IKSP
Institut pro kriminologii
a sociální prevenci

Jiří Vlach
Kateřina Kudrlová
Viktorie Paloušová

Kyberkriminalita v kriminologické perspektivě

Praha 2020

Ediční řada Studie

Institut pro kriminologii a sociální prevenci Praha 2020

Kyberkriminalita v kriminologické perspektivě

Jiří Vlach
Kateřina Kudrlová
Viktorie Paloušová

Autorský kolektiv:
Mgr. Jiří Vlach
Mgr. et Mgr. Kateřina Kudrlová, Ph.D.
Mgr. Viktorie Paloušová

Recenzenti:
doc. JUDr. Tomáš Gřivna, Ph.D. (Právnická fakulta Univerzity Karlovy)
Mgr. Tomáš Najman (Policejní akademie České republiky)

Technická spolupráce:
Lucie Černá

ISBN 978-80-7338-189-9

www.kriminologie.cz

Obsah

I.

Teoretický úvod

V posledních desetiletích došlo k výrazným změnám ve společnosti v souvislosti s rychlým rozvojem digitálních technologií. Tak jako zavedení telegrafu a telefonu zásadně relativizovalo časoprostorové komunikační bariéry, o současných moderních informačních a komunikačních technologiích lze říci totéž. Představit si pod nimi lze celou řadu zařízení a způsobů komunikace, jejichž potenciál využití dynamicky roste. Slouží především k uživatelským účelům, zejména ke 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.

Informační a komunikační technologie zahrnují především svět internetu a mobilních technologií, souhrnně označovaný jako **kyberprostor**.[1] 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 e-mailu, instant messagingu (odesílání a přijímání zpráv v reálném čase) a sociálních sítí. Běžné je využívání videohovorů (např. Skype) i videokonferencí, trendem jsou rozšiřující se jednosměrná videoposelství a sebepropagace (zejména prostřednictvím nahrávání vlastních videí na YouTube).[2] 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 platforma pro reklamu: běžnou, cílenou a virální marketing.[3] Vzhledem k tomu, že s využíváním moderních informačních a komunikačních technologií 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/producenti sami jsou si navzájem zároveň publikem/konzumentem.

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 dosta-

1 Kromě internetu i další, lokální sítě – firemní, univerzitní atp.

2 Včetně tzv. youtuberů.

3 Virální marketing využívá princip živelného šíření zpráv především prostřednictvím sociálních sítí.

tečné množství osob považuje za reálně existující, stává skutečným ve svých důsledcích.[4] Virtuální realita v tomto pojetí tvoří určitý paralelní svět k fyzicky existující realitě, který je skutečný ve svých důsledcích. Rozlišení mezi virtuálním a reálným světem se ovšem postupně stírá, kyberprostor se prolíná s realitou a stává se jí.[5]

K podstatným rysům patří i soustavně stoupající počet uživatelů internetu nepochybně jdoucí ruku v ruce s rostoucím počtem uživatelských míst.[6] Např. oproti roku 2009, kdy bylo v České republice zhruba 56 % uživatelů internetu (starších šestnácti let), v roce 2014 činil jejich podíl již 74 % a nakonec v roce 2019 to bylo 81 %, viz tabulka 1. Lze předpokládat, že jejich množství dále poroste - na jedné straně stále roste počet prvouživatelů starších šestnácti let,[7] na straně druhé se přes hranici šestnácti let dostávají ti, kdo používají internet již od útlého věku (jejichž procentuální zastoupení taktéž roste).

Roste též počet dětských uživatelů, a to spolu s tím, jak se počítač stává běžným vybavením domácnosti, resp. spíše lze říci, že děti patří k příčinám růstu počtu domácností s připojením k internetu. Tento trend dokumentuje fakt, že v roce 2009 při celkovém množství 49 % domácností s přístupem k internetu je poměr takových domácností bez dětí 39 %, zatímco domácností s dětmi majícími přístup k internetu je 76 %. V roce 2014 již bylo domácností s připojením k internetu 72 %, resp. 65 % domácností bez dětí a celých 93 % domácností s dětmi. Počet připojených domácností stoupal až na celkových 81 % v roce 2019, včetně 75 % bezdětných domácností a 97 % domácností s alespoň jedním dítětem, viz tabulka 1.

Tabulka 1: Uživatelé internetu starší 16 let a domácnosti s přístupem k internetu[8]

Rok	Množství uživatelů internetu starších 16 let v ČR (%)	Celkové množství domácností s přístupem k internetu (%)	Množství bezdětných domácností s přístupem k internetu (%)	Množství domácností s alespoň jedním dítětem s přístupem k internetu (%)
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

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 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 Uživatelskými místy míníme např. vytváření různých internetových kaváren a dalších míst, která zpřístupňují internet blíže neurčenému počtu uživatelů, a zároveň stále dostupnější možnost přístupu na internet, zejména prostřednictvím mobilního telefonu a využití Wi-Fi.

7 Tedy osob, které se učí vůbec s počítači zacházet, zejména ze starších generací.

8 Zdrojem informací Český statistický úřad – Informační společnost v číslech (Český statistický úřad), Kapitola B a Kapitola C.

Rok	Množství uživatelů internetu starších 16 let v ČR (%)	Celkové množství domácností s přístupem k internetu (%)	Množství bezdětných domácností s přístupem k internetu (%)	Množství domácností s alespoň jedním dítětem s přístupem k internetu (%)
2014	74	72	65	93
2015	76	73	65	94
2016	77	76	69	95
2017	79	77	71	96
2018	81	81	74	98
2019	81	81	75	97

Naléhavost problematiky vyvstává zejména 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.“[9]

Opomenout nelze ani tzv. digitální propast (či digitální rozdělení), tj. propastný rozdíl mezi uživateli a neuživateli moderních informačních a komunikačních technologií. Záleží přitom na technologické dostupnosti kyberprostoru i na vlastních schopnostech dotyčného (včetně schopnosti, ochotě a možnosti osvojit si uživatelské dovednosti).[10] Zejména 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 namístě.[11]

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.[12]

9 Viz metodické materiály Národního centra bezpečnějšího internetu, z. s., pro projekt Škola bezpečného internetu, především kapitola Bezpečné a etické užívání internetu (k dispozici pouze pro Pardubický kraj, nepublikováno).

10 Překážky mohou být různorodé: fyzický přístup k připojenému zařízení, finanční, sociodemografické (Zejména vzdělání, příjem a věk), kognitivní (úroveň informační gramotnosti), designové (dotýká se především osob se zdravotním postižením), institucionální, politické, kulturní - např. jazyk (Wikipedie, 2003).

11 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, zejména v rozvojových zemích (Internet World Stats).

12 Také 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).

Protože kyberprostor má svá specifika, odpovídá tomu i charakter kriminality s ním spojené – 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, a další, 2015, str. 336). Mnohdy také stačí jen velmi malé náklady k získání velkého vlivu, způsobení vysoké škody atp.[13]

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 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 informačních a komunikačních technologií 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, včetně prostoru pro to „být slyšen". Bez zajímavosti není ani tvorba různých skupin a jejich působení nebo sociodemografické údaje uživatelů. 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 např. 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 lze snad považovat za stěžejní.

Spolu s rozvojem technologií a rozšiřováním jejich využití (jak co do množství uživatelů vzhledem ke stále větší cenové i technologické dostupnosti, tak co do oblastí užívání) se objevují i nové podoby kriminality, přičemž její tradiční formy využívají nových prostředků. K novým, specifickým podobám kyberkriminality lze zařadit např. DDoS útoky, hacking, různé formy malwaru (cílící na sledování uživatele, ovládnutí či poškození systému atp.) nebo kybergrooming.[14] Mezi nejčastější tradiční formy využívající nových prostředků patří podvody, porušování autorských práv, dětská pornografie aj.[15]

Jednotná a v širším měřítku ustálená **definice kybernetické kriminality** dosud neexistuje. Dle definice Evropské komise se jedná o kriminalitu páchanou online s využitím elektronických komunikačních sítí a informačních systémů,[16] setkat se lze i se širší definicí

13 Včetně „nákladů" v podobě technologických znalostí útočníka, kterému může stačit i běžná uživatelská zdatnost.

14 Blíže k tomu viz např. (Wall, 2007, str. 52).

15 Přiléhavě je lze označit za „tradiční kriminalitu v novém kabátě" (Gřivna, a další, 2015, str. 338).

16 Komise dále specifikuje kyberkriminalitu především na oblast jednání souvisejících s internetem, podvod a padělání a nezákonný obsah dostupný online (European Commission).

hovořící o jakékoliv kriminalitě zahrnující využití informačních technologií.[17] Podrobnější definici nabízí např. V. Smejkal, který vymezuje počítačovou kriminalitu[18] jako páchání trestné činnosti, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení včetně 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).[19] Definice sama tak v sobě nese již i určité členění. Podobně hovoří o kyberkriminalitě např. J. Kolouch a další jako o jednání namířeném proti počítačovému systému, počítačové síti, datům či uživatelům nebo jako jednání, při němž je počítačový systém použit jako nástroj pro spáchání trestného činu (Kolouch, a další, 2019, str. 83). Zjednodušeně jde o obecně používané členění rozlišující využití informačního systému coby předmětu anebo prostředku útoku.[20] Z hlediska členění lze v českém prostředí zmínit ještě např. rozlišování podle míry využití technických znalostí a sociálního inženýrství (Jirovský, 2007, str. 195).[21]

V zahraničí se (kromě např. výše zmíněné směrnice) kyberkriminalita často člení podle budapešťské Úmluvy Rady Evropy o počítačové kriminalitě z roku 2001.[22] Do první skupiny spadají trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů: malware, hacking, útoky na elektronické bankovnictví, DDoS, nigerijské dopisy, phishing aj. Druhou skupinu tvoří trestné činy související s počítači: falšování údajů a podvod. Třetí skupina zahrnuje trestné činy související s obsahem: dětskou pornografií

17 Viz např. Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions: Creating a safer information society by improving the security of information infrastructures and combating computer-related crime [COM(2000) 890]. Sdělení mimo jiné považuje za synonyma pojmy jako „počítačová kriminalita", „kriminalita související s počítači", „kriminalita související s vyspělými technologiemi", „kyberkriminalita" – vzhledem k tomu, že všechny popisují a) použití informačních a komunikačních sítí bez geografického omezení a b) přenos nehmotných a nestálých dat.

18 Terminologie pracující s pojmem „počítač" může být z jazykového hlediska současného uživatele zavádějící, neboť odpovídá dřívějšímu charakteru digitálních technologií před nástupem tzv. internetu věcí, nepochybně však zahrnuje informační a komunikační technologie vůbec.

19 Ještě o krok podrobněji definuje kyberkriminalitu např. Výkladový slovník kybernetické bezpečnosti jako trestnou činnost, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení (včetně dat), nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět zájmu této trestné činnosti (s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité) nebo jako prostředí (objekt) nebo jako nástroj trestné činnosti (Jirásek, a další, 2013).

20 Výraz „informační systém" pravděpodobně v dohledné době vhodně nahradí v českém právním řádu doposud používanou terminologii „počítačový systém", viz Návrh zákona, kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, zákon č. 45/2013 Sb., o obětech trestných činů a o změně některých zákonů (zákon o obětech trestných činů), ve znění pozdějších předpisů, a některé další zákony, který je v době vydání této publikace vládním návrhem zákona předloženým k projednání Poslaneckou sněmovnou jako tisk 980 (Poslanecká sněmovna, 8. období, od 2017).

21 Zde uvedená členění se částečně překrývají, nejsou však zcela totožná.

22 Convention on Cybercrime, ETS No. 185, dále jen Úmluva o počítačové kriminalitě. Uvádí se zde též definice některých pojmů jako „počítačový systém", „počítačová data" aj.

(včetně virtuální). Čtvrtá skupina sestává z trestných činů porušujících autorské právo a práva příbuzná autorskému právu. Dodatkový protokol pak hovoří o trestných činech ve spojení s rasistickým a xenofobním obsahem.[23]

Jiné časté členění rozlišuje trestnou činnost závislou nebo pouze usnadněnou využitím informačních a komunikačních technologií. Závislá činnost (cyber-dependent) může být prováděna pouze s použitím počítačů, počítačových sítí nebo jiných forem informačních a komunikačních technologií: malware, hacking, DDoS aj. Naproti tomu trestná činnost usnadněná využitím informačních a komunikačních technologií 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).

Kyberkriminalita představuje velmi širokou a stále se proměňující oblast. V průběhu analýzy trestních spisů se ukázalo, že spokojit se lze cum grano salis i s nejširší z uvedených definic (kriminalita zahrnující využití informačních technologií). Přinejmenším pro oblast počítačových trestných činů je však vhodné jiné než dosud uvedená členění, a to základní rozdělení na majetkovou trestnou činnost a tzv. virtuální násilí (se zbytkovou kategorií „ostatní"), blíže k tomu viz Analýza trestních spisů, zejména Členění na virtuální násilí a majetkový zájem.

I.1. Stávající poznání

Počátky kriminalizace kyberkriminality v českém prostředí lze spatřovat ve skutkové podstatě trestného činu poškození a zneužití záznamu na nosiči informací dle § 257a zák. č. 140/1961 Sb., trestní zákon (dále jen sTZ).[24] Ta byla v rozšířené podobě přejata do nového trestního zákoníku jako skutková podstata uvedená v § 230 zák. č. 40/2009 Sb., trestní zákoník (dále jen 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 okolností.

K tzv. **počítačovým trestným činům** patří ještě opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat dle § 231 TZ a poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti dle § 232 TZ. Z uvedených tří počítačových trestných činů (§ 230-232 TZ) je skutková podstata neoprávněného přístupu k počítačovému systému a nosiči informací zdaleka nejvyužívanější: před rokem 2017 šlo o pouhých 45 stíhaných, podezřelých, obžalovaných nebo obviněných osob z opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (jednalo se výlučně o fyzické osoby) oproti 752 takovým osobám (včetně 1 právnické osoby) u neoprávněného přístupu k počítačo-

23 Blíže k tomu viz Úmluva o počítačové kriminalitě a její Dodatkový protokol, ETS No. 189 (Kudrlová, 2014).

24 Mimo národní právo je nejvýznamnějším dokumentem již zmíněná Úmluva o počítačové kriminalitě (Gřivna & Polčák, 2008, str. 103).

vému systému a nosiči informací; skutková podstata poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti nebyla do roku 2017 využita vůbec.

Na kyberkriminalitu dopadá i řada dalších skutkových podstat, typicky např. podvod (§ 209 TZ) nebo porušení tajemství dopravovaných zpráv (§ 182 TZ), k nimž dochází v online prostředí hojně. Stručně lze skutkové podstaty v tomto směru kategorizovat jako 1. počítačové trestné činy, 2. trestné činy potenciálně související s kyberprostorem [porušení tajemství dopravovaných zpráv (§ 182 TZ), porušení tajemství listin a jiných dokumentů uchovávaných v soukromí (§ 183 TZ) a poškození a ohrožení provozu obecně prospěšného zařízení (§ 276 TZ), v nedbalostní formě dle § 277 TZ], 3. skutkové podstaty reagující na kyberprostor zvlášť přitěžující okolností spočívající ve spáchání činu veřejně nebo veřejně přístupnou počítačovou sítí nebo spojené se zveřejněním nebo učiněním veřejně přístupným určitého obsahu, 4. ostatní skutkové podstaty, které na první pohled nejsou sice výslovně zaměřené na kyberkriminalitu, nicméně páchání kybernetické kriminality velmi často spadá do jejich rámce – typicky jde o již zmíněná podvodná jednání, dále pak např. vydírání.[25] Mimoto reaguje trestní zákoník na kyberkriminalitu i dalšími ustanoveními. Činí tak především prostřednictvím uvedení zvlášť přitěžující okolnosti u některých skutkových podstat spočívající ve spáchání činu veřejně nebo veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem dle § 117 písm. a) TZ (Kudrlová, 2014).[26]

Výzkum se vzhledem k rozmanitosti kybernetické kriminality zaměřuje zpravidla na jednotlivá témata (např. sexuální zneužívání, kyberšikana, DDoS atp.) nebo naopak poměrně obecné údaje,[27] společným jmenovatelem všech je pak předpokládaná vysoká latence, kdy oběť mnohdy ani neví, že se stala terčem úspěšného útoku nebo že prostřednictvím jejího zařízení útočník napadá vzdálený server atp. (Gřivna, a další, 2015, str. 337). Dosavadní výzkum se pak zaměřoval např. na problematiku sexuálního zneužívání, kyberšikany a chování dětí a dospívajících v online prostředí obecně (Univerzita Palackého v Olomouci, a další, 2014).

Z kriminologického hlediska u nás nejsou dosud formy kriminality, páchané s využitím Internetu, případně sociálních sítí, dlouhodobě systematicky sledovány a dostatečně popsány. Výjimku představuje dlouhodobá analýza soudních rozhodnutí v případech kybernetické kriminality probíhající na katedře trestního práva Právnické fakulty Univerzity Karlovy pod vedením doc. Tomáše Gřivny (Gřivna & Drápal, 2018), problematika dezinformací online (Zvol si info) nebo aktivity centra PRVoK[28] se zaměřením především na děti. K zásadním pramenům v českých podmínkách patří především obsáhlá publikace

25 V kyberprostoru kromě „tradičních" forem vydírání i v podobě tzv. ransomwaru, tj. malwaru vedoucího obvykle k zašifrování zařízení a zobrazení požadavku platby (zpravidla v bitcoinech) za uvedení do původního stavu.

26 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, a další, 2012, str. 1300).

27 Viz např. (Livingstone, a další, 2016) a kapitola Dotazníkové šetření.

28 Centrum prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci.

V. Smejkala Kybernetická kriminalita (Smejkal, 2018), dále pak CyberSecurity J. Kolouch a (Kolouch, a další, 2019) a dalších a Kyberkriminalita a právo T. Gřivny a R. Polčáka (Gřivna & Polčák, 2008).

Ze zahraničních výzkumů a publikací lze vybrat namátkou např. projekt EU Kids Online zaměřený na děti,[29] problematiku nákladů kyberkriminality, na kterou se zaměřuje Home Office, sledování různých stránek darknetu[30] J. Bartlettem nebo kyberkriminality vůbec D. S. Wallem, R. Leukfeldtem, T. J. Holtem, M. McGuirem, A. Bosslerem, B. Dupontem, T. Berenblumovou a řadou dalších, přičemž počet autorů a institucí se stále rozšiřuje podobně jako spektrum jejich pozornosti.[31]

Za zmínku stojí také řada konferencí k problematice kyberprostoru, které se ovšem zaměřují spíše na aspekty technického rázu. Výjimku představuje v českém prostředí již tradiční konference Cyberspace a v zahraničí nově se etablující konference Human factor in cybercrime. Humanitně orientovaný pohled na online prostředí (včetně právních otázek) bývá dále zahrnut alespoň coby dílčí téma v rámci velkých konferencí bez bližšího tematického určení.[32]

Kromě odborné literatury a setkání jsou cenným zdrojem informací alespoň o části kybernetické kriminality v rámci České republiky **statistiky** Ministerstva vnitra a Policie ČR. Jsou publikované každý rok ve formě Zpráv o bezpečnostní situaci na území České republiky a Statistických přehledů kriminality.[33] Je však namístě si připomenout, že kybernetická kriminalita vykazuje velmi vysokou míru latence a zmíněné statistiky nám tak ukazují pouze příslovečnou špičku ledovce, nemluvě o problematickém vykazování po technické stránce vůbec (Diblíková, a další, 2019, str. 122). Statistické přehledy kriminality skýtají mimo jiné souhrnné údaje pro počítačové trestné činy.[34] Nezanedbatelná část dalších trestných činů, které bychom mohli též řadit ke kybernetické kriminalitě je však skryta pod celou řadou dalších skutkových podstat a nelze je tak ve statistických údajích odlišit od klasické kriminality.[35] I přes toto omezení mohou zmíněné statistické údaje skýtat řadu cenných informací.

29 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, včetně USA a Ruska. Publikované zprávy vychází pod standardním označením ISSN 2045 256X a dostupné jsou všechny online (eukidsonline.net).

30 Část internetu, která je dostupná pouze prostřednictvím speciálního prohlížeče (využívají ji zejména uživatelé, kteří chtějí zvýšit svou anonymitu a zakrýt své aktivity online).

31 Viz např. (eukidsonline.net; Costs of Cyber Crime Working Group, 2018; Bartlett, 2015; Wall, 2007; Leukfeldt & Holt, 2019) aj.

32 V evropském měřítku především v rámci každoroční konference Eurocrim.

33 Gestorem těchto zpráv je Odbor bezpečnostní politiky a prevence kriminality MV, jsou dostupné on-line (Ministerstvo vnitra; Policie ČR).

34 Ve Statistických přehledech kriminality jsou Policií ČR skutky dle § 230 – 232 TZ vykazovány pod jednotným takticko-statistickým kódem 865 „poškozování a zneužívání záznamu na nosiči informací" v rámci hospodářské kriminality.

35 Typickým příkladem jsou internetové podvody, které jsou v některých případech stíhány a souzeny pouze dle § 209 TZ a v některých dle § 209 TZ v souběhu s § 230 TZ (Smejkal, 2018, str. 133).

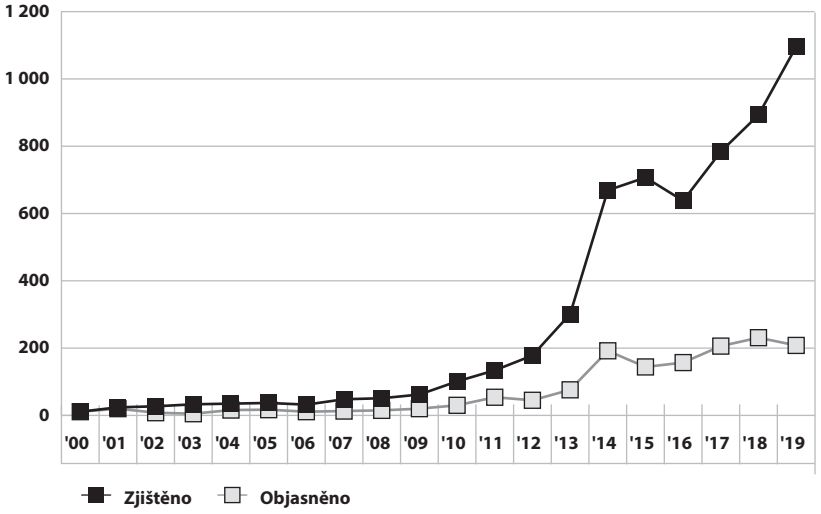
Tabulka 2: Přehled statistických údajů o skutcích dle § 230 – 232 TZ (§ 257a sTZ)

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
2014	669	192	29	75	55	46
2015	707	144	20	167	113	51
2016	638	157	25	184	127	73
2017	784	206	26	176	116	111
2018	893	231	26	189	123	173
2019	1096	208	19	185	139	146

Ze statistik je zřejmé, že v letech 2000 až 2015 docházelo k postupnému zvyšování počtu zjištěných skutků, přičemž od roku 2010 vykazuje tento růst o poznání větší dynamiku. Nevětší meziroční nárůst v tomto období činící 122 % (tj. o 368 skutků více) byl zaznamenán mezi roky 2013 a 2014. Mezi lety 2015 a 2016 byl zaznamenán největší meziroční pokles ve sledovaném období (o 69 skutků méně). V následujících letech však již počet zjištěných skutků opět začal vykazovat vzrůstající tendenci. Podrobnější údaje jsou uvedeny v tabulce 2 a grafu 1.[36]

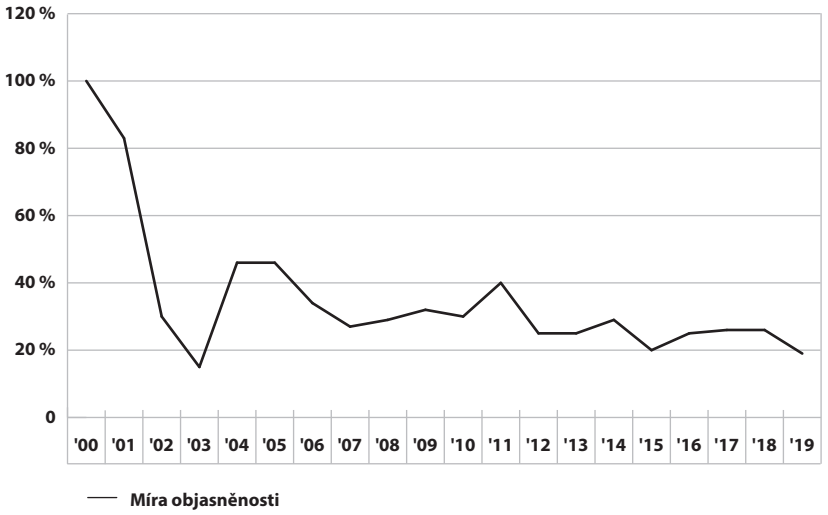
36 Údaje byly čerpány ze **S**tatistických přehledů kriminality (Policie ČR), Statistických ročenek kriminality a systému CSLAV (Ministerstvo spravedlnosti).

Graf 1: Vývoj skutků dle § 230–232 TZ (§ 257a sTZ) v letech 2000–2019



Naproti tomu míra objasněnosti těchto skutků vykazuje ve sledovaném období převážně klesající trend. Její nejvýraznější propad lze zaznamenat mezi lety 2000 až 2003, kdy z počáteční 100% objasněnosti došlo k poklesu až na 15 %. Po opětovném zvýšení míry objasněnosti v následujícím roce se v dalších letech pohybovala, byť s několika výkyvy, kolem průměru 30 % s mírně klesající tendencí, viz tabulka 2 a graf 2.

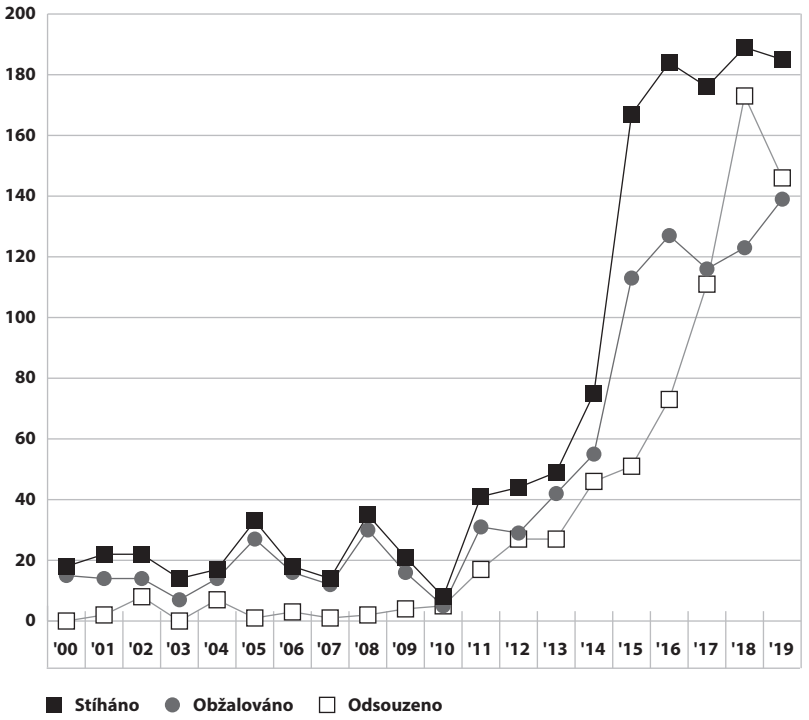
Graf 2: Míra objasněnosti skutků dle § 230–232 TZ (§ 257a sTZ) v letech 2000–2019



Dalším, nikoliv zanedbatelným zdrojem informací o kyberkriminalitě jsou statistické údaje resortu Ministerstva spravedlnosti, publikované v podobě statistických ročenek kriminality. Podobně jako u statistických údajů uvedených výše lze i ve vývoji počtu stíhaných, obžalovaných a odsouzených osob pro počítačové trestné činy zaznamenat výrazný vzestupný trend po roce 2010. Nevětší, 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 % (tj. o 19 osob více), viz tabulka 2 a graf 3.

Graf 3: Vývoj počtu osob stíhaných, obžalovaných a odsouzených za počítačové trestné činy v letech 2000–2019



Výše uvedené statistické údaje pochopitelně doprovází i rostoucí pozornost věnovaná kybernetické kriminalitě ze strany různých institucí a organizací, které pak v rámci prevence vydávají informace, varování a doporučení jdoucí již nad rámec poměrně úzce vymezených počítačových trestných činů.

Veškeré uváděné informace je ovšem třeba brát s určitou rezervou, a to hned z několika důvodů. Na jedné straně stojí samozřejmě předpokládaná vysoká latence kyberkriminality. Dalším důvodem je dosud ne zcela sjednocená právní kvalifikace mnohých jednání.[37] Informace a data publikovaná komerčními společnostmi zároveň nepochybně do jisté míry odráží jejich vlastní zájmy, resp. soustředí se na určité pole působnosti, tj. pouze na určitou výseč kyberkriminality.[38]

37 Např. neoprávněný přístup a využití e-mailového klienta 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).

38 Např. vývoj a prodej specifických ochranných nástrojů proti té či oné hrozbě.

Setkat se tak lze v prvé řadě např. s řadou ad hoc zpráv publikovaných na webu Národního úřadu pro kybernetickou a informační bezpečnost, CZ.NIC coby provozovatele národního CSIRT[39] a na webech komerčních společností,[40] dále pak věnují pozornost kyberkriminalitě i další instituce, neboť se jedná již o nedílnou součást kriminality jako takové. Typicky se lze setkat s každoročně publikovanými zprávami o proběhlých útocích za uplynulý rok spolu s očekáváními pro rok nadcházející, a to zejména ze strany poskytovatelů ochranného softwaru (ESET, Kaspersky, McAfee atp.).

Určité informace o rozsahu kyberkriminality v ČR lze vyčíst kromě policejních a justičních statistik (s výhradou vysoké latence) a pravidelných i ad hoc publikovaných zpráv i z jiných výzkumných projektů věnovaných online prostředí, které se ovšem věnují počítačovým trestným činům spíše jen okrajově, pokud vůbec (zaměřují se převážně na sexuální zneužívání dětí, používání sociálních sítí a kyberšikanu).[41]

39 Computer Security Incident Response Team.

40 Viz např. internetový magazín Dvojklik společnosti ESET (ESET).

41 Viz např. výzkum České děti a FB 2015 (Univerzita Palackého v Olomouci, 2015), Výzkum rizikového chování českých dětí v prostředí internetu (Univerzita Palackého v Olomouci, a další, 2014) nebo EU Kids Online (eukidsonline.net).

II.

Představení projektu

Problematice kybernetické kriminality byla v předchozích letech v rámci výzkumných úkolů Institutu pro kriminologii a sociální prevenci (dále jen „IKSP“) věnována pozornost pouze okrajově. Výjimku v tomto směru představuje studie Ing. Karla Nováka Počítačová kriminalita – Úvod do problematiky z roku 1992 (Novák, 1992) a studie RNDr. Stanislava Musila Počítačová kriminalita – Nástin problematiky (Kompendium názorů specialistů) z roku 2000 (Musil, 2000). Vzhledem ke vzrůstajícímu trendu kriminálních aktivit páchaných v kyberprostoru poskytlo IKSP součinnost při výzkumu T. Gřivny a J. Drápala (Gřivna & Drápal, 2018) a do střednědobého plánu výzkumných úkolů na období let 2016–2019 zahrnulo také výzkumný úkon „Identifikace a posouzení druhů a trendů kriminality páchané prostřednictvím Internetu (cyber crime), případně dalších sociálních sítí“.

Předmětem výzkumu byly vybrané formy kybernetické kriminality v ČR.[42] Původním záměrem bylo zaměření se především na prevalenci kyberkriminality ve stanoveném období, a to zejména kyberkriminality páchané prostřednictvím manipulace využívající informační a komunikační technologie. Předmětem výzkumu mělo být též povědomí veřejnosti o hrozbách v kyberprostoru a spektru ohrožených zařízení, o možnostech efektivní uživatelské sebeochrany, jakož i osobní zkušenosti se zmíněnými hrozbami a ochranou před nimi.

Deklarovaným cílem bylo proto především získání, analýza a vyhodnocení nových poznatků o prevalenci vybraných forem kyberkriminality, pachatelích a jejich trestné činnosti. Cílem též bylo získání, analýza a vyhodnocení poznatků o povědomí veřejnosti o možných hrozbách v kyberprostoru a možnostech ochrany před těmito hrozbami, jakož i zjištění míry viktimizace a reálného využívání ochrany před hrozbami v kyberprostoru.

V České republice se jedná o první výzkum kybernetické kriminality prostřednictvím analýzy soudních spisů, který se zabývá počítačovými trestnými činy, jde nad rámec případových studií a publikovaných statistik a klade si za cíl získat statisticky zpracovatelná a do budoucna srovnatelná data.[43]

S ohledem na kapacitu výzkumného týmu byly vybrány konkrétní oblasti zasluhující podrobnější prozkoumání, a to počítačové trestné činy a zkušenosti uživatelů s vybranými formami kyberkriminality.

K řešení výzkumného úkolu byly použity následující metody:

- studium domácí a zahraniční odborné literatury a relevantních oficiálních dokumentů – přehled o stavu poznání v dané oblasti;
- analýza české právní úpravy včetně dostupné judikatury – přehled o stavu a vývoji právní úpravy zkoumaných jevů;
- analýza justičních a policejních statistik – základní přehled o odhalené části kyberkriminality;
- analýza vybraného vzorku trestních spisů – informace o častém průběhu páchání vybraných typů kyberkriminality. Byla zaměřena na počítačové trestné činy a vzorek čítal

42 Při použití širší definice kyberkriminality coby kriminality zahrnující využití informačních technologií.

43 Tzn. data zobecněná tak, aby mezi ně bylo možné řadit i jevy, které výzkum výslovně nepředpokládal a v budoucnu i takové, které se dnes zatím nevyskytují, a přitom natolik členěná, aby umožnila bližší porozumění.

několik desítek spisů, v nichž bylo pravomocně rozhodnuto v roce 2015. Cílem této analýzy bylo zejména získat bližší poznatky o pachatelích a jejich trestné činnosti;
- konzultace s vybranými odborníky – praktické poznatky o aktuálních hrozbách v kyberprostoru a úskalích odhalování a dokazování kybernetické kriminality v ČR formou polostrukturovaného rozhovoru s několika osobami (Policie ČR a IT pracovníci);
- dotazníkové šetření provedené na reprezentativním souboru uživatelů internetu (16-74 let) – zaměřeno především na míru viktimizace a formu sebeochrany před hrozbami v kyberprostoru;[44]
- účast na odborných konferencích – prezentace vlastních dílčích výsledků, přehled o aktuálním bádání a stavu poznání v dané oblasti.

II.1. Podrobnější vymezení a realizace projektu

Po vypracování návrhu výzkumného úkolu a jeho předložení oponentní radě v roce 2017 probíhal v letech 2017-2018 sběr dat z trestních spisů a rešerše odborné literatury; v letech 2019-2020 příprava a realizace dotazníkového šetření a sepsání předložené publikace; ostatní činnosti pak průběžně v letech 2017-2020: studium dostupné odborné literatury a analýza právní úpravy, sběr a analýza statistických údajů Ministerstva spravedlnosti a Ministerstva vnitra, analýza údajů zjištěných z trestních spisů, konzultace s vybranými odborníky, prezentace dílčích výsledků na konferencích a v odborné literatuře.

Vzhledem ke svému všezahrnujícímu charakteru představují digitální technologie, resp. kriminalita s nimi spojená obrovskou oblast. Lze ji jen těžko výzkumně uchopit, aniž by se výzkumník spokojil s obecnými závěry poukazujícími na vysokou latenci, šíři projevů, značně variující výši škod a profilů pachatelů i obětí, nemluvě o kapacitě výzkumného týmu.

Zúžení analyzované oblasti na počítačové trestné činy přineslo v tomto směru určité zlepšení, leč při kategorizaci sledovaných jednání se ukázalo, že jakkoliv se zdají být obvykle používané typologie všeobsažné, trpí nedostatky. Předně členění podle Úmluvy o počítačové kriminalitě nedopadá na veškeré relevantní jevy (např. kybergrooming). Jednak proto, že se záměrně vztahuje pouze k těm vnímaným jako nejpalčivější na mezinárodní úrovni, jednak proto, že Úmluva o počítačové kriminalitě je pevně zakotvena v určitém časovém rámci, zatímco technologický vývoj a uživatelské zvyklosti v kyberprostoru spějí nezadržitelně dále. Naproti tomu dělení na trestnou činnost závislou nebo usnadněnou informačními a komunikačními technologiemi sice zahrnuje prakticky neomezenou škálu jevů, nicméně (právě proto) je, podobně jako rozlišování informačního systému („počítače“) jako předmětu či prostředku útoku nebo podle míry využití sociálního inženýrství a technických znalostí, naopak příliš obecné.

V úvahu připadalo i vlastní rozdělení zohledňující specifika určitých oblastí, a to zásah do systému (často jen prostředek dalšího jednání), majetková kyberkriminalita, krádež identity, virtuální násilí, černý trh, sexuální zneužívání, porušování autorských a příbuzných práv a cyber war,[45] přičemž každá oblast by zahrnovala další podoblasti (např. sexuální

44 Vzhledem k opoždění dotazníkového šetření v důsledku hygienických opatření v souvislosti s nákazou COVID-19 v roce 2020 budou výsledky průzkumu zveřejněny samostatně až po vydání této publikace.

45 Různé podoby kybernetické války, např. mezistátní špionáž.

zneužívání by zahrnovalo kybergrooming, nakládání s dětskou pornografií atp.).[46] Při aplikaci na data získaná analýzou trestních spisů se však většina z uvedených kategorií ukázala prakticky obsolentní, přinejmenším za vybraný rok 2015 (viz dále). Do popředí naopak vystoupily dvě poměrně vyrovnané oblasti, a to majetková sféra (33 obviněných) a virtuální násilí (29 obviněných), přičemž většinu sledovaných jednání spadajících pod počítačové trestné činy lze zařadit do jedné či druhé (zbytková kategorie ostatních jednání zahrnuje všeho všudy 6 obviněných).

Analýza trestních spisů byla tedy zaměřena na počítačové trestné činy. Ovšem dotazníkové šetření se na ně neomezuje – naopak ponechává v pozornosti poměrně široké spektrum jednání.[47] Odlišné zaměření analýzy spisů a dotazníkového šetření by tak mj. mohlo napovědět něco o překrytí kyberkriminality s počítačovými trestnými činy vůbec.

Tato publikace předkládá především výsledky analýzy trestních spisů, ale také dostupných statistických údajů a vlastní úvahy řešitelů projektu. Kromě výše uvedeného obsahuje stručné informace o použitých zdrojích, vybrané údaje z trestních spisů a jejich analýzu (včetně několika podrobněji zpracovaných tematických oblastí), některé poznatky z konzultací s vybranými odborníky, základní informace k dotazníkovému šetření (včetně rešerše dostupných statistických údajů)[48] a závěrečné zamyšlení nad možnostmi budoucího výzkumu v oblasti kyberkriminality. Pro lepší orientaci v problematice přikládáme též stručný zjednodušující slovníček některých častěji použitých pojmů.

II.1.1. Zdroje - odborná literatura a právní úprava

V rámci studia odborné literatury a relevantních dokumentů jsme vycházeli z odborných monografií, článků a informací publikovaných online na příslušných webech. Kromě učebnic a odborných právních komentářů šlo o řadu monografií, článků a výzkumných zpráv, ale také např. o informace zveřejňované na webech různých organizací. Mezi ty nejsledovanější patřil např. Národní úřad pro kybernetickou a informační bezpečnost, EC3 (European Cybercrime Center spadající pod Europol) nebo poskytovatelé ochranného softwaru i hardwaru (např. ESET, Symantec, Kaspersky, McAfee aj.), zejména jejich (a dalších) každoročně publikované zprávy o proběhlých a očekávaných útocích. V závěru této publikace proto uvádíme výčet použitých pramenů rozdělených na monografie, učebnice a komentáře, dále články a studie a nakonec webové stránky různých organizací spolu se zprávami o trendech v oblasti kyberkriminality, dostupnými obvykle tamtéž.

46 Blíže k tomu viz příslušná kapitola učebnice Kriminologie (Gřivna, a další, 2015) nebo (Kudrlová, 2017 b). Podrobnější rozpracování lze nalézt v jedné z nepublikovaných prací v rámci studentské vědecké odborné činnosti, které jsou dostupné na vyžádání (Kudrlová, 2016).

47 Probíhá v době přípravy této publikace a jeho výsledky budou prezentovány samostatně.

48 Nad rámec dat uvedených v kapitole Zdroje – statistické údaje.

II.1.2. Zdroje – statistické údaje

Část výzkumu spočívala v analýze dostupných statistických údajů, které byly čerpány především ze systému CSLAV Ministerstva spravedlnosti (Ministerstvo spravedlnosti). Využití našly zejména přehledy statistických listů a statistické ročenky kriminality, dále např. každoroční zprávy o činnosti Nejvyššího státního zastupitelství.

Přehledy statistických listů:

- Přehled o pravomocně vyřízených fyzických osobách podle paragrafů (odsouzených + vyřízených jinak) - právní předpis TZ;
- Přehled o pravomocně vyřízených fyzických osobách podle paragrafů - právní předpis TZ2009;
- Přehled o pravomocně vyřízených fyzických osobách podle soudů (odsouzených + vyřízených jinak);
- Oběti trestných činů - právní předpis TZ;
- Oběti trestných činů - právní předpis TZ2009.

Kromě veřejně dostupných statistických přehledů kriminality lze v rámci interního přístupu v resortu Ministerstva spravedlnosti čerpat z databáze CSLAV i další údaje. Počínaje daty z roku 2018 tak lze vybrat mezi sledovanými okolnostmi trestného činu i prvek „kyberkriminalita". Ten zahrnuje jak počítačové trestné činy, tak trestnou činnost páchanou prostřednictvím internetu, tedy včetně trestných činů jako je podvod, šíření pornografie atp.[49] V rámci projektu tak bylo uvedené kritérium využitelné jen omezeně (před rokem 2018 nebyl prvek kyberkriminality žádným způsobem statisticky vykazován), do budoucna však skýtá velký výzkumný prostor.

Jako další významný statistický zdroj sloužily policejní statistiky dostupné prostřednictvím webu Policie ČR pod záložkou Informační servis – Statistiky – Statistiky kriminality (Policie ČR). Z resortu Ministerstva vnitra jsme dále pracovali s každoročními zprávami ohledně extremismu a zprávami o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky (Ministerstvo vnitra).

Část dat byla také čerpána z údajů Českého statistického úřadu, především ze záložek Statistiky – Informační technologie - Informační společnost v číslech a Statistiky – Obyvatelstvo – Věková struktura obyvatel (Český statistický úřad).

Údaje vztahující se k dětským uživatelům internetu byly často čerpány z projektu EU Kids Online a s ním spojených publikací.[50] EU Kids Online sestává z výzkumné sítě odborníků ze všech zúčastněných zemí, kteří společně i jednotlivě postupně publikují svá

49 Viz Návod k vyplňování statistického listu trestního pro fyzické osoby (přístupný pouze v rámci resortu Ministerstva spravedlnosti).

50 Viz výše a Zdroje - odborná literatura a právní úprava. Tým autorů souhrnných zpráv vede obvykle Sonia Livingstone.

zjištění a z nich vyplývající doporučení.[51] Zaměřují se na děti online a podávají poměrně přesný obrázek zkoumaných jevů jako je kyberšikana, sexting[52] aj., ale i uživatelské praxe, dovedností a návyků dětí souvisejících s online prostředím vůbec.

II.1.3. Zdroje - trestní spisy

Stěžejní část projektu spočívala v analýze relevantních trestních spisů.[53] Vyžádané spisy zahrnovaly věci, ve kterých byla podána obžaloba pro naplnění skutkové podstaty některého z počítačových trestných činů a trestní řízení pravomocně skončilo v roce 2015.[54] 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,[55] zároveň bylo možné zpracovat za daný rok spisy všechny a souhrnná statistická data v resortu justice byla již k dispozici v roce 2017.

Kyberkriminalita zpravidla využívá nebo cílí na digitální zařízení nebo systém, a proto na ni zpravidla dopadá skutková podstata uvedená v § 230 TZ: neoprávněný přístup k počítačovému systému a nosiči informací (případně v souběhu s dalším trestným činem či činy). Další počítačové trestné činy, tj. opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 TZ) a poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232 TZ) nachází uplatnění pouze minimálně.

Na kyberkriminalitu ovšem dopadá i řada dalších skutkových podstat (Kudrlová, 2014), typicky např. podvod (§ 209 TZ) nebo vydírání (§ 175). S ohledem na personální možnosti projektu bylo nicméně nutné zúžit analyzované množství spisů na únosnou míru, a tedy zvolit způsob výběru vzorku. Navíc prvek kyberkriminality začal být v rámci databáze CSLAV vykazován až od roku 2018 - do té doby prakticky nebylo vůbec možné vyseparovat v rámci těchto jiných trestných činů ty, které úzce souvisí s kyberprostorem (pokud nebyly zároveň posuzovány jako počítačový trestný čin).[56]

51 Dosud poslední, IV. vlny průzkumu se zúčastnilo 19 zemí včetně České republiky.

52 Komunikace se sexuálním obsahem prostřednictvím informačních a komunikačních technologií, typicky posílání erotických fotografií mobilním telefonem.

53 Se všemi osobními údaji bylo nakládáno v souladu s GDPR.

54 Přesněji řečeno jde o ta pravomocně skončená řízení, jejichž údaje (statistické listy trestní) byly v roce 2015 odeslány do evidence statistiky Ministerstva spravedlnosti. Data proto 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 nicméně hovoří o věcech „pravomocně skončených v roce 2015", byť s výhradou tohoto drobného „převisu" případů z předchozího a do následujícího roku.

55 Počet počítačových trestných činů (včetně § 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, v roce 2018 to bylo již 166 osob (Ministerstvo spravedlnost).

56 Blíže k tomu viz Zdroje – statistické údaje.

Trestní věci zahrnující počítačové trestné činy (výlučně i v souběhu s dalšími trestnými činy) čítají za rok 2015 příhodně několik desítek věcí, rozhodli jsme se proto vzít coby základní kritérium pro výběr sledovaných spisů právě řízení vedené pro počítačový trestný čin. Zpracováno tak bylo 66 trestních spisů z celkového počtu 71 věcí pravomocně skončených v roce 2015, jednalo se o 68 obviněných.[57] 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.

Původním kritériem výběru sledovaných věcí byla trestněprávní kvalifikace jednání jako počítačový trestný čin uvedená v obžalobě. Ukázalo se však směrodatnější orientovat se na počítačový trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 TZ, pod který bylo subsumováno každé ze sledovaných jednání.[58]

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 zejména v protokolech o výpovědích a z hlavního líčení. Převážnou většinu sledovaných údajů se nakonec podařilo dohledat, nicméně výjimečně ten či onen údaj chyběl (např. zaměstnání obviněného, jeho předchozí trestná činnost aj.). Vždy však šlo o ojedinělou absenci a nikdy o vícero chybějících údajů v rámci jedné věci.

Prostřednictvím záznamových listů bylo sledováno 50 položek zahrnujících především základní údaje o obviněném (a okrajově též o poškozených), trestném činu samotném a o průběhu trestního řízení. Většina údajů zahrnuje osoby obviněné, tj. pachatele i ty, jejichž trestní stíhání bylo skončeno jinak než odsouzením.

Protože může jít o jednorázové i relativně dlouho trvající jednání, věk pachatele zde uváděný se nevztahuje k době spáchání trestného činu (dokončení trestněprávně relevantního jednání naplňujícího znaky dané skutkové podstaty). Namísto toho odpovídá okamžiku zahájení úkonů trestního řízení. Bylo tak možné využít předem stanovený jednotný časový bod srovnatelný napříč sledovanými skutky včetně 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 samotný skutek a jeho charakteristiky. Zejména způsob spáchání a „komunikační kanál" (tj. převažující platforma jednání), také některé z indikátorů byly jen obtížně jednoznačně zařaditelných pod kon-

57 Obvinění zahrnují odsouzené pachatele i osoby, které byly obžaloby zproštěny nebo jejichž trestní řízení bylo zastaveno. 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). Používáme proto výraz „vzorek", ačkoliv představuje plných 93 % z celého souboru.

58 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.

krétní znaky:[59] např. prolomení hesla a následné ovládnutí profilu poškozené na sociální síti 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). Bylo proto třeba se vypořádat mimo jiné s formulací proměnných i kategorizací indikátorů. Navzdory těmto úskalím (běžně provázejícím prvovýzkum) se podařilo získat množství zajímavých informací uvedených dále.

Konkrétní sledované položky byly následující:[60]

- obecné: spisová značka (pro zpětnou kontrolu a pro spárování věcí při společném řízení) a soud (ten, který vydal ve věci konečné meritorní rozhodnutí);
- ke skutku podle obžaloby: přesná kvalifikace skutku, stručný popis skutku, souběh s dalšími trestnými činy, spolupachatelství/účastenství;
- ke konečnému rozhodnutí ve věci: konečné rozhodnutí, způsob rozhodnutí, uložený trest (druh a výměra), vedlejší trest (jeho uložení a druh), ochranné opatření (jeho uložení a druh), výchovné opatření (jeho uložení a druh), polehčující a přitěžující okolnosti (jejich využití a druh);
- k průběhu trestního řízení: prvotní podnět k zahájení úkonů trestního řízení, celková délka trestního řízení, délka řízení před soudem, vazba (uvalení a trvání), řádný a mimořádný opravný prostředek (zda byly využity);
- k osobě obviněného: pohlaví, občanství, věk (v době zahájení trestního stíhání), stav (rodinný), socioprofesní status (zaměstnanec v dělnické profesi, jiný zaměstnanec, OSVČ/podnikatel, nezaměstnaný vedený na úřadu práce, bez zaměstnání, žák/student, invalidní důchodce, starobní důchodce, na mateřské/rodičovské dovolené, jiné), konkrétní profese, měsíční příjem, dosažené vzdělání, recidiva (předchozí pravomocné odsouzení, četnost předchozích odsouzení, dříve odsouzené skutky - pravá či nepravá recidiva), postavení úřední osoby, poměr pachatele k poškozenému subjektu;
- ke spáchanému skutku: způsob spáchání (sociální inženýrství, technické prostředky, kombinace sociálního inženýrství a technických prostředků, zneužití přístupu jinak oprávněnou osobou, jiný), komunikační kanál (e-mail, Facebook, sociální síť jiná než Facebook, hovor či SMS prostřednictvím mobilního telefonu, jiný), zneužití osobních údajů, použité prostředky (stolní počítač/notebook, mobilní telefon, jiné), primární cíl útoku (osobní údaje, osobnost, majetek, jiné), motivy trestného činu (zda a jaké byly výslovně uvedeny), poškozený subjekt (zda byl zjištěn, fyzická osoba, právnická osoba, fyzická i právnická osoba, počet poškozených), počet útoků (počet dokonaných útoků a počet pokusů), škoda (způsobená a zamýšlená), nemajetková újma.

II.1.4. Zdroje – konzultace s vybranými odborníky

Metodologii a konkrétní zaměření projektu jsme zejména na jeho počátku, ale i průběžně konzultovali s vybranými osobami, které se pohybují v dané oblasti jak na straně expertů, tak výzkumníků. Tyto konzultace jsme doplnili polostrukturovanými rozhovory se třemi osobami, abychom se ujistili, že naše orientace v problematice odpovídá i jejich

59 Mezi indikátory patří např. pohlaví pachatele, mezi znaky pak „muž" či „žena" (Gřivna, a další, 2015, str. 200).

60 Podrobněji jsou rozvedeny v rámci příslušných kapitol v části Analýza trestních spisů.

odbornému pohledu. Jednalo se o policistu z obvodního oddělení Policie ČR (vedoucí výjezdové skupiny SKPV)[61] za účelem zjištění, v jaké míře a podobě se Policie ČR setkává s kyberkriminalitou na bázi běžné agendy. Dále o vedoucího sekce IT bezpečnosti v soukromé společnosti zařazené do kritické infrastruktury,[62] zejména s ohledem na bezpečnostní specifika kritické infrastruktury. Nakonec o řadového IT zaměstnance v soukromém sektoru v kategorii SME,[63] abychom nahlédli pod pokličku běžných problémů, které řeší IT oddělení. Dotazovali jsme se mimo jiné na jejich zkušenosti s kyberkriminalitou v rámci jejich profese, pohled na aktuální i možné budoucí hrozby a preventivní doporučení.

II.1.5. Zdroje – odborné konference a semináře

Protože kyberkriminalita se rychle mění a rozvíjí, odborné konference a semináře na národní i mezinárodní úrovni představují důležitý zdroj informací o vývoji a stavu poznání v dané oblasti. Jednotliví členové řešitelského týmu se proto zúčastnili celé řady konferencí, které se zcela nebo alespoň v rámci separátního bloku věnovaly problematice kyberkriminality.[64] Za nejvýznamnější z nich, které se pravidelně opakují, lze považovat na národní úrovni konference Cyberspace a České kriminologické dny, na mezinárodní úrovni pak Eurocrim a Human Factor in Cybercrime.[65]

Konkrétně šlo především o následující akce:

- odborný seminář s mezinárodní účastí „Vybrané aspekty kybernetické kriminality" pořádaný v Praze v říjnu 2016 Institutem pro kriminologii a sociální prevenci;
- odborná konference s mezinárodní účastí „Kriminologie a její přínos pro bezpečnost státu" pořádaná v Praze v říjnu 2017 Policejní akademií ČR;
- odborná konference s mezinárodní účastí „Řešení elektronického násilí a kyberkriminality" pořádaná v Jihlavě v říjnu 2017 Krajem Vysočina, Krajským ředitelství Policie Kraje Vysočina a Policejní akademií ČR;
- mezinárodní odborná konference „VI. Kriminologické dny" pořádaná v Olomouci v lednu 2018 Českou kriminologickou společností a Právnickou fakultou Univerzity Palackého v Olomouci;
- odborná konference s mezinárodní účastí „Trestně právní a kriminalistické aspekty dokazování" pořádaná v Praze v březnu 2018 Vysokou školou finanční a správní;
- mezinárodní odborná konference „Paralely a divergencie (slovensko-české kriminologické dni)" pořádaná v Modre (Slovenská republika) v říjnu 2018 Filozofickou fakultou ve spolupráci s Právnickou fakultou Univerzity Komenského v Bratislave, Slovenskou sociologickou spoločností, Českou kriminologickou společností a Českou sociologickou společností;
- mezinárodní odborná konference „Human Factor in Cybercrime" pořádaná v Jeruzalémě (Izrael) v říjnu 2018 Hebrew University of Jerusalem;

61 Služba kriminální policie a vyšetřování.

62 Velký podnik čítající několik tisíc zaměstnanců.

63 Malé a střední podniky, v tomto případě s cca 60 zaměstnanci.

64 Vlastní aktivní vystoupení na jednotlivých akcích jsou uvedena v kapitole Dílčí publikované výsledky výzkumu.

65 Posledně jmenovaná se konala zatím pouze dvakrát, nepochybně však bude pro rostoucí zájem pokračovat dalšími ročníky.

- mezinárodní odborná konference „Cyberspace 2018" pořádaná v Brně v listopadu 2018 Ústavem práva a technologií Právnické fakulty Masarykovy univerzity v Brně;
- mezinárodní odborná konference „VII. Kriminologické dny" pořádaná v Ústí nad Labem v lednu 2019 Českou kriminologickou společností a Fakultou sociálně ekonomickou Univerzity J. E. Purkyně v Ústí nad Labem;
- mezinárodní odborná konference „VIII. Kriminologické dny" pořádaná v Brně v lednu 2020 Českou kriminologickou společností a Mendelovou univerzitou v Brně.

II.1.6. Dílčí publikované výsledky výzkumu

V rámci projektu byl nejprve uspořádán odborný seminář „Vybrané aspekty kybernetické kriminality" (13. října 2016) Na Květnici. V rámci tohoto odborného semináře byl přednesen příspěvek „Kybernetická kriminalita ve výzkumech IKSP".

Dílčí výsledky projektu byly v průběhu let 2017-2020 publikovány především formou odborných článků a vystoupení na odborných konferencích a po nezbytných úpravách jsou zařazeny do této publikace.[66] Články byly zveřejněny online i offline, v rámci časopisů a konferenčních sborníků a jejich seznam je následující:

- Kudrlová, K. & Vlach, J. (2017). Kyberkriminalita (nejen) v ČR – její stav a trendy. *Kriminalistika*, 2017, 256-269 (Kudrlová & Vlach, 2017);
- Kudrlová, K. (2017a). Kybergrooming – 3 roky kriminalizace. *Právo-Bezpečnost--Informace*. Zvláštní vydání mezinárodní konference Jihlava. Získáno 5. 9. 2018, z: http://teorieib.cz/pbi/files/334-Kudrlova.pdf (Kudrlová, 2017a);
- Kudrlová, K. (2017 b). *Přehled a trendy kyberkriminality.* Získáno 29. 8. 2017 z: http://www.mvcr.cz/soubor/trendy-kyberkriminality-iksp-docx.aspx (Kudrlová, 2017 b);
- Vlach, J. (2018). Kybernetická kriminalita - dílčí poznatky z výzkumu I. In Ščerba, F. (ed). Kriminologické dny 2018: Sborník příspěvků z VI. ročníku mezinárodní konference, Olomouc, 18.–19. 1. 2018 (str. 138-147). Získáno 3. 8. 2020, z: http://www.czkrim.cz/cs/soubory-ke-stazeni/sbornik-z-konference-vi-kriminologicke-dny-2018 (Vlach, 2018);
- Kudrlová, K. (2018a). Kybernetická kriminalita - dílčí poznatky z výzkumu II. In Ščerba, F. (ed). Kriminologické dny 2018: Sborník příspěvků z VI. ročníku mezinárodní konference, Olomouc, 18.–19. 1. 2018 (str. 148-157). Získáno 3. 8. 2020, z: http://www.czkrim.cz/cs/soubory-ke-stazeni/sbornik-z-konference-vi-kriminologicke-dny-2018 (Kudrlová, 2018a);
- Kudrlová, K. (2018 b). Počítačové trestné činy v České republice v roce 2015. In Lubelcová, G. (Ed.), *Paralely a divergencie: Zborník z medzinárodnej vedeckej konferencie, Modra - Harmónia, 3.-5. X. 2018* (str. 128-139). Bratislava: Univerzita Komenského Bratislava (Kudrlová, 2018 b);
- Virtuální násilí nebo hamižnost? *Česká kriminologie*.[67]

66 Prezentovány byly také prostřednictvím přednášek pro posluchače kurzu Kriminologie II na Právnické fakultě Univerzity Karlovy v Praze, v rámci Univerzity 3. věku tamtéž a v rámci učebnice Kriminologie, kapitola Kyberkriminalita (Gřivna, a další, 2019).

67 V době vydání této publikace probíhá recenzní řízení.

Dílčí výsledky byly dále prezentovány formou vystoupení na odborných konferencích:

- mezinárodní konference Řešení elektronického násilí a kyberkriminality, 19.–20. 10. 2017, pořadatel Kraj Vysočina ve spolupráci s Krajským ředitelstvím Policie Kraje Vysočina a Policejní akademií ČR, prezentace K. Kudrlové „Kybergrooming – 3 roky kriminalizace“;
- konference Bezpečné klima ve školách Pardubického kraje, 21. 11. 2017, pořadatel Pardubický kraj, prezentace K. Kudrlové „Bezpečnost i v kyberprostoru“;
- mezinárodní konference VI. kriminologické dny, 18.–19. 1. 2018, pořadatelem Česká kriminologická společnost a Právnická fakulta Univerzity Palackého v Olomouci, prezentace J. Vlacha „Kybernetická kriminalita – dílčí poznatky z výzkumu I“;
- mezinárodní konference VI. kriminologické dny, 18.–19. 1. 2018, pořadatelem Česká kriminologická společnost a Právnická fakulta Univerzity Palackého v Olomouci, prezentace K. Kudrlové „Kybernetická kriminalita – dílčí poznatky z výzkumu II“;
- mezinárodní konference Paralely a divergencie (slovensko-české kriminologické dni), 3.–5. 10. 2018, pořadatelem Filozofická a Právnická fakulta Univerzity Komenského v Bratislavě, Slovenská sociologická spoločnosť, Česká kriminologická společnost a Česká sociologická společnost, prezentace K. Kudrlové „Počítačové trestné činy v České republice v roce 2015“;
- mezinárodní konference VII. kriminologické dny, 21.–22. 1. 2019, pořadatelem Česká kriminologická společnost a Univerzity J. E. Purkyně v Ústí nad Labem, prezentace K. Kudrlové „Dílčí poznatky z výzkumu kyberkriminality“;
- mezinárodní konference VIII. kriminologické dny, 20.–22. 1. 2020, pořadatelem Česká kriminologická společnost a Mendelova univerzita v Brně, prezentace J. Vlacha „Kybernetická kriminalita páchaná zaměstnanci“;
- mezinárodní konference VIII. kriminologické dny, 20.–22. 1. 2020, pořadatelem Česká kriminologická společnost a Mendelova univerzita v Brně, prezentace K. Kudrlové „Virtuální násilí nebo hamižnost?“

III.

Analýza trestních spisů

Následující stránky předkládají vybrané výsledky analýzy zpracovaných trestních spisů, doplněné případně statistickými údaji z jiných zdrojů. Rozdělení obsahu odpovídá původnímu členění záznamového listu, přičemž některá zjištění jsou zpracována podrobněji v samostatných kapitolách.

III.1. Obecné indikátory

Samozřejmou součástí záznamového listu jsou spisové značky. Ty umožňují spárovat údaje zapisované podle jednotlivých obviněných v případě společného řízení vedeného proti více osobám (ať už jde o trestnou součinnost v podobě spolupachatelství nebo účastenství). Zároveň dávají možnost dohledat prostřednictvím systému CSLAV některé údaje i po vrácení spisu soudu (resp. bez ohledu na to, kde se spis fyzicky nachází).

Další sledovanou položkou byl **soud, který ve věci meritorně rozhodl** - ve všech sledovaných řízeních soud prvního stupně. Kromě jediného řízení tak učinil okresní soud, onou výjimkou bylo rozhodování 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,[68] viz tabulka 3.

Tabulka 3: Meritorně rozhodující soudy a počty pravomocně rozhodnutých věcí za rok 2015

Brno (krajský soud)	1	**Olomouc (okresní soud)**	2
Brno (městský soud)	6	**Ostrava (okresní soud)**	1
Brno - venkov (okresní soud)	1	**Pardubice (okresní soud)**	2
Bruntál (okresní soud)	3	**Pelhřimov (okresní soud)**	1
Česká Lípa (okresní soud)	1	**Plzeň - město (okresní soud)**	1
České Budějovice (okresní soud)	1	**Praha 10 (obvodní soud)**	2
Frýdek-Místek (okresní soud)	3	**Praha 2 (obvodní soud)**	1
Havlíčkův Brod (okresní soud)	3	**Praha 3 (obvodní soud)**	1
Hradec Králové (okresní soud)	1	**Praha 4 (obvodní soud)**	2
Chomutov (okresní soud)	1	**Praha 5 (obvodní soud)**	1
Jablonec nad Nisou (okresní soud)	3	**Praha 6 (obvodní soud)**	1
Karlovy Vary (okresní soud)	1	**Praha 7 (obvodní soud)**	1
Karviná (okresní soud)	2	**Praha 8 (obvodní soud)**	3
Kolín (okresní soud)	2	**Prostějov (okresní soud)**	2
Kutná Hora (okresní soud)	1	**Přerov (okresní soud)**	2
Liberec (okresní soud)	2	**Příbram (okresní soud)**	1
Litoměřice (okresní soud)	1	**Strakonice (okresní soud)**	1
Louny (okresní soud)	1	**Šumperk (okresní soud)**	3
Most (okresní soud)	1	**Tábor (okresní soud)**	2
Nový Jičín (okresní soud)	1	**Tachov (okresní soud)**	2

68 Dle § 17 odst. 1 a § 21 odst. 1 zák. č. 141/1961 Sb., trestní řád, dále jen TŘ.

III.2. Ke skutku podle obžaloby

K indikátorům zařazeným pracovně do kategorie „ke skutku podle obžaloby" patřila mimo jiné přesná kvalifikace skutku, tedy včetně odstavce a písmene zákonné úpravy počítačového trestného činu, který záznamový list sledoval. Skutkem (v hmotněprávním smyslu)[69] zde byl počítačový trestný čin, i když šlo o souběh s dalším či dalšími trestnými činy a počítačový trestný čin představoval spíše vedlejší trestnou činnost vedle té, za niž byl pachateli nakonec uložen trest. Při souběhu více počítačových trestných činů sledoval záznamový list primárně neoprávněný přístup k počítačovému systému a nosiči informací dle § 230 TZ. Kromě přesné kvalifikace skutku a případného souběhu obsahovaly záznamové listy i stručný popis skutku, tedy trestněprávně i jinak relevantní okolnosti a průběh jednání. Při trestné součinnosti (účastenství v užším i širším smyslu) sledovaly záznamové listy každého z účastníků samostatně.

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),[70] pouze v jediném případě šlo o zločin [§ 14 odst. 3 a § 230 odst. 2 písm. a), d), odst. 5 písm. a) TZ].[71] 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 přístupového zařízení a hesla k počítačovému systému a jiných takových dat dle § 14 odst. 2, § 231 odst. 1 písm. b) TZ, viz tabulka 4.

69 Jednání zakládající z hlediska hmotného práva trestný čin pokračující představuje jeden skutek. Na rozdíl oproti procesněprávnímu pojmosloví, které za „skutek" označuje každý dílčí útok pokračujícího trestného činu (Jelínek, a další, 2008, str. 129).

70 V jednom případě, kdy 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 dle § 329 odst. 1 písm. a) TZ, aniž by se soud v průběhu řízení k zúžení trestněprávní kvalifikace jakkoliv vyjádřil. Pravidlo výběru sledovaných spisů ovšem hovoří o takových trestních řízeních, v nichž bylo jednání posouzeno jako některý z počítačových trestních činů již v obžalobě, a nikoliv v následujícím soudním rozhodnutí, a proto i tento případ splnil kritéria pro zařazení do analýzy.

71 Z hlediska časové působnosti trestních zákonů (§ 2 TZ) byly všechny sledované činy posuzované podle nového trestního zákoníku, žádný jako poškození a zneužití záznamu na nosiči informací podle starého trestního zákona (§ 257a sTZ).

Tabulka 4: Trestní řízení o počítačových trestných činech, která byla po podání obžaloby pravomocně skončena v roce 2015[72]

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. 5 písm. a) TZ (zločin)[73]	1
§ 230 odst. 1-4 TZ + § 231 odst. 1 písm. b) TZ	2
§ 232 TZ	0

Za účasti více obviněných měly proběhnout 4 kauzy, přičemž v rámci sledovaných věcí pravomocně skončených v roce 2015 šlo o 6 obviněných. Dva z nich manipulovali s výherními automaty, 3 spolupachatelé v rámci dvou věcí zneužili svůj přístup do interního informačního systému,[74] jeden návodce vnukl rozhodnutí jinak oprávněné osobě zneužít její přístup do interního informačního systému.[75]

Velmi často se obviněný měl dopustit v souběhu s neoprávněným přístupem k počítačovému systému a nosiči informací i dalšího či dalších trestných činů – pro samotný uvedený trestný čin byl obviněný souzen v pouhých 25 případech, resp. šlo o 27 případů počítačových trestných činů bez dalšího sbíhajícího se jednání.[76] Ve 23 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.[77] Shrnuto, souběh celkově nastal v necelých dvou třetinách případů (60 %), viz graf 4.

72 Všechny následující tabulky zobrazují data vztahující se ke sledovaným řízením, tj. trestním řízením vedeným pro spáchání některého z počítačových trestných činů, v nichž byla podána obžaloba a která byla pravomocně skončena v roce 2015.

73 Resp. v tomto případě § 230 odst. 2 písm. a), d) odst. 5 písm. a) TZ, viz výše.

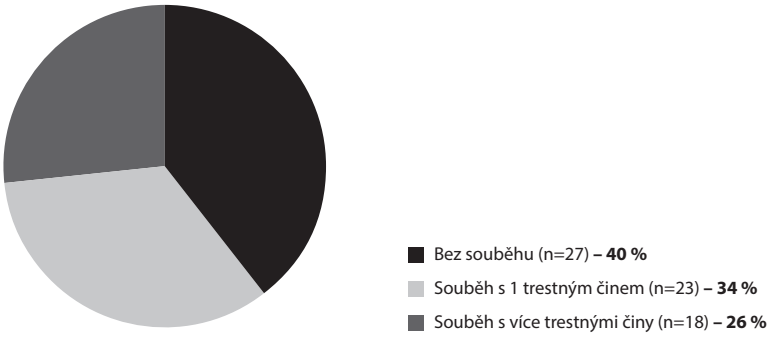
74 V jedné z těchto věcí nabylo meritorní rozhodnutí právní moci v roce 2015 pouze ve vztahu k jednomu ze spolupachatelů.

75 Obžaloba návodce chybně označila jako pomocníka.

76 Se zohledněním pouze těch jednání, která více či méně souvisela se spácháním neoprávněného přístupu k počítačovému systému a nosiči informací – vícečinný souběh nestejnorodý zde není brán v potaz, pokud s počítačovými trestnými činy nikterak nesouvisel.

77 Pachatel neoprávněně pronikal do cizích facebookových profilů 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].

Graf 4: Souběh s dalšími trestnými činy



Neoprávněný přístup k počítačovému systému a nosiči informací jde nejčastěji ruku v ruce s útokem směřujícím proti majetku: krádež (§ 205 TZ, 8 souběhů), podvod a úvěrový podvod (§ 209 a 211 TZ, celkem 12 souběhů).[78] Zařazení počítačových trestných činů v rámci hlavy V. zvláštní části trestního zákoníku, tj. mezi trestnými činy proti majetku, je tak zcela namístě, byť nelze opominout ani ty případy, kdy se pachatel dopustí neoprávněného přístupu k počítačovému systému a nosiči informací nikoliv ze zištných, ale spíše z nenávistných nebo žárlivých pohnutek a usiluje především o zasažení osobnosti a způsobení nemajetkové újmy poškozenému.[79] Za zmínku pak stojí ještě zneužití pravomoci úřední osoby (§ 329 TZ, 8 souběhů, zejména zneužití přístupu k jinak neveřejnému informačnímu systému),[80] vydírání (§ 175 TZ, 6 souběhů) a porušení tajemství dopravovaných zpráv (§ 182 TZ, 5 souběhů).

Nutno ovšem podotknout, že samotné podřazování jednání obviněného pod skutkovou podstatu neoprávněného přístupu k počítačovému systému a nosiči informací 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.[81] V prvním odstavci § 230 TZ je chráněna primárně důvěrnost počítačových dat a počítačového systémů, v druhém pak jejich integrita a dostupnost (Šámal, a další, 2012, str. 2086). Pachatel tak může zasáhnout jeden, druhý, nebo i oba chráněné objekty.[82] V některých případech je

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

79 Např. neoprávněný přístup k profilu poškozené osoby na sociální síti a rozesílání urážlivých zpráv jejím jménem.

80 Přičemž ze spáchání neoprávněného přístupu k počítačovému systému a nosiči informací v souvislosti s postavením úřední osoby bylo obviněno 10 osob.

81 První hned v prvním odstavci dopadajícím na jakýkoliv neoprávněný přístup do počítačového systému po překonání překážky bez dalšího, druhá ve druhém odstavci dopadajícím na neoprávněnou manipulaci s daty bez ohledu na to, zda pachatel získal samotný přístup do počítačového systému oprávněně (např. administrátor) nebo nikoliv, třeba i po překonání překážky (Novotný, a další, 2010, str. 210).

82 Např. pachatel si pouze ze žárlivosti prohlédne po neoprávněném vniknutí do e-mailové 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 e-mailové schránky pronikl neoprávněně.

nepochybně namístě uvažovat o faktické konzumpci skutkové podstaty uvedené v prvním odstavci naplněním znaků té druhé (zejména při naplnění znaků některé z kvalifikovaných skutkových podstat), a obžaloba i soudy tak ve svých rozhodnutích činí,[83] 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 ve druhém odstavci.[84] 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 (Šámal, a další, 2012, str. 133), což podtrhuje i skutečnost, že trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací je při naplnění znaků druhé základní skutkové podstaty přísněji trestný.[85]

III.3. Ke konečnému rozhodnutí ve věci

V rámci konečného rozhodnutí ve věci obsahoval záznamový list informaci o podobě konečného rozhodnutí, tedy zda došlo ke zproštění obžaloby, odsouzení, trestní stíhání bylo zastaveno (a zda zastaveno dle § 172 odst. 1 nebo 2 TŘ, tedy zda obligatorně nebo fakultativně), věc byla postoupena, došlo k podmíněnému zastavení trestního stíhání, narovnání, nebo bylo rozhodnuto jinak. Zapisovali jsme též způsob rozhodnutí (rozsudek či zjednodušený rozsudek, usnesení, trestní příkaz). Zajímal nás uložený trest a jeho výměra (hlavní i vedlejší, pokud nebyl uložen samostatný trest), ochranná opatření, výchovná opatření a výslovně uvedené polehčující i přitěžující okolnosti.

Ve třech čtvrtinách případů došlo k odsouzení pachatele. Naproti tomu soud rozhodl u 9 obviněných o zproštění obžaloby. Tři trestní stíhání byla dle § 172 odst. 2 TŘ zastavena a tři zastavena podmíněně dle § 307 TŘ, viz tabulka 5.

83 Byť jim lze vytknout, že tak činí zpravidla mlčky.

84 Typicky např. pachatel neoprávněně pronikne do počítačového systému, ve kterém smaže určitá data – např. neoprávněně vstoupí do profilu na sociální síti, kde smaže fotografie.

85 Pachateli hrozí trest odnětí svobody až na tři léta oproti nejvýše dvěma rokům hrozícím za naplnění znaků pouze prvního odstavce (trest zákazu činnosti nebo propadnutí věci zůstávají v obou případech beze změny), viz § 230 odst. 1 a 2 TZ.

Tabulka 5: Meritorní rozhodnutí

	Počet	Podíl (%)
Zproštění obžaloby	9	13,2
Odsouzení	52	76,5
Trestní stíhání zastaveno dle § 172 odst. 2	3	4,4
Podmíněné zastavení trestního stíhání dle § 307	3	4,4
Jiné	1[86]	1,5
Celkem	68	100

Ve dvou třetinách případů rozhodl soud rozsudkem (či zjednodušeným rozsudkem), ve více jak čtvrtině trestním příkazem a v desetině usnesením, viz tabulka 6.

Tabulka 6: Forma rozhodnutí

	Počet	Podíl (%)
Rozsudek, zjednodušený rozsudek	42	61,8
Usnesení	7	10,3
Trestní příkaz	19	27,9
Celkem	68	100

III.3.1. Odsouzení

Odsouzeným pachatelům (n=52) byl ve třech čtvrtinách (75 %) uložen podmíněný trest odnětí svobody v délce trvání od 3 do 36 měsíců (v průměru 13 měsíců), přičemž stanovená délka zkušební doby se pohybovala od 12 do 60 měsíců (v průměru 27 měsíců). V osmi případech uložil soud nepodmíněný trest odnětí svobody, a to v délce trvání od 8 do 114 měsíců (v průměru 39 měsíců). Pět pachatelů dostalo trest obecně prospěšných prací ve výměře od 30 do 200 hodin (v průměru 136 hodin), viz tabulka 7.

Tabulka 7: Uložený trest (u mladistvých trestní opatření)

	Počet	Podíl (%)	Podíl v rámci odsouzených (%)
Podmíněné odsouzení k trestu odnětí svobody	39	57,4	75
Nepodmíněné odsouzení k trestu odnětí svobody	8	11,8	15,4
Obecně prospěšné práce	5	7,4	9,6
Celkem odsouzených	**52**	**76,5**	**100**
Nedošlo k odsouzení	16	23,5	
Celkem	**68**	**100**	

86 V jednom případě obviněný v průběhu trestního řízení zemřel, a tudíž bylo zastaveno dle § 223 odst. 1 a § 11 odst. 1 písm. e) TŘ.

Vedlejší trest byl uložen v necelé čtvrtině věcí. Soud takto udělil trest propadnutí věci (4x), zákaz činnosti (7x) a peněžitý trest spolu se zákazem řízení motorového vozidla. V jednom případě bylo v souvislosti s přechováváním dětské pornografie (§ 192 TZ) uloženo ochranné léčení, viz tabulka 8.

Tabulka 8: Uložen vedlejší trest

	Počet	Podíl (%)	Podíl v rámci odsouzených (%)
Ne	40	58,8	76,9
Ano	12	17,6	23,1
Hlavní trest uložen celkem	**52**	**76,5**	**100**
Nedošlo k odsouzení	16	23,5	
Celkem	**68**	**100**	

V rámci osmi rozhodnutí hrály při stanovení druhu a výměry trestu (§ 39 odst. 3 TZ) roli polehčující okolnosti, přičemž soudy většinou zohlednily, že pachatel vedl dosud řádný život [§ 41 písm. o) TZ]. Naopak u deseti odsouzených rozsudek ovlivnily okolnosti přitěžující, a to nejčastěji spáchání více trestných činů [§ 42 písm. n) TZ].

III.3.2 Zproštění obžaloby

U devíti obviněných došlo ke zproštění obžaloby, viz tabulka 5. U pěti případů nebylo prokázáno, že se skutek stal [zproštěno podle § 226 písm. a) TŘ], přičemž tyto případy byly většinou vedeny v souběhu s další trestnou činností. Třikrát se neprokázalo, že skutek spáchal obžalovaný [zproštěno podle § 226 písm. c) TŘ] a jeden skutek nebyl shledán trestným činem [zproštěno podle § 226 písm. b) TŘ].

Celková délka řízení trvala průměrně 2,5 roku, přičemž přípravné řízení (předsoudní stadium trestního procesu) trvalo oproti řízení u soudu kratší dobu.[87] To však ovlivňují dva procesy k jedné kauze údajně provedené ve spolupachatelství, kdy trestní řízení trvalo déle než 5 let. Bez nich by trestní řízení, ve kterém došlo nakonec ke zproštění obžaloby, probíhalo průměrně 1,6 roku s téměř vyrovnanou délkou přípravného a soudního řízení. Ve čtyřech trestních řízeních byl využit řádný opravný prostředek.

Do této skupiny patří osoby (včetně dvou žen) všech věkových kategorií (od 21 do 56 let, v průměru 37 let), různých socioekonomických statusů i vzdělání. Čtyři souzení mají s trestnou činností již zkušenost, dva z nich recidivně.

Většinou se jednalo o zneužití přístupu k neveřejnému informačnímu systému, případně zneužití znalosti cizího hesla. Obvinění vyšli povětšinou z řad zaměstnanců (případně bývalých zaměstnanců či spolupracujících osob) nebo blízkých (rodina, ex-partneři, známí). Především sem spadají případy s majetkovým zájmem (dvě třetiny), zbývající lze zahrnout

87 K podrobnostem ohledně počítání délky řízení viz K průběhu trestního řízení.

pod virtuální násilí. Pokud byla vyčíslena škoda, pohybovala se v rozmezí od 50 tisíc po necelé 3 miliony Kč (v průměru cca 600 Kč). V pěti případech se hovořilo o nemajetkové újmě, především v podobě online poškození (smazání dat, poškození důvěryhodnosti atp.).

III.3.3. Rozhodnutí trestním příkazem

O třetině odsouzených (35 %) rozhodl soud trestním příkazem (28 % z celkového počtu). Jednání pachatelů odsouzených trestním příkazem státní zástupci v obžalobách subsumovali zhruba v polovině případů (53 %) pod obě základní skutkové podstaty trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací (podle § 230 odst. 1 a 2 TZ). Ve 42 % kvalifikovali jednání jako neoprávněný přístup (podle § 230 odst. 1 TZ), zatímco v plných 90 % mělo jít (výlučně či v souběhu s neoprávněným přístupem) o neoprávněnou manipulaci s daty (jejich smazání, vložení, úprava atp.), tj. podle § 230 odst. 2 TZ.[88] Souběh s další trestnou činností nastal zhruba v polovině případů (53 %), v nichž byl vydán trestní příkaz.[89]

Trestní příkaz může vydat za určitých podmínek samosoudce (v souladu s § 314e a násl. TŘ). Zjednodušeně lze říci, že přichází v úvahu u méně závažných jednání, kde nejsou pochybnosti o skutkovém stavu (Fenyk, a další, 2015, str. 443). Tomu odpovídá i odlišný poměr řízení vedených pro samotný neoprávněný přístup k počítačovému systému a nosiči informací vůči řízením vedeným pro souběh tohoto počítačového trestného činu s nějakým dalším trestným jednáním: v celkovém souboru analyzovaných věcí posuzoval soud nestejnorodý souběh zhruba ve dvou třetinách případů, zatímco při vyčlenění věcí rozhodnutých trestním příkazem šlo o zhruba polovinu případů (viz výše). Trestní řízení v těchto (jednodušších, méně závažných) případech také trvalo v průměru poměrně krátkou dobu (necelý rok), přičemž výrazně delší trvání mělo přípravné řízení. Konkrétně trvalo přípravné řízení průměrně 7 měsíců, následné řízení před soudem pak již jen 2 měsíce.

Až na dva případy obecně prospěšných prací měli všichni pachatelé strpět trest odnětí svobody v délce trvání od 4 do 12 měsíců (v průměru 9 měsíců), podmíněně odložený na zkušební dobu 12 až 36 měsíců (v průměru 22 měsíců). Jednou soud uložil i vedlejší peněžitý trest.[90]

Mezi pachateli podmíněně odsouzených trestním příkazem byly 3 ženy, věkový průměr činil 32 let (17-54 let). Dvě třetiny z nich byli svobodní (68 %), čtvrtina v partnerském vztahu (26 %) a jeden rozvedený. Polovina byla buď zaměstnaná, nebo provozovala samostatně výdělečnou činnost. Dvě třetiny (63 %) měly nižší vzdělání (bez maturity). Necelá třetina pachatelů (32 %) z této skupiny byla recidivisty. Mezi těmito pachateli nebyla žádná úřední osoba.

Nejčastěji (32 %), byla porušena důvěra, kdy pachatel znal heslo nebo měl přístup do systému, stejným dílem bylo heslo získáno (pomocí sociálního inženýrství, technickým

88 Rozlišování obou základních skutkových podstat uvedených v § 230 v odst. 1 a 2 TZ však nutno brát s určitou rezervou, viz Ke skutku podle obžaloby.

89 Souběh nestejnorodý, tzn. mimo skutkovou podstatu § 230 TZ.

90 Trestním příkazem lze uložit pouze některé tresty, jejichž výčet uvádí § 314e odst. 2 TŘ.

prostředkem či uhodnutím hesla) a ve čtvrtině případů (26 %) bylo zneužito nalezené heslo. Tzn. kromě dvou případů obviněný zneužil přístupové údaje, ať už vlastní nebo cizí. Polovina pachatelů odsouzených trestním příkazem (47 %) zneužila ke své trestné činnosti sociální sítě, třetina (32 %) elektronické bankovnictví, třetina svou fyzickou přítomnost u konkrétního zařízení.[91] Ve většině případů (84 %) se tak dělo přes počítač či notebook a ve čtvrtině (26 %) prostřednictvím mobilních telefonů.

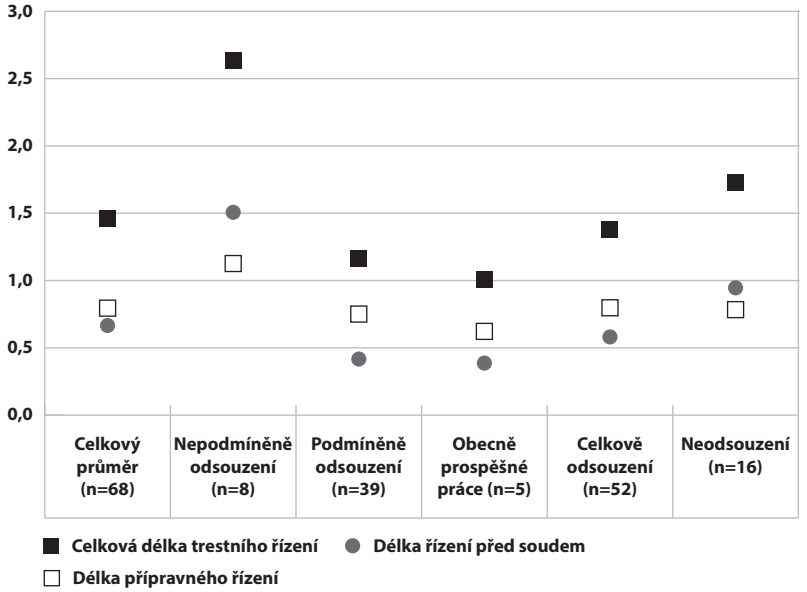
Majetkový zájem byl zjištěn u poloviny případů (47 %, z toho 2 útoky směřovaly na osobní údaje), 42 % spadalo do virtuálního násilí a 2 případy zůstaly nezařazeny. Poškozeny byly vždy 1-2 subjekty se způsobenou škodou u necelé poloviny případů (42 %) v rozmezí 1 200-128 000 Kč (v průměru 41 000 Kč). Nemajetkovou újmu uváděli poškození ve dvou třetinách případů (63 %, nejčastěji psychická újma, dále zamezení přístupu a online poškození). Poškozený byl pachateli vždy známý, a to většinou z blízkého okolí (80 %) nebo méně často ze zaměstnaneckého kolektivu (21 %).

III.3.4. Nepodmíněný trest odnětí svobody

Skupinu nepodmíněně odsouzených tvoří sedm pachatelů v rámci osmi případů (tj. 12 % z celkového počtu případů), kterým soud uložil trest ve výši od 8 do 114 měsíců, v průměru 39 měsíců. Věkové rozmezí se pohybuje od 24 do 58 let (v průměru 37 let). Mezi nimi je jedna žena ve věku 41 let, která spáchala nejpřísněji hodnocený trestný čin (s výměrou 114 měsíců). Ve všech případech kybernetické útoky probíhaly v souběhu s dalšími trestnými činy v souvislosti s charakterem daného útoku. Průměrná doba řízení byla výrazně vyšší oproti celkovému průměru, a to především díky délce samotného řízení před soudem (viz graf 5).

91 Např. počítač pamatující si přihlašovací údaje k elektronickému bankovnictví v kombinaci s vedle položeným mobilním telefonem bez dalšího zabezpečení (potažmo volně dostupnou potvrzovací SMS nezbytnou pro přihlášení do internetového bankovnictví) – zcela tak selhalo i tzv. dvoufaktorové ověření totožnosti (něco, co zná pouze uživatel – zde přihlašovací údaje - v kombinaci s něčím, co má k dispozici pouze uživatel – zde mobilní telefon).

Graf 5: Průměrná doba řízení (roky)



Ve skupině nepodmíněně odsouzených lze sledovat určité odlišnosti, a to při jejich rozdělení podle věku a rozdělení podle předchozí trestné činnosti. Mladší pachatelé (24, 25, 28 a 35 let) byli již někdy v minulosti trestáni (ve třech případech jim tato okolnost v rozsudku přitížila) – tři z nich recidivně, přičemž dva byli již více než 10 krát pravomocně odsouzení. Naproti tomu starší pachatelé (41, 42, 44 a 58 let) vedli doposud převážně řádný život (přičemž ve třech případech jim tato okolnost v rozsudku polehčila).[92]

Dva z mladších pachatelů řešili trestnou činností partnerské či ex-partnerské neshody (virtuální násilí), k čemuž se pojila i souběžná trestná činnost (porušování domovní svobody, krádež, vloupání, násilné vydírání, znásilnění atp.). Druhé dva případy byly motivovány finančním obohacením (majetkový zájem), kdy se nejmladšímu odsouzenému podařilo napáchat více než půl milionovou škodu. Oba tito pachatelé ukončili pouze základní vzdělání a jejich jednání díky tomu působí jako strategie k rychlému bezstarostnému přivýdělku.

U starších pachatelů šlo o jedince na prestižních pozicích (ve třech případech o příslušníky policie), kteří zneužili přístup k neveřejným informačním databázím. Především se jednalo o útoky na osobní údaje motivované buď finančním ziskem (majetkový zájem), nebo jako důkaz pro obhajobu v rámci jiného trestního řízení. Do této skupiny patří i výše zmíněná žena, která svou trestnou činností napáchala škodu dosahující téměř 27 milionů korun. Mimo tento případ k finančním škodám nedošlo, nicméně byla narušena ochrana osobních údajů a důvěrnost neveřejných (především policejních) databází. Kromě nepodmíněného odsouzení byl třem pachatelům uložen zákaz činnosti související s touto trestnou činností.

92 Jeden z pachatelů byl odsouzen ve dvou různých trestních řízeních konajících se (mimo jiné) pro neoprávněný přístup k počítačovému systému a nosiči informací, přičemž první z nich bylo zahájeno v jeho 42 letech, druhé pak ve 44 letech (blíže k časovému určení věku viz Zdroje – trestní spisy).

III.3.5. Odsouzení k obecně prospěšným pracím

Za zmínku stojí také pětice odsouzených k obecně prospěšným pracím (od 30 do 200 hodin, v průměru 136 hodin). Jedná se o mladé pachatele a jednu pachatelku do 22 let (průměr 20 let), studenty či nezaměstnané osoby. Až na mladou ženu s maturitou zatím všichni dosáhli pouze základního vzdělání. Přesto se mezi nimi nachází dva již zkušení recidivisté.

Cílem útoků byla vždy osobnost oběti, většinou z důvodu msty či žárlivosti na danou osobu (virtuální násilí). Pouze v jednom případě nastal souběh s další trestnou činností (dle § 183 odst. 1 TZ v souvislosti s neoprávněným šířením fotografií intimní povahy). V těchto případech nikdy nedošlo k finančním škodám, nicméně pachatelé svým obětem působili značnou nemajetkovou újmu od poškození pověsti přes ztrátu zaměstnání až po hospitalizaci v psychiatrickém zařízení.

III.3.6. Počítačové trestné činy bez souběhu

Ještě několik slov ke konečnému rozhodnutí ve věci a udílené tresty. Nutno podotknout, že jakmile se pachatel dopustil počítačového trestného činu v souběhu s dalším, nepočítačovým trestným činem, zpravidla je právě tento další trestný čin tím přísněji trestným, podle kterého pak soud ukládá trest (§ 43 odst. 1 TZ). To konec konců odpovídá charakteru skutkové podstaty neoprávněného přístupu k počítačovému systému a nosiči informací,[93] která má do jisté míry charakter předčasně dokonaného trestného činu (Šámal, a další, 2012, str. 237),[94] zejména při naplnění znaků výlučně prvního odstavce, tedy když pachatel pouze překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části.

Trestní řízení vedená pro samotný neoprávněný přístup k počítačovému systému a nosiči informací tak stojí za pozornost coby skupina per se. Nerozlišujeme zde však trestněprávní kvalifikaci dle prvního nebo druhého odstavce § 230 TZ a nebereme zřetel

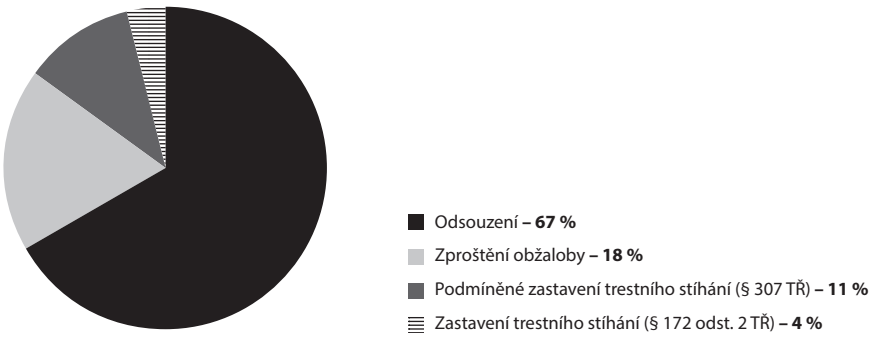
93 Tento trestný čin figuruje ve všech námi sledovaných trestních řízeních, viz Zdroje – trestní spisy a Ke skutku podle obžaloby.

94 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat dle § 231 TZ je předčasně dokonaným trestným činem samo o sobě, pouze poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti dle § 232 TZ takto označit nelze. Rozhodnutí zařadit do nového trestního zákoníku takto formulované skutkové podstaty počítačových trestných činů (vychází z velké části z mezinárodních závazků České republiky, a to zejména z Úmluvy o počítačové kriminalitě a práva Evropské unie - tehdy Rámcové rozhodnutí Rady EU 2005/222/SVV ze dne 24. února 2005 o útocích proti informačním systémům, nyní 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 (Jelínek, a další, 2015, str. 286).

na jednání v souběhu s dalším z počítačových trestných činů.[95] Zůstává tak celkem 27 relevantních případů, což sice nelze považovat za statisticky významný počet, nicméně přesto má určitou alespoň orientační vypovídací hodnotu.[96]

Z těchto 27 věcí v pěti případech soud obviněného zprostil obžaloby, v jednom bylo trestní stíhání zastaveno dle § 172 odst. 2 TŘ, ve třech bylo podmíněně zastaveno dle § 307 TŘ, ve zbývajících 18 došlo k odsouzení. Z toho ve 14 případech soud uložil trest odnětí svobody, který podmíněně odložil, viz graf 6.

Graf 6: Meritorní rozhodnutí (n=27)



Průměrná délka trestu činila 6 měsíců, s nejkratším trestem v trvání 3 měsíce a nejdelším 10 měsíců. Zkušební dobu uložil soud průměrně v délce 16 měsíců, nejméně 12 a nejvíce 30 měsíců.[97] Ve 4 případech soud uložil trest obecně prospěšných prací (třikrát 150 hod a jedenkrát 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.

Celková délka řízení se pohybovala okolo 1,4 roku, přičemž mírně převyšovala doba přípravného řízení. V případě odsouzených byla celková délka řízení v průměru o něco kratší (1,2 roku) a více ovlivněna trváním přípravného řízení (0,8 roku) oproti délce řízení před soudem (0,4 roku).

95 Rozlišování základních skutkových podstat § 230 TZ není jednotné, a tedy by jejich distinkce pravděpodobně vedla k lichým závěrům, viz Ke skutku podle obžaloby. U sbíhajících se trestných činů pak soudy ukládají trest zpravidla za jiný trestný čin než neoprávněný přístup k počítačovému systému a nosiči informací, a tedy by šlo o srovnání zcela rozdílných věcí.

96 V tomto směru nezbývá než doufat, že bude možné s obdobnou analýzou pokračovat i v dalších letech.

97 Tresty ve dvou případech souběhu s opatřením a přechováváním přístupového zařízení a hesla k počítačovému systému a jiných takových dat ve výši 7 a 6 měsíců se zkušební dobou 12 měsíců mezi ostatními nikterak nevynikají.

Průměrný věk obviněných byl 32 let (17-56 let), ze čtvrtiny šlo o ženy, polovina měla maturitu či vyšší vzdělání a pětina spadala mezi recidivisty. V případě odsouzených klesá průměrný věk (28 let, 17-54 let) i vzdělání (pouze třetina měla maturitu či vyšší vzdělání).

Z poloviny (48 %) se jednalo o případy, kdy měl obviněný přístup k informační technologii (9 x zneužití přístupu, 3 x znalost hesla). Druhá polovina byla rozdělena na ty, kdo zneužili sociální inženýrství, technický prostředek či uhodnuté heslo, a na ty, kdo heslo našli. Nejčastějšími komunikačními kanály byly sociální sítě (40 %) a e-mail (32 %).

Útoky byly vždy cílené na 1-2 subjekty, přičemž poškozenými byli buď známí obviněného (od partnerů po známé) nebo jeho zaměstnavatelé, potažmo firmy, kde pracoval. Pouze v jednom případě byla oběť neznámá. Finanční škoda vznikla v 6 případech (24 %), ale pouze v polovině z nich byl pachatel odsouzen. Odsouzené byly pouze případy s nízkou finanční škodou (1 200 Kč, 4 500 Kč, 19 389 Kč), druhá polovina obviněných v kauzách se značně vyššími škodami (50 000 Kč, 214 000 Kč, 2,9 milionů Kč) byla viny zproštěna. Nemajetkovou újmu působily tři čtvrtiny obviněných (76 %), a to především psychickou újmu či online poškození.

Polovinu případů lze zařadit do kategorie virtuální násilí (52 %, n=13, včetně 48 % útoků na osobnost), ve třetině byl zájem majetkový (32 %, n=8), čtvrtinu případů představovala kombinace majetkového zájmu i virtuálního násilí (24 %) a zbytek nespadal do žádné z těchto kategorií. Podívejme se nyní na některé z nich podrobněji.

Většinu pachatelů, jejichž trestná činnost zahrnovala převážně virtuální násilí, soud odsoudil a uložil jim trest odnětí svobody (podmíněně odložený) nebo trest obecně prospěšných prací. Odsouzení pachatelé byli spíše mladšího věku (v průměru 26,2 roku), nižšího vzdělání (8 z 10 nemělo maturitu) a polovina z nich už měla nějakou zkušenost s páchání trestné činnosti. Většinou se trestná činnost vztahovala k oběti, kterou pachatel znal. Pouze v jednom případě vznikla finanční škoda, ve všech byla zaznamenána nemajetková újma. Trestní řízení byla poměrně rychlá – v průměru 1,1 roku (od 0,2 do 2,2 roku), přičemž délku ovlivnila především délka přípravného řízení.

Z osmi obviněných, jejichž trestnou činnost motivoval převážně majetkový zájem, soud odsoudil pouze tři (uložil jim podmíněně odložený trest odnětí svobody). Většinou šlo o spory vedené v pracovním prostředí (například odcizení dat z firmy, zneužití firemní aplikace atp.). Až na jeden případ (obviněný byl již jednou souzen, a to za stejnou trestnou činnost) se jednalo o prvopachatele. Celková délka řízení oproti virtuálnímu násilí byla v průměru téměř dvojnásobná (2 roky), nicméně tento údaj výrazně navyšuje případ, který byl řešen 5,4 roku – při vyřazení této kauzy trvalo řízení průměrně 1,5 roku.

Čtyři případy nebylo možné zařadit pod virtuální násilí ani majetkový zájem, nicméně tři z nich jsou si poměrně podobné. Trestná činnost se vždy odehrává v pracovním prostředí, kde je zneužit informační systém. Motivace obviněných se však různí (například ochrana zákazníků před nevhodnou nabídku či vyhovění známému ohledně poskytnutí soukromé informace). Poslední, nezařazený případ byl sice souzen jako neoprávněný

přístup k počítačovému systému a nosiči informací (§ 230 TZ), protože obviněný smazal data z odcizeného notebooku, nicméně v tomto případě usiloval obviněný především o notebook samotný, nikoliv jeho obsah.[98]

III.4. K průběhu trestního řízení

Kromě samotných skutků a obviněných nás zajímaly i některé indikátory přiřazené k trestnímu řízení jako takovému. Především od koho vzešel podnět k zahájení úkonů trestního řízení, délka trestního řízení, uvalení vazby a využití opravných prostředků. Sledovali jsme proto mimo jiné celkovou délku trestního řízení (v grafech jen „CDŘ") a délku řízení před soudem (v grafech jen „SŘ"), potažmo délku přípravného řízení (v grafech jen „PŘ").[99] Jako oddělující mezníky při počítání délky řízení sloužily dny, kdy byly zahájeny úkony trestního řízení, kdy došla obžaloba soudu a nakonec kdy se stalo pravomocným meritorní rozhodnutí soudu.[100] Také jsme sledovali délku případně uvalené vazby, a který z opravných prostředků řízení některý z účastníků řízení využil.

Podnět vedoucí k trestnímu stíhání dala ve většině případů (79 %) poškozená strana, ať už se jednalo přímo o oběti, jejich příbuzné či pracovníky poškozených firem. V sedmi případech tak učinil některý z orgánů Policie ČR či Ministerstva vnitra, v šesti kauzách okolí pachatele (pracovní či rodinné).

Celková **délka trestního řízení**, tedy od zahájení úkonů trestního řízení policejním orgánem až po pravomocné rozhodnutí ve věci samé,[101] se pohybovala od 74 dní po téměř 5,5 roku (v průměru 1,5 roku), přičemž většina případů (90 %) byla vyřešena do 2,5 roku. Přípravné řízení trvalo od 4 dnů po něco málo přes 3 roky (v průměru 0,8 roku); řízení před soudem pak od 17 dnů po necelé 4 roky (v průměru 0,7 roku). Regresní analýza naznačuje, že největší vliv na délku řízení má využití opravného prostředku (pochopitelně) a trestná součinnost,[102] nicméně kvůli nízkým počtům relevantních analyzovaných případů nelze hovořit o zákonitosti. Kupodivu nebyla nalezena žádná korelace mezi délkou řízení a souběhem s další trestnou činností, dále ani s odsouzením pachatele, ani s případnou recidivou pachatele.

98 Přiřazení k námi používané kategorii majetkového zájmu tak není přiléhavé, neboť ta zahrnuje primárně majetkový zájem spojený s online prostředím (např. v podobě zpeněžení neoprávněně získaných dat).

99 Řízení „před soudem" označuje tu fázi trestního řízení, která probíhá od podání obžaloby. Nejde tedy o časové označení doby, po kterou probíhá trestní řízení předtím, než státní zástupce podá obžalobu nebo návrh na potrestání - v souvislosti s fázemi trestního řízení se používá výraz „před soudem" ve smyslu příslovečného určení místa, nikoliv času.

100 Jestliže soud při předběžném projednání obžaloby vrátil věc státnímu zástupci k došetření [podle § 188 odst. 1 písm. e) TŘ], započítáváme toto období stále do přípravného řízení (až do opětovného podání obžaloby, resp. do dne, kdy byla obžaloba opětovně doručena soudu).

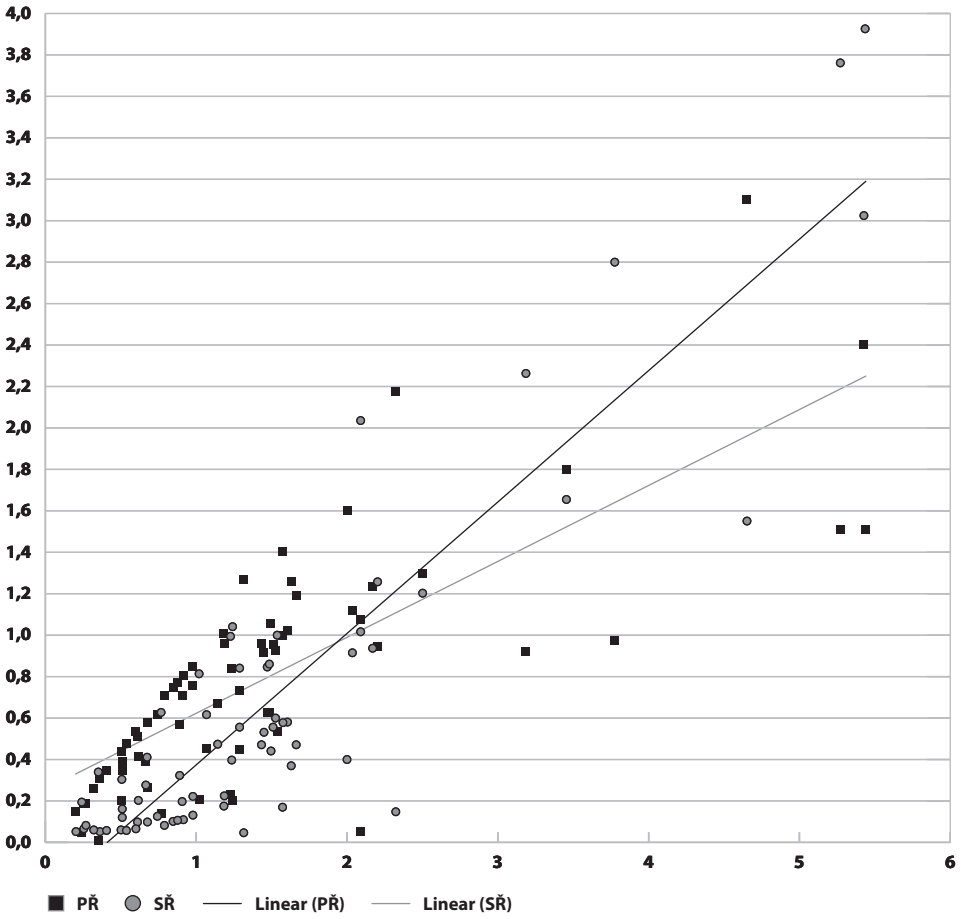
101 Přesněji od zahájení úkonů trestního řízení až po poslední pravomocné rozhodnutí ve věci samé (§ 12 odst. 10 TŘ).

102 Ať už v podobě spolupachatelství či účastenství v užším smyslu.

Řádný opravný prostředek byl využit ve čtvrtině všech případů (25 %), z toho v sedmi soud odvolání zamítl. K uplatnění mimořádného opravného prostředku došlo ve třech případech. V pěti věcech byla uvalena vazba, a to na dobu od 24 dnů po 0,7 roku (v průměru 0,3 roku).

Celková délka řízení o něco více koreluje s dobou řízení u soudu[103] než s délkou přípravného řízení.[104] Z vizualizace dat pomocí složeného regresního grafu dvou lineárních regresí závislosti celkové délky řízení za prvé na délce přípravného řízení a za druhé na době řízení před soudem (viz graf 7) je však zřejmé, že u většiny (78 %) případů vyřešených do 2 let dominuje doba přípravného řízení. Tato tendence se láme u případů s celkovou délkou řízení od 2 do 2,5 let. U déle řešených případů je naopak obecně delší doba řízení u soudu, nicméně tato skupina je velmi řídce zastoupená.

Graf 7: Délka řízení (roky)



103 Pearsonův korelační koeficient = 0,904, R^2 = 0,816.

104 Pearsonův korelační koeficient = 0,774, R^2 = 0,599.

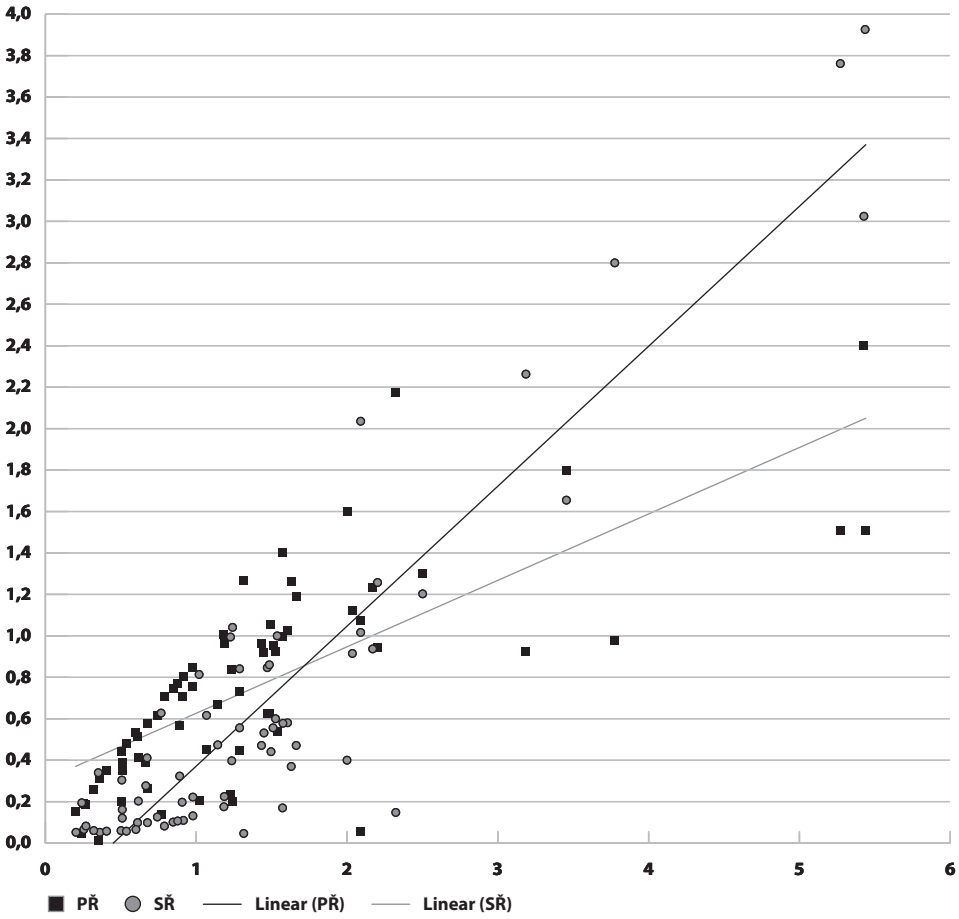
Osa X v tomto a následujících grafech představuje celkovou délku trestního řízení v letech. Osa Y (taktéž v letech) kombinuje 2 informace, a to jednak trvání přípravného řízení (zkratka PŘ), jednak stadium řízení před soudem (zkratka SŘ). V grafu je tedy každý případ reprezentován vždy jedním černým čtverečkem a šedým kolečkem nad sebou (v případě shody či blízkosti hodnot se čtvereček a kolečko mohou překrývat). Vertikální pořadí čtverečku a kolečka pak závisí na tom, zda dominovala délka přípravného řízení či řízení před soudem.

Vztahy mezi délkami řízení měříme pomocí Pearsonova korelačního koeficientu,[105] který je náchylný k extrémním případům. V našich datech se objevil jeden případ řešený znatelně delší dobu, kde oproti ostatním dominovala délka přípravného řízení (3,1 roku) oproti délce řízení před soudem (1,6 roku).[106] Uvádíme zde proto i vizualizaci dat bez tohoto případu, viz graf 8.

105 Pearsonův korelační koeficient měří vzájemný vztah dvou proměnných (zde celkové délky řízení na jedné straně, na straně druhé vůči délce přípravného řízení a vůči délce řízení před soudem), regresní analýza pak napoví, do jaké míry lze vysvětlit závisle proměnnou (zde celkovou délku trestního řízení) hodnotami nezávisle proměnných (zde délka přípravného řízení nebo řízení před soudem).

106 Šlo o zneužití přístupu do policejní databáze odhalené v rámci řešení jiné kauzy.

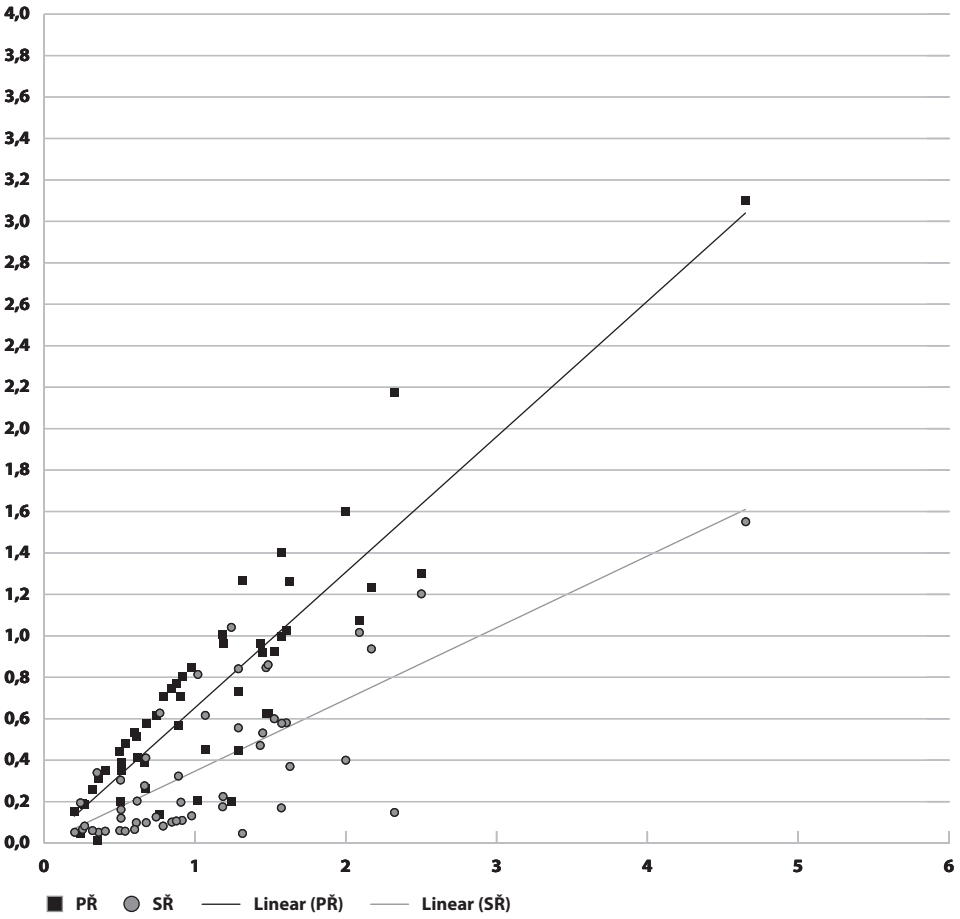
Graf 8: Délka řízení (roky) – bez extrémního případu



Po odebrání tohoto extrémního případu se Pearsonův korelační koeficient u délky řízení u soudu zvýšil (0,919) spolu se zvýšením predikce ($R^2 = 0{,}845$). U délky přípravného řízení se hodnota Pearsonova korelačního koeficientu (0,746) spolu s množstvím vysvětlených dat ($R^2 = 0{,}557$) naopak lehce snížila. To utvrzuje, že navyšování celkové délky řízení silně ovlivňuje délka řízení u soudu.[107]

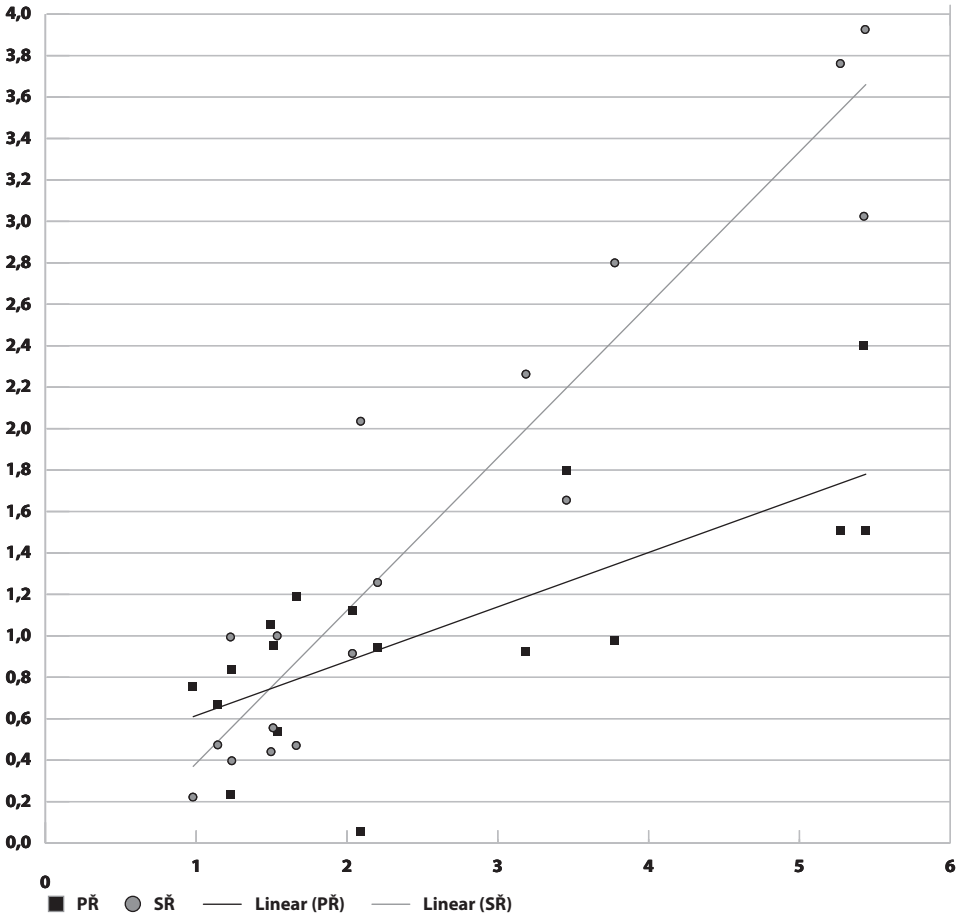
107 Zřejmě zejména s ohledem na případné využití opravných prostředků, jak uvádíme výše.

Graf 9: Délka řízení (roky) – bez využití ŘOP (n=51)



Z grafu 9 je patrné, že případy, kde nebyl využit řádný opravný prostředek (v grafech jen „ŘOP“, 75 % z celkového počtu), byly (až na zmíněný extrémní případ) vyřešeny do tří let. U těchto případů dominuje doba přípravného řízení (při odstranění extrémního případu $R^2 = 0{,}708$ a Pearsonův korelační koeficient = 0,841) nad délkou řízení před soudem (při odstranění extrémního případu $R^2 = 0{,}435$ a Pearsonův korelační koeficient = 0,660).

Graf 10: Délka řízení (roky) – s využitím ŘOP (n=17)



Řešení kauz, kde byl řádný opravný prostředek využit (25 % z celkového počtu), trvalo alespoň jeden rok a v úplných extrémech přesáhlo dobu pěti let. Od dvou let celkové doby řízení dominovala délka řízení před soudem (R^2 = 0,900, Pearsonův korelační koeficient = 0,913) oproti délce přípravného řízení (R^2 = 0,532, Pearsonův korelační koeficient = 0,783), viz graf 10.

III.4.1. Případy řešené déle než 3 roky

Podívejme se nyní podrobněji na případy řešené déle než tři roky. V těchto sedmi řízeních šlo vždy o porušení druhého odstavce § 230 TZ, tedy zjednodušeně řečeno o neoprávněnou manipulaci s daty (bez ohledu na oprávněnost či neoprávněnost samotného přístupu k nim).

Pro tyto případy bylo typické zneužití přístupu k danému komunikačnímu kanálu, ať už šlo o informační systém či soukromou databázi. Útoky směřovaly na osobní údaje a/

nebo na majetek a poškodily nejčastěji zaměstnavatele pachatele,[108] přičemž až na jeden případ spadají do kategorie majetkového zájmu. Odsouzení v těchto případech tvořili starší pachatelé (v průměru 42,6 roku), včetně jedné ženy.

V rámci celkové délky řízení převládala doba soudního stadia řízení. Výjimku tvořil případ neoprávněného zjišťování informací o osobách a vozidlech z policejní databáze, kdy délka přípravného řízení (3,1 roku) téměř dvojnásobně převyšovala délku řízení před soudem (1,7 roku).[109] Většina řízení v této kategorii se týkala i další, souběžné trestné činnosti obviněných.[110] Téměř všichni obvinění (až na jednoho) využili opravný prostředek. Kromě dvou spolupachatelů[111] soud všechny odsoudil a uložil jim převážně nepodmíněný trest odnětí svobody na dobu od 0,5 roku (podmíněně) do 9,5 roku (v průměru 3,8 roku) v kombinaci s vedlejším trestem zákazu činnosti spojené s řešenou kauzou.

III.5. K osobě obviněného

Další položky sledované v analyzovaných spisech se vztahovaly k osobě obviněného.[112] Jednalo se o pohlaví, občanství, věk (v době zahájení trestního řízení),[113] rodinný stav, socioprofesní status, vzdělání, recidivu a poměr obviněného k poškozenému. Znaky přiřazené pod socioprofesní status zahrnovaly: zaměstnanec v dělnické profesi, jiný zaměstnanec, OSVČ/podnikatel, nezaměstnaný vedený na Úřadu práce, bez zaměstnání, žák/student, invalidní důchodce, starobní důchodce, na mateřské/rodičovské dovolené, jiné. Zajímal nás také měsíční příjem obviněného, jeho konkrétní profese, a zda šlo o úřední osobu, tyto údaje však patřily k nejčastěji chybějícím.[114] U recidivistů (bez zohlednění nepravé recidivy) jsme sledovali četnost předchozích pravomocných odsouzení a o jaké činy šlo.

Věkové rozmezí obviněných se pohybuje od 17 do 58 let, v průměru je jim 34 let. Téměř polovině (47 %) je méně než 30 let, včetně jednoho mladistvého (viz graf 11), přičemž nejpočetněji jsou zastoupeni obvinění ve věku nepřevyšujícím 24 let.

108 Spolu se subjekty kompromitovaných osobních údajů. Blíže k tomu viz Zaměstnanci jako bezpečnostní riziko.

109 Jedná se o onen „extrémní případ" z předchozí části této kapitoly. K relativně krátké délce soudního stadia řízení přispěl i fakt, že proti meritornímu rozhodnutí v této kauze nepodal nikdo opravný prostředek.

110 Např. ve třech případech se měli dva obvinění ve služebním poměru (u jednoho z obviněných šlo o dvě různé kauzy) dopustit kromě neoprávněného přístupu k počítačovému systému a nosiči informací také (nejen) zneužití pravomoci úřední osoby, a to v souvislosti s neoprávněným využíváním některého z informačních systémů Policie ČR.

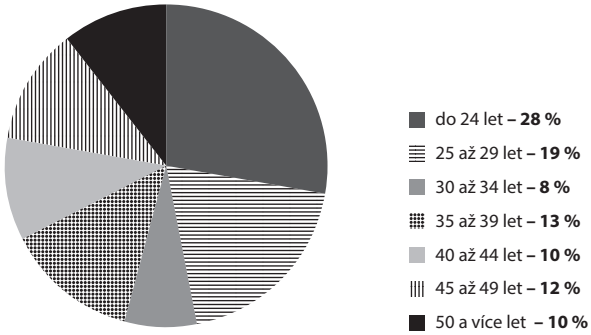
111 Přesněji řečeno obviněných, kteří měli být spolupachateli.

112 Sociodemografické údaje byly čerpány zpravidla z policejních protokolů o výslechu obviněného, nemusí se proto shodovat s údaji v době spáchání činu – typicky např. údaj o zaměstnanosti, měsíčním příjmu atp.

113 Blíže k určení věku viz Zdroje – trestní spisy.

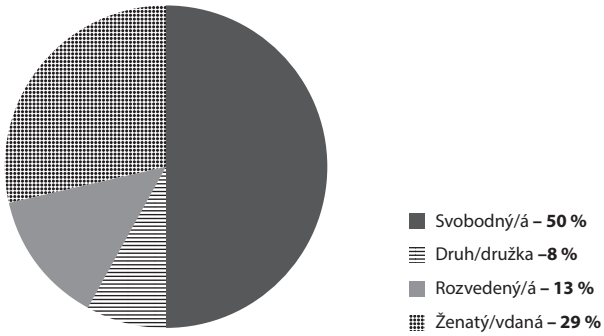
114 Řadu položek se v rámci této části nepodařilo dohledat (typicky např. měsíční příjem obviněného). Údaje zde uvedené proto vychází pouze ze zjištěných dat, tedy se např. procentuální podíl vypočítává bez zahrnutí obviněných, jejichž data v dané oblasti chybí.

Graf 11: Věkové rozložení obviněných (n=68)



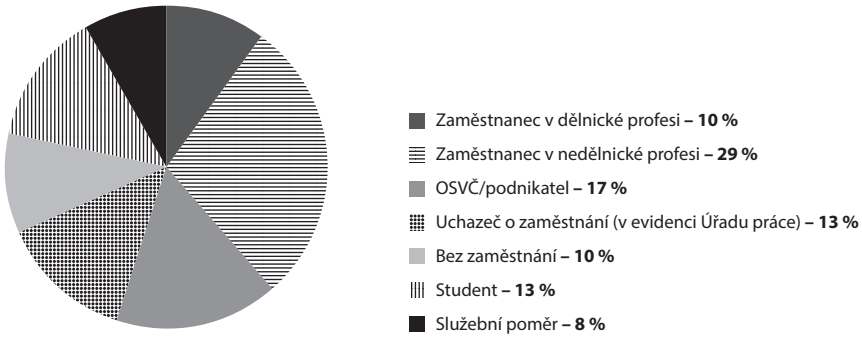
Až na dvě výjimky ze Slovenska se hlásili všichni obvinění k české národnosti. Polovina obviněných (n=33) byla svobodná, 5 osob žilo v družském poměru. Několik obviněných bylo rozvedených (n=9), necelá třetina žila v manželském svazku (n=19), viz graf 12.

Graf 12: Rodinný status obviněných (n=67)



Dále jsme se zajímali o socioprofesní status pachatelů. Nejpočetněji jsou zastoupeni pachatelé v zaměstnaneckém poměru v nedělnických profesích, kteří tvořili téměř třetinu našeho vzorku. Více než pětina pachatelů byla nezaměstnaných. Jistě není zcela bez zajímavosti, že pět pachatelů bylo v době spáchání trestného činu ve služebním poměru u Policie ČR. Deset obviněných bylo v postavení úřední osoby, viz graf 13 a tabulka 9.

Graf 13: Socioprofesní status obviněných (n=67)



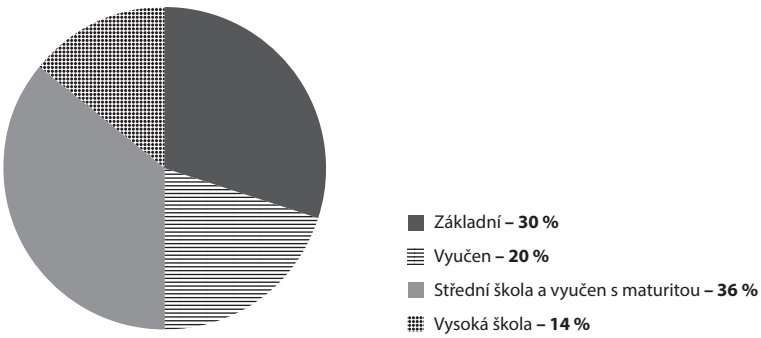
Tabulka 9: Socioprofesní status obviněných (n=67)

	Počet	Podíl (%)
Zaměstnanec v dělnické profesi	7	10
Zaměstnanec v nedělnické profesi	19	28
OSVČ / podnikatel	11	16
Uchazeč o zaměstnání (v evidenci Úřadu práce)	9	13
Bez zaměstnání	7	10
Student	9	13
Služební poměr	5	7
Nezjištěno	1	1
Celkem	**68**	**100**

Měsíční příjem obviněných v době páchání trestné činnosti se nám podařilo zjistit u necelých dvou třetin pachatelů (64,7 %, n=56), včetně 11 osob, které uvedly, že žádný příjem nemají.[115] Pohyboval se od 1 000 Kč do 47 000 Kč, v průměru přibližně 15 000 Kč (medián 14 000 Kč). Co se týče samotných zaměstnanců a OSVČ/podnikatelů, 81 % své příjmy uvedlo, a to ve výši od 4 000 Kč (s průměrnou výší přibližně 17 500 Kč), přičemž většina z nich (83 %) nepřesáhla 25 000 Kč.

Spisy obsahovaly informaci o nejvyšším dosaženém vzdělání u 64 obviněných. Nejvíce jich absolvovalo střední školu či učební obor s maturitou (23 osob). Na pomyslné druhé příčce se pak umístilo 19 obviněných se základním vzděláním. Téměř pětina obviněných absolvovala učební obory bez maturity. Nejméně zastoupenou skupinu tvořilo 9 vysokoškolsky vzdělaných obviněných, viz graf 14.

Graf 14: Nejvyšší dosažené vzdělání obviněných (n=64)



V téměř dvou třetinách případů nebyl obviněný dosud pravomocně odsouzen (n=42), viz tabulka 10. Ze zbývajících 25 dříve trestaných obviněných jich 7 bylo odsouzených pouze jednou, zatímco ti zbývající již několikrát. Mezi pomyslné rekordmany lze v rámci našeho vzorku zařadit dva pachatele, z nichž jeden byl v minulosti odsouzen již třináctkrát

115 Někteří pouze uvedli, že si přivydělávají brigádně (bez uvedení konkrétní výše výdělku).

a druhý jedenáctkrát. Nutno však podotknout, že mezi recidivisty byli pouze dva trestaní pro počítačové trestné činy. Bezesporu zajímavým se jeví zjištění, že trestná činnost obou těchto pachatelů vykazuje téměř shodný modus operandi. V obou případech se jednalo o neoprávněný přístup do cizích e-mailových schránek a následné zneužití m-plateb za pomoci mobilních telefonů a sociálních sítí. U jednoho z pachatelů nebylo jeho případnou kriminální minulost možno zjistit, neboť trestní spis neobsahoval opis z rejstříku trestů.

Tabulka 10: Kolikrát byl pachatel v minulosti pravomocně odsouzen

	Počet	Podíl (%)	Podíl v rámci zjištěných (%)
Ani jednou	42	61,8	62,7
Jednou	7	10,3	10,4
Víckrát než jednou	18	26,5	26,9
Celkem zjištěno	**67**	**98,5**	**100**
Nezjištěno	1	1,5	
Celkem	**68**	**100**	

III.5.1. Obviněné ženy[116]

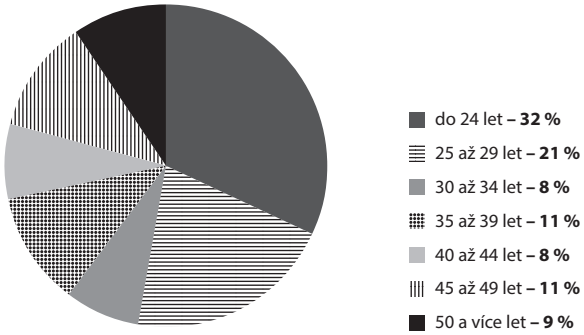
Skladba obviněných dle pohlaví se v rámci kriminality jako takové poněkud vymyká, neboť ženy (n=15) představují 22 % oproti běžným 12-15 % (Gřivna, a další, 2015, str. 97). Bylo by předčasné vytvářet na základě tak malého souboru dat teorie o tom, proč tomu tak je, jedním z faktorů však může být charakter kybernetické kriminality s předmětem útoku v podobě „počítačového systému nebo jeho části, nosiči informací… programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat" (Novotný, a další, 2010, str. 210). 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).

Přispět mohl také fakt, že byť hovoříme o takzvané kybernetické kriminalitě nebo počítačových trestných činech, jde o jednání ve většině případů v zásadě bez zvláštních požadavků na technické znalosti či schopnosti.[117] Jádro jednání u většiny skutků spadajících pod § 230 TZ nespočívá v technologiích jako takových (např. vytvoření malwaru, odposlech zařízení, prolamovač hesel atp.), nýbrž v běžných mezilidských interakcích, pro které technologie pouze nabízí jiné prostředí a propůjčuje jim určitou formu, zatímco sama podstata zůstává beze změny (např. neoprávněný přístup a využití e-mailové schránky díky prostému uhádnutí hesla).

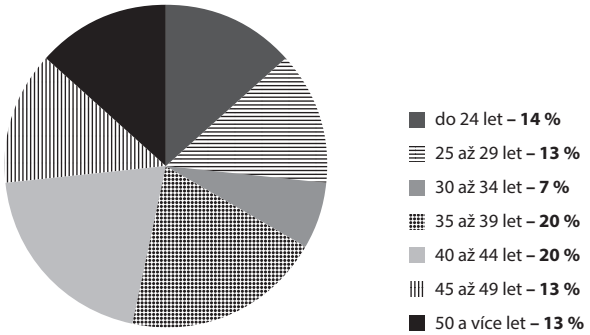
116 Žádný z uvedených rozdílů není statisticky signifikantní.

117 Nutno ovšem zdůraznit, že zjištěná data žádným způsobem nevypovídají o latentní kriminalitě, jejíž míra je pravděpodobně značná (Smejkal, 2015, str. 498; Gřivna, a další, 2014, str. 337).

Graf 15: Věkové složení obviněných mužů (n=53)

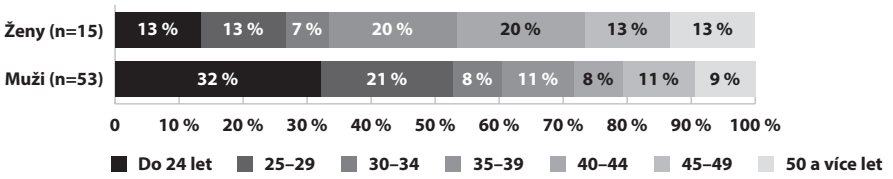


Graf 16: Věkové složení obviněných žen (n=15)



Věkově se obvinění muži a ženy v souhrnu pohybovali nejčastěji do 29 let, viz graf 11, ovšem při rozlišení obou pohlaví se jejich rozložení částečně liší, neboť průměrný věk obviněných žen se oproti obviněným mužům zvyšuje, převážně na věkovou skupinu 35-49 let (53 %), viz grafy 15 a 16. Ženy se pohybují ve věkovém rozmezí od 19 do 56 let, v průměru je jim 38 let – oproti mužům (průměrný věk 32 let) jsou tedy o něco starší, viz graf 17. Vysvětlení odlišností opět spočívá s největší pravděpodobností ve specifickém charakteru kybernetické kriminality (resp. zde počítačových trestních činů), ovšem stále s výhradou malého vzorku a statisticky nevýznamného počtu.[118]

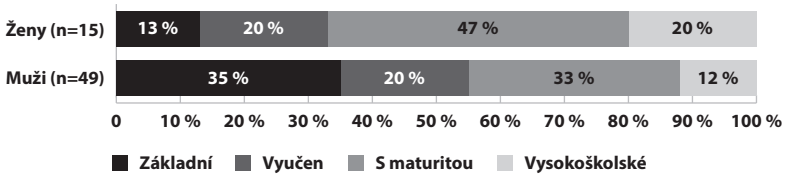
Graf 17: Rozložení obviněných mužů a žen podle věku (n=68)



118 A zde snad ještě více, neboť jednotlivé věkové kategorie zastupuje vždy pouze několik osob.

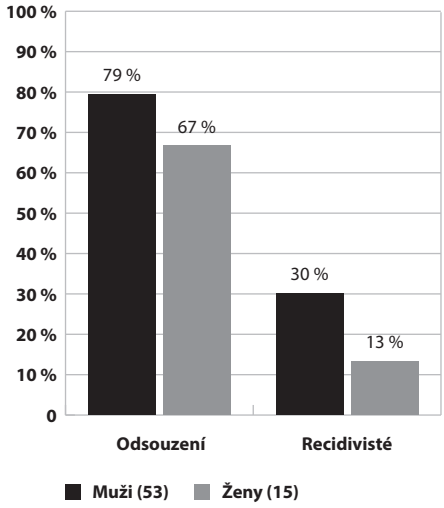
Pachatelky jsou také erudovanější – dvě třetiny mají alespoň maturitu, oproti mužům, u nichž je více než polovina méně vzdělaná, viz graf 18.[119]

Graf 18: Nejvyšší dosažené vzdělání obviněných (n=64)



Ve dvou případech soud obviněné zprostil obžaloby, u dalších dvou schválil narovnání (§ 309 TŘ) a jedné řízení zastavil dle § 172 odst. 2 TŘ (fakultativní zastavení trestního stíhání). Zbylým dvěma třetinám pachatelek soud uložil většinou trest odnětí svobody v rozsahu 0,5–3 roky (v průměru 1,4 roku, n=8), který podmíněně odložil na zkušební dobu 1–5 let (v průměru 2,6 roku).[120] K nepodmíněnému trestu odnětí svobody soud odsoudil jedinou pachatelku, a to na dobu 9,5 roku, přičemž se jedná za rok 2015 o nejpřísněji hodnocený případ.[121] Jednu ženu soud potrestal trestem obecně prospěšných prací (150 hodin). Třem pachatelkám soud také jako vedlejší trest zakázal nějakou činnost (dle § 73 TZ). Poměrově bylo odsouzeno o něco méně žen než mužů, viz graf 19. Na druhou stranu průměrná výše podmíněného trestu byla u pachatelek o 5 měsíců delší než při trestání mužů. S trestnou činností mají recidivní zkušenost pouze 2 pachatelky, na rozdíl od mužů, u nichž je třetinový podíl recidivistů, viz graf 19.

Graf 19: Souhrnný graf rozložení mužů a žen – odsouzení a recidiva



119 Částečně to může být ovlivněno vyšším věkem pachatelek, blíže k tomu viz Mladší a starší obvinění.

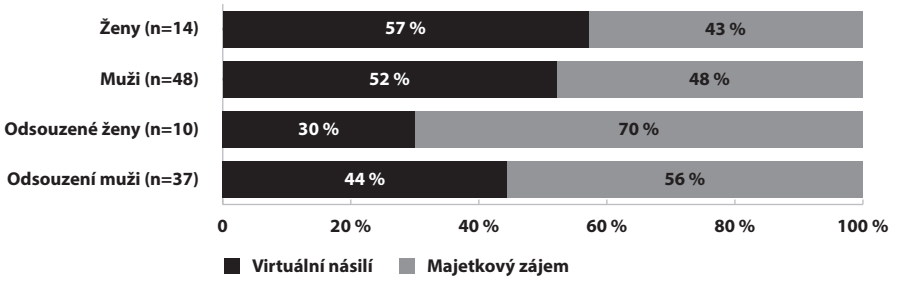
120 Těchto 10 pachatelek představuje 19 % z celkového počtu odsouzených (n=52).

121 Nutno podotknout, že soud zde ukládal úhrnný trest za souběh s neoprávněným opatřením, padělaním a pozměněním platebního prostředku a úvěrovým podvodem.

Odsouzené pachatelky byly v průměru o 2 roky mladší než celková skupina obviněných žen. Většina dosáhla alespoň středoškolského vzdělání (7 z 10). Poměr zaměstnaných k nezaměstnaným činil 6 ku 4, nicméně nezaměstnané tvořila mladší skupina žen do 30 let.[122] Většina žila v partnerském (manželském či družském) vztahu.[123]

Pokud se zaměříme na motivaci trestné činnosti,[124] u všech obviněných mužů i žen mírně převažuje virtuální násilí oproti majetkovému zájmu, viz graf 20.[125] U odsouzených je tendence opačná, přičemž u žen je rozdíl výrazný - 70 % odsouzených kauz bylo motivováno majetkovým zájmem. Tyto pachatelky většinou útočily na jedinou oběť. V polovině případů útočily obviněné primárně na svého zaměstnavatele, ostatní pak na někoho ze svého blízkého okolí. Počet útoků a výše napáchané škody se pohybují ve značném rozpětí od 2 do 234 zamýšlených útoků s celkovou škodou od 30 800 Kč až po necelých 27 milionů korun, přičemž milionových podvodů se dopustily tři ženy.

Graf 20: Rozložení (odsouzených) mužů a žen podle typu útoku



Většina obviněných (n=8) se dopustila trestného jednání v souběhu s další trestnou činností. Kromě nejzávažnějšího případu, který byl řešen 3,5 roku, byly všechny uzavřeny do 2 let, přičemž délka přípravného řízení byla v průměru o polovinu delší než délka řízení před soudem.

III.5.2. Mladší a starší obvinění

Obviněné dělí na téměř přesné poloviny věková kategorie rozlišující mladší (do 30 let, 47 %) a starší jedince (nad 30 let, 53 %). Tyto dvě skupiny jsou sociodemograficky poměrně značně odlišné (nepřekvapivě). Více než polovina mladších obviněných (55 %, viz graf

122 Průměrná mzda oněch 11 obviněných, které byly při zahájení trestního stíhání zaměstnané či osobami samostatně výdělečně činnými, činila necelých 18 000 Kč.

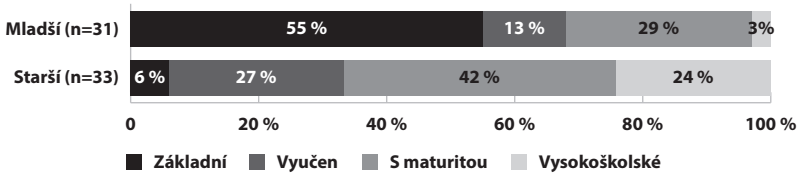
123 Konkrétně bylo 10 obviněných v partnerském vztahu, 2 svobodné a 3 rozvedené.

124 Blíže k tomu viz Ke spáchanému skutku, zejména Členění na virtuální násilí a majetkový zájem.

125 Graf zobrazuje údaje o 62 obviněných – bez jedné obviněné, jejíž trestní stíhání bylo podmíněně zastaveno dle § 307 TŘ, a pěti odsouzených mužů, jejichž jednání nespadá do kategorie majetkového zájmu ani virtuálního násilí.

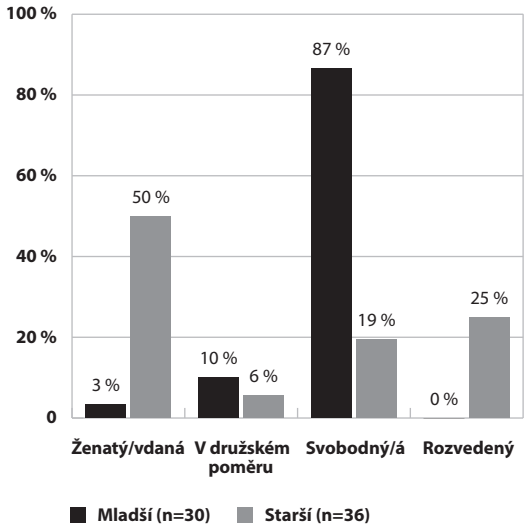
21) měla v době relevantního trestního řízení pouze základní vzdělání[126] - většina z nich stále ještě studovala, byla nezaměstnaná nebo pracovala jako brigádníci. To se projevovalo i na jejich průměrném přijmu, který se pohyboval okolo 8 000 Kč (u 4 jedinců nezjištěno), oproti starším obviněným, kteří pobírali v průměru 17 000 Kč (nezjištěno u 9 jedinců).

Graf 21: Struktura dosaženého vzdělání mladších a starších obviněných



Podle očekávání převažují mezi mladšími obviněnými svobodní (87 %), u starších pak osoby v manželském či obdobném poměru (56 %) nebo rozvedené (25 %), viz graf 22.

Graf 22: Rozložení mladších a starších obviněných podle rodinného stavu

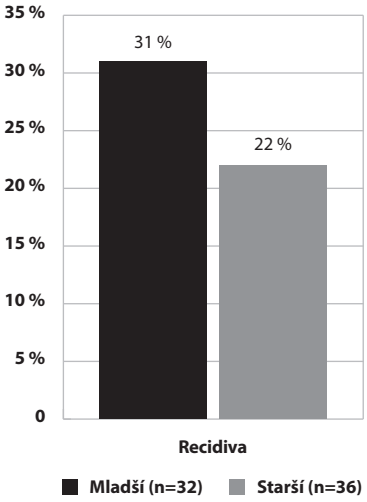


Překvapivý se však může zdát třetinový podíl recidivistů (31 %) mezi mladšími obviněnými a pětinový mezi staršími (22 %), viz graf 23. Mezi mladšími obviněnými je tedy recidivistů znatelně více, což lze u počítačových trestných činů na rozdíl od kriminality jako takové do jisté míry vysvětlit jejich přirozeným pohybem v prostředí kyberprostoru. Překvapivý je však jejich podíl zejména s ohledem na to, že na celkové kriminalitě se v roce 2015 podíleli recidivisté zhruba v polovině případů (52 %), tedy výrazně častěji. Zdá se, že počítačových trestných činů se častěji než jiných typů kriminality dopouštějí

126 Existuje statisticky významná tendence, že ve skupině mladších pachatelů jsou spíše méně vzdělaní jedinci (základní vzdělání a bez maturity) a naopak starší pachatelé jsou spíše vzdělanější (s maturitou a vyšší vzdělání). Vztah byl testován 2x2 kontingenční tabulkou chí-kvadrát testem dobré shody s hodnotou p=0,006 a koeficientem kontingence=0,325.

prvopachatelé.[127] Nabízí se několik úvah, proč tomu tak je: počítačové trestné činy nejsou společností odsuzovány tak jako jiná kriminalita (tudíž není takový sociální tlak odrazující od jejich páchání), škoda (ať už v podobě finanční škody nebo nemajetkové újmy) nemusí být patrná (např. „pouhý" neoprávněný přístup do nějakého systému), specifika kyberprostoru poskytují (domnělou) anonymitu a beztrestnost, dopustit se počítačového trestného činu nevyžaduje prakticky žádné zvláštní vlastnosti či odhodlání (např. uhodnutí hesla oproti vlastnoruční krádeži v obchodě) atd. Stále však jde o pouhé domněnky, které budou předmětem bližšího zkoumání v dalších letech.

Graf 23: Rozložení mladších a starších obviněných podle recidivy[128]

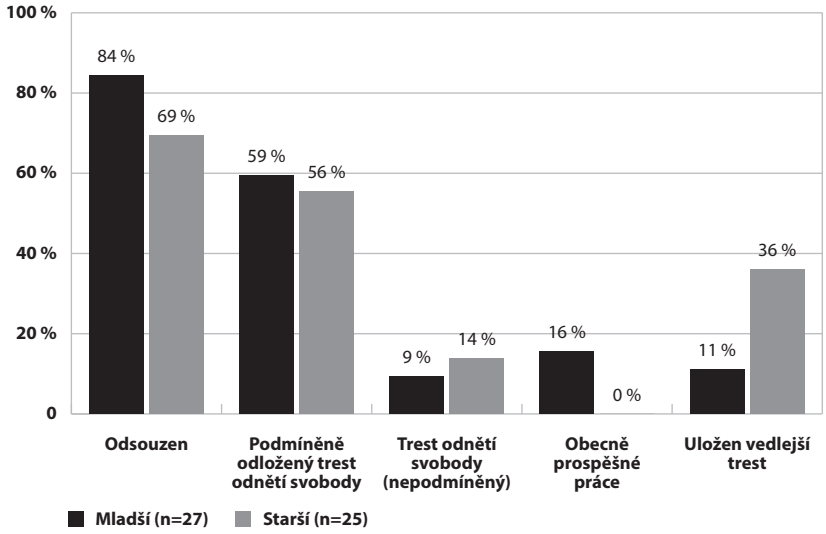


Při rozdělení trestné činnosti na virtuální násilí a majetkový zájem není patrný mezi oběma věkovými kategoriemi žádný zásadní rozdíl: o něco více než polovinu jednání motivoval majetkový zájem, o něco méně než polovinu pak virtuální násilí. Pokud byla způsobena finanční škoda, tak se u mladších obviněných pohybovala v rozmezí 12–700 tisíc korun (v průměru okolo 175 tisíc korun), nicméně jejich záměr byl v průměru o více než polovinu vyšší. Starší obvinění působili podstatě vyšší škody, a to od 5 000 Kč do necelých 27 milionů korun (průměrně přes 3 miliony korun). Při odebrání nejvyšší způsobené škody se průměr snížil na necelých 750 tisíc korun. Pokud byl zjištěn záměr, pak téměř pokaždé obvinění dosáhli svého cíle.

127 Nutno ovšem podotknout, že existuje hned několik statistik referujících o „recidivě", každá ovšem z jiného úhlu pohledu. Onen poloviční podíl recidivistů vychází z policejní statistiky kriminality a jde o stíhané či vyšetřované osoby v roce 2015 (Ministerstvo vnitra). Justiční statistiky pracují naproti tomu s pojmem „recidiva" ve smyslu recidivistů označených tak soudem v rámci daného trestního řízení (soud přihlédl k faktu, že obviněný je recidivistou), a jsou proto v tomto směru nepoužitelné - podíl takovýchto „recidivistů" označených v rámci trestních řízení pravomocně skončených v roce 2015 se pohybuje v pouhých jednotkách procent. Blíže k této problematice viz např. (Rozum, a další, 2016).

128 Graf zobrazuje, kolik obviněných bylo v každé z kategorií (zde mladší a starší obvinění) již dříve odsouzeno pro nějaký trestný čin.

Graf 24: Rozložení mladších a starších pachatelů podle odsouzení



Odsouzeno bylo více mladších pachatelů, viz graf 24.[129] Lze vyslovit tezi, že tomu bylo částečně díky ukládání trestu obecně prospěšných prací, ke kterému sáhli soudci právě v případech mladších odsouzených.[130] Je pravděpodobné, že v těchto kauzách, které se spíše podobaly kyberšikaně, volili soudci obecně prospěšné práce z důvodu prevence, odstrašení mladších pachatelů před další trestnou činností. Mezi některými kauzami starších souzených lze totiž pozorovat podobné vzorce, nicméně v jejich případech k odsouzení nedošlo.[131] Na druhou stranu starším pachatelům byl výrazně častěji uložen vedlejší trest, a to především zákaz činnosti v souvislosti se spáchaným skutkem.

III.5.3. Vzdělaní a méně vzdělaní obvinění

Soubor obviněných se dělí podle výše vzdělání přesně na dvě poloviny, tj. na 32 a 32 osob.[132] Jednu skupinu představují ti, kdo dosud dokončili pouze základní školu nebo byli vyučeni bez maturity. Druhou pak osoby, které složily maturitu nebo dosáhly vyššího vzdělání.

III.5.3.1. Méně vzdělaní obvinění

Obviněných s pouze základním vzděláním (včetně dvou žen) je v rámci této skupiny o něco více (59 %, n=19) než vyučených bez maturity (41 %). Jsou převážně svobodní a výrazně mladší (průměrně 24,2 roku s rozptylem 17-54 let oproti vyučeným s průměrným

129 Podíl odsouzených pachatelů vychází z celkového počtu mladších (n=32) a starších (n=36) obviněných. Zbytek údajů je počítán již jen ze skupiny odsouzených, tzn. ze skupiny 27 mladších pachatelů a skupiny 25 starších pachatelů.

130 Blíže k tomu viz Odsouzení k obecně prospěšným pracím.

131 (Ne)odsouzení v souvislosti s trestnou činností na hraně kyberšikany ve spojení s věkem obviněných představuje jedno z mnoha témat, která budou při sběru dalších dat jistě stát za pozornost.

132 Údaj o nejvyšším dosaženém vzdělání se u 4 obviněných nepodařilo dohledat.

věkem 36,7 roku při rozptylu 25-56 let), což ovšem naznačuje, že jejich celoživotní vzdělávání ještě nemuselo být dokončeno. To potvrzuje i fakt, že se většinou jedná o studenty, nezaměstnané či brigádníky s případným příjmem do 10 tisíc korun měsíčně.

Obvinění ve skupině osob vyučených bez maturity (včetně 3 žen) zde pravděpodobně zůstanou i nadále. Většinou se již zařadili na pracovní trh (převážně jako zaměstnanci či osoby samostatně výdělečně činné), a pokud byl zjištěn jejich plat, pak se v průměru pohyboval okolo 12 tisíc korun měsíčně.

Přibližně polovina méně vzdělaných obviněných má již předchozí zkušenost s trestnou činností (10 osob se základním vzděláním a 7 osob vyučených bez maturity), a to většinou recidivně.

Podle motivace útoku se případy méně vzdělaných obviněných dělí opět na dvě poloviny. Ty s majetkovým zájmem (n=15) většinou proběhly v souběhu s další trestnou činností (n=11). Oběťmi se stali především rodina a známí pachatelů (n=8), 4 poškození neměli vůči pachateli žádný vztah a 3 poškození jej zaměstnávali. Pokud byla způsobena škoda, tak ve výši od 1 200 Kč po necelé tři miliony korun (v průměru přibližně 350 tisíc korun). Trestní řízení trvalo v průměru 1,8 roku, přičemž o něco převažovala délka přípravného řízení (jeden rok oproti 0,8 roku řízení před soudem). Pouze dva odsouzení požádali o opravný prostředek, z toho jeden dosáhl zproštění obžaloby. Většina pachatelů byla odsouzena (n=11), a to nejčastěji k podmíněně odloženému trestu odnětí svobody v délce 0,5-1,5 roku (průměrně 1 rok), ve čtyřech případech pak nepodmíněně v délce 1,5-3,8 roku (průměrně na 2,9 roku).

K virtuálnímu násilí (n=16) v souběhu s další trestnou činností došlo pouze v polovině věcí (n=8). Oběti byly až na jeden případ vždy z blízkého kruhu pachatele. K finanční škodě v těchto kauzách na rozdíl od nemajetkové újmy nedošlo. Kromě psychických obtíží se oběti musely často vypořádávat se zamezením přístupu k účtu či napadené technologii, případně došlo k online poškození v podobě vymazání dat. Trestní řízení bylo průměrně o polovinu kratší než u majetkově motivovaných činů (0,9 roku), výrazně déle trvalo přípravné řízení (0,6 roku oproti stadiu před soudem trvajícímu 0,3 roku). I v těchto případech podali dva odsouzení opravný prostředek, z toho jednoho soud následně zprostil obžaloby. Většině odsouzených pachatelů soud uložil podmíněně odložený trest odnětí svobody v délce 0,3-2,3 roku (v průměru 0,8 roku), jednomu nepodmíněný v délce 0,7 roku, čtyřem pachatelům pak trest obecně prospěšných prací v rozmezí 30-200 hodin (v průměru 133 hodin).

III.5.3.2. Vzdělanější obvinění

Zhruba třetinu vzdělanějších obviněných tvořily ženy (34 %). Bez ohledu na pohlaví převažovaly oproti těm vysokoškolsky vzdělaným (28 %) osoby, které dosáhly zatím nejvýše maturity (72 %). Věkový průměr středoškolsky vzdělaných (35,4 roku s rozptylem 20-51 let) je podobný jako u obviněných vyučených bez maturity, a zároveň poměrně nižší než u vysokoškolsky vzdělaných (43,1 roku s rozptylem 22-58 let). Obvinění měli téměř vždy zaměstnání (případně živnost) a jejich průměrný příjem se pohyboval okolo 18 tisíc korun.

Oproti předchozí kategorii méně vzdělaných obviněných je zde menší podíl osob s dřívější zkušeností s trestnou činností (22 %, n=7), z toho pouze u tří recidivně (mezi vysokoškolsky vzdělanými byli dokonce všichni doposud bezúhonní).

Zastoupení případů podle rozdělení motivace na virtuální násilí a majetkový zájem bylo poměrně rovnoměrné (44 % majetkový zájem a 41 % virtuální násilí), nicméně se zde objevilo i pět nezařazených případů (16 %). Zahrnovaly neoprávněný přístup k bankovnímu účtu a sdělení zůstatku třetí osobě zaměstnancem banky, zneužití policejního informačního systému k vlastní obhajobě, neoprávněnou změnu údajů v databázi bývalého zaměstnavatele ve snaze ochránit své klienty, šíření poplašné zprávy prostřednictvím napadené Wi-Fi a nakonec opakovaný neoprávněný přístup do informačního systému Ministerstva vnitra.

Případy s majetkovým zájmem byly většinou spáchány v pracovním prostředí obviněného a v souběhu s další trestnou činností. Zjištěná škoda se pohybovala v rozmezí necelých 9 tisíc až po téměř 27 milionů korun. Často byla zjištěna i nemajetková újma, a to v podobě narušení důvěryhodnosti poškozeného subjektu. Délka trestního řízení se v průměru pohybovala okolo 2 let s vyrovnanou délkou přípravného řízení a řízení před soudem, přičemž necelá polovina obviněných využila řádný opravný prostředek. Čtyři obviněné soud zprostil obžaloby, ostatním uložil podmíněně odložený trest odnětí svobody v délce 0,3-3 roky (průměrně 1,5 roku), až na jednu pachatelku s nepodmíněným trestem odnětí svobody v délce 9,5 roku.

Virtuální násilí bylo také většinou doplněno další trestnou činností, převážně však na obětech z blízkého okolí pachatele. Až na jeden případ nedošlo k finanční škodě, nicméně vždy byla zaznamenána nemajetková újma, a to především psychického rázu. Délka trestního řízení trvala v průměru 1,4 roku s o něco delším trváním přípravného řízení (0,8 roku) oproti řízení před soudem (0,6 roku), přičemž 5 odsouzených využilo řádný opravný prostředek. Čtyři obviněné soud zprostil obžaloby, většinu však odsoudil a uložil jim podmíněně odložený trest odnětí svobody v délce 0,3-3 roky (v průměru 1,2 roku). Jednomu z odsouzených pachatelů uložil trest odnětí svobody v délce 2,5 roku nepodmíněně a jednomu 150 hodin trest obecně prospěšných prací.

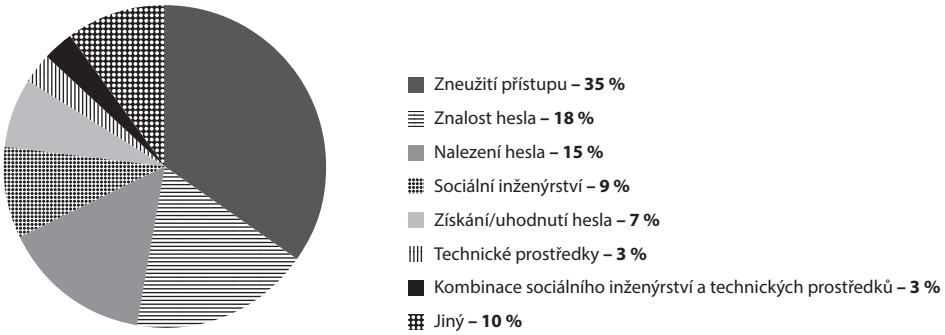
III.6. Ke spáchanému skutku

K nejzajímavějším částem sběru dat patřily údaje o samotném skutku. Sledovali jsme v prvé řadě způsob jeho spáchání, tedy zda dotyčný využil sociální inženýrství (manipulaci uživatele s cílem přimět ho k určitému jednání či naopak k pasivitě), technické prostředky (např. softwarový prolamovač hesel) nebo kombinaci obojího. Zajímalo nás, jaké prostředky obvinění pro svou trestnou činnost využívali, a to zejména e-mail, Facebook nebo jinou sociální síť či SMS. Pozornost jsme věnovali také zneužití osobních údajů (typicky přihlašovací údaje poškozených) a použitým zařízením (stolní počítač/notebook,[133] mobilní telefon či jiné). Zvláštní pozornost si oproti původnímu očekávání vynutilo sledování primárního cíle útoku (osobnost či konkrétněji osobní údaje, dále majetek a jiné) a výslovně uvedené

133 Analýza potvrdila náš předpoklad, že orgány činné v trestním řízení nebudou až na výjimečné případy rozlišovat mezi použitím stolního počítače a notebooku.

motivy trestného činu, neboť tyto kategorie získaly výrazně větší vypovídací hodnotu v okamžiku jejich transformace do jedné skupiny rozlišující virtuální násilí a druhé majetkový zájem (a třetí skupiny jiné).[134] V rámci údajů o skutku jsme zaznamenávali také údaje o poškozeném subjektu (zda byl uveden, zda šlo o fyzickou či právnickou osobu nebo obojí a jaký byl počet poškozených) a počtu zjištěných útoků (dokonaných i ve stádiu pokusu). Posledním, nikoliv však nepodstatným indikátorem byla výše škody (způsobené i zamýšlené) a nemajetková újma, pokud je orgány činné v trestním řízení zaznamenaly.[135]

Graf 25: Způsob spáchání (n=68)

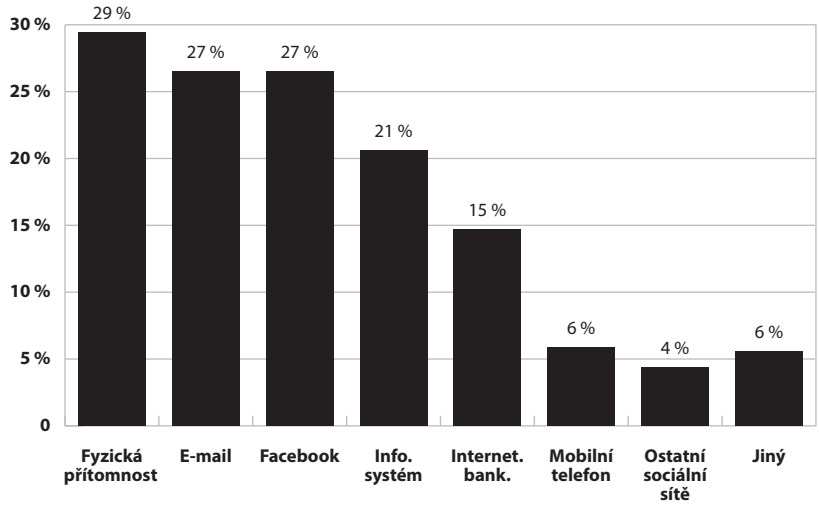


Největší podíl souzené trestné činnosti (35 %, viz graf 25) připadá na zneužití přístupu k informačním technologiím. Jednání umožnil obviněným zpravidla pracovní vztah (přístup k databázím, k informačním systémům či know-how) nebo přátelská důvěra (povolení přístupu do počítače, telefonu atp.). Další častější způsob spáchání představuje znalost cizích přihlašovacích údajů (18 %), od přihlášení se do počítače přes účet na sociálních sítích či e-mailu až po bankovní účty. Podobně časté (15 %) je také nalezení hesla buď přímo v počítači či telefonu (automatické přihlašování) nebo fyzicky zaznamenaného offline (např. na papírku v bytě nalezené spolubydlícím). Naopak méně zastoupené jsou složitější techniky jako sociální inženýrství (9 %), jiný způsob získání či uhodnutí hesla (7 %), páchání skrze technické prostředky prolomení zabezpečení (3 %) a kombinace sociálního inženýrství a technických prostředků (3 %).

134 Primární cíl útoku a motivace se nemusí nutně vzájemně překrývat, neboť motivace vypovídá o vnitřním vztahu pachatele vůči danému jednání či jeho následkům, kdežto primární cíl útoku o dopadu jeho jednání ve vnějším, reálném světě. Navzdory tomu se zdá, že jejich seskupení do jediné kategorie umožňuje lepší porozumění. Blíže k tomu viz Členění na virtuální násilí a majetkový zájem.

135 O řadě údajů z této oblasti (spáchaný skutek) se již hovoří v rámci jiných kapitol (např. výše škod spáchaných obviněnými ženami v kapitole Obviněné ženy atp.).

Graf 26: Komunikační kanál (n=68)



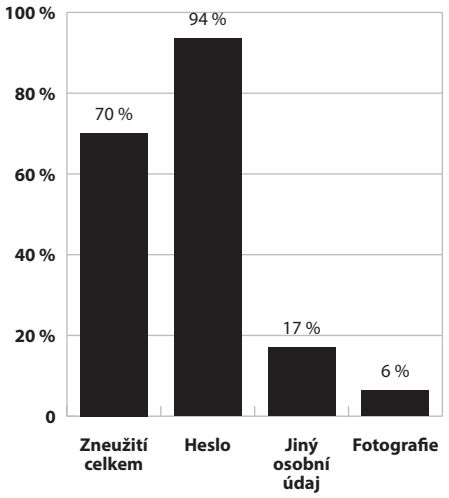
Obvinění využili k páchání trestné činnosti většinou počítač (85 %), dále pak mobilní telefon (15 %) a v 6 případech jiný prostředek (tablet, platební karta, výherní automat). Naproti tomu vybrané sledované komunikační kanály byly zastoupeny poměrně vyrovnaně, a to fyzická přítomnost u konkrétního zařízení (29 %), e-mail (27 %) a sociální síť Facebook (27 %), viz graf 26. Dále měli obvinění poměrně často zneužít různé informační systémy (21 %) a internetové bankovnictví (15 %).[136] Ke skutkům spáchaným prostřednictvím mobilního telefonu mělo dojít spíše výjimečně (6 %),[137] podobně k použití jiné sociální sítě než Facebook (4 %).[138]

136 Některá jednání využívala komunikačních kanálů vícero.

137 Aniž by sloužil mobilní telefon coby kapesní počítač umožňující např. přístup k internetu, v úvahu tak přichází např. zasílání výhružných SMS či žádost o přeposlání potvrzovací SMS atp.

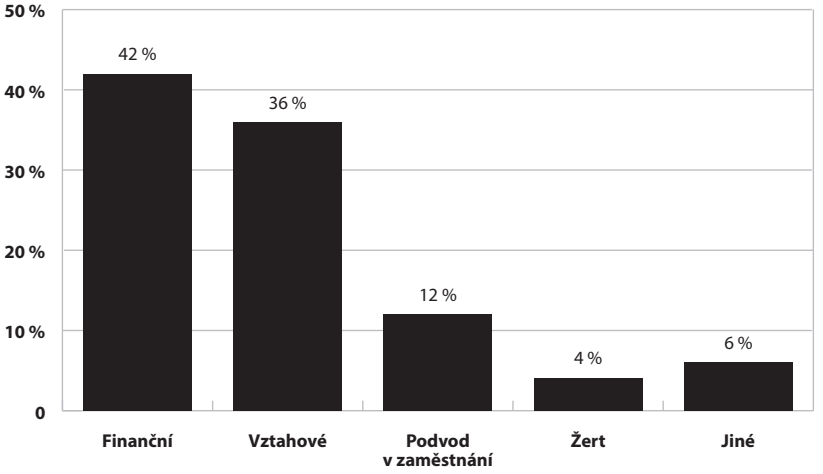
138 Např. dnes již neexistující sociální sítě Spolužáci.

Graf 27: Zneužití osobních údajů (n=47)



Ke zneužití osobních údajů došlo ve více jak dvou třetinách případů (70 %), viz graf 27.[139] V naprosté většině se jednalo o zneužití přihlašovacích údajů (94 %), méně často pak o zneužívání jiné informace (17 %). Osobní údaje vizuálního charakteru (intimní fotografie) se vyskytly pouze ve 3 případech.

Graf 28: Uvedené motivy (n=50)



Případy se celkem rovnoměrně dělí na ty s majetkovým zájmem (53 %) a na virtuální násilí (47 %). Do toho však nepočítáme šest skutků, které nespadají do žádné z těchto kategorií. Motivy ke spáchání trestné činnosti byly výslovně uvedeny v necelých třech čtvrtinách případů (74 %). Za zmínku stojí finanční přilepšení (42 %) či komplikovaná

139 Sloupec „zneužití celkem" vychází z celkového počtu obviněných (n=68), ostatní případy pak odpovídají podílu v rámci zneužití osobních údajů.

vztahová situace (především v partnerském či ex-partnerském kontextu, 36 %), viz graf 28. Méně často se pak vyskytují podvody v souvislosti s pracovní sférou (zneužití databází pro osobní účely nebo vykrádání know-how pro vlastní podnikání atp., 12 %). Ve dvou případech se jednalo pouze o nepovedený žert.

III.6.1. Členění na virtuální násilí a majetkový zájem

Jak je uvedeno výše,[140] při aplikaci na data získaná analýzou trestních spisů vystoupily do popředí dvě poměrně vyrovnané oblasti, a to majetková sféra (33 obviněných) a virtuální násilí (29 obviněných), přičemž většinu sledovaných jednání spadajících pod počítačové trestné činy lze zařadit do jedné či druhé (zbytková kategorie ostatních jednání zahrnuje všeho všudy 6 obviněných). V rámci virtuálního násilí směřovalo 15 útoků na e-mailovou schránku poškozených, 13 útoků na jejich profil na Facebooku.[141]

Ukázkou typického jednání zasahujícího do **majetkové sféry** budiž např. pachatel, který našel vytištěné přihlašovací údaje do internetového bankovnictví své spolubydlící a následně uzavřel jejím jménem ve svůj prospěch 7 úvěrových smluv (tyto a další peníze následně neoprávněně vybral platební kartou nalezenou tamtéž). Naproti tomu se objevilo i několik méně zřejmých kauz, např. neoprávněný přístup do informačního systému Policie ČR ze strany jejího příslušníka. Ten zjišťoval informace o společnosti, s níž vedla jeho dcera pracovněprávní spor. Proti zařazení této věci do majetkové sféry lze namítnout, že pachatel tak činil nikoliv za účelem vlastního obohacení nebo v úmyslu způsobit jinému škodu, nýbrž v zájmu své dcery, avšak dané informace měly patrně sloužit k ukončení onoho pracovněprávního sporu ve prospěch pachatelovy dcery (v podobě získání ušlé mzdy, neplatnosti výpovědi atp.), s čímž byl pachatel přinejmenším srozuměn.

Kategorie **virtuálního násilí** nemusí být na první pohled zcela srozumitelná, s ohledem na zdánlivý oxymóron spočívající v sousloví „virtuální násilí". O specifickém násilí však nepochybně hovořit lze, neboť jde o zraňující jednání, které pouze namísto fyzického dopadu zasahuje psychickou stránku oběti.[142] Způsobuje primárně nemajetkovou újmu, a zároveň nevylučuje ani přidruženou majetkovou škodu.

Jako ukázku virtuálního násilí lze uvést pachatele, který uhodl heslo k e-mailové schránce své bývalé přítelkyně. Intimní fotografie, které zde nalezl, zveřejnil prostřednictvím internetové sociální sítě lidé.cz (de facto online seznamka). To vše pro své zadostiučinění a proto, aby se jí po rozchodu pomstil. Pochopitelně ale i kategorie virtuálního násilí skýtá určitá úskalí. K takovým sporným kauzám patří např. jednání bývalého externího správce sítě, který zneužil své přístupové údaje, které nebyly po ukončení spolupráce změněny. Prostřednictvím vzdáleného přístupu pak překonfiguroval hlavní router, čímž způsobil nefunkčnost firemní počítačové sítě. Při analýze spisu se totiž zdálo, že tak jednal v rámci pomsty za ukončení spolupráce, nebylo však možné jednoznačně vyloučit ani variantu, že tak činil ve snaze učinit se nepostradatelným a pokračovat ve spolupráci (což by poukazovalo naopak na majetkový zájem), případně jinou motivaci.

140 Viz dříve v rámci kapitol Ke spáchanému skutku a Podrobnější vymezení a realizace projektu.

141 V 6 případech pachatel napadl e-mailovou schránku i profil na Facebooku.

142 Nemluvě o případných fyzických dopadech v podobě psychosomatických potíží.

Nakonec zbývá ještě ilustrovat kategorii „**ostatní**". Sem lze zařadit jednání pachatele, který po neoprávněném přístupu k Wi-Fi nejmenované základní školy zaslal jejím prostřednictvím poplašnou zprávu o uložení několika výbušných zařízení v jednom krajském městě do schránky Policejního prezidia (pachatel se smíšenou poruchou osobnosti uvedl, že neví, proč tak učinil). Naopak sporným adeptem byl případ neoprávněného zjištění zůstatku na bankovním účtu a jeho sdělení neoprávněné osobě – tichému společníkovi poškozeného majitele účtu. Na první pohled by se mohlo jednat o zájem v majetkové sféře, nic dalšího však takové motivaci dle spisu nenasvědčovalo.

Je tedy patrné, že ani členění na kategorii majetkového zájmu a virtuálního násilí (a ostatní) není bez vady. Zdá se nicméně, že přinejmenším v hrubých rysech odpovídá realitě českého prostředí co do registrované kriminality posuzované jako počítačové trestné činy. Použitelnost takové kategorizace snad bude možné ověřit v následujících letech, zejména pak oblast „ostatní", která si možná vyžádá podrobnější rozdělení.

Členění na majetkový zájem a virtuální násilí (a ostatní) ovšem není samoúčelné, resp. neslouží pouze k více méně pracovnímu rozdělení sledované materie pro snazší uchopitelnost, jakkoliv už to samo o sobě přináší určitý užitek.[143] Vychází z předpokladu, že s vývojem digitálních technologií a jejich stále se rozšiřujícím spektrem a mírou využívání spolu s nástupem generace tzv. digitálních domorodců (Prensky, 2001, str. 1) dozná změn i kyberkriminalita, resp. její vnímání, jak ukazuje následující část.

Jako digitální domorodce lze zjednodušeně označit ty generace, které rostly již od útlého věku obklopené digitálními technologiemi (mobilními telefony aj.).[144] Představují pro ně tak přirozený svět, včetně vlastní kultury i jazyka.[145] Naproti tomu tzv. digitálním imigrantům, v současnosti stále ještě převážně generaci rodičů digitálních domorodců a starší, nezbývá než se více či méně úspěšně snažit s novým prostředím sžít, podobně jako se imigrant sžívá s novou kulturou.

Vraťme se nyní k již uvedeným kauzám, a to ke zneužití internetového bankovnictví a ke zveřejnění intimních fotografií na sociální síti. Není žádné pochybnosti o tom, že „krádež identity" za účelem majetkového obohacení a především samotná případná finanční škoda rozladí každého poškozeného.[146] V uvedené kauze získal pachatel neoprávněně přístup do internetového bankovnictví své spolubydlící, kde zřídil několik úvěrů jejím jménem. Tyto

143 Podle dosud zjištěných dat se zdá, že bude možné vysledovat i dílčí charakteristiky společné těmto jednotlivým skupinám pachatelů. V rámci analýzy dat z trestních spisů proto zahrnujeme na několika místech i specifika spojená s touto kategorizací.

144 Někdy se používá též označení „generace Z", tj. osoby, které se narodily v období již masového využívání tzv. nových médií.

145 Ve věku 15 let již užívají digitální technologie zcela běžně a samozřejmě, bylo by však mylné považovat je obecně za „digitální guru", neboť informační a komunikační technologie jim slouží spíše k usnadnění, nikoliv nahrazení běžných činností, blíže k tomu viz (Juhaňák, a další, 2019).

146 Hovoříme o použití přihlašovacích údajů někoho jiného a následné jednání jeho jménem a na jeho účet. Nejde proto o „krádež" z hlediska trestního práva, v tomto směru přichází v úvahu zejména poškození cizích práv (§ 181 TZ).

a další peníze následně vybral neoprávněně použitou platební kartou.[147] V tomto případě byla poškozenou osobou zčásti banka (poskytnutí peněz z úvěrových smluv), zčásti majitelka napadeného účtu (ostatní peníze vybrané z účtu). Při napadení internetového bankovnictví pachatelé běžně převádí finanční prostředky jeho prostřednictvím na jiný účet: buď na jiný účet stejného poškozeného (např. takový, ze kterého je mohou vybrat prostřednictvím platební karty, k níž mají taktéž přístup), anebo na svůj vlastní účet. Způsobená škoda tak bývá ve výši úměrné majetkovým poměrům poškozeného majitele účtu.[148] Domníváme se proto, že důsledky napadení internetového bankovnictví může vnímat mladý příležitostný brigádník stejně intenzivně jako postarší bohatý podnikatel, když bude způsobená škoda např. ve výši několikaměsíčního výdělku.[149]

Jiná situace však nastává u zveřejnění intimních fotografií. Zde bude již o poznání více záležet na pohybu poškozené osoby a jejího okolí v online prostředí. Vezměme v úvahu běžného uživatele, který není nijak mediálně exponovanou osobou, ani nevykonává pracovní činnost, která by tím mohla být ohrožena (nejde např. o učitele na základní škole nebo politika). Samotné zveřejnění intimních fotografií představuje jistě nepříjemný zásah do osobní sféry, ať už k němu dojde kdekoliv: na sloupech pouličního osvětlení nebo na sociální síti. Liší se však mírou onoho narušení. Osoba, která není sama na sociálních sítích aktivní a jejíž okolí se v online prostředí také běžně nepohybuje, zřejmě nebude pociťovat zveřejnění zdaleka tak palčivě jako někdo, kdo pečlivě utváří svou online identitu. Mezi digitálními domorodci a digitálními imigranty tak budou v tomto směru velké rozdíly,[150] a to především ze **čtyř následujících důvodů**.

Za prvé, děti (a v menší míře i dospívající, potažmo mladí dospělí) teprve utváří vlastní identitu, skrze vlastní prožívání a prostřednictvím druhých. V reakcích okolí na vlastní jednání zakouší různorodé pocity: úspěch, uznání, respekt atd., ale i jejich protějšky. Jsou nezkušení, důvěřiví a otevření, chybí jim vlastní zkušenost a zkušenost starších je zároveň obtížně přenosná (Brandejsová, a další, 2012). Na sociálních sítích se jim otevírá cesta k prakticky neomezenému množství „přátel", příspěvků a publiku, a tudíž i k obrovskému množství zpětných vazeb, které ovlivňují vlastní sebepojetí, neboť "skrze Tebe vidím sebe".[151] Virtuální prostředí se dotýká člověka přímo, bez fyzické bariéry působí bezprostředně na mysl, emoce, sebepojetí. A tak i zraňující jednání míří přímo do nitra,

147 Celé jednání bylo proto trestněprávně kvalifikováno jako souběh neoprávněného přístupu k počítačovému systému a nosiči informací (přístup a zneužití internetového bankovnictví), úvěrového podvodu (podvodné zřízení několika úvěrů prostřednictvím napadeného internetového bankovnictví), neoprávněného opatření, padělání a pozměnění platebního prostředku (zneužití platební karty) a krádež (nikoliv „krádež identity", nýbrž výběr peněz z bankomatu onou platební kartou).

148 I v případě zjednání (neplatných) úvěrových smluv, kdy je poškozenou osobou banka, vychází jejich výše zpravidla ze stávajících prostředků a finančního pohybu na napadeném účtu.

149 Ponechávám v tuto chvíli stranou případné bezpečnostní opatření spočívající v rozdělení finančních prostředků mezi různé účty tak, aby při napadení jednoho z nich mohl pachatel odčerpat pouze dílčí část spadající pod daný účet.

150 V současnosti lze zařadit mezi digitální domorodce děti, dospívající a mladé dospělé.

151 S určitým nadnesením v buberovském pojetí osoby poznávající sebe samu nahlédnutím do tváře druhého (Buber, 1996).

zejména s ohledem na orientaci dětí a dospívajících na přítomnost. V průběhu socializace (včetně vytváření vlastní identity a vztahu ke společnosti) tak hraje online prostředí významnou roli.

Za druhé, potřeba uznání ze strany ostatních v online prostředí vede k pozornosti věnované vlastní sebeprezentaci. Tzv. digitální „otisk" představuje stopu vlastní osobnosti v online prostředí, zčásti v podobě technických dat,[152] zčásti v podobě informací o konkrétní osobě, počínaje jejími vlastními komentáři na sociálních sítích až po údaje zpracovávané povinně ze zákona.[153] Původcem digitálního otisku je na jedné straně samotný otištěný subjekt, na straně druhé pak ostatní uživatelé a různé instituce a organizace. Vzniká cíleně, ale i nevědomky nebo bez vlastního přičinění subjektu. Jeho podobu utváří nejen to, co prezentuje, ale zároveň i to, co zůstává naopak skryto. Čím více pak jedinec pečuje o vlastní digitální otisk, tím větší dopad na něj může mít jeho deformace např. zveřejněním intimních fotografií.

Za třetí, (nejen) pro digitální domorodce představuje online prostředí významný komunikační prostředek. Zahrnuje komunikaci v rozličných podobách: textovou (např. chat), audio (např. telefonní hovor), vizuální (např. fotografie), audiovizuální (např. videokonference) atd.[154] Případný odklon od online prostředí (např. v důsledku natolik pokřiveného digitálního otisku, že daný jedinec raději z online prostředí zcela ustoupí) tak znamená i významnou překážku, resp. ztížení takové komunikace.[155]

Za čtvrté, podstatnou roli hraje také fakt, do jaké míry se kdo pohybuje v online prostředí vůbec. Pro osobu, která komunikuje se svým okolím převážně mimo online prostředí (např. telefonem či vůbec osobním kontaktem) a nepotřebuje vlastní prezentaci online (jako např. politik) zřejmě nebude narušení digitálního otisku představovat vážnější problém, neboť pravděpodobně ani její referenční skupiny nebudou považovat tuto oblast za významnou. A protože významnou referenční skupinu představují mimo jiné vrstevníci (případně vybraní vrstevníci), u digitálních domorodců si lze online prostředí jen těžko odmyslet.

Troufáme si proto říci, že zatímco v současnosti se někomu může zdát závažnost virtuálního násilí pochybná, časem se s postupně převažujícími digitálními domorodci tato pochybnost zcela rozptýlí. Nikdo jistě nyní nebude znevažovat majetkovou újmu způsobenou v online prostředí, stejně tak jako závažné případy virtuálního násilí jako je kyberšikana, kyberstalking,[156] krádež identity,[157] zveřejnění intimních fotografií atp.

152 Typicky např. provozní a lokalizační údaje nebo cookies.

153 Např. základní registry.

154 Z hlediska socializace hraje roli i možnost svým způsobem jednostranné komunikace, resp. možnost „být slyšen" např. formou online dostupného vlogu.

155 Např. napadení profilu na sociální síti a jeho znepřístupnění znamená i ztrátu navázaných „přátel".

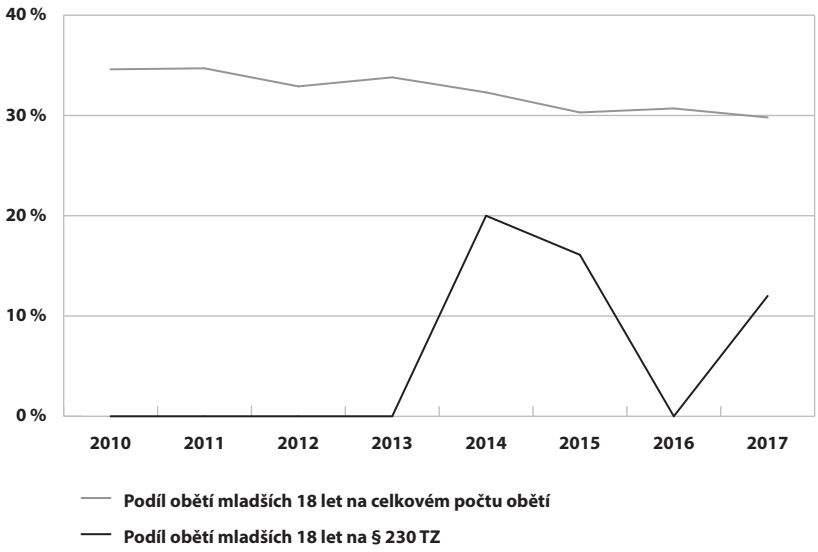
156 Pronásledování prostřednictvím informačních a komunikačních technologií, které dosahuje úrovně nebezpečného pronásledování, tedy když intenzita jednání nabude takové míry, že poškozený se např. cítí ohrožen na životě.

157 Vystupování jménem poškozeného nejen v majetkových vztazích – např. komunikace s nadřízeným v zaměstnání, s vrstevníky atp.

Pro starší generace, digitální imigranty, se však již může zdát sporná újma způsobená ve zdánlivě méně závažných případech, jako např. napadení a následné znepřístupnění profilu na sociální síti bez dalšího.[158] Jednoduše proto, že pro digitální domorodce představuje online prostředí přirozený svět neoddělitelný od toho reálného a napadení jejich osoby v online prostředí významný zásah do soukromí.[159] Záměrně zde ponecháváme zcela stranou oblast sexuálního obtěžování online, která by spadala pod virtuální násilí, neboť tam není pochyb o jeho závažnosti, ať už z pohledu digitálního domorodce či imigranta.

Rádi bychom tuto tezi podpořili statistikami z českého prostředí, pročež se nabízí pohled na počítačový trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 TZ. Vzhledem k dosud nízkému počtu těchto skutků však mají statistické údaje prakticky nulovou vypovídací hodnotu – např. v roce 2017 byly mezi oběťmi tohoto počítačového trestného činu všeho všudy 4 osoby mladší 18 let (z celkového počtu 30 obětí tohoto trestného činu), viz graf 29.[160]

Graf 29: Podíl obětí mladších 18 let na § 230 TZ a na celkovém počtu obětí kriminality



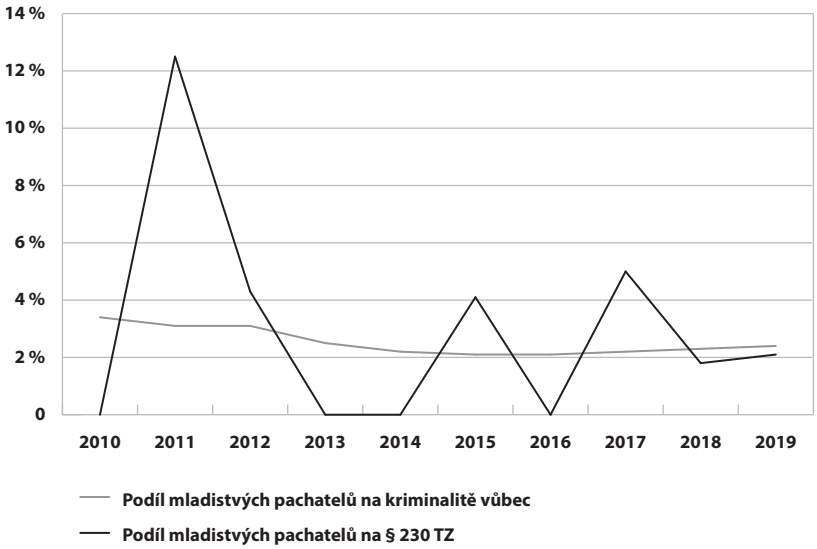
158 Tuto tezi do jisté míry potvrzuje v českém prostředí průzkum agentury Median z roku 2017, podle kterého vnímají krádež a zneužití osobních dat na internetu jako závažnější ti, kteří začali používat internet v mládí, viz (Median, 2017, str. 11).

159 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).

160 Viz CSLAV (Ministerstvo spravedlnosti), přehledy Oběti trestných činů - právní předpis TZ a přehledy Oběti trestných činů - právní předpis TZ2009. Za roky 2018 a 2019 bohužel nejsou k dispozici data vypovídající o počtu obětí mladších 18 let.

Podobně je tomu i s pachateli, když v roce 2017 bylo pravomocně odsouzeno za spáchání tohoto počítačového trestného činu celkem 6 mladistvých, v roce 2018 pouze 32 mladiství (z celkového počtu 166 odsouzených), viz graf 30.[161]

Graf 30: Podíl pravomocně odsouzených mladistvých pachatelů za § 230 TZ vůči pravomocně odsouzeným mladistvým vůbec

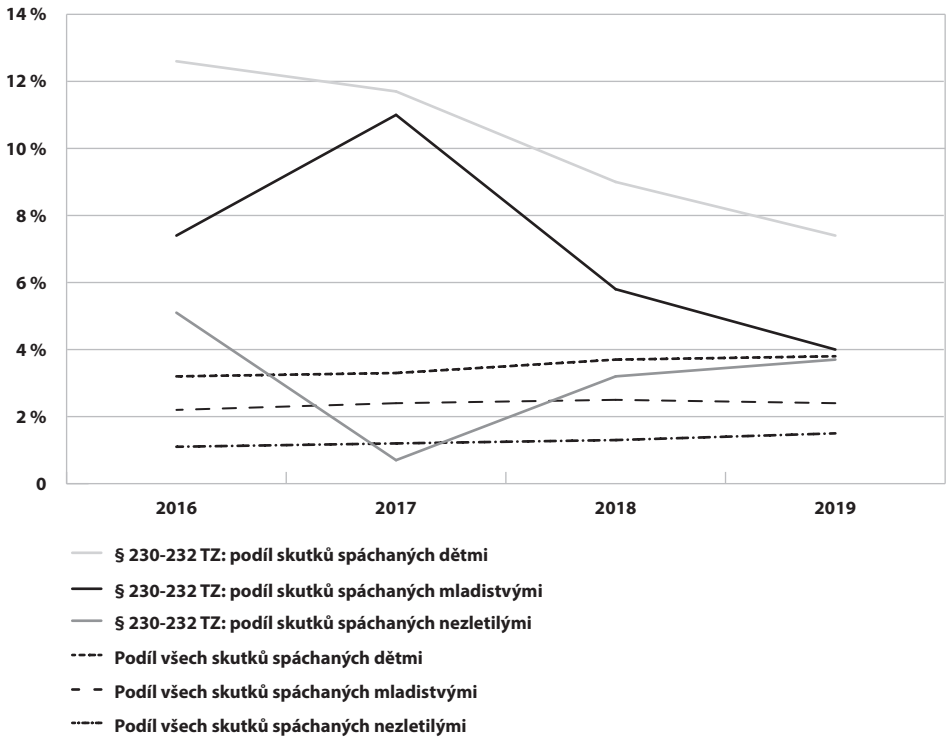


Obdobný trend demonstrují souhrnně pro počítačové trestné činy i policejní statistiky, viz graf 31. Ty sice pracují s podrobnějšími daty a poskytují i údaje o pachatelích mladších 15 let (označeni jako nezletilí), vzhledem ke změně způsobu evidence v roce 2016 však nejsou údaje srovnatelné s předchozími roky.[162]

161 Jde o podíl pravomocně odsouzených pachatelů v daných letech. Viz CSLAV (Ministerstvo spravedlnosti), přehledy Přehled o pravomocně vyřízených fyzických osobách podle paragrafů (odsouzených + vyřízených jinak) - právní předpis TZ, Přehled o pravomocně vyřízených fyzických osobách podle paragrafů - právní předpis TZ2009 a Přehled o pravomocně vyřízených fyzických osobách podle soudů (odsouzených + vyřízených jinak).

162 Blíže k tomu viz (Policie ČR), Statistické přehledy kriminality za rok 2016, 2017, 2018 a 2019.

Graf 31: Podíl počtu objasněných skutků dle § 230-232 TZ spáchaných mladistvými, nezletilými a osobami mladšími 18 let celkem vůči počtu objasněných skutků vůbec podle policejních statistik



Při posuzování vývoje počtu obětí a závažnosti dopadů kyberkriminality bude třeba vzít v potaz různé faktory. Kromě problematických aspektů spojených s vykazováním obětí vůbec (Diblíková, a další, 2019, str. 122) bude hrát roli i přístup samotných obětí, resp. potenciálních obětí. Např. děti a dospívající jsou kyberkriminalitou ohroženi jednak pro svou nevyzrálost, jednak pro svou větší přítomnost v online prostředí a jeho větší význam v jejich životě (viz výše). Na druhou stranu využívají řadu strategií, které jim pomáhají vyrovnat se s případnou újmou způsobenou v online prostředí, resp. pracují 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.). Řada skutků naplňujících skutkovou podstatu trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací tak vůbec není registrována (uživatel si např. sám zjedná opětovný přístup k napadenému účtu na sociální síti, a tím považuje celou záležitost za vyřešenou).

Naproti tomu senioři, kteří stojí na opačné straně uživatelské škály než děti a mladiství, sice netráví zdaleka tolik času a aktivit online, ale zároveň jim mnohdy chybí přiměřená obezřetnost vlastní mladším uživatelům znalým virtuálního prostředí. Jejich podíl coby obětí počítačového trestného činu neoprávněného přístupu k počítačovému systému

a nosiči informací dle § 230 TZ se však ještě výrazněji potýká s obdobnými problémy jako podíl obětí mladších 18 let, neboť jsou v justičních statistikách vykázány všeho všudy 2 oběti z řad seniorů, a to v roce 2015.[163]

Nicméně počet digitálních domorodců oproti množství digitálních imigrantů přirozeně poroste a spolu s tím se pravděpodobně etabluje i virtuální násilí coby neodmyslitelná součást kriminality vůbec. Až praxe ukáže, jak velký bude výsledný poměr majetkové kriminality online a virtuálního násilí. Jinými slovy – zda převažuje virtuální násilí nebo hamižnost. Nyní můžeme alespoň ukázat, jak se s virtuálním násilím a majetkovou trestnou činností online vypořádaly soudy v roce 2015.

III.6.1.1. Virtuální násilí a majetkový zájem v roce 2015

Jak již bylo výše zmíněno, případy se dělí takřka na dvě poloviny při rozdělení na majetkový zájem (n=33) a virtuální násilí (n=29). Charakter obviněných se podle pohlaví, věku a vzdělání téměř nelišil (viz tabulka 11), ale u virtuálního násilí bylo zaznamenáno o něco více recidivistů (35 % oproti 24 %). Pouze jediný pachatel v postavení úřední osoby sáhl k virtuálnímu násilí, u ostatních úředních osob převažoval majetkový zájem.

Tabulka 11: Základní charakteristika obviněných při rozlišení majetkového zájmu a virtuálního násilí

	Majetkový zájem		Virtuální násilí	
Pohlaví	Muži Ženy	76 % 24 %	Muži Ženy	79 % 21 %
Věk	Mladší Starší	49 % 52 %	Mladší Starší	48 % 52 %
Vzdělání	Méně vzdělaní Vzdělaní	52 % 48 %	Méně vzdělaní Vzdělaní	55 % 45 %
Recidiva	Ne Ano	76 % 24 %	Ne Ano	66 % 35 %
Pachatel úřední osobou	Ne Ano	79 % 21 %	Ne Ano	97 % 3 %

Podobně tomu bylo u skutků, kterých se měli obvinění dopustit ve spolupachatelství (15 %) – šlo dokonce výlučně o kauzy s majetkovým zájmem (viz tabulka 12). U případů s majetkovým zájmem je taktéž častější souběh s další trestnou činností (76 %) oproti virtuálnímu násilí (55 %) a následné uložení vedlejšího trestu (38 % případů s majetkovým

163 Viz CSLAV (Ministerstvo spravedlnosti), přehledy Oběti trestných činů - právní předpis TZ a přehledy Oběti trestných činů - právní předpis TZ2009. Za rok 2018 bohužel nejsou k dispozici ani data vypovídající o počtu seniorských obětí.

zájmem oproti 13 % virtuálního násilí). Nejspíš i díky tomu byla celková délka řízení delší u trestné činnosti s majetkovým zájem.[164] Opravné prostředky byly využity téměř totožně, a to v necelé čtvrtině obou skupin.

Tabulka 12: Další údaje při rozlišení majetkového zájmu a virtuálního násilí

	Majetkový zájem		Virtuální násilí	
Souběh	Ne Ano	24 % 76 %	Ne Ano	45 % 55 %
Spolupachatelství	Ne Ano	85 % 15 %	Ne Ano	100 % 0 %
Vedlejší trest	Ne Ano	63 % 38 %	Ne Ano	87 % 13 %
Opravný prostředek	Ne Ano	76 % 24 %	Ne Ano	76 % 24 %
Průměrná délka trestního řízení	1,8 roku		1,2 roku	
Průměrná délka přípravného řízení	0,9 roku		0,7 roku	
Průměrná délka řízení před soudem	0,8 roku		0,5 roku	

U deliktů s majetkovým zájmem ve více než polovině případů (55 %) docházelo ke zneužití přístupu k informačním technologiím. Obviněné lze až na výjimky rozčlenit na tři podskupiny: příslušníci Policie ČR, „vynalézavé ženy" a „datoví magnáti" (viz dále), všechno zaměstnanci různých institucí či firem.[165] Většinou šlo o poměrně vzdělané a zároveň bezúhonné jedince, kteří využili možnosti svého přístupu k informačním systémům. Přístup byl zneužit i v dalších případech, ty však byly zařazeny do dalších charakterově si bližších skupin: „geekové" a „online zloději". Nyní tedy k jednotlivým skupinám.

Čtyři **příslušníci Policie ČR** neoprávněně využili přístupu do policejních informačních systémů.[166] Kromě jednoho mladšího (27 let) byli tito muži starší 40 let, všichni ženatí, na vyšší pracovní pozici (inspektor či komisař) a vyučeni nebo vyučeni s maturitou. Většina policistů navzdory majetkovému zájmu nezpůsobila žádnou finanční újmu, pouze onen nejmladší policista škodu ve výši necelých 9 tisíc korun. Jednalo se však o závažná porušení ochrany osobních údajů, a proto byli všichni za svůj čin odsouzeni (ať už rozsudkem či zjednodušeným rozsudkem). Soud jim uložil trest odnětí svobody (v délce 0,5 roku, 1,5

164 Nutno ovšem připomenout, že při souběhu je obvykle přísněji trestný některý z ostatních sbíhajících se trestných činů, podle něhož pak soud ukládá úhrnný trest. Uložené tresty u majetkového zájmu oproti virtuálnímu násilí proto nelze dost dobře porovnat, aniž bychom vyčlenili jednání bez souběhu. Podobně je tomu při posuzování délky řízení, kterou lze předpokládat delší při řízení o sbíhajících se trestných činech.

165 Mezi zde uvedené skupiny nezahrnujeme tři odlišné případy spojené s majetkovým zájmem: jeden obviněný (nakonec zproštěn obžaloby) měl ve snaze popřít existující dluh vymazat obsah z notebooku, který mu zapůjčila jeho spolubydlící, jeden pachatel smazal data z odcizeného notebooku a jedna pachatelka porušila bankovní tajemství.

166 Blíže k jednomu z těchto případů viz Zaměstnanci jako bezpečnostní riziko.

roku, 3 roky a 3,5 roku), který u dvou pachatelů s nejnižší sazbou podmíněně odložil. Po dobu 1,5-7 let jim také zakázal předmětnou činnost. Trestní řízení trvalo průměrně 3,6 roku (1,2-5,4 roku), přičemž déle trvalo řízení před soudem (2 roky oproti průměrně 1,7 roku trvajícím přípravným řízením).

„**Vynalézavé ženy**" (n=4) doposavad vedly řádný život, žily v partnerském svazku, byly přinejmenším v době trestního řízení zaměstnané (většinou jako sociální pracovnice na úřadu práce) a vzdělané. Ve středním věku (po 40 letech) se však dostaly do tíživé finanční situace, kterou se snažily svépomocně vyřešit. Nakonec využily svého postavení a znalosti systému, ke kterému měly přístup, a „oživovaly" žadatele sociálních dávek, vytvářely fiktivní smlouvy atp.).[167] Jejich cílem nebylo ublížit někomu konkrétnímu, nicméně oběťmi jejich konání se staly samotné instituce, potažmo stát. Svojí důmyslností a nenápadností dokázaly způsobit škody v milionových částkách. Do roka od prvotního podnětu k trestnímu řízení byly postaveny před soud a za několik měsíců si vyslechly rozsudek včetně podmíněného odsouzení v délce trvání do 3 let a zákazu činnosti s hmotnou odpovědností ve státní správě a jinde. To však neplatilo pro ženu, která se svým jednáním dopustila škody dosahující bezmála 27 milionů korun, za něž byla odsouzena k trestu odnětí svobody v délce 9,5 roku.

Mezi „**datové magnáty**" (n=5) patří skupina zaměstnanců různých firem. Jejich záměrem bylo zmocnit se informací o klientech poškozených společností (které vždy dané jednání oznámily na Policii ČR) za účelem dalšího vlastního využití. Finanční škoda nebyla ve většině případů vyčíslena (u jedné kauzy je uvedena hodnota ukradených dat 2,9 milionu korun). Na druhou stranu měla být poškozena ochrana citlivých dat klientů a důvěryhodnost daných společností. Jednalo se o dvě obviněné ženy a tři muže, většinou starších věkových kategorií (25-59 let, v průměru 40,4 roku), zaměstnance či OSVČ, většinou alespoň s maturitou, dosud bezúhonné. Trestní řízení trvalo průměrně 1,6 roku s vyrovnanou délkou přípravného řízení i řízení před soudem, k souběhu s další trestnou činností došlo jen v jednom případě. V závěru byli odsouzeni pouze dva pachatelé, a to k podmíněnému trestu odnětí svobody na 0,3 a 0,5 roku.[168]

Další skupinu (n=7) představují obvinění, kteří měli jednak zneužít svůj přístup ke konkrétnímu zařízení či informačnímu systému, jednak využít hlubší znalosti digitálních technologií a online prostředí (hacking, phishing, krádež identity). Proto jsou označeni jako „**geekové**" coby osoby zapálené pro svůj obor, a to převážně z oblasti informačních technologií.[169] V tomto případě se jednalo o mladé muže (do 24 let) bez větších závazků, kteří ještě studovali nebo se teprve zařazovali na pracovní trh. Někteří však již měli zkušenost s podobnou trestnou činností. K obětem je většinou nepoutal blízký vztah, a možná proto se nebáli vyšších cílů svých útoků v řádu stovek tisíců korun. Před soud se dostali

167 Blíže ke dvěma z těchto případů viz Zaměstnanci jako bezpečnostní riziko.

168 V jedné z odsouzených kauz figuroval ještě spolupachatel, kterého však do této skupiny nezařazujeme, neboť nezneužil vlastního přístupu do informačního systému, nýbrž požádal oprávněnou osobu o její přístupové údaje.

169 Výraz „geekové" je poněkud nadnesený, neboť zejména krádeže identity nevyžadovaly žádné zvláštní schopnosti technického rázu, nicméně ve všech případech se jednalo o mladé osoby, které se přinejmenším pokročileji orientovaly v online prostředí a informačních technologiích.

do 1,5 roku, dále pak záleželo na okolnostech, zda útočníky po dlouhém procesu a odvolání soud zprostil viny, nebo zda vyvázli s podmínkou či několikaletým nepodmíněným trestem odnětí svobody.

„**Online zloději**" (n=10) získali (ať už náhodou nebo cíleně) přístupová hesla k účtům obětí z jejich bezprostředního okolí. Díky tomu si následně „půjčili" nebo převedli finanční prostředky. Počty útoků i obětí se pohybovaly v jednotkách, trestnou činnost prováděli pachatelé sami a v polovině případů se nejednalo o první zkušenost s porušením zákona. Šlo především o muže v širokém věkovém rozpětí (17-49 let, v průměru 32 let), převážně bez partnerského závazku a s nízkým socioekonomickým statusem.[170] Celý proces trestního řízení obvykle proběhl poměrně rychle. Přípravné řízení trvalo spíše déle (průměrně více než půl roku), soudy pak tyto případy vyřešily převážně do 3 měsíců. Ať už se škoda pohybovala v nízkých částkách nebo se vyšplhala k půlmilionovému úvěru, obvinění většinou skončili s podmíněně odloženým trestem odnětí svobody nejdéle na 1,5 roku, případně zproštěním obžaloby.

Na rozdíl od majetkových deliktů docházelo k virtuálnímu násilí zejména v souvislosti se vztahovými neshodami. Obvinění tak většinou činili ze žárlivosti (na současné či bývalé partnery), z pomsty (po rozchodu) atp. Nešlo jim proto primárně o peníze, majetek či jiné hodnoty v podobě informací, ale o ublížení oběti, s níž se téměř vždy znali (90 %). Část obviněných, kteří se měli dopustit virtuálního násilí, byla rozdělena do dvou podskupin podle užší motivace na „mstitele" a „žárlivce".[171] U ostatních obviněných chyběly informace o jejich motivaci k činu nebo nevytvořili dostatečně velkou skupinu pro stanovení podobného typu.

Řada obviněných se nechala při svém jednání unést touhou po pomstě, do skupiny „**mstitelů**" (n=7) jsme však zařadili jen některé. Šlo o zhrzené ex-partnery poškozených, kteří si přes internet vybíjeli vztek rozesláním intimních fotografií oběti, pomlouváním či jednáním jejím jménem na sociálních sítích. Vždy k tomu využili předchozí vztah s obětí, která jim v rámci projevené důvěry sdělila přihlašovací údaje (ať už k e-mailu nebo ke svému účtu na sociální síti), měla své heslo uložené v zařízení bývalého partnera, případně se obviněný k heslu dostal skrze znalost jiných osobních údajů.[172] Většinou se jednalo o mladší (průměrně 26 let) bezúhonné muže, kteří byli za své činy odsouzeni.[173] Soud jim obvykle uložil podmíněně odložený trest odnětí svobody na 0,8-2,3 roku (v průměru 1,6 roku), ve dvou případech pak trest obecně prospěšných prací (150 a 200 hodin). Oproti rychlému řízení před soudem (průměrně 0,3 roku) bylo trvání přípravného řízení poměrně dlouhé (průměrně 0,8 roku).

170 Většinou s nižším či žádným příjmem a vzděláním bez maturity, nicméně v řadě případů tyto údaje zcela chybí – proto zde ty zjištěné doplňujeme pouze v poznámce pod čarou pro úplnost.

171 Za drobnou zmínku stojí také „vtipálci" (n=3) – např. opilecký žert nebo snaha pachatele „vytrestat" neopatrného poškozeného uživatele tak, jako kdysi „vytrestal" někdo jeho samého.

172 Například prostřednictvím funkce obnovy zapomenutého hesla odpovědí na kontrolní otázku. Blíže k některým způsobům neoprávněného vstupu do informačního systému viz Lesk a bída e-mailu.

173 V jednom případě tak učinila kamarádka zhrzeného homosexuálně orientovaného přítele.

I „**žárlivci**" (n=9) často útočili na svého bývalého partnera (ve dvou případech i současného), nicméně namísto zveřejňování intimního obsahu spíše nějaký obsah mazali a usilovali o kontrolu nad činnostmi oběti. Oproti „mstitelům" byli pachatelé starší (průměrný věk 33,8 let), častěji již měli zkušenost s trestnou činností a třetinu tvořily ženy. K samotnému útoku využili především znalost hesla, ale i fyzický akt – napadení oběti, ukradení diáře s přihlašovacími údaji, vyhrožování (s cílem získat přihlašovací údaje).[174] Škála závažnosti těchto případů byla proto poměrně široká, od toho se pak odvíjela i přísnost uložených trestů – od obecně prospěšných prací přes podmíněně odložený trest odnětí svobody (na 0,5-0,8 roku) až po nepodmíněný trest odnětí svobody (na 0,7-2,5 roku).[175]

Zbývá ještě dodat, že aby bylo možné se virtuálním násilím seriózně zabývat s podporou statistických dat, bylo by nanejvýš žádoucí zařadit do veřejně přístupné evidence statistických údajů i prvek online prostředí.[176] To by umožnilo především vytřídit relevantní data vztahující se i k jiným než pouze počítačovým trestným činům, typicky podvodu či poškození cizích práv. Bylo by tak možné lépe odhadnout vztah mezi registrovanou kriminalitou online oproti offline, včetně kombinace obou. Časem se pak může ukázat, zda bude namístě věnovat zvláštní pozornost virtuálnímu násilí per se, případně zvážit zahrnutí prvku online prostředí i do samotného trestního zákona (ať už v podobě obecně či zvlášť přitěžující okolnosti), leč tuto úvahu je v současnosti nutno brát zatím s velkou rezervou.

III.6.2. Oběti a poškození

V případech, kde se podařilo dohledat informace o počtu poškozených (n=65), figurovaly mezi nimi jak fyzické, tak právnické osoby i obojí.[177] V necelých dvou třetinách věcí (65 %) byla poškozena fyzická osoba, ve více jak čtvrtině (27 %) právnická osoba a v 6 věcech (9 %) fyzická i právnická osoba.

Zdá se, že obvinění buď útočí na data vybraných jednotlivců, anebo se dopouštějí svého jednání naopak ve velkém měřítku: v 75 % případů (n=49) byla mezi poškozenými jediná fyzická (n=32) nebo právnická (n=17) osoba, ve 12 věcech 2-5 osob (z toho v 10 kauzách pouze 2 osoby). Ve zbývajících 4 případech s alespoň částečně známým počtem poškozených se jejich počet vyhoupl na 16, dále 75, 97 a dokonce 282 poškozených. Stále ovšem hovoříme o poškozených, tzn. o osobách s určitým procesním postavením dle § 43 TŘ, které jsou orgánům činným v trestním řízení známé.[178] Řada obětí není do trestního

174 Stále hovoříme o neoprávněném přístupu k počítačovému systému a nosiči informací dle § 230 TZ, tedy např. zneužití e-mailové schránky nebo účtu na sociální síti.

175 Kromě dvou pachatelů, kteří se sice trestné činnosti dopustili, nicméně jejich trestní stíhání bylo zastaveno (v jednom případě fakultativně dle § 172 odst. 2 TŘ, v druhém případě podmíněně dle § 307 TŘ).

176 Nyní je tento údaj přístupný pouze pro uživatele v rámci resortu Ministerstva spravedlnosti.

177 Celkový počet 68 obviněných se podílel na 66 kauzách (včetně 2 věcí ve spolupachatelství), v jednom řízení se soud ani obžaloba k poškozeným nijak nevyjádřili (pachatel neoprávněně zjišťoval informace z policejní databáze).

178 Proto ačkoliv na řadě míst hovoříme o „obětech", přesněji řečeno vypovídají uvedené statistické údaje vždy o „poškozených".

procesu zahrnuta, ať už proto, že o nich neví orgány činné v trestním řízení, proto, že nesplňují požadavky kladené na postavení poškozeného, nebo i proto, že samy neví, že jsou obětí (např. neví o zneužití jejich e-mailové schránky).[179]

Počet dílčích útoků se mnohdy ani nepodařilo zjistit, ba se tím obžaloba a soudy často podrobněji vůbec nezabývaly,[180] výjimku tvořily případy s prokázanou škodou. V necelé polovině případů, u nichž byl zjištěn počet útoků (47 %, n=57), se jednalo o jednorázové útoky, dalších 39 % čítalo do 10 útoků, ale v 8 případech se jednalo o desítky napadení v rozmezí od 18 do 782 útoků (v průměru 158).[181] Nejintenzivnější byl případ s 234 útoky provedenými jediným pachatelem. Útoky byly většinou úspěšné, v 6 případech částečně neúspěšné (nejvýše 5 nezdařených útoků, což někdy znamenalo i 100% neúspěšnost). V jedné kauze se ovšem nezdařilo 444 útoků z celkových 782 útoků na 282 obětí, což se odrazilo i na výši způsobené škody (cca půl milionu korun) oproti zamýšlené škodě (přes milion korun).

Zhruba ve 40 % případů byla způsobena finanční škoda (1 200 až téměř 27 milionů korun), převážně v rozmezí 10-500 tisíc korun.[182] Zamýšlená (a nedosažená) škoda byla zjištěna u patnácti obviněných, jejichž úspěšnost byla v průměru 72%. Sedm obviněných mělo vyšší ambice, a to od 4 tisíc až po více než půl milionu korun (v průměru přes 150 tisíc korun). Naproti tomu osmi obviněným se podařilo napáchat tolik škody, kolik zamýšleli.

Nemajetková újma byla zjištěna v 68 % případů (n=44).[183] Jednalo se nejčastěji o psychické potíže (51 %), online poškození (ve smyslu smazání dokumentů, zneužití databáze, porušení důvěryhodnosti atp., 37 %) a zamezení přístupu k nějakému účtu (21 %). Čtyři případy byly doprovázeny fyzickým napadením a jeden jinou nemajetkovou újmou (rozbití počítačové sítě). Požadovaná náhrada nemajetkové újmy byla vyčíslena ze strany poškozené pouze v jediném případě, nicméně bez bližší konkretizace.[184]

179 Blíže k rozlišení poškozených a obětí viz např. (Šámal, a další, 2012, str. 496).

180 S obvyklou formulací „v blíže neurčenou dobu," případně dokonce v kombinaci „s blíže neurčeným způsobem." Obžaloba i soud se v takových případech 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).

181 Zejména u vyšších počtů útoků jich však na jednotlivé oběti připadaly v průměru pouze jednotky (do tří útoků na osobu). Tyto útoky byly vždy motivovány finančním ziskem.

182 S ohledem na značný rozptyl výše způsobených (či zamýšlených) škod nemá smysl je průměrovat.

183 Např. zostuzení poškozené před spolupracovníky po rozeslání urážlivých e-mailů jejím jménem prostřednictvím neoprávněného přístupu do e-mailové schránky poškozené.

184 Poškozená požadovala náhradu nemajetkové újmy ve výši 600 tisíc korun v souvislosti se znepřístupněním profilu na Facebooku a zveřejněním inzerátu jejím jménem na erotické online seznamce.

Ve více než polovině případů (59 %) se poškozený s útočníkem znal, v necelé třetině (31 %) došlo k poškození zaměstnavatele zaměstnancem (stávajícím nebo bývalým)[185] a ve 13 % nebyl prokázán mezi nimi žádný vztah.[186] Někteří obvinění útočili na oběti s různým vzájemným vztahem.[187]

Pokud obviněný útočil na svého příbuzného (13 %), většinou se jednalo o online krádeže (viz „online zloději" výše). Pachatelé využili blízkosti jak fyzické (nalezení hesla), tak vztahové (důvěra, znalost osobních informací atp.). Díky tomu získali přístupové údaje potřebné k převedení financí či zřízení úvěru.[188] Tímto způsobili škodu v průměru přes 50 tisíc korun.

V případech, kdy byl poškozený partner či ex-partner obviněného (29 %), se většinou jednalo naopak o virtuální násilí, ať už motivované pomstou či žárlivostí (viz „mstitelé" a „žárlivci" výše). Opět zde hrála roli alespoň předchozí důvěra poškozených v obviněné, která zapříčinila nedostatečné zabezpečení přístupů do e-mailů, na sociální sítě a podobně. Dopady těchto útoků nebylo možné finančně vyčíslit (kromě dvou případů s majetkovým zájmem), ale poškození většinou uváděli psychickou újmu (narušení soukromí, pomluvy, zveřejnění intimních fotografií atp.), dále zamezení přístupu na svůj účet, případně smazání dokumentů (například fotografií). Útoky také častokrát doprovázela fyzická ublížení.

Ostatní případy již neměly tak homogenní charakteristiky. Tam, kde obvinění útočili na své známé (18 %), se jednalo častěji o virtuální násilí, jehož motivace se různily od žertu po mstu za neopětovaný vztah či jiné nevhodné chování. Část obviněných ovšem cílila na majetek s různě vysokými způsobenými (či zamýšlenými) škodami, a to od 1 200 korun po více než 130 tisíc způsobené převodem peněz či smazáním smlouvy. Opět využili znalosti či fyzické blízkosti oběti.

Podobně heterogenní byly i případy, kdy neměl obviněný k poškozenému subjektu žádný vztah (13 %). Spojujícím aspektem je zde právě vzájemná neznalost, která sehrála zásadní roli při způsobu spáchání trestné činnosti. Obvinění totiž museli využít složitější techniky jako je sociální inženýrství (vylákání hesla, phishing atp.) nebo být fyzicky přítomni u cizího počítače (např. zcizené nebo sdílené zařízení, ze kterého se poškozený po předchozím užití neodhlásil). Především se jednalo o finančně motivované útoky, jejichž škoda se pohybovala od necelých 2,5 tisíc korun do více než půl milionu.

Nejvíce obviněných mělo poškodit svého zaměstnavatele (31 %).[189] Tato trestná činnost byla doménou ženských pachatelek. Jednalo se především o případy s majetkovým zájmem, přičemž za majetek zde považujeme finance nebo data. Většina případů byla založena na zneužití přístupu k pracovnímu zařízení či informačnímu systému. Pokud došlo k finanční

185 Blíže k tomu viz Zaměstnanci jako bezpečnostní riziko.

186 Součet překračuje 100 %, protože v některých kauzách figuruje více kategorií poškozených.

187 Pachatel např. směřoval svůj útok zpočátku na svou bývalou partnerku, posléze ho rozšířil na její známé a následně na známé těchto známých, které již neznal osobně ani online.

188 Např. úvěr ve prospěch napadeného bankovního účtu, odkud následně pachatel peníze odčerpal na svůj vlastní účet.

189 Blíže k této skupině viz Zaměstnanci jako bezpečnostní riziko.

škodě, pak v některých případech dosahovala i několikamilionových částek. Pokud byla ukradena či zneužita data, pak to způsobilo především narušení důvěryhodnosti dané instituce.

III.6.3. Zaměstnanci jako bezpečnostní riziko

Pod pojmem kybernetická kriminalita si pravděpodobně nejčastěji představujeme propracovaný hackerský útok vedený zvenčí pachatelem disponujícím značnými dovednostmi a znalostmi v oblasti počítačových systémů za využití důmyslného malwaru. Zkušenosti expertů z oblasti informačních a komunikačních technologií však ukazují, že za významnou částí zaznamenaných bezpečnostních incidentů (hovoří se až o dvou třetinách případů) stojí nejslabší článek systému – lidský faktor v podobě vlastních zaměstnanců. Nedostatečně proškolený personál či liknavý přístup k dodržování pravidel bezpečného užívání informačních a komunikačních technologií zvyšuje pravděpodobnost, že případný pokus o proniknutí do informačního systému zaměstnavatele bude úspěšný.

Samostatnou kapitolou jsou však zaměstnanci páchající úmyslnou trestnou činnost zneužitím přístupu do informačního systému zaměstnavatele. Nemusí disponovat pokročilými znalostmi a dovednostmi z oblasti informačních a komunikačních technologií. Nemusí do systému složitě pronikat a k provedení jejich záměrů obvykle postačí uživatelské znalosti a vědomosti o zavedených postupech. Krádeži firemních dat, jejich pozměnění či smazání, sabotování činnosti zaměstnavatele, nebo například zneužití přístupu do systému k páchání podvodů již nestojí téměř nic v cestě.

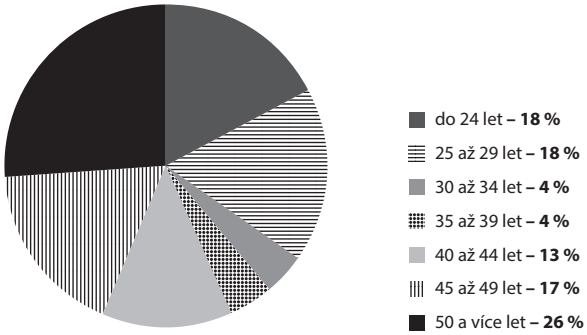
Mezi obviněnými, jejichž trestní řízení pravomocně skončilo v roce 2015, bylo 23 osob v zaměstnaneckém či služebním poměru s poškozeným subjektem. Z toho sedm bylo státními zaměstnanci – tři sociální pracovnice a čtyři příslušníci policie ČR, viz graf 32.

Graf 32: Obvinění z řad zaměstnanců

Průměrný věk obviněných z řad zaměstnanců činil necelých 38 let, přičemž nejmladšímu z nich bylo 21 let a nejstarší obviněné 56 let. Zatímco u celého vzorku výrazně převládaly mladší věkové skupiny,[190] mezi zaměstnanci (či bývalými zaměstnanci) je podíl obviněných starších čtyřiceti let více než poloviční, viz graf 33.

190 Blíže k tomu viz K osobě obviněného, zejména graf 11.

Graf 33: Věková struktura obviněných z řad zaměstnanců



Zastoupení pohlaví u pachatelů z řad zaměstnanců je více méně obdobné jako u celkového vzorku, viz tabulka 13.

Tabulka 13: Pohlaví obviněných

	Celý vzorek		Zaměstnanci	
	Počet	Podíl (%)	Počet	Podíl (%)
Muži	53	67	16	70
Ženy	15	33	7	30
Celkem	68	100	23	100

Co se týče socioprofesního statusu obviněných z řad zaměstnanců, není nikterak překvapivé jejich výrazně vyšší zastoupení v nedělnických profesích, viz tabulka 14.

Tabulka 14: Socioprofesní status obviněných

	Celý vzorek		Zaměstnanci	
	Počet	Podíl (%)	Počet	Podíl (%)
Zaměstnanec v dělnické profesi	7	10	1	4
Zaměstnanec v nedělnické profesi	19	28	11	48
OSVČ / podnikatel	12	18	4	17
Uchazeč o zaměstnání (v evidenci Úřadu práce)	9	13	0	0
Bez zaměstnání	7	10	0	0
Student	9	13	3	13
Služební poměr	4	6	4	17
Nezjištěno	1	1	0	0
Celkem	**68**	100	**23**	100

Poškozující jednání obviněných mělo různé podoby. Obvinění svému (někdy bývalému) zaměstnavateli např. znemožnili připojení k internetu, instalovali keylogger nebo zkopírovali či znehodnotili data ve firemní databázi (nejednou v rámci konkurenčního boje). Níže uvádíme tři kauzy ilustrující některé ze závažnějších případů.

III.6.3.1. Kauza „Živí mrtví"

Koncem února 2012 byla paní Mgr. D. W. (toho času ve věku 49 let) jako zaměstnankyně Úřadu práce zařazena na pracovní pozici sociální pracovnice jako referentka nepojistných sociálních dávek. Zanedlouho poté se přihodilo, že omylem zaslala dávku zemřelému klientovi a nic se nestalo, nikdo nic nekontroloval. Zjistila tak, že informační systém Úřadu práce není napojen na centrální registr obyvatel a data úmrtí klientů zadávají sami referenti na základě oznámení rodinných příslušníků. Toto zjištění paní D. W. vnuklo myšlenku, že by mohla poněkud přilepšit rodinnému rozpočtu. Bylo jednoduché smazat v systému datum úmrtí klienta, který tak znovu ožil a sociální dávky mu mohly být vypláceny dál. Tentokrát však již na účet vynalézavé úřednice. Po vyplacení této dávky zadala znovu do systému datum úmrtí a původní číslo účtu klienta. Do července 2014 takto přivedla opět k životu celkem 29 zemřelých klientů. Některé z nich dokonce opakovaně. Celkem tímto způsobem neoprávněně čerpala sociální dávky ve výši 1 224 000 Kč. Jednou však při zahlazování stop zadala do systému chybně datum úmrtí jednoho z klientů a v následujícím výplatním období byla sociální dávka vyplacena pozůstalým. Ti tuto skutečnost nahlásili Úřadu práce. Nadřízená paní D. W. následně nařídila detailní kontrolu. Po zjištění situace a celkové výši škod byla tato skutečnost nahlášena Policii ČR. Vynalézavá úřednice byla posléze obviněna ze zneužití pravomoci úřední osoby (§ 329 TZ), podvodu (§ 209 TZ) a neoprávněného přístupu k počítačovému systému a nosiči informací (§ 230). Okresní soud ji za tyto trestné činy odsoudil k úhrnnému trestu odnětí svobody v trvání 3 let, podmíněně odloženému na zkušební dobu v trvání 5 let. Dále jí byl uložen trest zákazu činnosti na dobu 5 let a povinnost nahradit způsobenou škodu.

V souvislosti s tímto případem je poněkud zarážející skutečnost, že zatímco pokladní v samoobsluze potřebuje ke zrušení špatně namarkované položky schválení nadřízeného pracovníka, informační systém úřadu práce ke znovuoživení zesnulého klienta obdobnou autorizaci nevyžadoval.

III.6.3.2. Kauza „Podvodné úvěry"

Paní J. H. pracovala od roku 1997 na jedné z poboček nejmenované banky. V červenci 2003 se rozhodla řešit svou tíživou finanční situaci tím, že s využitím osobních údajů jednoho z klientů banky podvodně sjednala spotřebitelský úvěr. Následující podvodné úvěry již uzavírala na fiktivní osoby. Údaje takových osob zadala do bankovního informačního systému, a to včetně fiktivního zaměstnavatele a fiktivního příjmu. Na základě těchto údajů byl následně úvěr schválen v bankovním systému. Zpočátku nebylo třeba do systému ukládat fotokopie příslušných dokladů, takže je stačilo pouze zadat. Tato praxe skončila v roce 2010, kdy byl bankovní systém změněn. Po této změně již bylo nezbytné do centrály banky prostřednictvím systému posílat pozměněné fotokopie osobních dokladů skutečných klientů banky. Podklady k podvodným úvěrům ve fyzické podobě pachatelka vytvářela jen v případě, měla-li na pobočce proběhnout pravidelná vnitřní kontrola. Od roku 2007

paní J. H. zastávala pozici vedoucí bankovní pobočky, což jí její počínání značně usnadnilo, neboť ji centrála vždy s předstihem informovala, které úvěrové smlouvy budou v rámci pravidelné vnitřní kontroly prověřovány. Celkem tímto způsobem uzavřela 234 úvěrových smluv o poskytnutí spotřebitelských úvěrů 153 fiktivním osobám. Od banky tak čerpala finanční prostředky v celkové výši více než 45 milionů korun, z nichž více než 18 milionů použila na částečné splácení jistin těchto úvěrů. Bance svým počínáním způsobila škodu téměř 27 milionů korun. V březnu 2012 oznámila jedna z klientek banky reklamačnímu oddělení, že je na její adresu opakovaně doručována bankovní korespondence pro osoby, které nezná a nikdy na její adrese neměly trvalý či přechodný pobyt. Následující interní šetření odhalilo neshody v dokladech uložených v bankovním systému. Poté co byla paní J. H. s tímto zjištěním konfrontována, svou činnost doznala. Celá věc byla oznámena Policii ČR a paní J. H. byla následně obviněna ze spáchání zločinu neoprávněného opatření, padělání a pozměňování platebního prostředku (§ 234 TZ), úvěrového podvodu (§ 211 TZ) a neoprávněného přístupu k počítačovému systému a nosiči informací (§ 230 TZ). Krajský soud ji uznal vinnou a odsoudil ji k úhrnnému trestu odnětí svobody v trvání 9,5 roku se zařazením do věznice se zvýšenou ostrahou. Dále ji byl uložen trest zákazu činnosti na dobu osmi let a povinnost nahradit způsobenou škodu.

III.6.3.3. Kauza „Pomáhat a chránit"

Nadpraporčík Š. P. pracoval jako inspektor jednoho z krajských ředitelství Policie ČR. Postupně se s celou rodinou dostal do značné finanční nouze a hrozila jim exekuce. Napadlo ho situaci řešit poskytováním informací o probíhajících trestních řízeních za úplatu. V několika případech poskytoval za drobné finanční částky, poskytnutí bezúročné půjčky či příslib sjednání úvěru údaje z policejního informačního systému ETŘ (Evidence trestního řízení), k němuž měl jako policista zřízen přístup. Jednalo se především o informace, zda nebylo trestní řízení zastaveno, jaké svědky již policie v dané věci vyslechla atp. Poté co se jeho jednání provalilo, šetřila věc Generální Inspekce Bezpečnostních Sborů (GIBS) a následně na něj podal státní zástupce obžalobu pro spáchání trestného činu zneužití pravomoci úřední osoby (§ 329 TZ), přijetí úplatku (§ 331 TZ) a neoprávněného přístupu k počítačovému systému a nosiči informací (§ 230 TZ). Okresní soud odsoudil policistu Š. P. k úhrnnému trestu odnětí svobody v trvání 3 let nepodmíněně, pro jehož výkon byl zařazen do věznice s dozorem. Dále mu byl uložen trest zákazu činnosti spočívající v zákazu služebního a pracovního poměru u bezpečnostních sborů po dobu 5 let.

III.6.4. Lesk a bída e-mailu

Ač byla paleta sledovaných jednání spadajících pod § 230 TZ s pravomocným skončením v roce 2015 poměrně pestrá, ukázalo se několikero opakujících se jevů. Jedním z nich je napadání e-mailových schránek. Zdánlivě banální jednání bez způsobení zjevné škody může znamenat i velký zásah do osobnostní a případně i majetkové sféry oběti. Pachatel si např. „jen" prohlédne uložený obsah a korespondenci, zároveň však může tímto způsobem získat i podrobné informace o aktivitách oběti, jejím harmonogramu (např. v kolik hodin obvykle odesílá poštu v rámci svého zaměstnání, kdy naopak není aktivní vůbec atp.) a kontaktech. Mimoto se mu může dostat do ruky klíč k dalším informacím prostřednictvím jiných aplikací (např. e-maily obsahující přihlašovací údaje do různých aplikací), nemluvě o propojení se sociálními sítěmi. Níže proto uvádíme pro ilustraci jednu z takových kauz.

Pachatelovo jednání lze stručně shrnout jako neoprávněné pronikání do cizích e-mailů za účelem prohlídky nebo stažení jejich obsahu. V jeho případě se jednalo o fotografie a videa s erotickou nebo přímo pornografickou tematikou, která využíval pro vlastní sexuální uspokojení: „*… nikde jsem je dále nešířil. Při prohlížení těchto fotografií jsem masturboval.*“[191] 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 pět 12° piv a 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.[192]

Pachatelův modus operandi byl po celou dobu jednání poměrně neměnný. Nejprve si vyhlédl osobu na sociálních sítích Lidé.cz nebo Najdise.cz. Mezi jeho objekty zájmu patřily především mladé dívky, a to výhradně ty, které uvedly jako kontaktní e-mail adresu s koncovkou @seznam.cz. Následně se pokusil u takto vybraných osob zjistit, zda existuje s jejich příjmením profil na sociální síti Spolužáci.cz, který by mohl patřit jejich matce,[193] neboť právě zde se často nacházelo vedle stávajícího příjmení dané osoby i její jméno za svobodna.[194]

Vyzbrojen těmito údaji (e-mailová adresa a rodné příjmení matky, případně i její jméno) se následně pachatel pokusil proniknout do e-mailové schránky prostřednictvím tzv. obnovy zapomenutého hesla. V předchozích letech poskytovatel e-mailových 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

191 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 (včetně dětské pornografie) jako takovou.

192 Z toho splácel úvěr 100 000 Kč vždy částkou 5 000 Kč měsíčně.

193 Vodítkem mu bylo např. místo narození, bydliště (zpravidla informace dostupná na některé sociální síti, nejčastěji Facebooku) nebo navštěvovaná škola, křestní jméno odhadoval.

194 Dnes již nefungující sociální síť Spolužáci.cz vznikla a byla 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.

otázka po rodném příjmení matky.[195] 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 však podle pachatele zdlouhavý a vyžadoval notnou 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 e-mailových schránek, do nichž se pachateli prokazatelně podařilo proniknout.

Jakmile se pachatel octl v e-mailové schránce, pokusil se vyhledat zejména v rámci odchozí pošty přílohy v 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, e-mailovou adresu a přihlašovací údaje k ní si poznamenal pro opakované pozdější použití: „*E-mailovou 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 e-mailových 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 e-mailů a stahuji si jejich fotky a videa poškozené nevěděly. Na text nějakého e-mailu jsem se podíval asi jen v jednom případě, ale to mě nijak nezajímalo, chtěl jsem pouze fotografie*."

Náš roztoužený pachatel se nakonec neomezil „pouze" na procházení obsahu napadených e- mailových schránek, ale jeho sexuální apetit si vyžádal další aktivity, a to v podobě stahování dětské pornografie prostřednictvím tzv. P2P sítí.[196] Soud mu proto uložil úhrnný trest ve výměře 1 roku za sbíhající se přečiny neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 odst. 1 TZ (týkalo se pouze neoprávněně navštívených e-mailových schránek) a § 230 odst. 2 TZ (z některých navštívených schránek pachatel přeposlal část obsahu na svůj e-mail) a dále za přečin výroby a jiného nakládání s dětskou pornografií dle § 192 odst. 1 TZ, který podmíněně odložil na zkušební dobu 3 roky.[197] Vedle

195 V současnosti již Seznam.cz upřednostnil obnovu zapomenutého hesla prostřednictvím tzv. ověřeného telefonu nebo e-mailu (uživatelem předem zadané číslo mobilního telefonu / e-mail, na který posléze přijde kontrolní zpráva s kódem potřebným pro ověření daného kontaktu), na který v případě zapomenutého hesla zašle heslo nové. Možnost obnovy hesla prostřednictvím kontrolní otázky zůstává pouze u dříve založených e-mailových schránek, jejichž uživatelé dosud žádný mobilní telefon ani e-mail neověřili.

196 Tzv. Peer-to-Peer síť značí přímé propojení zařízení bez zprostředkujícího serveru. Uživatelé obvykle dají část vlastního obsahu k dispozici ostatním pro stažení, zatímco sami mohou získat takto poskytnutý obsah od nich.

197 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 e-mailů, které však sama neposlala.

toho pak trest propadnutí věci (mimo jiné tří počítačů) a ochranné léčení sexuologické ambulantní formou.[198] Poškozené byly se svým nárokem na náhradu škody odkázány na řízení ve věcech občanskoprávních.

Ač si to mnozí neuvědomují, e-mail, resp. **e-mailová schránka** představuje do jisté míry vstupní bránu do virtuálního světa svého majitele. V prvé řadě zahrnuje vlastní aktivity spojené s e-mailovou komunikací jako takovou, zejména samotný obsah komunikace (včetně příloh) a e-mailové adresy osob, s nimiž dotyčný udržuje vztah nebo byl někdy v kontaktu. Z využívání e-mailové schránky lze do jisté míry vyčíst například i dobu aktivity a spánku, stav offline i online. Mimoto velmi často obsahuje i přihlašovací údaje k sociálním sítím a dalším aplikacím.[199] V neposlední řadě pak mnohdy slouží i pro 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 e-mail významnou roli zhruba ve čtvrtině případů (n=17). Útok byl cílený na obsah e-mailové schránky jako takové v devíti případech, přičemž v pěti případech byl blízký vztah mezi obviněným a poškozeným (ať už šlo o muže či ženy na obou stranách) – manželé či partneři, stávající i bývalí. Obvinění zejména pátrali po nevěře (v pěti případech), ale také např. hledali informace použitelné v rozvodovém řízení, jeden z obviněných si neoprávněně zálohoval „svou" firemní poštu po ukončení pracovního vztahu.

Napadení e-mailové schránky ovšem sloužilo ve zbývajících 8 případech i jako prostředek k dalšímu jednání, převážně šlo o zištnou motivaci nebo nějakou formu virtuálního násilí. Ve dvou případech virtuálního násilí pachatele motivovala touha po odplatě,[200] usiloval také o poškození dobré pověsti poškozené.[201]

Zištná motivace vedla jednoho z pachatelů k přeposílání dat o klientech zaměstnavatele konkurenční společnosti. Další prostřednictvím napadených e-mailových schránek získával přístup mimo jiné k sociální síti Facebook 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 tzv. m-platby[202] v různé výši, které využíval pro dobití

198 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.

199 Náš pachatel díky tomu ve dvou případech „navštívil" i profily poškozených na sociální síti Facebook, když vyhledal přihlašovací údaje právě v jejich napadených e-mailových schránkách.

200 Vůči bývalé přítelkyni po rozchodu a vůči sestře pro rodinné neshody.

201 Rozesíláním intimních fotografií poškozené a zveřejněním její jinak neveřejné komunikace na Facebooku.

202 Tj. platby prostřednictvím mobilního telefonu.

kreditu na několika pokerových portálech, na nichž hrál.[203] Poslední vybraný pachatel zachytával e-mailovou komunikaci obsahující výrazy jako „platba", „faktura" atp., aby v takových e-mailech následně pozměnil čísla účtů ve svůj prospěch.[204]

Všechny útoky na e-mailové schránky měly až na jedinou výjimku společné **nedostatečné zabezpečení hesla**, které nabývá několika základních podob: jednoduchost, nedostatek fyzického zabezpečení, neměnnost, zranitelnost obnovy. Příliš jednoduché heslo obvinění ve třech případech uhodli (např. heslo v podobě jména poškozené instituce). Fyzicky nezabezpečené heslo využili obvinění 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 partner ho znal ještě z časů bezproblémového soužití.[205]

Nakonec je zde ona zranitelnost obnovy hesla, s jejíž pomocí pachatel snadno obejde i jinak neprolomitelné a bedlivě střežené heslo, a která umožnila i našemu pachateli mnohé uspokojení. Při neoprávněném pronikání do e-mailových schránek byla v nějaké formě využita ve čtyřech případech (z toho ve třech šlo o kontrolní otázku zjišťující rodné jméno matky za svobodna, ve čtvrtém o oblíbenou filmovou postavu).[206]

Za zmínku stojí ještě tři případy již o něco sofistikovanějšího získání hesla, a to prostřednictvím tzv. phishingu, tj. e-mailu tvářícího se jako z důvěryhodného zdroje požadujícího po adresátovi určité jednání nebo informace. Šlo o e-mail zdánlivě pocházející od administrátorů sociální sítě 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.[207]

Samotná aktivita v rámci napadené e-mailové schránky obvykle spočívala v jednoduchém čtení zpráv a prohlížení příloh, případně jejich přeposlání na jinou adresu, ve vyhledání a změně přihlašovacích údajů k dané schránce a dalším aplikacím. Jeden z pachatelů šel dále a vytvořil postupně prakticky plně automatizovaný systém, který v napadených e-mailových schránkách zachytával pro něho zajímavou poštu (obsahující výrazy jako „platba", „faktura" atp.), kterou z napadené schránky dočasně odstranil. Z této dále vyfiltroval e-maily sdělující adresátům čísla účtů pro provedení plateb převyšujících určitou částku, se kterými dále pracoval: změnil platební údaje ve svůj prospěch a pozměněný e-mail „vrátil" původnímu adresátovi, pouze s určitým časovým odstupem, stejně jako

203 Počet poškozených zde dosáhl téměř 300, způsobená škoda téměř 470 tisíc korun (pachatel se pokusil způsobit škodu přesahující 1 milion korun).

204 Někdy své jednání doplnil vytvořením další e-mailové komunikace jménem poškozených – např. zrušil objednaný zájezd u cestovní kanceláře poté, co změnil ve svůj prospěch číslo účtu v e-mailu potvrzujícím rezervaci zájezdu adresovaném poškozené, aby tak oddálil okamžik zjištění jeho podvodu.

205 Zaměřeno pouze na zneužití hesla v souvislosti s neoprávněným proniknutím do e-mailové schránky.

206 Obojí lze při troše štěstí nalézt na sociálních sítích či se jednoduše zeptat pod smyšlenou záminkou samotného budoucího poškozeného (jeden z pachatelů tak úspěšně učinil).

207 V jednom z těchto případů pachatel oslovoval náhodně vybrané osoby, jejichž e-mailové adresy vyhledával na různých inzertních serverech atp.

pro pachatele jinak nezajímavé e-maily, které takto zachytil. Dle své výpovědi tak činil díky softwarové automatizaci prakticky v masovém měřítku, výslovně se zmínil o 20 tisících napadených e-mailových schránek, nicméně odsouzen byl za 5 dílčích útoků se způsobenou škodou necelých 700 tisíc korun.

III.7. Kybergrooming – 3 roky kriminalizace

Kybergrooming, navazování kontaktů s dětmi v online prostředí za účelem jejich sexuálního zneužití, je známý ve světě internetu již nějaký čas. V užším i širším chápání kybergroomingu je jedním z jeho atributů lákání oběti k osobnímu setkání, na což reagovalo trestní právo novou skutkovou podstatou trestného činu navazování nedovolených kontaktů s dítětem (§ 193 b TZ). Ještě před analýzou trestních spisů relevantních pro rok 2015 jsme se proto rozhodli stručně podívat na tuto problematiku pohledem justice, ačkoliv se tematicky poněkud vymyká ostatním částem projektu.[208]

Tak jako provází lidstvo odnepaměti prostituce, nedílnou součástí světa internetu je kybersex. Nejprve v podobě psaného textu, později přišly na řadu obrázky a s růstem přenosové kapacity a rychlosti nezůstaly pozadu ani videa a přenášení zvuku i obrazu v reálném čase.

Kromě zpestření všedního dne dospělých se ale s kybersexem setkávají i dětští uživatelé. Přinejmenším v podobě nevyžádaného kontaktování, mnohdy však i následného posílání fotografií a videí, nemluvě o sexuálně laděné konverzaci (ať už jde o monolog či dialog). V některých případech dojde na základě takové předchozí komunikace i k osobnímu setkání, během něhož je dítě sexuálně zneužito (například k výrobě dětské pornografie).

Průzkumy ukázaly, že takových kontaktů je poměrně nezanedbatelné procento: dle mezinárodního průzkumu EU Kids online v roce 2009 komunikovalo s osobou známou pouze z prostředí internetu 25 % dětí ve věku 9-16 let a 14 % se s takovou osobou i setkalo tváří v tvář (Livingstone, a další, 2016), v roce 2013 to bylo dle průzkumu Univerzity Palackého v Olomouci ve spojení se společnostmi Seznam a Google mezi dětmi ve věku 11-17 let již 53 %, 36 % respondentů by bylo ochotno na takovou schůzku jít (Univerzita Palackého v Olomouci, a další, 2014).

Sílily proto hlasy volající po výraznější prevenci a přísnějším právním postihu. V roce 2014 tak byla po drobných úpravách zavedena do trestního zákoníku mimo jiné nová skutková podstata navazování nedovolených kontaktů s dítětem (§ 193 b TZ). Do té doby bylo možné postihnout kybergrooming de facto pouze v souvislosti s výrobou dětské pornografie a zasíláním pornografie dítěti, případně jako ohrožování výchovy dítěte v důsledku sexuálně laděné textové komunikace a svádění k pohlavnímu styku při nabádání ke svlékání za úplatu před webkamerou atp. Samotné usilování o setkání však bylo trestněprávně postižitelné pouze jako příprava znásilnění (samozřejmě s problematickým

208 Informace zde uvedené proto odpovídají stavu v roce 2017, kdy jsme se tématem zabývali, nicméně časové řady uvedené v tabulce 15 jsou prodlouženy až do roku 2019.

dokazováním subjektivní stránky, tedy úmyslu pachatele). Nová skutková podstata míří již na předstupeň onoho setkání, tedy na jeho návrh, byť i zde musí být prokázán úmysl pachatele dítě nějakým způsobem sexuálně využít.[209]

III.7.1. Kybergrooming

Kybergrooming lze nejstručněji charakterizovat jako kontaktování dítěte za účelem jeho sexuálního využití (Lukášová, 2012). V užším slova smyslu kybergroomer kontaktuje dítě,[210] o němž průběžně zjišťuje informace dostupné z online prostředí. Naváže s ním komunikaci, kterou udržuje relativně dlouhou dobu (může jít i o měsíce). Kybergroomer postupně ladí komunikaci sexuálním směrem, zasílá cizí i vlastní fotografie či videa a zároveň vybízí osobu na druhé straně k zaslání vlastních fotografií, případně usiluje o reálný přenos obrazu.[211] Průběžně kybergroomer nabízí a poskytuje drobné dárky a úplatky (např. kredit do mobilu, koupi herního času oblíbené hry aj.) a buduje s dítětem důvěrný vztah, který prohlubuje předstíranou empatii. Ohroženější jsou proto děti s nějakými vlastními problémy, zejména v sociální oblasti, kterým tak kybergroomer nabízí náhradu za chybějící pocit sounáležitosti, úspěchu, obliby, přátelství či lásky. Postupně začne kybergroomer požadovat osobní setkání s tím, že už mu kontakt pouze prostřednictvím počítače či telefonu nestačí. Pokud dítě odmítá, hrozí ukončením vztahu, a pokud stále odmítá, neváhá přistoupit k vydírání: hrozí např. zveřejněním fotek a videí, která již od oběti obdržel, jejich zasláním rodičům dítěte, do školy, kterou oběť navštěvuje, jejím spolužákům, jejich rozvěšením v okolí bydliště oběti, rozšířením historek o její homosexualitě a sexuálních praktikách atp. Pokud k setkání dojde, kybergroomer zpravidla dítě sexuálně využije, kdy jde zejména o pohlavní zneužití (vzhledem k tomu, že dítě udržovalo vztah s kybergroomerem i několik týdnů až měsíců, pak půjde zřejmě o jednání ze strany dítěte v tu chvíli více méně dobrovolné) a výrobu dětské pornografie.[212]

V širším slova smyslu se kybergrooming odehrává v řádu několika dní, ale i pouhých hodin, i v těchto případech však dochází k usilování o setkání v reálném prostředí. Kybergroomer dítě kontaktuje nejčastěji prostřednictvím sociální sítě Facebook,[213] kde ho požádá 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?*“[214] Kybergroomer posléze posílá obrázky a videa vlastní i cizí, případně virtuální pornografii.[215] Zároveň požaduje fotografie od dítěte na druhé straně: nahé a obnažené nebo alespoň ve spodním prádle. V některých

209 Přičemž tento záměr musí být pojat již v okamžiku navržení setkání dítěti mladšímu 15 let.

210 Respektive vytipovanou osobu – nejčastěji právě dítě (častěji dívku).

211 Požaduje svlékání se před webkamerou, nabádá k plnění jím zadaných erotických úkolů aj.

212 Může ovšem zůstat u méně závažných jednání jako líbání, různé formy hlazení atp.

213 Případně na internetové seznamce nebo chatovací místnosti pro náctileté.

214 Přímé řeči jsou autentickými výňatky z proběhnuvší komunikace mezi některými z usvědčených pachatelů navazování nedovolených kontaktů s dítětem a jejich obětí.

215 Např. pornografické video s postavami z oblíbeného kresleného seriálu.

případech pachatel kromě požadování fotek žádá např. svléknutí se před webkamerou, další obrázky nebo videa či vybízí k jinému jednání se sexuálním podtextem, nezřídka pod hrozbou zveřejnění již získaných fotografií aj. materiálu.[216]

III.7.2. Navazování nedovolených kontaktů s dítětem

V některých případech usiluje o setkání s dítětem v reálném prostředí kybergroomer už po krátké komunikaci, a tomu má právě zabránit skutková podstata navazování nedovolených kontaktů s dítětem. Novela vstoupila v platnost 22. července 2014 a účinnou se stala 1. srpna 2014. Od té doby byla pravomocně skončena již řada trestních řízení, viz tabulka 15.[217]

Tabulka 15: Počet pravomocně vyřízených pachatelů

	2015	2016	2017	2018	2019
	3 odsouzení	6 odsouzených 1x zastaveno[218]	16 odsouzených	18 odsouzených	45 odsouzených
Počet prvopachatelů	2	2	10	11	31
Mladistvý pachatel (ve věku 15-17 let)	-	1	-	1	3
Pachatel ve věku 18-19 let	-	-	1	1	3
Pachatel ve věku 20-24 let	1	2	1	3	8
Pachatel ve věku 25-29 let	2	3[219]	5	8	12
Pachatel ve věku 30-39 let	-	1	7	3	6
Pachatel ve věku 40-49 let	-	-	2	2	10
Pachatel ve věku 50 a více let	-	-	-	-	3
Nepodmíněný trest odnětí svobody	-	1 (věznice s dozorem)	4 (3x věznice s dozorem, 1x s ostrahou)	2 (věznice s ostrahou)	1 (věznice s ostrahou)
Podmíněné odložení trestu odnětí svobody	3 (1 x s dohledem)	5	11 (4x s dohledem)	14 (4x s dohledem)	33 (2x s dohledem)

216 Začínají se objevovat případy vydírání dospělých mužů, kteří se takto nechali zlákat ke kybersexu domnívaje se, že komunikují s mladou slečnou (pachatel hrozí např. zveřejněním komunikace v médiích). Zde ovšem nejde o kybergrooming v pravém slova smyslu, neboť prvotním záměrem pachatele bývá namísto sexuálního uspokojení zisk (Europol, 2017).

217 Tabulka obsahuje vybrané veřejně přístupné statistické údaje (Ministerstvo spravedlnosti), nikoliv kompletní výčet uložených trestů či opatření.

218 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). Za roky 2017-2019 již tabulka zahrnuje pouze odsouzené pachatele.

219 Včetně obviněného, jehož trestní řízení bylo zastaveno, viz předchozí poznámka.

	2015	2016	2017	2018	2019
	3 odsouzení	6 odsouzených 1x zastaveno[218]	16 odsouzených	18 odsouzených	45 odsouzených
Upuštěno od potrestání a uloženo ochranné léčení (§ 47 TZ)	-	-	1	-	1
Uloženo ochranné léčení sexuologické	2	4	8	4	11

Pachatelů bylo nejprve poskrovnu, jak se ovšem dalo čekat vzhledem k relativně krátké účinnosti nové právní úpravy, nicméně jejich počet soustavně narůstá.[220] Všichni dosavadní pachatelé jsou muži a převažují ti ve věku mezi 20 až 29 lety, postupně se však přidávají i starší věkové skupiny.

Co se týče pachatelů pravomocně odsouzených v letech 2015 a 2016, obvykle je 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).[221]

Jejich oběťmi jsou zpravidla dívky ve věku 10-14 let, což pachatelé vědí prakticky od samého počátku (či téměř od samého počátku). Komunikace někdy probíhá převážně jednostranně, kdy pachatel iniciuje konverzaci a v jejím průběhu je aktivnější. Může ale jít i o dialog, kdy oběť nezůstává v sexuálně laděné komunikaci pozadu. K prvnímu kontaktu dochází nejčastěji prostřednictvím sociální sítě Facebook, komunikace pak někdy přechází 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" sociální sítě 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.

Jak je patrné, pachatelé trestného činu navazování nedovolených kontaktů s dítětem poměrně trefně odpovídají charakteristikám kybergroomingu. Lze tedy konstatovat, že tato nová skutková podstata se zdá být vcelku přiléhavou. Pachatel/kybergroomer kontaktuje oběť nejčastěji prostřednictvím Facebooku, oběť se (přinejmenším zpočátku) nebrání, ba naopak s dotyčným dobrovolně komunikuje, případně se nechá zlákat k poskytnutí intimních materiálů (fotografie, videa, online přenos v reálném čase). Návrh setkání pak v takovém kontextu zcela nepochybně sleduje sexuální záměr, ať už osoba na druhé straně odmítá nebo hraje v komunikaci roli téměř rovnocenného partnera.

220 Zde uvedené údaje vychází jak z veřejně dostupných statistických údajů Ministerstva spravedlnosti, tak z analýzy několika vybraných trestních řízení pravomocně skončených v letech 2015 a 2016.

221 Může jít samozřejmě o snahu dosáhnout nižšího trestu s ohledem na obecné zásady pro ukládání trestů (§ 39 odst. 1 TZ).

Pachatelů není mnoho, leč jejich jednání nelze přejít bez povšimnutí ani v případě, kdy na osobní setkání a fyzický kontakt v reálném prostředí nedojde[222] - zejména s ohledem na věk obětí a s tím spojenou naivitu, důvěřivost a omezenou schopnost domyslet důsledky svého jednání v online i reálném prostředí. Zároveň je namístě usilovat o jejich přísnější postih v případě, kdy se neomezí na sexuálně laděnou komunikaci a nabádání k výrobě dětské pornografie, ale usilují i o setkání v reálném prostředí.[223]

222 Uskuteční-li se ono setkání, pravděpodobně dojde ke spáchání dalšího, již přísněji postižitelného trestného činu.

223 Byť jde o přísnější postih de facto pouze ve smyslu zostření trestu v důsledku dalšího sbíhajícího se trestného činu, případně o přitěžující okolnost [§ 42 písm. n) TZ].

IV.

Konzultace s vybranými odborníky

Jak je uvedeno výše,[224] realizovali jsme polostrukturovaný rozhovor s policistou z obvodního oddělení Policie ČR (vedoucí výjezdové skupiny SKPV),[225] vedoucím sekce IT bezpečnosti ve velké soukromé společnosti zařazené do kritické infrastruktury a s řadovým IT zaměstnancem v soukromém sektoru v kategorii SME. Zajímaly nás jejich vlastní zkušenosti s kyberkriminalitou, resp. s jakými jejími projevy se v posledních letech setkali v rámci své profese, co považují v tomto směru za hlavní rizika a hrozby a jaká jsou jejich doporučení pro řešení takových incidentů a pro jejich předcházení.[226]

V souladu s našimi předpoklady zazněla při rozhovorech řada obecně známých informací, o kterých není nutno zde referovat.[227] Přesto každý z nich přinesl trochu jiný úhel pohledu, jiný důraz na to či ono, a především jsme se dozvěděli pokaždé i něco nečekaného. Respondent z řad Policie ČR kladl velký důraz na trestněprávní a přestupkovou rovinu, naproti tomu respondent pečující o kritickou infrastrukturu přistupoval k problematice zejména prizmatem zákona o kybernetické bezpečnosti a související legislativy. Poslední z respondentů pak doplnil předchozí hlediska pohledem řadového IT zaměstnance setkávajícího se s běžnými problémy uživatelů, ať už v souvislosti s plněním pracovních úkolů či zcela mimo ně.[228]

Každý z respondentů měl možnost nejprve hovořit o dílčích jevech v rámci kyberkriminality dle vlastního uvážení, poté v reakci na položené otázky zahrnující námi předem vybraná témata. Jediným takovým jevem, o kterém se ve větší míře zmínili všichni na základě vlastního popudu, byl **ransomware**,[229] jinak byla jejich paleta pestrá a vesměs rozdílná. Spojovali ho s napadáním firemního hardwaru,[230] přičemž výše výkupného bývá podle nich ve známých případech obvykle zvolena tak, aby napadenému subjektu stálo za to zašifrovaná data za takovou cenu zachránit.[231] Nutno ovšem podotknout, že před-

224 Viz Zdroje – konzultace s vybranými odborníky.

225 Coby vedoucí skupiny vykonává dozor nad prací ostatních členů v rámci tohoto oddělení služby kriminální policie a vyšetřování. Kromě toho se sám podílí na provádění běžných policejních úkonů, včetně přijímání trestních oznamování, realizace tzv. neodkladných a neopakovatelných úkonů aj. procesních úkonů.

226 Jeden z respondentů se netajil ani vlastní předchozí zkušeností v roli pachatele.

227 Typicky např. nutnost obezřetnosti při otevírání e-mailů z nedůvěryhodných zdrojů.

228 Oba IT zaměstnanci zajišťují mimo jiné správu a obranu vlastní firemní sítě a serverů.

229 Ať už jako samostatné téma nebo coby dílčí aspekt při používání kryptoměn.

230 Nesetkali se však s tím, že by byl ransomware součást tzv. APT útoku (advanced persistent threat) – sofistikovaného jednání sestávajícího z několikastupňového útoku (Security-Portal, 2013).

231 Není výjimkou, že poškozená společnost sice podá v souvislosti s ransomwarem trestní oznámení, nicméně bez ohledu na to požadované výkupné raději zaplatí.

pokládaná latence je zde značná.[232] Nejlepší vhodnou prevencí se zdá zveřejňování kauz, jednak aby byli uživatelé jednak dostatečně obezřetní, jednak aby preventivně pravidelně zálohovali svá data.[233]

Respondenti dále hovořili z vlastní volby kromě ransomwaru o podvodech v mezinárodním obchodě, dětské pornografii, slabinách infrastruktury (zejména zabezpečení lokální sítě), sociálním inženýrství (e-maily obsahující malware a tzv. baiting[234]), shromažďování dat velkými korporacemi, zabezpečení dat státních institucí, rizicích vyplývajících ze zanedbávání aktualizací, neoprávněných průnicích do lokálních sítí a na servery, využívání cloudů a samozřejmě o zaměstnancích coby potenciálním riziku a lidském faktoru vůbec (zejména neopatrnost spojená s přihlašovacími údaji).[235] Nevynechali ani problematiku odhalování a postihu s ohledem na nadnárodní charakter internetu a s tím spojené jevy jako je obtížná vymahatelnost práva (komplikovaná a zdlouhavá vzhledem k nutnosti přeshraniční spolupráce orgánů činných v trestním řízení) nebo organizovaný zločin disponující téměř neomezenými prostředky.[236]

Z uvedených jevů se podrobněji věnovali především **útokům na firemní sítě a servery**, a to zejména v souvislosti s e-mailovou komunikací a perimetrem mezi vnitřní (lokální) sítí a vnější sítí (Internetem). Na jedné straně dochází k útokům „zvenku", nejčastěji ze zahraničí. Zranitelným místem proto bývá tzv. VPN[237] a tzv. internet věcí, tedy zařízení připojená na internet (např. tiskárna).[238] Jde ovšem i o servery jako takové, neboť ty čelí prakticky permanentním útokům v různých podobách včetně phishingu,[239] kdy se útočník

232 Řada napadených subjektů pravděpodobně útok orgánům činným v trestním řízení vůbec neoznámí, už jen z toho důvodu, že chce napadená zařízení využívat bez přerušení vynuceném jeho nezbytnou analýzou policejním orgánem pro účely vyšetřování. Jiná situace ovšem nastává při detekci útoků směřujících do lokální sítě zvenčí, kdy by s ohledem na jejich množství ani nebylo v silách policejních orgánů se všemi takovými útoky zabývat – žádoucí je proto oznámit pouze takové útoky, o nichž má napadená společnost podrobnější informace, a kde je proto větší šance na případné dopadení pachatele: např. provozní a lokalizační údaje, charakter útoku, jeho směřování, motivace atd. Primárním zájmem napadené společnosti je přitom zpravidla zajistit bezpečnost vlastní sítě, tzn. vybudovat přiměřenou obranu a až poté se zabývat pátráním. Ne vždy se také podaří zajistit důkazní prostředky tak, aby byly použitelné v případném trestním řízení (prokázání, že s daty o proběhnuvším útoku nikdo nemanipuloval).

233 Při „úspěšném" útoku stačí namísto výkupného obnovit data ze záloh.

234 Tj. nastražení nejčastěji USB flash disku obsahujícího malware na místě veřejně přístupném nebo poblíž pracoviště s cílem nechat se zapojit do jinak střeženého zařízení neopatrným nálezcem. Slovy respondenta: *„stačí pohodit flešky"* (úředník či zaměstnanec flešku sebere a zapojí do interního systému, čímž malware nainstaluje).

235 Jimi zmíněná jednání nezahrnují pouze trestněprávně relevantní jednání, ale mají širší záběr.

236 Např. obrovský výpočetní výkon zajištěný armádou podřízených počítačů při DDoS útoku.

237 Virtual private network, vzdálený přístup.

238 Nejsou to však pouze věci / zařízení, ale i běžně používané aplikace, o nichž útočník ví, že je napadený subjekt využívá. Problematické proto mohou být i různě poskytované cloudové služby, včetně hostingu, kdy správci poskytované služby nezbývá než se spolehnout na dostatečnou obezřetnost a včasné aktualizace ze strany koncových uživatelů.

239 Útočníci zřejmě ustupují od bankovních aj. služeb, které využívají technologii 3D Secure a své klienty na rizika upozorňují, směrem k PayPal, eBay atp., kde stačí autentizace v podobě uživatelského jména a hesla.

snaží umístit na ně např. odkaz na falešné stránky či jiný obsah: „*Prostě máte nějakýho robota, který prochází internet, zkouší různý IP adresy, zkouší co tam je na nich dostupnýho… to jsou prostě roboti, který to imrvére zkoušej.*“ Zejména pak ve spojení s nedostatečnými **aktualizacemi** představují jakákoliv zařízení riziko, neboť útočník se může dostat jejich prostřednictvím „dovnitř“ lokální sítě, pokud např. zná cílové zařízení (např. konkrétní typ tiskárny) nebo aplikaci či program a jeho zranitelnost.[240] Samotný útok pak probíhá např. s využitím tzv. exploitu – malwaru určeného k určitému jednání (např. exploit umožňující využít konkrétní chybu v kódu operačního systému Windows XP): „*Když člověk dobře zná ten systém, jakej chce napadnout, tak má docela reálnou šanci, jak to napadnout nebo se tam dostat*.“

Klíčovou roli hraje v tomto směru **ochranný software**, tedy zpravidla firewall a antivirus, který má za úkol zamezit nežádoucím příchozím požadavkům, aniž by byly vpuštěny do vnitřní sítě. Z hlediska ohrozitelnosti zařízení hraje vždy důležitou roli čas, neboť i včasná aktualizace znamená aplikaci tzv. záplaty[241] až s určitým časovým odstupem, přičemž po celou tuto dobu jsou všechna zařízení daného typu zranitelná.[242] Od toho se odvíjí i preventivní doporučení,[243] jimž dominují včasné a opakované aktualizace (na všech úrovních), dále používání VPN jen v nezbytných případech a se zabezpečením,[244] omezení přístupu ze zahraničí, resp. omezení a kontrola veškerého příchozího provozu, zabezpečení lokální sítě ochranným softwarem[245] a uchovávání logů,[246] sledování neobvyklých událostí v lokální síti (např. náhle zvýšený provoz na určité IP adrese).[247]

240 Zatímco společnosti svou ochranu stále vylepšují, domácnosti směřují s připojováním dalších a dalších zařízení k rizikovému stavu, zejména ve spojení s laxností mnoha běžných uživatelů co do zajišťování ochrany v oblasti informačních a komunikačních technologií – např. nepoužívají žádná nebo jen jednoduchá hesla pro přístup do lokální sítě a přistupují na trend all-in-one chytré domácnosti, často propojené s mobilními telefony. Slovy respondenta: „*Dokážu si představit, že takhle napadnou ty* (řadové – pozn. taz.) *uživatele… ty to třeba neřešej, ty prostě dostanou modem nebo maj doma nějaký modem a neřeší nějaký nastavení, maj to tam všechno otevřený, že jo, a ten útočník se dokáže dostat do toho zařízení přes defaultní nějaký přihlašovací údaje, a tam vidí všechny počítače, že jo, který jsou na síti, a zkouší to dál do sítě, že jo, jakoby se dostat do dalších počítačů, klidně i třeba na televizi, do Xboxu, to už je v podstatě jedno, všechno už je dneska připojený k internetu, takže už se dá dostat všude*.“

241 Oprava zjištěné bezpečnostní slabiny.

242 Obvykle někdo objeví zranitelnost, vytvoří k jejímu využití exploit, ten se následně začne šířit a až po určitém čase a množství útoků tento exploit zachytí i ochranný software coby podezřelou komunikaci v síti a následně ho začne blokovat (samotné koncové zařízení tak činí až po stažení příslušné aktualizace).

243 Chybám ve zdrojovém kódu včetně bezpečnostních trhlin se totiž nelze dost dobře nikdy vyhnout: „*Obecně se říká, že na 100 řádků programového kódu je jedna chyba, takže když pak máte 10 tisíc, že jo, nebo 100 tisíc nebo i miliony řádků, tak těch chyb je tam strašně moc*.“

244 Slovy respondenta „*Jedna věc je dostat se za ten port, za ty dveře* (míněno využívání VPN – pozn. taz.)*, a pak za těma dveřma máte nějakou službu, kde už je nějaký ověřování, uživatelský jméno a heslo, takže tam už to může zkoušet* (míněn útočník – pozn. taz.)*, ale první věc je, že se musí dostat za ty první dveře, který jsou zamčený pro něj, že jo, což my zamykáme…*“

245 Množství útoků nezřídka dosahuje i milionů pokusů o neoprávněné překonání firewallu denně.

246 Informace o veškerém toku dat mezi vnitřní a vnější sítí.

247 To ovšem předpokládá dobrou znalost konkrétní sítě a jejího provozu, přičemž tuto zkušenost lze nabýt pouze vlastní praxí v dané společnosti: „*Každej ajťák si to dělá prostě po svým* (míněna správa systému – pozn. taz.)*… takže co ajťák, to bejvá ves*.“

V rámci firem však IT správci obvykle výše uvedených pravidel dbají, a proto bývá častější napadání lokální sítě „zevnitř", kdy např. neopatrný **zaměstnanec** otevřením přílohy e-mailu obsahující malware na počítači v rámci lokální sítě do ní útočníka vpustí: „*největší hrozba je od těch uživatelů, který jsou v tý lokální síti.*"[248] Dostáváme se tak k zaměstnancům coby výraznému rizikovému faktoru.[249] Jejich slabou stránkou bývá právě e-mailová komunikace,[250] dále pak přihlašovací údaje a fyzická ochrana zařízení a přihlašovacích údajů. Při e-mailové komunikaci sice někdy zaměstnanci sami správně vyhodnotí nedůvěryhodnost e-mailu, aniž by byl tento detekován ochranným softwarem, nicméně čas od času jsou to naopak zaměstnanci, kdo se nechá oklamat (mnohdy navzdory interním bezpečnostním zásadám): „*Máme sice nakázaný, aby jakoukoliv podezřelou komunikaci hlásili* (zaměstnanci – pozn. taz.)*, ale prostě podaří se… V dnešní době ty e-maily už jsou tak důvěryhodný, že to ty lidi dokáže zmást a otevřou to, co otevřít nemaj a ty skripty, co můžou něco udělat, můžou bejt v Excelu, můžou bejt ve Wordu, můžou bejt v [pédéefku]… takže už to není jako dřív, že to byl nějakej exáč nebo něco takovýho, kterej byl docela snadno odhalitelnej, ale dneska už je to docela sofistikovaný.*" Preventivní doporučení je v tomto směru poměrně jednoduché: „n*epouštět lidi do počítačů*".[251] Mimoto by mělo být v každé společnosti samozřejmé školení zaměstnanců v oblasti bezpečnosti informačních a komunikačních technologií, včetně jejich seznámení s aktuálními jevy a praktickými příklady. To vše v kombinaci s technickým zabezpečením všech zařízení, včetně dvoufaktorové autentizace.

Ta je žádoucí i v dalších směrech, např. při potvrzování důležitých informací, typicky u čísla účtu pro zaslání platby – útočník někdy napadne obsah e-mailové schránky tím způsobem, že např. přepíše ve svůj prospěch čísla účtu uvedená v e-mailu obsahujícím platební údaje.[252] V tomto směru by pomohla větší publicita věnovaná podobným kauzám, aby byli uživatelé dostatečně obezřetní.

Další rizikový faktor představují u zaměstnanců i řadových uživatelů **přihlašovací údaje**, od jednoduchosti hesel přes stejná hesla napříč mnoha aplikacemi až po jejich fyzické nezabezpečení (např. heslo napsané na papírku přilepeném na monitoru).[253] Jednoduchost hesel (a jejich snadné zapamatování) jde pak ruku v ruce se snadnou zjistitelností. Jednak prostým uhodnutím, jednak při použití brute force,[254] jednak pomocí sociálního inženýr-

248 Jinými slovy *„zlaté přání administrátorů je mít síť bez uživatelů."*

249 Se zdokonalováním ochrany po technické stránce budou v budoucnu nejspíš právě zaměstnanci představovat hlavní zranitelný bod důležitých informačních systémů (např. v elektrárně).

250 *„Stačí podvržený odkaz a 1 klik."*

251 Přesněji řečeno nedávat zaměstnancům administrátorská práva umožňující dělat v používaných zařízeních změny, instalovat software atp. Žádoucí je pak doplnit přísná pravidla dobrou komunikací mezi IT oddělením a ostatními zaměstnanci tak, aby tito vždy raději bez obav požádali o pomoc či radu IT oddělení namísto vlastní svévolné aktivity.

252 Pokud se k samotnému neoprávněnému přístupu do e-mailové schránky přidruží i takto dokonaný podvod, poškozený již takové jednání obvykle oznámí Policii ČR.

253 Slovy respondenta *„Jakmile nemáte fyzickou bezpečnost, nemáte nic!"* Z toho důvodu není příliš žádoucí trvat na tom, aby zaměstnanci svá hesla pravidelně obměňovali, neboť to obvykle vede k fyzickému nezabezpečení, protože hesla se nakonec vždy povalují někde na papíře.

254 Hrubá síla - např. robot zkoušející jedno slovo za druhým.

ství.[255] Zde je ovšem také poměrně snadná pomoc, protože i slabé nebo kompromitované heslo lze doplnit další úrovní obrany, a to volbou uživatelského jména, které může fungovat de facto jako druhé heslo: „*Když si dáte jako uživatelský jméno nějaký nesmysl, tak v podstatě máte dvě hesla, který musí ten útočník rozluštit: jednak uživatelský jméno, jednat to heslo, takže tím se dá taky dost rapidně ztížit ten samotnej průlom do toho systému*." Při používání stejného hesla napříč různými aplikacemi (a systémy) může podat pomocnou ruku tzv. klíčenka neboli správce hesel, díky němuž lze používat řadu silných hesel, aniž by je musel uživatel vymýšlet (díky možnosti vygenerování hesla) nebo si je pamatovat, nutno však uvážlivě vybrat, komu hesla svěřit.[256]

Zde se dostáváme ještě k jiné oblasti, a to uchovávání dat v cloudu. Ač by tomu tak být nemělo, řada osob využívá cloudové služby, aniž by si třeba plně uvědomovaly důsledky cloudu:[257] fyzické umístění dat na serveru – počítači spravovaném třetí osobou,[258] který může spadat i pod zcela jinou jurisdikci a pravidla nakládání s osobními údaji. Problematický je v tomto směru zejména outsourcing služeb ve spojení s orgány státní správy a jejich registry. Podobně i otázka zajištění důvěrnosti a přístupnosti dat (pouze) pro oprávněné subjekty.[259]

Na jedné straně tak máme bezpečnostní otázky spojené s důvěrností dat, na straně druhé pak množství dat a osobních údajů poskytovaných jednak dobrovolně na sociálních sítích atp.,[260] jednak nedobrovolně.[261] Množství takto dostupných údajů pak zdaleka přesahuje použitelnost pro personalizaci reklamy aj. obsahu. Kromě reklamní manipulace nepochybně probíhá na základě takto zjišťovaných dat i politická propaganda včetně manipulace voličů před volbami.

255 Vyzvídání hesla pomocí sociálního inženýrství může proběhnout kdekoliv, např. v hospodě u piva: *„Jak máš silný heslo? To moje má 10 znaků. -… to moje má jenom 6 znaků… – A co nějaký čísla, máš? Já jo. – Jasně, mám tam 3 čísla, taky hvězdičku…"* Každá taková informace výrazně zjednodušuje odhalení přes brute force a zkracuje dobu pro prolomení (útočník např. zná délku hesla a ví, že neobsahuje žádné číslo).

256 Např. Google jako jejich správce by neměl představovat riziko, neboť důvěra uživatelů v jeho bezpečnostní protokoly je pro něj nepochybně cennější než samotné osobní údaje, na druhou stranu s sebou nese oprávněné obavy z množství osobních údajů, kterými disponuje.

257 Cloudové služby využívá např. i hojně používaný Microsoft Office 365.

258 A s tím případně spojená rizika např. liknavých aktualizací zabezpečení nebo zneužití samotných dat. Může dojít i k selhání lidského faktoru a např. smazání dat chybou programátora pečujícího o server – nutno mít v tomto směru na paměti, že i cloudová data vyžadují zálohování.

259 Např. v souvislosti s elektronizací zdravotnických záznamů, uchovávání vzorků DNA Policií ČR, zabezpečení dat EET atp.

260 Včetně kvazidobrovolně poskytovaných dat dalšími osobami – typicky např. informace na sociálních sítích zveřejňované o někom jiném, včetně fotografií atp. Jen někteří uživatelé si také uvědomují, že např. aplikace nabízené „zdarma" (typicky např. některé hry pro mobilní telefony) zpravidla zdarma nejsou, neboť namísto přímé platby např. zpeněží vybraná uživatelská data.

261 Např. provozní a lokalizační údaje.

IV.1. Několik dalších poznámek

O výše uvedených oblastech v nějaké podobě hovořili vesměs všichni tři respondenti, každý z nich však podrobněji hovořil i o nějaké další. Jedním z takových dílčích témat, které zmínil příslušník Policie ČR, byla dětská pornografie, zejména ta vytvořená zobrazenými dětmi vědomě a dobrovolně.[262] Relativně běžně dochází k neoprávněnému přístupu k profilu na Facebooku, stažení uložených fotografií (pornografických i jiných) a jejich následnému šíření: nejčastěji umístěním na falešném profilu (opět na Facebooku) nebo prodejem některému z pornografických serverů. V závažnějších případech jde o děti výrazně mladší 15 let a hromadné šíření, např. v rámci školní třídy či celé školy jakou součást kyberšikany.[263] Dochází též k zakládání falešných profilů dospělými osobami za účelem vylákání **sexuálně laděného obsahu** a následného vydírání jeho prostřednictvím.[264] Orgány činné v trestním řízení se dozví pravděpodobně o minimu případů, mnohdy zcela náhodou v souvislosti s vyšetřováním jiné trestné činnosti pachatele. Překvapilo nás, že na otázku po preventivních doporučeních respondent uvedl jediné, a to větší kontrolu sociálních sítí.[265]

Další respondent by byl naopak opatrný s doporučováním jakékoliv kontroly internetu, neboť ten už nyní podle něj funguje jako velký sledovací systém: „*lidi musej pochopit, že internet je sledovací technologie*." Hovořil např. o (nezákonném) detekování klíčových slov vyhledávaných online nebo odposlechu a automatizované analýze VoIP[266] ze strany bezpečnostních složek. Přesto i on doporučoval větší kontrolu sociálních sítí, ovšem ze strany rodičů, nikoliv státem.

Při podrobnějším dotazování na další jevy respondenti shodně hovořili především o aktuálnosti problematiky **kryptoměn**. Zejména bitcoiny nachází s ohledem na extrémně obtížnou stopovatelnost uplatnění v řadě nelegálních činností, od plateb při ransomwaru nebo za nelegální zboží a služby po podvody s bitcoiny samotnými. O mnoho větší problém by však představovalo ovlivnění samotného systému, a to buď schopností falšovat transakce,[267] anebo svévolně získat přístup k uloženému bitcoinu, neboť v takovém případě by se celý systém zhroutil. Zejména v druhém případě by šlo o závažný problém ohrožující

262 Ohroženy jsou zejména děti sdílející vlastní sexuálně laděný obsah na sociálních sítích (nemusí jít výslovně o pornografii).

263 O kyberšikaně formou zveřejňování fotografií (pornografického nebo difamujícího charakteru) hovořil i další z respondentů v souvislosti s poskytováním hostingu. Zmínil se také o jiné špatné zkušenosti s hostingem, a to opakované řešení (nedobrovolné) dětské pornografie zobrazující velmi malé děti a odkazující na různá pornografická fóra.

264 De facto různé podoby kybergroomingu v širším pojetí, viz Kybergrooming.

265 Očekávali jsme obvyklou odpověď zdůrazňující osvětu a varování před vytvářením kompromitujícího obsahu.

266 Voice over internet protocol – zjednodušeně řečeno telefonování online.

267 Pokud by nějaký tzv. těžařský pool dokázal sdružit tolik dílčích těžařů, že by obsáhl nadpoloviční většinu těžebního výkonu, mohl by určovat, komu připadne vytěžený bitcoin a zpětně falšovat proběhnuvší transakce. Blíže k technologii bitcoinů viz (Kudrlová, 2015).

de facto celý internet, neboť by to předpokládalo schopnost vypočítat z tzv. hashe privátní klíč,[268] přičemž zabezpečení prostřednictvím hashe je technologie používaná napříč internetem (a jinde), včetně např. šifrování komunikace.[269]

Respondenti se dále vyjadřovali např. k tématu tzv. fake news a (nejen) politické propagandy, ochraně dětí před kyberšikanou nebo terorismu online, naopak tzv. nigerijské dopisy nebo sběr cookies považovali za zanedbatelný problém.[270]

Zatímco při výběru témat volili respondenti odlišně, na některých obecných vyjádřeních a preventivních opatřeních se poměrně shodovali, ač je zmiňovali v souvislosti s různými jevy. Shodně označovali jako velkou slabinu neznalost hrozeb a **lidský faktor**: „*nejslabším článkem všech útoků jsou lidi, největším rizikem lidský faktor.*" Velká část útoků proto podle nich míří na řadové uživatele, ačkoliv ti si to nepřipouští: „*Já to chápu… nikdo si neříká* (přesněji 'kdekdo si říká' – pozn. taz.) *'kdo by na mě útočil', ale není to o tom, že si někdo někoho vybere, ale zkoušej to ty roboti, že jo – zkoušej se dostat, získat data, něco nasadit třeba, třeba prostě jenom na odesílání e-mailů, že jo – potřebujete taky nějaký počítače, abyste přes ně mohli odesílat nějakej spam, protože spamování je samozřejmě trestnej čin.*" Právě člověk může mnohdy prostým zdravým rozumem rozpoznat např. podvodný e-shop, který začal fungovat krátce před vánočními svátky a nabízí podezřele levné zboží. Zranitelné jsou známé systémy, resp. hojně využívané systémy a jejich chyby (např. konkrétní služba VoIP).

Obecná preventivní doporučení zahrnují na technické úrovni především již zmíněné používání ochranného softwaru a jeho včasné aktualizace, také aktualizace veškerých používaných programů. Samozřejmostí by měla být náležitě silná hesla, resp. silná dle významu chráněného přístupu.[271] Uživatelé by se měli chránit především sami,[272] měli by ovšem být zpravováni o aktuálních jevech (např. formou informování o proběhlé kauze v televizním zpravodajství). Stát by měl investovat do policejních orgánů tak, aby se mohly vyrovnat kvalitou expertů možnostem organizovaného zločinu.[273] To i s ohledem na to, že

268 Zjednodušeně řečeno privátní klíč představuje např. dlouhou číselnou řadu, přičemž hash tuto řadu příslušným algoritmem výrazně zkracuje. Sebemenší změna v privátním klíči vede ke změně hashe, a je proto snadno odhalitelná, zatímco zpětný výpočet privátního klíče při znalosti pouze hashe je prakticky nemožný. Při extrémně velkém výpočetním výkonu to však není vyloučeno, pouze to v současnosti zřejmě není v reálných silách kohokoliv.

269 Šifrování komunikace jak mezi jednotlivci, tak používané státem. Její rozklíčování třetí osobou by tak znamenalo např. možnost upravit zasílanou zprávu dle svého, aniž by byla její úprava patrná, a tudíž by byla považována za pravou.

270 Nikoliv neaktuální, nýbrž zanedbatelný s ohledem jednak na všeobecné povědomí o něm, jednak vzhledem k předpokládanému malému množství poškozených a způsobených škod.

271 Např. heslo k přístupu na fanouškovský web oproti heslu do uzavřené firemní databáze obsahující důvěrné informace.

272 Děti navíc rodiči, zejména v jejich aktivitách na sociálních sítích. Do osvěty by se měla zapojit i školská zařízení a zejména zdůraznit, že *„co internet schvátí, to už nenavrátí."*

273 Chybí ovšem i prosté školení řadových policistů zaměřené na práci s důkazními prostředky v oblasti informačních a komunikačních technologií.

v online prostředí roste majetková kriminalita, zvláště pak v souvislosti s kryptoměnami. Žádoucí by bylo též sledovat statistické údaje vypovídající o proběhlých incidentech, problém však představuje jejich (ne)měřitelnost a (ne)srovnatelnost.

V budoucnu budou zřejmě častější teroristické útoky (třeba i po letech sledování cíleného systému a hledání jeho slabin), nepochybně však budou dále pokračovat stávající hrozby v podobném duchu jako doposud, ovšem bude se dále rozšiřovat spektrum připojených, a tudíž napadnutelných zařízení. Napadány budou korporace i jednotlivci, jejich majetková sféra i osobní údaje, nicméně s jednotnou převažující motivací: „n*a konci vždycky budou prachy, v konečným důsledku*."

v.

Dotazníkové šetření

Významnou součást řešeného projektu představuje dotazníkové šetření, avšak vzhledem ke komplikacím v souvislosti s nákazou COVID-19 na jaře a na podzim roku 2020 došlo k jeho zpoždění.[274] Výsledky a podrobné údaje budou proto publikovány samostatně v roce 2021, zde uvádíme jen základní informace.

Šetření proběhlo metodou self-reportu s využitím interaktivního online dotazníku zpřístupněného vybranému vzorku uživatelů internetu ve věku 16-74 let. S ohledem na okolnosti (COVID-19) nám nezbylo než opustit původní ideu dotazování probíhajícího metodou CAPI ve prospěch CAWI.[275] Vybrané věkové rozmezí vzorku umožňuje alespoň základní srovnání výsledků s údaji dostupnými prostřednictvím statistického úřadu Evropské unie Eurostat. S ohledem na zaměření dotazníku (kyberkriminalita) i zvolenou metodu dotazování odpovídají kvóty výběrového souboru internetové, nikoliv obecné populaci.[276]

Dotazování bylo zaměřené na tři oblasti, a to sebeochranu uživatelů informačních a komunikačních technologií, míru jejich viktimizace vybranými jevy (zejména různými formami podvodného jednání) a v neposlední řadě na jejich zkušenosti v roli pachatele, včetně zohlednění aktivit a zařízení spojených se zaměstnáním. Ptali jsme se proto především na zařízení používaná k přístupu na internet,[277] obchodování online (prostřednictvím e-shopů i inzertních portálů a v roli kupujícího i prodávajícího), používání internetového bankovnictví (svého i cizího), ransomware (v roli poškozeného i původce), sociální inženýrství v podobě nevyžádaných e-mailů požadujících zaslání peněz nebo sdělení osobních údajů (opět v roli poškozeného i původce), ochranu vlastních a přístup k cizím e-mailovým schránkám, používání sociálních sítí (vlastní i cizí účty a vybrané formy jejich zneužití) a nakonec na zkušenosti uživatelů s online herními účty.

Jednotlivá témata byla zvolena tak, aby se nepřekrývala s **dostupnými statistickými údaji** počínaje rokem 2015.[278] Eurostat hovoří např. o rozličných aktivitách online a používání internetu a počítačů vůbec, zkušenostech s podvody s platebními kartami a podvodnými maily (obecně), množství osob používajících internetové bankovnictví, obchodování online (včetně negativních zkušeností, obav a množství mladých uživatelů), počtu online hráčů, bezpečnostních obavách a opatřeních uživatelů (např. zálohování) včetně zabezpečení chytrých mobilních telefonů, péči o vlastní soukromí online (včetně např. používání sociálních sítí), využívání internetu a informačních a komunikačních technologií zaměstnanci (včetně školení o jejich bezpečném využívání), negativních zkušenostech

274 Zejména v důsledku hygienických opatření a omezení volného pohybu.

275 CAPI (computer assisted personal interviewing) označuje dotazování respondenta tazatelem tváří v tvář s využitím počítače (tabletu) namísto papírového dotazníku. Naproti tomu při použití CAWI (computer assisted web interviewing) respondent přímo vyplňuje dotazník přístupný přes webové rozhraní.

276 Zohledňují dostupné statistické údaje Českého statistického úřadu o počtech uživatelů internetu s ohledem na různé sociodemografické údaje.

277 Zejména mobilní telefon, stolní počítač, notebook a tablet.

278 Podrobná rešerše dostupných statistických dat bude publikována samostatně spolu s výsledky dotazníkového šetření.

s incidenty v oblasti informačních a komunikačních technologií ze strany zaměstnavatele, o IT sektoru (např. počet IT zaměstnanců), používání sociálních sítí, o napadení e-mailové schránky nebo účtu na sociální síti.[279]

Eurobarometr se zaměřuje na rozličné aktivity online a používání internetu vůbec (asebeomezování kvůli obavám ze zneužití online prostředí), nezákonný obsah (včetně reakce na něj, podvodů nebo porušování autorského práva), vnímání bezpečnosti, obchodování online (a přidružené obavy), viktimizaci ransomwarem, veřejné mínění o bezpečnosti a vymáhání práva mimo jiné v oblasti kyberkriminality (včetně transakcí a obchodování online, obtěžování zejména dětí, viktimizaci kyberkriminalitou, obavy o vlastní osobní údaje), krádež identity, malware, zneužití e-mailové schránky a sociálních sítí, podvody, dětskou pornografii, extremismus, fake news, ochranu vlastního soukromí online (např. přístup ke cookies), používání různých zařízení a jejich ochranu, důvěru ve vyhledávače a jejich používání, mínění o personalizaci obsahu, ochranu osobních údajů online, obavy v online prostředí, používání různých komunikačních prostředků online, důvěru v různá média (včetně sociálních sítí), fake news a extremismus, na organizace aktivní online (včetně např. e-shopu nebo vlastní sebeprezentace) nebo přeshraniční přístup k online obsahu.

Český statistický úřad poskytuje např. informace o používání internetového bankovnictví (počet uživatelů a jejich obavy, zkušenost s phishingem), krádeži identity, nakupování online (včetně sociodemografických údajů a negativních zkušeností kupujících), podvodných e-mailech, napadení virem, obavách při používání Wi-Fi nebo při stahování z internetu, obavách o soukromí a napadení účtu na sociálních sítích, o zneužití osobních údajů k šikaně či vydírání.

V publikacích z dílny IKSP je možné najít odpověď na používání internetu seniory a žádost o poskytnutí přístupových údajů k platební kartě či internetovému bankovnictví osob věku 65-80 let (Martinková & Biedermanová, 2019), dále informace o viktimizaci v souvislosti s nakupování online a podvodnými e-maily (Roubalová, a další, 2019). Agentura MEDIAN, s. r. o., vypovídá např. o bezpečnostních opatřeních uživatelů, včetně nastavení soukromí a používání Facebooku. IPSOS, s. r. o. se zaměřuje např. na fake news, obavy o soukromí online a bezpečnostní opatření (např. dvoufázové ověřování hesel), na internet coby usnadnění života. Agentura STEM/MARK, a. s., sleduje např. obavy ze zneužití e-mailové schránky nebo mediální gramotnost. CVVM[280] se dotazovalo na zařízení používaná k přístupu na internet a sledování celospolečenského dění online. V neposlední řadě pak velký mezinárodní projekt ISRD[281] zjišťoval názory mladých respondentů mimo jiné na nelegální stahování hudby a/nebo filmů a zesměšňování online.

279 Některé údaje se vztahují k internetové populaci, některé k obecné populaci a některé k osobám ve věku 16-29 let.

280 Centrum pro výzkum veřejného mínění - výzkumné oddělení Sociologického ústavu AV ČR.

281 International Self-Report Delinquency Study.

VI.

Závěr – sporná témata, sebereflexe a nástin budoucího výzkumu

Projekt zabývající se kyberkriminalitou s sebou přinesl hned několik výzev. Předně se jednalo vůbec o **vymezení výzkumného pole**, ať už z hlediska projektu jako takového či jednotlivých částí. Vzhledem k faktu, že online prostředí v současnosti představuje prakticky odraz toho reálného spíše než pouhý jeho doplněk, šíře trestněprávně relevantního jednání obdobně odpovídá tomu v reálném prostředí. Bylo proto nezbytné zúžit sledovanou oblast, tedy vybrat taková témata, která jsou kyberprostoru vlastní, přičemž jejich výčet zdaleka není vyčerpávající.[282]

V online prostředí najdeme zastoupení prakticky všech druhů kriminality – majetkovou, mravnostní, hospodářskou kriminalitu atd. Snad pouze námi vytvořenou kategorii virtuálního násilí lze jen stěží přirovnat k násilné kriminalitě v reálném prostředí, pokud si vezmeme za rozlišující faktor prvek „násilí" tak, jako ho vymezuje trestní zákoník (§ 119 TZ), tedy s důrazem na použití fyzické síly k překonání nebo zamezení odporu (Šámal, a další, 2012, str. 1306). Jestliže však toto hledisko opustíme a vezeme naopak za své kriminologické pojetí násilí, přiblížíme se spíše obsahu pojmu „agrese", který již zahrnuje nejen fyzickou, ale i psychickou bolest (Gřivna, a další, 2019, str. 273).

S virtuálním násilím souvisí i další výzva, a to kategorizace sledovaných jevů a jejich operacionalizace. Trestní spisy zabývající se počítačovými trestnými činy nebyly dosud analyzovány, a některé indikátory (i některé znaky) se tak ukázaly v praxi oproti očekávání poměrně problematické. Nejpatrnější změnu představovalo **vytvoření kategorie zahrnující majetkový zájem a virtuální násilí** (a jiné) namísto původního rozdělení na majetkovou trestnou činnost, útoky na osobnost a útoky na osobní údaje (a jiné). Životaschopnost uvedeného členění bychom si v budoucnu rádi ověřili.

Při analýze trestních spisů jsme se rozhodli zúžit sledovanou oblast na **počítačové trestné činy**. Připravili jsme se tak o řadu nepochybně zajímavých údajů, které bychom mohli vyčíst z vybraných kauz věnujících se podvodnému jednání online, sexuálnímu zneužívání online atp. V opačném případě bychom se však potýkali se značnými praktickými obtížemi při identifikaci relevantních spisů. Učinili jsme tak navzdory vědomí, že řada trestních řízení zahrnujících počítačový trestný čin nám zůstala přesto skryta, neboť orgány činné v trestním řízení pravděpodobně daná jednání nekvalifikují vždy jako souběh s počítačovým trestným činem, byť by to bylo namístě.[283]

Rozsah sledovaných počítačových trestných činů jsme dále omezili na ty, v nichž byla podána obžaloba a trestní řízení pravomocně skončilo v roce 2015. Hlavním důvodem byla dostupnost spisů již v roce 2017 a možnost zpracovat z hlediska lidských sil prakticky všechny relevantní spisy pro vybrané období.[284] Předložená analýza je ovšem míněna i jako základ pro budoucí srovnání dalších let a výchozí bod pro sledování dynamiky počítačových trestných činů.

282 S jednáním vpravdě „kybernetického" charakteru per se jsme se setkali jen v mizivé míře.

283 Jde o namátková zjištění, která by v budoucnu zasloužila více pozornosti a ověření.

284 Byť mají získané údaje ze statistického hlediska jen omezenou vypovídací hodnotu vzhledem k hraničním počtům případů.

Naproti tomu o výrazně širší pokrytí kyberkriminality jsme usilovali při přípravě **dotazníku** určeného internetové populaci. Vzhledem k předpokládané vysoké míře latence jsme zvolili formu self-reportového šetření s nadějí, že zjištěné údaje o zkušenostech respondentů v roli pachatelů budou alespoň částečně odpovídat informacím od obětí a napoví nám více o skutečné kriminalitě online. Dotazníkové šetření se dále potýká s problematikou výběrového souboru, který zahrnuje internetovou populaci. Dostupné statistické sociodemografické údaje o osobách používajících internet jsou nápomocny pouze částečně, neboť závisí na definici „uživatele", která není ustálená ani jednotná.

V rámci referovaného projetu jsme zvažovali realizaci expertního šetření zahrnujícího vždy několik osob v určité kategorii: komerční sektor (společnosti podnikající v oblasti informačních a komunikačních technologií, kritická infrastruktura), neziskový sektor (organizace zabývající se osvětou), NÚKIB, justice (jednotlivé orgány činné v trestním řízení, znalci, advokáti), akademická sféra. Od původního záměru jsme však ustoupili a spokojili se s několika **odbornými konzultacemi**. Zvažujeme zahrnutí rozhovorů s experty do budoucího projektu, avšak předpokládáme, že zjištěné informace budou z valné většiny odpovídat předem známému zaměření respondenta a veřejně dostupným informacím (např. poskytovatel ochranného softwaru a trendy kybernetických útoků technického charakteru). Expertní rozhovory proto zůstávají do budoucna zatím otevřeným tématem.

V příštích letech bychom rádi zrealizovali obdobný, **navazující projekt**. Nepochybně přínosná bude opět analýza trestních spisů zahrnujících počítačové trestné činy, ovšem tentokrát již s výběrem vzorku namísto zpracování prakticky všech relevantních, vzhledem k rapidně narůstajícímu počtu případů. Zvážíme též zahrnutí i jiných skutkových podstat, především podvodu (§ 209 TZ), pravděpodobně formou případové studie.

Budeme-li mít tu možnost, zopakujeme též dotazníkové šetření určené široké populaci, které bude částečně srovnatelné s již realizovaným. Srovnatelné pouze částečně z toho důvodu, že s ohledem na nyní zjištěné poznatky přizpůsobíme jednotlivá témata a formulace otázek tak, aby lépe pokrývaly sledované jevy, nerozptylovaly pozornost respondenta marginálními tématy a zachytily aktuální trendy.

Bez ohledu na případný navazující projekt se však budeme dále věnovat i některým dílčím tématům, k jejichž zpracování dosud nedošlo, ač by ho zasluhovaly: např. skupině mladších recidivujících pachatelů oproti starším prvopachatelům nebo pachatelům starším 40 let a recidivistům vůbec, charakteru útoku (např. využití příležitosti nebo využití znalosti), vlivu různých faktorů na poměr délky přípravného řízení oproti řízení před soudem, podrobnější srovnání sociodemografických údajů pachatelů kyberkriminality a celkové kriminality (včetně samostatného porovnání pachatelek), (ne)odsouzení v souvislosti s trestnou činností na hraně kyberšikany ve spojení s věkem obviněných, neopatrnost uživatelů (včetně zaměstnavatelů a bývalých zaměstnavatelů). Za pozornost by v budoucnu jistě stála také aplikace teorie sociální dezorganizace v online prostředí.[285]

Jak se ukázalo při bližším pohledu na skutky pravomocně odsouzené v roce 2015, řadu z nich lze označit za **skoro až banální jednání**: např. nahlédnutí do manželova mobilu

285 Absence sociální kontroly, vysoká heterogenita osob, chování a hodnot atd., viz chicagská škola.

a přeposlání si několika jeho SMS ze žárlivosti. Co na tom, že na takové situace pamatuje trestní řád zásadou oportunity a možností odklonu, když už není možné využít zásady subsidiarity trestní represe. Samotný fakt trestního řízení nepochybně značně ovlivní život obviněného a odčerpává z justice finanční i časové prostředky, které by zajisté našly uplatnění i jinde. Zároveň není možné zmírnit formulaci samotných základních skutkových podstat § 230 TZ vyplývajících z mezinárodních závazků České republiky, zejména Úmluvy o počítačové kriminalitě požadující dokonce kriminalizaci přípravy neoprávněného přístupu k počítačovému systému a nosiči informací.

Pakliže by se tato situace měla změnit, bylo by namístě uvažovat o určitém rozvolnění trestní represe v tomto směru, byť zcela jistě nikoliv o dekriminalizaci vůbec: např. přidáním dalších znaků k základním skutkovým podstatám. Mezi ty by mohlo patřit spáchání činu zvlášť zavrženíhodným způsobem, spáchání vůči zvlášť ohroženým osobám, v úmyslu získat pro sebe nebo pro jiného majetkový prospěch nebo z jiné zavrženíhodné pohnutky atp., případně zohlednění virtuálního násilí.

Zároveň by bylo namístě usilovat o určitou **privatizaci bezpečnosti** ve smyslu sebeochrany. Mimo jiné např. apelem na pozornost a péči věnovanou vlastnímu zabezpečení v online prostředí, neboť velká část sledovaného jednání vycházela nebo 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.

Nezbývá než dodat, že kyberkriminalita představuje širokou a rychle se vyvíjející oblast. Spolu s rozšiřujícím se spektrem připojených zařízení a rozličných podob využití informačních a komunikačních technologií i počtu uživatelů poroste nepochybně i její význam a závažnost.

Resumé

Dnešní společnost si lze jen stěží představit bez digitálních technologií. Prostupují každodenním životem s jednoduchou samozřejmostí: mobilní telefon, e-mail, sociální sítě, zpravodajství a nakupování online, od chytré domácnosti po chytré město. Nad tím vším se pomalu, ale jistě začínají kupit další a další připojená zařízení, která dala vzniknout výrazu „internet věcí". Soustavně roste počet připojených domácností a používání internetu pomalu, ale jistě proniká všemi věkovými kategoriemi.

Kyberprostor proto znamená mnohem víc než pouhou virtuální realitu nebo paralelní svět přístupný pouze mladým či technicky zdatným lidem. Představuje již neodmyslitelnou součást každodenní reality, spíše její emanaci než oddělenou část. Přesto jsou mu vlastní určité charakteristiky, které významně ovlivňují „pohyb" a komunikaci v jeho rámci oproti reálnému prostředí: především soustavnost (stále je někdo online), bezmeznost (internet nezná hranic) a absenci fyzična (absence neverbálních prvků komunikace). Nelze však opomenout ani specifika v rovině sociální (zejména sociální sítě), technologické (např. specifika kryptoměn), mocenské (např. regulace obsahu) i ekonomické (včetně např. obchodování online nebo internetového bankovnictví).

V souvislosti s vývojem technologií a kyberprostoru se objevuje i kriminalita s nimi spojená, kyberkriminalita. Zahrnuje jak „tradiční kriminalitu v novém kabátě", tak zcela nové formy kriminality nemyslitelné bez virtuálního prostředí (typicky malware). Můžeme se spokojit s jejím označením za kriminalitu využívající informační a komunikační technologie, ačkoliv se lze setkat s řadou jiných, košatějších definic. Naproti tomu pak stojí různá členění, nejčastěji podle Úmluvy o počítačové kriminalitě nebo na kriminalitu umožněnou nebo pouze usnadněnou použitím informačních a komunikačních technologií, případně typologie sdružující určitá jednání (např. sexuální zneužívání online, černý trh atp.). Každé z nich přináší výhody i nevýhody, nicméně v návaznosti na poznatky získané analýzou trestních spisů nabízíme jinou formu členění, a to na virtuální násilí (vyhrožování, znemožnění přístupu k účtu na sociální síti, dehonestace atp.) a majetkovou trestnou činnost online (a ostatní).

Ať už zůstaneme u dat a zpráv publikovaných v ČR nebo se podíváme dále do světa, pokračující trend růstu kyberkriminality je zjevný a její paleta pestrá. Dopadá na ni řada skutkových podstat jako podvod, porušení tajemství listin a jiných dokumentů uchovávaných v soukromí, poškození a ohrožení provozu obecně prospěšného zařízení aj., ale především tzv. počítačové trestné činy (§ 230-232 TZ, dříve § 257a sTZ). Od samého počátku jejich kriminalizace pozorujeme rapidní nárůst detekovaných útoků, nemluvě o značné latenci. Navzdory více či méně se zvyšujícímu počtu objasněných skutků se zdaleka nedaří pokrýt jejich nápad, a tak se objasněnost pohybuje v posledních letech zhruba na úrovni třetiny. Z hlediska justiční statistiky se situace zdá jen o málo lepší, když počet odsouzených oproti stíhaným osciluje v nadpolovičním množství, oproti obžalovaným pak kolem tří čtvrtin.

Základní údaje o kyberkriminalitě nacházíme ve statistikách, zejména v kombinaci policejních a justičních statistik, případně s doplněním především souhrnných údajů Českého statistického úřadu. Pozornost se obvykle zaměřuje na počítačové trestné činy, vzhledem k obtížné, ba až nemožné separaci kyberkriminality např. u podvodného jednání souhrnně podřazeného pod § 209 TZ.

Určité informace o rozsahu kyberkriminality v ČR lze vyčíst i z jiných výzkumných projektů věnovaných online prostředí, tyto se ovšem věnují převážně naopak jiným jevům než počítačovým trestným činům, zejména kyberšikaně, sexuálnímu zneužívání dětí, používání sociálních sítí a v posledních letech i fake news. Obrázek doplňují různé dílčí výzkumné projekty (zabývající se kyberkriminalitou jen okrajově) a ad hoc nebo pravidelně publikované zprávy různých institucí a organizací (např. NÚKIB). Problematice se pochopitelně věnuje i odborná literatura, v českém prostředí stojí za pozornost především práce V. Smejkala, J. Koloucha, R. Polčáka nebo T. Gřivny, případně jimi vedených autorských kolektivů. Nakonec také řada odborných konferencí a podobných setkání, v České republice především každoročně pořádaná konference Cyberspace.

Projekt a jeho realizace

Na rostoucí význam kyberkriminality reagovalo IKSP výzkumným úkolem „Identifikace a posouzení druhů a trendů kriminality páchané prostřednictvím Internetu (cyber crime), případně dalších sociálních sítí". Jeho předmětem byly vybrané formy kyberkriminality v ČR a zkušenosti veřejnosti s nimi. Projekt cílil na získání, analýzu a vyhodnocení nových poznatků o prevalenci vybraných forem kyberkriminality, pachatelích a jejich trestné činnosti. Dále na získání, analýzu a vyhodnocení poznatků o povědomí veřejnosti o možných hrozbách v kyberprostoru, vlastních zkušenostech s nimi v roli oběti i pachatele a o jejich sebeochraně. V České republice jde o první výzkum kyberkriminality prostřednictvím analýzy soudních spisů, který se zabývá počítačovými trestnými činy, jde nad rámec případových studií a publikovaných statistik a klade si za cíl získat statisticky zpracovatelná a do budoucna srovnatelná data.

Prvním krokem bylo studium domácí a zahraniční odborné literatury a relevantních oficiálních dokumentů, včetně právní úpravy a dostupné judikatury. Následovala analýza justičních a policejních statistik. Poté jsme přistoupili ke stěžejní části projektu - seznámení se s vybranými trestními spisy a k analýze zjištěných poznatků. Ty se staly základem pro zaměření dotazníkového šetření určeného široké internetové populaci, resp. reprezentativnímu výběrovému souboru uživatelů internetu ve věku 16-74 let, jehož výsledky budou publikovány samostatně. Zjištěné údaje jsme doplnili konzultacemi s vybranými odborníky (policista, dva IT specialisté včetně zaměstnance v rámci kritické infrastruktury). Dílčí výsledky projektu byly průběžně prezentovány v tištěné podobě, online i osobně zejména formou konferenčních vystoupení.

Pro analýzu trestních spisů jsme vybrali řízení, v nichž byla podána obžaloba pro spáchání některého z počítačových trestných činů (ve všech případech šlo o neoprávněný přístup k počítačovému systému a nosiči informací podle § 230 TZ, případně v souběhu s dalším počítačovým trestným činem), a která byla pravomocně skončena v roce 2015. K dispozici jsme měli nakonec 66 trestních spisů (z celkového počtu 71 věcí) zahrnujících 68 obviněných. Počet leží na hranici statisticky relevantních dat, jde však o prakticky kompletní pravomocnou soudní agendu za rok 2015.

Analýza trestních spisů probíhala formou vyhledávání a zaznamenávání sledovaných proměnných do záznamových listů. Takto bylo sledováno 50 položek zahrnujících především základní údaje o obviněném (a okrajově též o poškozených), trestném činu samotném

a o průběhu trestního řízení. Většina údajů zahrnuje osoby obviněné, tj. pachatele i ty, jejichž trestní stíhání bylo skončeno jinak než odsouzením. Sledovali jsme obecné údaje (např. soud, který vydal ve věci meritorní rozhodnutí), informace o právním posouzení skutku (např. kvalifikace, souběh aj.), o konečném rozhodnutí ve věci (včetně např. uloženého trestu), o průběhu trestního řízení (zejména délku jednotlivých fází řízení), o obviněném (sociodemografické údaje, předchozí trestnou činnost aj.), o skutku jako takovém (zejména způsob jednání a použitou platformu, motivaci, údaje o poškozených, způsobenou újmu aj.).

Vybrané výsledky

Analýza trestních spisů poskytla řadu zajímavých informací, byť s výhradou omezené vypovídací hodnoty s ohledem na nízké počty a na předpokládanou vysokou latenci. O počítačových trestných činech rozhoduje obvykle okresní (obvodní) soud, zhruba ve dvou třetinách případů pachatel jednal v souběhu s dalším skutkem (především majetkového charakteru). Ve čtvrtině věcí soud obviněného zprostil obžaloby nebo řízení zastavil, odsouzeným pak uložil nejčastěji trest odnětí svobody, který podmíněně odložil.

Mezi nepodmíněně odsouzenými lze sledovat skupinu mladších recidivujících pachatelů (24-35 let) oproti starším prvopachatelům (41-58 let), kteří zneužili své pracovní pozice k neoprávněnému přístupu k neveřejným informačním systémům. Naproti tomu např. pachatelé, kterým soud uložil trest obecně prospěšných prací, se dopouštěli virtuálního násilí (většinou ze msty či žárlivosti), a to ve věku nepřevyšujícím 22 let (námi uváděný věk odpovídá vždy okamžiku zahájení úkonů trestního řízení).

U méně závažných jednání, kde nebyly pochybnosti o skutkovém stavu, a mohl proto rozhodnout o věci samosoudce trestním příkazem, šlo v drtivé většině o manipulaci s daty (smazání, úprava, vložení cizích dat). Pachatelé útočili převážně na osoby ze svého blízkého okolí (80 %), dále pak ve spojitosti se zaměstnáním (kolegové, zaměstnavatelé, 21 %).

Zajímavou kategorii představuje 27 řízení vedených za jednání bez souběhu, neboť soud v takových případech ukládá trest vskutku za počítačový trestný čin. Ve všech případech šlo o neoprávněný přístup k počítačovému systému a nosiči informací (§ 230 TZ bez rozlišení prvního a druhého odstavce). Soud odsoudil 18 pachatelů, z toho 14 uložil trest odnětí svobody (v délce průměrně 6 měsíců), který podmíněně odložil. Řízení trvalo celkově průměrně 1,4 roku, o něco delší byla obvykle fáze přípravného řízení. Zhruba v polovině případů pachatelé zneužili přístup k informační technologii (fyzický přístup např. k notebooku nebo znalost cizího hesla).

Trestní řízení trvala průměrně 1,5 roku (74 dní až téměř 5,5 roku), 90 % věcí bylo skončeno do 2,5 roku. Přípravné řízení zabralo průměrně 0,8 roku (4 dny až 3 roky), řízení před soudem 0,7 roku (17 dnů až 4 roky). Roli hraje v tomto směru pravděpodobně využití opravných prostředků (řádný byl využit zhruba ve čtvrtině věcí), zatímco např. souběh s další trestnou činností nikoliv. Celková délka řízení o něco více koreluje s dobou řízení u soudu než s délkou přípravného řízení, přičemž u většiny věcí vyřešených do 2 let převažuje doba přípravného řízení.

V kauzách řešených déle než 3 roky (n=7) obvinění v průměrném věku 43 let a motivovaní až na jeden případ majetkovým zájmem zneužili svého přístupu k informačnímu systému, čímž poškodili nejčastěji svého zaměstnavatele (a případně subjekty napadených osobních údajů).

Nejpočetněji jsou zastoupeni obvinění ve věku do 24 let, v rozmezí 17-58 let a s průměrným věkem 34 roky, téměř polovina jich je mladší 30 let. Zhruba 40 % jich bylo v době zahájení úkonů trestního řízení v manželském či obdobném svazku. Deset obviněných se dopustilo svého jednání v souvislosti se svým postavením úřední osoby, včetně pěti příslušníků Policie ČR. Mezi celkem 26 recidivisty byli pouze dva, u nichž šlo o speciální recidivu zahrnující počítačový trestný čin (v obou případech zneužití cizích e-mailových schránek a tzv. m-plateb za pomoci mobilních telefonů a sociálních sítí).

Celou pětinu obviněných tvořily ženy, z nichž polovina je ve věku 35-49 let (v rozmezí 19-56 let s průměrným věkem 38 let). Dvě třetiny z nich mají maturitu či vyšší vzdělání (více než polovina obviněných mužů je vzdělaná méně). Podobně dvě třetiny soud odsoudil a uložil jim nejčastěji podmíněně odložený trest odnětí svobody. Odsouzeno tak bylo menší procento žen oproti mužům, nicméně uložené tresty měly mít v průměru delší trvání. Oproti obviněným recidivujícím mužům (30 %) zaujímají recidivující pachatelky zhruba třetinový podíl (cca 13 % obviněných žen). Zatímco jednání obviněných mužů i žen lze označit zhruba v polovině případů za virtuální násilí a v druhé polovině za majetkovou trestnou činnost, při pohledu na odsouzené pachatelky se tento poměr mění na (pouhých) 30 % virtuálního násilí.

Zhruba na polovinu lze obviněné rozdělit také na mladší a starší podle věkové hranice 30 let, polovina mladších obviněných měla v době trestního řízení pouze základní vzdělání. Oproti zhruba polovičnímu podílu recidivistů na celkové kriminalitě v roce 2015 nacházíme mezi mladšími obviněnými pouhou třetinu recidivistů, mezi staršími dokonce pětinu. Zdá se proto, že počítačové trestné činy jsou doménou prvopachatelů. Starším pachatelům soud častěji ukládal spolu s hlavním i vedlejší trest, převážně zákaz činnosti.

Přesně polovina obviněných dosáhla alespoň maturity (včetně třetinového podílu žen), z toho třetina vysokoškolského titulu, přičemž všichni vysokoškolsky vzdělaní byli dosud bezúhonní. Mezi méně vzdělanými obviněnými jich má zhruba polovina předchozí zkušenost s trestnou činností.

Více než ve třetině kauz měli obvinění zneužít přístup k informační a komunikační technologii umožněný v souvislosti se zaměstnáním nebo díky důvěře poškozených. V téměř pětině případů měli obvinění zneužít cizích přihlašovacích údajů k různým účtům (především k sociálním sítím a e-mailům, dále k internetovému bankovnictví). Podobně často přihlašovací údaje někde nalezli (např. uložené v počítači, napsané na papíře). K využití technických prostředků došlo jen minimálně. K největším slabinám ochrany tak patří fyzické zabezpečení, dále ochrana e-mailových schránek, profilů na sociální síti Facebook a informačních systémů přístupných zaměstnancům. Z osobních údajů dochází v drtivé většině případů ke zneužití hesla.

Jednání lze rozdělit opět zhruba na polovinu na virtuální násilí a majetkovou trestnou činnost, přičemž toto rozdělení na dvě podobné části prochází napříč různými kategoriemi, včetně např. věku nebo vzdělání. Odlišnosti nacházíme např. při zohlednění postavení úřední osoby (všichni až na jednoho sledovali majetkový zájem) nebo souběhu (obvinění se měli dopustit svého jednání v souběhu u tří čtvrtin věcí s majetkovým zájmem, ale pouze u poloviny virtuálního násilí). Konkrétněji šlo ve 40 % případů o snahu o finanční přilepšení a ve 30 % odůsledek komplikované vztahové situace (ostatní podoby - např. žert - byly méně časté). Pachatelé tak např. zveřejňovali intimní fotografie poškozených, neoprávněně vstupovali na jejich účty na sociálních sítích a do e-mailových schránek nebo oslovovali jejich jménem další osoby atp. Předpokládáme, že smysluplnost členění na virtuální násilí a majetkovou trestnou činnost (a ostatní) se v budoucnu jen potvrdí a umožní dobrou výzkumnou uchopitelnost. Tomu by významně napomohlo např. zařazení do veřejně přístupné evidence statistických údajů i prvku online prostředí.

U deliktů s majetkovým zájmem došlo v polovině případů ke zneužití přístupu k informačním a komunikačním technologiím. Za zmínku stojí tři typové skupiny zahrnující většinou vzdělané a bezúhonné osoby: příslušníci Policie ČR, kteří zneužívali přístup do policejních informačních systémů; „vynalézavé ženy", které při řešení své špatné finanční situace zneužily svého postavení v zaměstnání; a „datoví magnáti", kteří zneužívali osobní údaje klientů z informačních systémů zaměstnavatele. Další skupiny s majetkovým zájmem představují „geekové", kteří zneužili své schopnosti v oblasti informačních a komunikačních technologií a přístup ke konkrétnímu zařízení či informačnímu systému, a „online zloději", kteří získali přihlašovací údaje k různým účtům obětí (ze svého bezprostředního okolí), jejichž prostřednictvím si zjednali přístup k finančním prostředkům.

Naproti tomu u virtuálního násilí (obviněný v 90 % kauz znal oběť) shledáváme pouze dvě typové skupiny, a to „mstitele" a „žárlivce". Zhrzení mstitelé, mladší bezúhonní muži (průměrně 26 let), škodili svým bývalým partnerům pomluvami, napadáním online, zneužíváním jejich účtů na sociálních sítích atp. Žárlivci útoky směřovali na partnery bývalé i současné a škodili stejně jako mstitelé, ale také usilovali o kontrolu nad svými oběťmi. V obou skupinách zneužívali hesla nebo zařízení obětí, která se dozvěděli nebo používali v rámci partnerského vztahu.

V procesním postavení poškozeného se nacházely fyzické i právnické osoby. Ve třech čtvrtinách věcí šlo o jediného poškozeného, ve zbývajících věcech o 2-5 osob, až na 4 trestní řízení, kde figurovaly desítky až stovky poškozených. Pachatelé se dopustili až 782 útoků (dílem neúspěšných) a ve 40 % kauz způsobili finanční škodu ve výši od 1 200 korun po 27 milionů. Nemajetkovou újmu uváděli poškození v 70 % věcí, avšak vyčíslena byla pouze v jediném případě. V necelých dvou třetinách věcí se obvinění s poškozenými osobně znali (ve třetině šlo o jejich stávající či bývalé partnery, v pětině o prosté známé a v desetině o příbuzné), ve třetině útočili na své zaměstnavatele (stávající či bývalé).

Obvinění v zaměstnaneckém či služebním poměru s poškozeným subjektem byli o něco starší, ve věku průměrně 38 let (21-56 let). Mezi 23 obviněnými v této souvislosti bylo i sedm státních zaměstnanců (tři sociální pracovnice, čtyři příslušníci policie ČR). Poškozující jednání nabývalo rozmanitých podob. Např. sociální pracovnice čerpala sociální dávky namísto zemřelých osob, zaměstnankyně banky zřizovala ve svůj prospěch

úvěry s využitím osobních údajů fiktivních osob (s nejvyšší způsobenou škodou 27 milionů korun a nejdelším uloženým trestem odnětí svobody na 9,5 roku), příslušník Policie ČR poskytoval za úplatu informace o probíhajících trestních řízeních. Dále došlo např. ke znehodnocení dat ve firemní databázi nebo jejich předání konkurenci.

Mezi opakující se jevy patřilo napadání e-mailových schránek, od prostého prohlédnutí obsahu až po manipulaci s ním nebo převzetí identity jeho majitele (komunikace jeho jménem). E-mailová schránka přitom obsahuje řadu významných informací: např. kontakty nebo část denního harmonogramu majitele schránky, a především samotný obsah komunikace, často včetně přihlašovacích údajů k dalším aplikacím, zejména sociálním sítím, případně slouží jako kontaktní e-mail k obnovení přístupu. E-mailová schránka hrála významnou roli zhruba ve čtvrtině případů a zahrnovala virtuální násilí (např. pátrání po nevěře nebo komunikace jménem poškozeného) i majetkový zájem (např. pozměňování fakturačních údajů nebo přeposílání e-mailů konkurenci). Takové jednání zpravidla usnadnili sami poškození, kteří dostatečně nezabezpečili svá hesla. Ta byla jednoduchá (např. jméno napadené instituce), fyzicky přístupná (např. uložené v zapůjčeném notebooku), neměnná (zneužito např. bývalým zaměstnancem po ukončení pracovního poměru nebo partnerem po rozchodu), případně pro pachatele snadno obnovitelná (např. díky jednoduché bezpečnostní otázce).

V rámci projektu jsme věnovali část pozornosti i specifické problematice kybergroomingu, navazování kontaktů s dětmi v online prostředí za účelem jejich sexuálního zneužití. Útočníci oběti kontaktují, udržují s nimi sexuálně laděnou komunikaci, budují emoční závislost, vylákávají intimní obsah (zejména fotografie a videa až pornografického materiálu) a vydírají i vyhrožují ve snaze získat další takový obsah, případně přimějí oběť k osobnímu setkání a sexuálním aktivitám fyzického rázu. Od roku 2014 je proto takové jednání kriminalizováno (mimo jiné) coby navazování nedovolených kontaktů s dítětem (§ 193 b TZ). Počet odsouzených případů (většinou prvopachatelé a častěji mladší 30 let) od té doby narůstal až po 45 odsouzených pachatelů v roce 2019, přičemž jejich charakteristiky a modus operandi zhruba odpovídal předpokladům uváděným v odborné literatuře.

Realizovali jsme také tři polostrukturované rozhovory s vybranými odborníky (příslušník Policie ČR a dva IT zaměstnanci, včetně jednoho pečujícího o kritickou infrastrukturu). Všichni hovořili (z vlastního popudu) o ransomwaru, alespoň ve dvou se pak shodli na dalších tématech jako podvody v mezinárodním obchodě, dětská pornografie, slabiny infrastruktury (zejména zabezpečení lokální sítě a serverů), sociální inženýrství (mimo jiné ve vztahu k zaměstnancům), shromažďování dat velkými korporacemi, rizika vyplývající ze zanedbávání aktualizací, využívání cloudů a samozřejmě také o tématu zaměstnanců coby potenciálnímu riziku a o lidském faktoru vůbec (zejména neopatrnost spojená s přihlašovacími údaji): „*největší hrozba je od těch uživatelů, který jsou v tý lokální síti*." Zmínili také problematiku odhalování a postihu s ohledem na nadnárodní charakter internetu a s tím spojené jevy jako obtížná vymahatelnost práva nebo organizovaný zločin. Podrobněji se věnovali též kryptoměnám a v menší intenzitě i fake news. Shodně doporučovali zejména pravidelně aktualizovaný ochranný software a osvětu - zajistit typickým či aktuálním kauzám náležitou publicitu a školit v oblasti bezpečnosti informačních a komunikačních technologií zaměstnance i řadové uživatele (s důrazem na obezřetnost v oblasti přihlašovacích údajů).

Poslední součást projektu představuje dotazníkové šetření, o němž bude referováno samostatně v roce 2021. V této publikaci se lze v příslušné kapitole seznámit s nastíněním rešerše výzkumů kyberkriminality relevantní pro ČR, metodologií (výběr respondentů a způsob dotazování) a jednotlivými oblastmi dotazníku podrobněji (sebeochrana uživatelů informačních a komunikačních technologií, míra jejich viktimizace vybranými jevy a jejich zkušenosti v roli pachatele, včetně zohlednění aktivit a zařízení spojených se zaměstnáním).

Závěrem se zamýšlíme nad některými nedostatky či slabými místy končícího projektu (např. zúžení analýzy trestních spisů na počítačové trestné činy a jejich počet), nad poznatky, které by snad zasloužili větší pozornost (např. mladší recidivující pachatelé oproti starším prvopachatelům), nad vlastními úvahami (např. rozdělení kyberkriminality na majetkový zájem a virtuální násilí) a v neposlední řadě nad zaměřením projektu budoucího (zejména pokračování analýzy trestních spisů).

Summary

Vlach, J., Kudrlova, K., Palousova, V. (2020) Cybercrime from a Criminological Perspective.

Today's society is virtually unimaginable without digital technologies. They permeate our everyday life as a simple matter of course: mobile phones, e-mails, social networks, online news and shopping, from smart homes to smart cities. Above all, they are being slowly, but surely joined by more and more connected devices, giving rise to the term "Internet of Things". The number of connected households has continued to grow, while the use of the internet has gradually penetrated all age groups.

Cyberspace thus means much more than mere virtual reality or a parallel world only accessible to the young or technically proficient. It's already become an integral part of everyday reality, though more its emanation than a separate part. Nevertheless, it has certain characteristics that significantly affect "movement" and communication within its framework compared to the real environment: in particular, constancy (someone is always online), limitlessness (the internet knows no boundaries) and the absence of physicality (nonverbal elements of communication). However, we must not overlook the specifics at social (especially social networks), technological (e.g. the specifics of cryptocurrencies), control (e.g. content regulation) and economic (including online trading or internet banking) level.

Nevertheless, the development of technology and cyberspace has progressed hand-in--hand with the advent of associated crime - cybercrime. This includes both "traditional crime in a new guise" and completely new forms of crime that are unthinkable without a virtual environment (typically malware). We can be content with its definition as crime using information and communication technologies, although a number of other, more expansive definitions can be found. On the other hand, there are various classifications, most often based on the Convention on Cybercrime or crime enabled or facilitated by the use of information and communication technologies, or typologies grouping certain offences (e.g. online sexual abuse, the black market, etc.). Although each has its advantages and disadvantages, following the findings of our analysis of criminal files, we offer a different form of classification, namely virtual violence (threats, denied access to social network accounts, defamation, etc.) and online financial crime (and others).

Whether we stick to data and reports published in the Czech Republic or look further around the world, a continuing upward trend in cybercrime is evident and its range is varied. It includes various criminal offences such as fraud, violating the confidentiality of private documents and other papers, damaging or threatening the operation of public benefit organisations, etc., but especially so - called computer crimes (Section 230-232 of the Criminal Code, formerly Section 257a of Act No. 140/1961 Coll., the Criminal Code). From the very beginning of their criminalisation, we have seen a rapid increase in detected attacks, not to mention considerable latency. Despite the increasing number of solved cases, the range of offences is far from covered, so the clearance rate in recent years has remained at around one third. The situation in terms of judicial statistics seems only slightly better, with the number of convicted offenders to those prosecuted wavering at over one half, and around three quarters to those accused.

Basic data on cybercrime can be found in statistics, especially a combination of police and judicial statistics, with the addition of summary data from the Czech Statistical Office. Attention is usually focused on computer crimes, due to the difficult, or virtually impossible separation of cybercrime, e.g. fraudulent conduct collectively classified under Section 209 of the Criminal Code.

Certain information on the extent of cybercrime in the Czech Republic can also be gleaned from other research projects studying the online environment, although these mainly focus on phenomena other than cybercrime, particularly cyberbullying, child sexual abuse, social networking and in recent years, fake news. The picture is complemented by various research projects (only marginally dealing with cybercrime) and ad hoc or regularly published reports by various institutions and organisations (e.g. National Cyber and Information Security Agency). Of course, professional literature also deals with the issue; in the Czech environment, the work of V. Smejkal, J. Kolouch, R. Polčák and T. Gřivna, or teams led by them, is particularly noteworthy. Finally, there are also a number of professional conferences and similar meetings, especially the annual Cyberspace conference in the Czech Republic.

The project and its implementation

The Institute of Criminology and Social Prevention responded to the growing importance of cybercrime with the research task "Identification and Assessment of Types and Trends of Crime Committed via the Internet (Cybercrime) or Other Social Networks". The subject was selected forms of cybercrime in the Czech Republic and public experience with these crimes. The project was aimed at acquiring, analysing and evaluating new information about the prevalence of selected forms of cybercrime, offenders and their criminal activities, together with the acquisition, analysis and evaluation of information on public awareness of potential threats in cyberspace, their own experiences with cybercrime in the role of victims or offenders and self-protection measures. This is the first research project in the Czech Republic examining cybercrime through an analysis of court files, which goes beyond case studies and published statistics and aims to obtain statistically processable data that can be compared over time.

The first step was a study of national and foreign professional literature and relevant official documents, including legislation and available case law. This was followed by an analysis of judicial and police statistics. We then approached the core part of the project - studying selected criminal files and analysing the findings. These became the basis for the focus of the questionnaire survey for the general internet population, or respectively a representative sample of internet users aged from 16-74, the results of which will be published separately. We supplemented this data by consulting with selected experts (police officer, two IT specialists, including an employee in critical infrastructure). Partial results of the project were continuously presented in print form, online and in person, especially in the form of conference presentations.

For the analysis of criminal files, we selected proceedings in which an indictment was filed for the commission of a computer crime (in all cases this was unauthorised access to computer systems and information media pursuant to Section 230 of the Criminal Code,

or in conjunction with another computer crime), which ended with a final verdict with legal force in 2015. We ultimately had 66 criminal files (out of a total of 71 cases) involving 68 accused. This number is on the threshold of statistically relevant data, but constitutes virtually the complete relevant judicial agenda for 2015.

The analysis of criminal files took place by searching for and recording monitored variables on record sheets. Fifty items were monitored this way, primarily comprising basic data about the accused (and marginally on the victims), the crime itself and the course of criminal proceedings. Most data included the accused, i.e. offenders, as well as those whose prosecution ended with a verdict other than conviction. We monitored general data (e.g. the court that issued the decision on the merits of the case), information on the legal assessment of the offence (e.g. qualification, concurrence, etc.), the final decision in the case (including the sentence imposed), the course of criminal proceedings (especially the length of individual stages of proceedings), the accused (sociodemographic data, previous criminal activity, etc.), the offence as such (especially the manner it was conducted and the platform used, the offender's motivation, data on victims, the damages caused, etc.).

Selected results

The analysis of criminal files provided lots of interesting information, albeit subject to its limited indicative value in view of the low numbers and expected high latency. Computer crimes are usually decided by a district court; in about two thirds of cases, the offender acted in concurrence with another offence (mainly of a financial/economically motivated nature). In one quarter of cases, the court acquitted the defendant or discontinued proceedings; convicted offenders were most often sentenced to imprisonment, which was conditionally suspended.

Unconditionally convicted offenders included a group of younger recidivists (aged 24-35), against older first-time offenders (aged 41-58), who abused their job positions to gain unauthorised access to non-public information systems. On the other hand, for example, offenders sentenced to community service by the court committed acts of virtual violence (mostly for revenge or out of jealousy), at an age not exceeding 22 (the stated age corresponds to the moment criminal proceedings commenced in all cases).

In less serious cases, where there was no doubt of the facts, and the matter could therefore be decided by a single judge who issued a criminal order, the vast majority of cases involved the manipulation of data (deletion, modification, insertion of third-party data). The offenders mostly attacked people from their immediate surroundings (80%), or in connection with their employment (colleagues, employers 21%).

An interesting category was the 27 proceedings involving offences without concurrence, where the court imposed a penalty solely for computer crime. In all cases, this was unauthorised access to a computer system and information media (Section 230 of the Criminal Code, without distinction between the first and second paragraph). The court convicted 18 offenders, 14 of whom received a prison sentence (on average 6 months), which the court conditionally suspended. The proceedings lasted an average of 1.4 years, while pre-trial

proceedings were usually a bit longer. In about one half of cases, the offenders abused access to information technology (physical access to, for example, a laptop or knowledge of someone else's password).

Criminal proceedings lasted an average of 1.5 years (74 days to almost 5.5 years); 90% of cases were completed within 2.5 years. Pre-trial proceedings took an average of 0.8 years (4 days to 3 years), and trial proceedings 0.7 years (17 days to 4 years). The use of remedies probably played a role in this respect (they were duly used in about one quarter of cases), while concurrence with other criminal activity, for example, did not. The total length of proceedings correlates slightly more with the length of trial proceedings than with the length of pre-trial proceedings, with the duration of pre-trial proceedings prevailing in most cases resolved within 2 years.

In cases pending for more than 3 years (n = 7), offenders, with an average age of 43 and economically motivated interests with the exception of one case, abused their access to an information system, thus most often damaging their employer (and possibly the subjects of attacked personal data).

The most numerous group were accused under the age of 24, in the range of 17-58, with an average age of 34, almost half are under the age of 30. Approximately 40% of accused were in a marital or similar relationship at the time criminal proceedings commenced. Ten accused committed their offences in connection with their position as a public official, including five members of the Police of the Czech Republic. Of the total of 26 recidivists, there were only two with special recidivism involving computer crime (in both cases the misuse of someone else's e-mail and so-called m-payments using mobile phones and social networks).

One fifth of accused were women, half of whom were aged 35-49 (in the range of 19-56, with an average age of 38). Two thirds of them had a high school diploma or higher education (more than one half of accused men were less educated). Similarly, the court convicted two-thirds of accused women, the most frequent sentence being a suspended prison sentence. Thus, a smaller percentage of women were convicted than men, however, imposed sentences were on average longer. Compared to accused male recidivists (30%), female recidivists accounted for about one third, approximately 13% of accused women. While offences committed by accused men and women can be described as virtual violence in about one half of cases and financial crime in the other half, this ratio changes to (only) 30% virtual violence when looking at convicted female offenders.

Accused can also be divided into roughly half based on an age limit of 30; the younger half of accused had only basic education at the time of criminal proceedings. Compared to an approximately 50% share of recidivists in total crime in 2015, we only found one third of recidivists among younger accused, and only one fifth in the older category. Therefore, cybercrime seems to be the domain of first-time offenders. The court more often imposed a secondary sanction with the main sentence in the case of older offenders, usually in form of prohibition of activity.

Exactly one half of accused had at least a high school diploma (including one third of women), of whom one third had a university degree, while all university graduates had hitherto clean criminal records. Among less educated defendants, about one half had previous experience of crime.

In more than one third of cases, the accused were suspected of misusing access to information and communication technologies provided in connection with their employment or through the trust of the victims. In almost one fifth of cases, the accused were suspected of misusing another person's login data to various accounts (mainly social networks and e-mails, as well as internet banking). Similarly, they often found login data somewhere (e.g. stored on a computer, written on a piece of paper). The use of technical means was minimal. The weakest points of protection thus include physical security, as well as the protection of e-mails, profiles on Facebook and information systems accessible to employees. Of personal data, the most widely misused are passwords.

Offences can again be roughly divided in half into virtual violence and financial/economically motivated crime, where this division cuts across various different categories, including age and education. We find differences, for example, when taking into account the position of a public official (all but one pursued financial interests) or concurrence (in three quarters of cases the accused acted concurrently with financial interests, but only in half of virtual violence). More specifically, in 40% of cases, the offence was an attempt to improve the accused's financial situation and in 30% a consequence of a complicated relationship situation (other forms - such as a prank - were less common). For example, offenders posted intimate photos of the victims, accessed their accounts on social networks and e-mails without authorisation, or contacted other people on their behalf, etc. We expect the merits of the classification into virtual violence and financial/economically motivated crime (and others) to be confirmed in the future and enable good research comprehension of this topic. This would be significantly helped, for example, by the inclusion of the online environment in publicly accessible registers of statistical data.

For offences with financial interests, in one half of cases access to information and communication technologies was misused. Three type groups are worth mentioning - mostly educated people without criminal records: members of the Police of the Czech Republic who abused access to police information systems; "resourceful women" who abused their position at work to resolve their poor financial situation; and "data moguls" who misused clients' personal data from their employer's information systems. Other groups with financial interests include "geeks" who abuse their skills in information and communication technologies to access a specific device or information system, and "online thieves" who obtain login data to the various accounts of victims (from their immediate surroundings) through which they gained access to funds.

In contrast, in virtual violence (where the accused knew the victim in 90% of cases), we only find two type groups, namely "avengers" and "jealous people". Jilted avengers, younger men (on average 26 years old) without previous criminal records, harmed their former partners through slander, online attacks, misusing their social media accounts, etc.

Jealous attacks targeted past and present partners and harmed them in the same way as avengers, but they also sought control of their victims. In both groups, offenders misused victims' passwords or devices that they learned or used during their relationship.

Both natural and legal persons were injured parties in proceedings. In three quarters of cases there was only one victim, with 2-5 individuals in the remainder, except for 4 criminal proceedings, where there were dozens to hundreds of victims. The offenders committed up to 782 attacks (partly unsuccessful) and in 40% of cases caused financial damage in the amount of CZK 1,200 to CZK 27 million. Non-pecuniary damages were reported in 70% of cases, but were only quantified in one case. In just under two thirds of cases, the accused knew the victims personally (in one third this was their current or former partner, one fifth were simply acquaintances and one tenth were relatives) and one third attacked their employer (current or former).

Accused in an employment or in a service relationship to the injured party were slightly older, averaging 38 (21-56) years of age. Among the 23 accused in this context, seven were civil servants (three social workers, four members of the Czech Police). Offences took many forms. For example, a social worker drew social benefits instead of deceased clients; a bank employee set up loans to her benefit using the personal data of fictitious persons (with the highest damages of CZK 27 million and longest sentence of 9.5 years in prison); a member of the Czech Police provided information on ongoing criminal proceedings for payment. In other cases, for example, there was the corruption of data in a company database or data transferred to competitors.

Recurring phenomena included e-mail attacks, from simply viewing the contents to their manipulation or taking over the identity of the mailbox owner (communicating on their behalf). E-mails contain a wide range of important information: e.g. the mailbox owner's contacts or part of their daily schedule, and especially the contents of the communication itself, often including login details for other applications, particularly social networks, or serving as the contact e-mail for restoring access. E-mails played a significant role in about one quarter of cases and included virtual violence (e.g. searching for infidelity or communicating on behalf of the victim) as well as financial interests (e.g. changing billing information or forwarding e-mails to competitors). As a rule, such actions were facilitated by the victims themselves, who did not sufficiently secure their passwords. These were simple (e.g. the name of the attacked institution), physically accessible (e.g. stored on a borrowed laptop), unchanged (misused by a former employee after the termination of their employment or a partner after a breakup), or easily recoverable for offenders (e.g. thanks to a simple security question).

As part of the project, we also examined the specific issue of cyber-grooming, establishing contact with children in the online environment for the purpose of their sexual abuse. Offenders contact the victim, maintain sexually oriented communication with them, build emotional addiction, lure intimate content from them (especially photos and videos to pornographic material) and then blackmail and threaten to obtain more such content, or force the victim to meet in person and engage in sexual activities of a physical nature. Such conduct has therefore been criminalised (among other things) since 2014 under the establishment of illegal contact with a child (Section 193 b of the Criminal Code). The

number of convicted cases (mostly first-time offenders and more often under the age of 30) has since increased to 45 convicted offenders in 2019, with their characteristics and modus operandi roughly corresponding to those presented in professional literature.

We also conducted three semi-structured interviews with selected experts (a member of the Police of the Czech Republic and two IT employees, including one involved in critical infrastructure). They all talked (on their own initiative) about ransomware, at least two of them agreed on other topics such as fraud in international trade, child pornography, infrastructure weaknesses (especially local network and server security), social engineering (in relation to, among other things, employees), data collection by large corporations, risks due to neglected updates, the use of cloud services and of course the topic of employees as a potential risk and the human factor in general (especially carelessness associated with login data): "*the biggest threat is from users in the local network*." They also mentioned the issue of detecting and sanctioning offences given the transnational nature of the internet and related phenomena such as difficult law enforcement or organised crime. They also focused more attention on cryptocurrencies and, to a lesser extent, fake news. In particular, they consistently recommended regularly updated protection/security software and education, ensuring that typical and current cases receive appropriate publicity and training employees and ordinary users in the field of security of information and communication technologies (with an emphasis on caution relating to login data).

The last part of the project is a questionnaire survey, which will be reported separately in 2021. This publication presents an outline of cybercrime research relevant to the Czech Republic, the methodology (selection of respondents and method of questioning) and individual areas covered by the questionnaire in more detail (self-protection by users of information and communication technologies, the degree of their victimisation by selected phenomena and their experience in the role of offender, including consideration of activities and devices related to employment).

In conclusion, we reflect on some of the shortcomings or weaknesses of the ending project (e.g. narrowing the analysis of criminal files to computer crimes and their number), on findings that would perhaps deserve more attention (e.g. younger recidivists compared to older first-time offenders), our own considerations (e.g. the classification of cybercrime into financial/economically motivated crime and virtual violence) and, last but not least, the focus of any future project (especially the continuing analysis of criminal files).

Translated by: Presto

Použité prameny

Bartík, V., & Janečková, E. (2016). *Ochrana osobních údajů v aplikační praxi (vybrané problémy).* 4. vydání. Praha: Wolters Kluwer.

Bartlett, J. (2015). *The Dark Net: Inside the Digital Underworld.* Brooklyn: Melville House.

Buber, M. (1996). *Já a Ty.* Olomouc: Votobia.

Costs of Cyber Crime Working Group. (2018). *Understanding the costs of cyber crime.* Získáno dne 14. 1. 2019 z: https://www.gov.uk/government/publications/understanding-the-costs-of-cyber-crime

Diblíková, S., Cejp, M., Hulmáková, J., Raszková, T., Roubalová, M., Scheinost, M., Večerka, K. & Zhřívalová, P. (2019). *Analýza trendů kriminality v České republice v roce 2018*. Praha: Institut pro kriminologii a sociální prevenci.

Eckertová, L., & Dočekal, D. (2013). *Bezpečnost dětí na internetu. Rádce zodpovědného rodiče.* Brno: Computer Press.

Fenyk, J., Císařová, D., & Gřivna, T. (2015). *Trestní právo procesní.* 6. vydaní. Praha: Wolters Kluwer.

Giddens, A. (2000). *Sociologie.* Praha: Argo.

Gregor, M., & Vejvodová, P. (2018). *How to manipulate: the techniques of online disinformation media.* Brno: Albatros Media, a. s.

Gřivna, T., & Polčák, R. (2008). *Kyberkriminalita a právo.* Praha: Auditorium.

Gřivna, T., Scheinost, M., Zoubková, I., a další (2015). *Kriminologie.* 4. vydání. Praha: Wolters Kluwer.

Gřivna, T., Scheinost, M., Zoubková, I., a další (2019). *Kriminologie.* 5. vydání. Praha: Wolters Kluwer.

Hinduja, S. K., & Patchin, J. W. (2014). *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying.* Thousand Oaks: Corwin.

Hulanová, L. (2012). *Internetová kriminalita páchaná na dětech.* Praha: Triton.

Chaloupková, H., & Holý, P. (2012). *Autorský zákon. Komentář.* 4. vydání. Praha: C.H.Beck.

Jelínek, J., a další (2008). *Trestní právo hmotné.* 3. vydání. Praha: Linde Praha, a. s.

Jelínek, J., a další (2015). *Trestní právo Evropské unie a jeho vliv na právní řád České republiky a Slovenské republiky.* Praha: Leges.

Jirásek, P., Novák, L. & Požár, J. (2013). *Výkladový slovník kybernetické bezpečnosti*. Praha: Policejní akademie ČR.

Jirovský, V. (2007). *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada.

Kolouch, J., Bašta, P., Kropáčová, A. & Kunc, K. (2019). *CyberSecurity.* Praha: CZ.NIC, z.s.p. o.

Krčmářová, B. (2012). *Děti a online rizika.* Praha: Sdružení Linka bezpečí.

Lavický, P., a další. (2014). *Občanský zákoník I. Obecná část (§ 1–654). Komentář.* Praha: C. H. Beck.

Leukfeldt, R. & Holt, T. (Eds.). (2019). *The Human Factor of Cybercrime*. London: Routledge.

Lister, M., Dovey, J., Giddings, S., Grant, I., & Kelly, K. (2003). *New Media: A Critical Introduction.* New York: Routledge.

Manovich, L. (2001). *The Language of New Media.* Cambridge: MIT Press.

Marešová, A. (Ed.). (2015). *Analýza trendů kriminality v ČR v roce 2014.* Praha: IKSP.

Martinková, M., & Biedermanová, E. (2019). *Senioři v České republice jako oběti i pachatelé kriminálních deliktů.* Praha: Institut pro kriminologii a sociální prevenci.

Matějka, M. (2002). *Počítačová kriminalita.* Praha: Computer press.
Musil, S. (Ed.). (2000). *Počítačová kriminalita. Nástin problematiky. Kompendium názorů specialistů.* Praha: Institut pro kriminologii a sociální prevenci.
Novák, K. (1992). *Počítačová kriminalita – Úvod do problematiky.* Institut pro kriminologii a sociální prevenci.
Roubalová, M., Holas, J., Kostelníková, Z., & Pešková, M. (2019). *Oběti kriminality. Poznatky z viktimizační studie.* Praha: Institut pro kriminologii a sociální prevenci.
Rozum, J., Tomášek, J., Vlach, J., & Háková, L. (2016). *Efektivita trestní politiky.* Praha: Institut pro kriminologii a sociální prevenci.
Smejkal, V. (2018). *Kybernetická kriminalita.* 2. vydání. Plzeň: Aleš Čeněk.
Suler, J. (nedatováno). *PSychology of Cyberspace*. Získáno dne 23. 08 2018 z: http://www--usr.rider.edu/~suler/psycyber/psycyber.html
Šámal, P., a další (2012). *Trestní zákoník. Komentář.* 2. vydání. Praha: C. H. Beck.
Válková, H., Kuchta, J. a další (2012). *Základy kriminologie a trestní politiky.* 2. vydání. Praha: C.H.Beck.
Wall, D. S. (2007). *Cybercrime. The Transformation of Crime in the Information Age.* Cambridge: Polity Press.
Willard, N. (2012). *Cyber Savvy: Embracing Digital Safety and Civility.* Thousand Oaks: Corwin Press.

Články, studie

Auxéméry, Y., & Fidelle, G. (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* (7).
Bárta, O., Juhaňák, L., Záleská, K., & Zounek, J. (2018). Presentation at Cyberspace conference 2018: Ambivalence in ICT-related learning (with examples). Získáno 28. 12 2018, z: http://zounek.cz/presentation-at-cyberspace-conference-2018-ambivalence-in-ict-related-learning
Bhardwaj, J. (2012). *Tor and the Deepnet: What price does society pay for anonymity?* Získáno 3. 7. 2018 z: Nakedsecurity.sophos.com/2012/12/06/tor-deepnet-anonymity
Brandejsová, J., Lukášová, K., Mašková, A., & Pacák, R. (2012). Metodika: Výchova k bezpečnému a etickému užívání internetu. Získáno 22. 1. 2019 z: https://www.ncbi.cz/odborna-knihovna/category/6-metodiky-ucebni-materialy.html?download=49:metodika-vychova-k-bezpecnemu-a-etickemu-uzivani-internetu
Broniatowski, D., a další (2018). Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate. Získáno 24. 8. 2018 z: https://ajph.aphapublications.org/doi/10.2105/AJPH.2018.304567
Capin, T. K., Pandzic, I. S., Thalmann, N. M., & Thalmann, D. (1999). Realistic Avatars and Autonomous Virtual Humans in VLNET Networked Virtual Environments. V J. Vince, & R. Earnshaw, *Virtual Worlds on the Internet.* Los Alamitos: Wiley-IEEE Computer Society Press.
Chaudron, S., a další (2015). Young Children (0-8) and digital technology: A qualitative exploratory study across seven countries. *Report EUR 27052 EN*. Joint Research Centre, European Commission.
Dardayrol, J.-P. (2013). L'Internet des objets : quelles perspectives pour les acteurs de la logistique? *Annales des Mines - Réalités industrielles,*(2).

d'Haenens, L., Vandoninck, S., & Donoso, V. (2013). How to cope and build online resilience?. Získáno 31. 8. 2018 z: http://eprints.lse.ac.uk/48115/ http://eprints.lse.ac.uk/48115/1/How%20to%20cope%20and%20build%20online%20resilience%20%28lsero%29.pdf

Europol. (2017). Online sexual coercion and extortion is a crime. Získáno 2. 10. 2017 z: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/online-sexual-coercion-and-extortion-crime

Fialová, E. (2010). Krádež virtuálních předmětů v příkladech z nizozemské judikatury. *Revue pro právo a technologie* (1), 23-28. Získáno z: https://journals.muni.cz/revue/article/view/3980

Freyssinet, É. (2013). L'Internet des objets : un nouveau champ d'action pour la cybercriminalité. *Annales des Mines - Réalités industrielles* (2).

Gřivna, T., & Drápal, J. (2018). Attacks on the confidentiality, integrity and availability of data and computer systems in the criminal case law of the Czech Republic. *Digital Investigation* (28), 1-13.

Chlad, R. (2000). Historie Internetu v České republice. Získáno 30. 8. 2020 z: www.fi.muni.cz/usr/jkucera/pv109/2000/xchlad.htm

Imperva. (2017). Advanced Persistent Threat (APT). Získáno 23. 1. 2019 z: https://www.incapsula.com/web-application-security/apt-advanced-persistent-threat.html

Juhaňák, L., Zounek, J., Záleská, K., Bárta, O., & Vlčková, K. (2019). The relationship between the age at first computer use and students' perceived competence and autonomy in ICT usage: A mediation analysis. *Computers & Education*, Vol. 141.

Kopecký, K., & Szotkowski, R. (2016). Národní výzkum kyberšikany učitelů. Výzkumná zpráva. Univerzita Palackého v Olomouci, Cetnrum prevence rizikové virtuální komunikace, O2, Seznam.cz. Získáno 26. 1. 2019 z: https://www.e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/86-kybersikana-ucitelu-2016-vyzkumna-zpraava/file

Kopecký, K., & Szotkowski, R. (2017). Sexting a rizikové seznamování českých dětí v kyberprostoru. Výzkumná zpráva. Univerzita Palackého v Olomouci, Centrum rizikové virtuální komunikace, O2. Získáno 26. 1. 2019 z: https://drive.google.com/file/d/0B5sdIAT8WtLBUmV5VDdZNlJyRXc/view

Kopecký, K. (2010). *Kybergrooming - nebezpečí kyberprostoru. Studie.* Olomouc: NET UNIVERSITY, s. r. o.

Kopecký, K. (2010). *Stalking a kyberstalking. Studie.* Olomouc: NET UNIVERSITY, s. r. o.

Kudrlová, K. (2014). Kyberkriminalita dnes. In P. Šturma, & Žákovská, K. (Eds.), *VII. konference studentské vědecké odborné činnosti. Sekce doktorandských prací* (pp. 20-33). Praha: Univerzita Karlova v Praze, Právnická fakulta.

Kudrlová, K. (2015). *Kyberkriminalita a dokazování. VIII. ročník SVOČ*. Nepublikovaná práce. Praha: Univerzita Karlova v Praze, Právnická fakulta.

Kudrlová, K. (2016). *Přehled a trendy kyberkriminality. IX. ročník SVOČ*. Nepublikovaná práce. Univerzita Karlova v Praze, Právnická fakulta.

Kudrlová, K. (2017a). Kybergrooming – 3 roky kriminalizace. *Právo-Bezpečnost-Informace*. Zvláštní vydání mezinárodní konference Jihlava. Získáno 5. 9. 2018, z: http://teorieib.cz/pbi/files/334-Kudrlova.pdf

Kudrlová, K. (2017 b). *Přehled a trendy kyberkriminality.* Získáno 29. 8. 2017 z: http://www.mvcr.cz/soubor/trendy-kyberkriminality-iksp-docx.aspx

Kudrlová, K. (2018a). Kybernetická kriminalita - dílčí poznatky z výzkumu II. In Ščerba, F. (ed). Kriminologické dny 2018: Sborník příspěvků z VI. ročníku mezinárodní konference, Olomouc, 18.–19. 1. 2018 (str. 148-157). Získáno 3. 8. 2020, z: http://www.czkrim.cz/cs/soubory-ke-stazeni/sbornik-z-konference-vi-kriminologicke-dny-2018

Kudrlová, K. (2018 b). Počítačové trestné činy v České republice v roce 2015. In Lubelcová, G. (Ed.), *Paralely a divergencie: Zborník z medzinárodnej vedeckej konferencie, Modra-Harmónia, 3.-5.X.2018* (str. 128-139). Bratislava: Univerzita Komenského Bratislava.

Kudrlová, K. (2018c). *Postihování neoprávněného přístupu k počítačovému systému a nosiči informací v roce 2015. XI. ročník SVOČ*. Nepublikovaná práce. Univerzita Karlova v Praze, Právnická fakulta.

Kudrlová, K. & Vlach, J. (2017). Kyberkriminalita (nejen) v ČR – její stav a trendy. *Kriminalistika*, 2017, 256-269

Livingstone, S. & Haddon, L. (2009). EU Kids Online: Final Report. London: LSE. Získáno 29. 12. 2018 z: http://www.lse.ac.uk/media%40lse/research/EUKidsOnline/EU%20Kids%20I%20%282006-9%29/EU%20Kids%20Online%20I%20Reports/EUKidsOnlineFinalReport.pdf.

Livingstone, S., Haddon, L., Görzig, A. & Ólafsson, K. (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. Získáno 29. 12. 2018 z: http://eprints.lse.ac.uk/33731/1/Risks%20and%20safety%20on%20the%20internet%28lsero%29.pdf

Livingstone, S., a další (2016). EU Kids Online. The London School of Economics and Political Science. Získáno 30. 8 2017 z: http://www.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx

Lukášová, K. (2012). Kybergrooming. Získáno 27. 06 2018, z moodle.prf.cuni.cz: https://moodle.prf.cuni.cz/mod/data/view.php?d=8 & rid=188

Madliak, J., Mihaľov, J., Porada, V. & Štefanková, S. (2008). Počítačová kriminalita. *Karlovarská právnická revue* (1), 45-63.

Macháčková, H., & Šerek, J. (2017). Does 'clicking' matter? The role of online participation in adolescents' civic development. *Cyberpsychology* (4).

Masarykova univerzita. (nedatováno). *Výzkum: Náruživé hraní online počítačových her není závislost*. Získáno 24. 8. 2018 z: https://www.muni.cz/pro-media/archiv-tiskovych-zprav/65 027344

Merton, R. K. (1948). The Self-Fulfilling Prophecy. *The Antioch Review* (2).

Ministerstvo školství mládeže a tělovýchovy. (nedatováno). *Strategie digitálního vzdělávání do roku 2020*. Získáno 27. 7. 2018 z: http://www.msmt.cz/vzdelavani/skolstvi-v-cr/strategie-digitalniho-vzdelavani-do-roku-2020

Ministerstvo zdravotnictví. (nedatováno). *Národní strategie elektronického zdravotnictví. Vize*. Získáno 18. 1. 2019 z: http://www.nsez.cz/dokumenty/vize_12546_31.html

Němec, L. & Tornová, J. (2018). K právní regulaci kryptoměn, díl I. Právní rádce. Získáno 29. 12. 2018 z: http://www.glatzova.com/data/attachments/K_pravni_regulaci_kryptomen_dil_1.pdf

Němec, L. & Tornová, J. (2018). K právní regulaci kryptoměn, díl II. Právní rádce. Získáno 29. 12. 2018 z: http://www.glatzova.com/data/attachments/K_pravni_regulaci_kryptomen_dil_2.pdf

Prensky, M. (2001). Digital Natives, Digital Immigrants Part 1. *On the Horizon* (5).

Răcătău, I.-M. (2013). Adolescents and identity formation in a risky online environment. The role of negative user-generated and xenophobic websites. *Journal of Media Research* (3), 16-36.

Reporters Without Borders. (2014). Reporters Without Borders and Torservers.net, partners against online surveillance and censorship. Získáno 14. 7. 2018 z: https://rsf.org/en/news/reporters-without-borders-and-torserversnet-partners-against-online--surveillance-and-censorship

Sabatini, F., & Sarracino, F. (2017). Online Networks and Subjective Well-Being. *Kyklos* (3), 456-480.

Tyson, B. (2018). Fathoming the Depth of the Web: Dark & Deep Web Searches. Získáno 3. 7. 2018, z: www.brighthub.com/internet/google/articles/114820.aspx#imgn_0

Univerzita Palackého v Olomouci, Pedagogická fakulta. (2015). *České děti a Facebook 2015*. Získáno 29. 8. 2017 z: https://drive.google.com/file/d/0B5sdIAT8WtLBZWVQM1FBMTU0WWs/view

Univerzita Palackého v Olomouci, Seznam.cz, Google. (2014). *Výzkum rizikového chování českých dětí v prostředí internetu.* Získáno 29. 8. 2017 z : https://www.e-bezpeci.cz/index.php/ke-stazeni/doc_download/61-vyzkum-rizikoveho-chovani-eskych-dti-v-prostedi-internetu-2014-prezentace

Vejvodová, A. (2018). *Facebookový profil a e-mail díky GDPR budou až od 15 let se souhlasem rodičů*. Získáno 28. 8. 2018 z: https://pravniradce.ihned.cz/c1-66108830-facebookovy--profil-a-e-mail-diky-gdpr-budou-az-od-15-let-se-souhlasem-rodicu

Vejvodová, P. (2018). How to manipulate: the techniques of online disinformation media. Získáno 8. 1. 2019 z: https://www.muni.cz/vyzkum/publikace/1483977

Vláda České republiky. (2018). *Programové prohlášení vlády*. Získáno 21. 7. 2018 z: https://www.vlada.cz/cz/jednani-vlady/programove-prohlaseni/programove-prohlaseni--vlady-165960

Vlach, J. (2018). Kybernetická kriminalita - dílčí poznatky z výzkumu I. In Ščerba, F. (ed). Kriminologické dny 2018: Sborník příspěvků z VI. ročníku mezinárodní konference, Olomouc, 18.–19. 1. 2018 (str. 138-147). Získáno 3. 8. 2020, z: http://www.czkrim.cz/cs/soubory-ke-stazeni/sbornik-z-konference-vi-kriminologicke-dny-2018

Zlatkovský, M. (2016). Jak poznat falešnou zprávu? 9 tipů, jak se vyhnout hoaxům a dezinformacím. Získáno 23. 1. 2019 z: https://www.irozhlas.cz/zpravy--z-domova/jak-poznat-falesnou-zpravu-9-tipu-jak-se-vyhnout-hoaxum-a-dezinformacim_1611280515_

Weby, zprávy o trendech

CZ.NIC. (nedatováno). Získáno 30. 8. 2020, z: https://www.nic.cz

Český statistický úřad. (nedatováno). *Informační společnost v číslech*. Získáno 13. 2. 2020, z: https://www.czso.cz/csu/czso/informacni_spolecnost_v_cislech

Deep Web Links | Deep Web Sites | The Deepweb 2019. (nedatováno). Získáno 29. 1. 2019, z: https://www.deepwebsiteslinks.com/#tableofcontent

ENISA (2017). *ENISA Threat Landscape Report 2016. 15 Top Cyber-Threats and Trends.* Získáno 30. 08 2017, z enisa.europa.eu: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

ENISA. (2018). *ENISA Threat Landscape Report 2017*. Získáno 4. 9. 2018 z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017

ESET. (nedatováno). *Dvojklik*. Získáno 30. 8. 2017 z: 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%7 cutmccn=(organic) %7cutmcmd=organic%7cutmctr=(not%2520 provided)

ESET. (2017). *The year in security: Trends 2017*. Získáno 30. 8. 2017 z: https://www.welivesecurity.com/2017/01/04/year-security-trends-2017

ESET. (2018). *Cyber Security trends of 2018*. Získáno 4. 9. 2018 z: https://www.eset.com/uk/about/newsroom/corporate-blog/blog/cyber-security-trends-of-2018

eukidsonline.net. (nedatováno). *EU Kids Online. Findings, methods, recommendations*. Získáno 29. 08 2018, z lsedesignunit.com: https://lsedesignunit.com/EUKidsOnline/html5/index.html?page=1 & noflash

European Commission. (nedatováno). *Cybercrime*. Získáno 16. 08 2020, z ec.europa.eu: https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en

Europol. (nedatováno). *Europol*. Získáno 30. 8. 2020 z: https://www.europol.europa.eu

Hewlett Packard. (2018). *2018 Cybersecurity Guide: Hackers and defenders harness design and machine learning*. Získáno 4. 9. 2018 z: http://www8.hp.com/h20195/v2/GetPDF.aspx/4AA7-2519ENW.pdf

Hidden Wiki. (nedatováno). *Hidden Wiki. Tor.onion urls directories*. Získáno 14. 4. 2016 z: http://thehiddenwiki.org

IBM. (nedatováno). *IBM X-Force Threat Intelligence Index 2018*. Získáno 4. 9. 2018 z: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=77014377USEN

Internet World Stats. (nedatováno). *The Digital Divide, ICT and Broadband Internet*. Získáno 13. 07 2015, z internetworldstats.com: https://www.internetworldstats.com/links10.htm

Kaspersky Lab. (nedatováno). *Kaspersky Lab Threat Predictions for 2018*. Získáno 4. 9. 2018 z: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07164714/KSB_Predictions_2018_eng.pdf

Kovacs, N. (2017). *Top Ten Cyber Security Predictions for 2017 (Symantec)*. Získáno 30. 8. 2017 z: https://community.norton.com/en/blogs/norton-protection-blog/top-ten-cyber-security-predictions-2017

Lemos, R. (2016). *2016 Emerging Cyber Threats Report*. (Georgia Institute of Technology) Získáno 30. 8. 2017 z: http://www.iisp.gatech.edu/2016-emerging-cyber-threats-report

Malek, M. (2017). *2017 cybercrime trends*. (Future Processing) Získáno 30. 8. 2017, z future-processing.com: https://www.future-processing.com/blog/2017-cybercrime-trends

McAfee Labs. (2017). *2018 Threats Predictions*. Získáno 4. 9. 2018 z: https://www.mcafee.com/enterprise/en-us/assets/infographics/infographic-threats-predictions-2018.pdf

MEDIAN (2017). *e-Government, bezpečnost na internetu*. Získáno 10. 09. 2020, z: https://www.median.eu/cs/wp-content/uploads/2017/02/Kyberneticke_hrozby_MEDIAN_leden_2017.pdf

Ministerstvo spravedlnosti. (nedatováno). *infoData. Statistika a výkaznictví*. Získáno 5. 10. 2020, z: https://cslav.justice.cz/InfoData/uvod.html?timeout=true

Ministerstvo vnitra. (nedatováno). *Statistiky kriminality – dokumenty*. Získáno 10. 09. 2020, z: https://www.mvcr.cz/clanek/statistiky-kriminality-dokumenty.aspx

Národní úřad pro kybernetickou a informační bezpečnost. (nedatováno). *Hrozby*. (Národní bezpečnostní úřad) Získáno 23. 1. 2019, z: https://www.govcert.cz/cs/informacni--servis/hrozby

Patterson, D. (2016). *2017 cybercrime trends: Expect a fresh wave of ransomware and IoT hacks*. (CBS Interactive) Získáno 30. 8. 2017 z: http://www.techrepublic.com/article/2017-cybercrime-trends-expect-a-fresh-wave-of-ransomware-and-iot-hacks

Policie ČR. (nedatováno). *Kriminalita*. Získáno 20. 10. 2020 z: https://www.policie.cz/statistiky-kriminalita.aspx

RSA. (2018). *2018 Current State of Cybercrime*. Získáno 4. 9. 2018, z: https://www.rsa.com/content/dam/premium/en/white-paper/2018-current-state-of-cybercrime.pdf

Security-Portal. (2013). *Seznamte se - APT*. (Security-Portal) Získáno 23. 01 2019, z security-portal.cz: http://www.security-portal.cz/clanky/seznamte-se-apt

Symantec. (2017). *Internet Security Threat Report*. Získáno 30. 8. 2017, z symantec.com: 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

Symantec. (nedatováno). *2018 Internet Security Threat Report*. Získáno 4. 9. 2018 z: https://resource.elq.symantec.com/LP=5840?cid=70138000000rm1eAAA

torservers.net. (nedatováno). Torservers.net. Získáno 14. 7. 2018 z: https://torservers.net

Trend Micro. (2017). *Security Predictions for 2018. Paradigm Shifts*. Získáno 4. 9. 2018 z: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2018

TrendLabs. (2016). *The Next Tier. Trend Micro Security Predictions for 2017*. (TREND MICRO) Získáno 30. 8. 2017, z trendmicro.com: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2017

Wikipedia. (2003). *Digital Divide*. Získáno 13. 7. 2015 z: https://en.wikipedia.org/wiki/Digital_divide

Zvol si info. (nedatováno). *Zvol si info*. Získáno 8. 1. 2019, z: http://zvolsi.info

Cloud - služby či programy uložené na serverech poskytovatele, k nimž uživatel přistupuje na dálku přes internet

CSLAV - Centrální statistika a výkaznictví, informační systém Ministerstva spravedlnosti

DDoS - Distributed Denial of Service, tzv. odmítnutí služby, útok spočívající v zahlcení serveru

Digitální otisk - stopa vlastní osobnosti v online prostředí, zčásti v podobě technických dat, zčásti v podobě informací o konkrétní osobě

Fake news - falešné zprávy, dezinformace

Hacking - neoprávněný průnik do systému. Účelem může být získání informací, poškození, ale i opravení bezpečnostních a jiných chyb systému

Hardware - fyzická součást nebo příslušenství počítače či jiného zařízení, např. procesor, klávesnice atp.

Hosting - pronájem serveru, např. jako úložiště pro fotografie a jiný obsah nebo pro umístění vlastních webových stránek

Informační a komunikační technologie - technologie používané pro komunikaci a práci s informacemi. Zahrnují hardware (např. mobilní telefon) i software a přidružené služby (např. aplikace pro videokonferenci). Společně s jejich uživateli vytváří kyberprostor

Krádež identity - vystupování jménem oběti, jednání jejím jménem a na její účet, často po zneužití přihlašovacích údajů k nějakému účtu – např. komunikace na sociální síti prostřednictvím profilu oběti

Kybergrooming - kontaktování a psychická manipulace oběti (nejčastěji dítěte) prostřednictvím informačních a komunikačních technologií s cílem sexuálně ji zneužít

Kyberkriminalita - kriminalita spojená s využitím informačních (a komunikačních) technologií

Kyberprostor - prostředí tvořené informačními a komunikačními technologiemi a jejich uživateli

Kyberšikana - šikana zneužívající informační a komunikační technologie

Malware - škodlivý software, program určený k poškození nebo vniknutí do systému (slouží např. ke sledování online aktivit uživatele)

Ochranný software - software sloužící k zabezpečení zařízení a minimalizaci případných škod způsobených neoprávněným přístupem do systému, zejména antivirus, firewall aj.

Phishing - e-mail ze zdánlivě důvěryhodného zdroje usilující nejčastěji o přihlašovací údaje adresáta (např. přihlašovací údaje k účtu na sociální síti) nebo jiné osobní údaje (např. číslo bankovního účtu)

Počítačové trestné činy - trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací (§ 230 TZ), opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 TZ) a poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232 TZ), dříve též poškození a zneužití záznamu na nosiči informací (§ 257a sTZ)

Ransomware - zašifrování zařízení (nebo jeho části) bez vědomí jeho uživatele a s požadavkem výkupného za opětovné zpřístupnění

286 Slovníček obsahuje pouze některé z častěji použitých výrazů, přičemž většina z nich je pro srozumitelnost záměrně zjednodušena.

Sociální inženýrství - manipulace uživatele s cílem přimět ho k určitému jednání či naopak k pasivitě

Software - program, aplikace

VPN - Virtual Private Network, vzdálený přístup k nějakému systému

Wi-Fi - bezdrátové připojení k síti (nejčastěji k internetu)

Přehled titulů vydaných v edici Institutu pro kriminologii a sociální prevenci od roku 2012

Ediční řada Studie:

2020

462 Scheinost, M., Barbořík, M., Čáp, J., Diblíková, S., Frydrych, J., Holas, J., Hulmáková, J., Karban, M., Linhartová, H., Martinková, M., Raszková, T., Večerka, K. & Zhřívalová, P. *Analýza trendů kriminality v České republice v roce 2019.*

464 Rozum, J., Háková, L., Hulmáková, J., Špejra, M. & Zhřívalová, P. *Zprávy PMS pro účely rozhodnutí v trestním řízení: kvalita, význam, efektivita*.

2019

449 Roubalová, M., Holas, J., Kostelníková, Z. & Pešková, M. *Oběti kriminality. Poznatky z viktimizační studie.*

452 Tomášek, J., Diblíková, S., Hamplová, N. & Rozum, J. *Rodinné skupinové konference.*

453 Zeman, P., Blatníková, Š., Grohmannová, K., Koňák, T., Novák, P., Roubalová, M. & Trávníčková, I. *Uživatelé drog ve vězení – hodnocení účinnosti terapeutických programů.*

454 Diblíková, S., Cejp, M., Hulmáková, J., Raszková, T., Roubalová, M., Scheinost, M., Večerka, K. & Zhřívalová, P. *Analýza trendů kriminality v České republice v roce 2018.*

455 Roubalová, M., Grohmannová, K., Trávníčková, I. & Zeman, P. *Možnosti zjišťování míry a struktury sekundární drogové kriminality v podmínkách České republiky.*

457 Martinková, M. & Biedermanová, E. *Senioři v České republice jako oběti i pachatelé kriminálních deliktů.*

2018

447 Diblíková, S., Cejp, M., Hulmáková, J., Pešková, M., Scheinost, M. & Večerka, K. *Analýza trendů kriminality v České republice v roce 2017.*

446 Scheinost, M., Cejp, Diviák, T. & Pojman, P. *Trendy vývoje organizovaného zločinu a jeho vybraných forem.*

2017

440 Zeman, P. (ed.) *Research on Crime and Criminal Justice in the Czech Republic (selected results of research activities of IKSP in the years 2012–2015).*

441 Tomášek, J., Faridová, P., Kostelníková, Z., Přesličková, H., Rozum, J. & Zhřívalová, P. *Zaměstnání jako faktor desistence.*

443 Karabec, Z., Diblíková, S., Hulmáková, J., Vlach, & Zeman, P. *Criminal Justice System in the Czech Republic. 3rd amended and revised edition.*

444 Budka, I. *Využití právních nástrojů pro potírání organizovaného zločinu.*

445 Diblíková, S., Hulmáková, J., Karban, M., Martinková, M., Scheinost, M. & Večerka, K. *Analýza trendů kriminality v České republice v roce 2016.*

2016

431 Blatníková, Š., Faridová, P., Vranka, M. *Kriminální styly myšlení: Inventář PICT-cz.*

432 Marešová, A., Biedermanová, E., Rozum, J., Tamchyna, M. & Zhřívalová, P. *Výkon nepodmíněného trestu odnětí svobody – kriminologická analýza.*

433 Blatníková, Š. *Nebezpečnost a násilí ve vězeňském prostředí.*

435 Holas, J., Háková, L., Krulichová, E. & Scheinost, M. *Regionální kriminalita a její odraz v kvalitě života obyvatel.*

437 Diblíková, S., Cejp, M., Martinková, M., Smejkal, V. & Štefunková, M. *Analýza trendů kriminality v České republice v roce 2015.*

438 Tomášek, J., Diblíková, S. & Scheinost, M. *Probace jako efektivní nástroj snižování recidivy.*

439 Rozum, J., Háková, L., Tomášek, J., & Vlach, J. *Efektivita trestní politiky z pohledu recidivy.*

2015

423 Scheinost, M., Háková, L., Rozum, J., Tomášek, J. & Vlach, J. *Trestní sankce – jejich uplatňování, vliv na recidivu a mediální obraz v televizním zpravodajství. (Teoretické a trestněpolitické aspekty reformy trestního práva v oblasti trestních sankcí III.).*

424 Marešová, A., Havel, R., Martinková, M. & Tamchyna, M. *Násilná kriminalita v nejisté době.*

425 Marešová, A., Biedermanová, E., Diblíková, S., Požár, J. & Martinková, M. *Analýza trendů kriminality v ČR v roce 2014.*

426 Zeman, P., Štefunková, M. & Trávníčková, I. *Drogová kriminalita a trestní zákoník.*

427 Večerka, K. & Štěchová, M. *Preventivní praxe po novelizaci zákona o sociálně-právní ochraně dětí.*

428 Blatníková, Š., Faridová, P. & Zeman, P. *Znásilnění v ČR – trestné činy a odsouzení pachatelé.*

429 Scheinost, M., Válková, H., (eds.) *Sankční politika a její uplatňování. (Teoretické a trestněpolitické aspekty reformy trestního práva v oblasti trestních sankcí IV.).*

430 Cejp, M., Blatníková, Š., Háková, L., Holas, J., Trávníčková, I. & Vlach, J. *Společenské zdroje vývoje organizovaného zločinu.*

422 Škvain, P. *Zabezpečovací detence z pohledu vybraných zahraničních právních úprav.*

2014

414 Martinková, M., Slavětínský, V. & Vlach, J. *Vybrané problémy z oblasti domácího násilí v ČR.*

415 Štěchová, M. & Večerka, K. *Systémový přístup k prevenci kriminality mládeže.*

417 Marešová, A., Cejp, M., Holas, J., Martinková, M. & Rozum, J. *Analýza trendů kriminality v roce 2013.*

418 Blatníková, Š., Faridová, P. & Zeman, P. *Násilná sexuální kriminalita – téma pro experty i veřejnost.*

419 Scheinost, M., Háková, L., Rozum, J., Tomášek, J. & Vlach, J. *Sankční politika pohledem praxe. (Teoretické a trestněpolitické aspekty reformy trestního práva v oblasti trestních sankcí II.).*

2013

403 Košťál, J. *Vybrané metody vícerozměrné statistiky.* (Vybrané metody kriminologického výzkumu – svazek 4).

404 Pojman, P. *Ruský a ukrajinský organizovaný zločin.*

405 Tomášek, J. *Self-reportové studie kriminálního chování.* (Vybrané metody kriminologického výzkumu – svazek 5).
406 Holas, J. *Politický radikalismus a mládež.*
408 Zeman, P., Diblíková, S., Slavětínský, V. & Štefunková, M. *Zkrácené formy trestního řízení – možnosti a limity.*
410 Scheinost, M., a kol. *Trestní sankce a jejich odraz v praxi, tisku a v názorech veřejnosti. (Teoretické a trestněpolitické aspekty reformy trestního práva v oblasti trestních sankcí I.).*
411 Marešová, A., Cejp, M., Holas, J., Kuchařík, K., Martinková, M. & Scheinost, M. *Analýza trendů kriminality v roce 2012.*
412 Holas, J. & Večerka, K. *Stát a občan v prevenci kriminality.*

2012

397 Cejp, M. (ed.) *Selected Results of Research Activities of ICSP in the Years 2008–2011.*
398 Marešová, A., Cejp, M., Martinková, M., Tomášek, J., Vlach, J. & Zeman, P. *Crime in the Czech Republic in 2010.*
399 Večerka, K. *Mládež o kriminalitě a etice každodennosti.*
402 Marešová, A., Biedermanová, E., Cejp, M., Holas, J., Martinková, M. & Tomášek, J. *Analýza trendů kriminality v roce 2011.*

Ediční řada Prameny:

2020

461 *Globální studie o pašování migrantů 2018.*

2019

448 Heiskanen, M. & Lietonen, A. *Kriminalita a gender. Studie zaměřená na zastoupení mužů a žen v mezinárodní statistice kriminality.*
450 *Škody působené kybernetickou kriminalitou. Zpráva shrnující hlavní poznatky Pracovní skupiny k nákladům kyberkriminality.*
451 *Příručka k evaluaci. Pokyny k navrhování, provádění a používání nezávislé evaluace v UNODC.*

2017

442 UNODC: *Mezinárodní klasifikace trestných činů pro statistické účely.*

2016

434 Heiskanen, M., Aebi, M. E., van der Brugge, W., Jehle, J.-M. *Evidence alternativních trestů a zjišťování míry atrice. Metodologická studie komparativních dat v Evropě.*
436 *13. kongres OSN o prevenci kriminality a trestní justici. Dauhá, Katar, 12.-19. dubna 2015*

2015

420 Francis, B., Humphreys, L., Kirby, S. & Soothill, K. *Kriminální kariéra v organizovaném zločinu.*
421 Mendel, R. A. *Mládeži nepřístupno. Argumenty pro snižování počtu odnětí svobody u mladistvých.*

2014

416 Benes, M. & Astbury, B. (eds.) *Problémy trestního soudnictví: evaluace programů, prevence kriminality, strach z kriminality a recidiva – pohledem australských kriminologů.*

2013

407 United Nations Office on Drugs and Crime *Odhad nezákonných finančních toků plynoucích z obchodu s drogami a jiného nadnárodního organizovaného zločinu.*

409 United Nations Office on Drugs and Crime *Světová zpráva o obchodování s lidmi 2012.*

413 European Forum for Urban Security *Pouliční násilí v EU: Skupiny mladistvých a násilí na veřejnosti.*

2012

395 Cejp, M. (ed.) *Britské strategické dokumenty k prevenci a potírání závažné trestné činnosti.*

396 Goodey, J. & Aromaa, K. (eds.) *Trestné činy z nenávisti (příspěvky ze Stockholmského kriminologického sympozia 2006 a 2007).*

400 Marešová, A. (ed.) *Trendy kriminality ve světě a nové problémy a reakce v oblasti prevence kriminality a trestní justice.*

401 Diblíková, S. (ed.) *Rada Evropy a International Juvenile Justice Observatory k soudnictví nad mládeží.*

Plné texty všech titulů, publikovaných v edici Institutu pro kriminologii a sociální prevenci od roku 2000, jsou volně dostupné na webu IKSP www.kriminologie.cz v sekci Publikace.

Kyberkriminalita v kriminologické perspektivě

Autoři:	Jiří Vlach Kateřina Kudrlová Viktorie Paloušová
Vydavatel:	Institut pro kriminologii a sociální prevenci Nám. 14. října 12, Praha 5
Určeno:	Pro odbornou veřejnost
Design:	addnoise.org
Sazba:	Lukáš Pracný, sazbaknih.cz
Tisk:	Reprocentrum, a. s., Blansko
Dáno do tisku:	prosinec 2020
Vydání:	první
Náklad:	200 ks

www.kriminologie.cz

ISBN 978-80-7338-189-9