Univerzita Karlova v Praze
Právnická fakulta

Kyberkriminalita dnes

Studentská vědecká a odborná činnost

Kategoriedoktorské studium

Autor/Autoři: Mgr. et Mgr. Kateřina Kudrlová

2014
VII. ročník SVOČ

Čestné prohlášení a souhlas s publikací práce

Prohlašuji, že jsem práci předkládanou do VII. ročníku Studentské vědecké a odborné činnosti (SVOČ) vypracovala samostatně za použití literatury a zdrojů v ní uvedených. Dále prohlašuji, že práce nebyla ani jako celek, ani z podstatné části dříve publikována, obhájena jako součást bakalářské, diplomové, rigorózní nebo jiné studentské kvalifikační práce a nebyla přihlášena do předchozích ročníků SVOČ či jiné soutěže.

Souhlasím s užitím této práce rozšiřováním, rozmnožováním a sdělováním veřejnosti v neomezeném rozsahu pro účely publikace a prezentace PF UK, včetně užití třetími osobami.

V Praze dne 15. dubna 2014.

……. ……

Mgr. et Mgr. Kateřina Kudrlová

Kyberkriminalita dnes

Text se věnuje z hmotněprávního pohledu skutkovým podstatám počítačových trestných činů a dalším relevantním ustanovením trestního zákoníku, včetně návrhu jeho novelizace projednávaném v současnosti v Poslanecké sněmovně ČR. Závěr obsahuje stručný výčet nejčastějších společensky škodlivých jednání spojených s kyberprostorem.

Cybercrime today

The text deals with so called computer crimes and other relevant provisions of the Czech Criminal Code (from the point of view of the substantive law), including the draft currently discussed in the Chamber of Deputies of the Czech Republic. It contains also a brief list of the most common socially harmful conduct associated with cyberspace.

Kyberkriminalita dnes

Kyberkriminalita dnes.[1] Co si pod tím představit? Na jednu stranu tak úzké téma, na stranu druhou naopak velmi, velmi široké. Zůstaňme nejprve u toho užšího, resp. nejužšího. Kyberkriminalita v tomto smyslu znamená určitou specifickou výseč kriminality obecně jako takové, ať už se hovoří o kriminalitě zjevné či latentní. Budeme-li chtít být skutečně úzkostní co do obsahu kyberkriminality, zůstaneme v rámci trestního zákona u několika málo skutkových podstat specifických pro kyberkriminalitu, a to trestné činy neoprávněný přístup k počítačovému systému a nosiči informací dle § 230 zákona č. 40/2009 Sb., trestní zákoník (dále jen „TZ"), opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat podle § 231 TZ a poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti podle § 232 TZ. Stručné, jasné, jednoduché. Leč realitu nepostihující.

Následující text se proto věnuje z hmotněprávního pohledu uvedeným skutkovým podstatám a dalším relevantním ustanovením trestního zákoníku, včetně návrhu jeho novelizace projednávaném v současnosti v Poslanecké sněmovně ČR. Závěr pak obsahuje stručný výčet nejčastějších společensky škodlivých jednání spojených s kyberprostorem.

Počítačové trestné činy

Uvedené tři tzv. počítačové trestné činy zahrnují celkem čtyři samostatné a zároveň základní skutkové podstaty. Trestným činem se dvěma základními skutkovými podstatami je neoprávněný přístup k počítačovému systému a nosiči informací dle § 230 TZ,[2] který v prvním odstavci dopadá na jakýkoliv neoprávněný přístup k počítačovému systému a nosiči informací,[3] tzn. takový přístup, při němž pachatel překoná bezpečnostní opatření mající za úkol přístup omezit.[4] V současné době se jedná nejčastěji o překážku omezující přístup

[1] Příspěvek vznikl za podpory programu rozvoje vědních oblastí na Univerzitě Karlově (PRVOUK) P06 "Veřejné právo v kontextu europeizace a globalizace" – koordinátor prof. JUDr. PhDr. Michal Tomášek, DrSc.

[2] Vzhledem k tomu, že se jedná o nejfrekventovanější z počítačových trestných činů, je mu zde věnován větší prostor.

[3] Takovým nosičem je typicky např. harddisk, DVD, USB flash disk aj.

[4] Viz Šámal, P. a kol. Trestní zákoník: komentář. 2. vyd. C.H. Beck: Praha, 2012, str. 2305.

k fyzickému zařízení prostřednictvím internetu v podobě firewallu,[5] obvykle též zároveň za použití ochranného softwaru typu antivirového programu,[6] případně tzv. antispyware.[7] Bezpečnostních opatření si uživatel nemusí ani býti zcela vědom (např. má určité povědomí o tom, že používá nějaký antivirový program zabraňující průniku nevyžádaného softwaru do vlastního zařízení a vyhledávající takový škodlivý software (tzv. malware) již případně nevědomky nainstalovaný, netuší však již, že součástí daného antivirového programu je zároveň antispyware, který má za úkol nedovolit žádnému softwaru bez předchozího souhlasu uživatele sledovat data v zařízení.[8] A samozřejmě nelze opomenout ani základní ochranu obsahu či přístupu prostřednictvím hesla, bez ohledu na jeho snadnou prolomitelnost[9] či naopak sílu.

Naplnění objektivní stránky skutkové podstaty trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 odst. 1 TZ může být samotným cílem pachatele (např. pachatel chce zjistit obsah nosiče informací, např. USB flash disku chráněného heslem, aniž by však měl v úmyslu s daty tam uloženými jakýmkoliv způsobem manipulovat či k nim přidat data jiná).

Nebude však výjimkou, aby uvedené jednání sloužilo jako příprava k dalšímu jednání, zejm. v podobě naplňující objektivní stránku základní skutkové podstaty trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 odst. 2 TZ. Zde již nezáleží na oprávněnosti získání přístupu k počítačovému systému nebo nosiči informací. Může tedy jít o přístup oprávněný, jako například přístup administrátora spravujícího firemní

---

[5] Firewall je „síťové zařízení, které slouží k řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení," viz Wikipedie, Firewall. Dostupné na http://cs.wikipedia.org/wiki/Firewall (11. dubna 2014). Zjednodušeně lze firewall popsat jako částečně prostupnou mřížku propouštějící oběma směry pouze určitá do jisté míry ověřená data (včetně zohlednění místa jejich určení).

[6] Tzv. antivir je „počítačový software, který slouží k identifikaci, odstraňování a eliminaci počítačových virů a jiného škodlivého software (malware)," viz Wikipedie, Antivirový program. Dostupné na http://cs.wikipedia.org/wiki/Antivir (11. dubna 2014).

[7] Tzv. spyware je počítačový „program, který využívá internetové stránky k odesílání dat z počítače bez vědomí jeho uživatele," viz Wikipedie, Spyware. Dostupné na http://cs.wikipedia.org/wiki/Spyware (11. dubna 2014).

[8] Tzv. spyware nemusí znamenat přímé ohrožení zařízení jako např. při napadení virem, avšak samotné sledování dat může být výrazným zásahem do soukromí uživatele, nemluvě o případech „odposlechu" či „odpozorování" citlivých osobních údajů, hesel atp.

[9] V případě příliš krátkých hesel, hesel jako „heslo", „aaaaa", „123456789" atp.

síť v rámci pracovněprávních povinností, stejně tak jako přístup neoprávněný, kterým je zároveň naplněna skutková podstata trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 odst. 1 TZ, která však pravděpodobně bude fakticky konzumována.

Skutkovou podstatu trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 odst. 2 TZ lze naplnit pestrou škálou jednání spočívajících zpravidla v neoprávněném nakládání s uloženými daty, k nimž pachatel získal přístup. Dle § 230 odst. 2 písm. a) TZ tak lze učinit neoprávněným užitím uložených dat. Dle § 230 odst. 2 písm. b) TZ tak lze učinit jejich neoprávněným vymazáním nebo jejich jiným zničením, poškozením, změnou, potlačením, snížením jejich kvality nebo jejich učiněním neupotřebitelnými. Dle § 230 odst. 2 písm. c) TZ tak lze učinit jejich padělaním nebo pozměněním tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá. Dle § 230 odst. 2 písm. c) TZ tak lze učinit jejich neoprávněným vložením nebo jiným zásahem do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat.

Ke znakům kvalifikované skutkové podstaty patří úmysl způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch, nebo úmysl neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat, nebo spáchání činu uvedeného v odstavci 1 nebo 2 jako člen organizované skupiny, způsobení takovým činem značné škody nebo škody velkého rozsahu[10] nebo nebo získání značného prospěchu nebo prospěchu velkého rozsahu[11] nebo způsobení vážné poruchy v činnosti orgánu státní správy, územní samosprávy, soudu nebo jiného orgánu veřejné moci nebo způsobení vážné poruchy v činnosti právnické nebo fyzické osoby, která je podnikatelem.

Objektivní stránku skutkové podstaty trestného činu opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat dle § 231 TZ lze naplnit pouze v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) TZ nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2 TZ, a to nakládáním s prostředkem určeným k takovému jednání. Může jím být dle § 231 odst. 1 písm. a) TZ např. zařízení nebo jeho součást nebo počítačový program, vytvořené nebo přizpůsobené k neoprávněnému přístupu do sítě

[10] K výši škody zde a dále srov. § 138 odst. 1 TZ.

[11] K výši prospěchu zde a dále srov. § 138 odst. 2 TZ.

elektronických komunikací, k počítačovému systému nebo k jeho části; dle § 231 odst. 1 písm. b) TZ např. počítačové heslo, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části. V obou případech musí dojít k nakládání v podobě výroby, uvedení do oběhu, dovezení, vyvezení, provezení, nabízení, zprostředkování, prodeje nebo jiného zpřístupnění, sobě nebo jinému opatření nebo přechovávání.

I zde lze naplnit kvalifikovanou skutkovou podstatu spácháním činu jako člen organizované skupiny nebo získáním takovým činem pro sebe nebo pro jiného značného prospěchu nebo prospěchu velkého rozsahu.

Objektivní stránku skutkové podstaty trestného činu poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti dle § 232 TZ může naplnit, kdo způsobí na cizím majetku porušením povinnosti vyplývající ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté značnou škodu[12] tím, že určitým způsobem znehodnotí data uložená v počítačovém systému nebo na nosiči informací (zničí, poškodí, pozmění nebo učiní neupotřebitelnými), nebo učiní zásah do technického nebo programového vybavení počítače nebo jiného technického zařízení pro zpracování dat.

Spáchat uvedené tři tzv. počítačové trestné činy může za splnění uvedených podmínek fyzická i právnická osoba, viz § 7 zákona č. 418/2011 Sb, o trestní odpovědnosti právnických osob a řízení proti nim (dále jen „ZTOPO“).[13] Pouze skutková podstata trestného činu poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti dle § 232 TZ vyžaduje speciální subjekt – tím může být „jednak osoba (fyzická nebo právnická), která vykonává zaměstnání, povolání, postavení nebo funkci, jednak i jiná osoba (fyzická nebo právnická), která porušila zákonem uloženou nebo smluvně převzatou povinnost.“[14]

Objektem počítačových trestných činů je „zájem na ochraně počítačových systémů a jejich částí, dále dat v nich uložených a dat uložených na nosičích informací a také na ochraně počítačů nebo jiných technických zařízeních pro zpracování dat před neoprávněnými přístupy

[12] Způsobením škody velkého rozsahu lze naplnit kvalifikovanou skutkovou podstatu trestného činu poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti dle § 232 odst. 1, 2 TZ.

[13] K tomu blíže srov. § 110 TZ a § 1 odst. 1 a 2 ZTOPO.

[14] Viz Šámal, P. a kol. Trestní zákoník: komentář. 2. vyd. C.H. Beck: Praha, 2012, str. 2323.

a zásahy.[15]

Z hlediska subjektivní stránky vyžadují základní skutkové podstaty trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 odst. 1 TZ a dle § 230 odst. 2 TZ a trestného činu opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat dle § 231 odst. 1 TZ úmyslné zavinění, zatímco k naplnění skutkové podstaty trestného činu poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti dle § 232 odst. 1 TZ postačí zavinění z hrubé nedbalosti, jak ostatně název naznačuje. Hrubá nedbalost je taková, kdy „přístup pachatele k požadavku náležité opatrnosti svědčí o zřejmé bezohlednosti pachatele k zájmům chráněných trestním zákonem.“[16]

Co se týče subjektivní stránky u kvalifikovaných skutkových podstat počítačových trestných činů, úmysl se vyžaduje pro naplnění skutkové podstaty trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 odst. 3 písm. a) i b) TZ, stejně tak dle § 230 odst. 4 písm. a) TZ (v tomto případě vyplývá z povahy věci), totéž platí pro naplnění subjektivní stránky skutkové podstaty trestného činu opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat dle § 231 odst. 2 písm. a) TZ. Ve všech ostatních případech kvalifikovaných skutkových podstat počítačových trestných činů postačí nedbalostní zavinění okolnosti zvlášť přitěžující, zde vždy v podobě těžšího následku.[17]

Zde uvedené tři počítačové trestné činy jsou zařazeny v rámci hlavy V. trestního zákoníku. Kromě kvalifikované skutkové podstaty trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 odst. 1, 5 TZ nebo dle § 230 odst. 2, 5 TZ, kdy jde o zločin,[18] jedná se ve všech případech o přečiny.[19]

---

[15] Viz Novotný, O., Vokoun, R., Šámal, P. a kol. Trestní právo hmotné. 6. vyd. Wolters Kluwer ČR, a.s.: Praha, 2010, str. 209.

[16] Viz Šámal, P. a kol. Trestní zákoník: komentář. 2. vyd. C.H. Beck: Praha, 2012, str. 2323.

[17] Srov. § 17 písm. a) TZ a § 230 odst. 4 písm. b), c), d) a e), odst. 5 TZ, § 231 odst. 2 písm. b), odst. 3 TZ a § 232 odst. 2 TZ.

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

[19] Za uvedená jednání hrozí trest odnětí svobody s horní hranicí šest měsíců, jeden rok, dvě léta, tři léta nebo pět

Další relevantní ustanovení

Vyjma tzv. počítačových trestných činů ovšem reaguje trestní zákoník i dalšími ustanoveními na „kyberrealitu“, tj. realitu neodmyslitelně spojenou s kyberprostorem.[20] Činí tak především prostřednictvím uvedení zvlášť přitěžující okolnosti u některých skutkových podstat spočívající ve spáchání činu veřejně nebo veřejně přístupnou počítačovou sítí. Dle § 117 písm. a) TZ je trestný čin spáchán veřejně mimo jiné tehdy, je-li spáchán veřejně přístupnou počítačovou sítí.[21] Z hlediska spáchání činu veřejně přístupnou počítačovou sítí jakožto okolnosti podmiňující použití vyšší trestní sazby[22] se jedná o skutkovou podstatu trestného činu neoprávněného nakládání s osobními údaji dle § 180 odst. § 3 písm. b) TZ, pomluvy dle § 184 odst. 2 TZ, šíření pornografie dle § 191 odst. 3 písm. b) TZ, výroby a jiného nakládání s dětskou pornografií dle § 192 odst. 3 písm. b) TZ, šíření toxikomanie dle § 287 odst. 2 písm. c) TZ, křivého obvinění dle § 345 odst. 3 písm. b) TZ, násilí proti skupině obyvatelů a proti jednotlivci dle § 352 odst. 3 písm. b) TZ, hanobení národa, rasy, etnické nebo jiné skupiny osob dle § 355 odst. 2 písm. b) TZ, podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod dle § 356 odst. 3 písm. a) TZ, založení, podpory a propagace hnutí směřujícího k potlačení práv a svobod člověka dle § 403 odst. 2 písm. a) TZ a podněcování útočné války dle § 407 odst. 2 písm. b) TZ. Pachatelem trestného činu dle § 192 odst. 3 písm. b) TZ, § 352 odst. 3 písm. b) TZ, § 355 odst. 2 písm. b) TZ a § 356 odst. 3 písm. a) TZ může být i právnická osoba, viz § 7 ZTOPO.

---

let – ve všech těchto případech se jedná o přečin (v případě přečinu poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti dle § 232 TZ již vzhledem k tomu, že se jedná o nedbalostní trestný čin), srov. § 14 odst. 2 TZ.

[20] Kyberprostor zahrnuje veškerý virtuální prostor, tedy i svět mobilních telefonů a obecně i všech zařízení pracujících ve spojení s internetem, resp. v prostoru sítí. Z kyberprostoru by proto neměla být vynechávána ani např. problematika webových kamer, bezdrátových tiskáren aj. obdobných zařízení, bezpečnostních alarmů atp. Spolu s rozvojem informačních a komunikačních technologií se stále rozšiřuje oblast jejich použití: již dávno se nejedná o pouhou komunikaci prostřednictvím e-mailů nebo různých komunikátorů (software zajišťující psanou komunikaci v reálném čase – tzv. „instant messaging“), naopak kyberprostor zasahuje do mnoha dalších oblastí, vč. např. dálkového ovládání rodinného domu, přesunování agendy veřejné správy na internet a do podoby různých veřejně přístupných databází, také včetně virtuálních konferencí, zdravotnických úkonů prováděných na dálku, sledování pohybu zásilek i osob, získávání osobních údajů (ať už se souhlasem subjektu údajů nebo bez něj) atp.

[21] 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,“ viz Šámal, P. a kol. Trestní zákoník: komentář. 2. vyd. C.H. Beck: Praha, 2012, str. 1300.

[22] Viz § 17 TZ.

Ani výše uvedenými skutkovými podstatami se však vztah ke kyberprostoru zcela nevyčerpává. Vzhledem ke znění § 117 písm. a) TZ, podle něhož je trestný čin spáchaný veřejně přístupnou počítačovou sítí spáchán veřejně, je nutno sledovat i tento znak, tedy spáchání trestného činu veřejně, neboť je možné ho naplnit mimo jiné právě prostřednictvím veřejně přístupné počítačové sítě. Relevantní jsou proto též skutkové podstaty trestného činu teroristického útoku dle § 311 odst. 2 alinea 2 TZ, hanobení národa, rasy, etnické nebo jiné skupiny osob dle § 355 odst. 1 písm. a) i b) TZ, podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod dle § 356 odst. 1 TZ, podněcování k trestnému činu dle § 364 TZ, schvalování trestného činu dle § 365 odst. 1 TZ, projevu sympatií k hnutí směřujícímu k potlačení práv a svobod člověka dle § 404 TZ, popírání, zpochybňování, schvalování a ospravedlňování genocidia dle § 405 TZ a podněcování útočné války dle § 407 odst. 1 TZ. Pachatelem trestného činu dle § 311 odst. 2 alinea 2 TZ, § 355 odst. 1 písm. a) i b) TZ, § 356 odst. 1 TZ, § 364 TZ, § 404 TZ a § 405 TZ může být i právnická osoba, viz § 7 ZTOPO.

Do skupiny právě uvedené spadá i skutková podstata trestného činu týrání zvířat dle § 302 odst. 1 písm. b) TZ, kterou naplní ten, kdo týrá zvíře surovým nebo trýznivým způsobem veřejně nebo na místě veřejnosti přístupném, a skutková podstata trestného činu výtržnictví dle § 358 odst. 1 TZ, kterou naplní, kdo se dopustí veřejně nebo na místě veřejnosti přístupném hrubé neslušnosti nebo výtržnosti. Místo veřejnosti přístupné je „každé místo, kam má přístup široký okruh lidí individuálně neurčených a kde se také zpravidla více lidí zdržuje, takže týrání zvířete může vnímat více lidí, byť v době činu tam nemusí být přítomni. Takové místo však nemusí být přístupné bez omezení komukoli a kdykoli ..., nýbrž postačí, že jsou přístupné jen některým osobám určeným např. povahou jejich zaměstnání nebo jinak a v určitou dobu ...“[23] Takovým neveřejným místem proto může být z hlediska kyberprostoru např. i uzavřená firemní počítačová síť, ke které bude mít přístup široký okruh blíže neurčených osob (např. po zadání příslušných přihlašovacích údajů opravňujících uživatele-zaměstnance ke vstupu do prostoru sítě), aniž by se však jednalo o veřejně přístupnou počítačovou síť. V případě, že k takové uzavřené síti bude mít přístup jen malý okruh blíže neurčených osob, nemělo by se jednat o spáchání činu na místě veřejnosti přístupném a tím spíše ne o spáchání činu veřejně přístupnou počítačovou sítí, nicméně stále může dané jednání z hlediska okruhu možných zasažených osob[24] dosáhnout takové intenzity, aby se jednalo o

[23] Viz Šámal, P. a kol. Trestní zákoník: komentář. 2. vyd. C.H. Beck: Praha, 2012, str. 3013 a 3324.

[24] Zasažených osob ve smyslu těch, na koho může mít pozorované jednání vliv – typicky přihlížející.

spáchání činu veřejně dle § 117 písm. a) TZ, a to „jiným obdobně účinným způsobem“.

Další prvek kyberprostoru lze nalézt u těch skutkových podstat, které operují se zveřejněním určitého obsahu nebo jeho učiněním veřejně přístupným, kdy takovým zveřejněním bude i zveřejnění nebo zpřístupnění na veřejně přístupné počítačové síti, typicky na Internetu. Ovšem zejména v případě zveřejnění nebo zpřístupnění na tzv. sociální síti[25] bude třeba zabývat se každým jednotlivým konkrétním případem z hlediska posouzení, zda je zveřejnění nebo zpřístupnění takové intenzity, jaké odpovídá spáchání činu veřejně přístupnou počítačovou sítí dle § 117 písm. a) TZ. Již dříve bylo judikováno, že spáchání činu e-mailem takové intenzity bez dalšího nedosahuje. V případě profilu na sociální síti je třeba nejprve rozlišit, zda je veřejný nebo naopak neveřejný. U veřejného profilu k němu má přístup zpravidla kdokoliv, případně s omezující podmínkou vlastního účtu na dané sociální síti.[26] Zveřejnění nebo zpřístupnění obsahu na takovém profilu proto bude svou intenzitou odpovídat spáchání činu veřejně přístupnou počítačovou sítí. U neveřejného profilu je obvykle přístup ostatních uživatelů dané sítě nějakým způsobem dále omezen. Je proto třeba sledovat, kolik osob mohlo nebo stále ještě může mít přístup ke zveřejněnému obsahu. Škála variací začíná u několika málo osob, které mají přístup ke zveřejněnému obsahu na daném účtu, a přes menší či větší skupiny (např. žáci jedné školní třídy nebo celé školy) se dostává až na tisíce uživatelů.[27] Jsou ovšem i takové profily, kde naopak jejich obsah není viditelný nikomu kromě samotného uživatele-autora. Proto lze teprve na základě takového posouzení dojít k závěru, zda se mohlo jednat o spáchání činu s obdobnou intenzitou jako spáchání veřejně přístupnou počítačovou sítí. Z hlediska relevantních skutkových podstat v tomto směru přichází v úvahu skutková podstata trestného činu neoprávněného nakládání s osobními údaji dle § 180 odst. 1 a 2 TZ, porušení tajemství listin a jiných dokumentů uchovávaných v soukromí dle § 183 odst. 1 TZ, šíření pornografie dle § 191 odst. 1 TZ a výroby a jiného nakládání s dětskou pornografií dle § 192 odst. 2 TZ. Pachatelem trestného činu dle § 192 odst. 2 TZ může být i právnická osoba, viz § 7 ZTOPO.

---

[25] Sociální síť je „virtuální propojení skupiny lidí, umožňující mezi nimi sdílet různé typy informací,“ viz Aktuálně.cz, Sociální sítě. dostupné na http://www.aktualne.cz/wiki/veda-a-technika/socialni-site/r~i:wiki:1456/ (10.4.2014).

[26] U nejčastěji používaných sociálních sítí typu Facebook, Google + aj. je vzhledem k množství uživatelů tato podmínka z hlediska omezení množství osob s přístupem k profilu, na němž je obsah zveřejněn, prakticky bezvýznamná, u lokálních sítí, přístupných např. pouze pro určitou omezenou skupinu osob (např. studenti jedné třídy), by bylo třeba posoudit každý případ samostatně.

[27] Např. Facebook omezuje množství kontaktů, tzv. „přátel“, které jsou navázány na jeden profil, na pět tisíc.

Svým způsobem se dotýkají oblasti kyberprostoru i některé další skutkové podstaty, k nimž patří i trestný čin porušení tajemství dopravovaných zpráv dle § 182 TZ. V prvním odstavci se vztahuje mimo jiné k úmyslnému porušení tajemství datových, textových, hlasových, zvukových či obrazových zpráv posílaných prostřednictvím sítě elektronických komunikací a přiřaditelných k identifikovanému účastníku nebo uživateli, který zprávu přijímá, a k neveřejnému přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková počítačová data,[28] viz § 182 odst. 1 písm. b) a c) TZ. Typicky proto půjde např. o e-mail, se kterým se dosud adresát neměl možnost seznámit.[29] Klíčový je proto okamžik, kdy poprvé vstoupí uživatel do své e-mailové schránky poté, co e-mail dorazil na místo svého určení, tj. na příslušný server, jehož prostřednictvím se může adresát s obsahem e-mailu seznámit. Dále se dotýká kyberprostoru i druhý odstavec § 182 TZ, když se zde hovoří o prozrazení nebo využití tajemství, o němž se pachatel dozvěděl z přenosu prostřednictvím sítě elektronických komunikací, který nebyl určen jemu. Obdobně též základní skutková podstata trestného činu porušení tajemství dopravovaných zpráv dle § 182 odst. 5 písm. c) TZ, kterou může naplnit pouze speciální subjekt, a to mimo jiné zaměstnanec provozovatele počítačového systému anebo kdokoli jiný vykonávající komunikační činnosti, pokud pozmění nebo potlačí mimo jiné zprávu podanou neveřejným přenosem počítačových dat nebo jiným podobným způsobem. Pachatelem trestného činu dle § 182 odst. 1 písm. b) a c) TZ i § 182 odst. 5 písm. c) TZ může být i právnická osoba, viz § 7 ZTOPO.

Vynechat nelze ani skutkovou podstatu trestného činu porušení tajemství listin a jiných dokumentů uchovávaných v soukromí dle § 183 odst. 1 TZ, která taktéž dopadá na neoprávněné nakládání s e-maily a dalším obsahem,[30] když postihuje jednání spočívající v neoprávněném porušení tajemství mimo jiné počítačových dat nebo jiného záznamu[31] uchovávaného v soukromí jiného tím, že je zveřejní, zpřístupní třetí osobě nebo je jiným způsobem použije. Z hlediska e-mailu se bude jednat o takové neoprávněné nakládání s ním od okamžiku, kdy se adresát mohl s jeho obsahem seznámit,[32] bez ohledu na to, zda tak

[28] Vztahuje se k tzv. počítačovým datům, viz Šámal, P. a kol. Trestní zákoník: komentář. 2. vyd. C.H. Beck: Praha, 2012, str. 1809.

[29] Srov. rozhodnutí Nejvyššího soudu ČR 8 Tdo 407/2011 a 11 Tdo 349/2009.

[30] Např. zprávy na sociálních sítích, jakékoliv uložené soubory – fotografie či obrázky, videa, dokumenty atp.

[31] Může jít např. o záznam zachycený pomocí webové kamery v počítači , viz Šámal, P. a kol. Trestní zákoník: komentář. 2. vyd. C.H. Beck: Praha, 2012, str. 1823.

[32] K tomu srov. výše uvedené ohledně vstupu do e-mailové schránky a možnosti seznámit se s obsahem e-mailu.

skutečně učiní či nikoliv.

Aby byl výčet nejčastěji relevantních skutkových podstat úplný, je třeba přidat ještě skutkovou podstatu trestného činu poškození a ohrožení provozu obecně prospěšného zařízení dle § 276 odst. 1 a příp. i 2 písm. b) TZ (skutková podstata trestného činu poškození a ohrožení provozu obecně prospěšného zařízení z nedbalosti dle § 277 odst. 1 TZ zde nepřipadá s ohledem na subjektivní stránku v úvahu). Dle výkladového ustanovení uvedeného v § 132 TZ je obecně prospěšným zařízením mimo jiné i zařízení a sítě elektronických komunikací, kdy proto takovým zařízením bude typicky např. server, ať už půjde o server firemní či využívaný širokou veřejností v rámci zapojení do sítě Internet. V úvahu proto připadá tato skutková podstata zejména v případě tzv. DoS nebo DDoS útoků.[33]

Zde uvedené skutkové podstaty jsou ty, jež reagují na oblast kyberkriminality přímo konkrétními ustanoveními. Z hlediska trestněprávní kvalifikace kriminality spojené s kyberprostorem však přichází ke slovu samozřejmě i řada dalších skutkových podstat, typicky např. skutková podstata trestného činu podvodu dle § 209 TZ[34] nebo porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 270 TZ.[35] V obou uvedených případech může být pachatelem i právnická osoba, viz § 7 ZTOPO.

De lege ferenda

Pro doplnění je ovšem třeba uvést relevantní plánované změny trestního zákoníku de lege ferenda. Jedná se o návrh předložený vládou sněmovně k projednání dne 3. prosince 2013 jako sněmovní tisk č. 45.[36] Návrh počítá s úpravou skutkové podstaty trestného činu šíření pornografie dle § 191 TZ přidáním nové základní skutkové podstaty spočívající v použití informační nebo komunikační technologie v úmyslu získat přístup k dětské pornografii,

[33] K tomu viz dále.

[34] Příkladem mohou být podvodná jednání v souvislosti s aukčními servery, kdy např. poškozený po uhrazení požadované částky obdrží namísto slíbeného mobilního telefonu balíček karet.

[35] Např. rozšiřováním softwaru bez příslušné opravňující licence. Zásah do práva autorského ovšem musí být nikoli nepatrný, přičemž v úvahu je třeba vzít především „intenzitu takového zásahu, způsob provedení činu, jeho následky, ..., v případě déletrvajících a opakovaných zásahů i počet takových případů, délku doby narušování konkrétního chráněného práva apod.“ Viz Šámal, P. a kol. Trestní zákoník: komentář. 2. vyd. C.H. Beck: Praha, 2012, str. 2753.

[36] Návrh je v současnosti projednáván v rámci Ústavněprávního výboru

přičemž informačními nebo komunikačními technologiemi jsou veškeré informační technologie umožňující komunikaci a práci s počítačem. Jedná se o informační technologie hardwarového i softwarového typu, nejčastěji jde proto v praxi o osobní i stolní počítač, mobilní telefon, internet a internetový prohlížeč.[37] Objektem této nové základní skutkové podstaty trestného činu výroby a jiného nakládání s dětskou pornografií podle § 192 odst. 2 TZ je ochrana dítěte před sexuálním vykořisťováním a omezení nebo alespoň zabránění šíření dětské pornografie prostřednictvím informačních nebo komunikačních technologii.[38] Objektivní stránku naplní, kdo použije informační nebo komunikační technologii v úmyslu získat přístup k dětské pornografii, tedy bez ohledu na to, zda přístup k dětské pornografii skutečně získá či nikoli. Pachatelem může byt kdokoli, musí vsak jednat úmyslné a v zákonem požadované pohnutce získat přístup k dětské pornografii, přičemž zavinění ve vztahu k dětské pornografii musí být ve formě úmyslu přímého.[39]

Dále výše uvedený návrh zavádí dvě zcela nové skutkové podstaty, a to účast na pornografickém představení jako § 193a TZ a navazování nedovolených kontaktů s dítětem jako § 193b TZ.[40] Skutková podstata trestného činu účasti na pornografickém představení jako § 193a TZ dopadá na účast na pornografickém představení nebo jiném vystoupení, ve kterém účinkuje dítě, přičemž účastnit se takového představení lze i prostřednictvím informačních a komunikačních technologií. Objektem této skutkové podstaty je ochrana dítěte před pohlavním zneužíváním a pohlavním vykořisťováním a omezení nebo alespoň zabránění šíření dětské pornografie prostřednictvím informačních nebo komunikačních technologií. Pachatelem může být kdokoli, zavinění musí být úmyslné. Pachatelem trestného činu dle § 193a TZ by měla moci být i právnická osoba, viz článek III části třetí navrhovaného zákona a důvodovou zprávu k němu.

Nově navrhovanou skutkovou podstatu trestného činu navazování nedovolených kontaktů s dítětem dle § 193b TZ[41] pak naplní, kdo prostřednictvím informačních nebo komunikačních technologii navrhne setkání dítěti mladšímu patnácti let v úmyslu spáchat trestný čin podle §

[37] Viz bod 4. článku I části první navrhovaného zákona a důvodovou zprávu k němu.

[38] S ohledem na potenciální masový dosah co do počtu příjemců, rychlosti a snadnosti šíření informaci v kyberprostoru, vzhledem k jeho časovým, prostorovým a uživatelským specifikům.

[39] Nepřímý úmysl (srozumění) zahrnuje určitý prvek lhostejnosti, ovsem lhostejnost principiálně vylučuje pohnutku, která již vyjadřuje určitý pozitivní vztah k dané okolnosti, viz § 15 odst. 1 písm. a) a b) TZ.

[40] Viz bod 6. článku I části první navrhovaného zákona a důvodovou zprávu k němu.

[41] Viz bod 6. článku I části první navrhovaného zákona a důvodovou zprávu k němu.

187 odst. 1, § 192, § 193, § 202 nebo jiný sexuálně motivovaný trestný čin (takovým jiným sexuálně motivovaným trestným činem může být např. právě nově kriminalizovaná účast na pornografickém představení podle § 193a TZ). Objektem této skutkové podstaty je ochrana dětí mladších patnácti let před sexuálním vykořisťováním, ke kterému je návrh setkání prostředkem, přičemž použití informačních a komunikačních technologii za tím účelem typově zvyšuje společenskou škodlivost takového jednání. Objektivní stránku pachatel naplní, vyvine-li aktivní komunikační činnost směrem k dítěti prostřednictvím informačních nebo komunikačních technologii ve snaze vzbudit v něm rozhodnuti zúčastnit se vzájemné osobni schůzky, a to v úmyslu spáchat některý z vyjmenovaných trestných činů či jiný sexuálně motivovaný trestný čin. Pachatelem trestného činu navazování nedovolených kontaktů s dítětem může být kdokoli, musí však jednat v úmyslu přímém a v zákonem požadované pohnutce spáchat některý z vyjmenovaných trestných činů nebo jiný sexuálně motivovaný trestný čin.[42] Pachatelem trestného činu dle § 193b TZ by měla moci být i právnická osoba, viz článek III části třetí navrhovaného zákona a důvodovou zprávu k němu.

Útoky v prostředí kyberprostoru

Oblast kybernetické kriminality zahrnuje pestrou škálu společensky škodlivých jednání, pro jejichž bližší vymezení zde již není prostor. Přesto však nelze pojmout kyberkriminalitu jako takovou bez poznání alespoň některých nejčastějších jednání.

Kyberkriminalitu lze rozdělit do několika podskupin v návaznosti na Úmluvu o kyberkriminalitě[43] (dále jen „Úmluva“) a její Dodatkový protokol[44] (dále jen „Protokol“). Do první skupiny spadají trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů.[45] Lze sem zařadit většinu jednání známého pod názvem sociální inženýrství.

[42] Znak pohnutky musí být obligatorně naplněn, přičemž se musí jednat o úmysl přímý. K tomu viz výše poznámka číslo 39.

[43] ETS No.: 185, Convention on Cybercrime. Lze se setkat též s názvem Úmluva o počítačové kriminalitě, viz např. Gřivna, T., Polčák, R. Kyberkriminalita a právo. Praha: Auditorium, 2008. Úmluva vznikla v roce 2001 a vstoupila v účinnost 1. 7. 2004. Česká republika ji podepsala 9. února 2005 a ratifikovala 22. srpna 2013.

[44] ETS No.: 189, Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. Česká republika ji podepsala 17. května 2013, dosud však neratifikovala.

[45] Úmluva uvádí též definice některých pojmů jako „počítačový systém“, „počítačová data“ aj.

Zahrnuje např. tzv. nigerijské dopisy, phising, pharming, malware,[46] útoky mířené na DNS,[47] hacking,[48] útoky spojené s elektronickým bankovnictvím,[49] DoS či DDoS.[50] Do této skupiny lze zařadit též tzv. APT útoky (Advanced Persistent Threat) spočívající v sofistikovaném dlouhodobě plánovaném promyšleném útoku např. na server velké společnosti, vládní instituce atp. za využití sociálního inženýrství i technologických znalostí. APT útok mnohdy cílí na síť jako takovou, a tudíž na obecně prospěšné zařízení.[51]

Útoky výše uvedené jsou mnohdy páchány prostřednictvím organizované skupiny, případně organizované zločinecké skupiny.[52]

Do druhé skupiny trestných činů dle řazení Úmluvy patří trestné činy související s počítači, a to falšování údajů a podvod související s počítači. Třetí skupina zahrnuje trestné činy související s obsahem, který se týká dětské pornografie.[53] Ve čtvrté skupině jsou pak

---

[46] Škodlivý software v mnoha různých podobách. Může se jednat o tzv. trojského koně (uživatel např. z internetu stahuje určitý obsah, aniž by si byl vědom, že jeho součástí je skrytý malware) nebo jiné formy (červ ad.). Malware má obvykle omezit či zcela vyřadit funkčnost napadeného zařízení, získat z napadeného zařízení data nebo si ho podřídit.

[47] DNS (Domain Name System) je zjednodušeně řečeno překladač složité IP adresy do podoby např. www.seznam.cz. Útok vedený na DNS např. přesměruje dožadující zařízení bez vědomí uživatele na jinou cílovou adresu.

[48] Včetně tzv. hacktivismu, tj. ideologicky orientovaného hackerského útoku jako určitá forma kyberterorismu.

[49] Zejm. ve spojení se sociálním inženýrstvím a nigerijskými dopisy – útočník např. zašle na vybrané adresy e-mail vizuálně odpovídající oficiálnímu e-mailu bankovní nebo jiné instituce, v němž vyzývá adresáta k potvrzení přihlašovacích údajů na odkazované stránce (zpravidla s odkazem na snahu o větší zabezpečení).

[50] DoS (Denial of Service) i DDoS (Distributed Denial of Service) míří na zneprovoznění konkrétního serveru. Útočníci obvykle vytvoří nejprve tzv. botnet, tj. síť podřízených počítačů (např. jejich předchozím zasažením příslušným malwarem), jejichž prostřednictvím následně požaduje po cíleném serveru určitou činnost. V závislosti na množství takových požadavků pak může dojít k zahlcení daného serveru a jeho znepřístupnění. V případě DoS a DDoS útoků může trestněprávní kvalifikace jednání poměrně variovat především podle toho, zda je takový „úspěšný“ útok proveden prostřednictvím podřízených počítačů bez vědomí jejich uživatelů (a tudíž zpravidla po předchozím neoprávněném přístupu k počítačovému systému a neoprávněném vložení dat do něj) a zda cílený server skutečně zasáhl nebo zůstal takříkajíc přede dveřmi, tj. na úrovni firewallu – ten není obecně prospěšným zařízením (srov. § 132 TZ), avšak zahlcení firewallu může vést k ohrožení využívání serveru jakožto obecně prospěšného zařízení, neboť v jeho důsledku je znemožněn přístup k serveru ostatním uživatelům.

[51] K tomu blíže viz výše.

[52] Viz § 129 TZ.

[53] Včetně diskutované problematiky virtuální dětské pornografie.

zařazeny trestné činy související s porušením autorského práva a práv příbuzných autorskému právu.

Dodatkový protokol k Úmluvě pak hovoří o trestných činech ve spojení s rasistickým a xenofobním obsahem.

Pro úplnost výčtu je třeba ještě alespoň zmínit jednání známá jako kyberšikana, kyberstalking a kybergrooming. Kybergrooming představuje typizované jednání spočívající v manipulaci oběti prostřednictvím informačních a komunikačních technologií s cílem sexuálně ji využít, ať už v rámci kyberprostoru (např. sváděním oběti k výrobě dětské pornografie a jejímu odeslání útočníkovi) nebo v reálném světě (sexuální zneužití po vylákání na osobní schůzku). Lze rozlišit dvě hlavní formy kybergroomingu, kdy v prvním případě útočník manipuluje s obětí dlouhodobě, oběť se na něm stává emocionálně závislou. V druhém případě kybergroomer zneužívá oběti především k výrobě dětské (aj.) pornografie a nezřídka i k dětské prostituci (mnohdy však nikoliv proti jejich vůli).

Závěr

Předložený text usiluje o nastínění z hmotněprávního pohledu základních specifických ustanovení trestního zákoníku určených k postihu kyberkriminality jako takové a kriminality s určitým prvkem kyberprostoru, včetně návrhu de lege ferenda. Věnuje se proto podrobněji skutkovým podstatám tzv. počítačových trestných činů uvedených v § 230-23 TZ. Dále pak uvádí další relevantní skutkové podstaty trestných činů, vymezené v rámci § 180, 182, 183, 184, 191, 192, 276, 287, 302, 311, 345, 352, 355, 356, 358, 365, 403-405, 407 TZ, příkladmo též v rámci § 209 a 270 TZ a de lege ferenda v rámci § 192, 193a a 193b TZ.

Pro lepší představu o pestrosti společensky škodlivých jednání v oblasti kyberprostoru je text zakončen přehledem nejčastějších projevů kyberkriminality v návaznosti na jejich členění dle Úmluvy o kyberkriminalitě a jejího Dodatkového protokolu. Zařazeny jsou tak útoky proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů, trestné činy související s počítači, trestné činy související s obsahem a trestné činy související s porušením autorského práva a práv příbuzných autorskému právu.

Kyberkriminalita je vzhledem k zasahování kyberprostoru do mnoha oblastí každodenního života a neustálému vývoji moderních informačních a komunikačních technologií aktuální

problematikou, která zajisté zasluhuje pozornost věnovanou jak legislativnímu rámci, tak ale i vlastním projevům – tímto směrem by se proto měly ubírat další úvahy navazující na tuto práci.

Bibliografie

Aktuálně.cz, Sociální sítě. dostupné na http://www.aktualne.cz/wiki/veda-a-technika/socialni-site/r~i:wiki:1456/ (10.4.2014)

ETS No.: 185, Convention on Cybercrime

ETS No.: 189, Additional Protocol to the Convention on Cybercrime

Gřivna, T., Polčák, R. Kyberkriminalita a právo. Praha: Auditorium, 2008

Novotný, O., Vokoun, R., Šámal, P. a kol. Trestní právo hmotné. 6. vyd. Wolters Kluwer ČR, a.s.: Praha, 2010

Rozhodnutí Nejvyššího soudu ČR 8 Tdo 407/2011

Rozhodnutí Nejvyššího soudu ČR 8 Tdo 11 Tdo 349/2009

Sněmovní tisk 45/0. Návrh zákona, kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, zákon č. 141/1961Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, a zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, včetně důvodové zprávy. Dostupné na http://www.psp.cz/sqw/text/tiskt.sqw?O=7&CT=45&CT1=0 (13. dubna 2014)

Šámal, P. a kol. Trestní zákoník: komentář. 2. vyd. C.H. Beck: Praha, 2012

Wikipedie, Firewall. Dostupné na http://cs.wikipedia.org/wiki/Firewall (10. dubna 2014)

Wikipedie, Antivirový program. Dostupné na http://cs.wikipedia.org/wiki/Antivir (11. dubna 2014)

Wikipedie, Spyware. Dostupné na http://cs.wikipedia.org/wiki/Spyware (11. dubna 2014)