkem/technikou řešení prožívaných konfliktů. Jejich sebevědomí a úspěšnost bývají nízké, sami si netroufají projevit své pocity (bezmoc, frustraci, nenávist, touhu po seberealizaci). Ve skupině obdobně smýšlejících a cítících se to ale mění - vzájemně se podporují, sdílejí obdobné názory, přejímají charakterizující znaky (způsob oblékání,

[428] Např. podle šetření mezi experty Policie ČR po roce 2010 se tito cca v polovině relevantních případů zabývali i vytvářením a/nebo rozšiřováním závadového obsahu, vč. online (Holas, 2013 str. 78).
[429] Publikováno jako Problematika extremismu na území České republiky (Ministerstvo vnitra ČR).

symboliku, hudbu apod.). Samotné extremistické projevy online se však mládeže coby pachatelů dotýkají zřejmě jen v malé míře.[430]

Internet a zejm. SNS představují živnou půdu prakticky pro jakoukoliv formu radikalizace nejen coby platforma extremismu, ale zejm. jako místo pro sdružování skupin reprezentujících nepřeberné množství názorů, hodnotových představ i emočních přesvědčení a (i)racionálních argumentů (vč. těch odporujících si, nepravdivých, nepřesných atp.). Kromě nesporných pozitiv (viz kapitola **Komunikace a identita**) to může vést paradoxně k faktickému omezení diskuse, neboť řada uživatelů vyhledá raději podobně smýšlející osoby, než by své výroky ospravedlňovali před názorovými odpůrci. Čím vyhraněnější je smýšlení dané skupiny, tím méně se v ní objevují kritické názory odporující převažujícímu mínění, což ještě umocňuje onu vyhraněnost, a to až po odtržení od reality v zajetí vlastních iluzí (např. přesvědčení o dlouhodobě plánované likvidaci evropské populace zavalením muslimskými imigranty).[431] K tomu se přidává tendence přikládat větší význam informacím podporujícím vlastní stávající názor (s upozaděním těch opačných),[432] což ještě umocňují cookies, díky nimž vyhledávače, zpravodajské servery aj. vybírají nabízený obsah částečně v souladu s tím, co uživatel nedávno vyhledal.

K právu na svobodu projevu a porušování základního lidského práva na ochranu důstojnosti a cti viz kapitola Kyberšikana, kromě samotných projevů nesnášenlivosti poškození trpí např. zveřejňováním osobních údajů (jméno, adresa atp.) i výzvami k útokům na ně online i offline. Často se jedná o obsah umístěný fyzicky na serverech ve státech s nižším právním omezením daných jednání (např. v USA s převažujícím zájmem na ochraně svobody slova).[433] Trestní zákon však považuje za trestný čin spáchaný na území České republiky i takový, jímž pachatel v ČR porušil nebo ohrozil zájem chráněný trestním zákonem nebo měl-li alespoň zčásti takový následek v ČR nastat [§ 4 odst. 2 písm. b) TZ].[434] Z hlediska místní působnosti lze proto zákon ČR co do trestnosti případného spáchání trestného činu v případě webových stránek aplikovat vždy, je-li možné vyvolat daný obsah na území ČR (tj. zobrazit prostřednictvím ICT, např. v mobilním telefonu). K tomu ovšem musí přistoupit záměr pachatele, aby webová stránka byla vyvolána právě v ČR, samotná pouhá možnost vyvolání

[430] Zaznělo na konferenci VII. kriminologické dny v Ústí n. Labem v lednu 2019 (Kalibová, 2019). V podobném duchu se vyjadřují i učitelé středních a zejména základních škol, kteří se dle svých slov setkávají s projevy extremismu u dětí jen zřídkakdy.
[431] Blíže k tomuto procesu viz The Lone Wolf (Bartlett, 2015).
[432] Nedávno potvrdil i probíhající výzkum (Vejvodová, 2018).
[433] Potvrdil i výzkum probíhající v letech 2010-2015 (Holas, 2013 str. 83 a 85).
[434] Srov. např. rozhodnutí Najvyššího soudu Slovenské socialistické republiky ze dne 30.11.1970 sp. zn. Tpj 28/70-VIII.

jistě nebude dostačující (Pospíšil, 2002), a pochopitelně princip trestního práva coby ultima ratio (§ 12 odst. 2 TZ).

V trestněprávní rovině přichází v úvahu řada skutkových podstat trestných činů. Trestného činu hanobení národa, rasy, etnické nebo jiné skupiny osob se dopustí, kdo veřejně hanobí[435] některý národ, jeho jazyk, některou rasu nebo etnickou skupinu, nebo skupinu osob pro jejich skutečnou nebo domnělou rasu, příslušnost k etnické skupině, národnost, politické přesvědčení, vyznání nebo proto, že jsou skutečně nebo domněle bez vyznání, a tento čin spáchá veřejně přístupnou počítačovou sítí [§ 355 odst. 1 písm. a) nebo b), odst. 2 písm. b) TZ]. Kdo veřejně podněcuje k nenávisti k některému národu, rase, etnické skupině, náboženství, třídě nebo jiné skupině osob nebo k omezování práv a svobod jejich příslušníků, aniž by tak činil např. prostřednictvím projevů sympatií k hnutí směřujícího k potlačení práv a svobod člověka, a tento čin spáchá veřejně přístupnou počítačovou sítí, dopustí se trestného činu podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod [§ 356 odst. 1, 3 písm. a) TZ]. Trestný čin násilí proti skupině obyvatelů a proti jednotlivci má hned tři základní skutkové podstaty. První z nich se dopustí, kdo skupině obyvatelů vyhrožuje usmrcením, ublížením na zdraví nebo způsobením škody velkého rozsahu (§ 352 odst. 1 TZ). Vyhrožování násilím nemusí být bezprostřední, avšak musí být objektivně způsobilé vyvolat obavu z jeho naplnění a adresát musí mít možnost se o vyhrožování dovědět (Šámal, 2012 str. 3278). Druhá základní skutková podstata přidává znak nesnášenlivosti (zjednodušeně řečeno pro rasu, etnicitu, národnost, politické přesvědčení, vyznání) a alternativní znak k vyhrožování v podobě užití násilí (§ 352 odst. 2 TZ). Nakonec je zde třetí skutková podstata zahrnující spolčení se (vč. online) za výše uvedeným účelem (§ 352 odst. 3 TZ).

Kdo propaguje hnutí, které prokazatelně směřuje k potlačení práv a svobod člověka, nebo hlásá rasovou, etnickou, národnostní, náboženskou či třídní zášť nebo zášť vůči jiné skupině osob, a tento čin spáchá veřejně přístupnou počítačovou sítí, dopustí se trestného činu založení, podpory a propagace hnutí směřujícího k potlačení práv a svobod člověka [§ 403 odst. 1, 2 písm. a) TZ]. „Propagování“ lze definovat jako „jednání, kterým se pachatel ... snaží toto hnutí uvádět ve známost, šířit jeho ideologii mezi lidmi. Může být uskutečňována jak přímo (veřejné oslavování a vyzdvihování hnutí, hlásání jeho ideologie, tezí a cílů), tak i nepřímo (prostřednictvím publikace či jiného uveřejňování názorů, záměrů, ideologie takového hnutí ...“ (Šámal, 2012 str. 3501). Pod propagaci prostřednictvím veřejné počítačové

[435] „Hanobením se rozumí subjektivní, hrubě urážlivý projev směřující k hrubému znevážení“ rozhodnutí Nejvyššího soudu sp. zn. Tpjn 302/2005 ze dne 13.12.2006.

sítě lze podřadit např. tvorbu webu zaměřeného na hlásání neonacistické ideologie. Trestného činu projevu sympatií k hnutí směřujícímu k potlačení práv a svobod člověka (§ 404 TZ) se dopustí, kdo na rozdíl od trestného činu založení, podpory a propagace hnutí směřujícího k potlačení práv a svobod člověka takové hnutí přímo nepropaguje, nýbrž vyjadřuje pozitivní vztah či obdiv k tomuto hnutí, avšak bez úmyslu získávat tomuto hnutí další přívržence či jinak posilovat jeho pozici (Šámal, 2012 str. 3506), a to veřejně, tedy např. veřejnou počítačovou sítí (§ 117 TZ). Obdobně se dopustí trestného činu popírání, zpochybňování, schvalování a ospravedlňování genocidia, kdo veřejně popírá, zpochybňuje, schvaluje nebo se snaží ospravedlnit nacistické, komunistické nebo jiné genocidium nebo jiné zločiny nacistů a komunistů proti lidskosti (§ 405 TZ).

V ostatních případech, kdy nese jednání znaky trestného činu z nenávisti, soud k takové motivaci přihlédne jako k obecně přitěžující okolnosti: pachatel spáchal trestný čin z národnostní, rasové, etnické, náboženské, třídní či jiné podobné nenávisti nebo z jiné zvlášť zavrženíhodné pohnutky [§ 42 písm. b) TZ].

Zveřejnění násilného jednání online může být trestným činem týrání zvířat (nemluvě pochopitelně o samotném aktu týrání, § 302 TZ), dále pak opět násilím proti skupině obyvatelů a proti jednotlivci (viz výše, § 352 TZ), podněcováním k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod (§ 356 TZ), výtržnictvím (§ 358 TZ), podněcováním k trestnému činu (§ 364 TZ) nebo schvalováním trestného činu (je-li schvalován zločin, § 365 TZ). Při opakovaném zasílání násilných videí dítěti pak i ohrožováním výchovy dítěte [§ 201 odst. 1 písm. a) TZ].

Odhalování a postihování projevů nesnášenlivost představuje tvrdý oříšek. Na jednu stranu se společnost v online prostředí zjevně radikalizuje, na druhou stranu právo na svobodu projevu představuje jednak základní lidské právo, jednak jeden ze základních principů internetu vůbec. Objevují se snahy bojovat proti nesnášenlivosti ze strany velkých mediálních hráčů (zejm. Youtube a FB), ať už v podobě hate speech, hate crime, násilí nebo radikalismu. Úvahy směřují např. k automatizovanému rozeznávání uživatele a/nebo jeho věku prostřednictvím webkamery na základě dříve známé fotografie, což by umožnilo sofistikovanou filtraci obsahu. Přesto se nelze ubránit určitému mrazení v zádech z představy aplikace sledující identitu uživatele a rozhodující o tom, zda mu povolí přístup, nemluvě o dalekosáhlých důsledcích implementace přístupu ke službě online až po předchozí de facto biometrické identifikaci i dříve neznámého uživatele (zejm. pak s ohledem na snahu o

zvyšování ochrany osobních údajů online). Proti zneužívání propagandistických, násilných a nesnášenlivých videí ze strany zejm. radikálů chce pak Youtube bojovat formou úpravy přesměrovávání na další videa, které by místo na další radikální obsah oslavující násilí a nesnášenlivost přesměrovalo uživatele na obsah zcela opačný, tj. na utrpení obětí a podporování tolerance (2017). Lze vyjádřit pochybnosti nad smyslem takového opatření, které by zřejmě mohlo vést k „obrácení" některých jedinců a když nic dalšího, omezilo by snad virální šíření násilného obsahu, opět však zůstává otázkou míra, v jaké by takto Youtube rozhodoval o tom, komu povolí ten či onen obsah. Přesto nelze takovou úvahu rovnou odmítnout, neboť konec konců již dnes pracují velké vyhledávače s personalizovaným obsahem a zobrazují výsledky vyhledávání s ohledem na předchozí hledané výrazy, navštívené stránky atd.

12.1. Shrnutí k násilí a hate crime

Projevy nesnášenlivosti stojí na hraně mezi ochranou svobody projevu a ochranou osobnosti a menšin. Škála zahrnuje hate speech (vč. trollingu), násilný obsah (vč. happy slappingu) až hate crime. Zvlášť násilný obsah může být atraktivní zejm. pro dospívající chlapce, extremistické skupiny pak pro sociálně bezmocné jedince s komplexem méněcennosti. K šíření obsahu a komunikaci se využívají mnohé kanály: weby, blogy, profily na SNS, videoportály, sdílení emailem a P2P, obsah může být skrytý i zřejmý na první pohled. Princip sdružování online paradoxně umocňuje postupnou radikalizaci, neboť ještě podtrhuje obecnou tendenci k vyhledávání potvrzení vlastních názorů a upozadění odporujících argumentů (a osob), a to za přispění personalizace obsahu zpravodajskými aj. servery a vyhledávači v souladu s vlastním zaměřením uživatele (ten však může zůstat v iluzi objektivní nabídky zpráv). Proti nesnášenlivosti a šíření extremismu se snaží bojovat i poskytovatelé služeb (vč. Youtube a FB), byť jsou jejich opatření diskutabilní.

Odpovědnosti za narušování ochrany osobnosti a práv menšin se mnohdy původci vyhýbají umístěním obsahu na serverech v zahraničí, přesto není jejich trestněprávní postih podle zákona ČR vyloučen, a to zejm. pro trestný čin hanobení národa, rasy, etnické nebo jiné skupiny osob, podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod, násilí proti skupině obyvatelů a proti jednotlivci, založení, podpory a propagace hnutí směřujícího k potlačení práv a svobod člověka, projevu sympatií k hnutí směřujícímu k potlačení práv a svobod člověka, popírání, zpochybňování, schvalování a ospravedlňování

genocidia [§ 355, 356, 352 odst. 1 a/nebo 2 a/nebo odst. 3 písm. a), § 403, 404, 405 TZ]. Vynechat nelze ani obecně přitěžující okolnost spáchání činu z nenávisti [§ 42 písm. b) TZ]. V souvislosti se zveřejněním či šířením násilného obsahu přichází v úvahu skutková podstata trestného činu týrání zvířat, opět násilí proti skupině obyvatelů a proti jednotlivci, podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod výtržnictví, podněcování k trestnému činu nebo schvalování trestného činu a při šíření k dítěti i ohrožování výchovy dítěte [§ 302, 352, 356, 358, 364, 365 a 201 odst. 1 písm. a) TZ].

13. Prevence

Rychlý technologický pokrok provází odpovídající vývoj kriminality a přesun části tradiční kriminality (s modifikacemi) do online prostředí. Digitální propast rozděluje digitální imigranty znalé tradičních hrozeb, ale nikoliv nových médií, a digitální domorodce, znalé nových médií, ale nikoliv tradičních hrozeb. Rychlým změnám se jen pomalu a se zpožděním přizpůsobují odpovídající zákonné normy. O některých důsledcích panují jen nejasné dohady (např. vliv SNS a ICT vůbec na psychosomatický vývoj jako de facto velký nekontrolovaný sociální experiment). Mnozí si odmítají připustit faktické totální prolnutí reálného a virtuálního světa mladých generací, odmítají připustit či neznají rizika s kyberprostorem spojená a nové bezpečnostní návyky si osvojují jen postupně (vč. jejich přenosu na děti a na druhé straně seniory). Velkou roli proto hraje primární prevence srozumitelná cílové skupině (zejm. děti nebo senioři) a zaměřená na obecná pravidla kyberprostoru, resp. užívání internetu vůbec: používání antiviru, silných hesel atp. Probíhá např. formou krátkých videospotů dostupných online i vysílaných v TV,[436] a tedy přístupných i jinak převážně „offline lidem“ (typicky senioři). Ostatní preventivní úsilí už spoléhá na aktivitu ze strany samotných uživatelů, kterým nabízí návody, rady tipy, počínaje (ne)státními institucemi a organizacemi přes komerční společnosti a poskytovatele služeb až po samotné uživatele radící a pomáhající si navzájem.[437]

Možností prevence kyberkriminality je řada, počínaje prevencí zaměřenou na uživatelské návyky a konče právními důsledky protiprávního jednání. Na prevenci kriminality online a určité kultivaci kyberprostoru ve vztahu k dětem se podílí řada osob, nicméně převážnou část útoků může zhatit samotný obezřetný uživatel bez většího úsilí, případně alespoň minimalizovat škody (např. zálohováním dat), a to přijetím za své několika zásad. Jakékoliv zařízení používající internet musí být technicky chráněno, nezbytným minimem je firewall a pravidelně aktualizovaný antivir (nejlépe doplněný antispywarem). Aktualizovány by měly být i veškeré používané programy, aby nedošlo k napadení zařízení jejich prostřednictvím. K žádoucím opatřením patří i šifrování komunikace, používání pouze důvěryhodných cloudů, zabezpečených Wi-Fi sítí a neignorování varovných bezpečnostních hlášení. V online prostředí však snad více než jinde platí, že každé bezpečnostní opatření je jen tak silné, jak

[436] Např. spoty sdružení CZ.NIC vysílané od roku 2012 na ČT a dostupné online (CZ.NIC, 2012).
[437] Instituce a organizace jako sdružení CZ.NIC (provozující i národní CSIRT), NÚKIB, Ministerstvo vnitra ČR provozující portál prevencekriminality.cz, Národní centrum bezpečnějšího internetu, z.s., Centrum prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci aj., společnosti jako Microsoft, UPC, Seznam.cz aj., s širokou technickou podporou a tipy online, uživatelé typicky v konkrétně zaměřených diskusích (např. jak zabezpečit webovou kameru proti vzdálenému přístupu).

obezřetný je člověk, který ho provádí. Hlavní břemeno předcházení rizik tak spočívá na uživatelích samotných. Ti by měli zabezpečit svá zařízení vůbec fyzicky[438] v rámci ochrany před zcizením a pro ten případ a pro případ neoprávněného užití: např. uzamčením displeje telefonu po určitém čase bez aktivity, možností vzdáleného zablokování a smazání obsahu (ovšem se zvláštní pozorností věnovanou přístupovým údajům k takové aktivitě), pravidelným zálohováním dat vč. fotografií atp. (zejm. pro případ ransomwaru). Hesla by měla být silná (tj. kombinace alespoň 8 znaků, vč. čísel a písmen) a pro různá místa odlišná. Podobně jako klíče, i hesla k různým aplikacím mají rozdílnou zneužitelnost. Mezi ta zvlášť hlídaná by mělo patřit heslo k emailu a SNS a samozřejmě elektronickému bankovnictví a veškerým aplikacím využívajícím platební údaje. Spíše než o častou změnu hesel by měl uživatel dbát o jejich sílu a nedostupnost. Lze doporučit používání tzv. klíčenky – software nebo hardware (nikoliv však v podobě cloudové služby dostupné online). Doporučit lze též používání více emailových schránek určených pro odlišné aktivity (soukromé, školní atp.), vč. rozdílné míry zabezpečení s ohledem na jejich využití.

K veřejným ICT zařízením a službám mají přístup různé osoby a nelze dost dobře zjistit případný odposlech (keylogger, spyware, klonování obrazovky atp.) – nemělo by proto být používáno k soukromým účelům (elektronické bankovnictví, intimní konverzace a obsah atp.). Sběr osobních údajů provádí i řada aplikací, je proto vhodné vždy věnovat pozornost jejich požadovaných přístupovým oprávněním (např. přístup k sms v mobilním telefonu pro aplikaci s kuchařskými recepty). S ohledem na digitální otisk je žádoucí vždy zvážit zveřejnění jakéhokoliv osobního obsahu online (vlastního i cizího), neboť internet je v prvé řadě veřejný prostor[439] a s trochou nadsázky je jakýkoliv digitální obsah online věčný, kopírovatelný, globální a dohledatelný. Protože nikdy není možná 100% kontrola nad podobou digitálního otisku, každý by se měl čas od času pokusit vyhledat o sobě dostupné informace pro jejich kontrolu, vč. fotografií.

Zvláštní pozornost by měl každý přikládat varovným signálům. Při podivném chování osoby na SNS ověřit jeho identitu, nestahovat aplikace z nedůvěryhodných zdrojů, neotevírat podezřelé emaily, nereagovat na nepřiměřeně výhodné nabídky, nepřeposílat potvrzovací sms atp. V zájmu kultivace kyberprostředí nešířit hoaxy a řetězové emaily,[440] případně zkusit

[438] K fyzickému zabezpečení prvků (nejen) kritické infrastruktury viz (Kolouch, a další, 2019 str. 282 a 411).
[439] I zdánlivě skryté informace se mohou stát de facto veřejnými např. v důsledku nepovedené aktualizace zabezpečení SNS.
[440] Hoaxy obvykle v podobě šíření poplašné zprávy, viz např. Recyklované mléko (Hoax.cz), řetězové emaily pak v podobě „pošli tuhle zprávu 5 lidem...“ atp.

ověřit důvěryhodnost - autor, vyvolaný dojem, aktuálnost atp. (Zlatkovský, 2016). Digitální propast pomáhá zmenšovat mezigenerační dialog, zejm. mezi dětmi a seniory. Zatímco děti uživatelsky rozumí ICT a používají je hojně a rádi, senioři mohou poskytnout potřebný nadhled, odstup, širší souvislosti. Zvlášť důležitou úlohu hrají rodiče, v ideálním případě sami provází děti kyberprostorem.

Sekundární prevence již cílí na konkrétní ohrožené skupiny, především opět děti a seniory. Odlišuje i jednotlivé hrozby: např. sexting ve vztahu k mládeži a nigerijské dopisy ve vztahu k seniorům. V obecné rovině se prevence směřující k dětem zaměřuje na doporučení primární prevence (diskursem dětí), snahu vštípit bezpečnostní poučky,[441] rozšíření digitální gramotnosti a pozitivního využívání ICT (např. podpora kreativního vytváření pozitivního obsahu pro děti a dětmi), porozumění mediálnímu průmyslu a kritické uvažování nad obsahem vlastním i cizím (O'Neill, a další, 2018). Ve vztahu k dětem se prevence jednotlivých jevů zaměřuje především na sexuální vykořisťování a pornografii, kyberšikanu, hate speech, zákeřné návody a porušování autorských práv, přičemž posledně jmenované zahrnuje především uvážlivé používání cizích autorských děl a jejich náležitou citaci.[442]

Předcházení sexuálnímu vykořisťování dětí se věnuje zejm. osvětě, zvlášť co do kybergroomingu, ale i hrozícím dopadům sextingu, zejm. po relativně běžném zveřejnění intimního obsahu zasílaného vzájemně mezi partnery jedním z ex-partnerů po rozchodu (používá se např. tzv. babiččino pravidlo: „neměl/a bych odeslat nic, co by neměla vidět moje babička"). Prevence kyberšikany hovoří o traumatizujících dopadech na oběť, které si mnohdy (zejm. v počátcích jednání) agresoři ani neuvědomí či nepřipouští. Nabádá oběti a přihlížející, aby se nenechali zatáhnout do prohlubující se spirály útoků. Agresory varuje před postihem, který může přijít a obvykle v nějaké podobě přichází.[443] Vysvětluje učitelům a rodičům, jak rozpoznat varovné signály (typicky náhlá změna v užívání ICT, podobně jako při komunikaci s kybergroomerem). Proti násilí online a různým projevům nesnášenlivosti bojují různé informační kampaně zaměřené na veřejné odsouzení takových projevů, vyzdvihující

[441] Děti mnohdy pravidla znají, ale uniká jim smysl – např. „toho člověka přece ZNÁM, píšeme si už celý týden každý den, proč bych mu tedy o sobě něco neřekla..."

[442] Typicky při používání wikipedie jako zdroje pro školní referát a používání obrázků nebo hudby nalezených online při tvorbě vlastní prezentace. Naproti tomu odrazování od sdílení neoprávněně zpřístupněných autorských děl (zejm. filmy, hudba, počítačové hry) není tak patrné, neboť do jisté míry odpadl zájem o taková díla – např. zvuková díla jsou obvykle dostupná ve velké míře za drobný měsíční poplatek či přímo zdarma (viz např. Spotify), oblíbené MMO hry bývají ke stažení zcela zdarma a fungují formou samostatně placeného herního času.

[443] Ať už v podobě projednání ve třídě, kázeňského opatření, náhrady škody nebo i přestupkové či trestněprávní odpovědnosti. Klíčové sdělení představuje fakt, že po kyberšikanujícím jednání bude následovat sankce, samotná její podoba a závažnost již není z hlediska prevence tak podstatná.

toleranci k odlišnostem a odrazující od podílení se na šíření násilí a nesnášenlivosti. Některé školy/učitelé zařazují do výuky vedle etikety i tzv. netiketu, tj. soubor pravidel slušného chování online.

V online prostředí najdeme i terciární prevenci (nad rámec internetu jako pouhé platformy pro komunikaci), byť v omezené míře – např. pachatel kyberšikany zveřejnivší kajícnou omluvu na místě s původním dehonestujícím obsahem. Oběti při troše úsilí snadno naleznou doporučení pro technické zabezpečení (např. jak blokovat nežádoucí komunikaci), na koho se obrátit, jak nahlásit porušení pravidel (útok většinou porušuje vnitřní pravidla dané služby).

Ať už jsou preventivní opatření jakákoliv, jako červená nit se jimi vine apel na sebeochranu. V online prostředí probíhá řada útoků automatizovaně a v masovém množství (DDoS, phishing aj.). Spoléhání se pouze na následné prosazení práva a podávání trestního oznámení s každým takovým útokem by bylo absurdní pro všechny zúčastněné, byť většina z nich z formálního hlediska naplní přinejmenším skutkovou podstatu neoprávněného přístupu k počítačovému systému a nosiči informací (§ 230 TZ). Mnohem efektivnějším řešením je vlastní obrana představující ve většině případů pouze pravidelnou aktualizaci softwaru a obezřetné jednání. To samé platí pro předcházení zneužití osobních údajů aj. obsahu, vč. využívání ICT ke kyberšikaně – mnohem účinnější než spoléhání se na ochranu ze strany autorit (ať už v rámci dané aplikace, systému, školy, rodičů atp.) je vzít své bezpečí do vlastních rukou a dbát o ně.[444]

Nyní si dovolím malé zamyšlení.[445] V souvislosti s prevencí nežádoucích jevů online se obvykle upíná pozornost na oběť (zejm. ze strany neziskových organizací), až v druhé řadě pak stojí preventivní/terapeutická/výchovná/represivní práce s agresorem a případně i s přihlížejícími. Do jisté míry tím ale možná přispíváme k ukotvení vnímání agrese v kyberprostoru jako „normálního“ chování (ve smyslu propojení bourdieuovského potvrzování fenoménu hovořením o něm a mertonovského sebenaplňujícího se proroctví, viz kapitola **Identita**). Je-li veškerá pozornost upřena na oběť a na to, jak se má bránit, jako bychom potvrzovali agresivitu jako standardní formu interakce. Jakmile se pak potenciální oběť stane obětí reálnou, důvod se spatřuje v její nedostatečné ochraně a obraně, de facto s

[444] Mimoto napříč různými formami rizikových oblastí a újem online, se kterými se děti setkávají, ty děti, které se aktivně brání (resp. např. při kyberšikaně aktivně jednají ve smyslu blokace útočníka), vnímají následnou újmu méně citlivě a kratší dobu (Livingstone, a další, 2011), (d'Haenens, a další, 2013).
[445] Viz (Ochráníme děti před sexuálním zneužíváním kriminalizací jednání?, 2013).

upozaděním agrese útočníka.[446] Výsledkem je hned dvojí nežádoucí dopad: jednak zlehčujeme vinu agresora odkazem na lehkomyslnost oběti, jednak tím pádem snižujeme míru sociálního tlaku na agresora a zároveň klademe určitou část viny na oběť. Útok je pojímán jako výsledek nedostatečné ochrany a obrany oběti, nikoliv aktu agrese.

V současnosti jako bychom měli dva světy vedle sebe (a vzájemně se překrývající), kdy ten reálný disponuje kontinuitou vštěpování morálních aj. pravidel sociálního soužití, zatímco ve virtuálním podobné mantinely do jisté míry chybí. Důvod lze spatřovat mj. ve faktu, že zdatnými a častými uživateli internetu aj. moderních technologií spojených s kyberprostorem je především mládež. Přenos vzorců chování mezi reálným a virtuálním světem nepochybně probíhá - uživatelé s sebou do kyberprostoru vnáší obvykle alespoň část svých sociálních návyků, stejně tak jako návyky získané v kyberprostoru pronikají do reálného světa.[447] Otázkou zůstává, který svět v tom či onom případě získá navrch co do převažujícího vlivu na chování a jednání konkrétní osoby. V případě, že chování a jednání jedince začnou více ovlivňovat návyky spojené s virtuálním světem, o to více nabude na významu vnímání agresivity jako normy ve virtuálním světě. Čím více osob bude takto ovlivněno, tím závažnější bude dopad na sociální vztahy ve společnosti, potažmo případný nárůst agrese a radikalizace společnosti.[448]

Prevence by proto neměla zapomínat na odrazování útočníků. V tomto směru by mělo být možné využít přenosu vzorců jednání mezi reálným a virtuálním světem, protože tím nejzákladnějším a vlastně i nejjednodušším je morální apel („buďme na sebe hodní“) a odsouzení („agrese je vždy špatná“). V rámci reálného světa se zdají být takové myšlenky liché (samozřejmě neodstraníme kriminalitu apelem na morální hodnoty pachatelů), ovšem ve virtuálním světě nabývají na významu, protože na rozdíl od reálného světa zde/tam nemá kdo předávat dalším generacím jaké hodnoty kromě těch, které se nyní utváří. Kyberprostor hraje v životě každého jednotlivce v moderní společnosti významnou roli, reálné a virtuální prostředí se stále více prolínají. Proto čím více morálních a sociálních zvyklostí přeneseme do kyberprostoru, tím méně je snad budeme postrádat v reálném světě.

[446] Byť lze určité ospravedlnění nalézt v přijatelnějším pocitu usilování o předejití obdobného útoku v budoucnu poučením se z vlastních chyb oproti bezmoci nad předchozí viktimizací.
[447] Např. neschopnost hluboké koncentrace spojená s multitaskingem vlastním používání ICT nebo naopak vraždící střelec napodobující postavu počítačové hry.
[448] Radikalizace nastartovaná a umocněná sdružováním s okruhem osob smýšlejících obdobně, viz kapitola **Násilí** a hate crime.

Na poli prevence se lze setkat s mnoha aktéry. Klíčová je především role rodičů (obvykle zároveň zákonní zástupci dítěte). Ti vykonávají rodičovskou odpovědnost (§ 855 an., zejm. § 858 NOZ), jejímž obsahem je mj. péče o citový, rozumový a mravní vývoj dítěte, jeho ochrana a zajišťování výchovy a vzdělání. Nevykonávají-li ji řádně a vyžaduje-li to zájem dítěte, soud ji omezí (§ 870 NOZ) – např. při opakovaných neřešených výchovných problémech dítěte (např. sexting za úplatu). Rodič nebo jiná osoba odpovědná za výchovu dítěte má právo při výkonu svých práv a povinností požádat o pomoc OSPOD aj. relevantní státní orgány, popřípadě pověřené osoby; tyto orgány v rozsahu své působnosti a pověřené osoby v rozsahu svého pověření jsou tuto pomoc povinny poskytnout (§ 9 ZSPOD).

Rodiče dítěte plní základní výchovnou roli v jeho životě, předávají mu první vzorce chování, hodnotovou orientaci, dodávají sebevědomí a zprostředkovávají vlastní zkušenosti, poskytují existenční prostředky a naplňují citové potřeby. Stejně jako v přípravě na vlastní život dítěte v reálném prostředí, měli by ho připravit i na kyberprostor. Zřejmě nejlepším rodičovským přístupem je v tomto směru provázení novými médii prakticky od prvních krůčků dítěte, počínaje prvními zkušenostmi s ICT (typicky mobilní telefon nebo tablet) přes bezpečné, učící aplikace rozvíjející digitální schopnosti a gramotnost až po vlastní zodpovědné užívání nových médií dítětem samotným (Livingstone, a další, 2011). Na rodiče to klade značné nároky: vlastní uživatelskou schopnost, orientaci v aplikacích, zkušenosti s jejich používáním a především povědomí o přidružených rizicích.

Ovšem i rodič neznalý a s ICT si nerozumějící může dítěti poskytnout potřebnou zpětnou vazbu v reakci na obsah, s nímž se setkalo online (např. násilí, pornografie, šikana) a především uspokojovat jeho základní citové potřeby a dát mu dostatečnou pozornost. Bude-li se dítě cítit v bezpečí, úspěšné a milováno, není pravděpodobné, že by sklouzlo k netholismu nebo snadno podlehlo kybergroomerovi. Zároveň i případné kyberšikanující útoky ponese snáze, pokud k nim vůbec dojde. Důležitou oporu a pomoc při řešení již nastalých nežádoucích situací představuje také možnost si o nich promluvit. Nakonec jsou to rodinné zvyklosti a aktivity, které v raném věku dítěte dodávají základní návyky, vč. způsobu trávení volného času a toho, zda si dítě aktivně hledá zábavu nebo se raději pasivně nechá zabavit, potažmo kolik času tráví offline a kolik online.

S věkem dítěte nabývá na významu škola, která hraje roli zejm. v oblasti (kyber)šikany (prevence i následné řešení). MŠMT sice vydává své metodické pokyny, nicméně záleží především na konkrétních učitelích a dětech, jak případná opatření fungují. Školní prostředí

představuje svět per se, kde se děti učí vzájemnému jednání a chování, zažívají pocit (ne)úspěchu a (ne)uznání ze strany ostatních, kde jsou již samy za sebe bez přítomnosti dohlížejících rodičů. Vhodná práce s novými médii může proto velmi ovlivnit jejich užívání a přístup ze strany dětí, např. předcházení zneužívání ICT ukázáním jejich lepšího využití zapojením do výuky nebo tvorbou pozitivního obsahu.[449] Na druhé straně stojí přístup eliminující používání ICT ve školním prostředí (např. omezení používání SNS a mobilních telefonů), který sice může v krátkodobém horizontu pomoci zklidnit probíhající kyberšikanu, v dlouhodobém hledisku se tím ale škola zbavuje možnosti výchovného působení a podtrhává pocit kyberprostoru bez pravidel a autorit, obdobu „divokého západu" (spolu s tím, jak rodiče postupně omezují a ztrácí nad dětmi kontrolu). Ve školním prostředí pak děti také absolvují různé preventivní přednášky, vč. těch věnovaných kyberšikaně a online nástrahám.

Škola má ohlašovací povinnost vůči OSPOD. Je povinna oznámit bez zbytečného odkladu obecnímu úřadu obce s rozšířenou působností mj. skutečnosti (§ 10 odst. 4 ZSPOD), které mohou nepříznivě ovlivnit vývoj dítěte a nasvědčují tomu, že: rodiče dítěte (či osoby, jimž je dítě svěřeno) neplní povinnosti plynoucí z rodičovské zodpovědnosti nebo nevykonávají nebo zneužívají práva z ní plynoucí [§ 6 písm. a) bod 2. nebo 3. ZSPOD] – např. se odmítají dostavit do školy v souvislosti s šetřením kyberšikany při podezření na jejich útočícího potomka; některé z dětí vede zahálčivý nebo nemravný život [§ 6 písm. c) ZSPOD] – např. provozuje sexting za úplatu; na některém z dětí byl spáchán trestný čin ohrožující jeho mravní vývoj [§ 6 písm. e) ZSPOD] – např. navazování nedovolených kontaktů kybergroomera s dítětem. OSPOD[450] sám pak tyto děti vyhledává a pracuje s nimi a s jejich rodiči (§ 10 ZSPOD), kterým také poskytuje na jejich žádost pomoc (§ 9 ZSPOD). Požádat o ni mohou i samy děti (§ 8 odst. 1 ZSPOD).

Obecní úřad obce s rozšířenou působností mj. pomáhá rodičům při řešení výchovných nebo jiných problémů souvisejících s péčí o dítě, poskytuje nebo zprostředkovává jim poradenství při výchově a vzdělávání dítěte (§ 11 dost. 1 ZSPOD). Povinnost využít odbornou poradenskou pomoc jim může i uložit, pokud např. nejsou schopni řešit problémy spojené s výchovou dítěte bez odborné poradenské pomoci (§ 12 odst. 1 ZSPOD). Vyžaduje-li to zájem na řádné výchově dítěte, může obecní úřad obce s rozšířenou působností (případně soud) dítě nebo jeho rodiče vhodným způsobem napomenout, stanovit a provádět nad dítětem dohled (za

[449] Např. využití výukové počítačové hry (Evropa 2045, Československo 38-89 aj.), výuka za pomoci rozšířené reality s použitím tabletu, společně vytvářený web atp.
[450] Tj. krajské, obecní a újezdní úřady a obecní úřady obcí s rozšířenou působností, Ministerstvo práce a sociálních věcí ČR, Úřad pro mezinárodněprávní ochranu dětí a Úřad práce ČR (§ 4 ZSPOD).

součinnosti školy, popřípadě dalších institucí a osob), uložit dítěti i rodičům omezení bránící působení škodlivých vlivů na výchovu dítěte, uložit dítěti i rodičům povinnost využít odbornou poradenskou pomoc, účastnit se prvního setkání s mediátorem nebo terapie (§ 13 odst. 1 ZSPOD). Obecní úřad obce s rozšířenou působností dále případně podává návrh soudu na omezení/zbavení rodičovské odpovědnosti anebo omezení/pozastavení jejího výkonu, na nařízení/prodloužení/zrušení ústavní výchovy, na svěření (prodloužení a zrušení umístění) dítěte do péče zařízení pro děti vyžadující okamžitou pomoc (§ 14 dost. 2 ZSPOD). Činí tak poté, co projednal s rodiči důvody, pro něž má dojít/došlo k podání návrhu soudu, poučil je srozumitelně a prokazatelně o jejich právech a povinnostech vyplývajících z rodičovské odpovědnosti a důsledcích jejich neplnění, v rámci případové konference projednal důvody podání návrhu a zabýval se možnými způsoby jejich řešení (není-li zřejmé, že by její uspořádání bylo nemožné/zjevně neúčelné), uskutečnil opatření sociálně-právní ochrany (zejm. poskytl či zprostředkoval poradenství a pomoc při výchově rodičům, popřípadě uložil povinnost využít odborné pomoci) a zvážil uložení výchovných opatření (§ 14 odst. 2 ZSPOD).

Konstrukce sociálně-právní ochrany dětí představuje potenciálně poměrně dobře nastavený systém zachycení ohrožených dětí a možné práce s nimi, i zde však záleží především na konkrétních osobách, které ji vykonávají. Zvlášť důležitý je kromě samotného faktu zabývání se daným případem/podezřením v souladu s platnými normami[451] především citlivý přístup ke všem zúčastněným a nejvíce ze všech k ohroženému dítěti, tj. vstřícný a chápající, ale také důsledný a odpovídající potřebám konkrétního dítěte.

Problematice kriminality a jiným sociálně škodlivým jevům spojených s využíváním nových médií dětmi se věnuje i řada neziskových aj. organizací. Vytváří osvětové materiály (dostupné online a případně i v tištěné podobě) a pořádají školení a kurzy: primární prevence ve školách zaměřená na děti, školení pro vybrané skupiny (učitelé, sociální pracovníci, rodiče aj.) i širokou veřejnost. Zajišťují také lokální i celonárodní osvětové kampaně a pořádají různé akce, zejm. u příležitosti tzv. Safer internet day (vždy 1. únorové úterý), kdy zúčastnění (neziskové organizace, školy, dětské kolektivy atp.) pořádají soutěže, divadelní představení, koncerty, debaty, vytváří obrázky, prezentace atp., vše s tématikou vztahující se k ICT a vybranému tématu (v roce 2018 „publikování na internetu s respektem k sobě samým a ostatním online uživatelům," v roce 2019 „společně za lepší internet").

[451] Vč. volby takových opatření sociálně-právní ochrany, která na sebe navazují a vzájemně se ovlivňují, a to při dodržení standardů sociálně-právní ochrany dětí (§ 9a odst. 2 a 4 ZSPOD).

V ČR (Ministerstvo vnitra ČR) působí např. Národní centrum bezpečnějšího internetu (NCBI), mezi jehož hlavní aktivity patří i poradenské centrum Online Helpline a kontaktní centrum Stop Online. Centrum prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci (PRVoK) provozuje poradnu E-bezpečí a provádí a spolupodílí se na výzkumech.[452] Sdružení Linka bezpečí poskytuje krizovou intervenci a poradenství (telefon, chat, email). Projekt Bezpečný internet.cz poskytuje informace pro různé cílové skupiny vč. dětí, za zmínku stojí i někteří jeho partneři (případně i s vlastními preventivními aktivitami): CZ.NIC, Seznam.cz, Hoax.cz, Microsoft, s.r.o., Policie ČR aj. Za zmínku stojí např. také aktivity Akademie CZ.NIC, Horké linky (zejm. spolupráce s FB) nebo Dětského krizového centra. Svou „horkou linku" provozovala ještě v roce 2018 i Policie ČR, v současnosti její provoz nahradila „linka" STOPonline provozovaná sdružením CZ.NIC (Policie ČR, 2018), (SToPonline). Na celounijní úrovni je realizován především projekt Better internet for kids, pokračování projektu Safer internet. Zahrnuje mj. i výzkumnou síť odborníků ze všech zúčastněných zemí, kteří společně i jednotlivě postupně publikují svá zjištění a z nich vyplývající doporučení, vč. doporučení pro vytváření lepšího prostředí a podmínek jak pro děti, tak pro rodiče a učitele, resp. školy. Jejich dobře prováděné výzkumy poskytují validní a reliabilní data podávající poměrně přesný obrázek zkoumaných jevů (kyberšikana, sexting, netholismus aj.).

Obvyklou (samozřejmou) součástí činnosti výše uvedených organizací a projektů je provozování informačního webu, často členěného na přístup a informace pro různé cílové skupiny (děti, rodiče, senioři, učitelé aj.). Zájemci zde naleznou informace o relevantních negativních jevech online: jak je poznat, jak jim čelit v průběhu a jak je následně řešit, mohou se setkat také s příklady dobré praxe a s příběhy obětí.[453] Síť horkých linek Inhope zaměřená na minimalizaci sexuálního zneužívání aj. škodlivého obsahu online působí ve 40 zemích (Inhope) a zajišťuje mj. předávání oznámení policejním orgánům členského státu, který se zdá být nejrelevantnějším místem pro postih daného obsahu.

Nakonec si lze jen těžko odmyslet roli médií, tradičních i nových. Spoluformují vzorce chování a atmosféru ve společnosti, vybírají zprávy k rozšíření, propagují, baví atd. Vliv médií je dobře známý, ukázal se např. při informování o hře Modrá velryba ve spojení

[452] Např. Kyberšikana učitelů, České děti a FB, Nebezpečí internetové komunikace.
[453] Ukazují např. obětem kyberšikany, že jejich situace není ojedinělá a má řešení, byť to tak v danou chvíli nevypadá.

s varující tiskovou zprávou vydanou Policií ČR,[454] po nichž dle výpovědí řady učitelů následovala vlna zděšení a vážných obav ze strany dětí zároveň spolu s vyhledáváním informací a pokusy o ní. Zvláštní roli jako „informační" kanál plní Youtube, zvláště pak ve spojení s oblíbenými youtubery. Nelze sice každého youtubera považovat za pozitivní sociální vzor, vyplnili však prázdné místo v kyberprostoru, který získal své „hrdiny". Mimoto youtubeři, kteří se nebojí „odkouzlit", ukazují světu i své „normální já" a hovoří o svých běžných radostech, starostech i pocitech, což představuje určitý protipól většiny sebeprezentací na SNS.[455] Prevenci kriminality online páchané dětmi formou vytváření pozitivního obsahu youtubery (někdy i výslovně zaměřeného na odsouzení kyberšikany, hate speech aj.) lze označit za formu tzv. peer-to-peer prevence, tedy mezi vrstevníky navzájem. Děti možná postrádají nadhled a širší souvislosti, které chápou dospělí, ale nejlépe rozumí vlastním pocitům, trápení, obavám a nejistotám, i touhám a úspěchům - hovoří „stejnou řečí" a nebojí se mluvit. Mimoto funguje (zpravidla ve školním prostředí) i řada dětských iniciativ, které samy vytváří a šíří preventivní obsah: od informačních letáčků po přednášky realizované ve vlastní škole i jinde, vč. zapojení se do Safer Internet Day, konferencí atp.

13.1. Shrnutí k prevenci

Primární prevence škodlivých jednání v kyberprostoru se zaměřuje na jeho obecná pravidla, využívá online i offline prostředky a spoléhá i na vlastní aktivitu uživatelů. Zejm. oni mohou předcházet úspěšným útokům v kyberprostoru, mnohdy za přijetí alespoň zásadních zásad sebeochrany: fyzické zabezpečení zařízení (vč. vzdáleného přístupu), aktualizovaný ochranný software a veškeré aplikace, šifrování citlivé komunikace a dat, používání pouze důvěryhodných zdrojů (cloud, e-shop, Wi-Fi aj.), neignorování bezpečnostních varování, zálohování dat, silná a různá hesla (zejm. k emailu, SNS a aplikacím pracujícím s platebními údaji), nevyužívání veřejného zařízení k soukromým účelům, obezřetné udělování oprávnění aplikacím, péče o vlastní digitální otisk (sebeprezentace a kontrola), zvýšená ostražitost (vůči podezřelému jednání i obsahu), ověřování pravosti a pravdivosti. Sekundární prevence ve vztahu k dětem cílí především na sexuální zneužívání ve všech jeho podobách, kyberšikanu a hate speech, v obecnější rovině usiluje o zvýšení digitální gramotnosti a kritického myšlení a

[454] Původní zpráva (Policie ČR, 2017) byla sice posléze označena médii za hoax, přesto po ní následovalo několik desítek poznatků (Policie ČR, 2017).
[455] Byť si ne každý sledující uvědomuje, že pravděpodobně žádný z vlogů (videologů) nevznikl napoprvé a ve výsledném časovém rámci a že zdánlivě neuspořádané okolí, úvahy atp. mohly projít před natočením dlouhou přípravou a před samotným zveřejněním přísným sebekritickým filtrem.

pozitivní využívání ICT vůbec. Terciární prevence nabízí zejm. technická doporučení k odstranění obsahu, hlášení porušení pravidel atp. Prevence by ovšem neměla zapomínat ani na odrazování útočníků, aby důraz na sebeochranu potenciálních obětí mimoděk nepotvrzoval škodlivé jednání v kyberprostoru coby normu.

V prevenci hraje roli řada aktérů, zejm. v raném věku dětí pak především rodiče, a to jednak provázením dítěte online prostředím, volbou aplikací, základním varováním a předáváním vzorců chování v kyberprostoru, jednak naplňováním citových aj. potřeb dítěte vůbec. Později nabývá na významu role školy, která může kromě osvětové činnosti výrazně ovlivnit digitální gramotnost dětí, pozitivní přístup k ICT i netiketu. Především v prostředí školy probíhá peer-to-peer prevence, jinou její častou podobu reprezentují youtubeři. Při ohrožení konkrétního dítěte (v roli oběti i pachatele) se škola (povinně), rodiče i dítě mohou obrátit o pomoc mj. na OSPOD, který na jedné straně poskytuje pomoc, na straně druhé může i ukládat určité povinnosti k nápravě. Kromě uvedených aktérů se v prevenci v oblasti kyberprostoru angažuje i řada institucí a organizací, zejm. v podobě osvěty: tvorba online i offline informačních zdrojů, přednášek, projektů atp.). Za zmínku stojí např. Safer Internet Day, Ministerstvo vnitra ČR (portál PrevenceKriminality.cz), NCBI (Online Helpline a Stop Online), PRVoK (E-bezpečí), Linka bezpečí, portál BezpečnýInternet.cz, CZ.NIC, EU (Better Internet for Kids), Inhope (horké linky) aj.

14. Aktuální trendy[456]

Pozornost věnovaná kybernetické kriminalitě vůbec (bez specifikace vztahu k dětem) se zaměřuje obvykle na různé podoby malwaru a sociálního inženýrství. Mnohé instituce a organizace vydávají informace o předchozím roce a varování a doporučení v obecné rovině pro daný rok na základě vlastních zkušeností a očekávání.[457] Je ovšem třeba brát je s určitou rezervou z několika důvodů: vysoká latence kyberkriminality, nesjednocená právní kvalifikace mnohých jednání,[458] odraz vlastních zájmů a oblasti podnikání (např. vývoj a prodej ochranného nástroje pro konkrétní typ útoku). Setkat se tak lze s ad hoc zprávami např. ze strany NÚKIB (Národní úřad pro kybernetickou a informační bezpečnost), CZ.NIC (CZ.NIC) a na webech komerčních společností[459] aj.

Dále věnují pozornost kyberkriminalitě coby nedílné součásti kriminality vůbec i další instituce. Najdeme ji tak i v pravidelně publikovaných zprávách Ministerstva vnitra ČR o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území ČR (Ministerstvo vnitra ČR). Zpráva o roce 2016 hovořila mj. o nenávistných projevech na SNS a jinde, hoaxech, phishingu, podvodných internetových obchodech a praním peněz ve spojení s BTC, kyberšpionážních kampaních cílící na data vč. přístupových aj. osobních údajů, ransomwaru (Ministerstvo vnitra ČR, 2017 str. 67). Za rok 2017 zpráva zmiňuje opět podvodná jednání (vč. spojení s BTC a legalizaci výnosů z trestné činnosti), phishing (zejm. vůči bankovním účtům a informačním systémům veřejné správy) a ransomware (zejm. ve spojení s IoT), dále DDoS, průniky na emailové servery státní správy a do kritické infrastruktury, mravnostní trestné činy online (zejm. dětská pornografie, navazování nedovolených kontaktů s dítětem, účast na pornografickém představení), hate crime, hoax (zejm. na SNS), „krádež“ identity, zejm. na SNS a ve spojení následným podvodným jednáním (Ministerstvo vnitra ČR, 2018).[460] Zpráva o činnosti státního zastupitelství za rok 2016 hovoří o zneužívání naivity a neodpovědného chování poškozených při nakupování online, phishingu (ve spojení s odčerpáním peněz), podvodných jednáních, útocích na informační systémy (vč. emailů a SNS), mravnostních a autorskoprávních deliktech a násilných a nenávistných projevech. Varuje také před trendem přesunu podstatné části jiných druhů kriminality na internet (prodej

[456] Část kapitoly byla publikována jako spoluautorský text (Kudrlová, a další, 2017).
[457] Souhrnné zprávy bývají publikovány v 1. čtvrtletí, za rok 2018 proto nejsou dosud dostupné.
[458] Např. neoprávněné využití emailové schránky poškozeného je někdy kvalifikováno jako samotný neoprávněný přístup k počítačovému systému a nosiči informací (§ 230 TZ), jindy v souběhu s porušením tajemství listin a jiných dokumentů uchovávaných v soukromí (§ 183 TZ) nebo s porušením tajemství dopravovaných zpráv (§ 182 TZ).
[459] Viz např. internetový magazín Dvojklik společnosti ESET (ESET, 2017).
[460] Zpráva za rok 2018 není dosud k dispozici.

drog, padělání atp.).[461] V roce 2017 informuje např. o průnicích do emailových schránek (podvodná komunikace a sběr osobních údajů jejich prostřednictvím), phishingu (vůči bankovním účtům, vč. jejich využití k legalizaci výnosů z trestné činnosti), podvodech (inzerát, e-shop), kyberstalkingu (kyberšikaně), prolamování přístupových údajů (účty bankovní, herní, SNS, email), využívání BTC (nákup neoprávněně získaných osobních údajů, platby ransomware, podvodné nabídky BTC), manipulaci s tachografem (kamionová doprava), hate speech, mravnostní kriminalitě páchané na dětech (Nejvyšší státní zastupitelství, 2018).

Vyjdeme-li dále z předpovědí některých z významnějších hráčů na poli kybernetické bezpečnosti, jejich očekávání se sice v dílčích aspektech liší, nicméně lze vyčíst určité shodné rysy. Předpovědi čerpají zpravidla z vlastních skrytých databází,[462] samotná data tak nebývají dostupná. V roce 2016[463] dominovaly očekávání 4 oblasti: APT, IoT, útoky na chytré mobilní telefony a „tržní" kyberkriminalita. U APT útoků roste očekávaná sofistikovanost a s tím i náročnost odhalení, zejm. ve spojení s tzv. spear phishingem, tj. phishingem „na míru" konkrétním adresátům (Marinos, 2016 str. 63), často zaměstnancům v budoucnu napadené organizace. U útoků na IoT jde prozatím spíše o nastupující trend, nicméně roste spektrum napadnutelných zařízení co do druhu i množství, vč. tzv. Point-of-Sale (platební místa: e-shop, bankomat, pokladna v kamenném obchodě atd.). Chytré telefony integrují další a další funkce, a představují tak širokospektrou platformu pro útok i úložiště množství osobních údajů (odposlech, podvodné aplikace, zpoplatněné sms atp.). Tržní charakter kyberkriminality začíná být patrný zejm. v dark webu: např. recenze uživatelů (resp. recenze hodnotící konkrétní uživatele i zboží a služby, a to na straně nabídky i poptávky). V jinak anonymním prostředí hraje ostatními uživateli ověřená důvěryhodnost daných osob,[464] potažmo transakcí důležitou roli při rozhodování, zda dané nabídky/poptávky využít (Bartlett, 2015).

Část předpovědí pro nárůst kyberkriminality v roce 2017[465] se naplnila v podobě masově rozšířeného ransomwaru WannaCry a jeho modifikací (EC3, 2017), (Wikipedia, 2017):

[461] Viz textová část zprávy (zejm. str. 6, 8 a 17) dostupné na webu Nejvyššího státního zastupitelství (Nejvyšší státní zastupitelství, 2016).
[462] Vychází z vlastních šetření i hlášení uživatelů, ať už lze dané jevy považovat za bezpečnostní události či přímo bezpečnostní incidenty dle ZoKB (§ 7 odst. 1 a 2).
[463] Viz (McAfee, 2015), (Hewlett Packard Enterprise Development LP, 2015), (IBM, 2015), (Lemos, 2016), (McAfee, 2015), (risk3sixty LLC, 2015), (RSA, 2015), (Drew, 2015), (ESET, 2014), (ESET, 2015).
[464] Paradoxně se dá říci, že anonymita prostředí vzhledem k nemožnosti ověření v reálném prostředí tlačí uživatele k osobení si relativně stabilní online identity.
[465] Viz (Malek, 2017), (Patterson, 2016), (ESET, 2017), (European Union Agency for Network and Information Security (ENISA), 2017), (Symantec, 2017), (TrendLabs, 2016), (Kovacs, 2017), (Hewlett Packard Enterprise Development LP, 2015).

předpokládal se nárůst ransomwaru co do počtu útoků i napadených zařízení. Zvláště ohroženy nejen ransomwarem měly být nadále zejm. chytré mobilní telefony. Ozývaly se hlasy volající po lepším zabezpečení IoT (nejen ve spojení s ransomwarem), zejm. wearables a zařízení chytré domácnosti, ale i zdravotních pomůcek, čipů (implantovaných i vestavěných), webkamer a dronů. Panovaly obavy z napadení kritické infrastruktury a očekávány byly DDoS, vč. využití tzv. business zombie (zjednodušeně řečeno podřízené zaměstnanecké počítače namísto soukromých). Řada zdrojů varovala před spywarem a sběrem osobních údajů jako předstupněm převzetí účtu či identity poškozeného nebo jejich vytvoření (e-shop, SNS aj.). Nakonec nutno zmínit ještě specifickou herní oblast: narůstá obliba MMO her a her dostupných online a provozovatelé herních platforem se sice snaží své systémy (herní i organizační) zabezpečit proti možnému zneužití, přesto představují lákavý cíl s ohledem na množství zpracovávaných osobních údajů, objevují se i převzetí herních účtů.

Předpovědi pro rok 2018[466] lze shrnout do několika skupin. Na prvních místech bývá uváděn ransomware a malware, zejm. zaměřené na mobilní telefony. Hovoří se o zranitelném bankovním systému (bankomaty, bankovní účty a phishing, „krádeže" identity a sociální inženýrství vůbec, praní peněz, bankovní systém jako takový, nové platební metody). Roste intenzita varování v souvislosti s IoT coby rozšiřujícím se spektrem napadnutelných zařízení, přičemž k formám zneužití se nově přidává jejich zneužití jako součásti botnetu (zejm. útoky na herní platformy a těžba BTC), zvláštní pozornost se věnuje chytrým autům (odemykací aplikace, ovládací software aj.) a zdravotnickým IoT (zdroj osobních údajů i ovládnutelný předmět). Několik zdrojů zmiňuje též propagandu, především na SNS (vč. zneužívání sítě falešných profilů k ovlivňování mínění, reklamě atp.), a útoky na veřejnou správu (vč. přístupu občanů k informačním systémům státní správy a jejich osobní údaje). Očekávána byla protiprávní jednání ve spojení s kryptoměnami, zejm. BTC: legalizace výnosů z trestné činnosti, těžící botnet (vč. zapojení IoT a webového rozhraní – tzv. cryptojacking), podvodné obchodování. Panovalo přesvědčení o pokračujícím a rozšiřujícím se zneužívání osobních údajů z různých zdrojů: IoT, SNS, cloudových aj. aplikací, mobilních telefonů. Předpokládaly se průniky do firemních systémů s cílem získání dat, ať už provedené špionáží, BYOD[467] nebo jako součást APT. Zřejmé bylo pokračování útoků cílících na děti, zejm. na jejich osobní údaje na SNS a sexuální vykořisťování. Mělo se dále ztížit odhalování pachatelů

[466] Viz (McAfee Labs, 2017), (ESET, 2018), (Hewlett Packard, 2018), (EC3), (IBM), (ENISA, 2018), (Symantec), (Kaspersky Lab), (RSA, 2018), (Trend Micro, 2017)
[467] Bring Your Own device – používání soukromých zařízení v rámci pracovněprávních vztahů.

využívajících tzv. blockchain hosting,[468] šifrování a dark web. Pachatelé, mnohdy organizovaní v dobře finančně zabezpečených uskupeních, měli stále více využívat tzv. machine learning (schopnost počítače učit se), sociální inženýrství (spolu s přesunem podvodného jednání na SNS a Fraud-as-a-Service: nabídkou podvodu jako služby), spam botnety k šíření malwaru, útoky na routery a modemy, útoky prostřednictvím webů. Předpokládány byly i útoky na kritickou infrastrukturu. Objevilo se přesvědčení, že útočníci se zřejmě předpokládaným trendům a zveřejněným zprávám bezpečnostních expertů přizpůsobí dle svého.

14.1. Shrnutí k aktuálním trendům

Mezi aktuálními trendy škodlivých jednání v kyberprostoru, před nimiž varují aktéři věnující se jeho zabezpečení a postihu, bývá zmiňováno jen málokteré jednání ve vztahu k dětem vyjma sexuálního vykořisťování a protiprávního sběru osobních údajů. Více informací v tomto směru proto poskytují zejm. ad hoc varování ze strany neziskových organizací (např. před Modrou velrybou, konkrétním hoaxem, nebezpečným návodem atp.). Ad hoc i souhrnné zprávy (bez zaměření na mládež) vydávají i jiní, v českém prostředí např. NÚKIB, CZ.NIC, Ministerstvo vnitra ČR, Nejvyšší státní zastupitelství atd. Ty opakovaně zmiňují např. zneužívání SNS, praní peněz ve spojení s BTC, ransomware, phishing, DDoS, průniky do PS, hoaxy, nenávistné projevy, podvody, sexuální vykořisťování dětí. V roce 2016 byly mezi hlavními trendy APT (vč. spear phishingu), útoky na IoT a chytré mobilní telefony a rozvoj tržního charakteru kyberkriminality. Rok 2017 měl přinést zejm. ransomware, další útoky na mobilní telefony a IoT, dále na kritickou infrastrukturu (vč. DDoS), sběr osobních údajů a přebírání účtů (e-shop, SNS, herní platforma aj.). Pro loňský rok pak panovaly obavy z dalšího nárůstu ransomwaru aj. malwaru, zejm. vůči mobilním telefonům. Dále pak ze zabezpečení bankovního systému a IoT (vč. využití jako součást botnetu), propagandy, útoků na veřejnou správu, zneužívání BTC, sběru osobních údajů (vč. firemních dat), útoků na mládež (zejm. sběr osobních údajů a sexuální vykořisťování). Horší se také odhalitelnost pachatelů, kteří zřejmě stále více využívají dark web, šifrování, organizovanost, tržní mechanismy, machine learning, sofistikované sociální inženýrství atp. a zřejmě se také přizpůsobují vydaným varováním.

[468] Velmi zjednodušeně řečeno decentralizovaná alternativa DNS, stále spíše v experimentální podobě.

15. Shrnutí

Současné období se někdy nazývá „doba digitální“, neboť digitální technologie se dotýkají až na výjimky ve větší či menší míře prakticky celého světa a v moderní společnosti mají až totální, všeprostupující charakter. Od prvních pokusů o vzájemné propojení několika počítačů v 60. letech 20. st. se rozvinuly až do podoby IoT a kyberprostoru coby de facto paralelní reality. K nejvýraznějším aspektům kyberprostoru patří komunikace se svými specifiky, nová média, časoprostorové rozpojení, platforma pro sdružování, sdílení obsahu atd., ale také kriminalita tradiční i nová. Kyberprostor sice představuje širší oblast než internet jako takový, nicméně právě internet s ním bývá nejčastěji spojován coby hlavní propojující prvek a nové médium. V ČR vytrvale roste počet jeho uživatelů, přičemž se pohybuje v současnosti přes 80 % osob starších 16 let, co do domácností s dětmi a s přístupem k internetu pak již překročil 95 %. Bude se zřejmě zvyšovat i nadále spolu s tím, jak dorůstají generace, pro něž tvoří kyberprostor stejně přirozený svět jako ten reálný, a zároveň odchází starší generace, kterým je naopak zcela cizí.

Práce usiluje o uchopení kriminality spojené s využíváním nových médií dětmi z několika úhlů pohledu, které se snad mohou zdát na první pohled zbytečně obsáhlé, leč až ve svém souhrnu podávají plastický obraz reality, neboť to, co je pro digitálního domorodce zcela samozřejmé, může být pro digitálního imigranta naprosto nepochopitelné a naopak. Pokusila jsem se přemostit tuto digitální propast zohledněním obou přístupů. Cestou k tomu mi bylo především studium dokumentů a odborné literatury, analýza statistických dat, zpracování poznatků získaných v rámci výzkumu IKSP, účast na řadě relevantních konferencí i vlastní zkušenosti nabyté od účastníků školení v oblasti kyberkriminality ve vztahu k dětem, kterých jsem vedla coby lektorka pro vybrané cílové skupiny (zejm. učitelé a sociální pracovníci) několik desítek. Obecná část práce zahrnuje technické aspekty fungování internetu, sociologický pohled na kyberprostor vůbec (vč. nových médií), specifika komunikace a utváření identity digitálních domorodců online, digitální otisk ve spojení se sebeprezentací zejm. na SNS, netholismus a zvláštní postavení avatara. V rámci právního rámce kyberprostoru přechází obsah ve zvláštní část mj. v podobě analýzy počítačových trestných činů. Následuje nastínění fungování BTC coby častého platidla ve spojení s kyberkriminalitou vůbec, bez ohledu na její členění. Dílčí poznatky z výzkumu IKSP (zejm. analýza souzených počítačových trestných činů) se vztahují i k mládeži, přičemž následující kapitola ještě dále doplňuje některá jejich online specifika. Další kapitoly se již více méně monotematicky zaměřují na sexuální vykořisťování dětí, kyberšikanu aj. projevy násilí a nesnášenlivosti.

Práci zakončuje nezbytná prevence a stručný nástin trendů kyberkriminality vůbec, samozřejmě s následným shrnutím a závěrem.

Nyní tedy již k obsahu samému. Zjednodušeně řečeno, jakoukoliv digitálně zapsanou informaci (vč. textu, obrázku atp.) lze převést do binárního kódu v podobě jedniček a nul. Souhrn 8 jedniček a nul tvoří 1 byte, [bajt], tyto dále kilobyte, megabyte atd. Při posílání obsahu internetem se tento rozdělí na tzv. packety, tj. "balíčky" o velikosti nejvýše 1,5 kB, které obsahují jednak část dat posílaného souboru, jednak provozní informace. Packety poté síťové zařízení odešle na příslušnou IP adresu prostřednictvím putování mezi sérií uzlových bodů (např. router), z nichž každý zašle každý jednotlivý packet v daný okamžik nejrychlejší cestou směřující k cíli - každý packet proto může fakticky probíhat jinudy. IP adresy, tj. číselné označení daného zařízení převádí tzv. DNS překladače do podoby např. „seznam.cz". Hierarchická struktura umožňuje packetům rychlou cestu, neboť pokud uzlový bod nezná konkrétní adresu, zašle jej k uzlovému bodu na vyšším stupni a tak dále, až nalezne DNS server, který ji zná a který ho nasměruje na nižší úroveň až k samotnému cíli. Servery hostí kromě DNS překladačů především www službu, tj. webové stránky a aplikace (případně s omezeným přístupem). Bez zprostředkování serverem lze uskutečnit P2P spojení. S DNS překladači spolupracuje i indexace obsahu vyhledávači, které poskytují na základě zadaného dotazu z jejich pohledu nejvíce relevantní, za použití cookies zpravidla alespoň částečně personalizované odkazy. Málo využívané adresy a ty, které indexování zakazují, zůstávají skryty, podobně jako obsah přístupný pouze po autorizaci – tzv. deep web (oproti surface webu). Část z nich je navíc přístupná pouze při použití speciálního anonymizovaného prohlížeče Tor, tzv. dark web. Od technické stránky internetu se odvíjí řada protiprávních jednání nebo takových, které mají protiprávní jednání umožnit či zakrýt: útoky na DNS překladače, maskování IP a MAC adresy, ovládnutí routeru, DDoS a další. Mládež coby pachatelé využívají technickou stránku internetu spíše jen pomálu nad rámec běžného uživatele, přesto i mezi mladistvými se čas od času vyskytne např. hacker využívající exploit. Častější je ovšem postavení oběti, a to především následkem setkání se s nevhodným obsahem (pornografie, násilí aj.), kterému ovšem mohou v mnoha případech zabránit právě technická opatření, vč. tzv. rodičovské ochrany. Za obsah nesouladný s právem může za určitých okolností kromě původce odpovídat i poskytovatel služby. O dětech, podobně jako o ostatních uživatelích, pak řada aplikací sbírá údaje (vč. cookies), nakládání s nimi upravuje GDPR a de lege ferenda také zákon o zpracování osobních údajů. Nikoliv výjimečný je odposlech či jiné napadení zařízení používaného mládeží.

Kyberprostor představuje nikoliv paralelní realitu, nýbrž již imanentní součást všudypřítomné reality. Děti jsou nezkušené, důvěřivé a otevřené a rodiče jim sice mohou zprostředkovat vlastní nadhled, nemohou se s nimi však rovnat co do přirozenosti jednání a vystupování v online prostředí. Tzv. digitální propast rozděluje digitální domorodce (děti) a digitální imigranty (starší generace). Digitální domorodci rozumí jazyku, kultuře, hodnotám, stylu a rychle se přizpůsobují změnám, kyberprostor je pro ně přirozený svět. Naproti tomu digitální imigranti se vždy teprve učí sžít s jinak cizí kulturou a těžko opouští vlastní kořeny. Chování dětí online proto může působit pro starší generace naprosto nepochopitelně (např. nerozlišování virtuálních a reálných vztahů). Sdílení v kyberprostoru nabývá nebývalých rozměrů, neboť od tradičních médií s konkrétními adresáty a později i blíže neurčitými recipienty se jakýkoliv obsah šíří prostřednictvím nových médií (zejm. internet a SNS) mnohonásobně rychleji a masověji (mj. i s ohledem na časoprostorové rozpojení). Zahrnuje to i obsah nepravdivý, zavádějící, zraňující či nebezpečný. Děti a mladiství se v tomto směru ocitají v pozici pachatelů i obětí, zejména při kyberšikaně a sextingu, přičemž pozice oběti může být ve spojení s konkrétním obsahem i opakovaná, neboť nad digitalizovaným obsahem nelze nikdy spolehlivě získat opětovnou kontrolu.

Ke kyberprostoru nerozlučně patří komunikace, neboť (i díky časoprostorovému rozpojení) lze komunikovat prakticky s kýmkoli, odkudkoli, o čemkoli a kdykoli. Přesto pouze ochuzenou formou s absentující neverbální řečí těla, mimikou a bezprostřední okolní situací. Při procesu (de)kódování tak mnohé nevyřčené zůstane opravdu skryto a mnohé napsané nepochopeno, emočně i věcně. Odtud plynou někdy i zbytečné konflikty vycházející z nedorozumění, snadná eskalace jinak bezvýznamné neshody po vzájemných neadekvátních reakcích, ale vzhledem k nezpozorování varovných signálů také snazší podlehnutí podvodnému jednání, např. v podobě lákání peněz či důvěrného a intimního obsahu, předstírání virtuální lásky atd., zvlášť s ohledem na větší otevřenost a důvěrnost komunikace online oproti tváří v tvář. K nedorozuměním přispívá i specifický jazyk kyberprostoru a zjednodušující komunikace využívající v hojné míře zkratky a emotikony. Absence fyzické bariéry sice komunikaci v jistém smyslu usnadňuje, případné útoky i nedorozumění však zraňují o to niterněji. Protože člověk je bytost sociální, společnost, její uznání dotyčného a zároveň jeho uznání společnosti tvoří nedílnou součást identity, která se formuje od raného dětství prostřednictvím rodiny, posléze i vrstevníků a širokého okolí. Uznání společnosti ze strany jednotlivce se odvíjí od vnímání její (ne)spravedlivosti, přičemž klíčovou roli hraje zakoušení pocitů (ne)uznání ostatními. Společnost ovšem není bezbřehým množstvím osob,

nýbrž strukturou složenou z mnoha (často se překrývajících) referenčních skupin a párových kategorií, které sice rozdrobeností přispívají k anomii, zároveň ale snižují její tlak možným předefinováním hodnot. Některé párové kategorie mohou působit nespravedlivě, nikoli však nutně z dlouhodobého hlediska, vzhledem ke vzájemné převoditelnosti různých forem kapitálu (symbolický, ekonomický, sociální, kulturní) v reálném prostředí i v kyberprostoru. Kromě sociálního uznání vycházejícího z jedinečnosti ale potřebuje člověk naplnit i potřebu sebeuskutečnění, které je umožněno jeho právním uznáním coby člena společnosti a zajištěním individuální autonomie. Předpokladem k tomu je vnitřní a vnější svoboda sebevyjádření, jednak jeho realizace. Na řadu proto přichází komunikativní paradigma a požadavek, aby jedinec i skupina mohli hovořit za sebe samé a zároveň mohli být slyšeni (přestože vyjadřovací prostor není bezbřehý, nýbrž podléhá vnitřní a vnější cenzuře). Moderní státy proto obvykle usilují i o určitou digitalizaci státní správy. Internet nabízí pro vyjádření řadu možností i mimo participaci na věcech veřejných: SNS, chaty, blogy, videoportály, weby atd. Svůj hlas tak výrazně více než dřív získávají i děti a dospívající, vč. hojného zastoupení mladými youtubery. Ti a další pak více či méně kultivují online prostředí, mj. i postupným rozvíjením a respektováním netikety. Mládež online hojně komunikuje především vzájemně, součástí však bývá i napadání druhého (záměrně i z nedorozumění), typicky při kyberšikaně aj. formách virtuálního násilí. A to ve zvlášť zranitelném období vytváření vlastní identity odvíjející se z velké části od zpětné vazby ze strany vrstevníků a referenčních skupin.

V kyberprostoru má každý svůj otisk, vědomý i nevědomý. Jednak v podobě technických provozních, lokalizačních aj,. údajů, jednak v podobě informací vztahujících se k uživateli. Mezi původce takových informací patří v prvé řadě sami uživatelé svou sebeprezentací (zejm. na SNS), digitální otisk ovšem dovytváří i další osoby, instituce a organizace. Ve veřejném sektoru se tak děje zpravidla na základě zákona, případně v kombinaci s autorizací subjektu údajů. V soukromém sektoru pak obrázek doplňují např. zájmové organizace, zaměstnavatelé a především jiní uživatelé (opět zejm. na SNS). Děti samy začínají vytvářet svůj otisk na SNS (zejm. FB, Youtube, WhatsApp, Instagram, Lidé.cz aj.) poměrně záhy (cca v 8 letech), mezi dospívajícími tak činí cca 90 % osob, a to s dosahem vlastní sebeprezentace na „přátele“ (a jejich zpětnou vazbu) v řádech stovek až tisíců. Kromě textů sdílí i fotografie a videa zahrnující je samé i další uživatele. Zneužitelná data představují zejm. identifikační údaje (fyzické ohrožení) a údaje vztahující se k osobě a projevům dotyčného ve virtuálním prostředí. Mládež coby pachatelé je využívá zejm. při kyberšikaně a virtuálním násilí

z pomsty (typicky např. zveřejnění sextingu), na straně obětí pak strádá kromě těchto obdobně při kybergroomingu a vydírání.

U řady dětí a dospívajících dochází k excesivnímu užívání aplikací spojených s internetem (nejčastěji počítačové hry nebo SNS), které může přerůst i v závislost a sebepoškozování, přidají-li se další okolnosti (např. absence úspěchu v reálném životě, problémy s vrstevníky aj.), ovšem i samotné excesivní užívání může mít negativní dopady na poměr času, aktivit a sociálních kontaktů online oproti offline, případně preferenci virtuálního prostředí a vztahů oproti těm reálným. S nadsázkou lze označit za určité dobrovolné sebepoškozování už samotné setrvávání na SNS, neboť ty sice napomáhají sociabilitě a komunikaci, sdílení všeho vč. pocitů (radostných i negativních) a široká zpětná vazba však mohou působit i enormně negativně, pokud se převažující mínění obrátí výrazně v neprospěch uživatele. U některých uživatelů se může dostavit i tzv. syndrom FoMO provázený postupným přesunem veškerých aktivit na SNS a odpovídajícím odloučením od reálného okolí vč. rodiny. Mimoto hojné využívání SNS zřejmě snižuje vlastní pocit pohody a štěstí, neboť nahlíženo prizmatem úrovně obrázku života podávaného SNS, vlastní život se zdá šedivý a nudný. Jiné, již zřejmější formy sebepoškozování nachází v online prostředí vyjádření v podobě podpůrných webů (zvlášť v případě poruch příjmů potravy), odrazujících i vybízejících k sebepoškozování, a to vč. nejzávažnějších sebevražd. Závislostní potenciál počítačových her pak spočívá především v prožívání úspěchu a uznání ze strany ostatních hráčů, zejm. nedostává-li se jich hráči v reálném prostředí. Virtuální hra/prostředí tak může snížit případnou frustraci a zprostředkovat i zcela reálný prožitek (kromě dalších možných psychických i fyziologických pozitiv), o to více však uživatele k sobě připoutává, zejm. tehdy, identifikuje-li se se svým avatarem, tj. vlastní reprezentací ve virtuálním prostředí.

Avatarů může být více nebo jen jeden, krátkodobý i dlouhodobý (přetrvávající roky). U těch pak tzv. telepresence spojuje v mysli prožitek z daného prostředí s konkrétním avatarem, který to „zažil“. Kromě samotné sebeprezentace slouží avatar zejm. ke komunikaci s ostatními lidmi/avatary a jeho prostřednictvím se uživatel např. stává členem určité skupiny. Mohou mít proto relativně vysokou hodnotu (než jak se obvykle očekává od pouhé herní postavy), ať už subjektivní odvíjející se od vlastního sepjetí uživatele s avatarem, nebo ekonomickou vyplývající z měsíce až roky vylepšované postavy investicemi herního času i finančními. Avatar existuje v podobě datového souboru (není však počítačovým programem), a jako takový ho lze považovat dle NOZ za nehmotnou movitou věc, v závislosti na konkrétním avatarovi zastupitelnou i nezastupitelnou a zuživatelnou i nezuživatelnou. Ve

většině případů, nikoliv však vždy půjde o (oddělitelnou) součást věci hlavní – herního účtu. Výjimečně bude možné ho považovat za autorské umělecké výtvarné dílo (neodvozené od původního počítačového programu), vyloučit nelze ani jeho pojetí coby součást osobnosti uživatele (nad rámec emanace osobnosti tvůrce do jeho autorského díla) jako projev osobní povahy per se – klíčová je v takovém případě otázka, zda „mám" svého avatara, nebo „jsem" svým avatarem. Avatar je věcí i z hlediska trestního práva, mohou se ho proto dotýkat skutkové podstaty operující s věcí, autorským dílem i osobností. V úvahu přichází také znak pohrůžky jinou těžkou újmou nebo způsobení či pohrůžka jinou vážnou újmou (avatar jako součást osobnosti, prostředník vztahů a v neposlední řadě i „pracovní nástroj" profesionálního hráče), zejm. při zohlednění vztahu digitálního domorodce k vlastnímu avatarovi a na něj navázanému sociálnímu okolí. Avatara lze samozřejmě také využít jako prostředek k páchání trestné činnosti (např. vydírání jiného hráče prostřednictvím vzájemně komunikujících avatarů) a běžně bývá zneužíván v rámci kyberšikany. Nakonec může „dětský" avatar hrát roli i ve virtuální dětské pornografii.

Oblast kyberprostoru je regulována právem mezinárodním i národním. Základní rámec dává v ČR Ústava a Listina (zejm. ochrana osobnosti, právo na soukromí, ochrana listovního tajemství a jiných písemností, právo na svobodu slova a zásada nullum crimen sine lege). ZoKB a jeho prováděcí předpisy zajišťují ochranu kritické infrastruktury státu, potažmo infrastruktury internetu v ČR. Řada dalších předpisů pak upravuje různé dílčí otázky (např. zák. o některých službách informační společnosti), z těch obecnějších s přesahem na kyberprostor lze zmínit např. NOZ (zejm. ochrana osobnosti), zákon o některých přestupcích a evropské GDPR. Trestněprávní regulaci kyberprostoru, resp. kyberkriminality zajišťuje především TZ za přispění několika významných mezinárodních dokumentů: zejm. CoC a Dodatkového protokolu, Úmluvy o ochraně dětí před sexuálním zneužíváním a sexuálním vykořisťováním, směrnice o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii a směrnice o útocích na informační systémy.

TZ obsahuje v prvé řadě tzv. počítačové trestné činy, zejm. neoprávněný přístup k počítačovému systému a nosiči informací, který ve svých dvou základních skutkových podstatách kriminalizuje jednak samotný neoprávněný přístup, jednak neoprávněnou manipulaci s daty. Dále přichází v úvahu pro postih kriminality skutkové podstaty trestných činů souvisejících s elektronickou komunikací (porušení tajemství dopravovaných zpráv, porušení tajemství listin a jiných dokumentů uchovávaných v soukromí a poškození a ohrožení provozu obecně prospěšného zařízení v úmyslné i nedbalostní formě). Kyberprostor

může být též zvlášť přitěžující okolností při spáchání činu veřejně nebo veřejně přístupnou počítačovou sítí (nebo jiným obdobně účinným způsobem – např. zveřejnění v lokální uzavřené firemní síti). Z hlediska „zveřejnění“ nutno vždy posoudit především okruh osob, které mohou mít k obsahu přístup, a míru aktivity, kterou musí adresát vyvinout k zobrazení obsahu. Nakonec zbývají ještě hojně využívané „tradiční“ skutkové podstaty trestných činů, které však výrazně dopadají i na kyberprostor, typicky podvod nebo poškození cizích práv aj. Trestněprávní úpravu sexuálního vykořisťování dětí online výrazně ovlivňují (podobně jako počítačové trestné činy) i mezinárodní závazky ČR, ať už jde o nakládání s dětskou pornografií, zneužití dítěte k její výrobě nebo nové skutkové podstaty účasti na pornografickém představení a navazování nedovolených kontaktů s dítětem. Ve všech uvedených případech může být trestně odpovědná i právnická osoba.

Na pomezí legality se pohybují virtuální měny, zejm. nejrozšířenější BTC. S těmi lze obchodovat na finančních trzích, zájemci je však mohou také tzv. těžit, přičemž úspěšnost těžby se odvíjí především od výpočetní síly zařízení (objevují se proto těžařské botnety). „Těžba“ BTC spočívá ve výpočtu složitého matematického problému se začleněním prvku náhody, přičemž při vyřešení těžař vytvoří tzv. blok, který v sobě nese informaci o všech předchozích blocích a o všech BTC transakcích, k nimž došlo od vzniku předchozího bloku. Informace o blocích má podobu tzv. hashe, který lze velmi jednoduše ověřit, avšak velmi složitě vypočítat, a proto jej, potažmo BTC nelze kopírovat, zpětně upravit ani padělat. Adresy, na něž se BTC ukládají, se generují zcela náhodně a nelze je bez dalšího přiřadit ke konkrétním osobám (odtud vysoká anonymita). Ke každé patří veřejný a soukromý klíč (hash), přičemž veřejný slouží k přijetí BTC, soukromý k odeslání. Proto se při zničení hmotného nosiče s uloženou adresou nebo soukromým klíčem dané BTC navždy ztratí. Podaří-li se některou z adres ztotožnit, lze od ní sledovat všechny příchozí a odchozí transakce, byť v podobě veřejných adres. Z toho důvodu se využívají k další anonymizaci hromadné ePeněženky, které vzhledem k množství transakcí značně ztěžují sledování konkrétních plateb. BTC se proto hojně využívají pro platby související s trestnou činností (např. při ransomwaru).

Samotnou kyberkriminalitu lze členit různými způsoby. Nejčastěji to bývá dle CoC, která ale nezahrnuje celou její šíři, což činí sice lépe, leč příliš obecně dělení na kriminalitu usnadněnou ICT a kriminalitu závislou na ICT. Nabízí se proto vlastní rozlišení, a to v obecné rovině na kyberkriminalitu zaměřenou vůči PS jakožto cíli nebo prostředku, dle míry využití sociálního inženýrství oproti technickému prvku a (ne)využívání síťového charakteru.

Konkrétněji se jedná o zásah do systému (často pouhý prostředek k dalšímu jednání), majetkovou kriminalitu, „krádeže“ identity, virtuální násilí, černý trh, sexuální zneužívání, porušování autorských a příbuzných práv, cyber war. Při zaměření na mládež v roli potenciálního pachatele i oběti zahrnuje zásah do systému např. hacking a neoprávněný přístup do systému, různorodý malware cílící zejm. na mobilní telefony, odposlech (např. uložené fotografie), ransomware nebo úpravu dat (např. na SNS). Majetková kriminalita se týká především herní oblasti. Ke „krádežím“ identity dochází zejm. v souvislosti s virtuálním násilím, které zahrnuje mj. jednání z pomsty, kyberšikanu, verbální projevy nesnášenlivosti a násilný obsah. Na černém trhu se obchoduje mj. s dětskou pornografií, další formy sexuálního zneužívání dětí pak zahrnují zejm. kybergrooming a dětskou prostituci (vč. sextingu). K protiprávnímu nakládání s autorskými a příbuznými právy online dochází především v podobě porušování citační licence a podmínek volného užití, cyber war se cíleně mládeže obvykle nedotýká.

Probíhající výzkum IKSP v oblasti kyberkriminality se zaměřuje mj. na trestní řízení o počítačových trestných činech, v nichž byla podána obžaloba a která byla pravomocně skončena v roce 2015. Vychází z justičních a policejních statistik a analýzy 65 ze 71 trestních spisů, zahrnuje 68 obviněných (tzn. sice počet na hraně statistické významnosti, nicméně „vzorek“ představuje 92 % relevantních věcí, a tak přinejmenším orientačně naznačuje trend). Nezahrnuje ovšem ta řízení, v nichž sice mohlo dojít i ke spáchání počítačového trestného činu v souběhu, skutek tak ovšem nebyl kvalifikován (typicky např. podvod ve spojení s neoprávněným přístupem k počítačovému systému a nosiči informací kvalifikovaný pouze jako podvod bez souběhu). Nápad počítačových trestných činů od doby účinnosti TZ vesměs stoupá, pozvolna stoupá též počet obžalovaných a odsouzených skutků. Obvykle meritorně rozhoduje okresní soud, a to o přečinu neoprávněného přístupu k počítačovému systému a nosiči informací (§ 14 odst. 2, § 230 TZ), případně o dalších trestných činech spáchaných v souběhu – nejčastěji majetkových (zejm. podvody) či ve formě virtuálního násilí (např. vydírání), dále také v souběhu se zneužitím pravomoci úřední osoby. Při rozhodování výlučně o počítačových trestných činech (27 trestních řízení) soudy ukládaly nejčastěji podmíněně odložený trest odnětí svobody v průměrné délce 6 měsíců, případně trest obecně prospěšných prací. Pouhých 9 % obviněných mělo jednat ve spolupachatelství, většina byla prvopachateli, tj. bez předchozího pravomocného odsouzení za trestný čin (62 %). Obvinění muži byli v okamžiku zahájení trestního řízení obvykle ve věku do 29 let, ženy (22 %) starší: 35-49 let. Poškozených fyzických osob, právnických osob i obou skupin zároveň bylo vždy pouhých

několik (1-5), anebo naopak velké množství (desítky až stovky). Výše způsobených škod se pohybovala v rozmezí 1.200 Kč – 26 mil. Kč. Pachatelé hojně zneužívali přihlašovací údaje získané díky neopatrnosti či důvěře poškozených, vlastního jinak oprávněného přístupu a fyzického přístupu k určitému zařízení, jen výjimečně byla využita znalost ICT nad rámec běžného užívání. Napadán byl nejčastěji FB a emailové schránky, a to za účelem kontroly pošty, dehonestace a majetkového obohacení (osobnost vč. osobních údajů cílena v téměř 60 %, majetek cca ve 30 %). Řada posuzovaných jednání hraničila až s banalitou, bylo by proto vhodné trestní represi rozvolnit např. dalším fakultativním znakem základní skutkové podstaty § 230 TZ, což ovšem neumožňují mezinárodní závazky ČR. Některé z opakujících se jevů názorně demonstruje případová studie. Určité odlišnosti od dospělých pachatelů vykazují mladí obvinění (do věku 25 let k okamžiku zahájení trestního řízení, tj. 20 mužů a 2 ženy). Ti jednali zhruba v polovině případů v souběhu s alespoň 1 dalším trestným činem a téměř polovina byla již recidivisty. Výlučně za počítačové trestné činy jim soudy ukládali tresty obdobné jako ostatním odsouzeným. Útoky převážně prostřednictvím FB a emailové schránky směřovaly častěji na fyzické osoby, vyrovnaně na majetkovou sféru i osobnost poškozených (zejm. virtuální násilí ze strany expartnera).

Mládež je nezkušená, naivní, důvěřivá, a tudíž snadno manipulovatelná a zranitelná. Potrpí si na uznání širokého sociálního okolí, s jehož přispěním buduje svou identitu. Činí tak i zkoušením hranic vlastních i dovolených, aniž by domýšlela důsledky svého jednání výrazněji nad rámec „tady a teď“. Nedostatek vlastních a nepřenositelnost zkušeností starších osob, omezenost neverbální komunikace, nadměrné trávení času online a hojné využívání SNS s prakticky neomezeným množstvím přihlížejících a komentujících uživatelů představují hlavní kriminogenní i viktimogenní faktory. Komunikace s „přítelem“ na SNS snadno evokuje dojem skutečného přátelství (zejm. se zohledněním nerozlišování virtuálních a reálných vztahů digitálními domorodci), a tudíž i otevřenost, široké publikum pak přináší riziko enormní kritiky – obojí zvlášť ve vztahu k osobám ohroženým i v reálném prostředí (např. citová deprivace). Děti jako oběti mají své místo mj. v TZ (některé skutkové podstaty a obecně i zvlášť přitěžující okolnost) a zákoně o obětech trestných činů (zvlášť zranitelná oběť). Dětským a mladistvým pachatelům s přirozenou averzí vůči normám a autoritám v období dospívání nahrává online oproti reálnému prostředí vědomí určité anonymity a vysoká latence kyberkriminality. Přidává se také nereálná představa fyzických možností, každodennosti a konfliktních vztahů coby normy umocněná SNS a médii. Pokles evidované kriminality (nejen) mládeže a její předpokládaný přesun do online prostředí tak lze vysvětlit

mj. tím, že se zde/tam zároveň snáze zabaví (namísto protiprávních aktivit), anebo se pouze stává latentní, neboť nepodléhá takové kontrole. Mládeži coby pachatelům provinění nebo činu jinak trestného se věnuje zejm. ZSVM (vč. podmíněné příčetnosti), dětem mladším 15 let pak ještě zák. o zvláštních řízeních soudních a pachatelům ve věku blízkém věku mladistvých TZ. I nezletilé osoby mohou odpovídat za přestupek (zák. o odpovědnosti za přestupky a řízení o nich) a způsobenou škodu, případně spolu s osobou zanedbavší povinný dohled nad nezletilým (NOZ). Na samotných počítačových trestných činech se mladiství pachatelé podílejí oproti dospělým více než na kriminalitě vůbec, naopak mezi oběťmi figuruje mládež méně často.

Děti přirozeně objevují vlastní sexualitu a experimentují s ní, k čemuž využívají i pornografii. Soft pornografie (psychologické kritérium) přispívá ke zdravému sexuálnímu vývoji, nevhodná pornografie (vč. hard a deviantní) nikoliv. V online prostředí lze snadno narazit zejm. na prostou pornografii (právní kritérium), ať už v podobě výsledků vyhledávání nebo specializovaných webů, zpravidla „znepřístupněných“ dětem formou disclaimeru s požadavkem zadání věku. Do 16 let věku se v horizontu uplynulého roku setká s pornografií online zhruba třetina dětí. Pornografie je definována např. jako dílo, jehož jediným účelem je vyvolat/zvyšovat sexuální vzrušení, dětská pornografie zobrazuje nebo jinak využívá dítě (tj. osobu mladší 18 let) nebo osobu, jež se jeví být dítětem. Zahrnuje tedy i virtuální pornografii, a to i bez zneužití konkrétního dítěte s ohledem na zájem na ochraně mravních hodnot společnosti považující dětskou pornografii za škodlivou vůbec. Vzhledem k rychlosti a masovosti šíření obsahu online bylo proto (pod vlivem legislativy EU) kriminalizováno již samotné získání přístupu k dětské pornografii prostřednictvím ICT. Mezi relativně oblíbené kratochvíle mládeže patří kromě/v rámci konzumace pornografie i sexting (posílání a sdílení sexuálně laděného obsahu), který někdy slouží i jako forma přivýdělku (častěji u dívek). Cca pětina českých dětí ve věku 11-16 let obdržela sexting v horizontu předcházejícího roku, z toho polovina jich sexting odeslala. Mládež tak činí v rámci vlastního sexuálního zrání a sebeprezentace, chtějí upoutat pozornost a flirtují. Zhruba ve třetině případů tak činí na žádost (osoby známé i neznámé). Je-li předmětem sextingu prostá pornografie zasílaná dítěti, pachatel se může dopustit trestného činu šíření pornografie (s rozlišením, zda pornografii dítěti přenechává nebo nabízí). U mladistvých aktérů sextingové dětské pornografie přichází v úvahu spáchání trestného činu výroby a jiného nakládání s dětskou pornografií (šíření dětské pornografie). V souvislosti se sextingem může být dítě zneužito k výrobě pornografie a

může být ohrožována jeho výchova, může probíhat i formou pornografického představení (účast diváka na pornografickém představení).

Jiná forma sexuálního zneužívání, kybergrooming (manipulace prostřednictvím ICT s cílem přimět oběť k osobnímu setkání za účelem sexuálního zneužití), představuje zvlášť závažný průběh nevyžádaného kontaktování, přičemž zhruba polovina českých dětí ve věku 11-17 let komunikuje s osobou známou pouze virtuálně a třetina je dokonce svolná k setkání s ní. Kybergroomer vyhledává oběti online (zejm. SNS), vystupuje mnohdy s upravenou identitou. Získává si je vytrvalým budováním důvěry a izolací od okolí (i měsíce až po psychickou závislost oběti), drobnými úplatky, průběžně vybízí k sextingu. Získaný intimní obsah (fotografie, prozrazená tajemství atd.) následně využívá při naléhání na další sexting a později i osobní schůzku. Při setkání tváří v tvář je oběť zpravidla sexuálně využita. Názorný příklad podává jedna z mediálně známých kauz kybergroomingu v ČR. V širším významu kybergrooming označuje obecně nevyžádané kontaktování, kdy dotyčný mj. vybízí k sextingu (a praktikuje jej), případně i za úplatu. Oběť kybergroomera utrpí psychická zranění v podobě zrazení hluboké důvěry, manipulace a narušení sociálních vztahů. Při osobním setkání dochází k fyzickému ohrožení, i bez něj však mohou sdílená pornografie a sexting deformovat v citlivém období dospívání mravní hodnoty a vlastní sexualitu. I při kybergroomingu v širším smyslu se může oběť v budoucnu potýkat s negativními důsledky svého jednání vzhledem k množství digitalizovaného intimního obsahu, nad nímž odesláním kybergroomerovi ztrácí kontrolu. Pachatel bývá cílevědomý, chladnokrevný a inteligentní, běžný uživatel ICT zdatný v používání SNS, schopný předstírat empatii a znalý běžných zálib i problémů své cílové skupiny. Vybírá si nejčastěji zranitelné oběti ve věku 9-17 let (problémy v rodině, s vrstevníky atp.). Kybergroomer potenciálně ohrožuje výchovu dítěte, může poškodit cizí práva (podvodnou manipulací) a mnohdy šíří pornografii. Často dítě zneužije k výrobě pornografie a svádí ho k pohlavnímu styku (např. požadování striptýzu za úplatu). Výslednou dětskou pornografii pak přinejmenším přechovává, ať už dítě přiměl k její výrobě a zaslání či tak učinilo dobrovolně, případně bez vědomí zaznamenávání (výroba a jiné nakládání s dětskou pornografií). Při odmítání pokračování v sextingu nebo osobního setkání neváhá přistoupit k vydírání pod pohrůžkou jiné těžké újmy (hrozba ukončení vztahu, zveřejnění dosud získaného obsahu atp.), případně útisku (při již dostatečné emoční závislosti oběti na něm). Fyzické setkání pak zpravidla provází sexuální zneužití oběti (v úvahu přichází většina trestných činů proti lidské důstojnosti v sexuální oblasti). Zvlášť přiléhavou je od roku 2014 skutková podstata navazování nedovolených kontaktů s dítětem chránící děti

mladší 15 let před sexuálním vykořisťováním, ke kterému je návrh setkání prostředkem (de facto příprava sexuálního trestného činu), přičemž použití ICT za tím účelem typově zvyšuje společenskou škodlivost takového jednání. Navzdory určité problematičnosti a krátké době účinnosti se už před rokem 2018 vyskytlo již 25 pravomocně odsouzených pachatelů (muži zejm. ve věku kolem 29 let), jejichž oběťmi byly převážně dívky ve věku 10-14 let, kontaktované nejčastěji prostřednictvím FB.

Zcela odlišnou oblast představuje kyberšikana: záměrné a dlouhodobé, resp. intenzivní zákeřné jednání prostřednictvím ICT s jednoznačně rozdělenými rolemi oběti a agresora. Probíhá ve virtuálním prostředí bez časového a prostorového omezení, s potenciálně nezměrným publikem, potažmo traumatizací oběti, která roste s počtem přihlížejících, zatímco agresoři mohou zůstat skryti. S kyberšikanou má zkušenost zhruba čtvrtina až polovina českých dětí ve věku 9-17 let, přičemž 5-10 % jich přiznalo vlastní zraňující aktivní jednání. Oběti (především děti, v cca 20 % i učitelé) zakouší verbální útoky, průniky na účty (zejm. SNS a emailové schránky), obtěžující prozvánění, vyhrožování a zastrašování, ponižování, ztrapňování (zejm. šířením fotografií a videí), „krádeže“ identity, vydírání. Nejvíce probíhají útoky na SNS (zejm. verbální útoky a zesměšňující fotografie), často prostřednictvím mobilního telefonu (typicky vyfocení oběti a prakticky okamžitý upload na FB nebo Youtube s patřičným komentářem). Bývá zahlcována emailová schránka oběti (např. pornografií) a oběť online ostrakizována (např. v počítačové hře). Kyberšikana se zpravidla prolne s tradiční šikanou a jednání se účastní především vrstevníci ze školní třídy. Od jednotlivých fází, kterými (kyber)šikana prochází, se odvíjí míra zapojení přihlížejících, intenzita útoků a psychické dopady na oběť (ale i na zapojivší se přihlížející), počínaje ignorováním a konče kyberšikanováním ze strany celého kolektivu coby norma běžného chování. Agresoři bývají necitliví, nadprůměrně inteligentní, toužící po sebeprosazení, s poruchou psychického vývoje a s předchozí vlastní zkušeností s (kyber)šikanou. Obětí může být kdokoli (deklarovaný důvod bývá jen zástupný), obecně znamená zvýšenou vulnerabilitu jakákoliv výrazná odlišnost a předchozí zkušenost s (kyber)šikanou v roli oběti. Na rozvoj prvotního jednání v kyberšikanu má zásadní vliv atmosféra celého kolektivu – zda ji akceptuje či odmítne.

Kyberšikany se dotýkají metodické pokyny MŠMT, školský zákon a prováděcí předpisy, neboť agresoři obvykle porušují školní řád. Dále je zde občanskoprávní rovina (NOZ) vzhledem k obvyklému porušování ochrany osobnosti v mnoha podobách (zejm. důstojnost, vážnost, čest, soukromí, projevy osobní povahy), případně odpovědnost za škodu. Dochází i

k přestupkům, zejm. proti občanskému soužití, případně proti majetku (zák. o některých přestupcích). V souvislosti s kyberšikanou hojně dochází k neoprávněnému přístupu k počítačovému systému a nosiči informací, a to zejm. neoprávněnými průniky a manipulací s daty na SNS, předcházet (s následnou faktickou konzumpcí) může opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat. Se „zabráním" cizího profilu (např. změna přístupových údajů) a jeho používání jménem původního uživatele přichází v úvahu zejm. poškození cizích práv a/nebo poškození cizí věci (v důsledku neupotřebitelnosti účtu v hodnotě alespoň 5.000 Kč). Ad hoc vytvářené weby, blogy a profily i stránky na SNS mohou obsahovat i hate crime či pomluvu. Méně často pak dochází i na nebezpečné pronásledování a nebezpečné vyhrožování, vydírání a útisk (ve vyšších fázích kyberšikany). Emailová schránka bývá zahlcována pornografií (šíření pornografie) a její obsah bývá zveřejněn, podobně jako obsah „vypůjčeného" mobilního telefonu (porušování tajemství listin a jiných dokumentů uchovávaných v soukromí, méně často pak porušení tajemství dopravovaných zpráv). Vyloučena není ani loupež, krádež, podvod (zejm. v souvislosti s herními účty), výjimečně pak i účast na sebevraždě. De lege ferenda lze zvážit z hlediska prevence především snížení hranice pro souhlas subjektu se zpracováním jeho osobních údajů (potažmo používání SNS) z plánovaných 15 na nejnižších možných 13 let, které by umožnilo výchovnou práci se SNS již v rámci základní školy.

Internet představuje pro projevy nesnášenlivosti i nad rámec kyberšikany přímo živnou půdu, a to nejen z obvyklého úhlu pohledu zdůrazňujícího právo na svobodu projevu a ochranu menšin v protikladu k prezentaci extremistů a problematický postih protiprávního obsahu. Radikalizace společnosti nezačíná u extremistických hnutí, ale v drobných, leč vytrvalých názorových posunech. Vzhledem ke snadnosti nalezení prakticky jakékoliv názorově blízké skupiny osob, online prostředí tíhne k seskupování a sdružování podobně zaměřených lidí, kteří se vzájemně utvrzují ve svých postojích. Snadno pak začnou vytěsňovat osoby s odlišným pohledem a postupně se vzdalovat realitě (např. původní nejasně formulovaná obava z imigrace přeroste v přesvědčení o cílené likvidaci evropské populace). Částečně k tomu přispívá i personalizace obsahu zpravodajskými aj. servery a vyhledávači v souladu s vlastním zaměřením uživatele. Nesnášenlivost a násilí online nabývá podob od hate speech (vč. tzv. trollingu) přes tzv. happy slapping po hate crime. Množství násilného obsahu koluje na SNS a videoportálech a láká ke shlédnutí a sdílení zejm. dospívající chlapce s malou představou o fyzickém kontaktu. Přidruží-li se komplex méněcennosti a (nenaplněná) touha po uznání a moci, dotyčný snadno přilne k extremistické skupině, která jej přijme za svého.

Extremistické a radikální skupiny využívají prakticky všechny ICT média, vlastní obsah může být zřejmý i skrytý (např. zdánlivě vzdělávací kanál, prezentace hudební skupiny atp.), hojně bývají využívány zdánlivě nevinné symbolické znaky. Trestněprávní postih podle zákona ČR není vyloučen ani v případě (častého) umístění serverů s protiprávním obsahem fyzicky mimo ČR, a to zejm. pro některý z trestných činů narušujících soužití lidí nebo trestných činů proti lidskosti, případně jiný trestný čin s obecně přitěžující okolností spáchání činu z nenávisti. Při zveřejnění či šíření násilného obsahu přichází v úvahu dále ještě týrání zvířat, výtržnictví, podněcování nebo schvalování trestného činu a případně ohrožování výchovy dítěte. Poskytovatelé služeb sice mnohdy usilují o omezení násilného a radikalizujícího obsahu, leč rozporuplnými způsoby.

Rychlý vývoj ICT a digitální propast kladou značné nároky na preventivní úsilí, jednak pro pestrou paletu předcházených jednání a dopadů, jednak pro odlišnosti samotných uživatelů. Primární prevence se proto zaměřuje obecně na základní pravidla bezpečného užívání ICT vůbec, nejčastěji v podobě preventivního obsahu nabízeného ze strany mnoha institucí a organizací i uživateli samými, případně formou krátkých videospotů (v TV či online na vyžádání). Klíčovým bezpečnostním faktorem je uživatel, prevence proto apeluje na nezbytné minimum základních bezpečnostních návyků: zejm. aktualizovaný a ochranný software, neignorování bezpečnostních varování, fyzické zabezpečení používaných zařízení, silná a různá hesla, zálohování dat, nepoužívání veřejného zařízení k práci s citlivými daty, obezřetná instalace aplikací a udílení oprávnění, kontrola a minimalizace vlastního digitálního otisku, vědomí digitálního charakteru obsahu online, ověřování identity aj. informací, používání pouze důvěryhodných zdrojů, blokace podezřelých emailů a uživatelů, hoaxů a řetězových emailů, nepřeposílání potvrzovacích sms, konzultace v rámci mezigeneračního dialogu. Sekundární prevence cílí zejm. na mládež ve vztahu k jednotlivým hrozbám a věnuje se především osvětě v oblasti sexuálního zneužívání (zvlášť rizika sextingu a kybergroomingu) a kyberšikany (trauma oběti, varovné signály), zvýšení digitální gramotnosti, pozitivnímu využívání ICT, kritickému uvažování a netiketě. Terciární prevence zahrnuje např. omluvný obsah na SNS nebo doporučení pro technické zabezpečení. Prevence by ovšem neměla zapomínat ani na odrazování útočníků, aby důraz na sebeochranu potenciálních obětí mimoděk nepotvrzoval škodlivé jednání v kyberprostoru coby normu. Na preventivních aktivitách se podílí řada osob, institucí a organizací, počínaje rodiči vykonávajícími rodičovskou odpovědnost. Dítě vychovávají a více či méně provází i kyberprostorem, podobně jako reálným světem. Vytváří základní rámec bezpečí a dispozice dítěte

k protiprávnímu jednání a vulnerabilitě. Škola a učitelé představují malý svět per se, kde se děti učí vzájemné interakci. Může děti vést k zodpovědnému a pozitivnímu přístupu k ICT, vede osvětu a probíhá zde i peer-to-peer prevence, jinak zajišťovaná především youtubery. OSPOD spolupracuje v zájmu dítěte s ním samým, rodiči, školou a dalšími osobami, poskytuje pomoc, a může i ukládat určité povinnosti k nápravě. Řada institucí a organizací vytváří osvětové materiály, pořádá školení, provozuje horké linky a nabízí technické nástroje (např. rodičovská kontrola). Za zmínku stojí především evropský projekt Better Internet for Kids, NCBI, PRVoK, Seznam.cz, Akademie CZ.NIC, Linka bezpečí, Horká linka (spolupracující s mezinárodní sítí Inhope), BezpečnýInternet.cz aj.

Co se týče trendů kyberkriminality, ve vztahu k mládeži lze čerpat převážně z ad hoc varování vydávaných neziskovými organizacemi věnujícími se prevenci v online prostředí. Již bez bližšího zaměření na děti pak vydávají ad hoc i souhrnné zprávy a varování mnozí aktéři ze státního i komerčního sektoru: např. NÚKIB, CZ.NIC, Ministerstvo vnitra ČR, Nejvyšší státní zastupitelství, nad rámec ČR pak společnosti jako Eset, McAfee, IBM atp. Mezi nejvýraznější a vytrvale rostoucí trendy patří sběr osobních údajů aj. dat, ohrožení IoT (zvyšuje se jejich množství i využití), útoky na chytré mobilní telefony, ransomware, útoky na veřejnou správu, DDoS, přebírání účtů (zejm. SNS, elektronické bankovnictví, herní platformy), nakládání s dětskou pornografií, využívání dark webu (a BTC) a rostoucí sofistikovanost útoků a organizace pachatelů vůbec. S ohledem na stále užší provázanost ICT s každodenním životem a rozvoj IoT lze předpokládat, že se budeme potýkat s kyberkriminalitou i nadále a zřejmě stále častěji.

Zbývá shrnout ověřované hypotézy, tedy 1. mládež, tj. děti a mladiství jsou v online prostředí ohroženy kriminalitou; 2. mládež se v online prostředí dopouští provinění a činů jinak trestných. K ohrožení kriminalitou v online prostředí dochází od raného věku dítěte, počínaje možným zneužitím digitálního otisku utvářeného druhými a setkáním se s nevhodným obsahem (byť tento nemusí vždy dosahovat trestněprávní roviny). V citlivém období utváření vlastní identity a potřebě uznání ze strany ostatních v průběhu dětství a dospívání dochází k sexuálnímu zneužívání prostřednictvím sextingu, manipulaci při kybergroomingu a traumatizaci při projevech kyberšikany, umožněných a umocněných snadností, rychlostí a masovostí sdíleného digitalizovaného obsahu na SNS. Zvýšeně ohrožena je mládež s vyšší vulnerabilitou i v reálném prostředí, varovným signálem může být mj. netholismus či excesivní užívání ICT. Děti a mladiství pachatelé v online prostředí využívají zejm. SNS a oproti dospělým častěji jednají ve formě virtuálního násilí, ať už jde o nejběžnější

kyberšikanu nebo jednání z pomsty či žárlivosti expartnerů zveřejňujících sexting. K protiprávnímu jednání online přispívá na jedné straně větší anonymita a nižší kontrola oproti reálnému prostředí, na druhé straně nedomýšlení důsledků vlastního jednání ve spojení s fyzicky nepřítomnou obětí. Opomenout nelze ani další faktory jako specifika komunikace bez neverbální složky, čas trávený online na úkor offline, nerozlišování reálných a virtuálních vztahů aj. Pachatelé útočí především na vrstevníky a většinou je neohrožují fyzicky, leč způsobená psychická zranění jsou přinejmenším srovnatelná s fyzickými dopady.

ZÁVĚR

Problematika kriminality spojené s využíváním nových médií dětmi představuje poměrně širokou oblast, kterou lze pojmout hned z několika úhlů pohledu: kromě právního také sociologicky, psychologicky, ale i se zohledněním biologických aspektů života. Nabízí se i dílčí oblasti, které zasluhují velkou (větší) pozornost per se – např. vliv počítačových her nebo SNS a komunikační aspekty vůbec, vliv kyberprostoru na psychosomatiku, vztah mezi sebepojetím, sebevědomím a pocitem pohody v reálném světě či naopak frustrace v závislosti na čase stráveném v online hře a tam dosaženou mírou úspěchu a uznání aj. Pokusila jsem se alespoň částečně uchopit zvolené téma se zohledněním všech výše zmíněných, a přestože si uvědomuji v důsledku toho snad až povrchnost vyjádření v některých místech, domnívám se, že je zcela namístě pokusit se podat plastický obrázek pracující se všemi těmito paradigmaty, neboť teprve v jejich souhrnu vyvstávají některé aspekty s náležitým významem.

Na závěr zbývá ještě několik úvah nad tím, co zasluhuje zvláštní pozornost a nedostalo se jí (vyjma samostatného zpracování celého tématu výlučným paradigmatem toho kterého oboru a již navržených otázek). Z praktických otázek lze jmenovat statistické údaje k trestnému činu výroby a jiného nakládání s dětskou pornografií, které by umožnily podrobnější pohled zohledňující §192 odst. 2 TZ coby základní skutkovou podstatu a její praktické využití. Nanejvýš žádoucí by bylo také pokračování výzkumu IKSP doplněním časové řady o další roky při sledování stejných proměnných za účelem srovnání, vyloučení nahodilostí a predikce. Výzkum IKSP vůbec upozornil na některé zajímavé otázky, které by stály za hlubší promyšlení, např. neopatrnost uživatelů (vč. zaměstnavatelů a bývalých zaměstnavatelů), odlišné zapojení pachatelek, ale i zvláštnosti mladých dospělých pachatelů. Další pozornost by zasloužila také podrobnější analýza viktimizačních faktorů a psychosociální aspekty obětí různých typů kyberkriminality, pro lepší prevenci kybergroomingu pak možnosti zamezení nežádoucího kontaktování a odrazení od pokračování v již započaté komunikaci. Možných námětů je nepřeberné množství: kyberstalking, droni a porušování soukromí, nakupování online a personalizovaná reklama, hoaxy, malware, hazard online, spam, umělá inteligence a přidružená problematika vč. filosofických otázek (např. vývoj a použití „AI kamaráda“), ochrana osobních údajů zejm. v souvislosti se sběrem a používáním biologických dat (rozpoznávání věku a osoby vůbec, otisky prstů používané k přístupu k aplikaci či zařízení atp.), vzdělávání 4.0 atd. Časoprostorové rozpojení výrazně ovlivňuje tzv. kolonizaci času ve směru časového i prostorového rozšíření činností jednotlivce nad rámec tradičních zón. Zřejmě proto dojde změn i „tradiční“ časoprostorové mapování činností, vč. mapování

kriminality, neboť např. tradičně geograficky určená „horká místa“ (hot spots), tj. místa s výrazně vyšší koncentrací kriminálních činností, lze najednou chápat jako místa lokalizovatelná nikoliv fyzicky prostorově, nýbrž „v síti“. Podobně by se mohlo i tradiční mapování sociálních kontaktů a kriminálních vazeb použít pro „mapování“ vztahů a pohybu na internetu (např. souvztažně navštěvované stránky), nicméně zde bychom zcela jistě narazili na ochranu osobních údajů co do sběru dat a záhy i pokročilé způsoby maskování při použití mapování k rozkrývání kyberkriminality. Ráda bych také ověřila funkčnost teorie sociální dezorganizace v online prostředí.

Kyberprostor se rozvinul v paralelní, virtuální svět, v duchu sebenaplňujícího se proroctví zcela reálný ve svých důsledcích. Provázanost s reálným prostředím (z velké části díky IoT) dostoupila takové míry, že si ho již dost dobře nelze bez kyberprostoru představit. Není proto již namístě hovořit o virtuální „a“ skutečné (fyzické) realitě, nýbrž jen a pouze o jejich vzájemném propojení ve svébytné podobě jediné reality. Snad bychom proto mohli mít i základní lidské právo na virtuální identitu.

Seznam zkratek a některých pojmů

AI	Artificial Intelligence, umělá inteligence
AutZ	zákon č. 21/2000 Sb., autorský zákon
BTC	BTC, virtuální měna
CoC	Convention on Cybercrime, CETS No. 185, Úmluva o počítačové kriminalitě
ČR	Česká republika
DDoS	Distributed Denial of Service, distribuované odmítnutí služby
Dodatkový protokol	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, dodatkový protokol k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů
EU	Evropská unie
FB	sociální síť Facebook
GDPR	General Data Protection Regulation, nařízení Evropského parlamentu a Rady 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
ICT	Information and communication technologies, informační a komunikační technologie
IKSP	Institut pro kriminologii a sociální prevenci
IoT	Internet of Things, internet věcí
Listina	ústavní zákon č. 2/1993, Listina základních práv a svobod
malware	škodlivý software
MŠMT	Ministerstvo školství, mládeže a tělovýchovy ČR
NOZ	zákon č. 89/2012 Sb., občanský zákoník
NÚKIB	Národní úřad pro informační a komunikační bezpečnost
počítačové trestné činy	Trestné činy uvedené v § 230-232 TZ a v § 257a sTZ
P2P	peer-to-peer spojení, tj. přímé propojení konkrétních zařízení
PS	počítačový systém
SNS	Social networks, sociální sítě online (FB aj.)
sTZ	zákon č. 140/1961 Sb., trestní zákon
škola	škola a školské zařízení dle školského zákona
TOPO	zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim
TŘ	zákon č. 141/1961 Sb., trestní řád
TZ	zákon č. 40/2009 Sb., trestní zákoník
Ústava	ústavní zákon č. 1/1993, Ústava ČR
VoIP	Voice over Internet Protocol, přenos řeči po internetu
Výzkum IKSP	výzkum kybernetické kriminality zaměřený na počítačové trestné činy probíhající v IKSP v letech 2016-2019
ZoKB	zákon č. 181/2014 Sb., o kybernetické bezpečnosti
ZSPOD	zákon č. 359/1999 Sb., o sociálně-právní ochraně dětí
ZSVM	zákon č. 218/2003 Sb., o soudnictví ve věcech mládeže

Seznam použitých zdrojů

1. Seznam použité literatury

1.1. Učebnice, komentáře

Draštík, Antonín, a další. 2015. *Trestní zákoník. Komentář.* Praha: Wolters Kluwer, 2015. ISBN 978-80-7478-790-4

Fenyk, Jaroslav, Císařová, Dagmar a Gřivna, Tomáš a kol. 2015. *Trestní právo procesní.* 6. vyd. Praha: Wolters Kluwer, 2015. ISBN 978-80-7478-750-8

Gřivna, Tomáš, Scheinost, Miroslav, Zoubková, Ivana a kol. 2015. *Kriminologie.* Praha: Wolters Kluwer, 2015. ISBN 978-80-7478-614-3

Gřivna, Tomáš, Šámal, Pavel a Válková, Helena et al. 2014. *Zákon o obětech trestných činů. Komentář.* Praha: C.H.Beck, 2014. ISBN 978-80-7400-513-8

Hrušáková, Milana a Žatecká, Eva. 2015. *Zákon o soudnictví ve věcech mládeže. Komentář.* Praha: Wolters Kluwer, 2015. ISBN 978-80-7478-849-9

Hrušáková, Milana, a další. 2014. *Občanský zákoník II. Rodinné právo (§ 655−975).* Praha: C. H. Beck, 2014. ISBN 978-80-7400-503-9

Hulmák, Milan et al. 2014. *Občanský zákoník VI. Závazkové právo. Zvláštní část (§ 2055–3014). Komentář.* Praha: C.H.Beck, 2014. ISBN 978-80-7400-287-8

Chaloupková, Helena a Holý, Petr. 2012. *Autorský zákon. Komentář.* 4. vyd. Praha: C.H.Beck, 2012. ISBN 978-80-7400-432-2

Jelínek, Jiří et al. 2017. *Trestní právo hmotné.* 6. vyd. Praha: Leges, s.r.o., 2017. ISBN 978-80-7502-236-3

—. 2008. *Trestní zákon a trestní řád.* 26. vyd. Praha: Linde, 2008. ISBN 978-80-7201-731-7

Jemelka, Luboš a Vetešník, Pavel. 2017. *Zákon o odpovědnosti za přestupky a řízení o nich. Zákon o některých přestupcích. Komentář.* Praha: C. H. Beck, 2017. ISBN 978-80-7400-666-1

Lavický, Petr et al. 2014. *Občanský zákoník I. Obecná část (§ 1−654). Komentář.* Praha: C. H. Beck, 2014. ISBN 978-80-7400-529-9

Maisner, Martin. 2016. *Zákon o některých službách informační společnosti.* Praha: C.H.Beck, 2016. ISBN 978-80-7400-449-0

Šámal, Pavel et al. 2016. *Trestní právo hmotné*. 8. vyd. Praha: Wolters Kluwer ČR, 2016. ISBN 978-80-7552-358-7

—. 2012. *Trestní zákoník. Komentář.* 2. vyd. Praha: C. H. Beck, 2012. ISBN 978-80-7400-428-5

Šámal, Pavel, a další. 2011. *Zákon o soudnictví ve věcech mládeže,* 3. vyd. Praha: C.H.Beck, 2011. ISBN 978-80-7400-350-9

Švestka, Jiří, Dvořák, Jan, Fiala, Josef et. al. 2014. *Občanský zákoník komentář, svazek 1.* Praha: Wolters Kluwer, 2014. ISBN 978-80-7478-370-8

Telec, Ivo a Tůma, Pavel. 2007. *Autorský zákon. Komentář.* Praha: C.H.Beck, 2007. ISBN 978-80-7179-608-4

Válková, Helena a Kuchta, Josef a kol. 2012. *Základy kriminologie a trestní politiky.* Praha: C.H.Beck, 2012. ISBN 978-80-7400-429-2

Wagnerová, Eliška, a další. 2011. *Listina základních práv a svobod. Komentář.* Praha: Wolters Kluwer, 2011. ISBN 978-80-7357-750-6

1.2. Výzkumné zprávy, studie, zdroje statistických dat

Capin, Tolga K., a další. 1999. Realistic Avatars and Autonomous Virtual Humans in VLNET Networked Virtual Environments. In Vince, John a Earnshaw, Rae. *Virtual Worlds on the Internet.* Los Alamitos: Wiley-IEEE Computer Society Press, 1999

Costs of Cyber Crime Working Group. 2018. *Understanding the costs of cyber crime*. London: Home Office, 2018. ISBN 978-1-78655-392-8

Chaudron, Stephane et al. 2015. Young Children (0-8) and digital technology: A qualitative exploratory study across seven countries. *Report EUR 27052 EN.* Joint Research Centre, European Commission, 2015. ISBN 978-92-79-45023-5 ISSN 1831-9424

Kopecký, Kamil. 2010. *Kybergrooming - nebezpečí kyberprostoru. Studie.* Olomouc: NET UNIVERSITY s.r.o., 2010. ISBN 978-80-254-7573-7

—. 2010. *Stalking a kyberstalking. Studie.* Olomouc: NET UNIVERSITY s.r.o., 2010. ISBN 978-80-254-7737-3

1.3. Vlastní publikace

(Ne)uživatelé internetu – malý průvodce kybernástrah. **Kudrlová, Kateřina. 2015.** Svratka: Masarykova česká sociologická společnost, 2015. Ohrožené a rizikové skupiny současnosti. Stránky 119-123. ISBN 978-80-905443-2-1

Avatar jako kriminogenní faktor. **Svatoš, Roman a Kříha, Josef (eds.). 2014.** České Budějovice: Vysoká škola evropských a regionálních studií, o.p.s., 2014. II. kriminologické dny. Stránky 108-115. ISBN 978-80-87472-65-1

Kudrlová, Kateřina a Vlach, Jiří. 2017. Kyberkriminalita (nejen) v ČR - její stav a trendy. *Kriminalistika.* 2017, č. 4

Kyberkriminalita dnes. **Kudrlová, Kateřina. 2014.** In Šturma, Pavel a Žákovská, Karolina (eds.). Praha: Univerzita Karlova v Praze, Právnická fakulta, 2014. VII. konference studentské vědecké odborné činnosti. Sekce doktorandských prací. Stránky 20-33. ISBN 978-80-87975-12-1

Kybernetická kriminalita - dílčí poznatky z výzkumu II. **Kudrlová, Kateřina. 2018.** Olomouc: Iuridicum Olomoucense, 2018. Kriminologické dny 2018. Stránky 148-157. ISBN 978-80-88266-15-0

Lukášová, Kateřina. 2010. Etiologie kriminality a teorie nerovností Charlese Tillyho. *Studentská odborná vědecká činnost.* Praha: Univerzita Karlova v Praze, Právnická fakulta, 2010

—. 2009. Principy spravedlnosti - pohled na současnou diskusi. *Diplomová práce.* Praha: Fakulta sociálních věd Univerzity Karlovy v Praze, katedra sociologie, 2009

—. 2012. Škodlivý obsah na internetu. *Acta Universitatis Iuridica.* 2012, č. 4

Ochráníme děti před sexuálním zneužíváním kriminalizací jednání? **Lukášová, Kateřina. 2013.** Praha: Masarykova česká sociologická společnost, 2013. Prevence sociálních deviací – přání, naděje a realita. Sborník příspěvků z konference sekce sociální patologie MČSS. Stránky 189-194. ISBN 978-80-905443-0-7

Vybrané navrhované změny trestního zákoníku - § 192, 193b TZ. **Lukášová, Kateřina. 2013.** [editor] Pavel (ed.) Šturma. Praha: Univerzita Karlova v Praze, Právnická fakulta, 2013. VI. konference studentské vědecké odborné činnosti. Stránky 55-68. ISBN 978-80-87146-84-2

1.4. Monografie

Bartík, Václav a Eva, Janečková. 2016. *Ochrana osobních údajů v aplikační praxi.* Praha: Wolters Kluwer, 2016. ISBN 978-80-7552-141-5

Bartlett, Jamie. 2015. *The Dark Net: Inside the Digital Underworld.* Brooklyn: Melville House, 2015. ISBN 978-1-61219-489-9

Bauman, Zygmunt. 2000. *Myslet sociologicky.* Praha: SLON, 2000. ISBN 80-85850-90-7

Berger, Peter L. a Luckmann, Thomas. 1999. *Sociální konstrukce reality.* Brno: Centrum pro studium demokracie a kultury, 1999. ISBN 80-85959-46-1

Bernstein, Basil. 1971. *Class, Code and Control: Volume 1 – Theoretical Studies Towards a Sociology of Language.* London, Boston: Routledge & Kegan Paul Books, 1971. ISBN 9780710070609

Bourdieu, Pierre. 2000. *Nadvláda mužů.* Praha: Karolinum, 2000. ISBN 80-7184-775-5

Buber, Martin. 1996. *Já a ty.* Olomouc: Votobia, 1996. ISBN 80-7198-042-1

Cviklová, Lucie, Krýsl, Šimon a Vomlelová-Weissová, Kateřina. 1999. *Čítanka kritické teorie. Díl 1. Rozhovory s Jürgenem Habermasem.* Praha: SLON, Nadace Open Society Fund, 1999. ISBN 80-238-4738-4

Čírtková, Ludmila. 2008. *Moderní psychologie pro právníky.* Praha: Grada, 2008. ISBN 978-80-247-2207-8

Elders, Fons, Foucault, Michel a Chomsky, Noam. 2005. *Člověk, moc a spravedlnost.* Praha: Intu, 2005. ISBN 80-903355-3-5

Eckertová, Lenka a Dočekal, Daniel. 2013. *Bezpečnost dětí na internetu. Rádce zodpovědného rodiče.* Brno: Computer Press, 2013. ISBN 978-80-251-3804-5

Fischer, Slavomil a Škoda, Jiří. 2009. *Sociální patologie.* Praha: Grada, 2009. ISBN 978-80-247-2781-3

Foucault, Michel. 1994. *Diskurz, Autor, Genealogie.* Praha: Svoboda, 1994

Fraser, Nancy a Honneth, Axel. 2004. *Přerozdělování nebo uznání?* Praha: Filosofia, 2004. ISBN 80-7007-200-8

Fraser, Nancy. 2007. *Rozvíjení radikální imaginace.* Praha: Filosofia, 2007. ISBN 978-80-7007-251-6

Giddens, Anthony. 2003. *Důsledky modernity.* Praha: Sociologické nakladatelství SLON, 2003. ISBN 80-86429-15-6

—. 2000. *Sociologie.* Praha: Argo, 2000. ISBN 80-7203-124-4

Glasser, William. 2001. *Terapie realitou.* Praha: Portál, 2001. ISBN 80-7178-493-1

Goffman, Erving. 1999. *Všichni hrajeme divadlo.* Praha: Nakladatelství Studia Ypsilon, 1999. ISBN 978-80-262-1342-0

Gregor, M., Vejvodová, P., Zvol si info. 2018. *How to manipulate: the techniques of online disinformation media.* Brno: Albatros Media a.s., 2018

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

Habermas, Jürgen. 2001. Boje o uznání v demokratickém právním státě. In Taylor, Charles. *Multikulturalismus.* Praha: Filosofia, 2001. ISBN 80-7007-161-3

—. 2000. *Problémy legitimity v pozdním kapitalismu.* Praha: Filosofia, 2000. ISBN 80-7007-130-3

Günther, Klaus. 1997. Co znamená: „Každému to, co mu náleží?“ K novému odhalení distributivní spravedlnosti. In Velek, Josef (ed.). *Spor o spravedlnost.* Praha: Filosofia, 1997. ISBN 80-7007-115-X

Hinduja, Sameer K. a Patchin, Justin W. 2014. *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying.* Thousand Oaks: Corwin, 2014. ISBN 978-1-4833-4993-0

—. 2012. *Cyberbullying prevention and response: expert perspectives.* New York: Routledge, 2012. ISBN 978-0-41589-237-7

Hlavenka, Jiří et al. 1997. *Výkladový slovník výpočetní techniky a komunikací.* 3. vyd. Praha: Computer Press, 1997. ISBN 80-7226-023-5

Holas, Jakub. 2013. *Politický radikalismus a mládež.* Praha: Institut pro kriminologii a sociální prevenci, 2013. ISBN 978-80-7338-131-8

Honneth, Axel. 1996. *Sociální filosofie a postmoderní etika.* Praha: Filosofia, 1996. ISBN 80-7007-082-X

Hulanová, Lenka. 2012. *Internetová kriminalita páchaná na dětech.* Praha: Triton, 2012. ISBN 978-80-7387-545-9

Chmelík, Jan. 2000. *Symbolika extremistických hnutí.* Praha: Armex, 2000. ISBN 80-86244-14-8

Jelínek, Jiří a Ivor, Jaroslav et. al. 2015. *Trestní právo Evropské unie a jeho vliv na právní řád České republiky a Slovenské republiky.* Praha: Leges, 2015. ISBN 978-80-7502-080-2

Jelínek, Jiří et al. 2013. *Trestní odpovědnost právnických osob v České republice - bilance a perspektivy.* Praha: Leges, 2013. ISBN 978-80-87576-58-8

Jirásek, Petr, Novák, Luděk a Požár, Josef a kol. 2013. *Výkladový slovník kybernetické bezpečnosti.* Praha: Policejní akademie ČR, Policejní akademie ČR & Česká pobočka AFCEA, 2013. ISBN 978-80-7251-397-0

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

Kakalios, James. 2018. *Fyzika superhrdinů.* Praha: Argo, 2018. ISBN 978-80-257-2515-3

Kolář, Michal. 2011. *Nová cesta k léčbě šikany.* Praha: Portál, 2011. ISBN 978-80-7367-871-5

—. 1997. *Skrytý svět šikanování ve školách.* Praha: Portál, 1997. ISBN 80-7178-123-1

Kolouch, Jan a Bašta, Pavel a kol. 2019. *CyberSecurity.* Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-34-8

Krčmářová, Barbora. 2012. *Děti a online rizika.* Praha: Sdružení Linka bezpečí, 2012. ISBN 978-80-904920-2-8

Krištoufek, Karel. 1982. *Výpočetní a řídící technika.* Praha: SNTL, 1982

Křivohlavý, Jaro. 1988. *Jak si navzájem lépe porozumíme.* Praha: Svoboda, 1988

Le Bon, Gustave. 2016. *Psychologie davu.* Praha: Portál, 2016. ISBN 978-80-262-1028-3

Lechner, Tomáš. 2013. *Elektronické dokumenty v právní praxi.* Praha: Nakladatelství Leges, 2013. ISBN 978-80-87576-41-0

Lister, Martin, a další. 2003. *New Media: A Critical Introduction.* New York: Routledge, 2003. ISBN 9780415223782

Manovich, Lev. 2001. *The Language of New Media.* Cambridge: MIT Press, 2001. ISBN 9780262133746

Marešová, Alena a kol. 2015. *Analýza trendů kriminality v ČR v roce 2014.* Praha: IKSP, 2015. ISBN 978-80-7338-150-9

Matějka, Michal. 2002. *Počítačová kriminalita.* Praha: Computer press, 2002. ISBN 8072264192

Mauss, Marcel. 1999. *Esej o daru, podobě a důvodech směny v archaických společnostech.* Praha: SLON, 1999. ISBN 808585077X

Merton, Robert K. 2007. *Studie ze sociologické teorie.* Praha: SLON, 2007. ISBN 978-80-86429-70-0

Michalski, Krzysztof, Dahrendorf, Ralf, Taylor, Charles a další. 1994. *Liberální společnost.* Praha: Filosofie, 1994. ISBN 80-7007-063-3

Ministerstvo spravedlnosti ČR. 2017. *Statistická ročenka kriminality. Rok 2016.* 2017

Müller, Karel. 2003. *Češi a občanská společnost.* Praha: TRITON, 2003. ISBN 80-7254-387-3

Murphy, Robert F. 1998. *Úvod do kulturní a sociální antropologie.* Praha: Sociologické nakladatelství SLON, 1998. ISBN 978-80-86429-25-0

Musil, Stanislav (ed.). 2000. *Počítačová kriminalita. Nástin problematiky. Kompendium názorů specialistů.* Praha: Institut pro kriminologii a sociální prevenci, 2000. ISBN 80-86008-80-0

Nakonečný, Milan. 2009. *Sociální psychologie.* Praha: Academia, 2009. ISBN 978-80-200-1679-9

Navara, Luděk a Albrecht, Josef. 2010. *Abeceda komunismu.* Brno: HOST, 2010. ISBN 978-80-7294-340-1

Nešpor, Karel. 2018. *Návykové chování a závislost.* Praha: Portál, 2018. ISBN 978-80-262-1357-4

Otto, Jan. 1888. *Ottův slovník naučný.* Praha: J. Otto, 1888

Parsons, Talcott. 1971. *Společnosti: vývojové a srovnávací hodnocení.* Praha: Svoboda, 1971

Přibáň, Jiří. 1996. *Sociologie práva.* Praha: SLON, 1996. ISBN 80-85850-18-4

Rawls, John. 1995. *Teorie spravedlnosti.* Praha: Victoria Publishing, a.s., 1995. ISBN 80-85605-89-9

Rogers, Vanessa. 2011. *Kyberšikana.* Praha: Portál, 2011. ISBN 978-80-7367-984-2

Slaměník, Ivan a Výrost, Jozef et al. 2001. *Aplikovaná sociální psychologie II.* Praha: Grada, 2001. ISBN 8024700425

Smejkal, Vladimír. 2018. *Kybernetická kriminalita.* 2. vyd. Plzeň: Aleš Čeněk, 2018. ISBN 978-80-7380-720-7

Sokol, Jan. 1998. *Malá filosofie člověka. Slovník filosofických pojmů.* Havlíčkův Brod: Vyšehrad, 1998. ISBN 80-7021-253-5

Taylor, Charles. 2001. *Multikulturalismus.* Praha: Filososofia, 2001. ISBN 80-7007-161-3

Tilly, Charles. 1998. *Durable inequality.* Barkeley / Los Angeles / London: University of California Press, 1998. ISBN 9780520221703

Vágnerová, Marie. 2014. *Současná psychopatologie pro pomáhající profese.* Praha: Portál, 2014. ISBN 978-80-262-0696-5

Vince, John a Earnshaw, Rae (eds.). 1999. *Virtual Worlds on the Internet (Practitioners).* Los Alamitos: Wiley-IEEE Computer Society Press, 1999. ISBN 978-0-8186-8700-6

Vymětal, Jan. 2008. *Průvodce úspěšnou komunikací - efektivní komunikace v praxi.* Praha: GradaPublishing a.s., 2008. ISBN 8024726144

Wall, David S. 2007. *Cybercrime. The Transformation of Crime in the Information Age.* Cambridge: Polity Press, 2007. ISBN 978-07-4562-736-6

Willard, Nancy. 2012. *Cyber Savvy: Embracing Digital Safety and Civility.* Thousand Oaks: Corwin Press, 2012. ISBN 978-1412996211

Wittgenstein, Ludwig. 1922. *Tractatus Logico-Philosophicus.* London / New York: K. Paul, Trench, Trubner & Co., Ltd. / Harcourt, Brace & Company, Inc., 1922

Zeman, Petr, a další. 2010. *Názory a postoje občanů v oblasti trestní politiky.* Praha: Institut pro kriminologii a sociální prevenci, 2010. ISBN 978-80-7338-098-4

1.5. Ostatní

Auxéméry, Yann a Fidelle, Geneviève. 2010. Impact d'Internet sur la suicidalité. À propos d'une "googling study" sur la rétro-information médiatique d'un pacte suicidaire échafaudé sur le Web. *Annales médico-psychologiques.* 2010, č. 7

Čírtková, Ludmila. 2010. Threatassessment: psychologické posuzování nebezpečnosti výhrůžek a hrozeb. *Kriminalistika.* 2010, č. 2

Daine, Kate, a další. 2013. The Power of the Web: A Systematic Review of Studies of the Influence of the Internet on Self-Harm and Suicide in Young People. *PLoS One.* 2013, č. 10

Dardayrol, Jean-Pierre. 2013. L'Internet des objets: quelles perspectives pour les acteurs de la logistique ? *Annales des Mines - Réalités industrielles.* 2013, č. 2

Fialová, Eva. 2010. Krádež virtuálních předmětů v příkladech z nizozemské judikatury. *Revue pro právo a technologie* 2010, č. 1

Freyssinet, Éric. 2013. L'Internet des objets: un nouveau champ d'action pour la cybercriminalité. *Annales des Mines - Réalités industrielles.* 2013, č. 2

Granic, Isabela, Lobel, Adam a Engels, Rutger C. M. E. 2014. The Benefits of Playing Video Games. *American Psychologist.* 2014, č. 1

Gřivna, Tomáš a Drápal, Jakub. 2018. Attacks on the confidentiality, integrity and availability of data and computer systems in the criminal case law of the Czech Republic. *Digital Investigation.* 2018, č. 28

Hay, Carter a Meldrum, Ryan. 2010. Bullying Victimization and Adolescent Self-Harm: Testing Hypotheses from General Strain Theory. *Journal of Youth and Adolescence.* 2010, č. 5

Herczeg, Jiří. 2008. Virtuální dětská pornografie? Zločin bez oběti? Vanduchová, Marie, Gřivna, Tomáš (eds.). *Pocta Otovi Novotnému k 80. narozeninám.* Praha: ASPI, Wolters Kluwer, 2008. ISBN 978-80-7357-365-2

Hill, Russel a Dunbar, Robin. 2003. Social network size in humans. *Human Nature.* 2003, č. 1

Ikegami, Eiko. 2011. Visualizing the networked self. *Social Research.* 2011, č. 4

Jansa, Lukáš. 2017. Použití open source v rámci vývoje a jeho licencování. *IT Systems.* 2017, č. 1-2

Kriminalita mladistvých imigrantů. **Pošíková, Lenka. 2013.** Žilina: EUROKÓDEX, 2013. Trestnoprávne a kriminologické aspekty kriminality mládeže. Stránky 169-182. ISBN 978-80-8155-025-6

Kybernetická kriminalita - dílčí poznatky z výzkumu I. **Vlach, Jiří. 2018.** Olomouc: Iuridicum Olomoucense, 2018. Stránky 38-147. ISBN 978-80-88266-15-0

Látal, Ivo. 1998. Počítačová (informační) kriminalita a úloha policisty při jejím řešení. *Policista.* 1998, č. 3

Lauria, Rita M. a Robinson, George S. 2013. From Cyberspace to Outer Space: Existing Legal Regimes Under Pressure from Emerging Meta-Technologies. *University of La Verne Law Review.* 2013, č. 2

Lhotka, Ladislav. 2005. Obecná veřejná licence GNU. *Zpravodaj ÚVT MU.* 2005, č. 5

Lindsay, David, de Zwart, Melissa a Collins, Francesca. 2010. My Self, My Avatar, My Rights? Rights of Avatar Identity and Integrity in Virtual Worlds. In Říha, Daniel (ed.). *Humanity in Cybernetic Environments.* Oxford: Inter-Disciplinary Press, 2010, stránky 147-157. ISBN 9781904710714

Loučka, Martin. 2016. Právní povaha konfiguračních souborů a jejich ochrana. *Revue pro právo a technologie.* 2016, č. 13

Luxton, David D., June, Jennifer D. a Fairall, Jonathan M. 2012. Social Media and Suicide: A Public Health Perspective. *American Journal of Public Health.* 2012, č. 2

Madliak, Jozef, Mihal'ov, Ján, Porada, Viktor, Štefanková, Simona. 2008. Počítačová kriminalita. *Karlovarská právnická revue.* 2008, č. 1

Macháčková, Hana a Šerek, Jan. 2017. Does 'clicking' matter? The role of online participation in adolescents' civic development. *Cyberpsychology.* 2017, č. 4

Merton, Robert K. 1948. The Self-Fulfilling Prophecy. *The Antioch Review.* 1948, č. 2

Mohr, Pavel. 2017. Co přinese nová klasifikace MKN-11? *Česká a slovenská psychiatrie.* 2017, č. 4

Prensky, Marc. 2001. Digital Natives, Digital Immigrants Part 1. *On the Horizon.* 2001, č. 5

Primack, Brian A., a další. 2012. Role of Video Games in Improving Health-Related Outcomes. *American Journal of Preventive Medicine.* 2012, č. 6.

Răcătău, Ionela-Maria. 2013. Adolescents and identity formation in a risky online environment. The role of negative user-generated and xenophobic websites. *Journal of Media Research.* 2013, č. 3

Rodham, Karen, a další. 2013. An investigation of the motivations driving the online representation of self-injury: a thematic analysis. *Archives of Suicide Research.* 2013, č. 2

Rosen, Lawrence. 2001. Derivative Works. *Linux Journal.* 2001, č. 105

Sabatini, Fabio a Sarracino, Francesco. 2017. Online Networks and Subjective Well-Being. *Kyklos.* 2017, č. 3

Sedláček, Mojmír. 2018. O sebevraždě je třeba mluvit. *Psychologie dnes.* 2018, č. 6

Subjective well-being prediction from social networks: A review. **Singh, Simarpreet a Kaur, Pankaj Deep. 2016.** Waknaghat: IEEE, 2016. 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC). Stránky 90-95

Tomíšek, Jan. 2014. Software jako věc v režimu nového občanského zákoníku. *Revue pro právo a technologie.* 2014, č. 14

Volek, Jaromír, Jirák, Jan a Köpplová, Barbara. 2006. Mediální studia: východiska a výzvy. *Mediální studia.* 2006, č. 1

Weinborn, Cristobal, a další. 2018. Spatiotemporal patterns and distributions of harm within street segments: The story of the "harmspot". *Policing An International Journal of Police Strategies and Management.* 2018, č. 3

Williams, Matthew. 2007. Avatar watching: participant observation in graphical online environments. *Qualitative Research.* 2007, č. 1

Wolfendale, Jessica. 2007. My avatar, my self: Virtual harm and attachment. *Ethics and Information Technology.* 2007, č. 2

Zaheer, Hussain a Griffiths, Mark D. 2008. Gender Swapping and Socializing in Cyberspace: An Exploratory Study. *Cyberpsychology & Behavior.* 2008, č. 1

2. Seznam použitých internetových zdrojů

2.1. Výzkumné zprávy, studie, zdroje statistických údajů

Bennington-Castro, Joseph. 2015. 6 Ways Video Games May Improve MS Symptoms. *everydayhealth.com.* [Online] [Citace: 24. 08. 2018] https://www.everydayhealth.com/multiple-sclerosis/symptoms/ways-video-games-may-improve-ms-symptoms/

Cooper, Anderson. 2018. Groundbreaking study examines effects of screen time on kids. *cbsnews.com.* [Online] [Citace: 18. 01. 2019] https://www.cbsnews.com/news/groundbreaking-study-examines-effects-of-screen-time-on-kids-60-minutes/

Český statistický úřad. Informační společnost v číslech. *czso.cz.* [Online] [Citace: 19. 07. 2018] https://www.czso.cz/csu/czso/informacni_spolecnost_v_cislech

—. Informační technologie v domácnostech a mezi jednotlivci. *czso.cz.* [Online] [Citace: 17. 07. 2018] https://www.czso.cz/csu/czso/domacnosti_a_jednotlivci

—. 2018. Věkové složení obyvatelstva - 2017. *czso.cz.* [Online] [Citace: 04. 08. 2018] https://www.czso.cz/csu/czso/vekove-slozeni-obyvatelstva-2017

—. 2017. Využívání informačních a komunikačních technologií v domácnostech a mezi jednotlivci za období 2017. *czso.cz.* [Online] [Citace: 04. 08. 2018] https://www.czso.cz/documents/10180/46014700/06200417.pdf/a0bd4497-d2b6-450b-95f0-2f70c50786d5?version=1.1

d'Haenens, Leen, Vandoninck, Sofie a Donoso, Verónica. 2013. How to cope and build online resilience? [Online] [Citace: 31. 08. 2018] http://eprints.lse.ac.uk/48115/ http://eprints.lse.ac.uk/48115/1/How%20to%20cope%20and%20build%20online%20resilience%20%28lsero%29.pdf

Drew, Shawn. 2015. Cebr Survey Highlights Key Trends in Cybercrime and What They Mean for CISOs. *veracode.com.* [Online] [Citace: 30. 08. 2017] https://www.veracode.com/blog/2015/10/cebr-survey-highlights-key-trends-cybercrime-and-what-they-mean-cisos-sw

ENISA. 2018. ENISA Threat Landscape Report 2017. *enisa.europa.eu.* [Online] [Citace: 04. 09. 2018] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017

ESET. 2018. Cyber Security trends of 2018. *eset.com.* [Online] [Citace: 04. 09. 2018] https://www.eset.com/uk/about/newsroom/corporate-blog/blog/cyber-security-trends-of-2018/

—. 2014. Cybercrime Trends & Predictions for 2015. *welivesecurity.com.* [Online] [Citace: 30. 08. 2017] http://www.welivesecurity.com/2014/12/18/cybercrime-trends-predictions-2015

—. 2017. The year in security: Trends 2017. *welivesecurity.com.* [Online] [Citace: 30. 08. 2017] https://www.welivesecurity.com/2017/01/04/year-security-trends-2017

—. 2015. Trends for 2015. Targeting the corporate world. *welivesecurity.com.* [Online] [Citace: 30. 08. 2017] http://www.welivesecurity.com/wp-content/uploads/2015/02/trends-2015-targeting-corporate-world.pdf

eukidsonline.net. EU Kids Online. Findings, methods, recommendations. *lsedesignunit.com.* [Online] [Citace: 29. 08. 2018] https://lsedesignunit.com/EUKidsOnline/html5/index.html?page=1&noflash

European Union Agency for Network and Information Security (ENISA). 2017. ENISA Threat Landscape Report 2016. 15 Top Cyber-Threats and Trends. *enisa.europa.eu.* [Online] [Citace: 30. 08. 2017] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

Granic, Isabela. 2013. Video Games Play May Provide Learning, Health, Social Benefits, Review Finds. *apa.org.* [Online] [Citace: 28. 08. 2018] http://www.apa.org/news/press/releases/2013/11/video-games.aspx

Handwerk, Brian. 2009. Video Games Improve Vision, Study Says. *news.nationalgeographic.com.* [Online] [Citace: 10. 05. 2010] http://news.nationalgeographic.com/news/2009/03/090329-video-game-vision.html

Hewlett Packard Enterprise Development LP. 2015. HPE Security Research. Cyber Risk Report 2015. *hpe.com.* [Online] [Citace: 30. 08. 2017] h20195.www2.hpe.com/V4/getpdf.aspx/4aa5-0858enn

IBM. 2015. Four top cyber crime trends. *ibm.com.* [Online] [Citace: 30. 08. 2017] http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=SA&subtype=WH&htmlfid=SEL03045USEN

Kaspersky Lab. Kaspersky Lab Threat Predictions for 2018. *asperskycontenthub.com.* [Online] [Citace: 04. 09. 2018] https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07164714/KSB_Predictions_2018_eng.pdf

Kopecký, Kamil a Szotkowski, René. 2016. Národní výzkum kyberšikany učitelů. Výzkumná zpráva. Olomouc: Univerzita Palackého v Olomouci, Cetnrum prevence rizikové virtuální komunikace, O2, Seznam.cz, 2016 [Online] [Citace: 26. 01. 2019] https://www.e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/86-kybersikana-ucitelu-2016-vyzkumna-zpraava/file

—. 2017. Sexting a rizikové seznamování českých dětí v kyberprostoru. Výzkumná zpráva. Olomouc: Univerzita Palackého v Olomouci, Centrum rizikové virtuální komunikace, O2, 2017 [Online] [Citace: 26. 01. 2019] https://drive.google.com/file/d/0B5sdIAT8WtLBUmV5VDdZNlJyRXc/view

Kovacs, Nadia. 2017. Top Ten Cyber Security Predictions for 2017. *community.norton.com.* [Online] [Citace: 30. 08. 2017] https://community.norton.com/en/blogs/norton-protection-blog/top-ten-cyber-security-predictions-2017

Lemos, Rob. 2016. 2016 Emerging Cyber Threats Report. *iisp.gatech.edu.* [Online] [Citace: 30. 08. 2017] http://www.iisp.gatech.edu/2016-emerging-cyber-threats-report

Livingstone, Sonia a Haddon, Leslie. 2009. *EU Kids Online: Final Report.* London: LSE, 2009. [Online] [Citace: 29. 12. 2018] http://www.lse.ac.uk/media%40lse/research/EUKidsOnline/EU%20Kids%20I%20%282006-9%29/EU%20Kids%20Online%20I%20Reports/EUKidsOnlineFinalReport.pdf. ISBN 978-0-85328-355-3

Livingstone, Sonia, a další. 2011. Risks and safety on the internet. The perspective of European children. Full findings and policy implications from the EU Kids Online their parents in 25 countries. *EU Kids Online.* 2011. [Online] [Citace: 29. 12. 2018] http://eprints.lse.ac.uk/33731/1/Risks%20and%20safety%20on%20the%20internet%28lsero%29.pdf

Livingstone, Sonia, Haddon, Leslie et al. 2016. EU Kids Online. *http://www.lse.ac.uk.* [Online] The London School of Economics and Political Science, 2016. [Online] [Citace: 29. 12. 2018] http://www.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx

Livingstone, Sonia, Ólaffson, Kjartan a Staksrud, Elisabeth. 2010. Social networking, age and privacy. *EU Kids Online.* 2010. [Online] [Citace: 29. 12. 2018] http://eprints.lse.ac.uk/35849/1/Social%20networking%2C%20age%20and%20privacy%20%28LSERO.pdf

Malek, Marta. 2017. 2017 cybercrime trends. *future-processing.com.* [Online] [Citace: 30. 08. 2017] https://www.future-processing.com/blog/2017-cybercrime-trends/

Marinos, Louis, Belmonte, Adrian, Rekleitis, Evangelos. 2016. ENISA Threat Landscape 2015. *enisa.europa.eu.* [Online] [Citace: 30. 08. 2017] https://www.enisa.europa.eu/publications/etl2015

Masarykova univerzita. 2016. Výzkum: Náruživé hraní online počítačových her není závislost. *muni.cz.* [Online] [Citace: 24. 08. 2018] https://www.muni.cz/pro-media/archiv-tiskovych-zprav/65027344

McAfee. 2015. 2016 Threats Predictions. *McAfee.com.* [Online] [Citace: 30. 08. 2017] http://www.mcafee.com/sg/resources/reports/rp-threats-predictions-2016.pdf

McAfee Labs. 2017. 2018 Threats Predictions. *mcafee.com.* [Online] [Citace: 04. 09. 2018] https://www.mcafee.com/enterprise/en-us/assets/infographics/infographic-threats-predictions-2018.pdf

Ministerstvo spravedlnosti ČR. infoData. Statistika a výkaznictví. *cslav.justice.cz.* [Online] [Citace: 18. 01. 2019] https://cslav.justice.cz/InfoData/uvod.html

Ministerstvo vnitra ČR. Extremismus. *mvcr.cz/.* [Online] [Citace: 01. 09. 2018] http://www.mvcr.cz/clanek/ctvrtletni-zpravy-o-extremismu-odboru-bezpecnostni-politiky-mv.aspx

—. 2018. Projevy extremismu a předsudečné nenávisti. Souhrnná situační zpráva, 3. čtvrtletí roku 2018. [Online] [Citace: 29. 12. 2018] https://www.mvcr.cz/soubor/extremismus-souhrnna-situacni-zprava-za-3-ctvrtleti-roku-2018-pdf.aspx

—. Statistiky kriminality - dokumenty. *mvcr.cz.* [Online] [Citace: 23. 01. 2019] http://www.mvcr.cz/clanek/statistiky-kriminality-dokumenty.aspx

—. 2018. Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky v roce 2017. *mvcr.cz.* [Online] [Citace: 23. 01. 2019] https://www.mvcr.cz/soubor/zprava-o-stavu-vbavp-za-2017-1-7-pdf.aspx

—. 2017. Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území ČR v roce 2016 (ve srovnání s rokem 2015). *mvcr.cz.* [Online] [Citace: 30. 08. 2017] http://www.mvcr.cz/soubor/zprava-o-situaci-v-oblasti-vnitrni-bezpecnosti-2016-pdf.aspx

—. 2018. Projevy extremismu a předsudečné nenávisti. Souhrnná situační zpráva, 2. čtvrtletí roku 2018. [Online] [Citace: 29. 12. 2018] file:///C:/Users/KK/AppData/Local/Temp/Extremismus_-_Souhrnna_situacni_zprava_za_2_ctvrtleti_roku_2018.pdf

Nejvyšší státní zastupitelství. 2016. Zpráva o činnosti 2016. *nsz.cz.* [Online] [Citace: 30. 08. 2017] http://www.nsz.cz/index.php/cs/udaje-o-cinnosti-a-statisticke-udaje/zprava-o-innosti/1897-zprava-o-innosti-2016

—. 2018. Zpráva o činnosti 2017. *nsz.cz.* [Online] [Citace: 04. 09. 2018] http://www.nsz.cz/index.php/cs/udaje-o-cinnosti-a-statisticke-udaje/zprava-o-innosti/2095-zprava-o-innosti-2017

O'Neill, Brian a Dinh, Thuy. 2018. The Better Internet for Kids Policy Map: Implementing the European Strategy for a Better Internet for Children in European Member States. European Commission, 03. 2018. [Online] [Citace: 29. 12. 2018] https://www.betterinternetforkids.eu/documents/167024/2637346/BIK+Map+report+-+Final+-+March+2018/a858ae53-971f-4dce-829c-5a02af9287f7

Patterson, Dan. 2016. 2017 cybercrime trends: Expect a fresh wave of ransomware and IoT hacks. *techrepublic.com.* [Online] [Citace: 30. 08. 2017]

http://www.techrepublic.com/article/2017-cybercrime-trends-expect-a-fresh-wave-of-ransomware-and-iot-hacks/

Policie ČR. Kriminalita. *http://www.policie.cz.* [Online] [Citace: 30. 08. 2017] http://www.policie.cz/statistiky-kriminalita.aspx

Reid, Fergal a Harrigan, Martin. 2013. An Analysis of Anonymity in the Bitcoin System. *anonymity-in-bitcoin.blogspot.com.* [Online] [Citace: 16. 04. 2015] http://anonymity-in-bitcoin.blogspot.com/2011/07/bAnonymity-in-bitcoin.blogspot.cz/2011/07/bitcoin-is-not-anonymous.htmlitcoin-is-not-anonymous..html

risk3sixty LLC. 2015. 2016 Cyber Risk Reports Reveal the Need for Effective Risk Assessments to Better Allocate Resourses. *risk3sixty.com.* [Online] [Citace: 30. 08. 2017] http://www.risk3sixty.com/2015/12/07/2016-cyber-risk-reports-reveal-the-need-for-effective-risk-assessments-to-better-allocate-resourses/

RSA. 2018. 2018 Current State of Cybercrime. *rsa.com.* [Online] [Citace: 04. 09. 2018] https://www.rsa.com/content/dam/premium/en/white-paper/2018-current-state-of-cybercrime.pdf

—. 2015. Cybercrime 2015. An Inside Look at the Changing Threat Landscape. *emc.com.* [Online] [Citace: 30. 08. 2017] risk3sixty.com

Symantec. 2018 Internet Security Threat Report. *symantec.com.* [Online] [Citace: 04. 09. 2018] https://resource.elq.symantec.com/LP=5840?cid=70138000000rm1eAAA

—. 2017. Internet Security Threat Report. *symantec.com.* [Online] [Citace: 30. 08. 2017] https://resource.elq.symantec.com/LP=3980?cid=70138000001BjppAAC&mc=202671&ot=wp&tt=sw&inid=symc_threat-report_regular_to_leadgen_form_LP-3980_ISTR22-report-main

Trend Micro. 2017. Security Predictions for 2018. Paradigm Shifts. *trendmicro.com.* [Online] [Citace: 04. 09. 2018] https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2018

TrendLabs. 2016. The Next Tier. Trend Micro Security Predictions for 2017. *trendmicro.com.* [Online] [Citace: 30. 08. 2017] https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2017

Tsaliki, Liza, Chronaki, Despina a Ólafsson, Kjartan. 2014. Experiences with sexual content: what we know from the research so far. *EU Kids Online.* London 2014. [Online] [Citace: 04. 09. 2018] http://eprints.lse.ac.uk/60143/1/__lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_EU%20Kids%20Online_EU_Kids_Online_Sexual%20content%20report%20%202014.pdf

Univerzita Palackého v Olomouci, Pedagogická fakulta. 2015. České děti a Facebook 2015. *www.e-bezpeci.cz.* [Online] [Citace: 29. 08. 2017] https://drive.google.com/file/d/0B5sdIAT8WtLBZWVQM1FBMTU0WWs/view

Univerzita Palackého v Olomouci, Seznam.cz, Google. 2014. Výzkum rizikového chování českých dětí v prostředí internetu. *www.e-bezpeci.cz.* [Online] [Citace: 29. 08. 2017] https://www.e-bezpeci.cz/index.php/ke-stazeni/doc_download/61-vyzkum-rizikoveho-chovani-eskych-dti-v-prostedi-internetu-2014-prezentace

2.2. Vlastní publikace

Brandejsová, Jana, a další. 2012. Metodika Kybergrooming a kyberstalking. *ncbi.cz.* [Online] [Citace: 22. 01. 2019] https://www.ncbi.cz/odborna-knihovna/category/6-metodiky-ucebni-materialy.html?download=37:metodika-kybergrooming-a-kyberstalking

—. 2012. Metodika Kyberšikana. *ncbi.cz.* [Online] [Citace: 22. 01. 2019] https://www.ncbi.cz/odborna-knihovna/category/6-metodiky-ucebni-materialy.html?download=38:metodika-kybersikana

—. 2012. Metodika Nezákonný a nevhodný obsah na internetu. *ncbi.cz.* [Online] [Citace: 22. 01. 2019] https://www.ncbi.cz/odborna-knihovna/category/6-metodiky-ucebni-materialy.html?download=39:metodika-nezakonny-a-nevhodny-obsah-na-internetu

—. 2012. Metodika Výchova k bezpečnému a etickému užívání internetu. *ncbi.cz.* [Online] [Citace: 22. 01. 2019] https://www.ncbi.cz/odborna-knihovna/category/6-metodiky-ucebni-materialy.html?download=49:metodika-vychova-k-bezpecnemu-a-etickemu-uzivani-internetu

Kudrlová, Kateřina. 2017. Kybergrooming – 3 roky kriminalizace. *Právo-Bezpečnost-Informace.* 2017. http://teorieib.cz/pbi/files/334-Kudrlova.pdf

—. 2015. Kyberkriminalita a dokazování. *VIII. ročník SVOČ.* [studentská vědecká odboná činnost]. Praha: Univerzita Karlova v Praze, Právnická fakulta, 2015. druhé (dělené) místo

—. 2018. Postihování neoprávněného přístupu k počítačovému systému a nosiči informací v roce 2015. *XI. ročník SVOČ.* místo neznámé: Univerzita Karlova v Praze, Právnická fakulta, 2018

—. 2017. Přehled a trendy kyberkriminality. *http://www.mvcr.cz.* [Online] [Citace: 29. 08. 2017] http://www.mvcr.cz/soubor/trendy-kyberkriminality-iksp-docx.aspx

—. 2016. Tisková zpráva ze zasedání Republikového výboru pro prevenci kriminality. *mvcr.cz.* [Online] [Citace: 28. 08. 2018] http://www.mvcr.cz/migrace/docDetail.aspx?docid=21975345&docType=ART

—. 2016. Trendy kyberkriminality. *IX. ročník SVOČ (studentská vědecká odborná činnost).* místo neznámé: Univerzita Karlova v Praze, Právnická fakulta, 2016

Lukášová, Kateřina. 2012. Kybergrooming. *moodle.prf.cuni.cz.* [Online] [Citace: 27. 06. 2018] https://moodle.prf.cuni.cz/mod/data/view.php?d=8&rid=188

—. 2011. Význam vzdělávání v rámci sociální prevence kriminality. *moodle.prf.cuni.cz.* [Online] [Citace: 27. 06. 2018] https://moodle.prf.cuni.cz/pluginfile.php/46963/mod_data/content/213/82.pdf

2.3. Wikipedie aj.

bitcash.cz. Bitcoin. *bitcoinforum.cz.* [Online] [Citace: 16. 04. 2015] https://bitcoinforum.cz/rates/?bitcoin&s=

bitcoinwiki. Anonymity. *en.bitcoin.it.* [Online] [Citace: 16. 04. 2015] https://en.bitcoin.it/wiki/Anonymity

—. Block. *en.bitcoin.it.* [Online] [Citace: 16. 04. 2015] https://en.bitcoin.it/wiki/Block

—. Block hashing algorithm. *en.bitcoin.it.* [Online] [Citace: 16. 04. 2015] https://en.bitcoin.it/wiki/Block_hashing_algorithm

—. Block chain. *en.bitcoin.it.* [Online] [Citace: 16. 04. 2015] https://en.bitcoin.it/wiki/Block_chain

—. Weaknesses. *en.bitcoin.it.* [Online] [Citace: 16. 04. 2015] https://en.bitcoin.it/wiki/Weaknesses#Attacker_has_a_lot_of_computing_power

blockexplorer.com. blockcount. *blockexplorer.com.* [Online] [Citace: 14. 01. 2019] https://blockexplorer.com/api/status?q=getBlockCount

wikiHow. How to Change a Computer's Mac Address in Windows. *wikihow.com.* [Online] [Citace: 16. 04. 2015] https://www.wikihow.com/Change-a-Computer's-Mac-Address-in-Windows

Wikipedia. Google. *en.wikipedia.org.* [Online] [Citace: 03. 08. 2015] https://en.wikipedia.org/wiki/Google_(verb)

—. List of suicides that have been attributed to bullying. *en.wikipedia.org.* [Online] [Citace: 01. 09. 2018] https://en.wikipedia.org/wiki/List_of_suicides_that_have_been_attributed_to_bullying

—. 2017. WannaCry ransomware attack. *en.wikipedia.org.* [Online] [Citace: 30. 08. 2017] https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

—. Wikipedia. *en.wikipedia.org.* [Online] [Citace: 17. 07. 2015] https://en.wikipedia.org/wiki/Wikipedia#cite_note-2

Wikipedie. Bitcoin. *cs.wikipedia.org.* [Online] [Citace: 16. 04. 2015] https://cs.wikipedia.org/wiki/Bitcoin

—. Blog. *cs.wikipedia.org.* [Online] [Citace: 17. 07. 2015] https://cs.wikipedia.org/wiki/Blog

—. Cenzura na internetu. *cs.wikipedia.org.* [Online] [Citace: 14. 07. 2018] https://cs.wikipedia.org/wiki/Cenzura_na_internetu

—. Česká Wikipedie. *cs.wikipedia.org.* [Online] [Citace: 17. 07. 2015] https://cs.wikipedia.org/wiki/Česká_Wikipedie

—. Flow. *cs.wikipedia.org.* [Online] [Citace: 25. 08. 2018] https://cs.wikipedia.org/wiki/Flow#cite_note-Csikszentmihalyi1990-1

—. Google. *cs.wikipedia.org.* [Online] [Citace: 03. 08. 2015] https://cs.wikipedia.org/wiki/Google

—. Moodle. *cs.wikipedia.org.* [Online] [Citace: 17. 07. 2015] https://cs.wikipedia.org/wiki/Moodle

—. Průmysl 4.0. *cs.wikipedia.org.* [Online] [Citace: 21. 07. 2018] https://cs.wikipedia.org/wiki/Pr%C5%AFmysl_4.0

—. WhatsApp. *cs.wikipedia.org.* [Online] [Citace: 08. 03. 2018] https://cs.wikipedia.org/wiki/WhatsApp

Wikisofia. Sociální komunikace. *wikisofia.cz.* [Online] [Citace: 03. 08. 2015] https://wikisofia.cz/index.php/Sociální_komunikace

2.4. Ostatní

2013. Autorský zákon - principy nakládání s daty v rámci e-Gov. Koncepční dokument pro oblast řízení a koordinaci e-Gov. *asociacekraju.cz.* [Online] [Citace: 14. 08. 2018] http://www.asociacekraju.cz/files/files/dokumenty/PROJEKTY/egov/AKCR_IeGOV_A3-Koncepce_autorsky_zakon_2013_8_28_FINAL.pdf

Balucha, Martin. 2017. YouTube hledá tisíce kontrolorů. Budou vyhledávat a blokovat nevhodná videa. *irozhlas.cz.* [Online] [Citace: 02. 09. 2018] https://www.irozhlas.cz/zpravy-svet/youtube-kontrolor-video_1712051415_pj

Barlow, John Perry. 1996. A Declaration of the Independence of Cyberspace. *eff.org.* [Online] [Citace: 07. 07. 2018] https://projects.eff.org/~barlow/Declaration-Final.html

Bárta, Ondřej, a další. 2018. Presentation at Cyberspace conference 2018: Ambivalence in ICT-related learning (with examples). zounek.cz. [Online] [Citace: 28. 12. 2018] http://zounek.cz/presentation-at-cyberspace-conference-2018-ambivalence-in-ict-related-learning/

BBC News. 2013. Dick Cheney: Heart implant attack was credible. *bbc.com.* [Online] [Citace: 30. 05. 2018] http://www.bbc.com/news/technology-24608435

Beal, Vangie. 2013. 5 Top Picks for Small Business Cloud-Based Accounting. *cio.com.* [Online] [Citace: 16. 04. 2015] https://www.cio.com/article/2388062/small-business/5-top-picks-for-small-business-cloud-based-accounting.html

Beran, Vojtěch. 2015. Hmotný nosič díla výtvarného umění a autorskoprávní omezení jeho vlastníka. *epravo.cz.* [Online] [Citace: 15. 08. 2018] https://www.epravo.cz/top/clanky/hmotny-nosic-dila-vytvarneho-umeni-a-autorskopravni-omezeni-jeho-vlastnika-97756.html

Bhardwaj, Julian. 2012. Tor and the Deepnet: What price does society pay for anonymity? *nakedsecurity.sophos.com.* [Online] [Citace: 03. 07. 2018] Nakedsecurity.sophos.com/2012/12/06/tor-deepnet-anonymity

Blue Maestro. 2015. New Year and New Products. *the-reseller-network.com.* [Online] [Citace: 17. 07. 2015] https://www.the-reseller-network.com/article/830/new-year-and-new-products/

Bořánek, Roman. 2014. Je Bitcoin anonymní? Všechny transakce je možné dohledat. *root.cz.* [Online] [Citace: 30. 08. 2017] https://www.root.cz/clanky/je-bitcoin-anonymni-vsechny-transakce-je-mozne-dohledat

Broniatowski, David A., a další. 2018. Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate. *ajph.aphapublications.org.* [Online] [Citace: 24. 08. 2018] https://ajph.aphapublications.org/doi/10.2105/AJPH.2018.304567

Brown a R., Andy. 2012. Suicide solutions? Or, how the emo class of 2008 were able to contest their media demonization, whereas the headbangers, burnouts or 'children of ZoSo' generation were not. *Popular Music History.* 2012, č. 1. file:///F:/konference/CKS/III%20krim%20dny%20-%202015%20-%20Hradec%20Kralove%20-%20Kyberprostor%20a%20sebeposkozovani/prispevek/podklady/suicide%20solutions%20-%20emo%20-%20media%20demonization%20-%20Brown.pdf

Burk, Dan L. 2008. Information ethics and the law of data representations. *Ethics and Information Technology.* 2008, č. 2-3. https://link.springer.com/article/10.1007/s10676-008-9161-y

Burrus, Daniel. 2014. The Internet of Things Is Far Bigger Than Anyone Realizes. *wired.com.* [Online] [Citace: 16. 07. 2018] http://www.wired.com/2014/11/the-internet-of-things-bigger/

BusinessIT. 2015. Internet věcí: Nové příležitosti i hrozby. *businessit.cz.* [Online] [Citace: 27. 08. 2018] http://www.businessit.cz/cz/internet-veci-nove-prilezitosti-i-hrozby.php

Council of Europe. No Hate Speech Youth Campaign. *coe.int.* [Online] [Citace: 01. 09. 2018] https://www.coe.int/en/web/no-hate-campaign

CZ.NIC. Aktuálně z bezpečnosti (RSS). *csirt.cz.* [Online] [Citace: 23. 01. 2019] https://www.csirt.cz/news/security/

—. 2012. Jak na internet. *jaknainternet.cz.* [Online] [Citace: 02. 09. 2018] https://www.jaknainternet.cz/

cz.nic. mojeID. *mojeid.cz.* [Online] [Citace: 19. 08. 2018] https://www.mojeid.cz/

CZ.NIC. Turris. *turris.cz.* [Online] [Citace: 16. 04. 2015] www.turris.cz/cs/

CzechPOINT. Co je Czech POINT? *czechpoint.cz.* [Online] [Citace: 21. 07. 2018] http://www.czechpoint.cz/public/statistiky-a-informace/co-je-czech-point/

Čermák, Miloš. 2015. Experiment: Co udělá s člověkem týden bez Facebooku? Přestane se stresovat a je šťastnější. *magazin.aktualne.cz.* [Online] [Citace: 28. 08. 2018] https://magazin.aktualne.cz/tyden-bez-facebooku-mene-stresu-a-vice-socialni-interakce/r~2e5e7c28886411e58f1e002590604f2e/

Čížek, Jakub. 2013. Korejci dokončili vyšetřování. Březnový kyberútok vedla KLDR. *zive.cz.* [Online] [Citace: 27. 08. 2018] https://www.zive.cz/bleskovky/korejci-dokoncili-vysetrovani-breznovy-kyberutok-vedla-kldr/sc-4-a-168392/default.aspx#utm_medium=selfpromo&utm_source=zive&utm_campaign=RSSfeed

—. 2012. Roboti-novináři už roky sepisují články. Třeba na Forbesu. *zive.cz.* [Online] [Citace: 28. 08. 2018] https://www.zive.cz/clanky/roboti-novinari-uz-roky-sepisuji-clanky-treba-na-forbesu/sc-3-a-162933/default.aspx#utm_medium=selfpromo&utm_source=zive&utm_campaign=copylink

ČT24. 2009. Soud poslal muže za zneužívání chlapců na osm let do vězení. *ct24.ceskatelevize.cz.* [Online] [Citace: 07. 01. 2012] https://ct24.ceskatelevize.cz/domaci/1422179-soud-poslal-muze-za-zneuzivani-chlapcu-na-osm-let-do-vezeni

ČTK. 2019. Facebook zavřel účty skrytě napojené na Rusko. *tyden.cz.* [Online] [Citace: 17. 01. 2019] https://www.tyden.cz/rubriky/zahranici/rusko-a-okoli/facebook-zavrel-manipulativni-ucty-skryte-napojene-na-rusko_510518.html

—. 2013. Hackeři vyplašili svět zprávou o explozích v Bílém domě a zraněném Obamovi. *novinky.cz.* [Online] [Citace: 27. 08. 2018] https://www.novinky.cz/zahranicni/amerika/299992-hackeri-vyplasili-svet-zpravou-o-explozich-v-bilem-dome-a-zranenem-obamovi.html

—. 2017. Policie varuje: Pozor na hru Modrá velryba, vyžádala si životy. *e15.cz.* [Online] [Citace: 25. 08. 2018] https://www.e15.cz/domaci/policie-varuje-pozor-na-hru-modra-velryba-vyzadala-si-zivoty-1331245

—. 2009. Zneužil 21 chlapců. Soud mu vyměřil osmiletý trest. *tyden.cz.* [Online] [Citace: 07. 01. 2012] https://www.tyden.cz/rubriky/domaci/cerna-kronika/zneuzil-21-chlapcu-soud-mu-vymeril-osmilety-trest_103925.html?showTab=nejnovejsi

—. 2009. Zneužil chlapce na vrátnici, dostal osm let. *zpravy.aktualne.cz.* [Online] [Citace: 07. 01. 2012] https://zpravy.aktualne.cz/domaci/zneuzil-chlapce-na-vratnici-dostal-osm-let/r~i:article:628861/

DeepWebSitesLinks. Deep Web Links | Deep Web Sites | The Deepweb 2019. *deepwebsiteslinks.com.* [Online] [Citace: 29. 01. 2019] https://www.deepwebsiteslinks.com/#tableofcontent

2009. Deviant Hovorka se dočkal za zneužití dvaceti chlapců mírnějšího trestu. *zpravy.idnes.cz.* [Online] [Citace: 31. 08. 2018] https://zpravy.idnes.cz/odvolaci-soud-rozhodne-o-trestu-za-zneuziti-jednadvaceti-chlapcu-p9q-/krimi.aspx?c=A090526_073207_krimi_cen

digiczech. 2016. Společnost 4.0 a Aliance Společnost 4.0. *digiczech.eu.* [Online] [Citace: 21. 07. 2018] https://digiczech.eu/pilire-spolecnosti-4-0/spolecnost-4-0/#spolecnost40-cil-04

2003. Digital Divide. *wikipedia.cz.* [Online] [Citace: 13. 07. 2015] https://en.wikipedia.org/wiki/Digital_divide

Dočekal, Daniel. 2015. Facebook už umí rozpoznávat obličeje stejně dobře jako lidé. *lupa.cz.* [Online] [Citace: 29. 08. 2018] https://www.lupa.cz/clanky/facebook-uz-umi-rozpoznavat-obliceje-stejne-dobre-jako-lide/

Dohnal, Radomír. 2017. Hráči on-line her nejsou závislí, ale vytěsňují tak problémy, říká věda. *xman.idnes.cz.* [Online] [Citace: 24. 08. 2018] https://xman.idnes.cz/on-li-hry-pareni-zavislost-problemy-db9-/xman-styl.aspx?c=A171102_161440_xman-styl_fro

E-Bezpeci. 2009. Případy kybergroomingu I. *e-bezpeci.cz.* [Online] [Citace: 07. 01. 2012] http://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/kybergrooming/33-112

EC3. IOCTA 2017. *europol.europa.eu.* [Online] [Citace: 04. 09. 2018] https://www.europol.europa.eu/iocta/2017/EXECUTIVE_SUMMARY.html

—. 2017. Wannacry Ransomware. *europol.europa.eu.* [Online] [Citace: 30. 08. 2017] https://www.europol.europa.eu/wannacry-ransomware

Eichler, Pavel a Vedral, Jan. 2006. Neonacisté v Česku snadno koupí „to pravé“ oblečení. *zpravy.idnes.cz.* [Online] [Citace: 29. 10. 2018] https://zpravy.idnes.cz/neonaciste-v-cesku-snadno-koupi-to-prave-obleceni-f7q-/domaci.aspx?c=A061006_150831_krimi_pei

ESET. 2017. Dvojklik. *dvojklik.cz.* [Online] [Citace: 30. 08. 2017] https://www.eset.com/cz/?__utma=127111570.985830894.1498056971.1498568301.1504089041.4&__utmb=127111570.3.10.1504089041&__utmc=127111570&__utmx=-&__utmz=127111570.1498568301.3.3.utmcsr=google%7cutmccn=(organic)%7cutmcmd=organic%7cutmctr=(not%2520provided)

Europol. 2014. Global action against dark markets on Tor network. *europol.europa.eu.* [Online] [Citace: 14. 07. 2018] https://www.europol.europa.eu/newsroom/news/global-action-against-dark-markets-tor-network

—. 2017. Online sexual coercion and extortion is a crime. *europol.europa.eu.* [Online] [Citace: 02. 10. 2017] https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/online-sexual-coercion-and-extortion-crime

Evropa 2045. Chci řídit svou Evropu! *evropa2045.cz.* [Online] [Citace: 21. 07. 2015] http://www.evropa2045.cz/student.php

Facebook. 2018. Podmínky používání. *facebook.com.* [Online] [Citace: 05. 08. 2018] https://www.facebook.com/legal/terms

Feder, Barnaby J. 2008. A Heart Device Is Found Vulnerable to Hacker Attacks. *nytimes.com.* [Online] [Citace: 30. 05. 2018] http://www.nytimes.com/2008/03/12/business/12heart-web.html?_r=0

Fidrmuc, Jaroslav. 2017. Vzdělávání 4.0. *pocitacveskole.cz.* [Online] [Citace: 27. 07. 2018] https://www.pocitacveskole.cz/system/files/soubory/fidrmuc-2017.pdf

Fillner, Karel. 2014. První obousměrný bitcoin bankomat v ČR – ohlédnutí. *btctip.cz.* [Online] [Citace: 16. 04. 2015] https://btctip.cz/prvni-obousmerny-bitcoin-bankomat-v-cr-male-ohlednuti/

Fox-Brewster, Thomas. 2017. An NSA Cyber Weapon Might Be Behind A Massive Global Ransomware Outbreak. *forbes.com.* [Online] [Citace: 30. 08. 2017] https://www.forbes.com/sites/thomasbrewster/2017/05/12/nsa-exploit-used-by-wannacry-ransomware-in-global-explosion/#2668c260e599

Franklin, Curt. 2000. How Routers Work. *computer.howstuffworks.com.* [Online] [Citace: 27. 06. 2018] https://computer.howstuffworks.com/router.htm

Freeman, Mandy. 2018. ‘I Googled how to kill myself’. *health24.com.* [Online] [Citace: 24. 08. 2018] https://www.health24.com/Medical/Depression/Real-life-story/i-googled-how-to-kill-myself-20171120

GAMIFIQUE.cz. 2017. Česko má první profesionální hráče počítačových her. *gamifique.eurozpravy.cz.* [Online] [Citace: 20. 08. 2018] https://gamifique.eurozpravy.cz/esport/2470-cesko-ma-prvni-profesionalni-hrace-pocitacovych-her#

Gargasz, Zbigniew. 2009. How Internet works – DNS. *gargasz.info.* [Online] [Citace: 16. 04. 2015] http://www.gargasz.info/how-internet-works-dns/

Gibbs, Dana. 2012. Verbální a neverbální komunikace. *vyplnto.cz.* [Online] [Citace: 03. 08. 2015] https://www.vyplnto.cz/realizovane-pruzkumy/verbalni-a-neverbalni-komuni/

Google. Anonymní prohlížení. *support.google.com.* [Online] [Citace: 21. 07. 2018] https://support.google.com/chrome/answer/95464?hl=cs&co=GENIE.Platform%3DDesktop

—. Bezpečnost dětí na YouTube. *google.com.* [Online] [Citace: 22. 01. 2019] https://support.google.com/youtube/answer/2801999?hl=cs

—. Základní informace o sankcích za porušení pokynů pro komunitu. *google.com.* [Online] [Citace: 22. 01. 2019] https://support.google.com/youtube/answer/2802032?hl=cs

Gray, Peter. 2014. Čím je hraní počítačových her pro děti prospěšné. *svobodauceni.cz.* [Online] [Citace: 28. 08. 2018] https://www.svobodauceni.cz/clanek/hrani-pocitacovych-her/

Griffith, Eric. 2016. What Is Cloud Computing? *pcmag.com.* [Online] [Citace: 27. 06. 2018] https://www.pcmag.com/article2/0,2817,2372163,00.asp

Haupt, Michael. 2018. Co-Creating Society 4.0 - Our Only Hope for a Bright New Future. *medium.com.* [Online] [Citace: 21. 07. 2018] https://medium.com/society4/society4-f078444b5306

Hewlett Packard. 2018. 2018 Cybersecurity Guide: Hackers and defenders harness design and machine learning. *hp.com.* [Online] [Citace: 04. 09. 2018] http://www8.hp.com/h20195/v2/GetPDF.aspx/4AA7-2519ENW.pdf

Hidden Wiki. Hidden Wiki. Tor .onion urls directories. *thehiddenwiki.org.* [Online] [Citace: 14. 04. 2016] http://thehiddenwiki.org/

Hoax.cz. Recyklované mléko. *hoax.cz.* [Online] [Citace: 23. 01. 2019] http://hoax.cz/hoax/recyklovane-mleko/

Hogan, Michael. 2015. Facebook and the 'Fear of Missing Out' (FoMO). *psychologytoday.com.* [Online] [Citace: 24. 08. 2018] https://www.psychologytoday.com/intl/blog/in-one-lifespan/201510/facebook-and-the-fear-missing-out-fomo

Holušová, Alina. 2017. 'Sebevražedná hra' Modrá velryba je fake aneb Co nám vraždí naše děti? *zpravy.tiscali.cz.* [Online] [Citace: 25. 08. 2018] https://zpravy.tiscali.cz/sebevrazedna-hra-modra-velryba-je-fake-aneb-co-nam-vrazdi-nase-deti-296021

Honzák, Radkin. 2009. Problematika sebevražednosti v ordinaci praktického lékaře. *radkin.estranky.cz.* [Online] [Citace: 25. 08. 2018] http://www.radkin.estranky.cz/clanky/sebevrazedne-riziko.html

Horká linka. Odstranění obsahu z internetu. *ohlaste.horkalinkaczi.cz.* [Online] [Citace: 03. 09. 2018] http://ohlaste.horkalinkaczi.cz/

Houbaření - Atlas hub. Muchomůrka zelená. *houbareni.cz.* [Online] [Citace: 17. 07. 2015] http://www.houbareni.cz/houba.php?id=46

Hubbard, John. 1999. Indexing the Internet. *tk421.net.* [Online] [Citace: 03. 07. 2018] Www.tk421.net/essays/babel.html

chatib. chatib. *chatib.us.* [Online] [Citace: 20. 07. 2015] http://www.chatib.com

Chen, Caroline a Womack, Brian. 2015. Google Reveals Health-Tracking Wristband. *bloomberg.com.* [Online] [Citace: 17. 07. 2015] http://www.bloomberg.com/news/articles/2015-06-23/google-developing-health-tracking-wristband-for-health-research

Chlad, Radim. 2000. Historie Internetu v České republice. *fi.muni.cz.* [Online] [Citace: 03. 07. 2018] www.fi.muni.cz/usr/jkucera/pv109/2000/xchlad.htm

Choney, Suzanne. 2013. No Googling, says Google — unless you really mean it. *nbcnews.com.* [Online] [Citace: 03. 08. 2015] http://www.nbcnews.com/technology/no-googling-says-google-unless-you-really-mean-it-1C9078566

Chování.eu. Netiketa. *chovani.eu.* [Online] [Citace: 19. 07. 2018] http://www.chovani.eu/netiketa/c56

Chroust, Martin. 2013. LG: bezdrátové ovládání spotřebičů mobilem [CES] Více na: https://www.mobilmania.cz/clanky/lg-bezdratove-ovladani-spotrebicu-mobilem-ces/sc-3-a-1322575/. *mobilmania.cz.* [Online] [Citace: 03. 07. 2018] http://www.mobilmania.cz/clanky/lg-bezdratove-ovladani-spotrebicu-mobilem-ces/sc-3-a-1322575/

IBM. IBM X-Force Threat Intelligence Index 2018. *ibm.com.* [Online] [Citace: 04. 09. 2018] https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=77014377USEN

IETF. 1995. Netiquette Guidelines. *rfc-editor.org.* [Online] [Citace: 19. 07. 2018] https://www.rfc-editor.org/rfc/rfc1855.txt

Imperva. 2017. Advanced Persistent Threat (APT). *incapsula.com.* [Online] [Citace: 23. 01. 2019] https://www.incapsula.com/web-application-security/apt-advanced-persistent-threat.html

Inhope. At a Glance. *inhope.org.* [Online] [Citace: 03. 09. 2018] http://inhope.org/gns/who-we-are/at-a-glance.aspx

InspectLife. Asistenční dohledová služba. *dohled.inspectlife.cz.* [Online] [Citace: 16. 07. 2015] http://www.dohled.inspectlife.cz/cs/podrobne-informace/senior-a-rodina/asistence-na-miru#oddil2

Internet Archive. Wayback Machine. *archive.org.* [Online] [Citace: 02. 09. 2018] https://archive.org/

Internet World Stats. The Digital Divide, ICT and Broadband Internet. *internetworldstats.com.* [Online] [Citace: 13. 07. 2015] https://www.internetworldstats.com/links10.htm

2014. Internetem se šíří videa z veřejných poprav v Íranu. *echo24.cz.* [Online] [Citace: 01. 09. 2018] https://echo24.cz/a/wuH8v/internetem-se-siri-videa-z-verejnych-poprav-v-iranu

2015. IoT v roce 2020: 25 miliard věcí připojených k internetu. *businessit.cz.* [Online] [Citace: 17. 07. 2015] http://www.businessit.cz/cz/iot-v-roce-2020-25-miliard-veci-pripojenych-k-internetu.php

ip-adress.com. IP Tracing and IP Tracking. *ipaddress.ip-adress.com.* [Online] [Citace: 16. 04. 2015] https://ipaddress.ip-adress.com/

iSenior. 2010. Zkoušíme nouzové tlačítko. *isenior.cz.* [Online] [Citace: 16. 07. 2015] http://www.isenior.cz/zdravi/zkousime-nouzove-tlacitko

ISFE. Videogames in Europe: 2012 Consumer Study. *isfe.eu.* [Online] [Citace: 10. 09. 2015] https://www.isfe.eu/videogames-europe-2012-consumer-study

—. 2012. Videogames in Europe: 2012 Consumer Study. Czech Republic. *isfe.eu.* [Online] [Citace: 10. 09. 2015] https://www.isfe.eu/sites/isfe.eu/files/attachments/czech_republic_-_isfe_consumer_study.pdf

Jarolímková, Markéta. 2014. Proč si ubližujeme. *psychologie.cz.* [Online] [Citace: 25. 08. 2018] https://psychologie.cz/proc-si-ublizujeme/

Jílková, Michaela. 2007. Povolme animované dětské porno, říká sexuolog Weiss. *zpravy.idnes.cz.* [Online] [Citace: 30. 08. 2018] https://zpravy.idnes.cz/povolme-animovane-detske-porno-rika-sexuolog-weiss-fhs-/domaci.aspx?c=A071009_115203_domaci_nad

Kabátová, Šárka. 2017. Jako mluvčí má hovořit za prezidenta. Ovčáček si ale na sítích rád hraje na politika. *lidovky.cz.* [Online] [Citace: 27. 08. 2018] https://www.lidovky.cz/ma-tlumocit-prezidentovy-nazory-misto-toho-ovcacek-bloguje-a-hraje-si-na-politika-gi8-/zpravy-domov.aspx?c=A170512_145003_ln_domov_sk

Kasík, Pavel. 2013. Peníze, které vám vláda neukradne. Za bitcoiny koupíte heroin i dolary. *technet.idnes.cz.* [Online] [Citace: 03. 07. 2018] Technet.idnes.cz/bitcoin-virtualni-mena-074-/sw_internet.aspx?c=A130408_111554_sw_internet_pka

Kluska, Vladislav. 2017. Chcete spáchat sebevraždu? Facebook se vám v tom bude snažit zabránit Více na: https://www.zive.cz/clanky/chcete-spachat-sebevrazdu-facebook-se-vam-v-tom-bude-snazit-zabranit/sc-3-a-190690/default.aspx. *zive.cz.* [Online] [Citace: 02. 09. 2018] https://www.zive.cz/clanky/chcete-spachat-sebevrazdu-facebook-se-vam-v-tom-bude-snazit-zabranit/sc-3-a-190690/default.aspx

Kolář, Michal. 1999. Můžu si taky kopnout? *sikana.org.* [Online] [Citace: 01. 09. 2018] http://www.sikana.org/clanky_soubory/M_kopnout.html

Kopecký, Kamil. 2009. Co je sexting. *e-bezpeci.cz.* [Online] [Citace: 26. 01. 2019] https://www.e-bezpeci.cz/index.php/temata/sexting/137-154

—. 2009. Kybergrooming aneb Kdo loví v chatu. *ceskaskola.cz.* [Online] [Citace: 11. 02. 2012] http://www.ceskaskola.cz/2009/05/kamil-kopecky-kybergrooming-aneb-kdo.html

Kovar, Karel. 2012. Darknet: temná strana internetu. *chip.cz.* [Online] [Citace: 03. 07. 2018] https://www.chip.cz/casopis-chip/earchiv/vydani/r-2012/darknet/

KOVY. 2018. Druhé kolo. *youtu.be.* [Online] [Citace: 17. 07. 2018] https://youtu.be/vQwp7CC9mRM

Kranenburg, Rob. How to negotiate IoT into a political reality. *theinternetofthings.eu.* [Online] [Citace: 17. 07. 2015] https://www.theinternetofthings.eu/sites/default/files/[user-name]/Cybernetics%20%E2%80%93%20IoT_0.pdf

Krill, Paul. 2010. Cloud computing mění přístup k vývoji aplikací. *computerworld.cz.* [Online] [Citace: 27. 06. 2018] https://computerworld.cz/vyvoj/cloud-computing-meni-pristup-k-vyvoji-aplikaci-6560

Křešnička, Jakub. 2015. Až si lednička sama objedná nákup. *tyden.cz.* [Online] [Citace: 17. 07. 2015] http://www.tyden.cz/rubriky/byznys/az-si-lednicka-sama-objedna-nakup_339302.html#.Vakff9BmwUw

Kubátová, Eliška. 2018. Elektronické volby jsou v Česku hudbou budoucnosti. Proti hraje politika i riziko hackerských útoků. *info.cz.* [Online] [Citace: 29. 07. 2018] https://www.info.cz/volby/prezidentske-volby-2018/elektronicke-volby-jsou-v-cesku-hudbou-budoucnosti-proti-hraje-politika-i-riziko-hackerskych-utoku-22647.html

Kučera, Josef. 2009. Meziplanetární internet se stává skutečností. Pojede přes ISS. *technet.idnes.cz.* [Online] [Citace: 03. 07. 2018] technet.idnes.cz/meziplanetarni-internet-se-stava-skutecnosti-pojede-pres-iss-p69-/tec_vesmir.aspx?c=A090713_113417_tec_vesmir_vse

Loukota, Ladislav. 2011. Závislost na hrách je psychologická porucha. Názory i léčebné metody se ale různí. *bonusweb.idnes.cz.* [Online] [Citace: 24. 08. 2018] https://bonusweb.idnes.cz/zavislost-na-hrach-je-psychologicka-porucha-nazory-i-lecebne-metody-se-ale-ruzni-gfx-/Magazin.aspx?c=A110213_061630_bw-magazin_lou

Ludwin, Adam. 2015. How Anonymous is Bitcoin? *coincenter.org.* [Online] [Citace: 28. 08. 2018] https://coincenter.org/entry/how-anonymous-is-bitcoin

McAfee, John. 2015. John McAfee: Cyberwar is here, and China is the enemy. *digitaltrends.com.* [Online] [Citace: 30. 08. 2017] https://www.digitaltrends.com/opinion/john-mcafee-art-cyber-warfare/

McDonagh, Janet E. 2018. The age of adolescence…and young adulthood. *thelancet.com.* [Online] [Citace: 17. 07. 2018] https://www.thelancet.com/journals/lanchi/article/PIIS2352-4642(18)30079-8/abstract

McNeil, Donald G. Jr. 2018. Russian Trolls Used Vaccine Debate to Sow Discord, Study Finds. *nytimes.com.* [Online] [Citace: 24. 08. 2018] https://www.nytimes.com/2018/08/23/health/russian-trolls-vaccines.html

Mediagram. Vývoj médií od knihtisku po internet. *http://mediagram.cz.* [Online] [Citace: 12. 07. 2018] http://mediagram.cz/dejepis/vyvoj-medii-od-knihtisku-po-internet

Micajir. 2012. Sebenaplňující se proroctví. *oeconomia.info.* [Online] [Citace: 16. 08. 2015] http://oeconomia.info/cs/obsah/sebenaplnujici-se-proroctvi

Ministerstvo školství, mládeže a tělovýchovy ČR. Strategie digitálního vzdělávání do roku 2020. *msmt.cz.* [Online] [Citace: 27. 07. 2018] http://www.msmt.cz/vzdelavani/skolstvi-v-cr/strategie-digitalniho-vzdelavani-do-roku-2020

—. 2013. Strategie primární prevence 2013-2018. *msmt.cz.* [Online] [Citace: 02. 09. 2018] http://www.msmt.cz/file/28077

—. 2014. SWOT: Strategie digitálního vzdělávání do roku 2020 (MŠMT). *prezi.com.* [Online] [Citace: 27. 07. 2018] https://prezi.com/tc266f1j82kk/swot-strategie-digitalniho-vzdelavani-do-roku-2020-msmt/

Ministerstvo vnitra ČR. 2010. Czech POINT. *mvcr.cz.* [Online] [Citace: 21. 07. 2018] http://www.mvcr.cz/clanek/dokumenty-ouvs-czech-point.aspx

—. Kybernetická kriminalita. *prevencekriminality.cz.* [Online] [Citace: 23. 01. 2019] http://www.prevencekriminality.cz/kyberkriminalita-testovaci-provoz/prevence-kyberkriminality/

moodle. About Moodle. *docs.moodle.org.* [Online] [Citace: 17. 07. 2015] https://docs.moodle.org/29/en/About_Moodle

MŠMT. Metodické dokumenty (doporučení a pokyny). *msmt.cz.* [Online] [Citace: 31. 08. 2018] http://www.msmt.cz/vzdelavani/socialni-programy/metodicke-dokumenty-doporuceni-a-pokyny

Musilová, Anna. 2018. Dospělí až v 25 letech. Ve světě neomezených možností se mladí hledají déle. *zpravy.idnes.cz.* [Online] [Citace: 17. 07. 2018] https://zpravy.idnes.cz/adolescence-the-lancet-vynorujici-se-dospelost-martin-buchtik-lucie-kvaskova-adulting-studenti-iek-/domaci.aspx?c=A180407_220215_domaci_amu

2014. Na internetu nabízel kočárky, důvěřivé maminky připravil o dvě stě tisíc. *praha.idnes.c.* [Online] [Citace: 19. 07. 2018] http://praha.idnes.cz/podvodnik-si-nechal-posilat-penize-zbozi-uz-nedodal-fyc-/praha-zpravy.aspx?c=A140210_101600_praha-zpravy_bur#utm_source=rss&utm_medium=feed&utm_campaign=zpravodaj&utm_content=main

Národní centrum bezpečnějšího internetu. Projekt Škola bezpečně online. *ncbi.cz.* [Online] [Citace: 22. 01. 2019] https://www.ncbi.cz/projekty/ukoncene-projekty/op-vk/opvk-skola-bezpecne-online.html

Národní strategie elektronického zdravotnictví. Vize. *nsez.cz.* [Online] [Citace: 18. 01. 2019] http://www.nsez.cz/dokumenty/vize_12546_31.html

Národní úřad pro kybernetickou a informační bezpečnost. Hrozby. *www.govcert.cz.* [Online] [Citace: 23. 01. 2019] https://www.govcert.cz/cs/informacni-servis/hrozby/

narrative science. How the future gets written. *narrativescience.com.* [Online] [Citace: 10. 09. 2015] https://narrativescience.com/#home

NCBI. Proti nenávisti online. Žít, učit se a jednat pro lidská práva. *protinenavisti.saferinternet.c.* [Online] [Citace: 01. 09. 2018] https://protinenavisti.saferinternet.cz/

Nebuď oběť. Kybergrooming. *nebudobet.cz.* [Online] [Citace: 07. 01. 2012] http://nebudobet.cz/?cat=kybergrooming

Němec, Libor a Tornová, Jarmila. 2018. K právní regulaci kryptoměn, díl I. *Právní rádce.* [Online] [Citace: 29. 12. 2018] http://www.glatzova.com/data/attachments/K_pravni_regulaci_kryptomen_dil_1.pdf

—. 2018. K právní regulaci kryptoměn, díl II. *Právní rádce.* [Online] [Citace: 29. 12. 2018] http://www.glatzova.com/data/attachments/K_pravni_regulaci_kryptomen_dil_2.pdf

Nováková, Lucie. 2017. Senát schválil zákon o elektronické identifikaci. *mvcr.cz.* [Online] [Citace: 29. 07. 2018] http://www.mvcr.cz/clanek/senat-schvalil-zakon-o-elektronicke-identifikaci.aspx

Novinky. 2014. Japonsko kvůli územním nárokům přepisuje učebnice. *novinky.cz.* [Online] [Citace: 14. 07. 2018] https://www.novinky.cz/zahranicni/svet/325815-japonsko-kvuli-uzemnim-narokum-prepisuje-ucebnice.html

Novotný, Jan. 2015. Chytrý dudlík komunikuje s mobilem. *palmserver.cz.* [Online] [Citace: 17. 07. 2015] http://www.palmserver.cz/modules.php?name=News&file=article&sid=14201

NÚKIB. 2018. Software i hardware společností Huawei a ZTE je bezpečnostní hrozbou . *govcert.cz.* [Online] [Citace: 15. 01. 2019] https://www.govcert.cz/cs/informacni-servis/hrozby/2680-software-i-hardware-spolecnosti-huawei-a-zte-je-bezpecnostni-hrozbou/

—. Strategie / Akční plán. *govcert.cz.* [Online] [Citace: 13. 01. 201] https://www.govcert.cz/cs/informacni-servis/strategie-akcni-plan/

Nývlt, Václac. 2008. Jazyk jen pro vyvolené: zkratky v internetových chatech a diskusích. *technet.idnes.cz.* [Online] [Citace: 19. 07. 2018] http://technet.idnes.cz/jazyk-jen-pro-vyvolene-zkratky-v-internetovych-chatech-a-diskusich-1ph-/sw_internet.aspx?c=A080302_102951_sw_internet_NYV

officialpsy. 2012. PSY - GANGNAM STYLE (강남스타일) M/V. *youtube.com.* [Online] [Citace: 30. 05. 2018] https://www.youtube.com/watch?v=9bZkp7q19f0

Othman, Dlshad. 2013. Bypassing censorship by using obfsproxy and openVPN , SSH Tunnel. *dlshad.net.* [Online] [Citace: 14. 07. 2018] https://dlshad.net/bypassing-censorship-by-using-obfsproxy-and-openvpn-ssh-tunnel/

Oxford Dictionaries. FOMO. *en.oxforddictionaries.com.* [Online] [Citace: 24. 08. 2018] https://en.oxforddictionaries.com/definition/fomo

Paton, Graeme. 2014. Infants 'unable to use toy building blocks' due to iPad addiction. *telegraph.co.uk.* [Online] [Citace: 28. 08. 2018] https://www.telegraph.co.uk/education/educationnews/10767878/Infants-unable-to-use-toy-building-blocks-due-to-iPad-addiction.html

PCWorld. 2009. Sdílení souborů na Internetu a sítě P2P - základní technologický přehled. *http://pcworld.cz.* [Online] [Citace: 16. 04. 2015] http://pcworld.cz/internet/sdileni-souboru-na-internetu-a-site-p2p-zakladni-technologicky-prehled-8350

Pecina, Tomáš. iuridictum. *iuridictum.pecina.cz.* [Online] [Citace: 16. 08. 2016] http://iuridictum.pecina.cz/w/Hlavní_strana

Peterka, Jiří. 1996. Filosofie TCP/IP. *earchiv.cz.* [Online] [Citace: 27. 06. 2018] http://www.earchiv.cz/a95/a511c502.php3

picolsigns. 2009. History of the Internet. *youtube.com.* [Online] [Citace: 19. 07. 2018] https://www.youtube.com/watch?v=9hIQjrMHTv4

Policie ČR. 2017. Modrá velryba. *policie.cz.* [Online] [Citace: 03. 09. 2018] http://www.policie.cz/clanek/modra-velryba.aspx

—. 2014. Operace „ATELIER“. *policie.cz.* [Online] [Citace: 28. 08. 2018] http://www.policie.cz/clanek/operace-atelier.aspx

—. 2018. Ukončení provozu HOTLINE. *policie.cz.* [Online] [Citace: 03. 09. 2018] http://www.policie.cz/clanek/ukonceni-provozu-hotline.aspx

—. 2017. Vyjádření k internetové „hře“. *policie.cz.* [Online] [Citace: 03. 09. 2018] http://www.policie.cz/clanek/vyjadreni-k-internetove-hre.aspx

Pospíšil, Adam. 2008. Psaním SMS škodíme mateřštině. Už přes deset let. *mobil.idnes.cz.* [Online] [Citace: 19. 07. 2018] http://mobil.idnes.cz/psanim-sms-skodime-materstine-uz-pres-deset-let-ftd-/mob_tech.aspx?c=A080325_072738_mob_tech_apo

Pospíšil, Martin. 2002. Německo: Místní působnost trestních norem a Internet. *itpravo.cz.* [Online] [Citace: 01. 09. 2018] http://www.itpravo.cz/index.shtml?x=61318

2012. Potkali se na webu. *m.aktualne.centrum.cz.* [Online] [Citace: 07. 01. 2012] http://m.aktualne.centrum.cz/article.phtml?id=628684&p=107&ap=2

Procházková, Petra. 2016. ´Lživou západní propagandu´ Wikipedie nahradí v Rusku její státem vedená mutace. *lidovky.cz.* [Online] [Citace: 21. 07. 2018] https://www.lidovky.cz/lzivou-zapadni-propagandu-wikipedie-nahradi-v-rusku-jeji-statem-vedena-mutace-1hx-/zpravy-svet.aspx?c=A160927_161031_ln_zahranici_fas)

Rada Evropy. Convention on Cybercrime. *coe.int.* [Online] [Citace: 13. 01. 2019] https://www.coe.int/en/web/conventions/full-list/-/conventions/webContent/8601684

Redakce Chip. 2013. Chytrá domácnost - spotřebiče na dálkové ovládání. *chip.cz.* [Online] [Citace: 03. 07. 2018] http://www.chip.cz/novinky/chytra-domacnost-spotrebice-na-dalkove-ovladani/

Reporters Without Borders. 2014. Reporters Without Borders and Torservers.net, partners against online surveillance and censorship. *rsf.org.* [Online] [Citace: 14. 07. 2018] https://rsf.org/en/news/reporters-without-borders-and-torserversnet-partners-against-online-surveillance-and-censorship

Rouse, Margaret. Server. *whatis.techtarget.com.* [Online] [Citace: 16. 04. 2015] https://whatis.techtarget.com/definition/server

—. TCP/IP (Transmission Control Protocol/Internet Protocol). *searchnetworking.techtarget.com.* [Online] [Citace: 16. 04. 2015] https://searchnetworking.techtarget.com/definition/TCP-IP

2017. Ruské dějiny se znovu přepisují. Nové učebnice mají posílit vztah k předkům. *ct24.ceskatelevize.cz.* [Online] [Citace: 14. 07. 2018] https://ct24.ceskatelevize.cz/svet/2143704-ruske-dejiny-se-znovu-prepisuji-nove-ucebnice-maji-posilit-vztah-k-predkum

Satrapa, Pavel. 2005. Netiketa. *lupa.cz.* [Online] [Citace: 19. 07. 2018] https://www.lupa.cz/clanky/netiketa/

Security-Portal. 2013. Seznamte se - APT. *security-portal.cz.* [Online] [Citace: 23. 01. 2019] http://www.security-portal.cz/clanky/seznamte-se-apt

Seznam.cz. Buďte na internetu v bezpečí. *seznamsebezpecne.cz.* [Online] [Citace: 31. 08. 2018] https://www.seznamsebezpecne.cz/

Shen, Wade. Memex. *darpa.mil.* [Online] [Citace: 15. 04. 2016] https://www.darpa.mil/program/memex

Shuler, Rus. 2002. How Does the Internet Work? *theshulers.com.* [Online] [Citace: 16. 04. 2015] http://www.theshulers.com/whitepapers/internet_whitepaper/

Sláma, Jan. 2016. Misha: Rozhovor s neslavnějším mladým českým youtuberem. *abicko.cz.* [Online] [Citace: 17. 07. 2018] https://www.abicko.cz/clanek/precti-si-zabava/19782/misha-rozhovor-s-neslavnejsim-mladym-ceskym-youtuberem.html

Slunečnice.cz. As Chat Room. *slunecnice.cz.* [Online] [Citace: 19. 07. 2018] https://www.slunecnice.cz/sw/as-chat-room-android/diskuse/pridat/

2011. Sociální sítě. *aktualne.cz.* [Online] [Citace: 10. 04. 2014] https://www.aktualne.cz/wiki/veda-a-technika/socialni-site/r~i:wiki:1456?redirected=1535277021

2009. Soud potrestal zneužití jednadvaceti chlapců osmi lety vězení. *zpravy.idnes.cz.* [Online] [Citace: 07. 01. 2012] https://zpravy.idnes.cz/soud-potrestal-zneuziti-jednadvaceti-chlapcu-osmi-lety-vezeni-pvv-/krimi.aspx?c=A090205_101224_krimi_jba

SPYobchod. Odposlech telefonu Android PREMIUM. *spyobchod.cz.* [Online] [Citace: 21. 07. 2018] https://www.spyobchod.cz/odposlech-telefonu-android-premium-3-mesice/

SToPonline. Ohlaste nezákonný obsah. *stoponline.cz.* [Online] [Citace: 23. 01. 2019] https://www.stoponline.cz/stoponline/

Strickland, Jonathan. How Cloud Computing Works. *computer.howstuffworks.com.* [Online] [Citace: 16. 04. 2015] https://computer.howstuffworks.com/cloud-computing/cloud-computing.htm

Suler, John. PSychology of Cyberspace. *usr.rider.edu.* [Online] [Citace: 23. 08. 2018] http://www-usr.rider.edu/~suler/psycyber/psycyber.html

2015. Syndrom FOMO aneb Proč se všichni mají lépe než já? *spektrumzdravi.cz.* [Online] [Citace: 24. 08. 2018] http://www.spektrumzdravi.cz/syndrom-fomo-aneb-proc-se-vsichni-maji-lepe-nez-ja

Škorničková, Eva. GDPR. Obecné nařízení o ochraně osobních údajů prakticky. *gdpr.cz.* [Online] [Citace: 27. 08. 2018] https://www.gdpr.cz/

TechTerms. P2P. *techterms.com.* [Online] [Citace: 16. 04. 2015] https://techterms.com/definition/p2p

torservers.net. Torservers.net. *torservers.net.* [Online] [Citace: 14. 07. 2018] https://torservers.net/

tVPN Admin. 2012. RuneScape Theft – Dutch Supreme Court Decision. *virtualpolicy.net.* [Online] [Citace: 22. 08. 2018] http://www.virtualpolicy.net/runescape-theft-dutch-supreme-court-decision.html

Tyson, Bruce. 2018. Fathoming the Depth of the Web: Dark & Deep Web Searches. *brighthub.com.* [Online] [Citace: 03. 07. 2018] www.brighthub.com/internet/google/articles/114820.aspx#imgn_0

UITS. 2018. What is a troll? *kb.iu.edu.* [Online] [Citace: 24. 08. 2018] https://kb.iu.edu/d/afhc

Ulož.to. Zásady Uživatelského obsahu. *ulozto.cz.* [Online] [Citace: 19. 07. 2018] https://ulozto.cz/podminky/zasady-uzivatelskeho-obsahu

Univerzita Karlova. 2015. Moodle UK pro výuku 1. *dl1.cuni.cz.* [Online] [Citace: 17. 07. 2015] http://dl1.cuni.cz

ÚZIS. 2018. MKN Mezinárodní statistická klasifikace nemocí a přidružených zdravotních problémů. *uzis.cz.* [Online] [Citace: 23. 08. 2018] http://www.uzis.cz/katalog/klasifikace/mkn

Valeková, Anna. 2012. Věc v právním smyslu ve vztahu k autorskému právu. *epravo.cz.* [Online] [Citace: 14. 08. 2018] https://www.epravo.cz/top/clanky/vec-v-pravnim-smyslu-ve-vztahu-kautorskemu-pravu-82470.html

Válová, Irena. 2018. Kriminalita klesla za dvacet let téměř o polovinu, objasněnost trestných činů opět stoupá. *ceska-justice.cz.* [Online] [Citace: 29. 08. 2018] http://www.ceska-justice.cz/2018/02/kriminalita-klesla-za-dvacet-let-temer-polovinu-objasnenost-trestnych-cinu-opet-stoupa/

Vejvodová, Alžběta. 2018. Facebookový profil a e-mail díky GDPR budou až od 15 let se souhlasem rodičů. *pravniradce.ihned.cz.* [Online] [Citace: 28. 08. 2018] https://pravniradce.ihned.cz/c1-66108830-facebookovy-profil-a-e-mail-diky-gdpr-budou-az-od-15-let-se-souhlasem-rodicu

Vláda České republiky. 2018. Programové prohlášení vlády. *vlada.cz.* [Online] [Citace: 21. 07. 2018] https://www.vlada.cz/cz/jednani-vlady/programove-prohlaseni/programove-prohlaseni-vlady-165960/

Webopedia. 2006. The Difference Between a Router, Switch and Hub. *webopedia.com.* [Online] [Citace: 16. 04. 2015] https://www.webopedia.com/DidYouKnow/Hardware_Software/router_switch_hub.asp

WhatIsMyIPAddress. What is a Port? *whatismyipaddress.com.* [Online] [Citace: 16. 04. 2015] https://whatismyipaddress.com/port

2017. Youtube chce léčit islamisty. Přesměruje je na videa ukazující utrpení pod vládou IS. *info.cz.* [Online] [Citace: 04. 09. 2018] https://www.info.cz/strategie/youtube-chce-lecit-islamisty-presmeruje-je-na-videa-ukazujici-utrpeni-pod-vladou-is-13399.html

Youtube. Zásady a zabezpečení. *youtube.com.* [Online] [Citace: 22. 01. 2019] https://www.youtube.com/intl/cs/yt/about/policies/#community-guidelines

Youtuberi.tv. Žebříček top 100 nejlepších českých a slovenských youtuberů. *youtuberi.tv.* [Online] [Citace: 17. 07. 2018] https://www.youtuberi.tv/top-youtuberi/

2009. Za zneužití dvaceti chlapců půjde Hovorka na osm let do vězení. *mediafax.cz.* [Online] [Citace: 18. 04. 2012] http://www.mediafax.cz/krimi/2814724-Za-zneuziti-dvaceti-chlapcu-pujde-Hovorka-na-osm-let-do-vezeni

Zlatkovský, Michal. 2016. Jak poznat falešnou zprávu? 9 tipů, jak se vyhnout hoaxům a dezinformacím. *irozhlas.cz.* [Online] [Citace: 23. 01. 2019] https://www.irozhlas.cz/zpravy-z-domova/jak-poznat-falesnou-zpravu-9-tipu-jak-se-vyhnout-hoaxum-a-dezinformacim_1611280515_

Zvol si info. Zvol si info. *zvolsi.info.* [Online] [Citace: 08. 01. 2019] http://zvolsi.info/

3. Seznam použitých právních dokumentů

Důvodová zpráva k zákonu č. 121/2000 Sb., autorský zákon

Důvodová zpráva k zákonu č. 141/2014 Sb., změna trestního řádu

Důvodová zpráva k zákonu č. 251/2016 Sb., o některých přestupcích

Důvodová zpráva k zákonu č. 306/2009 Sb., změna trestního zákoníku

Důvodová zpráva k zákonu č. 40/2009 Sb., trestní zákoník

Důvodová zpráva k zákonu č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim

Důvodová zpráva k zákonu č. 455/2016 Sb., změna trestního zákoníku a dalších zákonů

Důvodová zpráva k zákonu č. 86/2015 Sb., změna zákona o výkonu zajištění majetku a věcí v trestním řízení

Důvodová zpráva k zákonu č. 89/2012 Sb., nový občanský zákoník (konsolidované znění)

ETS No. 185, Convention on Cybercrime, Úmluva o počítačové kriminalitě

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, dodatkový protokol k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů

General Data Protection Regulation, nařízení Evropského parlamentu a Rady 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

Sněmovní tisk 138. Poslanecká sněmovna Parlamentu ČR, VIII volební období. Vládní návrh zákona o zpracování osobních údajů, včetně důvodové zprávy

Sněmovní tisk 139. Poslanecká sněmovna Parlamentu ČR, VIII volební období. Vládní návrh zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů, včetně důvodové zprávy

Sněmovní tisk 384. Poslanecká sněmovna Parlamentu ČR, VIII volební období. Návrh skupiny poslanců zákona o změně trestního zákoníku a zákona o některých přestupcích, včetně důvodové zprávy

Úřad Vlády ČR. Návrh vyhlášky, kterou se mění vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění vyhlášky č. 205/2016 Sb. PID ALBSB77GWFYL

Ústavní zákon č. 1/1993, Ústava ČR

Ústavní zákon č. 2/1993, Listina základních práv a svobod

Vyhláška č. 205/2016 sb., kterou se mění vyhláška č. 317/2014 sb., o významných informačních systémech a jejich určujících kritériích

Vyhláška č. 317/2014 sb., o významných informačních systémech a jejich určujících kritériích

Vyhláška č. 357/2012 sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů

Vyhláška č. 437/2017 sb., o kritériích pro určení provozovatele základní služby

Vyhláška č. 48/2005 sb., o základním vzdělávání a některých náležitostech plnění povinné školní docházky

Vyhláška č. 82/2018 sb., o kybernetické bezpečnosti

Zákon č. 101/2000 sb., o ochraně osobních údajů a o změně některých zákonů

Zákon č. 111/2009 sb., o základních registrech

Zákon č. 127/2005 sb., o elektronických komunikacích

Zákon č. 133/2000 sb., o evidenci obyvatel

Zákon č. 140/1961 sb., trestní zákon

Zákon č. 141/1961 sb., trestní řád

Zákon č. 141/2014 sb., kterým se mění zákon č. 141/1961 sb., trestní řád, ve znění pozdějších předpisů, zákon č. 40/2009 sb., trestní zákoník, ve znění pozdějších předpisů, a zákon č. 418/2011 sb., o trestní odpovědnosti právnických osob a řízení proti nim, ve znění zákona č. 105/2013 sb.

Zákon č. 181/2014 sb., o kybernetické bezpečnosti

Zákon č. 184/1950 sb., o vydávání časopisů a o svazu československých novinářů

Zákon č. 187/2006 sb., o nemocenském pojištění

Zákon č. 21/2000 sb., autorský zákon

Zákon č. 218/2003 sb., o soudnictví ve věcech mládeže

Zákon č. 227/2000 sb., o elektronickém podpisu a o změně některých dalších zákonů

Zákon č. 247/1995 sb., o volbách do parlamentu české republiky a o změně a doplnění některých dalších zákonů

Zákon č. 250/2016 sb., o odpovědnosti za přestupky a řízení o nich

Zákon č. 251/2016 sb., o některých přestupcích

Zákon č. 269/1994 sb., o rejstříku trestů

Zákon č. 275/2012 sb., o volbě prezidenta republiky a o změně některých zákonů

Zákon č. 287/2018 sb., kterým se mění zákon č. 40/2009 sb., trestní zákoník, ve znění pozdějších předpisů, a některé další zákony

Zákon č. 292/2013 sb., o zvláštních řízeních soudních

Zákon č. 297/2016 sb., o službách vytvářejících důvěru pro elektronické transakce

Zákon č. 300/2008 sb., o elektronických úkonech a autorizované konverzi dokumentů

Zákon č. 301/2000 sb., o matrikách, jménu a příjmení a o změně některých souvisejících zákonů

Zákon č. 359/1999 sb., o sociálně-právní ochraně dětí

Zákon č. 365/2000 sb., o informačních systémech veřejné správy a o změně některých dalších zákonů

Zákon č. 40/1995, o regulaci reklamy a o změně a doplnění zákona č. 468/1991 sb., o provozování rozhlasového a televizního vysílání

Zákon č. 40/2009 sb., trestní zákoník

Zákon č. 418/2011 sb., o trestní odpovědnosti právnických osob a řízení proti nim

Zákon č. 45/2013 sb., o obětech trestných činů

Zákon č. 455/1991 sb., živnostenský zákon

Zákon č. 480/2004 sb., o některých službách informační společnosti

Zákon č. 499/2004 sb., o archivnictví a spisové službě a o změně některých zákonů

Zákon č. 561/2004 sb., školský zákon

Zákon č. 592/1992 sb., o pojistném na všeobecné zdravotní pojištění

Zákon č. 89/2012 sb., občanský zákoník

4. Seznam použité judikatury

Nález Ústavního soudu I. ÚS 1428/13 ze dne 20.8.2013

Nález Ústavního soudu Pl. ÚS 24/10 ze dne 22. 3. 2011, č. 94/2011 Sb.

Rozhodnutí Najvyššího soudu Slovenské socialistické republiky Tpj 28/70-VIII ze dne 30.11.1970

Rozhodnutí Najvyššieho súdu SSR 4 Tz 62/78 ze dne 14. 9. 1978

Rozhodnutí Nejvyššího soudu 11 Tdo 349/2009 ze dne 21.5.2009

Rozhodnutí Nejvyššího soudu 5 Tdo 1271/2016 ze dne 19.10.2016

Rozhodnutí Nejvyššího soudu 7 Tdo 1120/2017 ze dne 20.12.2017

Rozhodnutí Nejvyššího soudu 7 Tz 33/78 ze dne 21. 7. 1978, č. 10/1979-II. Sb. Rozh. Tr.

Rozhodnutí Nejvyššího soudu 8 Tdo 1467/2010 ze dne 12.1.2011

Rozhodnutí Nejvyššího soudu 8 Tdo 407/2011 ze dne 27.04.2011

Rozhodnutí Nejvyššího soudu Tpjn 302/2005 ze dne 13.12.2006

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

Usnesení Ústavního soudu IV. ÚS 606/03 ze dne 19. 4. 2004

5. Seznam ostatních zdrojů

Prezentace na konferencích Eurocrim 2018 pořádané Evropskou kriminologickou společností v Sarajevu v srpnu 2018 a opakovaně na konferenci Human Factor in Cybercrime pořádané Hebrew University of Jerusalem v Jeruzalémě v říjnu 2018. **Leukfeldt, Rutger, a další. 2018.** Organised(Cyber)Crime: About Old and New Bottlenecks, Bitcoins and Cash. *csrcl.huji.ac.il.* [Online] 16. 10. 2018. [Citace: 14. 01. 2019] https://csrcl.huji.ac.il/sites/default/files/csrcl/files/organised_cybercrime_leukfeldt_et_al.pdf

Prezentace na konferenci VII. kriminologické dny pořádané Českou kriminologickou společností v Ústí n. Labem v lednu 2019. **Kalibová, Klára. 2019.** Dva roky s nenávistí online. *VII. kriminologické dny.* Ústí n. Labem, 2019

Prezentace výsledků projektu Zvol si info na konferenci Cyberspace 2018 pořádané Masarykovou univerzitou v Brně v prosinci 2018. **Vejvodová, Petra. 2018.** How to manipulate: the techniques of online disinformation media. *muni.cz.* [Online] 2018. [Citace: 08. 01. 2019] https://www.muni.cz/vyzkum/publikace/1483977

Prezentace výsledků výzkumu Digitální technologie v každodenním životě a učení studentů na konferenci Cyberspace 2018 pořádané Masarykovou univerzitou v Brně v prosinci 2018. **Ústav pedagogických věd FF MU. 2017.** zounek.cz. *Výzkumný projekt zaměřený na digitální technologie v životě a učení studentů.* [Online] 09. 01. 2017. [Citace: 28. 12. 2018] http://zounek.cz/vyzkumny-projekt-zamereny-na-digitalni-technologie-v-zivote-a-uceni-studentu/

Résumé

Cílem práce je ověření dvou hypotéz, podle nichž je v online prostředí mládež ohrožena kriminalitou a také se kriminality dopouští. Převažuje kriminologická perspektiva se zohledněním technických, sociologických, psychologických a zejm. (trestně)právních aspektů. Vychází ze studia dokumentů a odborné literatury, analýzy statistických dat (vč. dat pocházejících z vlastního výzkumu kyberkriminality prováděného v rámci Institutu pro kriminologii a sociální prevenci), informací prezentovaných na relevantních odborných konferencích a nabytých od účastníků desítek školení vedených autorkou se zaměřením na danou problematiku. Jednotlivé kapitoly se věnují vždy určitým aspektům kyberprostoru, které hrají roli z hlediska využívání kyberprostoru dětmi a dospívajícími a konkrétním škodlivým jednáním v jejich rámci.

V České republice se blíží množství domácností s dětmi s přístupem k internetu ke 100 % a digitální technologie se již nerozlučně prolínají s každodenní realitou. Jako propojující prvek slouží zejm. internet coby nové médium per se a platforma pro komunikaci, sdílení, zábavu atd., ale i protiprávní jednání. Digitalizace prakticky jakéhokoliv obsahu znamená jeho převedení do binárního kódu se všemi důsledky, mj. šiřitelností prostřednictvím internetu. Digitální domorodci (kyberprostor jako přirozený svět) i imigranti sdílí množství obsahu zejm. na sociálních sítích, na nichž jsou patrně nejvíce zřetelná specifika komunikace online - především absence neverbální složky, a tedy snadná věcná i emoční nedorozumění, větší otevřenost atd. Zároveň sociální sítě umožňují masivní zpětnou vazbu mj. na sebeprezentaci při budování vlastní identity dospívajících, kteří tak činí zejm. na Facebooku, Youtube a Lidé.cz, čímž zároveň spoluutváří i svůj digitální otisk. Snadnost komunikace, pociťování uznání a úspěchu může vést i k excesivnímu užívání až netholismu převážně ve vztahu k sociálním sítím a počítačovým hrám a zejm. ze strany osob s neuspokojivým životem v reálném prostředí, které mohou upřednostňovat vlastní online reprezentaci (profil či avatara) na úkor offline aktivit a vztahů.

Oblast kyberprostoru reguluje řada norem, kromě ústavního rámce zejm. trestní zákoník (s vlivem mezinárodního práva), zákon o kybernetické bezpečnosti a další. Na kyberkriminalitu obvykle dopadá některý z počítačových trestných činů (především neoprávněný přístup k počítačovému systému a nosiči informací), případně v souběhu s dalším trestným činem. Těm se podrobněji věnuje i výzkum Institutu pro kriminologii a sociální prevenci, který zjistil mj. časté napadání profilů na sociálních sítích a emailových schránek, mnohdy za přispění samotného poškozeného. Mládež hojně experimentuje s vlastní sexualitou, od konzumace

pornografie po sexting, který může nabýt i charakteru dětské pornografie a být provozován za úplatu. Zcela jinou formu sexuálního zneužívání představuje kybergrooming, manipulace prostřednictvím informačních a komunikačních technologií (ICT) s cílem přimět oběť k osobnímu setkání za účelem sexuálního zneužití. Zejm. na něj proto dopadá relativně nová skutková podstata trestného činu navazování nedovolených kontaktů s dítětem. Kyberšikana, intenzivní zákeřné jednání prostřednictvím ICT s rozdělenými rolemi oběti a agresora bez časového či prostorového omezení přitahuje a postupně zapojuje množství přihlížejících zejm. na sociálních sítích, ale s prolnutím i do reálného prostředí. Odvíjí se mj. od atmosféry daného kolektivu a předchozích zkušeností aktérů s (kyber)šikanou. Online prostředí tíhne i k jiným projevům nesnášenlivosti a k radikalizaci názorů vůbec.

Do prevence škodlivého jednání online se zapojuje řada aktérů z veřejného i soukromého sektoru, a to preventivními aktivitami i vydáváním zpráv a varování před aktuálními trendy, v současnosti zejm. sběrem dat, útoky na tzv. internet věcí vč. mobilních telefonů, přebíráním účtů, rostoucím množstvím dětské pornografie a sofistikovaností útoků. Primární prevence se zaměřuje na základní bezpečnostní návyky spojené s užíváním ICT, sekundární na jednotlivé ohrožené skupiny (např. děti) a konkrétní jevy (např. kyberšikana), terciární na práci s pachateli (např. omluva online) a technické zabezpečení.

K ohrožení kriminalitou online dochází od raného věku dítěte, počínaje možným zneužitím digitálního otisku utvářeného druhými a setkáním se s nevhodným obsahem. V období dětství a zejm. dospívání dochází k sexuálnímu zneužívání prostřednictvím sextingu, manipulaci při kybergroomingu a traumatizaci kyberšikanou, umožněných a umocněných snadností, rychlostí a masovostí sdíleného digitalizovaného obsahu na sociálních sítích. Zvýšeně ohrožena je mládež s vyšší vulnerabilitou i v reálném prostředí, varovným signálem může být excesivní užívání ICT. Děti a mladiství pachatelé v online prostředí využívají zejm. sociální sítě a oproti dospělým častěji jednají ve formě virtuálního násilí (zejm. kyberšikana a pomsta expartnera zveřejnivšího sexting). K protiprávnímu jednání online přispívá dojem anonymity a nižší kontroly oproti reálnému prostředí, nedomýšlení důsledků vlastního jednání a fyzicky nepřítomná oběť. Opomenout nelze ani další faktory jako specifika komunikace bez neverbální složky, míra času online, nerozlišování reálných a virtuálních vztahů aj. Pachatelé útočí především na vrstevníky a většinou je neohrožují fyzicky, leč způsobená psychická zranění jsou přinejmenším srovnatelná. Na samotných počítačových trestných činech se mladiství pachatelé podílejí oproti dospělým více než na kriminalitě vůbec, naopak mezi oběťmi figuruje mládež méně často. S ohledem na stále užší provázanost ICT s každodenním

životem a rozvoj internetu věcí lze předpokládat, že se budeme potýkat s kyberkriminalitou i nadále a zřejmě stále intenzivněji.

Summary

The aim of the thesis is to verify two hypotheses: young people online are put at risk of crime and commit crime as well. The criminological perspective prevails, taking into account the technical, sociological, psychological and, in particular, (criminal) legal aspects. It is based on the study of documents and scientific literature, analyzing of statistical data (including data from undertaken cybercrime research conducted within the Institute of Criminology and Social Prevention). Furthermore, the paper presents information given at relevant scientific conferences and obtained from participants of dozens of training courses conducted by the author focusing on the issue. The chapters always focus on certain aspects of cyberspace that play a role in the use of cyberspace by children and adolescents and specific malicious actions within them.

In the Czech Republic, the number of households with children with access to the Internet is approaching 100% and digital technology has become inseparable from everyday reality. The main element is mostly the Internet as a new medium per se and a platform for communication, sharing, entertainment, etc., as well as illegal acts. Digitalizing means turning any content into a binary code with all the consequences, including possible dissemination over Internet. Both digital natives (cyberspace as a natural world) and immigrants share vast amount of content particularly on social networks. Specifics of online communication are the most obvious there - especially the absence of a non-verbal component, and thus easy emotional misunderstandings, greater openness etc. At the same time teenagers among other things build their own digital imprint and identity by self-representation and getting massive feedback from the others (mostly on Facebook, Youtube and Lidé.cz). Ease of communication, feeling of recognition and success can also lead to excessive use of online environment, mostly in relation to social networks and computer games, and especially by people with unsatisfactory lives in a real world that may prefer their own online representation (profile or avatar) over offline activities and relationships.

The area of cyberspace is governed by a number of legal norms, by the constitutional framework and in particular the Criminal Code (with the influence of international law), the Cyber Security Act and others. Cybercrime usually involves some of the computer crimes (especially unauthorized access to the computer system and the information carrier), possibly along with another crime. Cybercrime research conducted by Institute of Criminology and Social Prevention also focuses on the most frequent attacks on social networks and e-mail boxes, often with the contribution of the harmed person himself. Young people experiment

extensively with their own sexuality, from the consumption of pornography to sexting, which can also take the character of child pornography and be paid for. A completely different form of sexual abuse is cyber grooming, manipulation through information and communication technologies (ICT) in order to get the victim into a personal encounter for the purpose of sexual abuse. Therefore, the relatively new criminal offense of establishing illegal contacts with the child is applicable. Cyber bullying, intensive malicious behavior through ICT with the set up roles of the victim and the aggressor without time or space limitations attracts and gradually engages a number of people watching, especially on social networks, but with an overlap into a real world. It evolves, besides other things, from the atmosphere of the collective and actors´ previous experience with (cyber)bully. The online environment is also breeding ground for other expressions of intolerance and radicalization of opinions at all.

A number of public and private sector actors are involved in the prevention of harmful conduct online, through preventive activities, reporting and warning about current trends: presently data collecting, attacks on the so called Internet of Things (including mobile phones), taking over accounts, increasing amount of child pornography, and the sophistication of attacks. Primary prevention focuses on basic security habits associated with ICT usage, secondary one on individual vulnerable groups (e.g. children) and specific phenomena (e.g. cyber bullying) and tertiary one on work with perpetrators (e.g. excuse online) and technical security.

The threat of online crime occurs from the early age of the child, starting with the possible misuse of the digital imprint created by others and encountering inappropriate content. During childhood and especially adolescence, sexual abuse occurs through sexting, cyber bullying manipulation and cyber bullying trauma, allowed and enhanced by the ease, speed and massiveness of shared digitized content on the social networks. Extremely vulnerable are young people with higher vulnerability in a real world, a warning signal can be excessive ICT use. Juvenile offenders use mostly the social networks and act more often in the form of virtual violence compared to adults (especially cyber bully and revenge publication of sexting by an ex-partner). Online environment gives the impression of anonymity and less control compared to the real world, and the inconceivability of the consequences and a physically absent victim contributes to offending as well. Other factors can be mentioned such as the specifics of communication without a non-verbal component, the amount of time spent online, the non-differentiation of real and virtual relationships etc. Offenders attack mainly peers and do not physically threaten them, but the psychological injuries are at least comparable. In

cybercrime, juvenile offenders participate more often than in crime in general, youngsters are on the contrary less likely to be among the victims of cybercrime. With regard to the continually deeper interdependence of ICT with everyday life and the development of Internet of Things, we can assume that we will continue to face cybercrime with increasing urgency.

Kriminalita spojená s využíváním nových médií dětmi

Anotace: Práce potvrzuje dvě hypotézy, podle nichž je v online prostředí mládež ohrožena kriminalitou a také se kriminality dopouští. Vychází především ze studia dokumentů a odborné literatury a analýzy statistických dat. Převážně kriminologická perspektiva předestírá specifika kyberprostoru a zmiňuje některé jeho technologické, sociologické, psychologické a samozřejmě právní aspekty. Demonstruje využívání kyberprostoru mládeží a s jakými riziky se uživatelé setkávají. Podrobněji se věnuje technologii internetu, novým médiím, komunikaci a utváření identity (nejen) online, digitálnímu otisku, sociálním sítím, netholismu, avatarovi coby reprezentaci uživatele, právnímu rámci a trestněprávní regulaci kyberprostoru, bitcoinům, kyberkriminalitě vůbec, výzkumu kyberkriminality prováděnému Institutem pro kriminologii a sociální prevenci, sexuálnímu vykořisťování dětí (se zaměřením na dětskou pornografii, sexting a kybergrooming), kyberšikaně, projevům nesnášenlivosti a prevenci a trendům kyberkriminality. K ohrožení kriminalitou online dochází od raného věku dítěte, počínaje možným zneužitím digitálního otisku utvářeného druhými a setkáním se s nevhodným obsahem. V období dětství a zejm. dospívání dochází k sexuálnímu zneužívání prostřednictvím sextingu, manipulaci při kybergroomingu a traumatizaci kyberšikanou, umožněných a umocněných snadností, rychlostí a masovostí sdíleného digitalizovaného obsahu na sociálních sítích. Zvýšeně ohrožena je mládež s vyšší vulnerabilitou i v reálném prostředí, varovným signálem může být excesivní užívání ICT. Děti a mladiství pachatelé v online prostředí využívají zejm. sociální sítě a oproti dospělým častěji jednají ve formě virtuálního násilí. K protiprávnímu jednání online přispívá dojem anonymity a nižší kontroly oproti reálnému prostředí, nedomýšlení důsledků vlastního jednání a fyzicky nepřítomná oběť. Opomenout nelze ani další faktory jako specifika komunikace bez neverbální složky, míra času online, nerozlišování reálných a virtuálních vztahů aj. Pachatelé útočí především na vrstevníky a většinou je neohrožují fyzicky, leč způsobená psychická zranění jsou přinejmenším srovnatelná. Na samotných počítačových trestných činech se mladiství pachatelé podílejí oproti dospělým více než na kriminalitě vůbec, naopak mezi oběťmi figuruje mládež méně často.

Klíčová slova: internet, kyberkriminalita, mládež

Crime related to the use of new media by children

Abstract: The thesis confirms two hypotheses: young people online are put at risk of crime and commit crime as well. It is based mostly on the study of documents and scientific literature and analyzing of statistical data. The predominantly criminological perspective sets out the specifics of cyberspace and mentions some of its technological, sociological, psychological and at last but not least legal aspects. Furthermore, the thesis demonstrates the use of cyberspace by young people and the risks that users face. It focuses specifically on internet technology, new media, communication and identity (not only) online, digital imprint, social networks, netholism, an avatar as a user´s representation, legal framework and criminal law regulation of cyberspace, bitcoins, cybercrime in general, cybercrime research conducted by the Institute of Criminology and Social Prevention, sexual exploitation of children (focusing on child pornography, sexting and cyber grooming), cyber bullying, intolerance and finally prevention and cybercrime trends. The threat of online crime occurs from the early age of the child, starting with the possible misuse of the digital imprint created by others and encountering inappropriate content. During childhood and especially adolescence, sexual abuse occurs through sexting, cyber bullying manipulation and cyber bullying trauma, allowed and enhanced by the ease, speed and massiveness of shared digitized content on the social networks. Extremely vulnerable are young people with higher vulnerability in a real world, a warning signal can be excessive ICT use. Juvenile offenders use mostly the social networks and act more often in the form of virtual violence compared to adults. Online environment gives the impression of anonymity and less control compared to the real world, and the inconceivability of the consequences and a physically absent victim contributes to offending as well. Other factors can be mentioned such as the specifics of communication without a non-verbal component, the amount of time spent online, the non-differentiation of real and virtual relationships etc. Offenders attack mainly peers and do not physically threaten them, but the psychological injuries are at least comparable. In cybercrime, juvenile offenders participate more often than in crime in general, youngsters are on the contrary less likely to be among the victims of cybercrime.

Key words: cybercrime, internet, children