UNIVERZITA KARLOVA

Právnická fakulta

Pavla Stanková

Kriminalizace útoků na informační systémy

Diplomová práce

Vedoucí diplomové práce: JUDr. Dalibor Šelleng, Ph.D.

Katedra trestního práva

Datum vypracování práce (uzavření rukopisu): 31. října 2022

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

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 185 639 znaků včetně mezer.

V Praze dne …… ……..

Pavla Stanková

PODĚKOVÁNÍ

Děkuji touto cestou JUDr. Daliboru Šellengovi, Ph.D., za vedení mé diplomové práce, za cenné připomínky a rady, především pak za veškerý čas a trpělivost.

OBSAH

SEZNAM GRAFŮ

SEZNAM SCHÉMAT

SEZNAM TABULEK

ÚVOD

Informační a komunikační technologie se v posledním desetiletí staly nedílnou a velmi podstatnou součástí života každého z nás. Nalézt oblast lidské činnosti, která by nebyla spojena s jejich využíváním, je v současné době velmi nesnadný, ne-li nemožný úkol. Třebaže moderní technologie nezměrně ulehčily naše každodenní fungování, otevřely taktéž bránu zcela nových příležitostí pro páchání trestné činnosti. Škála kybernetických útoků je velmi rozsáhlá, a navíc se velmi pružně dokáže přizpůsobovat aktuálním situacím, což pro zákonodárce a orgány činné v trestním řízení představuje nepochybně nelehkou výzvu. Vzhledem k tomu, že nejenom jednotlivci, ale také státy, jsou na technologiích závislé, mohou kybernetické útoky mimo jiné představovat závažnou národní bezpečnostní hrozbu.

Kybernetická kriminalita představuje jednu z nejdynamičtěji se rozvíjejících oblastí trestné činnosti. Neustálá expanze kyberprostoru skýtá pachatelům, ať už více či méně technicky zdatným, příhodné prostředí pro páchání nelegálních aktivit, neboť značnou výhodu pro pachatele představuje vysoká míra anonymity, následně jejich ztížená identifikace a taktéž jednoduchý postup směřující k opatření si nástrojů ke spáchání útoků. Opatření takových nástrojů není v dnešní době složité, natož ani finančně náročné. Vše zmíněné navíc podporuje i opožděně reagující legislativa. Pachatelům svědčí i fakt, že kybernetické útoky jsou společensky mnohdy více tolerovány než běžná trestná činnost a často též záměrně přehlíženy.

Cílem diplomové práce je představit škálu kybernetických útoků, se kterými se v kyberprostoru lze setkat, a trestněprávně je klasifikovat. Vzhledem k tomu, že jde o problematiku přesahující geografické hranice státu, je nejdříve představen nadnárodní a mezinárodní rámec v oblasti boje proti kybernetické kriminalitě. Pozornost je dále koncentrována na otázky procesněprávního charakteru, zejména na to, jak je kybernetická trestná činnost odhalována, vyšetřována, jak je postupováno v rámci mezinárodní spolupráce a s jakými problémy se orgány činné v trestním řízení (a nejenom ony) v praxi potýkají. Snahou je taktéž zjistit, na jaké nedostatky v oblasti kyberzločinu naráží tuzemská právní úprava, eventuálně představit možné návrhy de lege ferenda. V neposlední řadě je cílem vyhodnotit dostupné statistické údaje týkající se kybernetické trestné činnosti a určit její možný budoucí vývoj. Závěrem jsou shrnuta zjištění o tom, jaké úskalí pro trestní právo přinesly aktuálně se vyskytující trendy v oblasti kyberprostoru. Mezi výzkumné metody, které byly v rámci diplomové práce využity, patří zejména deskripce, analyticko-syntetický postup, dedukce a komparace.

Se zřetelem k okolnosti, že se jedná o téma přesahující hranice českého právního řádu, bylo při zpracovávání práce čerpáno ze zahraničních zdrojů, zejména cizojazyčné knižní a časopisecké literatury, zahraniční judikaturu nevyjímaje. Opomenuty nejsou ani české prameny, jako jsou především zákony, důvodové zprávy, soudní judikatura, literatura knižní a časopisecká apod. Práce vychází z poznatků kriminologie, psychologie a informatiky, neboť se jedná o problematiku pokrývající nejenom oblast trestního práva, ale i další vědní obory.

1. VYMEZENÍ ZÁKLADNÍCH POJMŮ

Kybernetická kriminalita představuje relativně novou výseč trestné činnosti, jejíž počátky nalézáme v 70. letech minulého století, kdy začíná docházet k prudkým změnám v oblasti výpočetních a komunikačních technologií. Ačkoliv je v současné době pojem kybernetická kriminalita nadmíru užívaný, nepanují prozatím shody ohledně jeho jednotné terminologie. Vyjma pojmu kybernetické kriminality se nezřídka lze setkat i s pojmem kriminality počítačové, se kterým mimo jiné pracují například i tuzemské učebnice kriminalistiky.[1] Takové terminologické vymezení není dle mého názoru zcela vhodné, neboť evokuje, že jde o trestnou činnost páchanou výlučně počítačem, případně činnost, ve které nějakým způsobem počítač figuruje. Moderní doba nicméně umožňuje páchat nelegální aktivity nejen za pomocí počítačů, a tudíž se pojem jeví jako překonaný a lehce zastaralý. Obdobně lze narazit na termín high-tech kriminalita, který opět není zcela výstižný, neboť zahrnuje pouze nepokročilejší aktuálně dostupné technologie, jako jsou například nanotechnologie či bioinženýrství. Jako univerzální a nejvýstižnější se jeví právě pojem kybernetická kriminalita, kyberkriminalita či kybernetická trestná činnost.[2] Přes rozličné rozdíly v terminologii však obecně existuje soulad ohledně toho, co pod pojem kybernetické kriminality subsumujeme. Jednu z přiléhavých definic kybernetické kriminality podává Jirovský, který ji definuje jako kriminalitu *„namířenou proti počítačům, jejich hardwaru, softwaru, datům, sítím apod., nebo v ní vystupuje počítač pouze jako nástroj pro páchání trestného činu, případně počítačová síť a k ní připojená zařízení jsou prostředím, v němž se taková činnost odehrává“*.[3]

Kyberkriminalita se nejčastěji projevuje prostřednictvím kybernetických útoků (taktéž kyberútoků). Třebaže absentuje jednotná definice, chápeme je jako útoky páchané prostřednictvím kyberprostoru za účelem narušení informačního systému a také s cílem manipulovat s uloženými daty a zneužít je. Narušení může být činěno buď cíleně ve vztahu k určitému subjektu, tedy adresně, nebo naopak neadresně.

Veškerá trestná činnost se odehrává v kyberprostoru, jehož legální zakotvení nalezneme v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti. Paragraf druhý chápe kybernetický prostor jako digitální prostředí, které umožňuje vznik, zpracování a výměnu informací. Tvoří jej informační

[1] Srov. KONRÁD, Zdeněk, Viktor PORADA, Jiří STRAUS a Jaroslav SUCHÁNEK. *Kriminalistika: Kriminalistická taktika a metodiky vyšetřování*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, s. 334. ISBN 978-80-7380-547-0.

[2] CLOUGH, Jonathan. *Principles of Cybercrime*. Cambridge, UK; New York: Cambridge University Press, 2010, s. 9–11. ISBN 978-0-521-89925-3.

[3] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, s. 19. ISBN 978-80-247-1561-2.

systémy, služby a sítě elektronické komunikace. Jinak řečeno jde o virtuální nehmotný prostor, ve kterém dochází k výměně informací. Historicky poprvé byl termín kyberprostor užit již začátkem osmdesátých let americkým spisovatelem Williamem Gibsonem, jenž jej chápal dosti odlišně, a to jako lidmi stejně vnímanou halucinaci, se kterou se setkávají každý den.[4]

Kyberprostor se od běžného světa liší v několika aspektech. Tím hlavním z nich je značná anonymita a absentující regulace, která páchání trestné činnosti podstatně ulehčuje, ba dokonce umožňuje. Pachatelé mohou v kyberprostoru snadno skrývat svou identitu, a sice pomocí falešných identit či účtů, které nevyžadují po uživateli žádné ověření totožnosti. Možnou autentizací v kyberprostoru pak zbývá sledování IP adresy, která je přiřazena všem technickým zařízením připojitelných k síti. Zdatnější uživatelé mohou nicméně svou pravou IP adresu maskovat, a to za pomocí VPN sítě[5], proxy serverů[6] či jiných obdobných prostředků. V takových případech je k jejich odhalení nutná součinnost poskytovatele internetového připojení (ISP), třebaže ani tak se nemusí vždy danou IP adresu podařit vysledovat. Obdobně lze specifický aspekt spatřovat v tom, že kyberprostor není nijak omezen geografickými hranicemi a většinu kybernetických útoků charakterizuje přeshraniční prvek.

[4] GIBSON, William. *Neuromancer*. 20th anniversary ed. New York: Ace Books, 2004, s. 69. ISBN 978-0-441-01203-9.

[5] VPN síť (Virtual Private Network) je nástroj, který umožňuje skrýt uživatelovu IP adresu v prostředí internetu bez ohledu na to, kde se uživatel fyzicky nachází. Po připojení k VPN síti zůstane viditelná pouze adresa VPN serveru, nikoliv IP adresa. Vzhledem k anonymitě a šifrování přenášených dat našly VPN sítě využití i v oblasti kriminálních aktivit, a to především jako prostředek sloužící k připojení na tzv. dark web.

[6] Proxy server funguje obdobně jako VPN síť, neboť umožňuje skrýt lokaci, ze které se uživatel k internetu připojuje. Rozdíl spočívá v tom, že zde nedochází k šifrování připojení, a tedy úroveň anonymity není na takové úrovni jako u VPN sítě.

2. MEZINÁRODNĚPRÁVNÍ RÁMEC V BOJI PROTI KYBERNETICKÉ KRIMINALITĚ

Kybernetické hrozby mohou pocházet de facto z kteréhokoliv místa na světě, a proto není účelné koncentrovat pozornost pouze na národní bezpečnost. S ohledem na globální charakter kyberprostoru je zapotřebí spolupracovat nejenom na nadnárodní, ale také na mezinárodní úrovni. Za tímto účelem byla zformována řada různých organizací a center působících při Evropské unii, NATO a OSN.

2.1. Evropská unie

Primární právo Evropské unie žádné zmínky o kyberbezpečnosti neobsahuje, což je poměrně pochopitelné vzhledem k tomu, že v době, kdy se Evropská unie formovala, nebyl kyberzločin nikterak aktuálním tématem. S rozvojem moderních technologií a přesunem trestné činnosti do virtuálního světa se však situace nicméně změnila a v současné době představuje boj s kyberkriminalitou pro Evropskou unii jednu z hlavních priorit.[7] Tomu svědčí i fakt, že se Unie v rámci programu „Digitální Evropa" zavázala v letech 2021 až 2027 poskytnout necelé dvě miliardy eur do oblastí, jako je kybernetická bezpečnost nebo umělá inteligence.[8] Klíčová právní úprava postihující kyberzločin je obsažena v právu sekundárním, zejména ve směrnicích. Signifikantní roli zde zaujímá směrnice Evropského parlamentu a Rady 2013/40/EU o útocích na informační systémy, směrnice Evropského parlamentu a Rady 2011/93/EU o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii a směrnice Evropského parlamentu a Rady 2019/713 o potírání podvodů v oblasti bezhotovostních platebních prostředků a jejich padělání. Evropská unie, vědoma si toho, že kyberkriminalita se neomezuje pouze na vymezené území nýbrž postihuje celý svět globálně, začala sjednávat i v rámci své vnější politiky dohody s mimoevropskými zeměmi ohledně usnadnění přístupu k elektronickým důkazům, čímž mimo jiné také zdůrazňuje význam kybernetické diplomacie.

Lze říci, že v průběhu let Unie publikovala řadu rozličných právních předpisů a strategických dokumentů, ale také došlo k vytvoření poměrně širokého spektra institucí zabývajících se

[7] Boj s kyberkriminalitou byl vzhledem ke své důležitosti zařazen i do metodiky nazvané „The EU Policy Cycle to tackle Organised and Serious International Crime". Metodika byla vytvořena Evropskou unií účelem vymezení nejzávažnějších kriminálních hrozeb, které se v Unii objevují. Vyjma spolupráce mezi členskými státy je jedním z cílů také aplikace jednotných evropských opatření.

[8] EUROPEAN COMMISSION. *Shaping Europe's digital future – The Digital Europe Programme* [online]. [cit. 2022-06-01]. Dostupné z: https://digital-strategy.ec.europa.eu/en/activities/digital-programme

problematikou kybernetické kriminality. Někteří autoři tak z těchto důvodů vnímají přístup Unie ke kyberzločinu spíše jako roztříštěný, neboť obecný právní rámec se hledá poněkud složitě.[9]

2.1.1. Agentura Evropské unie pro kybernetickou bezpečnost (ENISA)

Hlavní prioritou agentury je dosáhnout společné vysoké úrovně kybernetické bezpečnosti po celé Evropě, čehož se snaží docílit pomocí vzájemné kooperace členských států, zvyšováním důvěry v digitální bezpečnost a sdílením získaných znalostí a postupů. Kromě jiného systemizuje certifikace kybernetické bezpečnosti.[10] Ačkoliv byla založena již v roce 2004, její význam v poslední době zejména kvůli pandemii COVID-19 vzrostl. V souvislosti s pandemií publikuje ENISA jednotné bezpečnostní rady, které členským státům napomáhají zajistit kybernetickou bezpečnost.[11]

2.1.2. Evropské centrum pro boj proti kyberkriminalitě (EC3)

EC3 bylo založeno v rámci Europolu v roce 2013 v souvislosti s bojem proti kyberkriminalitě. Pozornost zaměřuje zejména na kybernetické útoky páchané organizovanými zločineckými skupinami, dále na trestné činy směřující vůči dětem a v neposlední řadě na útoky poškozující unijní informační systémy. Mimo jiné poskytuje nonstop technickou podporu pro naléhavé kybernetické incidenty. EC3 v členských státech provádí rovněž i školení a osvětu. Za účelem užší spolupráce mezi EC3 a ostatními subjekty, byly vytvořeny speciální pracovní skupiny jako například EUCTF (European Union Cybercrime Task Force), J-CAT (Joint Cybercrime Action Taskforce) nebo EC3 Programme Board.[12]

EC3 každoročně publikuje zprávu nazvanou IOCTA (Internet Organised Crime Treat Assesment), ve které analyzuje zjištěné hrozby za daný rok, snaží se předpovídat budoucí kybernetické trendy a poskytuje adresátům bezpečnostní doporučení a rady. Velmi okrajově se též zabývá i světovou kybernetickou kriminalitou.

---

[9] Srov. CHRISTOU, George. *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*. London: Palgrave Macmillan UK, 2016, s. 102. ISBN 978-1-137-40052-9.

[10] Kybernetická certifikace osvědčuje, že dané služby a produkty splňují potřebná bezpečnostní minima. Tuzemský akreditační orgán je NÚKIB.

[11] ENISA. About ENISA – The European Union Agency for Cybersecurity. *ENISA* [online]. [cit. 2022-05-31]. Dostupné z: https://www.enisa.europa.eu/about-enisa

[12] EUROPOL. European Cybercrime Centre – EC3. In: *Europol* [online]. 1. března 2022 [cit. 2022-05-31]. Dostupné z: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

2.2. Rada Evropy

2.2.1. Úmluva Rady Evropy o počítačové kriminalitě

Prvním mnohostranným instrumentem v boji proti kyberkriminalitě se po více než 16 letech přípravných prací stala Úmluva o počítačové kriminalitě, přezdívaná Budapešťská úmluva. Primárním cílem Úmluvy bylo eliminovat, případně odstranit počet tzv. bezpečných útočišť, která chápeme jako země, ve kterých jsou určité trestné činy beztrestné a zasahují do jurisdikce státu jiného.[13]

Úmluva je rozdělena do tří částí, které upravují oblasti jak hmotného a procesního práva, tak mezinárodní spolupráce. Vyjma některých základních otázek trestní odpovědnosti, trestů a opatřeních, rozlišuje hmotněprávní část Úmluvy trestné činy[14] do čtyř následujících skupin:

1. trestné činy proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů;
2. trestné činy související s počítačem;
3. trestné činy související s obsahem;
4. trestné činy týkající se porušení autorského práva a práv souvisejících s právem autorským.

Kromě hmotněprávních ustanovení obsahuje Úmluva i procesněprávní instituty, konkrétně se zaměřuje na uchovávání a zajištění uložených počítačových dat. Dále řeší otázky shromažďování a odposlechu provozních dat. V neposlední řadě Úmluva upozornila na nutnost mezinárodní spolupráce v souvislosti s rozvojem informačních technologií. Pozornost je tak koncentrována na zásady týkající se mezinárodní spolupráce, konkrétně pak na zásady uplatňující se při vydávání osob a zásady vzájemné spolupráce. Úmluva pragmaticky zakotvila i postup u vzájemné pomoci v případě neexistence mezinárodní smlouvy.

Z důvodných obav o nemožnosti postihnout rasistické a xenofobní projevy skrze počítačové systémy vypracovala Rada Evropy dodatkový protokol, aby danou mezeru zaplnila.[15] Dodatkový

[13] CLOUGH, Jonathan. A world of difference: the Budapest Convention on Cybercrime and the challenges of harmonisation. *Monash University Law Review*. 2014, roč. 40, č. 3, s. 701. ISSN 0311-3140. Dostupné z: doi:10.3316/agis_archive.20152955

[14] Všechny trestné činy, které Budapešťská úmluva rozeznává jsou z hlediska zavinění trestnými činy úmyslnými, a sice není možné je spáchat nedbalostně.

[15] ALKIVIADOU, Natalie. The Legal Regulation of Hate Speech: The International and European Frameworks. *Politička misao*. Zagreb: Sveuciliste u Zagrebu, Fakultet Politckih Znanosti, 2018, 55(4), s. 220. ISSN 0032-3241. Dostupné z: doi:10.20901/pm.55.4.08

protokol Rady Evropy č. 189 o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů rozšířil oblast trestných činů o tyto:

1. šíření rasistického a xenofobního materiálu skrze počítačový systém;
2. rasisticky a xenofobně motivované výhružky;
3. rasisticky a xenofobně motivované urážky;
4. popírání, hrubé zlehčování, schvalování nebo ospravedlňování genocidy nebo zločinů proti lidskosti.

Přestože ustanovení Úmluvy vznikala několik desítek let nazpět, což se vzhledem k rozvoji informačních prostředí nemusí jevit již jako zcela aktuální, stále lze Úmluvu vnímat jako zdařilý posun na poli mezinárodního boje s kybernetickými útoky. Úspěšnost mimo jiné dokazuje i počet signatářů. V současně době je Úmluva závazná pro 66 smluvních států a jejich základna se neustále rozšiřuje i z řad mimoevropských zemí.

2.2.2. Výbor k Úmluvě o počítačové kriminalitě (T-CY)

Za účelem zajištění efektivní implementace ustanovení Úmluvy o počítačové kriminalitě byl odpovědným orgánem stanoven Výbor k Úmluvě o počítačové kriminalitě (Cybercrime Convention Committee). Svou činnost realizuje zejména na pravidelných neveřejných plenárních zasedáních, kterých se účastní zástupci smluvních států. Kromě zmíněného se zabývá přípravou legislativních návrhů, poskytuje podporu smluvním státům a také publikuje různá doporučení týkající se výkladu ustanovení Úmluvy.

Většina recentních plenárních zasedání se soustředila zejména na přípravu dalšího dodatkového protokolu k Úmluvě. Druhý dodatkový protokol k Úmluvě o počítačové kriminalitě o posílené spolupráci a zpřístupňování elektronických důkazů má za cíl zefektivnit spolupráci nejenom mezi státy, ale také se soukromým sektorem. Protokol byl 5. dubna 2022 schválen Radou EU.[16]

Činnost T-CY je v rámci spolupráce doprovázena činností kanceláře Rady Evropy nesoucí název Cybercrime Programme Office of the Council of Europe (C-PROC), přičemž cílem je obdobně zajistit implementaci Úmluvy o počítačové kriminalitě. Při své činnosti se C-PROC zaměřuje i na vzdělávání osob podílejících se na trestních řízeních, například poskytuje odborná školení státním zástupcům, soudcům a členům bezpečnostních sborů.

[16] Důvodová zpráva k návrhu Rozhodnutí Rady č. 2021/0383 (NLE), kterým se členské státy zmocňují, aby v zájmu Evropské unie ratifikovaly druhý dodatkový protokol k Úmluvě o počítačové kriminalitě o posílené spolupráci a zpřístupňování elektronických důkazů.

2.2.3. Konference Octopus

Vyjma legislativní činnosti pořádá Rada Evropy také každých dvanáct až osmnáct měsíců odborné konference zvané Octopus, které reprezentují jednu z největších platforem pro celosvětové přední experty na kybernetickou trestnou činnost. Témata prezentována na konferencích se snaží pružně reagovat na nejaktuálnější problémy z kybernetického světa. Poslední konference, konaná v roce 2021, nesla téma „spolupráce proti kyberkriminalitě“.[17] Obsahově byla řešena zejména problematika vlivu pandemie COVID-19 na útoky v kyberprostoru. Bylo upozorňováno na narůstající případy zneužívání dětí na internetu a kybergroomingu. Zajímavé podněty se objevily mimo jiné i v souvislosti s pomocí obětem kyberkriminality, kupříkladu bylo navrhováno provádět pravidelné viktimizační průzkumy a zaměřit se více na posílení restorativní justice. Jedním z navrhovaných řešení v boji s kyberzločinem bylo navrhováno oznamování trestné činnosti online prostřednictvím internetu.[18]

2.3. OSN

Snahy o harmonizaci práva v oblasti kybernetické kriminality se objevily i na půdě jedné z největších mezinárodních organizací – OSN. Pověřeným orgánem zabývajícím se kyberkriminalitou se stal UNODC (United Nations Office on Drugs and Crime). V rámci činnosti UNODC bylo vytvořeno speciální úložiště tzv. Cybercrime Repository, které má zemím usnadnit stíhat kyberzločin. Úložiště sestává z hmotněprávních i procesněprávních předpisů téměř všech členských zemích, dále judikatury související s elektronickými důkazy a v neposlední řadě obsahuje možné postupy a strategie na řešení kybernetických incidentů.[19]

Významným přínosem na poli s bojem proti kyberkriminalitě bylo schválení rezoluce OSN č. 74/247 ze dne 27. prosince 2019, kterou byl vytvořen ad hoc výbor odborníků, a to za účelem vypracování nové komplexní mezinárodní úmluvy o boji proti využívání informačních a komunikačních technologií pro účely trestné činnosti. Finální verze by měla být předložena Valnému shromáždění koncem roku 2024. V souvislosti s připravovaným návrhem se objevily otázky, zda by měla smlouva zahrnovat i trestné činy, které primárně nepostihují informační

[17] I podstatou předchozích ročníků konference byla tematika „spolupráce“, nicméně ta současná byla pořádána s dodatkem „spolupracovat, nástroje k dispozici jsou!“.

[18] COUNCIL OF EUROPE. *Octopus 2021: Cooperation against Cybercrime*. Key messages [online]. 18. listopadu 2021 [cit. 2022-06-01]. Dostupné z: https://rm.coe.int/octopus-conference-2021-key-messages-v18nov2021/1680a494e6

[19] UNITED NATIONS OFFICE ON DRUGS AND CRIME. *Cybercrime Repository* [online]. 2020 [cit. 2022-06-03]. Dostupné z: https://www.unodc.org/unodc/en/cybercrime/cybercrime-repository.html

technologie, ale tyto technologie hrají signifikantní roli při páchání nelegálních aktivit. Shoda prozatím nepanuje ani ohledně kriminalizace účastenství kybernetických trestných činů.[20] Jediným jasným faktem je skutečnost, že smlouva bude muset být schopna promptně reagovat na nově narůstající protiprávní aktivity v kyberprostoru.

2.4. NATO

Organizace Severoatlantické smlouvy představuje vojenskou alianci, jejímž cílem je řešení rozličných otázek týkajících se mezinárodní bezpečnosti. Na nárůst kybernetických hrozeb pružně reagovala i politika NATO, která oblast kybernetické obrany přijala jako součást svého kolektivního obranného systému. Aliance několikrát zdůraznila, že rozsáhlý kyberútok chápe ve smyslu ozbrojeného útoku, a tedy bude jej považovat za útok proti všem členům, čímž by mohlo dojít k uplatnění ustanovení o kolektivní obraně (srov. článek 5 Severoatlantické smlouvy).

Jedním z opakovaných cílů NATO je působit v kyberprostoru stejně výkonně jako na zemi, ve vzduchu a na moři. Vzhledem k tomu, že jde o vojenskou alianci, která dosahuje svých cílů především vojenskými prostředky, může být boj s virtuálním zločinem zajímavou výzvou.[21]

Kromě zmíněného působí NATO i v oblasti vzdělávání a prevence. V roce 2019 byla vytvořena NCI Akademie (NATO Communications and Information Academy), která poskytuje kybernetické vzdělávání o komunikačních a informačních systémech.[22] Mimo to pořádá NATO každoročně konference NIAS (NATO Information Assurance Symposium) zaměřené na problematiku kybernetické bezpečnosti.

2.4.1. Speciální centrum NATO pro obranu v kyberprostoru (CCDCOE)

Po několika koordinovaných útocích na estonskou kritickou infrastrukturu v roce 2007 začala mezinárodní společenství zaměřovat pozornost na vážná rizika spojená s možnou kyberválkou mezi státy. Ačkoliv se tehdy jednalo o poměrně jednoduché a neškodné DDoS útoky, daly podnět

[20] RODRIGUES, Katitza a Meri BAGHDASARYAN. UN Committee to begin negotiating new cybercrime treaty amid disagreement among states over its scope. In: *EFF* [online]. 15. února 2022 [cit. 2022-06-03]. Dostupné z: https://www.eff.org/deeplinks/2022/02/un-committee-begin-negotiating-new-cybercrime-treaty-amid-disagreement-among

[21] BRENT, Laura. NATO's role in cyberspace. In: *NATO Review* [online]. 12. února 2019 [cit. 2022-06-02]. Dostupné z: https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html

[22] NATO Communications and Information Agency. *About the NCI Academy* [online]. [cit. 2022-06-02]. Dostupné z: https://www.ncia.nato.int/what-we-do/nci-academy/about-the-nci-academy.html

ke vzniku nového kyberbezpečnostního centra CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence).[23]

Hlavním cílem centra je podporovat spolupráci mezi členskými státy a řešit otázky kybernetické obrany. Též poskytují školení a cvičení v oblastech, jako je právo, technologie a strategie.[24] Ve spolupráci s NATO pořádá CCDCOE každoročně od roku 2010 mezinárodní bezpečnostní cvičení s názvem Locked Shields. Cvičení testuje obranu národní kritické infrastruktury fiktivní země v reálném čase, přičemž útoky odpovídají závažným a sofistikovaným kybernetickým incidentům. Týmy odborníků z různých zemí se pak snaží incident co nejefektivněji vyřešit. Nadto má Locked Shields význam i v oblasti vzájemné mezinárodní spolupráce, neboť umožňuje členům sdílet získané zkušenosti a navazovat kontakty.[25] Mezi další obdobná cvičení patří Cyber Coalition a Crossed Swords. CCDCOE rovněž pořádá mezinárodní konference CyCon zaměřující se na kybernetické incidenty. Tématem pro rok 2022 jsou technologické výzvy a hrozby. V rámci nutnosti sjednotit roztříštěnou úpravu veškerých dokumentů publikovaných mezinárodními a nadnárodními organizacemi vznikla v rámci CCDCOE interaktivní databáze s názvem INCYDER (International Cyber Developments Review).

2.4.2. Tallinnský manuál

Jednou z počínajících aktivit CCDCOE bylo vypracování komplexního právního rámce ve věci aplikovatelnosti mezinárodního práva na případnou kybernetickou válku. Snahou odborníků bylo analyzovat současnou právní úpravu a její možnou aplikaci na nový druh války. Výsledkem bylo vypracování Tallinnského manuálu 1.0. Původní varianta byla později nahrazena zrevidovaným Tallinnským manuálem 2.0[26] tak, aby přiléhavěji reflektovala poznatky mezinárodního práva veřejného. Obsahově se manuál člení na čtyři části: obecnou úpravu mezinárodního práva a kyberprostoru, specializované režimy mezinárodního práva a kyberprostoru, mezinárodní mír a bezpečnost a na právo kybernetického ozbrojeného konfliktu.

[23] KOENDERS, Bert. Foreword. In: SCHMITT, Michael N. *Tallinn manual 2.0 on the International Law Applicable to Cyber Operations*. Second edition. Cambridge: Cambridge University Press, 2017, s. xxv. ISBN 978-1-316-63037-2.

[24] HILL, Steven. NATO and the International Law of Cyber Defence. In: TSAGOURIAS, Nicholas. a Russell. BUCHAN. *Research Handbook on International Law and Cyberspace*. 2. vydání. Northampton: Edward Elgar Publishing Limited, 2021, s. 512. ISBN 978-1-78990-424-6.

[25] CCDCOE. *Locked Shields* [online]. Tallinn: CCDCOE. [cit. 2022-06-02]. Dostupné z: https://ccdcoe.org/exercises/locked-shields/

[26] V roce 2021 byly zahájeny revize směřující k vydání Tallinnského manuálu 3.0.

Ačkoliv Tallinnský manuál představuje jednu z nejkomplexnějších mezinárodních analýz, reakce na jeho publikaci se zřetelně odlišují. Někteří jej vidí jako nezpochybnitelný přínos směřující ke snížení právní nejistoty v kybernetickém prostoru, nicméně obsahuje i několik oblastí, v nichž mezi odborníky panují rozepře a nejasnosti.[27] Podle některých autorů manuál naopak spíše prohlubuje nejistotu spojenou s otázkami ohledně kybernetické války, než aby se ji pokoušel eliminovat.[28] Ani reakce států na sebe nenechala dlouho čekat. Několik států pravidla z manuálu převzala a explicitně vyjádřila ve svých bezpečnostních strategiích.[29]

[27] EFRONY, Dan a Yuval SHANY. A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice. *The American Journal of International Law*. New York, USA: Cambridge University Press, 2018, roč. 112, č. 4, s. 584–585. ISSN 0002-9300. Dostupné z: doi:10.1017/ajil.2018.86

[28] KESSLER, Oliver a Wouter WERNER. Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare. *Leiden journal of international law*. Cambridge, UK: Cambridge University Press, 2013, roč. 26, č. 4, s. 773–774. ISSN 0922-1565. Dostupné z: doi:10.1017/S0922156513000411

[29] EFRONY, Dan a Yuval SHANY. A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice. *The American Journal of International Law*. New York, USA: Cambridge University Press, 2018, roč. 112, č. 4, s. 585. ISSN 0002-9300. Dostupné z: doi:10.1017/ajil.2018.86

3. TYPOLOGIE KYBERÚTOKŮ

Typickými projevy kybernetické kriminality jsou kyberútoky, přičemž existuje nespočetné množství rozdílných způsobů jejich možné klasifikace. V následující kapitole jsou kybernetické útoky rozděleny ve smyslu Úmluvy o počítačové kriminalitě. Předně je nutné předestřít, že výčet útoků není vyčerpávající, ale vzhledem k jejich dynamickému vývoji ani být nemůže. Problematiku typologie neulehčuje ani fakt, že některé útoky jsou mnohdy subsumovatelné do více kategorií. Pro zpřehlednění jednotlivých typů útoků slouží schéma uvedené v Příloze 1 – Schéma kybernetických útoků.

Jak bylo již zmíněno výše, Úmluva klasifikuje trestné činy související s kyberprostředím do těchto čtyř skupin:

1) trestné činy proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů;
2) trestné činy související s počítačem;
3) trestné činy související s obsahem;
4) trestné činy týkající se porušení autorského práva a práv souvisejících s právem autorským.

3.1. Útoky proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů

3.1.1. Hacking

Hacking chápeme jako zastřešující pojem pro všechny útoky subsumované pod „nezákonný přístup“ uvedený v článku 2 Úmluvy o počítačové kriminalitě. V obecné rovině se hacking definuje jako jakýkoliv průnik do cizího počítačového systému a mnohdy tak bývá nesprávně ztotožňován s pojmem cracking. Cracking nicméně představuje obcházení bezpečnostních prvků za účelem zneužití získaných údajů, a tedy jej chápeme pouze jako určitou výseč celé oblasti hackingu. V souvislosti s hackingem bývá často zmiňován pojem hacktivismus, který bývá vnímán jako hackerská činnost motivovaná nejčastěji politickými či ideologickými cíli.

Hacking se může projevovat v různých podobách, jako je prolamování hesel[30] (tzv. password cracking), phishing, malware, sniffing a mnoho dalších, o kterých je pojednáno níže.

[30] Způsobů sloužících k prolomení hesla je nespočet. Například se může jednat o hádání hesla na základě poznatků zjištěných při sociálním inženýrství (případně veřejně dostupných informací uvedených na sociálních sítích), testováním síly hesla a obdobně též zkoušením nejčastěji používaných hesel.

3.1.2. Phishing

Phishing, neboli česky rybaření, chápeme jako jednu z forem sociálního inženýrství, kdy útočník pomocí podvodné taktiky vylákává bezpečnostní údaje od uživatele. Pojem vznikl původně ze slova „fishing“ v tom smyslu, že rybář (zde chápaný útočník) využívá návnadu k lovu (zneužití osobních údajů, získání finančního prospěchu). Změna „f“ v „ph“ je odůvodňována tím, že jedna z původních forem hackerských útoků se zaměřovala na telefonní sítě (angl. Phone phreaking), a proto došlo v hackerské komunitě k nahrazení písmene „f“ za „ph“.[31]

Phishingový útok je realizován tak, že útočník zpravidla rozešle e-mail, který uživatele vyzývá k ověření přihlašovacích a identifikačních údajů. Aby útočník zvýšil úspěšnost svého útoku, vyvolá v uživateli pocit naléhavosti s tím, že mu sděluje, že se u jeho účtu se vyskytly potíže, které má vyřešit přihlášením k účtu. V zaslaném e-mailu je za tímto účelem umístěn přímý odkaz na podvodnou webovou stránku, která typicky napodobuje stránky internetového bankovnictví či přihlašovací okna sociálních sítí. Webové stránky mohou dnes již působit poměrně věrohodně a uživatel často ani nepojme podezření, že se jedná o stránky nedůvěryhodné. Možnost, jak phishing rozpoznat, je zvláštní e-mailová doména či pravopisné a gramatické chyby obsažené v textu. Příznačně útočník rozesílá tisíce podvodných zpráv, doufaje, že techniku neprohlédne alespoň malá část adresátů.[32]

Mnohdy útočníci nevyužívají pouze podvodných e-mailů, nýbrž i telefonických hovorů (Vishing) či SMS zpráv (SMiShing). V případě „hlasového“ phishingu je uživatel kontaktován telefonicky, a to opět za účelem získání přihlašovacích nebo jiných citlivých údajů. Odhalitelnost je ztížena tím, že pachatel začasté využívá funkce VOIP (Voice over Internet Protocol), konkrétně pak techniky caller ID spoofing[33] (falšování ID volajícího). Uživatel má posléze velmi redukované možnosti, jak phishing odhalit. Není neobvyklé, že u vishingu jsou využívány i tzv. audio deepfakes[34]. Naopak SMiShing, cílící na uživatele skrze podvodnou sms zprávu, není z hlediska

[31] KHONJI, Mahmoud, Youssef IRAQI a Andrew JONES. Phishing Detection: A Literature Survey. *IEEE Communications surveys and tutorials*. New York: IEEE, 2013, roč. 15, č. 4, s. 2092. ISSN 1553-877X. Dostupné z: doi:10.1109/SURV.2013.032213.00009

[32] DVOŘÁK, Marek. Phishing, pharming a jejich trestněprávní postih. *Trestněprávní revue*. 2018, č. 4, s. 84–89.

[33] Caller ID spoofing je taktika, při které jsou využity falešné informace o volajícím, za účelem zamaskování skutečného telefonního čísla.

[34] Deepfakes představují velmi sofistikovanou hyperrealistickou techniku, pomocí které jsou umělou inteligencí zaměněny obličeje na fotografiích a videích, případně také hlas na audio záznamech. Cílem je vytvořit klamavý záznam, který je takřka nerozpoznatelný od reality. Původně byla technika využita u pornografických děl, kde byly pomocí deepfakes obličeje pornografických herců „nahrazeny“ tvářemi mediálně známých osobnostní, nevyjímaje osoby z politické sféry. V současné době se taktika nicméně prosadila u mnohých typů útoků a bezesporu lze konstatovat, že bude v budoucnu představovat nezanedbatelný problém.

četnosti tak zásadní.[35] Sofistikovanějším druhem phishingu, je spear fishing, neboť ten se zaměřuje již na konkrétní osobu a celý plán útoku je individuálně přizpůsoben informacím získaným na základě předchozí interakce, která byla součástí procesu sociálního inženýrství.

Aktuálně novou phishingovou technikou, na kterou koncem března 2022 upozornil Národní úřad kybernetické a informační bezpečnosti (NÚKIB), je Browser in the Browser (BitB). Jde o podvodná přihlašovací okna, která se uživatelům otevírají jako součást běžného internetového prohlížeče. Nově otevřené okno pak nabídne možnost přihlásit se do různých účtů a aplikací pomocí uživatelova již existujícího účtu, jako je například Google account, Apple ID, nebo prostřednictvím facebookového účtu.[36]

3.1.3. Sniffing

Sniffing (v překladu čenichat, čmuchat) představuje typ aktivity, při níž útočník nelegálně odposlouchává komunikaci, a to prostřednictvím buď softwarového, nebo hardwarového systému nazvaného sniffer. Vzhledem k tomu, že se sniffing nijak navenek neprojevuje, nýbrž pouze sbírá data, která až následně útočník zneužije, bývá velmi často latentní. Sniffing, respektive sniffer, bývá mimo jiné využíván síťovými správci, a to za účelem analýzy chyb v síti, případně umožňuje správci navíc odhalit neoprávněná vniknutí do systému.

3.1.4. Man-in-the-middle attack (MitM)

MitM rozumíme metody zachycování veškerých dat přenášených mezi dvěma a více uživateli, případně různými technickými zařízeními. Ačkoliv lze spatřovat určitou obdobnost se sniffingem, nejedná se o totéž. Útoky MitM jsou daleko závažnější, a to z toho důvodu, že jakýkoliv přenos dat mezi uživateli, prochází automaticky rovněž skrze útočníkův počítač. Man-in-the-middle útočník pak na rozdíl of sniffera může získaná data upravit či změnit a následně bez povšimnutí zaslat druhému uživateli. Běžně k útokům dochází skrze nezabezpečené veřejné Wi-Fi sítě.

Zajímavým MitM útokem, který našel využití v oblasti bankovních automatů, je jackpotting. Při jackpottingu pachatel v nestřežený moment fyzicky vloží do portu bankomatu malé černé

[35] JONES, Caitlin. *Phishing, Vishing, SMiShing, Whaling And Pharming: How To Stop Social Engineering Attacks* [online]. 19. ledna 2022 [cit. 2022-06-04]. Dostupné z: https://expertinsights.com/insights/phishing-vishing-smishing-whaling-and-pharming-how-to-stop-social-engineering-attacks/

[36] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Kybernetické incidenty pohledem NÚKIB* [online]. 2022 [cit. 2022-06-04]. Dostupné z: https://nukib.cz/download/publikace/vyzkum/03-2022-Novinky.pdf

elektronické zařízení (útoku se také někdy podle zařízení říká blackbox[37]), skrze které je schopný systém odpojit od původního síťového jádra a připojit ho k vlastnímu zařízení. Jakmile získá pachatel přístup k systému bankomatu, může bez obtíží regulovat výdej bankovek. Kybernetické útoky na počítačové systémy v oblasti bankovnictví představují hrozbu, která by neměla být podceňována.

3.1.5. DoS a DDoS

Denial of Service (DoS) je typ útoku, jehož podstatou je generování nepřeberného množství požadavků v krátkém časovém intervalu, a to s cílem zahltit počítačový systém a omezit tak jeho funkčnost. Počítačový systém není posléze schopen množství dat zpracovat a dochází k jeho přetížení, respektive k nefunkčnosti. Podtypem DoS útoku je Distributed Denial of Service (DDoS). Útoky jsou velmi obdobné, nicméně DDoS zahlcuje cílový systém z několika různě rozmístěných zdrojů. Při DDoS útoku se útočník primárně snaží napadnout firewall a jiná bezpečnostní opatření, operační systém nebo aplikace. Uvádí se, že až 80 % veškerých DDoS útoků je odesíláno prostřednictvím tzv. botnetů, které lze definovat jako automatizovanou síť infikovanou typicky malwarem. Osoba, která pak botnet ovládá, se nazývá botmaster.[38]

DoS a DDoS představují typy útoků, které řadíme pod článek 5 Úmluvy o počítačové kriminalitě s názvem „zasahování do systému“.

3.1.6. Malware

Malware vznikl ze složení anglických slov „malicious“ a „software“, tedy lze ho volně přeložit jako škodlivý software, který neoprávněně získává přístup k počítačovému systému. Z hlediska Úmluvy představuje malware typy útoků subsumovatelné pod článek 4 Úmluvy s názvem „zasahování do dat“.

S malwarem se lze setkat v mnoha podobách. Mezi základní typy řadíme adware (vyskakující podvodná reklamní sdělení), spyware (program získávající bez vědomí uživatele statistická data o provozu), viry, trojské koně, rootkity (software maskující malware) a keyloggers (zaznamenávající stisknutí klávesnic za účelem monitoringu přihlašovacích údajů). Specifickým typem malwaru je

[37] Jackpotting lze uskutečnit dvěma odlišnými metodami. Místo černého elektronického zařízení připojí pachatel do bankomatu USB flash disk, který je infikovaný malwarem. Škodlivý software, obdobně jako blackbox, donutí systém vydat veškerou hotovost, kterou pachatel posléze vyzvedne.

[38] HOQUE, Nazrul, Dhruba K BHATTACHARYYA a Jugal K KALITA. Botnet in DDoS Attacks: Trends and Challenges. *IEEE Communications surveys and tutorials*. New York: IEEE, 2015, 17(4), s. 2243. ISSN 1553-877X. Dostupné z: doi:10.1109/COMST.2015.2457491

ransomware, který je sofistikovanou formou útoku umožňující zablokovat uživatelův počítačový systém, případně znepřístupnit pouze vybraná klíčová data. Za opětovné zpřístupnění souborů požaduje útočník zaplacení výkupného v podobě kryptoměn.[39]

3.2. Útoky související s počítačem

3.2.1. Počítačové padělání

Jakákoliv neoprávněná manipulace s počítačovými daty, která vede k jejich nepravosti, nicméně s úmyslem užít taková data jako pravá, je označována jako počítačové padělání. Řadíme sem i případy padělání platebních karet, tzv. skimming. Útočník z platební karty okopíruje data alokovaná v magnetickém proužku karty a přenese je na vlastní plastový nosič, vše bez souhlasu a vědomí držitele platebního prostředku.[40]

3.2.2. Počítačový podvod

Počítačový podvod definuje článek 8 Úmluvy o počítačové kriminalitě, a to tak, že jde o úmyslné způsobení majetkové škody prostřednictvím jakékoliv neoprávněné manipulace s počítačovými daty nebo jakýmkoliv obdobným zásahem do počítačového systému. Mezi obvyklé útoky řadíme tzv. scamy, tedy podvodné spamy. Nechvalně proslulým podvodem jsou Nigerijské dopisy, někdy obdobně označovány jako Scam 419[41]. Útočník, často vydávající se za advokáta, osloví uživatele internetu s tím, že v zahraničí probíhá dědické řízení a jediným pozůstalým dědicem, je právě adresát e-mailu. Za zahraniční převod několika desítek milionů korun dolarů si podvodný advokát účtuje pouze drobné administrativní poplatky spojené s převodem. Jinými příklady útoků jsou podvodné nabídky, jako například speciální metody zhodnocování peněz či „nadmíru výhodné" nabídky prací z domova.

3.2.3. Kyberterorismus

Definice kyberterorismu se poměrně odlišují, nicméně lze uvést, že se jedná o nezákonné použití hrozby síly, za účelem dosažení ideologických, politických nebo náboženských cílů, přičemž hrozba je uskutečňována ve virtuálním prostředí. Někteří autoři jej chápou jako jakékoliv použití počítačové sítě k narušení kritické národní infrastruktury. Možný nárůst kyberterorismu je

[39] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z. s. p. o., 2016. s. 204–210. ISBN 978-80-88168-18-8.
[40] POLICIE ČR. Skimming. In: *Policie.cz* [online]. [cit. 2022-06-05]. Dostupné z: https://www.policie.cz/clanek/ncoz-skimming.aspx
[41] Označení „419" v názvu odkazuje na nigerijský tamní trestní zákoník, který zmiňuje daná podvodná jednání.

podporován vzrůstající závislostí kritických infrastruktur na výpočetní technice. Podle Weimanna se tak státům zvyšuje počet „virtuálních Achillových pat“, které přitahují pozornost útočníků. Kyberterorismus má podle Weimanna oproti konvenčnímu terorismu pro pachatele nespočet výhod. Příkladmo uvádí nižší finanční nákladnost, větší anonymitu, širokou škálu potenciálních cílů útoků a příležitost páchat trestnou činnost distančně.[42]

3.3. Útoky související s obsahem

3.3.1. Dětská pornografie

Podle článku 9 Úmluvy o počítačové kriminalitě, zahrnuje pojem dětská pornografie veškerý materiál, který vizuálně zobrazuje nezletilou osobu podílející se na sexuální aktivitě, případně osobu, která se jeví jako nezletilá. Úmluva pod zmíněný článek zahrnuje poměrně široké spektrum útoků, příkladmo distribuci dětské pornografie pomocí počítačového systému, například prostřednictvím hypertextových odkazů či sdílených úložišť. Uvádí se, že moderní technologie napomohly sexuálním útočníkům v přístupu k pornografickým dílům a zároveň přispěly k povzbuzení nezletilých osob k sexuálním aktivitám.[43]

3.3.2. Hoax

Příkladem nežádoucího obsahu na internetu je hoax. Charakterizujeme jej jako poplašnou a zároveň nepravdivou zprávu, jejímž cílem je vyvolat a šířit strach, záměrně uvádět nepravdivé informace s vidinou manipulace názoru ostatních osob. Typicky se v uživateli snaží vyvolat pocit hrozby a paniky, doufaje, že zpráva bude řetězově rozeslána dalšímu okruhu osob. Speciální místo v oblasti hoaxů zaujímají tzv. virové hoaxy. Jde opět o jednu z technik sociálního inženýrství, která ovšem varuje před fiktivními bezpečnostními chybami, a to proto, aby uživatel v domnění, že jeho počítač byl infikován, dané soubory smazal.

3.3.3. Kyberšikana

Obdobně jako šikana v tradičním pojetí je kyberšikana chápána jako opakující se agresivní jednání, které tenduje k poškození osoby a způsobení jí újmy prostřednictvím internetu. Subsumujeme pod ni zveřejňování dehonestujících komentářů, vyhrožování na sociálních sítích a

[42] WEIMANN, Gabriel. Cyberterrorism: The Sum of All Fears? *Studies in conflict and terrorism*. Taylor & Francis Group, 2005, roč. 28(2), s. 130. ISSN 1057-610X. Dostupné z: doi:10.1080/10576100590905110

[43] CLOUGH, Jonathan. *Principles of Cybercrime*. Cambridge, UK; New York: Cambridge University Press, 2010, s. 183–192. ISBN 978-0-521-89925-3.

zasílání nevyžádaných obtěžujících zpráv.[44] Pyzalski rozlišuje šest typů kyberšikany v závislosti na tom, vůči komu směřuje. První formou je vzájemná virtuální agrese, kterou Pyzalski nazval jako možný zárodek budoucí kyberšikany. Dále rozlišuje šikanu vůči zaměstnancům školy, zranitelným osobám, náhodným osobám a vůči skupinám (například náboženským). Poslední skupinou je šikana veřejně známých osob.[45]

Kyberšikana má nezměrný počet forem a metod, které útočník může aplikovat. Jednou z nich je tzv. flaming, tedy zasílání agresivních a vulgárních zpráv dané osobě skrze SMS zprávy, případně e-maily. Další formou je tzv. masquerading, který chápeme jako vydávání se za jinou osobu a zveřejňování dehonestujících informací o oběti. V neposlední řadě lze uvést tzv. outing, tedy zveřejňování citlivých, soukromých nebo žinantních informací o oběti. Speciální metodou vyskytující se typicky u kyberšikany vyučujících, je cyberbaiting. Jedná se o vyprovokování učitele a následné natočení jeho reakce s tím, že záznam je pak zveřejněn na internetu.[46]

3.3.4. Kybergrooming

Proces postupného sbližování útočníka s dítětem skrze sociální sítě, herní platformy nebo internetové chaty, nazýváme kybergroomingem. Útočník si vytváří falešnou identitu tak, aby co nejdůvěryhodněji působil na potenciální oběť, a proto se často sám vydává za dítě či dospívajícího. S dítětem se postupně seznamuje a buduje důvěru, přičemž takový proces může trvat týdny i měsíce. Cílem útočníka je získat citlivé informace, zejména směřuje k získání pornografických materiálů. Kybergrooming se mnohdy z virtuálního prostředí může přesunou i do reálného světa, neboť někteří útočníci tendují posléze i k osobnímu setkání s dítětem. V širším pojetí je kybergrooming chápán jako jakákoliv onlinová komunikace mezi dospělou osobou a dítětem doprovázená sexuální tematikou.[47]

---

[44] WHITTAKER, Elizabeth a Robin M. KOWALSKI. Cyberbullying Via Social Media. *Journal of school violence*. London: Routledge, 2015, roč. 14, č. 1, s. 11–29. ISSN 1538-8220. Dostupné z: doi:10.1080/15388220.2014.949377

[45] PYZALSKI, Jacek. From cyberbullying to electronic aggression: typology of the phenomenon. *Emotional and behavioural difficulties*. Taylor & Francis, 2012, roč. 17, č. 3–4, s. 307. ISSN 1363-2752. Dostupné z: doi:10.1080/13632752.2012.704319

[46] KOPECKÝ, Kamil a René SZOTKOWSKI. Cyberbullying, cyber aggression and their impact on the victim – The teacher. *Telematics and informatics*. 2017, roč. 34, č. 2, s. 507. ISSN 0736-5853. Dostupné z: doi:10.1016/j.tele.2016.08.014

[47] LUKÁŠOVÁ, Kateřina. Škodlivý obsah na Internetu. *Acta Universitatis Carolinae – Iuridica*. 2012, č. 4, s. 19. ISSN 0323-0619.

3.4. Útoky týkající se porušení autorského práva a práv souvisejících s právem autorským

3.4.1. Warez

Warez je internetovým slangovým pojmem užívaným pro díla chráněná autorským právem, která jsou ovšem nelegálně sdílena a distribuována prostřednictvím internetu. Chráněná díla rozšiřuje tzv. warez komunita, která se sdružuje na vlastních fórech a platformách, kterým se opět říká warez. Nebezpečnost nespočívá pouze v porušování autorského práva, nýbrž i v šíření škodlivého softwaru. Soubory bývají mnohdy „obohaceny" o škodlivý virus, který uživatel nevědomky stáhne i s autorským dílem. Nutno zmínit, že primárním cílem warez útočníka není finanční obohacení, nýbrž získání prestiže v tamní komunitě. Členové se mezi sebou totiž předhání v tom, kdo daný materiál zveřejní první, což jim přináší posléze v komunitě respekt.

3.4.2. Softwarové pirátství

Útoky proti autorskému právu související s počítačovými programy označujeme jako softwarové pirátství. Ačkoliv by se mohlo zdát, že jde o termín totožný s pojmem warez, není tomu tak. Markantní odlišnost spočívá v motivu. Jak bylo výše zmíněno, warez útočník nesleduje primárně finanční zisk a komerční využití, kdežto softwarový pirát ano. Příkladem softwarového pirátství může být stahování softwaru z internetu bez licence.

3.4.3. Cybersquatting a typosquatting

Cybersquatting bývá běžně definován jako registrace internetové domény obsahující název ochranné známky, ke které však registrující osoba nemá žádná práva. Útočník následně vlastníkovi ochranné známky nabídne, že doménu zruší, pokud mu bude na oplátku vyplacena peněžitá odměna. V opačném případě útočník oběť vydírá tak, že na zaregistrovanou doménu zveřejní nevhodný obsah, například pornografická díla zobrazující děti. Četnost případů cybersquattingu klesá, neboť v roce 2004 byl zakotven právní rámec[48] pro registraci domén.[49]

[48] Jedná se o Nařízení Komise (ES) č. č. 874/2004 ze dne 28. dubna 2004, kterým se stanoví obecná pravidla pro zavádění a funkce domény nejvyšší úrovně .eu a zásady, jimiž se řídí registraceText s významem pro EHP. Národní vrcholnou doménu na tuzemské úrovni spravuje CZ.NIC., zájmové sdružení právnických osob, které stanovilo pravidla a postupy pro registraci jmen pod doménou s názvem „.cz".

[49] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z. s. p. o., 2016. s. 326. ISBN 978-80-88168-18-8.

Typosquatting funguje na obdobném principu, ale s tím rozdílem, že útočník zaregistruje již existující název domény, nicméně s překlepem nebo chybným pravopisem (např. doména facebook.com byla registrována jako face-book.com, faacebook.com apod.).[50] Pokud uživatel nezkontroluje URL adresu[51], mnohdy ani nezjistí, že otevřel klamavou stránku, neboť vzhledově mohou stránky vypadat zcela identicky. Problém nastává v momentě, kdy se uživatel na podvodné stránce přihlašuje či vyplňuje jakákoliv jiná data.

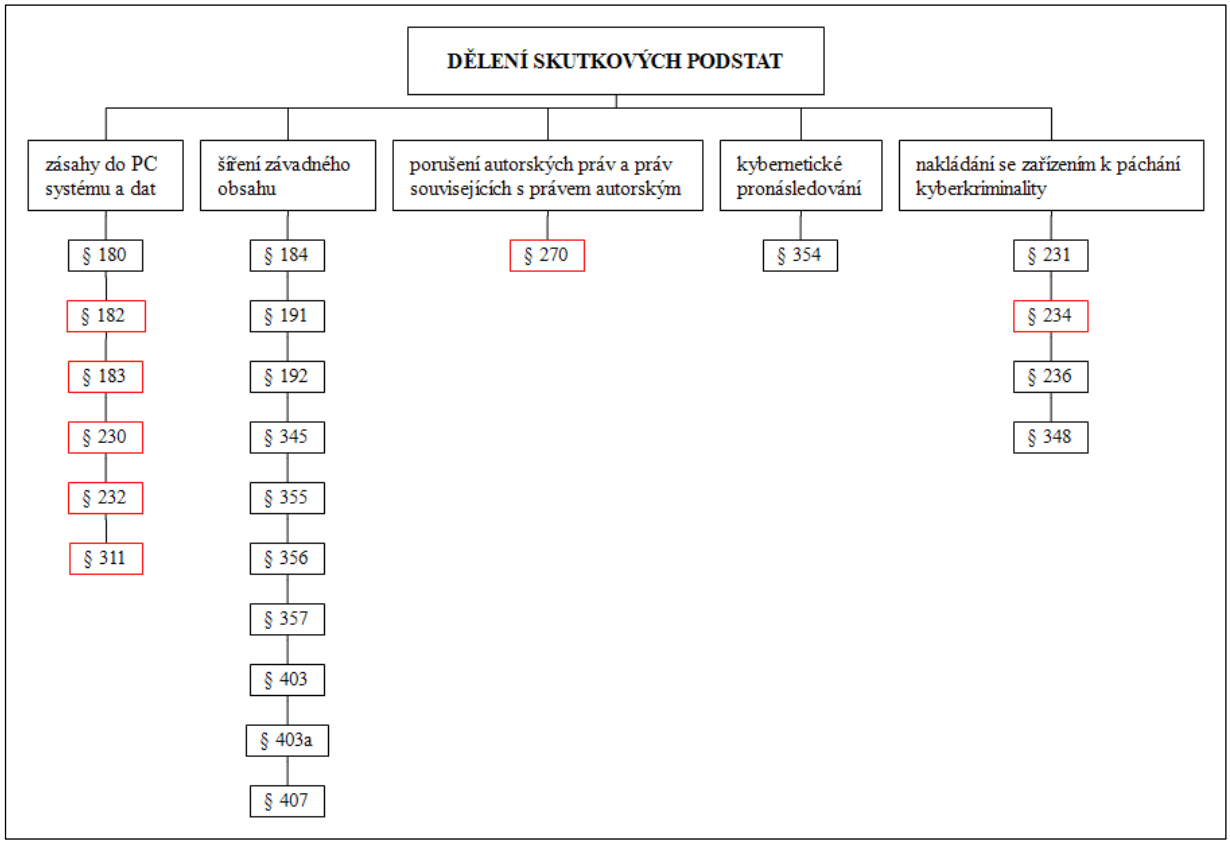
[50] TUNGGAL, Tyas Abi. *What is Typosquatting (and how to prevent it)* [online]. 8. května 2022 [cit. 2022-06-05]. Dostupné z: https://www.upguard.com/blog/typosquatting

[51] URL adresa (Uniform Resource Locator) slouží k jednoznačné identifikaci umístění webové stránky, případně souboru na internetu.

4. VYBRANÉ TRESTNÉ ČINY PODLE SOUČASNÉ PRÁVNÍ ÚPRAVY

Zvláštní část trestního zákoníku obsahuje řadu skutkových podstat trestných činů vztahujících se nějakým způsobem ke kybernetické kriminalitě. Jedná se buď o trestné činy, jejichž skutková podstata je naplněna užitím prostředků informační a komunikační technologie (tzv. cyber-enabled crimes), nebo jde o trestné činy, při nichž jsou terčem kyberútoku ICT technologie (tzv. cyber-dependent crimes). Podrobněji lze skutkové podstaty dělit do pěti skupin, a to na zásahy do počítačového systému a dat, šíření závadného obsahu, porušení autorských práv a práv souvisejících s právem autorským, kybernetické pronásledování a na nakládání se zařízením k páchání kyberkriminality.[52]

Schéma 1 – Dělení skutkových podstat do pěti skupin



Legenda:

▭	trestné činy, u kterých jsou prostředky ICT užity ke spáchání trestného činu
▭	trestné činy, při jejichž páchání je terčem útoku ICT prostředek

[52] VOLEVECKÝ, Petr. Kybernetické trestné činy v trestním zákoníku. *Trestní právo*. 2010, roč. 14, č. 7–8, s. 19–43.

Lze se setkat i s dělením skutkových podstat ve smyslu Úmluvy o počítačové kriminalitě – trestné činy proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů, trestné činy související s počítačem, trestné činy související s obsahem a trestné činy týkající se porušení autorského práva a práv souvisejících s právem autorským.

Následující kapitola obsahuje vybrané trestné činy uspořádané podle systematiky trestního zákoníku.

4.1. Trestné činy proti svobodě a právům na ochranu osobnosti, soukromí a listovního tajemství

4.1.1. Porušení tajemství dopravovaných zpráv (§ 182 TZ)

Cílem daného ustanovení je ochrana tajemství dopravovaných zpráv, přičemž tajemstvím se rozumí obsah písemností nehledě na jejich hodnotu. Porušení tajemství vykládá komentářová literatura jako *„jakékoli neoprávněné narušení přepravované písemnosti, posílané zprávy nebo neveřejného přenosu počítačových dat podle písmen a) až c) odst. 1 se snahou zjistit jejich obsah, aniž by tento obsah musel být někomu dalšímu sdělen“*.[53] Vyjma uzavřeného listu je poskytována ochrana i jiným písemnostem a záznamům zasílaných prostřednictvím sítě elektronické komunikace. Nutno zmínit, že ochrany nepožívají zprávy dosud nedoručené či rozepsané.

Z hlediska kybernetické kriminality je klíčový odst. 1 písm. b) a c) ustanovení 182 TZ. Písmeno b) chrání před porušením tajemství datové, textové, zvukové, případně obrazové zprávy zasílané prostřednictvím sítě elektronické komunikace. Při právní konstrukci trestného činu dle § 182 odst. 1 písm. b) TZ vycházel zákonodárce z pojmů[54] uvedených v zákoně č. 127/2005 Sb., o elektronických komunikacích. Podle Koloucha je taková konstrukce poněkud zužující, neboť je tak působnost trestních norem omezena pouze na tajemství dopravovaných zpráv prostřednictvím veřejných poskytovatelů připojení. Ochrany dle § 182 TZ by pak nepožívaly osoby, které mají jiné připojení než podle zákona o elektronických komunikacích.[55] Písmeno c) postihující porušení tajemství při neveřejném přenosu počítačových dat bylo do trestního zákoníku včleněno jakožto požadavek plynoucí ze směrnice Evropského parlamentu a Rady 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací. Klíčovým atributem je

[53] ŠÁMAL, Pavel. Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí – § 183. In: ŠÁMAL, Pavel a kolektiv. *Trestní zákoník II – komentář. Zvláštní část (§ 140–421)*. 2. vydání. Praha: C. H. Beck, 2012, s. 1805–1819. ISBN 978-80-7400-428-5.
[54] Jedná se o pojmy jako účastník, uživatel a síť elektronických komunikací.
[55] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z. s. p. o., 2016, s. 350. ISBN 978-80-88168-18-8.

zde neveřejnost zmíněného přenosu dat, k čemuž je však potřeba uvést, že podmínka neveřejnosti se vztahuje pouze na způsob přenosu, nikoliv na obsah písemnosti. Trestného činu podle § 182 TZ se tak dopustí i pachatel, jenž poruší tajemství neveřejně přenášené informace, byť obsah informace je již všem známý a dostupný.[56]

Ochrana listovního tajemství a tajemství dopravovaných zpráv není zcela bezmezná. Zákonnou výjimkou z ochrany podle § 182 TZ je nařízení odposlechu a záznamu telekomunikačního provozu ve smyslu § 88 a § 88a TŘ, případně taktéž institut sledování osob a věci dle § 158d odst. 3 TŘ. Mimo trestní řád lze výjimky nalézt v zákoně č. 169/1999 Sb., o výkonu trestu odnětí svobody (§ 17 odst. 2 a 3), zákoně č. 154/1994 Sb., o bezpečnostní informační službě (§ 7 a násl.) a též v § 7 a násl. zákona č. 289/2005 Sb., o Vojenském zpravodajství. Podle Smejkala jsou to právě ozbrojené složky, které nezřídka porušují tajemství dopravovaných zpráv.[57]

Nejčastější příčinou porušení tajemství dopravovaných informací bývá v kyberprostoru útok nazývající se sniffing, případně lze uvažovat i o útoku man-in-the-middle.

4.2. Trestné činy proti lidské důstojnosti v sexuální oblasti

4.2.1. Výroba a jiné nakládání s dětskou pornografií (§ 192 TZ)

Dětskou pornografii chápeme podle dikce trestního zákoníku jako dílo zobrazující nebo jinak využívající dítě, tedy osobu mladší 18 let. Objektem předmětného ustanovení je zájem společnosti na ochraně mravního vývoje dítěte a také jejich ochrana před sexuálním zneužíváním. S expanzí kyberprostoru nicméně vyvstala otázka, zda se tuzemská právní úprava vztahuje i na výrobu a nakládání s virtuální dětskou pornografií, neboť zákon nijak explicitně nediferencuje mezi pornografií skutečnou a virtuální.

Definici virtuální dětské pornografie poskytla Úmluva o počítačové kriminalitě, konkrétně pak článek 9, který mimo jiné pod pojem dětské pornografie subsumoval i realistické zobrazení nezletilé osoby při sexuálním chováním. Téměř totožně definuje pojem i směrnice o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii[58], která jej chápe jako realistické obrázky dítěte účastnícího se sexuálního jednání. Ze zmíněného lze tedy

[56] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z. s. p. o., 2016, s. 351. ISBN 978-80-88168-18-8.
[57] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018, s. 317. ISBN 978-80-7380-720-7.
[58] Směrnice Evropského parlamentu a Rady 2011/92/EU ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii.

vyvodit, že virtuální dětská pornografie je ta, která sice reálně zachycuje osobu dítěte, nicméně nedošlo k žádnému jejímu zneužití, a to z toho důvodu, že jde pouze o počítačem vygenerované zobrazení. Vyvystává otázka, zda je tedy možné na virtuálně vytvořenou osobu dítěte v pornografickém díle pohlížet jako na osobu jevící se být dítětem ve smyslu § 192 TZ?

Osobně se domnívám, že ačkoliv zákonodárce neposkytl zcela jasné interpretační vodítko, je nutné pojem dětské pornografie chápat v širším slova smyslu, a tedy reflektovat závazky vyplývající z mezinárodních smluv, zejména z již výše zmíněné Úmluvy o počítačové kriminalitě a směrnice o boji proti pohlavnímu zneužívání dětí. V souvislosti s tím je tedy možné říci, že virtuálně vyobrazené dítě bude moci být chápáno jako osoba jevící se být dítětem ve smyslu § 192 TZ a pachatel bude trestán stejně jako při výrobě a nakládání s tradiční dětskou pornografií.[59] Rozhodující zde nicméně bude hledisko realističnosti zobrazeného díla. Je však otázkou do budoucna, zda s neustálým vývojem v oblasti výpočetní techniky bude vůbec možné rozeznat skutečné dítě od dítěte vytvořeného počítačem.

Objevily se i otázky, zda kriminalizace virtuální pornografie je správná, respektive přiměřená. Argumenty pro dekriminalizaci virtuální dětské pornografie vycházely z premisy, že virtuální dílo by pro řadu deviantů mohlo představovat určitou alternativu, která by snižovala pravděpodobnost, že dojde ke skutečnému zneužití dítěte.[60] Jiní oponují tím, že virtuální pornografie má opačný efekt, tedy že zvyšuje deviantovo libido a posléze ho povzbuzuje k jednání ve skutečném světě.[61] Argumenty lze hledat mimo to i v objektu skutkové podstaty trestného činu. Jak bylo uvedeno na začátku, primárním smyslem ustanovení týkajících se dětské pornografie je ochrana dětí před sexuálním zneužíváním, potažmo též ochrana jejich mravního vývoje. Se zřetelem k tomu, že zde nedochází k sexuálnímu zneužití žádného reálně existujícího dítěte, je otázkou, zda by zmíněný chráněný objekt, byl takovým dílem vůbec přímo zasažen. V neposlední řadě je také nutné zkoumat společenskou škodlivost takového činu.

---

[59] Situace trestnosti virtuální dětské pornografie byla řešena i Nejvyšším soudem USA, konkrétně se jednalo o případ Ashcroft v. Free Speech Coalition (2002). Nejvyšší soud zde vyslovil názor, že virtuální pornografie nemá žádnou oběť, tedy nedochází zde ke spáchání žádného trestného činu. Myšlenka, že dílo může deviantovi dodat odvahu konat ve světě skutečném, nebyla pro tamní Nejvyšší soud přijatelná. Soud argumentoval tím, že domnělý impuls odvahy ke kriminálnímu chování není důvodem, aby taková činnost byla ještě zakázána. In: HERCZEG, Jiří. Virtuální dětská pornografie: Zločin bez oběti? In: VANDUCHOVÁ, Marie a Tomáš GŘIVNA. Pocta Otovi Novotnému k 80. narozeninám. Praha: Aspi, a.s., 2008, s. 47. ISBN: 978-80-7357-365-2.

[60] PIROCH, Jan a Jan BUMBA. Studie: Dostupnost dětské pornografie snižuje sexuální násilí na dětech. In: *iRozhlas* [online]. 2010 [cit. 2022-06-09]. Dostupné z: https://www.irozhlas.cz/clovek/studie-dostupnost-detske-pornografie-snizuje-sexualni-nasili-na-detech_201012131955_jpiroch

[61] HERCZEG, Jiří. Virtuální dětská pornografie: Zločin bez oběti? In: VANDUCHOVÁ, Marie, Tomáš GŘIVNA a Oto NOVOTNÝ. *Pocta Otovi Novotnému k 80. narozeninám*. Praha: ASPI, 2008, s. 47. ISBN 978-80-7357-365-2.

Pozoruhodná problematika se mimo jiné objevila i v souvislosti s distribucí dětské pornografie skrze virtuální prostředí onlinových her. Počítačová hra s názvem Second Life byla vyvinuta ve dvou verzích, jedna z nich byla určena pro dospělé hráče a druhá pro teenagery, přičemž kontrola věkové hranice nebyla nijak zajištěna. Zmíněná online počítačová hra nabídla hráčům kromě tvorby avatarů také možnost anonymně mezi sebou sdílet skrze hrací prostředí i libovolné fotografie a různá videa.[62] Absence jakékoliv regulace herního prostředí tak jenom otevřela dveře nelegálním aktivitám a ve virtuálním světě se posléze začaly objevovat případy, kdy docházelo k sexuálním aktivitám mezi dospěle vypadajícím avatarem a avatarem znázorňujícím dítě, navíc se zde také objevily i případy šíření klasické dětské pornografie skrze herní platformu.

Z kyberútoků, které lze řadit pod skutkovou podstatu § 192 TZ, lze jmenovat sexting[63]. Narůstajícím typem útoků jsou v současné době i případy tzv. revenge porn neboli nekonsenzuální pornografie, kterou chápeme jako *„zpřístupnění obrazového záznamu konkrétní osoby se sexuálním obsahem bez jejího souhlasu“.*[64]

4.2.2. Navazování nedovolených kontaktů s dítětem (§ 193b TZ)

Zákonodárce v trestném činu definovaném v § 193b TZ jako objekt vymezil zájem ochránit osoby mladší 15 let před navazováním sexuálně motivovaných kontaktů, které by mohly narušit jejich mravní, eventuálně i tělesný vývoj. Ustanovení bylo do českého právního řádu implementováno na základě čl. 6 směrnice Evropského parlamentu a Rady 2011/93/EU ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii. Podstatné je, aby šlo o návrh, který obsahuje znaky jednoho ze sexuálně motivovaných trestných činů (§ 187 odst. 1, § 192, § 193, § 202 odst. 2 TZ) vyjmenovaných v § 193b TZ, přičemž pachatel musí mít úmysl takový trestný čin spáchat. Kriminalizován je zde už samotný návrh, který je dítěti mladšímu 15 let učiněn, a to nejen osobně, ale také skrze informační a komunikační technologie, nejčastěji pak prostřednictvím sociálních sítí.[65] Nejvyšší soud se judikatorně musel vypořádat s argumentem, že navazování kontaktů prostřednictvím virtuálních sítí není reálné, a tedy

[62] GARCIA-RUIZ, Miguel A., Miguel Vargas MARTIN, Amin IBRAHIM, Arthur EDWARDS a Raul AQUINO-SANTOS. Combating Child Exploitation in Second Life. *2009 IEEE Toronto International Conference Science and Technology for Humanity (TIC-STH)*. IEEE, 2009, s. 761–766. Dostupné z: doi:10.1109/TIC-STH.2009.5444398

[63] Sexting je poměrně aktuálním fenoménem, jehož podstatou je rozesílání fotografií či videí se sexuální tematikou, a to prostřednictvím moderních technologií, nejčastěji skrze mobilní telefon.

[64] GARGULÁK, Michal. Kriminalizace nekonsensuální pornografie v České republice. *Trestněprávní revue*. 2018, č. 2, s. 30–35.

[65] FREMR, Robert. Navazování nedovolených kontaktů s dítětem - § 193b. In: DRAŠTÍK, Antonín, Robert FREMR, Tomáš DURDÍK, Miroslav RŮŽIČKA a Alexander SOTOLÁŘ. *Trestní zákoník: komentář (I. díl)*. Praha: Wolters Kluwer, 2015, s. 1042–1043. ISBN 978-80-7478-790-4.

neopodstatňuje společenskou škodlivost trestné činu. Soud velmi správně podotkl, že i virtuální komunikace představuje reálný prostředek k navázání kontaktu a současně též umožňuje možnost nabídnout dítěti osobní setkání. V takových případech nejde o domnělé či simulované jednání, neboť se odvíjí od skutečných pohnutek, je konáno reálně existující osobou, a navíc je provedeno v konkrétním časovém horizontu.[66]

Nabízí se nicméně otázka, proč byla zvolena ochrana pouze u dětí mladší 15 let, ačkoliv ustanovení § 192, respektive 193 TZ chrání dítě (osobu mladší 18 let). De lege ferenda by bylo vhodné rozšířit ochranu na mladistvé, tedy osoby, které dovršily patnáctý rok a nepřekročily osmnáctý rok věku.

Zmíněný trestný čin umožňuje postihnout jednání tzv. kybergroomingu.

4.3. Trestné činy proti majetku

4.3.1. Podvod (§ 209 TZ)

Podvodná jednání představují těžiště veškerých nelegálních aktivit páchaných v kyberprostoru. Typicky se jedná o situace, kdy pachatelé využívají výpočetní techniku včetně internetu jako nástroj k páchání trestné činnosti. Objektem daného trestného činu je cizí majetkové právo, respektive všechny jeho složky. Pachatel naplní objektivní stránku tím, že jiného uvede v omyl, jeho omylu využije nebo osobě zamlčí podstatné skutečnosti. Zároveň na cizím majetku musí být způsobena škoda nikoli nepatrná. Pachatelem může být jakákoliv odpovědná osoba, přičemž je vyžadováno, aby jednala úmyslně.[67]

V souvislosti s kyberprostorem vyvstala v praxi nejasnost, zda se lze podvodného jednání dopustit i prostřednictvím manipulace na počítači či jiném technickém zařízení. Zákonodárce vycházel z premisy, že ačkoliv určité počítačové programy fungují zcela automaticky bez něčího přičinění, vždy existuje konkrétní osoba, která zapříčinila, že byl daný program vůbec spuštěn či jednal v pachatelův prospěch.[68] Z tohoto důvodu byl do výkladových ustanovení trestního zákoníku vložen § 120, který vymezil, že uvést někoho v omyl nebo využít jeho omylu lze i provedením zásahu do počítačových informací nebo dat, zásahem do programového vybavení počítače nebo provedením jiné operace na počítači, zásahem do elektronického nebo jiného technického zařízení,

[66] Usnesení Nejvyššího soudu ze dne 25. 11. 2020, sp. zn. 8 Tdo 1041/2020.
[67] ŠÁMAL, Pavel. Podvod - § 209. In: ŠÁMAL, Pavel a kolektiv. *Trestní zákoník II – komentář. Zvláštní část (§ 140–421)*. 2. vydání. Praha: C. H. Beck, 2012, s. 2051–2052. ISBN 978-80-7400-428-5.
[68] ŠÁMAL, Pavel. Uvedení někoho v omyl a využití něčího omylu prostřednictvím technického zařízení - § 120. In: ŠÁMAL, Pavel a kolektiv. *Trestní zákoník I – komentář. Obecná část (§ 1–139)*. 2. vydání. Praha: C. H. Beck, 2012, s. 1307–1311. ISBN 978-80-7400-428-5.

včetně zásahu do předmětů sloužících k ovládání takového zařízení, anebo využitím takové operace či takového zásahu provedeného jiným.

Typickým útokem subsumovatelným pod trestný čin podvodu dle § 209 TZ je phishing. Jak bylo již uvedeno výše, podstatou phishingového útoku je přesměrování uživatele na podvodnou internetovou stránku. Uživatel uvedený v omyl následně na stránce zadává svá data, která pachatel zneužije za účelem získání prospěchu. Může dojít i k situaci, kdy je phishing kombinován s jiným typem útoku, nejčastěji malwarem, přičemž v takovém případě získá pachatel navíc i přístup k počítačovému systému nebo nosiči informací. Z hlediska trestněprávního lze v daném případě uvažovat o jednočinném souběhu § 209 TZ s § 230 odst. 2 TZ.[69]

Podvodná jednání se velmi pružně přizpůsobují aktuální situaci a nápaditost pachatelů nezná hranic. V souvislosti s válečným konfliktem na Ukrajině vzrostl počet podvodných internetových sbírek vyzývajících k humanitární pomoci. Neobvyklé nejsou ani e-maily či zprávy osob vydávajících se za válkou postižené ukrajinské občany žádající finanční prostředky, které jsou přijímány především v kryptoměnách. Společným atributem všech podvodných jednání v online prostředí zůstává psychosociologický aspekt, tedy snaha pachatelů vyvolat v oběti důvěru, soucit, lítost, případně dostat oběť do časové tísně.

4.3.2. Neoprávněný přístup k počítačovému systému a nosiči informací (§ 230 TZ)

Konec hlavy V. zvláštní části TZ obsahuje skupinu tří specifických trestných činů (§ 230, § 231 a § 232 TZ), které někdy bývají souhrnně označovány jako počítačové trestné činy, a jejichž právní zakotvení vzniklo především důsledkem implementace závazku plynoucího z Úmluvy o počítačové kriminalitě. Trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací sestává ze dvou základních skutkových podstat a ze tří kvalifikovaných.

§ 230 odst. 1 TZ

Objektem první základní skutkové podstaty je důvěrnost počítačového systému a dat, která v něm mohou být uložena. Objektivní stránka spočívá v tom, že pachatel musí neoprávněně získat přístup k počítačovému systému nebo jeho části, a to tak, že překoná bezpečnostní opatření. Bezpečnostní

[69] Usnesení Nejvyššího soudu ze dne 16. 5. 2018, sp. zn. 4 Tdo 456/2018.

opatření je komentářovou literaturou chápáno jako jakékoliv opatření, které chrání před neoprávněným přístupem, což obvykle bývá heslo, přístupový klíč či firewall.[70]

K překonání bezpečnostního opatření může pachatel využít poměrně širokého spektra nástrojů, ať už jde o nástroje softwarové (např. keyloggers) a hardwarové, nebo získané poznatky ze sociálního inženýrství. Nutno dodat, že skutková podstata bude naplněna i v případě, že překonání bezpečnostního opatření nebude pro pachatele nikterak náročné. Může proto jít i o velmi jednoduše uhodnutelné heslo (např. 1234) či o heslo, které bylo poznamenáno na papírku u daného zařízení. Odůvodnění lze spatřovat v tom, že pokud osoba jakkoliv (byť nejjednodušeji) zabezpečila svůj počítačový systém, projevila tím vůli, aby bez jejího souhlasu neměly do systému přístup další osoby.

Z kybernetických útoků, které lze subsumovat pod zmíněnou skutkovou podstatu, řadíme útoky označované jako hacking a cracking, tedy především prolamování hesel, pharming, spoofing či phishing.

§ 230 odst. 2 TZ

Druhý odstavec postihuje další možné protiprávní jednání osoby, která již získala přístup k počítačovému systému anebo nosiči informací. Je však zcela bez významu, jestli pachatel získal přístup neoprávněně ve smyslu překonání bezpečnostního opatření dle § 230 odst. 1 TZ či takový přístup získal zcela oprávněně. Oproti první skutkové podstatě je zde objektem spíše integrita a dostupnost počítačových systémů a dat. Aby mohlo dojít k naplnění objektivní stránky, musí pachatel naplnit svým jednáním jednu ze čtyř alternativ uvedených pod písmeny a) až d). První z nich postihuje jednání spočívající v neoprávněném užití dat, které bývá taktéž označováno jako počítačová špionáž. Takovým užitím je například zpřístupnění získaných dat jiným osobám. Písmeno b) postihuje neoprávněné vymazání či jiné zničení, poškození, změnu, snížení kvality nebo učinění dat neupotřebitelnými. Všechny tyto způsoby jsou označovány jako počítačová sabotáž. Třetí činnost, které se pachatel může dopustit, je padělání nebo pozměnění dat. *„Vychází se z myšlenky, že stále více informací má dnes elektronickou podobu, a proto je zapotřebí chránit je před padělám. Zatímco padělaná listina je mnohdy rozeznatelná od originální, při změně dat*

[70] KANDOVÁ, Katarína. Neoprávněný přístup k počítačovému systému a nosiči informací - § 230. In: ŠČERBA, Filip a kolektiv. *Trestní zákoník – komentář (§ 205–421)*. Praha: C. H. Beck, 2020, s. 1881–1882. ISBN 978-80-7400-807-8.

není padělání zjevné. O to je nebezpečnější.“[71] Posledním druhem jednání je neoprávněné vložení dat nebo učinění jiného zásahu do programového nebo technického vybavení počítače. Obdobně jako v prvním odstavci § 230 TZ, je i zde vyžadována úmyslná forma zavinění.

V souvislosti s neoprávněným přístupem k počítačovému systému a nosiči informací bývá mnohdy uváděna problematika trestního postihu (D)DoS útoků jakožto útoků zahlcujících servery opakovaným zasíláním nadměrného množství požadavků. Musíme však zmínit, že trestněprávní klasifikace (D)DoS útoků není v současné době nijak jednotná, a tedy ani nikterak jednoduchá. Nejvyšší soud ve své rozhodovací praxi uzavřel, že pokus provedení DDoS útoku splňuje všechny znaky trestného činu dle § 230 odst. 1 TZ.[72] S takovým tvrzením se nicméně nelze příliš ztotožnit, neboť v případě útoku (D)DoS útočník nepřekonává žádná bezpečnostní opatření ani nezískává přístup k počítačovému systému. Mnohdy se obrazně, nicméně výstižně uvádí, že (D)DoS útočník zůstává „před branami“, nezískává přístup k počítačovému systému a z toho důvodu není § 230 odst. 1 TZ možné aplikovat. Z uvedených důvodů je potřeba vyloučit i druhou základní skutkovou podstatu uvedenou v § 230 odst. 2 písm. b) TZ, neboť ani zde nebude splněna podmínka získání přístupu k počítačovému systému, ačkoliv útočník svým jednáním zcela jistě data v počítačovém systému učiní neupotřebitelnými, případně sníží jejich kvalitu. Přiléhavější řešení nabízí ustanovení § 230 odst. 3 písm. b) TZ, které říká, že pachatel svým neoprávněným jednáním omezí funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat. Taková definice se jeví jako perfektní a zcela odpovídající popisu (D)DoS útoku, nicméně odstavec třetí představuje kvalifikovanou skutkovou podstatu, a proto bude nezbytné naplnit vůbec jednu ze základních skutkových podstat uvedených v § 230 TZ, což může vzhledem k interpretaci, činit nemalé potíže.

Osobně jsem toho názoru, že v případě klasifikace (D)DoS útoků by bylo možné brát v potaz i ustanovení trestného činu poškození cizí věci ve smyslu § 228 TZ, a to za předpokladu, že napadený server se v důsledku útoku stane věcí neupotřebitelnou a vznikne škoda nikoliv nepatrná. Alternativně lze spekulovat o aplikaci § 276 TZ, eventuálně § 277 TZ, v případě, kdy by útokem došlo k poškození a ohrožení provozu obecně prospěšného zařízení, respektive spíše informačního systému obecně prospěšného zařízení.

[71] GŘIVNA, Tomáš. Neoprávněný přístup k počítačovému systému a nosiči informací - § 230. In: ŠÁMAL, Pavel a kolektiv. *Trestní zákoník II – komentář. Zvláštní část (§ 140–421)*. 2. vydání. Praha: C. H. Beck, 2012, s. 2311. ISBN 978-80-7400-428-5.

[72] Usnesení Nejvyššího soudu ze dne 13. 2. 2019, sp. zn. 8 Tdo 100/2019.

Úmluvou o počítačové kriminalitě ve spojení taktéž se směrnicí o útocích na informační systémy[73] mělo dojít k jednotnému postižení (D)DoS útoků prostředky trestněprávních norem. Vzhledem k tomu, že Česká republika tento závazek do svého právního řádu neimplementovala zcela přiléhavě, vzniklo v praxi nemálo aplikačních potíží. De lege ferenda by bylo žádoucí trestní zákoník rozšířit o novou skutkovou podstatu postihující podstatu (D)DoS útoků a mimo jiné tak vhodněji reagovat na požadavky plynoucí z mezinárodních závazků.

4.3.3. Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 TZ)

Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat je předčasně dokonaným trestným činem, jehož objektem je důvěrnost dopravovaných zpráv prostřednictvím sítě elektronických komunikací (§ 182 odst. 1 písm. b), c) TZ) nebo důvěrnost uložených dat v počítačovém systému (§ 230 odst. 1, 2 TZ). Vzhledem k tomu, že výše uvedená chráněná práva jsou taktéž garantována v LZPS, konkrétně v článku 13, je zde kladen větší důraz na jejich ochranu. Za tímto účelem zákon kriminalizuje již ohrožení zmíněných práv. Objektivní stránka sestává z různých jednání, jako je příkladmo výroba, uvedení do oběhu, vyvezení, provezení, nabízení, zprostředkování, prodání či přechovávání zařízení nebo počítačového hesla. Daný trestný čin navíc vyžaduje z hlediska zavinění specifický úmysl, tedy spáchat jednáním trestný čin uvedený v § 182 odst. 1 písm. b), c) TZ nebo § 230 odst. 1, 2 TZ. Pachatelem pak může být kterákoliv odpovědná osoba.[74]

4.3.4. Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232 TZ)

Dané ustanovení bylo do trestního zákoníku včleněno nad rámec požadavků plynoucích z mezinárodního společenství, zejména nad rámec Úmluvy o počítačové kriminalitě. *„Objektem trestného činu podle § 232 je ochrana dat a technického či programového vybavení počítače (jiného technického zařízení pro zpracování dat) před nedbalostním poškozovacím jednáním, pokud je těmito zásahy způsobena značná škoda.“*[75] Pachatelem v daném případě bude osoba,

[73] Směrnice Evropského parlamentu a Rady 2013/40/ES ze dne 12. 8. 2013 o útocích na informační systémy.

[74] KANDOVÁ, Katarína. Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat - § 231. In: ŠČERBA, Filip a kolektiv. *Trestní zákoník – komentář (§ 205–421)*. Praha: C. H. Beck, 2020, s. 1893–1898. ISBN 978-80-7400-807-8.

[75] GŘIVNA, Tomáš. Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti - § 232. In: ŠÁMAL, Pavel a kolektiv. *Trestní zákoník II – komentář. Zvláštní část (§ 140–421)*. 2. vydání. Praha: C. H. Beck, 2012, s. 2322. ISBN 978-80-7400-428-5.

která z hrubé nedbalosti poruší jí svěřenou povinnost vyplývající ze zaměstnaní, povolání, postavení nebo funkce nebo uloženou dle zákona či smluvně převzatou.[76] Typicky se může jednat například o zaměstnanecké využívání pracovních zařízení pro vlastní privátní účely. Aktuálním narůstajícím trendem, který by mohl vést k naplnění skutkové podstaty daného trestného činu, je BYOD[77] (Bring Your Own Device).

Závěrem lze shrnout, že trestné činy uvedené v § 230, § 231 a § 232 TZ bývají naukou často označovány jako počítačové trestné činy. Podle statistických údajů se nicméně jedná o skupinu trestných činů, jejichž objasněnost patří k těm nejnižším. V průběhu let 2017-2021 se míra jejich objasněnosti pohybovala kolem 18 %.[78]

4.4. Trestné činy hospodářské

4.4.1. Neoprávněné opatření, padělání a pozměnění platebního prostředku (§ 234 TZ)

Ustanovení § 234 TZ chrání tuzemské a zároveň cizozemské platební prostředky, čímž zajišťuje ochranu fungování platebního styku, především pak styku bezhotovostního, což v širším kontextu sleduje řádné fungování tržního hospodářství. Typickými platebními prostředky jsou platební karty, směnky, šeky, elektronické peníze, dokumentární akreditivy a inkasa. Objektivní stránka sleduje opatření, zpřístupnění, příjem nebo přechovávání cizího platebního prostředku. Druhý odstavec postihu opatření si, zpřístupnění, přijetí a přechovávání padělaného nebo pozměněného platebního prostředku. Poslední odstavec pak kriminalizuje jednání pachatele, který padělá nebo pozmění platební prostředek s úmyslem použít jej jako pravý nebo platný, nebo pachatel prostředek použije jako pravý nebo platný.[79]

Vzhledem k tomu, že v současnosti drtivá většina platebního styku probíhá bezhotovostně, bývají jedním z nejčastějších terčů kybernetických útoků elektronické peníze, které si lze představit jako

[76] Paragraf 232 TZ vylučuje jednočinný souběh s trestným činem porušení povinnosti při správě cizího majetku z nedbalosti podle § 221 TZ, neboť ustanovení § 232 TZ je speciální.

[77] BYOD v doslovném překladu znamená „přines si své vlastní zařízení“. Zaměstnanci k práci využívají vlastní výpočetní techniku, což pro zaměstnavatele z hlediska kyberbezpečnosti může představovat nezanedbatelné riziko.

[78] POLICIE ČR. Kriminalita – Statistické přehledy. In: *Policie.cz* [online]. [cit. 2022-06-15]. Dostupné z: https://www.policie.cz/statistiky-kriminalita.aspx

[79] ŠÁMAL, Pavel. Neoprávněné opatření, padělání a pozměnění platebního prostředku - § 234. In: ŠÁMAL, Pavel a kolektiv. *Trestní zákoník II – komentář. Zvláštní část (§ 140–421)*. 2. vydání. Praha: C. H. Beck, 2012, s. 2363–2365. ISBN 978-80-7400-428-5.

virtuální ekvivalent k tradiční hotovosti. Legální definici nalezneme v zákoně č. 370/2017 Sb., o platebním styku, konkrétně v § 4, který je definuje jako:

a) peněžní hodnotu představující pohledávku vůči tomu, kdo ji vydal
b) hodnotu uchovávanou elektronicky
c) hodnotu vydávanou proti přijetí peněžních prostředků za účelem provádění platebních transakcí
d) přijímanou jinou osobou než tou, která je vydala.

Problematika je také řešena i na evropské úrovni, a to směrnicí Evropského parlamentu a Rady 2009/110/ES ze dne 16. září 2009 o přístupu k činnosti institucí elektronických peněz, o jejím výkonu a o obezřetnostním dohledu nad touto činností a též směrnicí Evropského parlamentu a Rady 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu.

K trestnému činu neoprávněného opatření, padělání a pozměnění platebního prostředku dochází v oblasti kyberprostoru především u home bankingu[80]. Ověření totožnosti u internetových bankovnictví zabezpečuje zpravidla přístupové heslo společně s potvrzujícím autorizačním kódem zasílaným bankou. Padělání platebního prostředku se dopustí pachatel tehdy, jestliže bez vědomí majitele bankovního účtu užije jeho správných přihlašovacích údajů, čímž pronikne do jeho internetového bankovnictví, kde bez oprávnění vydá platební příkaz.[81] Praxe obdobně poukázala na časté jednočinné souběhy trestných činů podle § 234 odst. 3, § 230 odst. 2 a § 209 TZ.[82]

Dalším typem útoku naplňujícího skutkovou podstatu daného trestného činu je skimming, tedy neoprávněné kopírování údajů z platební karty. Nicméněně vzhledem k narůstající oblibě virtuálních platebních karet[83]počet útoků skimmingu klesá.

4.4.2. Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi (§ 270 TZ)

Co se týče systematického zařazení § 270 TZ, umístil ho zákonodárce do skupiny hospodářských trestných činů, ačkoliv primárním objektem je zde spíše zájem na ochraně práva osobnostního a majetkového. Předmětné ustanovení chrání zejména „*vědeckou a literární, hudební, výtvarnou,*

[80] Home banking (domácí bankovnictví) umožňuje majiteli bankovního účtu převádět peněžní transakce prostřednictvím programu v počítači.
[81] Usnesení Nejvyššího soudu ze dne 18. 1. 2012, sp. zn. 6 Tdo 1677/2011.
[82] Usnesení Nejvyššího soudu ze dne 16. 5. 2018, sp. zn. 4 Tdo 456/2018.
[83] Virtuální platební karty jsou nehmotným ekvivalentem klasické fyzické platební karty. Uživatel ji zpravidla nahrává do mobilního telefonu či na chytré hodinky pomocí Apple Pay či Google Pay.

audiovizuální a jinou uměleckou tvůrčí činnost a požitky z ní plynoucí, ale i práva výrobců zvukového záznamu a zvukově obrazového záznamu, dále práva rozhlasového a televizního vysílatele a práva pořizovatele databáze".[84] Nutno doplnit, že ochrany nepožívají pouze díla dokončená, ale též jejich jednotlivé fáze. Abychom mohli hovořit o porušení autorského práva a práv souvisejících s právem autorským, musí dojít ke splnění té podmínky, že pachatel zasáhne do zákonem chráněného práva v míře nikoliv nepatrné. Zásah v takové intenzitě je nutné chápat komplexně, a tudíž nevztahovat pouze na způsobenou výši škody. Nejvyšší soud judikoval, že je zapotřebí posuzovat intenzitu a délku zásahu, způsob jeho provedení včetně následku a také přihlédnout k osobě samotného pachatele.[85] Naopak za nepatrný zásah by mohl být považován ojedinělý nebo nevýznamný zásah do práva, přičemž by v takovém případě postačilo uplatnění odpovědnosti podle norem správního práva.[86] Dispozice normy trestného činu v § 270 TZ, obdobně jako u jiných hospodářských trestných činů, je blanketního charakteru, tedy odkazuje na jiný, mimotrestní předpis, kterým je zde myšlen zejména zákon č. 121/2000 Sb., autorský zákon (AZ).

V souvislosti s neustálým rozšiřováním technických, zvláště pak komunikačních prostředků se pachatelům naskytla nová škála možností k nelegálnímu šíření autorských děl. V návaznosti na to se soudy musely vypořádat s nelehkými a poměrně komplikovanými otázkami ohledně sdílení autorských děl za pomoci internetových odkazů. Problematika byla opakovaně řešena Nejvyšším soudem, který ve své rozhodovací praxi začal rozlišovat mezi sdílením děl pomocí prostých odkazů a sdílením tzv. embedded links (embedovaných odkazů). V případě prostého odkazu jsou uživatelům zpřístupněny pouze informace o umístění díla, naopak u embedovaného odkazu[87] je sdílen i jeho samotný obsah. *„Podle názoru Nejvyššího soudu je tedy metoda vloženého kódu, tzv. embedding, přímým prostředkem sdělování díla nebo jeho rozmnoženiny veřejnosti, protože umožňuje, že kdokoli může mít k chráněnému dílu či jeho rozmnožení přístup na místě a v čase podle své vlastní volby zejména počítačovou nebo obdobnou sítí."*[88] Za neoprávněný zásah ve smyslu § 270 TZ, označil také Nejvyšší soud jednání pachatele, který na svých webových stránkách umisťoval a následně ponechával embedded links odkazující na téměř 2 500

[84] ŠÁMAL, Pavel. Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi - § 270. In: ŠÁMAL, Pavel a kolektiv. *Trestní zákoník II – komentář. Zvláštní část (§ 140–421)*. 2. vydání. Praha: C. H. Beck, 2012, s. 2737. ISBN 978-80-7400-428-5.
[85] Usnesení Nejvyššího soudu ze dne 12. 3. 2014, sp. zn. 5 Tdo 196/2014.
[86] ŠÁMAL, Pavel. Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi - § 270. In: ŠÁMAL, Pavel a kolektiv. *Trestní zákoník II – komentář. Zvláštní část (§ 140–421)*. 2. vydání. Praha: C. H. Beck, 2012, s. 2752. ISBN 978-80-7400-428-5.
[87] Pomocí embedded links je uživatelům umožněno navštěvovat webovou stránku včetně jejího obsahu, bez toho, aniž by uživatel opustil stránku, na které byl embeddovaný odkaz umístěn.
[88] Usnesení Nejvyššího soudu ze dne 29. 5. 2013, sp. zn. 5 Tdo 271/2013.

audiovizuálních děl. Odkazy posléze umožnily komukoliv přístup k dílům na místě a v čase dle vlastní potřeby, tedy došlo k sdělování díla veřejnosti ve smyslu § 18 odst. 2 AZ.[89]

Nejasná povahou embeddingu a otázka zveřejňování děl veřejnosti byla navíc precizována i Soudním dvorem Evropské unie, který ovšem rozlišování mezi jednotlivými druhy odkazů v podstatě vyloučil. V usnesení SDEU ve věci Best Water International Gmbh proti Michael Mebes a Stefan Potsch (věc C-348/13) bylo řečeno, že pokud je chráněné dílo volně zpřístupněno na webových stránkách, a to i za předpokladu, že na stránku bylo vloženo pomocí metody tzv. framingu, nelze na takové jednání pohlížet ve smyslu „sdělování veřejnosti" definovaného v čl. 3 odst. 1 směrnice Evropského parlamentu a Rady 2011/29/ES ze dne 22. května 2001 o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti, jestliže tak dílo nebylo sdělováno nové veřejnosti a ke sdělení nedošlo za použití technologie odlišující se od technologie původního sdělování.[90] O tři roky později SDEU došel k závěru, že *„za účelem posouzení, zda umístění hypertextových odkazů na internetové stránce na chráněná díla, která jsou volně dostupná na jiné internetové stránce bez souhlasu nositele autorského práva, představuje „sdělování veřejnosti" ve smyslu [čl. 3 odst. 1 směrnice], je třeba určit, zda byly tyto odkazy poskytnuty nikoli za účelem dosažení zisku osobou, která nevěděla nebo nemohla rozumně vědět o protiprávní povaze zveřejnění těchto děl na této jiné internetové stránce, nebo zda naopak byly poskytnuty za účelem dosažení zisku, v kterémžto případě musí být taková znalost presumována".*[91]

4.5. Trestné činy proti České republice, cizímu státu a mezinárodní organizaci

4.5.1. Teroristický útok (§ 311 odst. 1 písm. a), § 311 odst. 1 písm. e) TZ)

Boj proti terorismu se po událostech ze dne 11. září 2011 stal i pro Evropskou unii jedním ze strategických cílů. Zákonodárce musel úpravou reagovat na požadavky z mezinárodních závazků vyplývajících z rámcového rozhodnutí Rady EU o boji proti terorismu. Rámcové rozhodnutí Rady EU, které bylo v roce 2016 nahrazeno směrnicí Evropského parlamentu a Rady 2017/541 o boji proti terorismu, reagovalo na možnost teroristického útoku prostřednictvím kyberprostoru. Směrnice tak pojem teroristického útoku doplnila o kybernetické útoky, které jsou páchány se

[89] Usnesení Nejvyššího soudu ze dne 27. 2. 2013, sp. zn. 8 Tdo 137/2013.
[90] Usnesení SDEU ze dne 21. 10. 2014 ve věci BestWater International GmbH proti Michael Mebes a Stefan Potsch (Věc-348/13).
[91] Rozsudek SDEU ze dne 8. 9. 2016 ve věci GS Media BV proti Sanoma Media Netherlands BV a další (Věc C-160/15).

zvláštním teroristickým úmyslem. Do nabytí účinnosti novely trestního zákoníku, do 1. února 2019, byly obdobné útoky postihovány podle trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 TZ.[92]

Ustanovení § 311 TZ odkazuje ve dvou rovinách na možné kybernetické útoky. První útok, spočívající ve zničení nebo poškození počítačového systému ve větší míře, na jehož fungování závisející zařízení, systém nebo plošina, s cílem vydat majetek v nebezpečí škody velkého rozsahu, je definován v § 311 odst. 1 písm. a) TZ. Písm. e) zmíněného ustanovení postihuje tři druhy různých útoků, a to (1) útoky proti počítačovým systémům, jejichž narušení má zásadní dopad na fungování státu, bezpečnost, zdraví nebo zajištění základních životních potřeb, dále (2) útoky mající dopad na větší počet počítačových systémů s tím, že jsou k tomu využity přizpůsobené počítačové programy a o (3) útoky působící značnou škodu. Aby byla naplněna skutková podstata, musí být tyto zmíněné typy útoků provedeny konkrétním způsobem, a to: vymazáním, zničením, poškozením, změnou nebo potlačením dat uložených v počítačovém systému nebo nosiči informací, dále pak snížením kvality počítačových dat nebo jejich znepotřebněním nebo vložením dat do počítačového systému.

Ačkoliv kyberterorismus nezpochybnitelně představuje velmi závažný typ útoku s obrovským kriminálním potenciálem, nelze tvrdit, že na tuzemské úrovni by se v současné době jednalo o expandující jev. Ba dokonce lze konstatovat, že ačkoliv je ochraně před kyberterorismem věnována pozornost i na globální úrovni, k žádnému takovému útoku doposud nedošlo. Možné důvody uvádí Drmola. Vzhledem k absenci fyzického násilí a výbušnin podle něj kybernetickým útokům absentuje tradiční symbolický efekt. Dále je to tím, že takové útoky vyžadují poměrně dlouhou a náročnou přípravu a potřebné znalosti o cílových systémech. Za relevantní argument se ale dá považovat spíše fakt, že většina kritických informačních systémů, je opatřena tzv. air gap technologií[93], která kybernetický útok velmi znesnadňuje a pro narušení je zpravidla vyžadována fyzická přítomnost pachatele.[94] Zahraniční literatura určila pět esenciálních atributů, které musí být splněny, aby se jednalo o kyberterorismus. Podmínky jsou následující: (1) cílem útoku je

[92] Důvodová zpráva k zákonu č. 287/2018 Sb. kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a některé další zákony, č. 287/2018 Dz.

[93] Air gap technologie fungující na principu fyzické izolace kritické infrastruktury mimo internetové připojení a lokální síť. Data na počítačových systémech tak mohou být přenášena ryze fyzicky (např. pomocí USB). Air gap bývá často využíván u vojenských, vládních, průmyslových počítačových systémů a dále u systémů jaderných elektráren apod. Nicméně je nutné zmínit, že ani tak se nejedná o neprolomitelnou techniku. In: NOHE, Patrik. What is an Air Gapped Computer? In: *hashedout by The SSL Store* [online]. 13. března 2018 [cit. 2022-06-11]. Dostupné z: https://www.thesslstore.com/blog/air-gapped-computer/

[94] DRMOLA, Jakub. Konceptualizace kyberterorismu. *Vojenské rozhledy*. 2013, č. 2, s. 99–100. ISSN 1210-3292.

narušit funkčnost počítačových systémů, (2) útok sleduje politický účel, (3) pachatel není státní subjekt, (4) účinky útoku jsou rovnocenné s ozbrojeným teroristickým útokem a (5) jde o porušení norem trestního práva pomocí počítačového systému.[95] Podle některých autorů tak žádný ze zatím provedených kybernetických útoků (např. útoky Anonymous či Stuxnet) nesplňoval všechny výše uvedené podmínky, a nelze tak hovořit o kyberterorismu v pravém slova smyslu.[96]

4.6. Trestné činy proti pořádku ve věcech veřejných

4.6.1. Nebezpečné pronásledování (§ 354 TZ)

Trestný čin nebezpečného pronásledování byl do české právní úpravy včleněn trestním zákoníkem č. 40/2009 Sb. do hlavy X,[97] v rámci tzv. anti-stalkingové legislativy. Objektem je zde zájem na ochraně nerušeného soužití mezi osobami, konkrétně pak ochrana osobní svobody a soukromí jedince.[98] *„Objektivní stránku přečinu představuje jednání spočívající v dlouhodobém pronásledování prováděné taxativně vymezenými formami, které jsou způsobilé v jiném vzbudit důvodnou obavu o jeho život nebo zdraví nebo o život a zdraví osob jemu blízkých. Společným jmenovatelem těchto forem je v souhrnu záměr jiného obtěžovat tak intenzivně, že to již ohrožuje jeho psychickou a v některých případech i fyzickou integritu.“*[99] Z hlediska zavinění je pak vyžadován úmysl, zpravidla téměř vždy úmysl přímý.

Nebezpečné pronásledování se zejména v zahraniční literatuře označuje termínem stalking. Specifickou formou stalkingu uskutečňovaného prostřednictvím kyberprostoru, je kyberstalking. Ačkoliv definice kyberstalkingu není jednotná, chápeme jej jako opakující se pronásledování a obtěžování osoby pomocí telekomunikačního zařízení nebo internetu, a to takovým způsobem, který v oběti vyvolává pocit nebezpečí nebo strachu.[100] Oproti tradičnímu stalkingu, využívá kyberstalker anonymizačních nástrojů na internetu (např. anonymních e-mailů), které znesnadňují oběti, potažmo orgánům činným v trestním řízení (OČTŘ) odhalit pachatelovu identitu. Mimo to

[95] HATHAWAY, Oona A., Rebecca CROOTOF, Philip LEVITZ, Haley NIX, Aileen NOWLAN, William PERDUE a Julia SPIEGEL. The Law of Cyber-Attack. *California law review*. Berkeley: Joe Christensen, Inc. for students of School of Law, University of California, Berkeley, 2012, 100(4), s. 833. ISSN 0008-1221.

[96] KENNEY, Michael. Cyber-Terrorism in a Post-Stuxnet World. *Orbis (Philadelphia)*. 2015, roč. 59, č. 1, s. 123–124. ISSN 0030-4387. Dostupné z: doi:10.1016/j.orbis.2014.11.009

[97] Vzhledem k systematice zvláštní části trestního zákoníku, je otázkou, proč nebyl trestný čin nebezpečného pronásledování z hlediska věcné blízkosti zařazen spíše do hlavy II – Trestné činy proti svobodě a právům na ochranu osobnosti, soukromí a listovního tajemství.

[98] VÁLKOVÁ, Helena. Nebezpečné pronásledování - § 354. In: ŠÁMAL, Pavel a kolektiv. *Trestní zákoník II – komentář. Zvláštní část (§ 140–421)*. 2. vydání. Praha: C. H. Beck, 2012, s. 3293. ISBN 978-80-7400-428-5.

[99] Usnesení Nejvyššího soudu ze dne 17. 12. 2013, sp. zn. 4 Tdo 1333/2013.

[100] CHANG, Wei-jung. Cyberstalking and Law Enforcement. *Procedia Computer Science*. Elsevier B.V, 2020, 176, s. 1190. ISSN 1877-0509. Dostupné z: doi:10.1016/j.procs.2020.09.115

může pachatel vystupovat pod několika falešnými identitami, a tedy vzbuzovat dojem útoku vyvolaného více osobami.

Co se týče kriminalizace jednání v podobě kyberstalkingu, subsumuje ho trestní zákoník pod § 354 odst. 1 písm. c) TZ. *„I pro toto jednání samozřejmě platí obecné znaky nebezpečného pronásledování, jež jsou společné všem formám jednání. Společnými znaky pro všechny formy jednání taxativně vypočtené v písmenech a) až e) je dlouhodobé pronásledování, které je způsobilé vzbudit důvodnou obavu o život nebo zdraví nebo o život a zdraví osob blízkých.“*[101] K atributu dlouhodobosti se nicméně vyjádřila nauka tak, že pachatel se musí alespoň desetkrát pokusit o kontakt s obětí během časového úseku minimálně čtyř týdnů.[102] Ani judikatura hranici dlouhodobosti přesně nedefinovala, pouze stanovila, že podmínku dlouhodobosti nebude splňovat sporadické nebo náhodné kontaktování oběti.[103] V takových případech bychom mohli uvažovat především o postihu podle norem správního práva, konkrétně podle zákona č. 251/2016 Sb., o některých přestupcích.

Pachatelem kyberstalkingu bývá v drtivé většině případů bývalý partner oběti. Takové jednání vykazuje jistě vyšší míru škodlivosti, neboť pachatel zná oběť a může cíleně využívat informace o ní získané během předchozího vztahu. S ohledem na uvedené by de lege ferenda bylo efektivní, aby kvalifikovaná skutková podstata nějakým způsobem reflektovala předchozí vztah pachatele a oběti, ačkoliv z hlediska prokazování existence takového vztahu se toto řešení jeví jako těžko proveditelné.

[101] SÝKORA, Michal. Trestní postih cyberstalkingu. *Acta Universitatis Carolinae – Iuridica*. 2012, č. 4, s. 98. ISSN 0323-0619.
[102] VANTUCH, Pavel. K postihu stalkingu (nebezpečného pronásledování) podle § 354 trestního zákoníku. *Trestní právo*. 2011, roč. 16, č. 2, s. 5–13.
[103] Usnesení Nejvyššího soudu ze dne 8. 9. 2011, sp. zn. 8 Tdo 1082/2011.

5. ODHALOVÁNÍ A VYŠETŘOVÁNÍ KYBERKRIMINALITY

S ohledem na variabilitu a dynamičnost nelegálních aktivit v kyberprostoru, se musela kriminalistika vypořádat s nedostatečností běžných vyšetřovacích metod a postupů. Z tohoto důvodu byly v rámci snahy odhalit pachatele vytvořeny speciální, modifikované kriminalistické metody, které mají celý proces odhalování a vyšetřování urychlit ve snaze odhalit pachatele.

5.1. Pachatelé

K pojmu pachatele kybernetické trestné činnosti byl praxí i teorií zaveden termín hacker. Ačkoliv původně hacker označoval osobu, která pracovala s nábytkem, byla definice s postupem času přizpůsobena moderní době a hackera dnes chápeme již jako osobu, která má oblibu ve zkoumání detailů programovatelných systémů a hledající jejich slabiny. Podle slovníku jde i o osoby mající rády intelektuální výzvy spočívající v obcházení bezpečnostních omezení.[104]

Množina pachatelů kyberzločinu je díky neustálému technickému rozvoji velmi široká a zahraniční i tuzemští autoři dělí hackery do rozličných skupin podle nejrůznějších kritérií. Jedno z dělení představil Marcus Rogers, který rozděluje hackery do osmi skupin v závislosti na jejich znalostech a sledovaných cílech, a to na:

1. nováčky (Script kiddies/Novice/Newbie – NV);
2. kyber-punkery (Cyber-punks – CP);
3. zaměstnance (Internals – IN);
4. drobné zlodějíčky (Petty Thieves – PT);
5. autory virů (Virus Writers – VW);
6. starou hackerskou gardu (Old guard hackers – OG);
7. profesionály (Professional criminals – PC);
8. informační bojovníky (Information Warriors – IW).[105]

Nováčci jsou podle něj osoby, jejichž programovací schopnosti a znalosti výpočetní techniky jsou omezené vzhledem k jejich často nízkému věku. Jde o začínající hackery, kteří se snaží začlenit do hackerské subkultury a jejichž motivací bývá hledání vzrušení a nabuzení ega. Faktory nízkých

[104] RAYMOND, Eric. *The New Hacker's Dictionary*. [b.m.]: MIT Press, 1996. s. 233–234. ISBN 0-262-68069-6.
[105] ROGERS, Marcus K. A Two-dimensional Circumplex Approach to the Development of a Hacker Taxonomy. *Digital investigation*. 2006, roč. 3, č. 2, s. 97–102. ISSN 1742-2876. Dostupné z: doi:10.1016/j.diin.2006.03.001

technických znalostí a touhy předvést se tvoří nebezpečnou kombinaci, v důsledku čehož mohou vzniknout rozsáhlé škody.[106]

Kyber-punkeři již disponují pokročilejšími dovednostmi a určitými programátorskými schopnostmi. V omezené míře jsou i schopni napsat vlastní software. Pozornost zaměřují na poškozování webových stránek, na spamming a také na krádeže údajů obsažených na kreditních kartách. Primární motivací skupiny je mediální pozornost, a proto jsou častými oběťmi kyber-punkerů jsou mediálně známé osoby či politicky exponované osoby. Sekundární motivací je pak finanční zisk.[107]

Třetí skupinou jsou zaměstnanci či bývalí zaměstnanci, jejichž primární motivací je pomsta zaměstnavateli. Taková skupina pak může být nebezpečnější než jiná zejména kvůli znalostem, které zaměstnanec během své pracovní kariéry shromáždil. Statistiky uvádí, že až 60 % úniků dat je způsobeno útokem zevnitř a počty kybernetických bezpečnostních incidentů se každoročně zvyšují.[108]

Drobní zlodějíčci se zaměřují především na oblasti online kreditních karet a zneužívání přihlašovacích údajů a hesel běžných koncových uživatelů internetu. Dominantní motivací je finanční zisk, chamtivost, v některých případech i msta. Naopak u nich absentuje zájem o mediální pozornost.[109]

Stará hackerská garda je skupina, jejíž technické dovednosti a znalosti dosahují vysoké úrovně. Ačkoliv sice sami nevykazují kriminální chování, nepřímo svými zveřejňovanými kódy podporují ostatní hackery. Hlavní motivací jsou pro ně intelektuální výzvy a zvědavost.

Autoři virů jsou poněkud specifickou skupinou hackerů. Gordon uvádí, že u této skupiny lze spatřovat určitý cyklus. Jedinci dle ní skupinu opouští, jakmile dosáhnou středního věku, a následně jsou nahrazeni novými, mladými, a ne tak zkušenými nástupci.[110]

---

[106] ROGERS, Marcus K. A Two-dimensional Circumplex Approach to the Development of a Hacker Taxonomy. *Digital investigation*. 2006, roč. 3, č. 2, s. 97–102. ISSN 1742-2876. Dostupné z: doi:10.1016/j.diin.2006.03.001

[107] Ibid.

[108] GILBERT, Nestor. 31 Crucial Insider Threat Statistics: 2022 Latest Trends & Challenges. In: *FinancesOnline* [online]. 2022 [cit. 2022-05-26]. Dostupné z: https://financesonline.com/insider-threat-statistics/

[109] ROGERS, Marcus K. A Two-dimensional Circumplex Approach to the Development of a Hacker Taxonomy. *Digital investigation*. 2006, roč. 3, č. 2, s. 97–102. ISSN 1742-2876. Dostupné z: doi:10.1016/j.diin.2006.03.001

[110] GORDON, Sarah. The Virus Writer and The Reporter. *Information security technical report*. 2001, roč. 6(4), s. 79. ISSN 1363-4127. Dostupné z: doi:10.1016/S1363-4127(01)00408-3

Profesionálové a informační bojovníci jsou zcela nepochybně nejnebezpečnější skupinou. V obou případech se jedná o odborníky, kteří využívají nejmodernější technické vybavení. Navzdory nebezpečnosti ze strany profesionálních zločinců o nich víme poměrně málo. Jirovský skupinu profesionálů rozděluje navíc pomocí kloboukového dělení[111] na tzv. white, grey a black hats.[112] White hats („bíle klobouky"), přezdívaní také etičtí hackeři, jsou zpravidla zaměstnávaní firmami, a to za účelem odhalení bezpečnostních chyb v softwarech. Black hats („černé klobouky") naopak vyvíjí nelegální aktivitu a pronikají do informačních systémů bez souhlasu jejich vlastníka za účelem získání dat. Poslední z nich grey hats („šedé klobouky") stojí někde na pomezí obou zmíněných skupin. Pravděpodobně jde o skupinu, která vznikla jako doplněk v klasifikaci hackerů a chápeme ji jako dočasné období začínajícího hackera, který ještě nemá své budoucí směřování určeno.[113]

Poměrně specifickou skupinou pachatelů, nicméně už prizmatem mezinárodního práva veřejného, je samotný stát. Abychom mohli označit stát jako pachatele kybernetického útoku, je zapotřebí vyřešit otázku přičitatelnosti. Podle mezinárodního práva se presumuje přičitatelnost státu u jednání státních orgánů, případně osob, které jednají jako zmocněnci státu. U nestátních aktérů lze hovořit o přičitatelnosti, jestliže stát měl nad pachatelem účinnou kontrolu.[114] Nesporně zde praxe v těchto situacích narazí na důkazní nouzi. V neposlední řadě bude kybernetický útok přičitatelný státu, pokud jej stát schválí a přijme za vlastní.[115]

Závěrem je zajímavé ke kategorizaci pachatelů uvést i genderové rozložení. Uvádí se, že kyberkriminalitě silně dominují mužští pachatelé, což je odůvodňováno obecně nízkým počtem žen v oblasti výpočetní techniky a IT. Někteří autoři poukazují na to, že nelegální aktivity v oblasti počítačové kriminality se mohou pomyslně dělit na činy technického rázu nebo činy spíše obecné,

[111] Kloboukové dělení pochází ze starších westernových filmů, kde hrdina nosil bílý nebo světlý klobouk, zatímco záporný hrdina měl klobouk černý. Časem bylo vytvořeno i několik dalších kategorií, jako green hat (nový, nezkušený hacker), blue hat (mstivý hacker) a red hat (agresivní hackeři soupeřící s black hats).

[112] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, s. 54–55. ISBN 978-80-247-1561-2.

[113] Ibid., s. 55.

[114] Rozsudek Mezinárodního soudního dvora ze dne 27. 6. 1986, Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). International Court of Justice Reports, 1986. s. 54–55.

[115] International Law Commission. Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries. Yearbook of the International Law Commission. 2001, vol. II, Part Two.

netechnické povahy (jako např. shoulder surfing)[116], přičemž ženám jsou přiřazovány spíše tyto méně technicky zaměřené aktivity.[117]

5.2. Motiv

Motivovaný útočník tvoří společně s vhodným cílem a nedostatečnou ochranou triádu, která vede k nezákonným aktivitám.[118] Z toho důvodu je zapotřebí porozumět motivacím, které jsou základem jednání hackerů. Porozumění motivaci přinese velkou výhodu nejenom OČTŘ, nýbrž i samotným technologickým vývojářům, kteří tak budou moci aplikovat vhodnější bezpečnostní opatření.

Vycházíme-li z premisy, že hackeři jsou stále jen lidé, a tudíž jsou jako všichni ovládáni racionálním i iracionálním chováním, je pro pochopení motivace nutné vycházet z poznatků behaviorální psychologie. Jednou z teorií, kterou se behaviorální vědy snaží objasnit kriminální chování kyberzločinců, je Beverenův model vývoje hackera. Beveren rozdělil motivace do čtyř skupin: a) nutkání k hackingu, b) zvědavost, c) pocit kontroly a touha po moci, d) uznání vrstevníků a sounáležitost ke skupině. Dále podle něj většina hackerů začíná jako nováčci, nicméně s postupem času se stávají poloprofesionály, neboť prohlubují získané znalosti a dovednosti. Tím poukazuje, že s rozvíjením dovedností, se vyvíjí i motivace.[119]

V praxi bylo představeno hojné množství různých studií a výzkumů snažících se o obecnou klasifikaci motivů hackerů. Taylor a Jordan rozlišují šest kategorií – závislost na počítačích, zvědavost, moc nad systémem, vzrušení z nelegální činnosti, uznání od ostatních hackerů a odhalování bezpečnostních mezer.[120] S poměrně zajímavým druhem motivace přišel v roce 1998 i Kremen, podle něhož většina hackerů není motivována zlými úmysly, jako je to patrné u jiných trestných činností, nýbrž jde spíše o nutkavou posedlost podobnou závislosti na hazardu. Hackerství pro ně může také představovat něco jako sportovní aktivitu.[121] Kromě výše uvedeného

[116] Shoulder surfing je jednou z metod sociálního inženýrství, jejíž cílem je získávání důvěrných dat a hesel přímým nahlížením přes rameno oběti.

[117] HUTCHINGS, Alice a CHUA Ting Yi. Gendering cybercrime. In: HOLT, Thomas J. *Cybercrime Through an Interdisciplinary Lens*. Abingdon, Oxon: Routledge, 2017, s. 167–168. ISBN 978-1-315-61845-6.

[118] COHEN, Lawrence E. a Marcus FELSON. Social Change and Crime Rate Trends: A Routine Activity Approach. *American sociological review*. 1979, roč. 44, č. 4, s. 589. ISSN 0003-1224.

[119] CHNG, Samuel, Han Yu LU, Ayush KUMAR a David YAU. Hacker types, motivations and strategies: A comprehensive framework. *Computers in human behavior reports*. 2022, roč. 5, s. 2 a násl. ISSN 2451-9588. Dostupné z: doi:10.1016/j.chbr.2022.100167

[120] JORDAN, Tim a Paul TAYLOR. A sociology of hackers. *The Sociological review (Keele)*. Oxford, UK: Blackwell Publishing. 1998, roč. 46, č. 4, s. 768–769. ISSN 0038-0261. Dostupné z: doi:10.1111/1467-954X.00139

[121] KREMEN, Stanley. Apprehending The Computer Hacker: The Collection and Use of Evidence. In: *Computer Forensics Online* [online]. 1998 [cit. 2022-05-22]. Dostupné z: http://www.shk-dplc.com/cfo/articles/hack.htm

lze uvést i přijetí technické výzvy, procvičování programovacích dovednostní, hacking z nenávisti, rekreační hacking, sexuálně motivovaný hacking, ideologický motiv a v neposlední řadě také finanční obohacení. Z mezinárodních empirických výzkumů lze například uvést projekt Hackers Profiling Project z let 2003–2004, který mimo jiné jako zjištěné motivy uvádí vztek, boj za svobodu a nadšení z nových technologií.

Závěrem lze sumarizovat, že motivace k páchání kyberzločinů jsou rozličné, navíc i s časem proměnlivé, a proto nelze uvést žádný jejich taxativní výčet. Motivace se u různých typů hackerů budou odlišovat, nicméně ani mezi nimi nemusí být hranice zcela jasně vymezena.

5.3. Digitální stopa a digitální důkaz

Historicky jednu z prvních definic digitální stopy poskytla v roce 1999 pracovní skupina SWGDE[122] (Scientific Working Group on Digital Evidence), která ji definuje jako *„jakoukoliv informaci s vypovídající hodnotou pro danou relevantní událost, uloženou nebo přenášenou v digitální podobě“*.[123] Poněkud úžeji vymezenou definici nabídla také mezinárodní organizace IOCE (International Organization on Computer Evidence), která definovala digitální stopu jako *„jakoukoliv informaci, uloženou nebo přenášenou v binární formě, která může být předložena soudu jako věcný důkaz“*.[124] Autoři Porada a Straus pojem digitální stopy ztotožňují s pojmem stopy počítačové.[125] K takovému pojetí se však nelze přiklonit, a to z toho důvodu, že daná definice je spíše restriktivní a nepočítá s dnes již širokou škálou nejrůznějších technických zařízení. Ačkoliv digitální stopy budou v oblasti kyberkriminality převažovat, lze se rovněž setkat i se stopami paměťovými a materiálními.

Hmotné nosiče dat obsahující digitální stopy subsumujeme na základě § 112 odst. 1 TZ do kategorie věcných důkazů. Naproti tomu do listinných důkazů budeme řadit data po jejich vytištění do papírové podoby. Dle Koloucha není ale zařazení digitálního důkazu pod jednu ze zmíněných kategorií zcela přiléhavé. Přestože současný trestní řád a celá právní úprava s pojmem digitálního důkazu nijak nepracují, objevují se návrhy de lege ferenda na jeho vytvoření, a to ve znění:

[122] SWGDE je vědecká pracovní skupina založená v roce 1998, jež se zaměřuje na zpracování mezioborových pokynů a postupů pro práci a uchovávání digitálních důkazů.

[123] RAK, Roman a Viktor PORADA. Vlastnosti digitálních stop a jejich dopady na forenzní šetření. *Soudní inženýrství*. 2005, roč. 16, č. 4, s. 183.

[124] PORADA, Viktor a Eduard BRUNA. Digitální svět a dokazování obsahu elektronických dokumentů. *Bezpečnostní technologie, systémy a management*. 2013, č. 3.

[125] PORADA, Viktor a Jiří STRAUS. *Kriminalistické stopy – Teorie, metodologie, praxe*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2012, s. 280. ISBN 978-80-7380-396-4.

„Digitálním důkazem jsou jakákoli data či informace, jež byly přeneseny, vytvořeny, uloženy či modifikovány za použití počítačového systému a které prokazují nebo vyvracejí dokazovanou skutečnost a mohou být prostředkem k odhalení a zjištění trestního činu a jeho pachatele, jakož i stopy trestného činu.“[126]

Totožnou definici digitálního důkazu poskytují i zahraniční autoři, jako například Eoghan Casey.[127] Oproti tomu Smejkal ve svém příspěvku na vědecké konferenci upozornil na nevhodnost legislativního zakotvením pojmu digitálního důkazu s tím, že úprava by podle něj byla příliš kazuistická, technicky orientovaná a s každým technologickým pokrokem by muselo docházet ke změně právní úpravy. V neposlední řadě je podle něj zakotvení nadbytečné, vzhledem k demonstrativnímu výčtu důkazů v § 89 odst. 2 TŘ.[128]

Osobně se přikláním k názoru, že na veškeré stopy a informace přenášené v digitální podobě, sloužící posléze v trestním řízení jako digitální důkazy, by mělo být nahlíženo ve smyslu nepřímých důkazů, a to vzhledem k jejich snadné falzifikaci.

Vlastnosti digitálních stop

Digitální stopy jsou charakteristické markantními odlišnostmi od běžných kriminalistických stop, což mimo jiné také determinuje celý proces sběru, manipulace, vyhodnocování a uchovávání takových stop.

Zpravidla se odlišují v tom, že jde o stopy nehmotné, latentní, časově trasovatelné, s velmi nízkou životností, ale na druhou stranu mnohdy obnovitelné. Nevýhodu představuje fakt, že pachatelé disponují nespočtem možností, jak digitální stopy zastřít, čehož dosahují pomocí jejich šifrování a různých anonymizačních metod. Odlišnost lze také nalézt v prostředí, ve kterém se stopy nacházejí. Informační a komunikační systémy jsou tvořeny heterogenním prostředím, které se může poměrně dynamicky v čase měnit. Specifické vlastnosti digitálních stop však většinou budou OČTŘ a znalcům v trestním řízení působit spíše komplikace.

---

[126] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z. s. p. o., 2016, s. 419. ISBN 978-80-88168-18-8.

[127] CASEY, Eoghan. *Digital evidence and computer crime: forensic science, computers and the Internet*. 3. vydání. Waltham, MA: Academic Press, 2011, s. 7. ISBN 978-0-12-374268-1.

[128] Mezinárodní vědecká konference: vliv nových technologií na právo. In: Youtube [online]. 24. března 2022 [cit. 2022-05-17]. Dostupné z: https://www.youtube.com/watch?v=5vL8Ye3xAKU. Kanál uživatele Právnická fakulta UK.

Zajišťování digitálních stop

Nezastupitelnou roli při zajišťování digitálních stop plní metody digitální forenzní analýzy[129] (DFA). První metoda, kterou DFA aplikuje, je tzv. tradiční neboli někdy také klasická digitální forenzní analýza, předpokládající pořízení identické bitové kopie původního hmotného nosiče dat. Bitové kopie se vytváří na pevné disky Policie ČR, a to po transportu hmotných nosičů na specializované pracoviště, případně výjimečně již v průběhu samotné domovní prohlídky. Praxe vyžaduje, aby byla vytvořena jedna hlavní kopie a minimálně jedna kopie vedlejší, a to z toho důvodu, že osoba provádějící zajišťování digitálních dat svým zkoumáním data modifikuje. Druhou metodou využívanou u běžících, neodpojitelných zařízeních, která nelze fyzicky zajistit, je metoda forenzní analýzy živých systémů (Live Forensics). Nevýhodou zajišťování stopy z „živých systémů" je však to, že v systému bude docházet k neustálým tokům dat, a tedy i ke změnám, a proto i kopie, která zde bude pořízena, se bude vztahovat pouze k okamžiku jejího provedení.

Co se týče osob oprávněných zajišťovat digitální stopy, půjde o kriminalistického technika, kriminalistického IT specialistu (na rozdíl od technika má oprávnění zajišťovat bitové kopie), znalce nebo policistu bez zvláštních technických znalostí, který je nicméně oprávněn pouze k fyzickému zajištění hmotných nosičů.[130]

Pro účely trestního řízení je vždy nutné na zajištěné digitální stopy pohlížet jako na potenciální důkazy, které budou v řízení předloženy, a proto je klíčové je zabezpečit tak, aby zajištěná data nebyla v průběhu celého procesu nijak upravována a pravost dat nemohla být nikterak zpochybněna. Obecný a fundamentální rámec pro práci s digitálními stopami poskytuje mezinárodní technická norma ISO 27037:2012 (Směrnice pro identifikaci, sběr, akvizici a uchování digitálních důkazů). Jako základní požadavek při sběru stop uvádí spolehlivost, dostatečnost, relevantnost a při práci s digitálními stopami také pak reprodukovatelnost, kontrolovatelnost a ospravedlnitelnost. Norma rovněž klade nároky i na osobu manipulující s digitálními stopami, kterou označuje jako DEFR (Digital Evidence First Responder). DEFR je speciálně vyškolenou osobou, která by měla na místě vyhledávat a zajišťovat digitální důkazy, přičemž by měla dodržovat následující:

[129] Digitální forenzní analýza je exaktní forenzní vědou, jejímž předmětem je zkoumání digitálních stop od jejich vzniku přes změnu až po zánik.

[130] ČÁP, Jan, Lukáš BREU a Zdeněk PROKEŠ. Zajišťování, zpřístupňování a vyhodnocování digitálních stop. *Bezpečnostní teorie a praxe*. 2022, č. 1. s. 89. ISSN 1801-8211.

- *„Minimalizovat manipulaci s digitálním zařízením či digitálními daty.*
- *Zdokumentovat veškeré akce a změny provedené s danou digitální stopou tak, aby si mohl nezávislý expert vytvořit názor na spolehlivost předložených důkazů.*
- *Postupovat v souladu se zákony dané země.*
- *DEFR by neměl postupovat nad rámec své působnosti“.*[131]

Norma také konkretizuje dílčí procesy při manipulaci s digitálními důkazy, jako je identifikace, zajištění zařízení, zajištění dat a uchování. Důraz je mimo jiné rovněž kladen na řádnou dokumentaci veškerých kroků, které osoba provedla. Přestože norma byla jakýmsi prvotním základním mezinárodním doporučením, setkala se s kritickým pohledem odborníků z praxe. Podle analytiků Vyskočila a Světlíka není daná norma nijak pravidelně aktualizována, a proto ani nemůže přiléhavě reagovat na rapidní vývoj technologií. Jako problém vidí autoři i to, že všechny osoby podílející se na zajišťování stop (například znalci), nedisponují stejnou mírou znalostí základních principů sběru dat. Potíže v praxi působí i to, že sběr často neprovádí ani osoby specializované na digitální stopy, nýbrž osoba zajišťující běžné fyzické stopy.[132]

Podle Caseyho je zapotřebí zavést pro práci s digitálními důkazy i další metodu, jako je pravděpodobnostní škála (tzv. Certainty Scale). OČTŘ by tak získaným důkazům přiřazovaly hodnocení od „chybný“ až po „určitý“, a to na základě sedmi stupňové pravděpodobnostní škály. Jako největší výhodu spatřuje Casey ve flexibilitě škály a její netechničnosti. Navrhovanou škálu podrobněji představuje následující tabulka.[133]

[131] VEBER, Jaromír, Zdeněk SMUTNÝ a Ladislav VYSKOČIL. Practice of Digital Forensic Investigation in the Czech Republic and ISO/IEC 27037:2012 [in Czech]. *Acta Informatica Pragensia*. 2015, roč. 4. s. 244.
[132] VEBER, Jaromír, Zdeněk SMUTNÝ a Ladislav VYSKOČIL. Practice of Digital Forensic Investigation in the Czech Republic and ISO/IEC 27037:2012 [in Czech]. *Acta Informatica Pragensia*. 2015, roč. 4. s. 253.
[133] CASEY, Eoghan. *Digital evidence and computer crime: forensic science, computers and the Internet*. 3. vydání. Waltham, MA: Academic Press, 2011, s. 70–72. ISBN 978-0-12-374268-1.

Úroveň	Popis	Hodnocení důkazu
C0	důkazy jsou v rozpory se zjištěnými fakty	chybný / nesprávný
C1	důkazy jsou velmi sporné	vysoce nejistý
C2	s důkazem bylo možné manipulovat	poněkud nejistý
C3	důkaz je obtížnější k falzifikaci, ale existují určité obsahové nesrovnalosti v získaných důkazech	možný
C4	důkaz byl chráněn před falzifikací nebo nebyl, ale více zdrojů získaný poznatek potvrzuje	pravděpodobný
C5	důkaz se shoduje z více nezávislých zdrojů, se kterými nebylo manipulováno	skoro jistý
C6	důkaz je nezpochybnitelný a nefalzifikovaný	určitý

Tabulka 1 – Navrhovaná pravděpodobnostní škála využitelná pro hodnocení digitálních důkazů v trestním řízení[134]

5.4. Znalecké dokazování

Vzhledem k odborným znalostem a zkušenostem zaujímají znalci v oblasti dokazování své nezastupitelné místo. Znalecká činnost je upravena zákonem č. 254/2019 Sb., o znalcích, znaleckých kancelářích a znaleckých ústavech, vyhláškou č. 503/2020 Sb., o výkonu znalecké činnosti, vyhláškou č. 504/2020 Sb., o znalečném, dále vyhláškou č. 505/2020 Sb., kterou se stanoví seznam znaleckých odvětví jednotlivých znaleckých oborů, a v neposlední řadě hlavou pátou zákona č. 141/1961 Sb., o trestním řízení soudním.

Hlavní činnost znalce spočívá ve vypracování znaleckého posudku, ve kterém prostřednictvím svých odborných znalostí posuzuje skutečnosti mu předložené zadavatelem posudku. „*Důkaz posudkem znalce je jedním z důkazních prostředků. Znalecký posudek ovšem nemá v trestním řízení žádné privilegované postavení, jde o důkaz jako každý jiný, platí pro něj všechny obvyklé zásady dokazování, zejména zásada volného hodnocení důkazů.*“[135] Ačkoliv bývají posudky zpracovány zpravidla písemně, není v oblasti kyberkriminality cizí ani elektronická podoba, zejména pokud se k posudku přikládají zajištěná data v elektronické podobě.

[134] CASEY, Eoghan. *Digital evidence and computer crime: forensic science, computers and the Internet*. 3. vydání. Waltham, MA: Academic Press, 2011, s. 70–72. ISBN 978-0-12-374268-1.
[135] JELÍNEK, Jiří. *Trestní zákoník a trestní řád s poznámkami a judikaturou*. 8. vydání. Praha: Leges, 2020, s. 826. ISBN 978-80-7502-395-7.

Smejkal uvádí, že i během znalecké činnosti v oblasti kybernetické kriminality dochází k různým chybám a problémům. Zejména jde podle něj o nedostatečnou kvalifikaci znalců, neaktuální programové zázemí, nedostatky informací o technologiích, ale také o časové prodlevy u ustanovení znalce, neboť v mezičase může dojít k modifikaci či smazání potřebných dat. V neposlední řadě podle něj bývají znalcům pokládány otázky, které jsou zavádějící či návodné.[136] Dle Koloucha je nutné zaměřit pozornost na úkony požadované od znalce. *„Obecně by měl orgán činný v trestním řízení od znalce zpravidla vyžadovat následující úkony: vytvoření identické kopie nosiče informací, zkopírování dat z počítače, obnovení všech smazaných dat nosiče informací a ověření komunikace uživatele ze záznamů uložených v počítačovém systému.“*[137]

Znalce lze dále v trestní řízení využít i jako konzultanta při ohledání, a to v případě, kdy půjde o zajištění počítačového systému nebo nosiče informací. Neodborné zásahy mohou vést ke ztrátě digitálních stop, a proto je účast znalce i v takových případech potřebná. Pokud nepůjde zajistit celý počítačový systém nebo nosič informací, může znalec vytvořit na místě identickou bitovou kopii nosiče.[138]

Znalecký posudek představuje pro trestní řízení významný důkazní prostředek, a je proto zapotřebí dbát na přesnou formulaci otázek a správný výběr osoby znalce. Pozitivní legislativní posun v problematice znaleckých posudků z oblasti kyberkriminality, lze spatřovat ve vytvoření nového seznamu znaleckých oborů, jako je obor informační a komunikační technologie a kybernetická bezpečnost.[139]

Obtížnost dokazování

Pro dokazování kybernetické kriminality, stejně jako pro dokazování jakékoliv jiné kriminality, platí ustanovení trestního řádu o dokazování (srov. § 89 a násl. TŘ). Nicméně se v oblasti kybernetické kriminality setkáváme s určitými specifickými aspekty, které dokazování poněkud ztěžují.

Úskalím celého procesu dokazování je bezpochyby čas. Vzhledem k dynamickému charakteru digitálních stop se možnost získání potřebných důkazů se zvyšující časovou prodlevou značně

[136] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018, s. 743–744. ISBN 978-80-7380-720-7.
[137] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016, s. 453. ISBN 978-80-88168-18-8.
[138] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016, s. 453. ISBN 978-80-88168-18-8.
[139] Seznam nových znaleckých oborů a odvětví byl zaveden do právního řádu zákonem č. 254/2019 Sb., resp. vyhláškou č. 505/2020 Sb., s účinností od 1. ledna 2021.

omezuje. V souvislosti s tím, je také nutné dodat, že s rostoucím časem získává samotný pachatel možnost, aby digitální stopy zastřel, pozměnil, případně i smazal. Dalším problematickým aspektem dokazování je čitelnost dat. Ve světe elektronických důkazů mohou poměrně často OČTŘ narazit na sofistikované formy zabezpečení souborů, které se jim nemusí vždy podařit rozšifrovat. V takovém případě nenabízí trestní řád OČTŘ žádné procesní nástroje, kterými by mohl být obviněný donucen ke zpřístupnění takových souborů.[140] Potíž představuje pro OČTŘ i autentizace. V případě, že OČTŘ získají potřebný soubor, vyvstává otázka, kdo je jeho autorem, případně kdo k němu měl přístup a mohl jej modifikovat. Řešení nabízí použití kvalifikovaných časových razítek a zaručených elektronických podpisů. Smejkal uvádí, že *„(…) uznávané elektronické podpisy jsou způsobilé zajistit nepopíratelnost původu a originalitu obsahu dat v elektronické podobě, ke kterým jsou připojeny“*.[141] Smejkal dále upozorňuje na dokazování skrze přeceňovaná metadata[142] souborů. Ačkoliv jsou metadata užitečná a běžně s nimi není záměrně manipulováno, je třeba mít na paměti, že více či méně sofistikovaní pachatelé je můžou bez problému dle potřeby pozměnit.[143]

5.5. Vyšetřování

Při vyšetřování kyberkriminality je klíčové postupovat co možná nejrychleji, a to z důvodu nízké životnosti a nestálosti digitálních stop. Způsoby páchání kyberzločinu jsou velmi rozličné, což vyšetřovatelům může působit potíže při sestavování vyšetřovacího plánu, respektive při plánování celé vyšetřovací situace. Je proto na místě vycházet nejenom z obecných kriminalistických metod, ale také ze specifických metod přizpůsobených právě trestné činnosti páchané v kyberprostoru.

Praxe vyšetřování a stíhání kyberkriminality se nicméně potýká s jistými problémy na straně vyšetřovatelů. Jde zejména o personální deficit pracovníků specializujících se na IT systémy. Podle Požára a Hníka jde dále o nedostatečné softwarové vybavení a nevhodné organizační uspořádání specializovaných policejních pracovišť.[144]

[140] Srov. se zásadou nemo tenetur se ipsum accusare.
[141] SMEJKAL, Vladimír. Elektronický podpis. *Právní rádce*. 2004, roč. XII, č. 12.
[142] Metadata jsou strukturovaná data poskytující informace o datech v digitalizovaných dokumentech.
[143] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018. s. 709–710. ISBN 978-80-7380-720-7.
[144] POŽÁR, Josef a Václav HNÍK. *Specifické problémy boje s kybernetickou kriminalitou* [online]. Praha: Policejní akademie ČR v Praze – Fakulta bezpečnostního managementu. [cit. 2022-03-28]. s. 23–24. Dostupné z: https://slideplayer.cz/slide/11176990/

Zvláštnosti předmětu vyšetřování

Při určování základního předmětu dokazování vycházíme z § 89 odst. 1 TŘ, nicméně kyberkriminalita vykazuje určité charakteristické atributy ve vztahu k předmětu dokazování. Ve všech formách kyberzločinu je zapotřebí určovat, zda se jedná o jeden či více skutků, zda došlo k zajištění původních souborů, jak byly operace na počítačovém systému provedeny a s jakým časovým odstupem byla technika po trestném činu zajištěna.[145] V souvislosti s tím je také potřeba vždy zkoumat jaká je výše způsobené škody, kolik bylo pachatelů a jaký byl jejich motiv, případně další okolnosti, které danou trestnou činnost umožnily. *„Společnou zvláštností dokazování (…) kybernetické kriminality je dále to, že její charakter nelze dovodit ze skutkové podstaty trestného činu aplikovaného na daný skutek. Charakter kybernetické kriminality je dovozován ze způsobu spáchání (modus operandi).“*[146]

Zvláštnosti podnětů k vyšetřování

Přestože mívá kybernetická kriminalita povahu pokračujících nebo trvajících trestných činů, zůstává zpravidla velmi dlouho neodhalena, což je způsobeno především tím, že většina trestných činů není ani orgánům činným v trestním řízení oznámena. Motivace neoznámení trestného činu je rozličná, nicméně lze říci, že u napadených institucí převládá strach ze ztráty dobrého jména a možnost ztráty klientů. V roce 2016 americká společnost SentinelOne, Inc., zaměřující se na kybernetickou bezpečnost, zveřejnila výzkum, ze kterého vyplynulo, že pouze 54 % firem zasažených ransomwarovým útokem o daném incidentu informovalo tamní orgány činné v trestním řízení.[147] Z uvedeného lze zpozorovat, že míra ochoty oznamovat kybernetické útoky, alespoň co se týče institucí, je poměrně značně oslabena.

Typické podněty k vyšetřování kybernetických trestných činů můžeme dle nauky dělit do čtyř kategorií: a) výsledky operativně pátrací činnosti orgánů činných v trestním řízení, b) oznámení kontrolních, inspekčních a revizních orgánů různých institucí, c) ústní, písemná a telefonická oznámení osob, d) ostatní druhy oznámení (např. anonymní oznámení nebo podněty skrze veřejné sdělovací prostředky). V neposlední řadě může orgánům činným v trestním řízení při vyšetřování

[145] PORADA, Viktor a Jiří STRAUS. Kriminalistika: (výzkum, pokroky, perspektivy). Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2013, s. 525. ISBN 978-80-7380-477-0.
[146] Ibid., s. 523–524.
[147] SENTINELONE, Inc. Ransomware Research Data Summary. In: *SentinelOne* [online]. 2016 [cit. 2022-03-28]. Dostupné z: https://go.sentinelone.com/rs/327-MNM-087/images/Data%20Summary%20-%20English.pdf

pomoci i institut podpůrných operativně pátracích prostředků, zejména pak osoba informátora (taktéž konfidenta).

Domovní prohlídka a prohlídka jiných prostor

Domovní prohlídky představují významný nástroj z hlediska opatřování elektronických důkazů a stop potřebných pro trestní řízení. Lze je vykonat, je-li důvodné podezření, že v bytě nebo jiné prostoře sloužící k bydlení nebo v prostorách k nim náležejících je věc nebo osoba důležitá pro trestní řízení (srov. § 82 TŘ). Vzhledem k tomu, že se jedná o zásah do ústavně zaručeného práva na nedotknutelnost obydlí (čl. 12 LZPS), je možné ji realizovat pouze za zákonem přísně stanovených podmínek. Domovní prohlídky nařizuje předseda senátu, v přípravném řízení pak soudce na návrh státního zástupce (srov. § 83 odst. 1 TŘ).

Při prohlídkách konaných v souvislosti s podezřením na kyberkriminalitu je zapotřebí předem stanovit, zda na místě prohlídky dojde k zajištění fyzických nosičů informací nebo budou zajištěny pouze otisky počítačových dat. Obecně můžeme říci, že při domovních prohlídkách koncentrují pozornost OČTŘ buď na údaje archivní (magnetická média) a zálohy dat, nebo dennodenně používané informace (nacházející se často na pevném disku).[148] V neposlední řadě je nutné se zaměřit i na připojení počítačového systému k internetu či zaznamenat připojení systémů do místní sítě. Takové úkony je pak vhodné konat za přítomnosti znalce nebo jiné osoby znalé IT systému, aby nedošlo k možnému znehodnocení případných důkazů.

Domovní prohlídku je možné provést i jako neodkladný a neopakovatelný úkon vzhledem k možnosti manipulace s potenciálními důkazy souvisejícími s počítačovou kriminalitou a v důsledku toho pak i k možnému maření účelu trestního řízení. *„I když lze v zásadě připustit, že (…) může mít domovní prohlídka v konkrétní věci charakter neodkladného úkonu (§ 160 odst. 4 TŘ) a že jako taková je ex lege přípustná (§ 83 odst. 1 al. 2 TŘ), jde v takovém případě o zvlášť závažný zásah do ústavně zaručeného základního práva na domovní svobodu, a proto také rozhodnutí, na jehož základě má být takový úkon proveden, musí být i z tohoto hlediska zvláštní závažnosti přiměřeně a dostatečně zdůvodněno.“*[149] V souvislosti s počítačovou kriminalitou byla rozhodovací praxí neodkladnost a neopakovatelnost specifikována. Nejvyšší soud ve svém rozhodnutí stanovil, že chybějící dostatečně podrobné odůvodnění neodkladnosti a

[148] PORADA, Viktor a kolektiv. Kriminalistika: technické, forenzní a kybernetické aspekty. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2016. s. 798–799. ISBN 978-80-7380-589-0.
[149] Nález Ústavního soudu ze dne 22. 5. 1997, sp. zn. III. ÚS 287/96.

neopakovatelnosti v příkazu nemusí nutně znamenat nezákonnost takové prohlídky.[150] *„Zásah do softwarového či hardwarového vybavení počítače nebo úprava na něm uložených dat před tím, než by byl odborně zjištěn a zadokumentován jeho reálný stav, by znamenal zmaření objasňování skutečností závažných pro trestní stíhání. Toto závažné riziko dostatečně odůvodňuje kvalifikaci napadeného úkonu jako neodkladného a neopakovatelného.“*[151]

Odposlech a záznam telekomunikačního provozu

Dalším klíčovým institutem pro potírání kriminality, zejména pak kriminality kybernetické, je odposlech a záznam telekomunikačního provozu. Odposlech chápeme jako *„záměrné a utajené a současné vnímání obsahu komunikace zprostředkované telekomunikačními zařízeními nebo sítěmi prostřednictvím k tomu určených zařízení. Záznamem je souběžné zachycení obsahu komunikace na nosičích záznamu (...)“.*[152] Jde o poměrně specifický institut, neboť na rozdíl od ostatních zajišťovacích prostředků, působí pro futuro, tedy směřuje na zajištění toho, co teprve vznikne v budoucnu. Vzhledem k tomu, že se jedná o velmi významný zásah do práva na listovní tajemství a tajemství jiných písemností a záznamů (viz čl. 13 LZPS), vymezuje trestní řád poměrně přísné podmínky pro jeho aplikaci.

Pozitivní úpravu daného institutu nalezneme v § 88 trestního řádu. Zákon omezuje využití odposlechů u zločinů, na které je stanoven trest odnětí svobody s horní hranicí trestní sazby nejméně osm let. Dále umožňuje nařídit odposlech pro taxativně vyjmenované trestné činy, jako je například trestný čin pletichy v insolvenčním řízení (§ 226 TZ), pletichy při veřejné dražbě (§ 258 TZ) či zneužití pravomoci úřední moci (§ 329 TZ). Jako třetí a poslední uvádí trestní řád možnost využít odposlechy u úmyslného trestného činu, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva. Z výše uvedeného je zcela nepochybně vidět snaha zákonodárce omezit okruh podmínek pro nařizování odposlechů a lze vyvodit, že aplikace tohoto institutu má být v praxi spíše subsidiární.

Je žádoucí zmínit, že naprostá většina počítačových zločinů, nebude subsumována pod trestné činy s trestem odnětí svobody s horní hranicí osmi let a také nepůjde o zákonem vyjmenované trestné

[150] Usnesení Nejvyššího soudu ze dne 15. 12. 2010, sp. zn. 5 Tdo 1312/2010.
[151] Usnesení Nejvyššího soudu ze dne 15. 12. 2010, sp. zn. 5 Tdo 1312/2010.
[152] ŠÁMAL, Pavel. Zajišťovací úkony a předběžná opatření. In: ŠÁMAL, Pavel, Jan MUSIL, Josef KUCHTA a kolektiv. *Trestní právo procesní*. 4. přepracované vydání. Praha: C. H. Beck, 2013, s. 325. ISBN 978-80-7400-496-4.

činy.[153] Proto je z hlediska kybernetické kriminality významné zaměřit se na podmínku poslední, tj. na trestné činy, které mají podklad v mezinárodních smlouvách nebo na ně navazují. Ze smluv je v daném případě relevantní Úmluva o počítačové kriminalitě, Úmluva o ochraně dětí proti sexuálnímu vykořisťování a pohlavnímu zneužívání či Dodatkový protokol k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů.

Stěžejní pro odposlech a záznam telekomunikačního provozu je definovat samotný pojem telekomunikační provoz. Zákon č. 127/2005, o elektronických komunikacích (dále jen „ZEK"), jej chápe jako jakoukoliv zprávu přenášenou podle daného zákona (§ 136 odst. 20 písm. a) ZEK), přičemž zprávu definuje jako informaci, která se přenáší mezi uživateli prostřednictvím veřejně dostupné služby elektronické komunikace (§ 89 odst. 2 ZEK). Taková definice by se pak ale vzhledem k atributu veřejnosti mohla zdát poněkud omezující a nedostačující. Pod „telekomunikační provoz" by nebylo možné zařadit provoz neveřejnými službami. Dostál navrhuje interpretovat telekomunikační provoz tak, *„že zahrnuje vše chráněné tajemstvím dopravovaných zpráv dle čl. 13 Listiny, tedy elektronický přenos jakýchkoli neveřejných zpráv a záznamů mezi nějakými osobami"*.[154]

V souvislosti s vyšetřováním kybernetické kriminality je v poslední době poměrně hojně diskutovaný nový procesní institut uchování dat (angl. data preservation) dle § 7b TŘ. Ustanovení bylo začleněno do trestního řádu v souvislosti s implementací článku 16 Úmluvy Rady Evropy o počítačové kriminalitě. Osobě, která data drží nebo je má pod svou kontrolou, může být nařízeno, aby je uchovala v nezměněné podobě po stanovenou dobu, dále aby činila opatření, aby nedošlo k zpřístupnění informací o tom, že jí takové nařízení bylo uloženo. Důvodová zpráva dále upřesňuje, že příkaz se vztahuje na všechny typy uložených počítačových dat.[155] Při aplikaci předmětného ustanovení tak součástí uchovaných dat mohou být i údaje o obsahu komunikace, čímž dojde k rozporu s institutem odposlechu telekomunikačního provozu. Podle autorek Tlapák

[153] Pro srovnání slovenská právní úprava pojala institut odposlechu poněkud šířeji. Klíčová odlišnost spočívá v tom, že se dá uplatnit již na trestné činy, na které zákon stavuje trest odnětí s horní hranicí trestní sazby převyšující 5 let, což z hlediska počítačové kriminality může mít zásadní význam.

[154] DOSTÁL, Otto. Zajišťování důkazů u počítačové kriminality – odposlech a údaje o komunikaci (2. díl). *Trestněprávní revue*. 2019, č. 4, s. 77–83.

[155] Důvodová zpráva k zákonu, kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a některé další zákony, sněmovní tisk 79/0.

Navrátilové a Galovcové se aplikací § 7b TŘ jedná o obcházení procesních podmínek odposlechu a tím pádem o neoprávněný zásah do základních práv jednotlivců.[156]

Vyžádání údajů o uskutečněném telekomunikačním provozu

Vyjma odposlechu a záznamu na telekomunikačním provozu umožňuje zákon využít obdobného institutu, a to vyžádání údajů o uskutečněném telekomunikačním provozu dle § 88a TŘ. Při vyžadování údajů o uskutečněném telekomunikačním provozu, OČTŘ zajišťují data, na která se aplikuje ochrana osobních a zprostředkovacích dat nebo která jsou předmětem telekomunikačního tajemství. Odposlech a vyžádání údajů se tak od sebe odlišuje v několika směrech.

Hlavní rozdíl mezi § 88 TŘ a § 88a TŘ spočívá v povaze zajišťovaných dat. Nebude zde zajišťován obsah zpráv, nýbrž provozní a lokalizační údaje. Například se bude jednat o údaje ohledně IP adresy, přístupy do e-mailových schránek či informace ohledně webových stránek. Nejednotně vnímaná problematika se také týká otázky, zda údaje dle § 88a TŘ lze vyžadovat pouze zpětně do minulosti nebo je lze vztáhnout i na data nově vzniklá. Z dikce samotného ustanovení § 88a TŘ nikterak nevyplývá, zda by údaje mohly být zajištěny jak do minulosti, tak do budoucnosti. Kolouch tvrdí, že údaje je možné vyžadovat jak do minulosti, tak i do budoucnosti, přičemž argumentuje aplikací jazykového a historického výkladu § 88a TŘ. Upozorňuje, že předchozí právní úprava obsahovala podmínku „o uskutečněném telekomunikačním provozu", kdežto nyní zákon hovoří pouze o zajištění údajů o telekomunikačním provozu.[157] Opačný názor zastává Dostál, který poukazuje na to, že pokud nějaká data mají být zajištěná, musí nejdříve vůbec existovat.[158] Ani judikatura však nezaujala shodný názor. V roce 2011 Nejvyšší soud jednoznačně potvrdil, že § 88 TŘ lze uplatnit do budoucna, kdežto § 88a TŘ nikoliv.[159] O několik let později ale připustil, že v odůvodněných případech lze § 88a TŘ vydat i do budoucna. Půjde tak o *„situaci, kdy se šetřená trestná činnost nachází ve stadiu přípravy a zjišťované údaje mají orgánům činným v trestním řízení poskytnout informace důležité pro odhalení či usvědčení pachatelů, popř. k zabránění dokonání připravované trestné činnosti anebo k zjištění jiných skutečností důležitých pro trestní řízení"*.[160]

[156] TLAPÁK NAVRÁTILOVÁ, Jana a Ingrid GALOVCOVÁ. Uchovávání dat uložených v počítačovém systému – poskytování součinnosti, nebo nahrazování činnosti orgánů činných v trestním řízení? *Bulletin advokacie*. 2019, (11), s. 36–39.

[157] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z. s. p. o., 2016, s. 443. ISBN 978-80-88168-18-8.

[158] DOSTÁL, Otto. Zajišťování důkazů u počítačové kriminality – odposlech a údaje o komunikaci (2. díl). *Trestněprávní revue*. 2019, č. 4, s. 77–83.

[159] Usnesení Nejvyššího soudu ze dne 29. 11. 2011, sp. zn. 4 Pzo 5/2011.

[160] Usnesení Nejvyššího soudu ze dne 7. 5. 2019, sp. zn. 4 Tdo 1591/2018.

Poslední odlišnost spočívá v tom, vůči komu daný institut působí. Vyžádání údajů o uskutečněném telekomunikačním provozu směřuje vůči držiteli lokalizačních a provozních dat. Držitelé takových dat mají pak povinnost je podle zákona uchovávat po dobu šesti měsíců (viz § 96 odst. 3 ZEK), což v praxi často představuje problém. Povinnost retence dat vyplynula ze směrnice 2006/24/ES[161] (dále jen „směrnice o uchovávání dat"), ve které byla členským státům uložena povinnost uchovávat data po dobu minimálně šesti měsíců, nejvýše však po dobu dvou let. Ačkoliv byla Směrnice o uchovávání dat již zrušena,[162] právní řády některých členských států příslušnou povinnost retence stále obsahují. Současnou úpravu uchovávání dat vybraných členských zemí EU přibližuje následující tabulka.

Země	**Povinnost retence dat**
Belgie	zrušena v roce 2021[163]
Česká republika	6 měsíců
Francie	12 měsíců
Itálie	30 měsíců
Polsko	12 měsíců

Tabulka 2 – Srovnání povinnosti uchovávání dat ve vybraných státech EU [164]

Závěrem je nutné ještě odkázat na možnost policejního orgánu požadovat poskytnutí provozních a lokalizačních údajů na základě zákona č. 273/2008 Sb., o Policii České republiky (dále jen „PolČR"). Policie může za zákonem stanovených specifických podmínek[165] žádat od fyzických a právnických osob zajišťujících veřejnou komunikační síť nebo službu zmíněná data (viz § 66 odst. 3 PolČR). Třebaže lze pozorovat určité obdobné znaky jako u § 88a TŘ, nelze dané instituty nikterak ztotožňovat. Vzhledem k velmi specifickému okruhu podmínek stanovených dle PolČR bylo nejspíše snahou zákonodárce minimalizovat pokusy obcházení § 88a TŘ.

[161] Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. 3. 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí.

[162] Směrnice byla zrušena ex tunc pro rozpor s Chartou základních práv EU.

[163] BERTHÉLÉMY, Chloé. New Belgian data retention law: a European blueprint? In: *EDRi* [online]. 2021 [cit. 2022-03-19] Dostupné z: https://edri.org/our-work/new-belgian-data-retention-law-a-european-blueprint/

[164] ROJSZCZAK, Marcin. The uncertain future of data retention laws in the EU: Is a legislative reset possible? *The computer law and security report*. 2021, roč. 41, s. 2–12. ISSN 0267-3649. Dostupné z: doi:10.1016/j.clsr.2021.105572

[165] Jde o podmínku zjištění totožnosti neznámé osoby, nebo mrtvoly (§ 68 odst. 2 PolČR). Druhá podmínka svědčí útvaru Policie ČR, který bojuje s terorismem a využije daná data za účelem odhalování teroristických hrozeb (§ 71 PolČR).

Operativně pátrací prostředky

Operativně pátrací prostředky chápeme jako systém činností policejních orgánů uskutečňovaných na základě trestního řádu. Zákon je taxativně vymezuje jako předstíraný převod (§ 158c TŘ), sledování osob a věcí (§ 158d TŘ) a použití agenta (§ 158e TŘ). Z hlediska boje proti kyberzločinu je pro nás stěžejní především institut sledování osob a věcí dle § 158d odst. 3 TŘ. Sledování osob a věcí může být využíváno například ke zjištění kontaktů z adresáře, zjištění obsahu e-mailové schránky či provedení její zálohy. Právě problematika e-mailových schránek, konkrétně zajišťování e-mailových zpráv, byla poněkud roztříštěná a musela být aplikační praxí upřesněna. Nejvyšší státní zastupitelství ve výkladovém stanovisku[166] vymezilo, že dle § 158d odst. 3 TŘ lze zjišťovat pouze aktuální obsah e-mailové schránky, tedy pokud by mělo dojít k zajištění obsahu komunikace budoucí, musel by OČTŘ uplatnit již institut dle § 88 TŘ. Judikatura je v tomto směru prozatím poměrně strohá, nicméně bylo prozatím dovozeno, že použití § 158 odst. 3 TŘ za účelem otisku elektronických dat na sledovaných zařízeních je přípustné.[167] V neposlední řadě lze i v rámci kyberkriminality využít institutu použití agenta dle § 158e TŘ, a to za účelem infiltrace skupin na dark webu.[168]

5.6. Mezinárodní spolupráce při vyšetřování kyberkriminality

S ohledem na přeshraniční a mezinárodní charakter kyberkriminality si v dnešní době nelze vystačit pouze s vnitrostátní úpravou. Pro vyšetřování a shromažďování elektronických důkazů je zcela klíčová spolupráce na nadnárodní úrovni. Evropská unie tak v rámci zefektivnění a ucelení přeshraničního získávání důkazů nabídla členským státům několik možných nástrojů.

5.6.1. Evropský vyšetřovací příkaz

Evropský vyšetřovací příkaz je institut, jenž je vydáván za účelem provedení konkrétních vyšetřovacích úkonů s cílem shromáždit elektronické důkazy ve vykonávajícím státě, případně i k získání důkazů, kterými disponují OČTŘ jiné jurisdikce. Byl zaveden směrnicí Evropského parlamentu a Rady 2014/41/EU o evropském vyšetřovacím příkazu v trestních věcech. Česká republika jej implementovala do vnitrostátního práva, a to zákonem č. 178/2018 Sb., kterým novelizovala zákon o mezinárodní justiční spolupráci ve věcech trestních.

[166] Výkladové stanovisko poř. č. 1/2015 Sb. v. s. Nejvyššího státního zastupitelství ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek ze dne 26. ledna 2015, sp. zn. 1 SL 760/2014.
[167] Usnesení Ústavního soudu ze dne 3. 10. 2013, sp. zn. III. ÚS 3812/2012.
[168] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z. s. p. o., 2016, s. 451. ISBN 978-80-88168-18-8.

Evropský vyšetřovací příkaz je založen na principu vzájemného uznávání, což znamená, že vykonávající orgán má povinnost danou žádost uznat a zajistit její výkon bez dalších formálních postupů. Směrnice dále stanoví, že se příkaz provádí za stejných podmínek a stejným způsobem, jako by jej nařídil vykonávající orgán. Pro zajištění spolupráce mezi státy bylo žádoucí určit i lhůty pro provedení vyšetřovacích úkonů. Bylo vymezeno, že úkony by měly probíhat se stejnou rychlostí a prioritou, jako by se postupovalo v obdobném případě na vnitrostátní úrovni. Nastaveným limitem je zde nejvýše 30 dnů na přijetí rozhodnutí a maximálně 90 dnů pro výkon požadovaného úkonu.

Nespornou výhodou dále je, že se jedná o příkaz formulářového typu s již předem danými formálními náležitostmi. V době svého vzniku byl formulář veřejností vnímán jako krok vpřed z hlediska zjednodušení formalit, zlepšení kvality a snížení nákladů na překlad.[169]

Ačkoliv se nepochybně jedná o průlomový institut ve světě elektronických důkazů, je nutné poukázat na několik možných nedostatků. První otázka se nabízí hned u překladu právní terminologie. Třebaže jde, jak již bylo výše uvedeno, o formulářový typ, vydávající orgán musí uvést a popsat jaké úkony mají být provedeny. Při překladu právních textů by měl orgán postupovat co možná nejkomplexněji a snažit se hledat ekvivalentní termíny i například v souvislosti s historickým kontextem. Právě jazyková bariéra a snaha nalézt vhodné ekvivalentní pojmy mezi různými právními řády pak může pro orgány představovat problém. Další nedostatek lze spatřovat v tom, že zmíněné lhůty pro přijetí rozhodnutí a jeho následný výkon, dle mého názoru, ne zcela pružně nereagují na povahu elektronických důkazů, respektive jakýchkoliv dat nacházejících se v kyberprostoru.

5.6.2. Společné vyšetřovací týmy

Evropský vyšetřovací příkaz není jediným použitelným nástrojem v oblasti přeshraničního zajišťování elektronických důkazů. Společné vyšetřovací týmy jsou tvořeny skupinou soudců a státních zástupců z několika různých členských států, jejichž působení vzniklo za účelem vedení trestního stíhání v jednom nebo více státech. Vyšetřovací týmy se zřizují obvykle na dobu 12 až 24 měsíců, a to na základě písemné dohody. Cílem je vyměňování důkazů a získaných informací,

[169] GUERRA, José Eduardo a Christine JANSSENS. Legal and Practical Challenges in the Application of the European Investigation Order. In: *EUCRIM – The European Criminal Law Associations Forum* [online]. 2019, vol. 1, s. 48–49 [cit. 2022-03-24]. Dostupné z: https://eucrim.eu/media/issue/pdf/eucrim_issue_2019-01.pdf

dále efektivní sdílení technických znalostí a zkušeností. Sekundárně je také členům týmů umožněno budovat vzájemné vztahy a důvěru, což vede k efektivnější a rychlejší spolupráci.[170]

5.6.3. Evropský předávací a uchovávací příkaz

V souvislosti s usnadněním zajištění a shromažďováním elektronických důkazů nalézajících se v cizí jurisdikci představila Evropská komise legislativní návrh nařízení o evropských předávacích a uchovávacích příkazech.[171] Návrh nařízení reagoval na roztříštěné právní úpravy členských států a na rostoucí aktivitu páchání trestných činů v oblasti kyberprostoru. Jestliže bude návrh přijat, budou vytvořeny mimo jiné dva zcela nové instituty, a to evropský předávací příkaz a evropský uchovávací příkaz. Oba příkazy by měly opět vycházet ze zásady vzájemného uznávání a lze je užívat pouze v trestním řízení, a to jak v přípravném řízení, tak v řízení před soudem.

5.6.4. Evropský předávací příkaz (EPP)

EPP je vyšetřovací opatření, které umožní justičním orgánům členského státu požadovat uložená data (např. e-mailovou komunikaci, textové zprávy atd.) přímo od poskytovatelů údajů z jiného členského státu. Lze si ze zmíněného vyvodit, že EPP má fungovat na principu obcházení systému justiční spolupráce, neboť zahraniční justiční orgány budou důkazy požadovat přímo od soukromého subjektu, který má důkazy v danou chvíli dostupné ve své sféře. Odůvodnění lze spatřovat v tom, že vnitrostátní justiční orgány mnohdy nedisponují dostačujícími prostředky, které by zajistily rychlé a efektivní zajištění elektronických důkazů. Na druhou stranu vyvstává problém, jak bude řešena situace, kdy po soukromém subjektu budou justičním orgánem cizí země požadovány například údaje, které v dané jurisdikci vyžadovány být vůbec nemohou. Zůstává otázkou, zda by nějakým způsobem neměla být zachována kontrola zákonnosti EPP ze strany příslušného justičního orgánu, v jehož jurisdikci se o důkaz žádá. Jistou výhodu, kterou lze spatřovat, jsou velmi krátké lhůty určené k poskytnutí elektronického důkazu. Poskytovatel údajů, respektive případných důkazů, bude vázán standardní lhůtou deseti dnů, aby na EPP zareagoval. Návrh rovněž počítá i s naléhavými případy, kdy lhůta může být zkrácena na šest hodin. Tyto poměrně krátké lhůty lze z hlediska kybernetické kriminality více než kvitovat a oproti lhůtám

[170] EUROPEAN UNION AGENCY FOR CRIMINAL JUSTICE COOPERATION. Joint investigation teams. *The purpose of JITs* [online]. [cit. 2022-03-24]. Dostupné z: https://www.eurojust.europa.eu/judicial-cooperation/eurojust-role-facilitating-judicial-cooperation-instruments/joint-investigation-teams

[171] Návrh nařízení Evropského parlamentu a Rady o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech ze dne 17. 4. 2018, č.j.: 2018/0108/COD. Ke dni 30. 10. 2022 je návrh přezkoumáván Radou Evropské unie v prvním čtení.

uvedeným v evropském vyšetřovacím příkazu (30 dnů na přijetí rozhodnutí + 90 dnů na jeho výkon), je lze hodnotit jako adekvátní vzhledem k nestálému charakteru kyberprostoru.

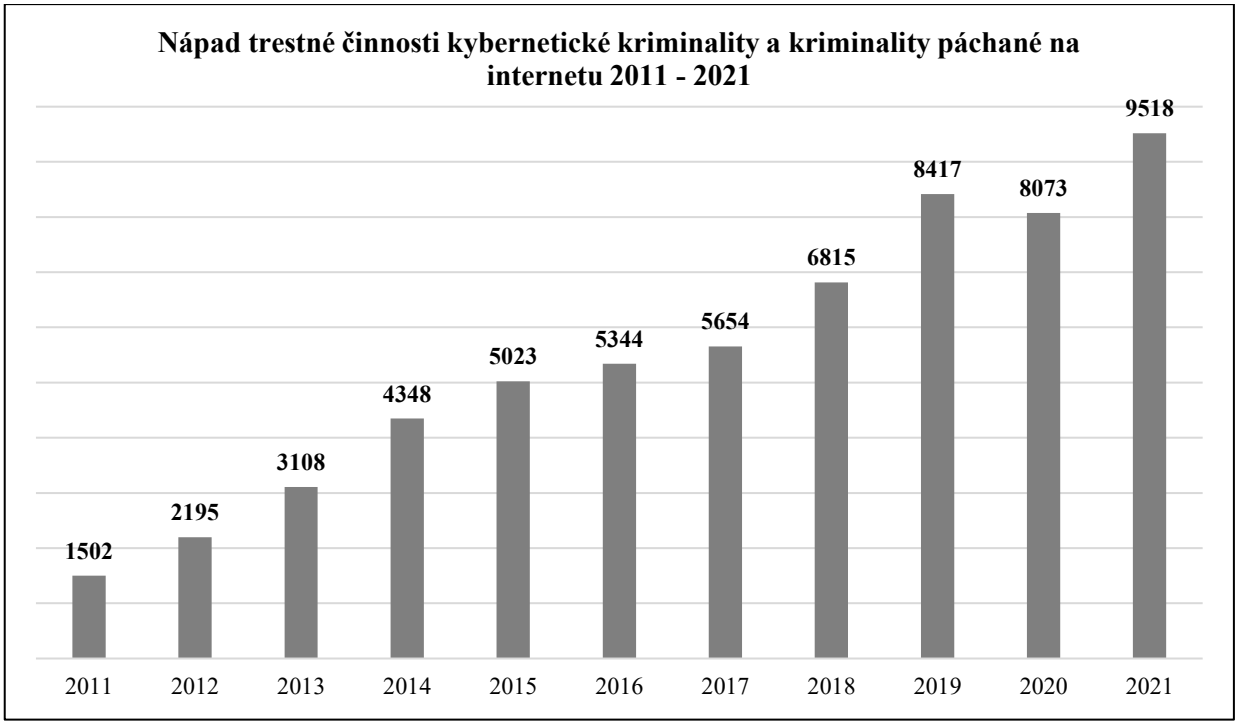
5.6.5. Evropský uchovávací příkaz (EUP)

EUP je adresován členskému státu, respektive poskytovateli údajů a služeb mimo jurisdikci vydávajícího státu, a to za účelem uchování určitých údajů. Je potřeba zmínit, že EUP se vztahuje pouze na údaje, které jsou již uloženy u poskytovatele v době vydání příkazu, tedy nepůjde o údaje zachycené teprve v budoucnu, tj. po obdržení EUP. Zatímco EPP lze vydat v souvislosti s jakýmkoliv trestným činem, EUP lze vydat jen u trestných činů, na které ve vydávajícím státě zákon stanoví trest odnětí svobody s horní hranicí sazby nejméně tři roky.

Závěrem lze poznamenat, že pokud dojde k přijetí zmíněného nařízení, evropský předávací příkaz ani evropský uchovávací příkaz nenahradí stávající evropský vyšetřovací příkaz, ale budou jen dalším alternativním řešením problematického přeshraničního zajišťování elektronických údajů.

6. SOUČASNÝ STAV A PŘEDPOKLÁDANÝ VÝVOJ KYBERNETICKÉ KRIMINALITY

Dle statistických údajů lze pozorovat, že nápad trestné činnosti kybernetické kriminality a kriminality páchané na internetu má v České republice od roku 2011 tendenci progresivního růstu. Výjimkou byl rok 2020, který přinesl mírný pokles oproti předchozímu roku, což je odůvodňováno narůstajícími případy koronavirového onemocnění COVID-19, ale především spíše legislativní změnou trestního zákoníku, která mimo jiné posunula hranice škody nikoliv nepatrné z původních pěti tisíc na deset tisíc korun.[172] K nejčastěji páchaným trestným činům prostřednictvím kyberprostoru řadíme majetkovou trestnou činnost, zejména podvodná jednání. Dále jsou ve větším množství páchány trestné činy podle § 230–232 TZ.



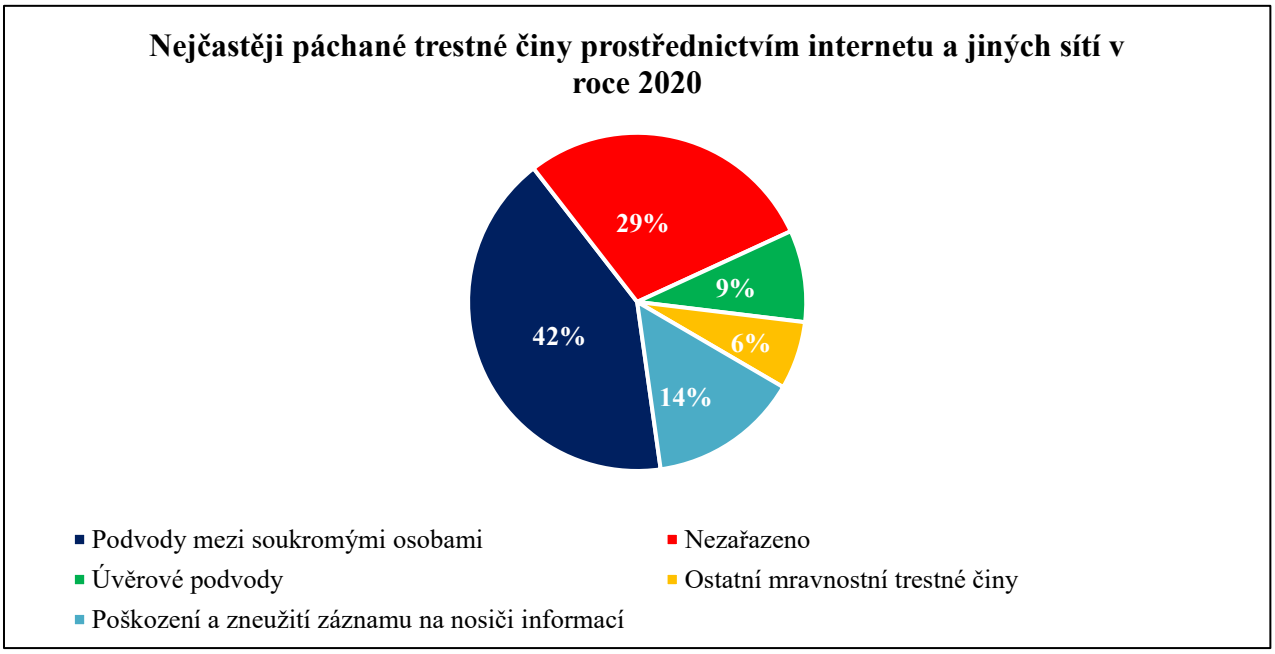
Graf 1 – Nápad trestné činnosti kybernetické kriminality a kriminality páchané na internetu v letech 2011–2021[173]

Podle oficiálních údajů tvoří nápad trestné činnosti kybernetické kriminality 6 % z celkové registrované trestné činnosti, z čehož by se dalo vyvozovat, že se jedná o problematiku ne tak důležitou. Je potřeba ovšem poznamenat, že na statistické údaje se nelze bezmezně spoléhat, neboť

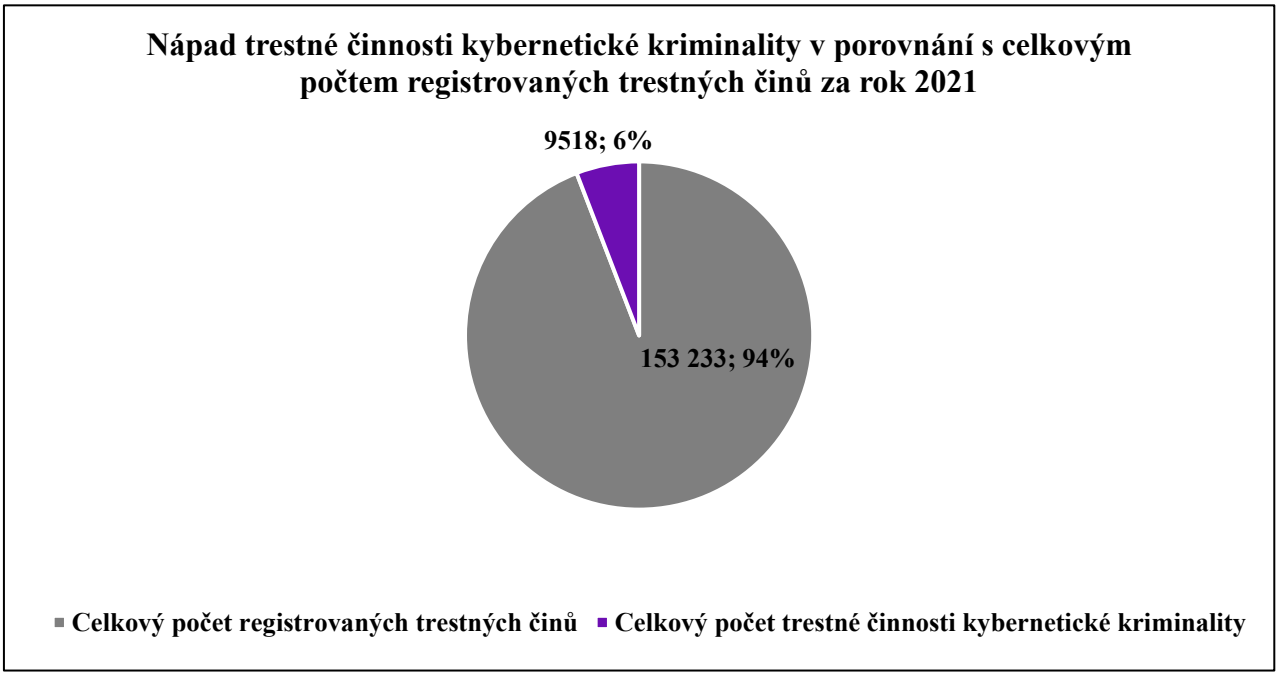
[172] Novela účinná od 1.10. 2020, provedená zákonem č. 333/2020 Sb., kterým se mění zákon č. 40/2009 Sb., trestní zákoník, zákon č. 141/1961 Sb., ve znění pozdějších předpisů.

[173] MINISTERSTVO VNITRA ČR. Statistiky kriminality – dokumenty. *Zpráva o situaci v oblasti veřejného pořádku a vnitřní bezpečnosti na území České republiky* [online]. [cit. 2022-02-22]. Dostupné z: https://www.mvcr.cz/clanek/statistiky-kriminality-dokumenty.aspx

kyberkriminalita se vyznačuje vysokou mírou latence a celkový počet trestných činů s největší pravděpodobností mnohonásobně převyšuje získané údaje. Statistiky také zkresluje skutečnost, že převážná část trestných činů, která by byla podřaditelná ke kyberkriminalitě, je subsumována pod jiné skutkové podstaty.



Graf 2 – Nejčastěji páchané trestné činy prostřednictvím internetu a jiných sítí v roce 2020[174]



Graf 3 – Nápad trestné činnosti kybernetické kriminality v porovnání s celkovým počtem registrovaných trestných činů za rok 2021

[174] MINISTERSTVO VNITRA ČR. Statistiky kriminality – dokumenty. *Zpráva o situaci v oblasti veřejného pořádku a vnitřní bezpečnosti na území České republiky* [online]. [cit. 2022-02-22]. Dostupné z: https://www.mvcr.cz/clanek/statistiky-kriminality-dokumenty.aspx

COVID-19 a kyberkriminalita

Česká republika, podobně jako ostatní státy, byla v roce 2020 a 2021 podstatně poznamenána vlivem pandemie onemocnění COVID-19. Hrozba kybernetických útoků v souvislosti s vypuknutím infekční nemoci zesílila, neboť koronavirová pandemie zcela nepopíratelně vedla k rapidnímu přesunu veškerých běžných aktivit do virtuálního světa. V souvislosti s tím došlo k nárůstu domén s názvy spojených s koronavirem, přičemž tyto domény byly posléze využívány převážně k podvodným jednáním na internetu a k šíření poplašných zpráv. V neposlední řadě bylo zpozorováno, že i obsah dark webu reflektoval koronavirovou situaci. Objevily se zde nabídky různých neidentifikovatelných látek, které byly vydávány za látky očkovací, nicméně u nich nebylo možné ověřit, zda mají potřebnou certifikaci nebo zda se jedná o čistě podvodná jednání.[175] Pachatele v kyberprostoru povzbudil též fakt, že se souvisejícími karanténami a prací z domova, došlo mezi zaměstnavateli k nárůstu přístupu BYOD (Bring Your Own Device). BYOD umožnil zaměstnancům používat svá osobní zařízení, jako jsou mobilní telefony a notebooky, k přístupu k firemním informacím a souborům. Výsledkem tak bylo, že zaměstnavatelé byli více vystaveni hrozbám kybernetických útoků, neboť práce z domova ve většině případů nezaručila stejnou kybernetickou bezpečnost jako zaručuje práce na pracovišti.

I cíle kybernetických útoků velmi přiléhavě reagovaly na koronavirovou situaci. Největší nárůst útoků byl zaznamenán u nemocnic a jiných zdravotnických zařízení. Nejvýznamnějším a nejzávažnějším útokem byl ransomový útok na Fakultní nemocnici v Brně, která následně musela velmi podstatně omezit svůj provoz. Dalším napadeným zdravotnickým zařízením byla také Psychiatrická nemocnice Kosmonosy.

Předpokládaný budoucí vývoj kyberkriminality

S neustálým zdokonalováním komunikačních a informačních technologií a nárůstem sofistikovanosti pachatelů lze důvodně předpokládat, že kyberzločin bude i nadále pronikat do všech možných aspektů našich každodenních životů, což mimo jiné potvrdila i výše zmíněná pandemie koronaviru. Zcela s jistotou lze konstatovat, že cíle útočníků budou nadále převážně sledovat zištné motivy. V současné době se v souvislosti s probíhajícím ozbrojeným konfliktem mezi Ruskou federací a Ukrajinou dá obdobně usuzovat, že budou narůstat útoky na kritické

[175] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020* [online]. [cit. 2022-02-22]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf

informační a komunikační systémy.[176] Lze mít za to, že kybernetická trestná činnost bude v budoucnu cílit na nejzranitelnější strategické cíle, jako je veřejný sektor.

Možným řešením je posílení kybernetické bezpečnosti v kritických oblastech, jako je energetika, průmysl a zdravotnictví. Následně by měla být pozornost koncentrována na spolupráci mezi orgány působícími v oblasti kybernetické bezpečnosti, jako je Policie ČR a NÚKIB. Intenzivní spolupráce se soukromým sektorem by také neměla zůstat opomenuta. Důležitým prostředkem v boji proti potenciální kriminalitě je dle mého názoru posilování mezinárodní spolupráce mezi státy.

Vize a cíle České republiky v oblasti kybernetické bezpečnosti

Národní úřad kybernetické a informační bezpečnosti zpracovává minimálně jednou za pět let národní strategii kybernetické bezpečnosti a k tomu přidružený akční plán. Činí tak na základě § 22 písm. q) zákona č. 181/2014 Sb., o kybernetické bezpečnosti, který transponuje požadavky směrnice Evropského parlamentu a Rady EU 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. Národní strategie kybernetické bezpečnosti ČR (dále jen „Národní strategie“) obsahuje cíle a vize republiky v oblasti kybernetické bezpečnosti, které pak následně konkretizuje v úkolech obsažených v rámci Akčního plánu.

Dle Národní strategie pro rok 2021–2025 je „*základním předpokladem pro účinnou obranyschopnost ČR ucelený systém detekce kybernetických hrozeb, závislý na schopnostech a kapacitách jednotlivých bezpečnostních složek, stejně jako na účinném fungování modelu národní spolupráce mezi bezpečnostními a dalšími složkami a koordinovaném, efektivním a včasném sdílení informací. Vzhledem k faktu, že narůstá riziko ohrožení státu prostřednictvím kyberprostoru, musí ČR reagovat na celé spektrum nových výzev“*.[177]

Druhým dokumentem, určujícím aktuální směřování České republiky v oblasti kybernetické bezpečnosti, je Strategie prevence kriminality v České republice na léta 2022–2027 (dále jen „Strategie“). Strategie je vypracována Ministerstvem vnitra v součinnosti s Republikovým

[176] Srov. NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. Varování ze dne 25. 2. 2022 před kybernetickými útoky na informační a komunikační systémy v České republice v souvislosti s ozbrojeným konfliktem, č.j.: 2384/2022-NÚKIB-E/350.

[177] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Národní strategie kybernetické bezpečnosti České republiky* [online]. 2020 [cit. 2022-03-11]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/

výborem pro prevenci kriminality. Rozvíjí již existující cíle a poznatky a promítají se zde i doporučení z mezinárodních dokumentů. Kromě obecné kriminality se zaměřuje na specifické druhy kriminality, jako je právě kromě jiného také kybernetická kriminalita a její prevence.

Strategie poukazuje, že kybernetická kriminalita má za trend cílit na nejzranitelnější skupinu, a to děti. Nejenom, že se stávají často oběťmi, ještě častěji se stávají pachateli. Jako celorepublikový problém vidí zvyšující se počty kriminálních jednání páchaných skrze sociální sítě. Hlavní boj proti tomuto trendu má představovat prevence a osvěta, zejména pak různá školení pro rizikové cílové skupiny.[178]

Vybrané strategické cíle Národní strategie a Strategie prevence uvádí následující tabulka.

dokument	**vybrané cíle**				
Národní strategie kybernetické kriminality	prevence a potírání kybernetické kriminality	zabezpečení digitální veřejné správy	efektivní mezinárodní spolupráce	sdílení schopností expertizy/ export know-how	důraz na sdílení informací, koordinaci a spolupráci
Strategie prevence kriminality	podpora obětí kybernetické kriminality	prevence a osvěta s důrazem na skupiny zvlášť zranitelné	spolupráce a vzdělávání na národní úrovni	zohlednění problematiky genderově podmíněného kybernásilí	podpora policejní spolupráce v oblasti řešení kyberkriminality

Tabulka 3 – Srovnání vybraných cílů strategických dokumentů v oblasti kybernetické bezpečnosti

[178] MINISTERSTVO VNITRA ČR. *Strategie prevence kriminality v České republice na léta 2022–2027* [online]. 5. října 2021 [cit. 2022-03-11]. Dostupné z: https://prevencekriminality.cz/wp-content/uploads/2021/10/04__spk-2022-2027_strategicka-cast.pdf

7. AKTUÁLNÍ TRENDY V OBLASTI KYBERPROSTORU Z POHLEDU TRESTNÍHO PRÁVA

7.1. Cloudová úložiště

Pro účely objasnění této problematiky je nutné si vymezit pojem cloudových úložišť. Podle Národního institutu pro standardy a technologie Spojených států amerických (zkr. NIST – National Institute of Standards and Technology) jde o „*model umožňující všudypřítomný, pohodlný, na vyžádání dostupný síťový přístup ke sdílenému souboru výpočetních zdrojů, které mohou být rychle opatřeny a uvolněny s minimálním úsilím na jejich správu anebo interakci ze strany poskytovatele služeb*“.[179]

Neustále se rozšiřující trend cloudových úložišť má své opodstatněné důvody. Nespornou výhodou je dostupnost uložených dat. Jelikož cloudy fungují na principu sdílení softwarových a hardwarových prostředků prostřednictvím sítě, je uživatelům umožněno získat data kdykoliv a odkudkoliv, z téměř všech druhů elektronických zařízení, a to během velmi krátkého časového úseku. Další značnou výhodou jsou nízké počáteční i provozní náklady, neboť vesměs uživatel platí pouze paušální měsíční poplatky. Na druhou stranu jsou s cloudy spojena nezanedbatelná právní rizika. Vzhledem k tomu, že každé úložiště má někde fyzicky umístěný svůj server, může dojít k jeho zničení, ať už nedbalostním, či úmyslným jednáním, případně událostí vis maior. Velmi hojně diskutovanou otázkou je i přistup třetích osob k uloženým datům a jejich možné zneužití.

I z prizmatu trestního práva jsou cloudová úložiště poměrně problematická, a to především pokud jde o zajišťování dat v rámci vyšetřování. Vzhledem k „všudypřítomnosti“ dat může vzniklá situace pro orgány činné v trestním řízení představovat výzvu, neboť je zapotřebí správně aplikovat procesní instituty trestního řádu, a to za účelem omezení, respektive vyloučení relativní, případně absolutní neúčinnosti získaných důkazů.

OČTŘ mohou pro zajištění dat z cloudových úložišť využít součinnosti cloud providera. V rámci trestního řízení si lze s odkazem na § 78 TŘ vyžádat zaslání dat na úložišti. Vzhledem k tomu, že servery bývají mnohdy umístěny na území jiného státu, eventuálně jsou lokalizovány na území vícero států, bude využití ediční povinnosti, z praktického hlediska ne zcela ideální možností.

[179] MELL, Peter a Timothy GRANCE. *The NIST Definition of Cloud Computing*. B.m.: National Institute of Standards and Technology [online]. 2011 [cit. 2022-02-22]. Dostupné z: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Situace bude odlišná, pokud OČTŘ budou požadovat získání hesla nebo obdobného přístupu k úložišti. V daném případě bude zapotřebí využít institutu sledování osob a věcí dle § 158d odst. 3 TŘ, a to na základě předchozího povolení soudce.

Odlišná situace se nabízí v případě, kdy uživatel data na cloudovém úložišti zpřístupní svou vůlí neurčenému a nedefinovanému okruhu osob. Tím pádem bude vyloučena soukromá povaha cloudového úložiště a přístupem do něj nebude narušeno právo na informační sebeurčení. OČTŘ tak postačí využít ohledání (dle § 113 TŘ), ke kterému se zpravidla přibere znalec. Spornou otázkou bude, pokud přístupová adresa bude skrývána omezenému okruhu osob, ačkoliv úložiště nebude chráněno heslem. V daném případě lze i tak hovořit o záznamech uchovávaných v soukromí a bude nutné využít postup dle § 158 odst. 3 TŘ.

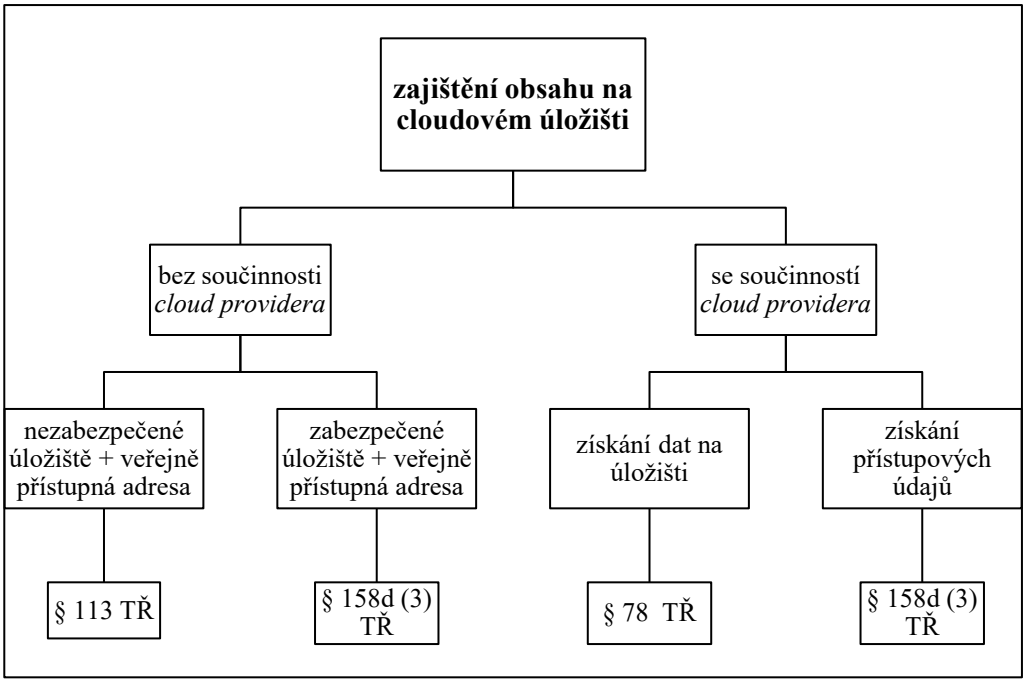


Schéma 2 – Aplikace procesněprávních institutů dle trestního řádu při zajišťování obsahu na cloudovém úložišti

Poměrně hojně diskutovanou otázkou v praxi je zajišťování obsahu cloudového úložiště během domovní prohlídky na základě § 82 a násl. TŘ. Dostál ve svém příspěvku uvádí, že při domovních prohlídkách lze získat přístup i do cloudového úložiště a nadále nebude zapotřebí samostatného zajišťovacího úkonu. Argumentuje především zrychlením celého procesu postihování trestné činnosti. Jako možné řešení navrhuje co nejšířeji formulovat obsah příkazu k domovní prohlídce tak, aby zahrnoval i vzdálená úložiště.[180] S takovým extenzivním výkladem institutu domovní

[180] DOSTÁL, Otto. Zajišťování důkazů u počítačové kriminality – dožádání, vydání věci a prohlídky (1. díl). *Trestněprávní revue*. 2019, č. 3, s. 66–71.

prohlídky se však nelze ztotožnit. Při zajištění důkazů nacházejících se na místě odlišném od místa konání domovní prohlídky, nabízí trestní řád jiné procesní instituty, jako například operativně pátrací prostředky dle § 158d TŘ. Pokud by při domovní prohlídce měla být zajištěna i „online" data, postupoval by OČTŘ dle mého názoru contra legem a získané důkazy by byly procesně nepoužitelné.

Volba správného procesního institutu zde nebude jediným úskalím. Problémem celého procesu je zejména roztroušenost dat a také fakt, že cloud provider má velmi často sídlo na území jiného státu, což pro trestní řízení znamená zajistit data, respektive vyžádat si právní pomoc na území jiného státu. Autoři K. Hlaváčová a O. Chorvát se ve své publikaci zabývají otázkou, který orgán činný v trestním řízení bude daný úkon provádět. Dle autorů je zapotřebí vycházet z principu teritoriality dat, což znamená, že orgány činné v trestním řízení, mohou zajistit pouze data nacházející se fyzicky na území České republiky.[181]

Pro účely zajištění dat na území cizího státu tak bude zapotřebí využít cestu mezinárodní justiční spolupráce. Oblast je v českém právní řádu zakotvena v § 62 zákona č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních. Z dikce zmíněného paragrafu lze vyčíst, že pro klasické „fyzické" přeshraniční sledování je vyžadován předpoklad mezinárodní smlouvy, avšak pro sledování skrze technické prostředky, nemusí být podmínka mezinárodní smlouvy splněna. Zákonodárce tak „bezesmluvním" stykem reagoval na rapidní vývoj informačních a telekomunikačních technologií a snažil se celý proces zjednodušit.[182] Z oblasti mezinárodních smluv je relevantní zmínit Úmluvu o počítačové kriminalitě, konkrétně pak článek 31, který se zabývá vzájemnou pomocí ve věcech přístupu k uloženým počítačovým datům. Vzhledem k nestálosti či možné ztrátě dat zakotvuje článek i možnost urychleného vyřízení žádosti.

Závěrem lze shrnout, že ačkoliv současná tuzemská právní úprava nereagovala zcela pružně na technologický vývoj vzdálených úložišť, potažmo veškerých elektronických důkazů, jsou stávající procesní instituty dostačující. Nejproblematičtějším místem však zůstává otázka mezinárodní justiční spolupráce, která celý proces komplikuje a zpomaluje. Najít vhodné řešení v této situaci nebude jednoduché, neboť se zde bude potřeba vyrovnat s kolizemi několika různých právních řádů.

[181] HLAVÁČOVÁ, Kateřina a Oliver CHORVÁT. Přístup orgánů činných v trestním řízení k datům uloženým v cloudu. *Revue pro právo a technologie*. 2016, č. 14, s. 18 a násl.
[182] KUBÍČEK, Miroslav a Přemysl POLÁK. *Zákon o mezinárodní justiční spolupráci ve věcech trestních: komentář*. Praha: Wolters Kluwer, 2014, s. 178. ISBN 978-80-7478-389-0.

Virtuální advokacie?

Zajímavá trestněprocesní otázka nastává v případě domovní prohlídky, přesněji řečeno prohlídky jiných prostor u advokáta, který využívá datová úložiště při výkonu advokacie. Advokát na cloudová úložiště ukládá informace, jež podléhají advokátnímu tajemství, a tedy je ukládá mimo fyzické prostory svého registrovaného sídla. Dle § 85b odst. 1 TŘ při provádění domovní prohlídky nebo prohlídky jiných prostor, v nichž advokát vykonává advokacii, pokud se zde mohou nacházet listiny, které obsahují skutečnosti, na něž se vztahuje povinnost mlčenlivosti advokáta, je orgán provádějící úkon povinen si vyžádat souhlas České advokátní komory. Lze tedy pod „jiné prostory, ve kterých advokát vykonává advokacii" zahrnout i vzdálená úložiště?

Odpověď přinesla až judikatura, jejíž vývoj nebyl v průběhu let poněkud konstantní. Soudy nebyly v jednoduché situaci a musely se vypořádat se střetem dvou principů, a to zásadou ochrany práv a svobod na jedné straně a náležitého objasnění trestných činů na straně druhé. Městský soud v Praze ve svém usnesení konstatoval, že nepochybně advokát může vykonávat advokacii na místech odlišných od registrovaného sídla u České advokátní komory, nicméně za místo výkonu advokacie nelze považovat prostory sloužící k úschově datových serverů, na kterých má advokát uložená svá data, a tudíž není třeba při prohlídce přítomnosti a souhlasu zástupce Komory k seznámení se s daty na serverech.[183] Městský soud argumentoval tím, že povinnost mlčenlivosti advokáta není bezbřehá a je zapotřebí nastavit mantinely tak, aby nedocházelo k jejímu cílenému zneužívání. K výkladu ustanovení se o necelý rok přidalo trestní kolegium Nejvyššího soudu ve svém stanovisku.[184] Stanovisko se mimo jiné zabývalo otázkou, zda se § 85b TŘ vztahuje i na místa, na která advokáti ukládají informace související s výkonem advokacie. Nejvyšší soud vyjádřil názor, že elektronická úložiště dat (kromě jiného i cloudová úložiště) lze subsumovat pod pojem „jiný prostor, v němž advokát vykonává advokacii" obsažený v § 85b trestního řádu. Názor Nejvyššího soudu následně potvrdil i Ústavní soud.[185]

7.2. Krádeže ve virtuálních světech

V současné době se setkáváme s fenoménem expanze kyberkriminality do různých prostředí, konkrétně pak i do virtuálních světů.

[183] Usnesení Městského soudu v Praze ze dne 9. 7. 2014, sp. zn. Nt 615/2014.
[184] Stanovisko trestního kolegia Nejvyššího soudu ze dne 25. 6. 2015, sp. zn. Tpjn 306/214.
[185] Usnesení Ústavního soudu ze dne 26. 10. 2015, sp. zn. I. ÚS 2878/14.

Pro pochopení problematiky je nutné si přiblížit pojem a podstatu virtuálních světů. Smejkal je definuje jako: *„počítačově implementovaná simulovaná prostředí, která se nacházejí v prostředí kyberprostoru“.*[186] Jiní autoři uvádí, že se jedná o místo, kde spolu interagují stovky uživatelů a ačkoliv existence virtuálního světa není závislá na přítomnosti uživatelů, mohou se podílet na jeho utváření.[187] Zatímco dříve byl virtuální svět spojován pouze s herním prostředím, setkáváme se dnes již se simulovanými sociálními virtuálními světy, kde uživatelé provozují běžné denní aktivity, jako je například seznamování, obchodování či provozování podnikatelské činnosti.

Zajímavá otázka nastává v případě, kdy uživatelé zvyšují hodnotu svých objektů nacházejících se ve virtuálním prostředí, a to buď investicí finančních prostředků, nebo dosahováním určitých herních úrovní. Je tedy možné, aby objekty ve virtuálním světě, například ve hře, byly předmětem vlastnictví a vztahovala se na ně relevantní právní úprava?

V roce 2003 se objevil případ, kdy společnost A zaměstnala skupinu osob za účelem profesionálního hraní MMORPG[188] hry vydané společností B. Zaměstnanci se tak dennodenně věnovali hraní onlinové hry, přičemž ve hře získávali různé virtuální suroviny a jiné statky, kromě jiného také zvyšovali úrovně svých avatarů. Společnost A následně získané virtuální objekty prodávala na několika internetových aukčních serverech, což jí přineslo nezanedbatelný zisk.

Z výše uvedeného případu vyplývá, že ačkoliv se nacházíme ve virtuálním světě, mohou zde díky činnosti uživatelů vznikat různé objekty (virtuální komodity, avataři apod.), které se prodávají a kupují na trhu jako každé jiné, zcela běžně obchodovatelné zboží. Závěrem lze shrnout, že v takovém pojetí bychom mohli uvažovat o virtuálních objektech jako o majetku, a bylo by tedy možné na ně aplikovat právní ochranu.

Postih virtuálních krádeží dle trestního práva

Poněkud složitější otázka vyvstává v případech právní kvalifikace odcizení virtuálních předmětů. Možný nástin řešení se pokusila nabídnout nizozemská judikatura, která se zabývala otázkou, zda má virtuální předmět povahu věci v rovině trestněprávní, a pokud má, zdali je vůbec možné takový předmět odcizit.

---

[186] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018, s. 779. ISBN 978-80-7380-720-7.

[187] ADRIAN, Angela. *Law and Order in virtual worlds: exploring avatars, their ownership and rights*. Hershey: Information Science Reference, 2010, s. 2. ISBN 978-1-61520-795-4.

[188] MMORPG (angl. massively multiplayer online role-playing game) je online počítačová hra, která umožňuje účast až tisíců hráčů v jeden moment.

V internetové hře RunScape došlo skupinkou mladistvých k protiprávnímu přivlastnění virtuálních peněz (posléze i různých virtuálních komodit), které poškozený ve hře získal díky intenzivnímu hraní a vysokému počtu nasbíraných bodů. Soud ve svém rozsudku[189] shledal pachatele jako trestně odpovědné za trestný čin krádeže.[190] Klíčová byla argumentace soudu ohledně virtuálních předmětů jako věcí ve smyslu holandského trestního zákoníku. Argument obhajoby, že se musí jednat o hmotnou věc, byl irelevantní. Již tamější předchozí judikaturou bylo řečeno, že i nehmotné věci, mohou být věcí. Důležitým faktorem bylo, že daná věc má pro vlastníka, respektive držitele určitou hodnotu, která nemusí být vyjádřena v penězích. Soud v neposlední řadě argumentoval tím, že pravidla hry neumožnila ani nepředpokládala získání virtuálních předmětů takovým nekalým způsobem, a proto se v daném případě jednalo o skutečné jednání, které jen herní prostřední ovlivnilo.

Druhý judikát[191] se zabýval oblíbenou hrou Habbo Hotel. Opět mladistvý pachatel se měl dopustit krádeže ve virtuálním prostředí internetové hry. Hra Habbo Hotel umožňuje hráčům zařizovat hotelové pokoje skrze kredity, které získali za skutečné peníze. Pachatel pomocí phishingové techniky získal přihlašovací údaje ostatních hráčů a z cizích účtů následně odcizil virtuální komodity, které si přemístil na svůj účet, přesněji řečeno do svého herního hotelového pokoje.[192] I zde se soud obdobně jako v prvním případě, přiklonil k trestní odpovědnosti za krádež.

Otázkou tedy je, zda by se i česká právní úprava dokázala vypořádat s aplikací trestného činu krádeže na odcizení virtuálních předmětů. Dle mého názoru bude poněkud problematické v našich současných podmínkách využít § 205 TZ, s ohledem na to, že dle zákona pachatel musí odcizit cizí věc. Komentářová literatura[193] chápe nicméně cizí věc v právním slova smyslu mj. jako ovladatelný hmotný předmět. Podmínku hmotného atributu však virtuální předměty nesplňují. Odlišná situace je v občanském právu, které chápe věc jako vše odlišné od osoby a sloužící potřebě lidí (§ 489 OZ).

Závěrem lze poznamenat, že česká právní úprava se poněkud odlišuje od nizozemské judikatury. Ačkoliv v daném případě nebudeme moci odcizení virtuálních objektů subsumovat pod § 205 TZ,

[189] Rozsudek soudu v Leeuwardenu ze dne 21. 10. 2008, č.j. 17/96/6123-07 VEV.
[190] Jedná se o překlad pojmu, v českém právní řádu by vzhledem k věku pachatelů bylo užito termínu „provinění" podle § 6 zákona č. 218/2003 Sb., o soudnictví ve věcech mládeže.
[191] Rozsudek soudu v Amsterdamu ze dne 2. 4. 2009, sp. zn. LJN: BH9789.
[192] CLOUGH, Jonathan. *Principles of Cybercrime*. Cambridge, UK; New York: Cambridge University Press. 2010. s. 19. ISBN 978-0-521-89925-3.
[193] ŠÁMAL, Pavel. Krádež - § 205. In: ŠÁMAL, Pavel a kolektiv. *Trestní zákoník II – komentář. Zvláštní část (§ 140–421)*. 2. vydání. Praha: C.H. Beck, 2012, s. 1979–1980. ISBN 978-80-7400-428-5.

využijeme jiná ustanovení, jako je např. ustanovení o trestném činu porušování autorského práva, práv souvisejících s právem autorským a práv k databázi (§ 270 TZ) či neoprávněném přístupu k počítačovému systému a nosiči informací dle § 230 TZ, která se prozatím jeví jako dostačující.

7.3. Virtuální měny

V souvislosti s rapidním rozvojem informačních a komunikačních technologiích došlo začátkem století k vývoji i nového typu měn, tzv. virtuálních, někdy též nazývaných jako kryptoměny. Ačkoliv původně vznikaly z důvodných obav možného opakování globální finanční krize[194], stávají se dnes čím dál tím více populární pro hackerské útoky v oblasti kyberprostoru.

Evropská centrální banka v roce 2012 definovala virtuální měnu jako: *„typ neregulovaných digitálních peněz, které jsou vydávány a obvykle i kontrolovány jejich tvůrci a jsou používány a přijímány mezi členy určité virtuální komunity“*.[195] Kryptoměny se stále těší velké oblibě nejenom ze strany investorů, ale i nepodnikajících fyzických osob, což potvrzuje mimo jiné i narůstající počet rozličných druhů kryptoměn. Odhaduje se, že aktuálně existuje již přes 18 tisíc druhů různých kryptoměn, přičemž nejznámější z nich reprezentuje Bitcoin (BTC), Ethereum (ETH), Litecoin (LTC), Cardano (ADA) a Monero (XMR).[196]

Výhody kryptoměn jsou mnohé. Jako příklad lze jmenovat usnadnění mezinárodních obchodních transakcí díky nízkým transakčním poplatkům a uchování hodnoty před inflací. Mezi nevýhody řadíme nutnost připojení k internetu a anonymitu. Absentující centrální autorita, která by měnu regulovala, je další uváděnou nevýhodou. Tyto negativní vlastnosti pak zapříčiňují, že OČTŘ a obecně pak státy mají velmi ztížené možnosti nelegální aktivity odhalit a následně potrestat.

Trestněprávní klasifikace činů spáchaných v souvislosti s kryptoměnami je tak poměrně složitá, neboť otázka virtuálních měn není prozatím v tuzemských trestních předpisech nijak explicitně upravena. Na začátek je tedy nezbytné vymezit právní povahu virtuálních měn. Podle § 489 OZ chápeme věc v právním slova smyslu jako cokoliv, co se odlišuje od osoby a slouží potřebě lidí.

[194] Tato finanční krize bývá často označována jako internetová bublina/horečka (angl. dot.com bubble), neboť šlo o masivní propad cen veškerých technologických akcií.

[195] EUROPEAN CENTRAL BANK. *Virtual Currency Schemes – October 2012* [online]. Frankfurt am Main, 2012, s. 5 [cit. 2022-05-28]. ISBN: 978-92-899-0862-7. Dostupné z: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

[196] HAYES, Adam. 10 Important Cryptocurrencies Other than Bitcoin. In: *Investopedia* [online]. 2022 [cit. 2022-05-28]. Dostupné z: https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/

Dozajista budou virtuální měny zmíněnou definici naplňovat a půjde tak o nehmotnou věc v právním slova smyslu (srov. § 496 odst. 2 OZ), což bude mít konsekvence i do práva trestního.

Aktuálně skokově rostoucí aktivitou v kyberprostoru představuje odcizování virtuálních měn z digitálních peněženek. Jestliže virtuální měny chápeme jako věci v právním slova smyslu, pak bychom takový skutek mohli kvalifikovat jako krádež podle § 205 TZ, což potvrdil i v roce 2017 Krajský soud v Brně, který pachatele za odcizení bitcoinů odsoudil za zvlášť závažný zločin krádeže.[197] Druhou otázkou, která zde vyvstává, je možnost aplikace § 230 TZ, tedy trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací. Bez pochyby bude pachatel překonávat bezpečnostní opatření, neboť digitální peněženky jsou zabezpečeny heslem, případně i privátním klíčem, nicméně se nabízí otázka, zda jsou peněženky vůbec samostatným počítačovým systémem. Komentářová literatura chápe počítačový systém jako hardwarovou a softwarovou výbavu, která zpracovává data automaticky, tedy bez lidského přičinění.[198] Nicméně zákonodárce se v recentní novele TZ, nabývající účinnosti 28. 6. 2022, rozhodl jít cestou přímé definice počítačového systému jako takového a definoval ho následovně: *„Počítačovým systémem se rozumí i data uložená, zpracovaná, opětovně vyhledaná nebo přenesená tímto zařízením anebo skupinou zařízení za účelem jeho nebo jejich provozu, použití, ochrany a údržby“.*[199] Osobně se domnívám, že aplikace § 230 TZ na kryptoměnové peněženky může být poněkud diskutabilní a bude zapotřebí stanovit určité mantinely alespoň judikaturou.

Relativní anonymita virtuálních měn je učinila nadmíru zajímavými i pro legalizaci výnosu z trestné činnosti a financování terorismu, ačkoliv dříve byly tradičně pro takové aktivity upřednostňovány hotovostní transakce, neboť ty nezanechávají téměř žádné dohledatelné stopy.[200] *„Virtuální měny přitom představují prvek, s jehož využitím lze přerušit stopu převáděných prostředků. Byť v důsledku zachování elektronické stopy mohou být takové platby dosledovatelné, s ohledem na anonymitu uživatelů a další podmínky těchto služeb je používání měny tohoto typu z hlediska opatření proti praní peněz a financování terorismu třeba považovat za velmi rizikové.“*[201]

[197] Rozsudek Krajského soudu v Brně ze dne 9. 10. 2017, sp. zn. 50T 4/2017.

[198] GŘIVNA, Tomáš. Neoprávněný přístup k počítačovému systému a nosiči informací - § 230. In: ŠÁMAL, Pavel a kolektiv. *Trestní zákoník II – komentář. Zvláštní část (§ 140–421).* 2. vydání. Praha: C.H.Beck, 2012. s. 2300–2315. ISBN 978-80-7400-428-5.

[199] Zákon č. 130/2022 Sb., znění účinné od 28.6.2022, 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.

[200] VANDEZANDE, Niels. *Virtual currencies: a legal framework*. Cambridge: Intersentia, 2018, s. 278–279. ISBN 978-1-78068-675-2.

[201] Důvodová zpráva k návrhu zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, s. 46, sněmovní tisk 385.

Na využívání kryptoměn k zastření nelegálních aktivit reagovala nedávno i Evropská unie s cílem stanovit jednotná pravidla pro sledování převodů kryptoaktiv. Hospodářský a měnový výbor Evropského parlamentu (ECON) dne 31. března 2022 schválil návrh zákona, který zpřísňuje pravidla pro uživatele kryptoměnových peněženek. Cílem tak je, aby veškeré podezřelé transakce mohly být snadněji sledovatelné, čehož se má dosáhnout identifikací uživatelů a následnou povinností prokázat původ finančních prostředků.[202] Ačkoliv prozatím nebyl návrh veřejností přijat s nadšením, z hlediska možné eliminace trestné činnosti spojené s kryptoměnami lze návrh vnímat jako pozitivní posun na nadnárodní úrovni.

Novým a v současnosti i narůstajícím trendem v oblasti kryptoměn, je cryptojacking. Cryptojacking představuje typ útoku, při němž pachatel pomocí malwaru (angl. coin miners programmes) napadne jakákoliv mobilní či počítačová zařízení a následně takový zdroj využívá k těžbě kryptoměn. Škodlivý malware je uživatelem nevědomky stažen z webových stránek nebo jako součást mobilních aplikací. Vzhledem k tomu, že samotná těžba kryptoměn je jinak velmi finančně náročná, představuje cryptojacking pro pachatele téměř nenákladnou metodu. Také na rozdíl od jiných útoků zůstává cryptojacking mnohdy po celou dobu neodhalen, a to vzhledem k tomu, že nijak nezneužívá data oběti, výhradně jen výpočetní výkon. Zůstává nicméně otázkou, zda je tuzemské trestní právo na takový typ útoku schopno nějak reagovat.

V neposlední řadě našly kryptoměny uplatnění i u ransomwarových útoků – v těchto případech půjde o tzv. crypto-ransomwarové útoky, tedy o škodlivé programy, které zašifrují uložená data a následně za ně požadují výkupné. Platby jsou samozřejmě ve všech případech vyžadovány v bitcoinech, případně jiných kryptoměnách tak, aby nebylo možné pachatele dohledat.

Virtuální měny jsou fenoménem, který vzhledem ke své anonymitě představuje pro pachatele trestné činnosti stále nové příležitosti, čemuž mimo jiné přispívá i fakt, že zákonodárce se této problematice věnuje opravdu jen zcela marginálně. Bylo by tedy dle mého názoru vhodné se kryptoměnami zabývat i v rovině trestněprávní, tedy koncentrovat pozornost nejenom na hmotněprávní úpravu (zejména zabývat se možnými novými druhy útoků a jejich promítnutím do skutkových podstat), ale spíše na aspekty procesněprávní. Je otázkou, jakými instituty by OČTŘ například vůbec zjistily, že obviněný nějaké kryptoměny vlastní, případně jak by k takovému účtu

[202] EUROPEAN PARLIAMENT. *Crypto assets: new rules to stop illicit flows in the EU* [online]. 31. března 2022 [cit. 2022-05-29]. Dostupné z: https://www.europarl.europa.eu/news/en/press-room/20220324IPR26164/crypto-assets-new-rules-to-stop-illicit-flows-in-the-eu

získaly přístup bez znalosti seed phrase[203]. Někteří autoři doporučují zaměřit pozornost na rozšíření Budapešťské úmluvy o ustanovení, která by popisovala nové druhy trestných činů souvisejících s nárůstem kryptoměn a dále rozšířit Budapešťskou úmluvu o zbývající státy, které ji doposud nepodepsaly.[204]

[203] Seed phrase je bezpečnostní fráze až 24 (náhodných) po sobě jdoucích slov, které se využívají k zabezpečení kryptoměnových peněženek.

[204] VIRGA, Joy Marie. International criminals and their virtual currencies: the need for an international effort in regulating virtual currencies and combating cyber crime. *Revista de Direito Internacional*. Brasilia: Centro Universitario de Brasilia – UniCEUB, 2015, 12(2), s. 525–526. ISSN 2236-997X. Dostupné z: doi:10.5102/rdi.v12i2.3557

ZÁVĚR

Kybernetická kriminalita je problematika nesporně nadmíru důležitá, neboť lze důvodně očekávat, že bude čím dál tím intenzivněji docházet k přesunu tradiční kriminality do virtuálního prostředí. Svědčí tomu zejména rapidní technologický pokrok, uživatelská neznalost kyberprostředí, lhostejnost uživatelů k možnostem digitálního zabezpečení a rostoucí technické dovednosti pachatelů. Dále tomu nasvědčuje fakt, že většina každodenních aktivit se pomalu, ale jistě přesouvá do kyberprostoru, což potvrdila mimo jiné i pandemie onemocnění COVID-19. Vše zmíněné je navíc taktéž umocněno bázlivou reakcí právního řádu, který se se specifickými atributy kybernetické trestné činnosti vypořádává vždy s určitým zpožděním.

Trestní zákoník v roce 2009 do jisté míry reagoval na narůstající společensky škodlivá jednání, která nebylo možné subsumovat podle skutkových podstat klasických trestných činů. Následně byly do zvláštní části včleněny tři skutkové podstaty trestných činů vztahujících se ke kybernetické kriminalitě, konkrétně vznikl § 230, § 231 a § 232 trestního zákoníku. Lze konstatovat, že současná hmotněprávní úprava je prozatím v rámci možností dostačující, a tedy že útoky páchané v kyberprostoru jsme schopni subsumovat právě pod zmíněné ryze počítačové trestné činy, případně je podřadit pod jinou skutkovou podstatu, nejčastěji pod trestný čin podvodu. Problematická situace z hlediska trestněprávní kvalifikace vyvstává u DoS, případně taktéž u DDoS útoků, které dle mého názoru nejsou adekvátně trestně postižitelné. V této oblasti by de lege ferenda bylo vhodné, aby došlo k vytvoření nové skutkové podstaty, která by byla schopna danou problematiku reflektovat. Obdobný nedostatek lze spatřovat u cryptojackingu.

Orgány činné v trestním řízení nejsou v jednoduché situaci, neboť odhalování a vyšetřování kybernetických útoků je náročné z toho důvodu, že vyžaduje kvalifikované lidské zdroje, moderní technické vybavení a sdílení získaných znalostí a postupů. Nadto je nutné disponovat efektivní procesní úpravou, která by jim práci usnadňovala. Nedostatek lze spatřovat v poměrně dlouhých lhůtách, se kterými trestní řád pracuje, což se z hlediska vyšetřování kybernetické trestné činnosti nemusí jevit jako dostačující. Extrémní dynamičnost digitálních stop může zapříčinit, že po určité době již stopy nebudou existovat, případně dojde k jejich modifikaci. Nelehká situace se jeví i v případě prokazování viny za pomocí elektronických důkazů, u kterých zpravidla nelze jednoznačně a bez důvodných pochybností dovodit, že daná osoba čin skutečně spáchala, a to vzhledem k možnosti jejich snadné manipulace. Z uvedeného vyplývá, že je zapotřebí elektronické důkazy chápat jako důkazy podpůrné a v rámci trestního řízení tak vytvořit ucelený a uzavřený řetězec nepřímých důkazů.

Úskalím pro trestní právo budou především kryptoměny, které nalezly v rámci nelegálních aktivit různorodé využití a těší se tak velké oblibě. Kromě toho, že bývají mnohdy terčem útoku, slouží taktéž k zastření nelegálního původu peněžních prostředků. Tuzemská právní úprava nikterak s virtuálními měnami nepracuje, možný právní rámec nabízí pouze evropské či mezinárodní právo. Problematickou oblastí bude pro trestní řízení otázka zajišťování kryptoměn. Orgány činné v trestním řízení aktuálně nedisponují žádnými procesními nástroji, které by jim umožnily zjistit, kam pachatel odcizené kryptoměny uložil. Následné zajištění a uchování virtuálních měn pro účely trestního řízení je rovněž poněkud obtížné.

Kyberkriminalita klade nároky nejen na zákonodárce a orgány činné v trestním řízení, nýbrž na každého uživatele internetu. Kromě problematiky týkající se potrestání samotného pachatele je stěžejní i otázka prevence, která by měla směřovat vůči každému koncovému uživateli internetu, neboť právě ten bývá velmi často terčem útoku. Prevence by především měla cílit na rizikové skupiny, jako jsou děti a mládež. Nejen, že tyto skupiny bývají kvůli své důvěřivosti velmi často oběťmi útoků jako kyberstalking, sexting či kyberšikana, ale stávají se mnohdy jejich samotnými pachateli. Signifikantní pro boj s kyberkriminalitou je posilování mezinárodní spolupráce, neboť kyberkriminalita se zřídka omezuje na hranice jednoho státu.

Třebaže ze statistických údajů vyplývá, že kybernetická trestná činnost tvoří poměrně nepodstatnou výseč veškeré páchané trestné činnosti, nelze z těchto důvodů danou problematiku opomíjet. Jak bylo již mnohokrát zmíněno, jde o činnost nadmíru latentní a ve většině případů neregistrovanou. Vzhledem k její dynamické proměnlivosti a zdlouhavé reakci zákonodárce, lze tvrdit, že pachatelé budou vždy při páchání kyberzločinu o krok před zákonem. Z těchto důvodů je stěžejní vytvořit takový obecný legislativní základ, který bude připraven vypořádat se s budoucím technologickým vývojem, a tudíž i novými způsoby páchání trestné činnosti. Zvyšující se nároky jsou mimo to kladeny i na samotný stát, který bude muset do budoucna být schopen zabezpečit kritické informační systémy a infrastrukturu, neboť lze očekávat, kupříkladu z důvodu probíhající digitalizace veřejné správy, že bude docházet k nárůstu kybernetických útoků směřujících vůči státu.

SEZNAM POUŽÍVANÝCH ZKRATEK

ADA	Cardano	
AZ		Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským
BIS		Bezpečnostní informační služba
BitB	Browser in the Browser	Prohlížeč v prohlížeči
BTC	Bitcoin	
BYOD	Bing Your Own Device	Přines si vlastní zařízení
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence	Centrum excelence NATO pro kybernetickou obranu
C-PROC	Cybercrime Programme Office of the Council of Europe	Kancelář Rady Evropy pro počítačovou kriminalitu
ČR		Česká republika
DDoS	Distributed Denial of Service	Distribuované odmítnutí služby
DEFR	Digital Evidence First Responder	Odborně kvalifikovaná osoba, která jako první nakládá s digitálním důkazem
DFA	Digital Forensics Analysis	Digitální forenzní analýza
DoS	Denial of Service	Odmítnutí služby
EC3	European Cybercrime Centre	Evropské centrum pro boj proti kyberkriminalitě
ECON	Committee on Economic and Monetary Affairs	Hospodářský a měnový výbor Evropského parlamentu
ENISA	The European Union Agency for Cybersecurity	Agentura Evropské unie pro bezpečnost sítí a informací
EPP		Evropský předávací příkaz
ETH	Ethereum	
EU	European Union	Evropská unie

EUCTF	European Union Cybercrime Task Force	Pracovní skupina Evropské unie pro boj s kyberkriminalitou
EUP		Evropský uchovávací příkaz
EUROPOL	European Police Office	Evropský policejní úřad
ICT	Information and Communication Technologies	Informační a komunikační technologie
INCYDER	International Cyber Developments Review	Interaktivní databáze nejdůležitějších dokumentů týkajících se kyberbezpečnosti
IOCE	International Organization on Computer Evidence	Mezinárodní organizace pro zajišťování počítačových důkazů
IOCTA	Internet Organized Crime Threat Assessment	Hodnocení hrozeb organizované trestné činnosti na internetu
IT	Information Technology	Informační technologie
IP	Internet Protocol	Protokol internetu
ISP	Internet Service Provider	Poskytovatel internetového připojení
J-CAT	Joint Cybercrime Action Taskforce	Společná pracovní skupina pro boj proti kyberkriminalitě
LTC	Litecoin	
LZPS		Listina základních práv a svobod
MitM	Man-in-the-middle attack	Kybernetický útok spočívající v zachycování přenášených dat
NATO	North Atlantic Treaty Organization	Severoatlantická aliance
NCI	NATO Communication and Information Academy	Akademie NATO zaměřující se na kybernetické vzdělávání
NIAS	NATO Information Assurance Symposium	Konference NATO o zajišťování informací
NIST	National Institute of Standards and Technology	Národní institut USA pro standardy a technologie
NÚKIB		Národní úřad pro kybernetickou a informační bezpečnost
OČTŘ		Orgány činné v trestním řízení

OSN		Organizace spojených národů
OZ		Zákon č. 89/ 2012 Sb., občanský zákoník
PolČR		Zákon č. 273/2008 Sb., o Policii ČR
SDEU		Soudní dvůr Evropské unie
SMS	Short Message Service	
SWGDE	Scientific Working Group on digital Evidence	Vědecká pracovní skupina zabývající se digitálními důkazy
T-CY	Cybercrime Convention Committee	Výbor k Úmluvě o počítačové kriminalitě
TŘ		Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád)
TZ		Zákon č. 40/2009 Sb., trestní zákoník
UNODC	United Nations Office on Drugs and Crime	Úřad OSN pro drogy a kriminalitu
ÚS		Ústavní soud
VOIP	Voice over Internet Protocol	Telefonní hovor uskutečněný skrze internetovou síť
VPN	Virtual Private Network	Soukromá virtuální síť
Wi-Fi	Wireless Fidelity	Bezdrátová síť
XMR	Monero	
ZEK		Zákon č. 127/2005 Sb., o elektronických komunikacích

SEZNAM POUŽITÝCH ZDROJŮ

Seznam použité literatury

ADRIAN, Angela. *Law and Order in virtual worlds: exploring avatars, their ownership and rights*. Hershey: Information Science Reference, 2010. ISBN 978-1-61520-795-4.

ALKIVIADOU, Natalie. The Legal Regulation of Hate Speech: The International and European Frameworks. *Politička misao*. Zagreb: Sveuciliste u Zagrebu, Fakultet Politckih Znanosti, 2018, 55(4), s. 220. ISSN 0032-3241. Dostupné z: doi:10.20901/pm.55.4.08.

ÅRNES, André. *Digital Forensics (1st ed.)*. Hoboken, NJ: John Wiley & Sons Inc., 2018. ISBN 978-1-119-26238-1.

BARTOŇ, Michal. Virtuální pornografie, limity svobody umělecké tvorby a svobody projevu a trestní zákon. *Právní rozhledy*. 2008, roč. 16, č. 17, s. 617–627.

BRUNER, Tomáš. O možnostech právní ochrany před kybernetickým útokem ze zahraničí podle mezinárodního práva veřejného. *Právník*. 2015, roč. 154. č. 4.

CASEY, Eoghan. *Digital evidence and computer crime: forensic science, computers and the Internet*. 3. vydání. Waltham, MA: Academic Press, 2011. ISBN 978-0-12-374268-1.

CLOUGH, Jonathan. A world of difference: the Budapest Convention on Cybercrime and the challenges of harmonisation. *Monash University Law Review*. 2014, roč. 40, č. 3, s. 701. ISSN 0311-3140. Dostupné z: doi:10.3316/agis_archive.20152955.

CLOUGH, Jonathan. *Principles of Cybercrime*. Cambridge, UK; New York: Cambridge University Press, 2010. ISBN 978-0-521-89925-3.

COHEN, Lawrence E. a Marcus FELSON. Social Change and Crime Rate Trends: A Routine Activity Approach. *American sociological review*. 1979, roč. 44, č. 4. ISSN 0003-1224.

ČÁP, Jan, Lukáš BREU a Zdeněk PROKEŠ. Zajišťování, zpřístupňování a vyhodnocování digitálních stop. *Bezpečnostní teorie a praxe*. 2022, č. 1. ISSN 1801-8211.

ČENTÉŠ, Jozef. *Odpočúvanie – procesnoprávne a hmotnoprávne aspekty*. Bratislava: C.H.Beck, 2013. ISBN 978-80-89603-09-1.

DOSTÁL, Otto. Zajišťování důkazů u počítačové kriminality – dožádání, vydání věci a prohlídky (1. díl). *Trestněprávní revue*. 2019, č. 3, s. 66–71.

DOSTÁL, Otto. Zajišťování důkazů u počítačové kriminality – odposlech a údaje o komunikaci (2. díl). *Trestněprávní revue*. 2019, č. 4, s. 77–83.

DOSTÁL, Otto. Zajišťování důkazů u počítačové kriminality – sledování, důkazy od oznamovatelů (3. díl). *Trestněprávní revue*. 2019, č. 5.

DOSTÁL, Otto. Zajišťování důkazů u počítačové kriminality – úložiště, e-maily, telefony, sociální sítě a logy (4. díl). *Trestněprávní revue*. 2019, č. 6.

DRAŠTÍK, Antonín, Robert FREMR, Tomáš DURDÍK, Miroslav RŮŽIČKA a Alexander SOTOLÁŘ. *Trestní zákoník: komentář (I.díl)*. Praha: Wolters Kluwer, 2015. ISBN 978-80-7478-790-4.

DRMOLA, Jakub. Konceptualizace kyberterorismu. *Vojenské rozhledy*. 2013, č. 2. ISSN 1210-3292.

DVOŘÁK, Marek. Phishing, pharming a jejich trestněprávní postih. *Trestněprávní revue*. 2018, č. 4.

EFRONY, Dan a Yuval SHANY. A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice. *The American Journal of International Law*. New York, USA: Cambridge University Press, 2018, roč. 112, č. 4, s. 584-585. ISSN 0002-9300. Dostupné z: doi:10.1017/ajil.2018.86.

FIALOVÁ, Eva. Krádež virtuálních předmětů v příkladech z nizozemské judikatury. *Revue pro právo a* technologie. 2010, č. 1.

GARCIA-RUIZ, Miguel A., Miguel Vargas MARTIN, Amin IBRAHIM, Arthur EDWARDS a Raul AQUINO-SANTOS. Combating Child Exploitation in Second Life. *2009 IEEE Toronto International Conference Science and Technology for Humanity (TIC-STH)*. IEEE, 2009, s.761-766. Dostupné z: doi:10.1109/TIC-STH.2009.5444398.

GARGULÁK, Michal. Kriminalizace nekonsensuální pornografie v České republice. *Trestněprávní revue*. 2018, č. 2, s. 30–35.

GIBSON, William. *Neuromancer*. 20th anniversary ed. New York: Ace Books, 2004. ISBN 978-0-441-01203-9.

GORDON, Sarah. The Virus Writer and The Reporter. *Information security technical report*. 2001, roč. 6(4). ISSN 1363-4127. Dostupné z: doi:10.1016/S1363-4127(01)00408-3.

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

HATHAWAY, Oona A., Rebecca CROOTOF, Philip LEVITZ, Haley NIX, Aileen NOWLAN, William PERDUE a Julia SPIEGEL. The Law of Cyber-Attack. *California law review*. Berkeley: Joe Christensen, Inc. for students of School of Law, University of California, Berkeley, 2012, 100(4). ISSN 0008-1221.

HLAVÁČOVÁ, Kateřina a Oliver CHORVÁT. Přístup orgánů činných v trestním řízení k datům uloženým v cloudu. *Revue pro právo a technologie*. 2016, č. 14, s. 3–24.

HOLT, Thomas J. *Cybercrime Through an Interdisciplinary Lens*. Abingdon, Oxon: Routledge, 2017. ISBN 978-1-315-61845-6.

HOQUE, Nazrul, Dhruba K BHATTACHARYYA a Jugal K KALITA. Botnet in DDoS Attacks: Trends and Challenges. *IEEE Communications surveys and tutorials*. New York: IEEE, 2015, 17(4). ISSN 1553-877X. Dostupné z: doi:10.1109/COMST.2015.2457491.

HŘEBÍČEK, Vladislav. *Prohlídky u advokátů: (§ 85b trestního řádu)*. Praha: Leges, 2017. Praha. ISBN 978-80-7502-231-8.

CHANG, Wei-jung. Cyberstalking and Law Enforcement. *Procedia Computer Science*. Elsevier B.V, 2020, 176, s. 1190. ISSN 1877-0509. Dostupné z: doi:10.1016/j.procs.2020.09.115.

CHIESA, Raoul, Stefania DUCCI a Silvio CIAPPI. *Profiling hackers: the science of criminal profiling as applied to the world of hacking*. Boca Raton: Auerbach Publications, 2009. ISBN 978-1-4200-8693-5.

CHNG, Samuel, Han Yu LU, Ayush KUMAR a David YAU. Hacker types, motivations and strategies: A comprehensive framework. *Computers in human behavior reports*. 2022, roč. 5, 100167. ISSN 2451-9588. Dostupné z: doi:10.1016/j.chbr.2022.100167.

CHRISTOU, George. *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*. London: Palgrave Macmillan UK, 2016. ISBN 978-1-137-40052-9.

JELÍNEK, Jiří. K chybějící právní úpravě tzv. prostorového odposlechu v trestním řádu. *Bulletin advokacie*. 2018, č. 7–8.

JELÍNEK, Jiří. *Trestní zákoník a trestní řád s poznámkami a judikaturou*. 8. vydání. Praha: Leges, 2020. ISBN 978-80-7502-395-7.

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

JORDAN, Tim a Paul TAYLOR. A sociology of hackers. *The Sociological review (Keele)*. Oxford, UK: Blackwell Publishing, 1998, roč. 46, č. 4. ISSN 0038-0261. Dostupné z: doi:10.1111/1467-954X.00139.

KALVODOVÁ, Věra, Milana HRUŠÁKOVÁ a kolektiv. *Dokazování v trestním řízení – právní, kriminologické a kriminalistické aspekty*. Brno: Masarykova univerzita, 2015. ISBN 978-80-210-8072-0.

KARMÁŠEK, Jaroslav a Lenka SUCHÁNKOVÁ. Prohlídka jiných prostor v nichž advokát vykonává advokacii – externí úložiště dat – cloud. *Bulletin advokacie*. 2014, č. 11.

KENNEY, Michael. Cyber-Terrorism in a Post-Stuxnet World. *Orbis (Philadelphia)*. 2015, roč. 59, č. 1, s. 123–124. ISSN 0030-4387. Dostupné z: doi:10.1016/j.orbis.2014.11.009.

KESSLER, Oliver a Wouter WERNER. Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare. *Leiden journal of international law*. Cambridge, UK: Cambridge University Press, 2013, roč. 26, č. 4, s. 773–774. ISSN 0922-1565. Dostupné z: doi:10.1017/S0922156513000411.

KHONJI, Mahmoud, Youssef IRAQI a Andrew JONES. Phishing Detection: A Literature Survey. *IEEE Communications surveys and tutorials*. New York: IEEE, 2013, roč. 15, č. 4, s. 2092. ISSN 1553-877X. Dostupné z: doi:10.1109/SURV.2013.032213.00009.

KIRWAN, Grainne a Andrew POWER. *Cybercrime: The Psychology of Online Offenders*. Cambridge: Cambridge University Press, 2013. ISBN 978-1-107-00444-3.

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

KONRÁD, Zdeněk, Viktor PORADA, Jiří STRAUS a Jaroslav SUCHÁNEK. *Kriminalistika: Kriminalistická taktika a metodiky vyšetřování*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. ISBN 978-80-7380-547-0.

KOPECKÝ, Kamil a René SZOTKOWSKI. Cyberbullying, cyber aggression and their impact on the victim – The teacher. *Telematics and informatics*. 2017, roč. 34, č. 2. ISSN 0736-5853. Dostupné z: doi:10.1016/j.tele.2016.08.014.

KSHETRI, Nir, Jeffrey VOAS a Jeffrey VOAS. Cryptojacking. *Computer (Long Beach, Calif.)*. Los Alamitos: IEEE, 2022, roč. 55, č. 1. ISSN 0018-9162. Dostupné z: doi:10.1109/MC.2021.3122474.

KUBÍČEK, Miroslav a Přemysl POLÁK. *Zákon o mezinárodní justiční spolupráci ve věcech trestních: komentář*. Praha: Wolters Kluwer, 2014. ISBN 978-80-7478-389-0.

LUKÁŠOVÁ, Kateřina. Škodlivý obsah na Internetu. *Acta Universitatis Carolinae - Iuridica*. 2012, č. 4, s. 19. ISSN 0323-0619.

MADARIE, Renushka. Hackers' Motivations: Testing Schwartz's Theory of Motivational Types of Values in a Sample of Hackers. *International journal of cyber criminology*. Thirunelveli: International Journal of Cyber Criminology, 2017, roč. 11(1). ISSN 0974-2891. Dostupné z: doi:10.5281/zenodo.495773.

MUSIL, Stanislav. *Počítačová kriminalita: nástin problematiky: kompendium názorů specialistů*. Praha: Institut pro kriminologii a sociální prevenci, 2000. ISBN 80-86008-80-0.

PAPEŽ, Vladimír. Nejvyšší soud zaujal stanovisko k výkladu pojmu „jiné prostory, v nichž advokát vykonává advokacii“. *Bulletin advokacie*. 2015, č. 9.

POBOŘILOVÁ, Michaela. Virtuální dětská pornografie. *Acta Universitatis Carolinae – Iuridica*. 2012, č. 4. ISSN 0323-0619.

POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kolektiv. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015. ISBN 978-80-210-8073-7.

PORADA, Viktor a Eduard BRUNA. Digitální svět a dokazování obsahu elektronických dokumentů. *Bezpečnostní technologie, systémy a management*. 2013, č. 3.

PORADA, Viktor a Jiří STRAUS. *Kriminalistické stopy – Teorie, metodologie, praxe*. Plzeň: Aleš Čeněk, 2012. ISBN 978-80-7380-396-4.

PORADA, Viktor a Karel RAIS a kolektiv. *Právní, kriminalistické a kybernetické aspekty kybernetické kriminality a bezpečnosti: pocta Vladimíru Smejkalovi*. Brno: Akademické nakladatelství CERM, 2021. ISBN 978-80-7623-065-1.

PORADA, Viktor a kolektiv. *Kriminalistika – Technické, forenzní a kybernetické aspekty*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2016. ISBN 978-80-7380-589-0.

POŠÍKOVÁ, Lenka. Získávání telekomunikačních dat jako nástroj v boji s internetovou kriminalitou. *Acta Universitatis Carolinae – Iuridica*. Univerzita Karlova v Praze, Nakladatelství Karolinum, 2012, (4). s. 39–56. ISSN 0323-0619.

PYZALSKI, Jacek. From cyberbullying to electronic aggression: typology of the phenomenon. *Emotional and behavioural difficulties*. Taylor & Francis, 2012, roč. 17, č. 3–4. ISSN 1363-2752. Dostupné z: doi:10.1080/13632752.2012.704319.

RAK, Roman a Viktor PORADA. Vlastnosti digitálních stop a jejich dopady na forenzní šetření. *Soudní inženýrství*. 2005, roč. 16, č. 4.

RAYMOND, Eric. *The New Hacker's Dictionary*. [b.m.]: MIT Press, 1996. ISBN 0-262-68069-6.

ROGERS, Marcus K. A Two-dimensional Circumplex Approach to the Development of a Hacker Taxonomy. *Digital investigation*. 2006, roč. 3, č. 2. ISSN 1742-2876. Dostupné z: doi:10.1016/j.diin.2006.03.001.

ROJSZCZAK, Marcin. The uncertain future of data retention laws in the EU: Is a legislative reset possible? *The computer law and security report*. 2021, roč. 41. ISSN 0267-3649. Dostupné z: doi:10.1016/j.clsr.2021.105572.

SCHMITT, Michael N. *Tallinn manual 2.0 on the International Law Applicable to Cyber Operations*. Second edition. Cambridge: Cambridge University Press, 2017, s. xxv. ISBN 978-1-316-63037-2.

SMEJKAL, Vladimír a Michal VALÁŠEK. Co všechno lze falzifikovat v ICT aneb důkazy nejsou vždy důkazy. In: *Sborník příspěvků z mezinárodní vědecké kriminalistické konference "Pokroky v kriminalistice 2017" konané na Policejní akademii České republiky v Praze ve dnech 12. a 13. září 2017*. Praha: Policejní akademie České republiky, 2018. ISBN 978-80-7251-485-4.

SMEJKAL, Vladimír. Elektronický podpis. *Právní rádce*. 2004, roč. XII, č. 12.

SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018. ISBN 978-80-7380-720-7.

SMEJKAL, Vladimír. Ochrana dat advokátů v elektronických úložištích. *Bulletin advokacie*. 2015, č. 3.

SVETLIK, Marian. Co je předmětem zkoumání digitální forenzní analýzy? *Digital Forensic Review*. 2019, č. 2. ISSN 2570-5059.

SÝKORA, Michal. Trestní postih cyberstalkingu. *Acta Universitatis Carolinae – Iuridica*. 2012, č. 4, s. 98. ISSN 0323-0619.

ŠÁMAL, Pavel a kolektiv. *Trestní řád – komentář I+II. díl*. 6. vydání. Praha: C.H. Beck, 2008. ISBN 978-80-7400-043-0.

ŠÁMAL, Pavel a kolektiv. *Trestní zákoník I – komentář. Obecná část (§ 1–139)*. 2. vydání. Praha: C.H. Beck, 2012. ISBN 978-80-7400-428-5.

ŠÁMAL, Pavel a kolektiv. *Trestní zákoník II – komentář. Zvláštní část (§ 140–421)*. 2. vydání. Praha: C.H. Beck, 2012. ISBN 978-80-7400-428-5.

ŠÁMAL, Pavel, Jan MUSIL, Josef KUCHTA a kolektiv. *Trestní právo procesní*. 4. přepracované vydání. Praha: C. H. Beck, 2013. ISBN 978-80-7400-496-4.

ŠČERBA, Filip a kolektiv. *Trestní zákoník – komentář (§ 205 až 421)*. Praha: C. H. Beck, 2020. ISBN 978-80-7400-807-8.

ŠELLENG, Dalibor. K některým aspektům trestného činu porušení autorského práva, práv souvisejících s právem autorským a práv k databázi podle § 270 trestního zákoníku. *Acta MUP – Právní ochrana duševního vlastnictví*. roč. 2018, č. 2, s. 37–45. ISSN 1804-6932.

TLAPÁK NAVRÁTILOVÁ, Jana a Ingrid GALOVCOVÁ. Uchovávání dat uložených v počítačovém systému – poskytování součinnosti, nebo nahrazování činnosti orgánů činných v trestním řízení? *Bulletin advokacie*. 2019, č.11.

TSAGOURIAS, Nikolaos a Russell BUCHAN. *Research Handbook on International Law and Cyberspace*. 2. vydání. Cheltenham, UK: Edward Elgar Publishing Limited, 2021. ISBN 978-1-78990-424-6.

VANDEZANDE, Niels. *Virtual currencies: a legal framework*. Cambridge: Intersentia, 2018. ISBN 978-1-78068-675-2.

VANDUCHOVÁ, Marie, Tomáš GŘIVNA a OTO NOVOTNÝ. *Pocta Otovi Novotnému k 80. narozeninám*. Praha: ASPI, 2008. ISBN 978-80-7357-365-2.

VANTUCH, Pavel. K postihu stalkingu (nebezpečného pronásledování) podle § 354 trestního zákoníku. *Trestní právo*. 2011, roč. 16, č. 2, s. 5–13.

VEBER, Jaromír, Zdeněk SMUTNÝ a Ladislav VYSKOČIL. Practice of Digital Forensic Investigation in the Czech Republic and ISO/IEC 27037:2012 [in Czech]. *Acta Informatica Pragensia*. 2015, roč. 4.

VIRGA, Joy Marie. International criminals and their virtual currencies: the need for an international effort in regulating virtual currencies and combating cyber crime. *Revista de Direito Internacional*. Brasilia: Centro Universitario de Brasilia - UniCEUB, 2015, 12(2). ISSN 2236-997X. Dostupné z: doi:10.5102/rdi.v12i2.3557.

VOLEVECKÝ, Petr. Kybernetické trestné činy v trestním zákoníku. *Trestní právo*. 2010, roč. 14, č. 7–8, s. 19–43.

WEIMANN, Gabriel. Cyberterrorism: The Sum of All Fears? *Studies in conflict and terrorism*. Taylor & Francis Group, 2005, roč. 28(2). ISSN 1057-610X. Dostupné z: doi:10.1080/10576100590905110.

WESTERLUND, Mika. The Emergence of Deepfake Technology: A Review. *Technology Innovation Management Review*. Ottawa: Talent First Network, 2019, 9(11). ISSN 1927-0321. Dostupné z: doi:10.22215/timreview/1282.

WHITTAKER, Elizabeth a Robin M. KOWALSKI. Cyberbullying Via Social Media. *Journal of school violence*. London: Routledge, 2015, roč. 14, č. 1. ISSN 1538-8220. Dostupné z: doi:10.1080/15388220.2014.949377.

Seznam použité judikatury

Nález Ústavního soudu ze dne 22. 5. 1997, sp. zn. III. ÚS 287/96.

Rozsudek Krajského soudu v Brně ze dne 9. 10. 2017, sp. zn. 50T 4/2017.

Rozsudek Mezinárodního soudního dvora ze dne 27. 6. 1986, Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). International Court of Justice Reports, 1986.

Rozsudek Nejvyššího soudu Spojených států amerických ze dne 16.4.2002, sp. zn. 535 U.S. 234.

Rozsudek SDEU ze dne 8. 9. 2016 ve věci GS Media BV v. Sanoma Media Netherlands BV a další (Věc C-160/15).

Rozsudek soudu v Leeuwardenu ze dne 21. 10. 2008, č.j. 17/96/6123-07 VEV.

Rozsudek soudu v Amsterdamu ze dne 2. 4. 2009, sp. zn. LJN: BH9789.

Stanovisko trestního kolegia Nejvyššího soudu ze dne 25. 6. 2015, sp. zn. Tpjn 306/214.

Usnesení Městského soudu v Praze ze dne 9. 7. 2014, sp. zn. Nt 615/2014.

Usnesení Nejvyššího soudu ze dne 12. 3. 2014, sp. zn. 5 Tdo 196/2014.

Usnesení Nejvyššího soudu ze dne 13. 2. 2019, sp. zn. 8 Tdo 100/2019.

Usnesení Nejvyššího soudu ze dne 15. 12. 2010, sp. zn. 5 Tdo 1312/2010.

Usnesení Nejvyššího soudu ze dne 16. 5. 2018, sp. zn. 4 Tdo 456/2018.

Usnesení Nejvyššího soudu ze dne 17. 12. 2013, sp. zn. 4 Tdo 1333/2013.

Usnesení Nejvyššího soudu ze dne 18. 1. 2012, sp. zn. 6 Tdo 1677/2011.

Usnesení Nejvyššího soudu ze dne 25. 11. 2020, sp. zn. 8 Tdo 1041/2020.

Usnesení Nejvyššího soudu ze dne 27. 2. 2013, sp. zn. 8 Tdo 137/2013.

Usnesení Nejvyššího soudu ze dne 29. 11. 2011, sp. zn. 4 Pzo 5/2011.

Usnesení Nejvyššího soudu ze dne 29. 5. 2013, sp. zn. 5 Tdo 271/2013.

Usnesení Nejvyššího soudu ze dne 7. 5. 2019, sp. zn. 4 Tdo 1591/2018.

Usnesení Nejvyššího soudu ze dne 8. 9. 2011, sp. zn. 8 Tdo 1082/2011.

Usnesení SDEU ze dne 21. 10. 2014 ve věci BestWater International GmbH proti Michael Mebes a Stefan Potsch (Věc C-348/13).

Usnesení Ústavního soudu ze dne 26. 10. 2015, sp. zn. I. ÚS 2878/14.

Usnesení Ústavního soudu ze dne 3. 10. 2013, sp. zn. III. ÚS 3812/2012.

Seznam použitých právních předpisů

Dodatkový protokol č. 9/2015 Sb. m. s. k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů.

Směrnice Evropského parlamentu a Rady 2001/29/ES ze dne 22. 5. 2001 o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti.

Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. 7. 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací.

Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. 3. 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí.

Směrnice Evropského parlamentu a Rady 2009/110/ES ze dne 16. 9. 2009 o přístupu k činnosti institucí elektronických peněz, o jejím výkonu a o obezřetnostním dohledu nad touto činností.

Směrnice Evropského parlamentu a Rady 2011/92/EU ze dne 13. 12. 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii.

Směrnice Evropského parlamentu a Rady 2013/40/ES ze dne 12. 8. 2013 o útocích na informační systémy.

Směrnice Evropského parlamentu a Rady 2014/41/EU ze dne 3. 4. 2014 o evropském vyšetřovacím příkazu v trestních věcech.

Směrnice Evropského parlamentu a Rady 2015/2366 ze dne 25. 11. 2015 o platebních službách na vnitřním trhu.

Úmluva o ochraně dětí proti sexuálnímu vykořisťování a pohlavnímu zneužívání. In: *Sbírka mezinárodních smluv České republiky*. 2016, částka 37, s. 1170–1214.

Úmluva o počítačové kriminalitě. In: *Sbírka mezinárodních smluv České republiky*. 2013, částka 56, s. 10785–10837.

Ústavní zákon č. 1/1993 Sb., Ústava České republiky.

Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod.

Vyhláška č. 503/2020 Sb., o výkonu znalecké činnosti.

Vyhláška č. 504/2020 Sb., o znalečném.

Vyhláška č. 505/2020 Sb., kterou se stanoví seznam znaleckých odvětví jednotlivých znaleckých oborů, jiná osvědčení o odborné způsobilosti, osvědčení vydaná profesními komorami a specializační studia pro obory a odvětví.

Zákon č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních.

Zákon č. 121/2000 Sb., autorský zákon.

Zákon č. 127/2005 Sb., o elektronických komunikacích.

Zákon č. 141/1961 Sb., o trestním řízení soudním.

Zákon č. 154/1994 Sb., o bezpečnostní informační službě.

Zákon č. 169/1999 Sb., o výkonu trestu odnětí svobody.

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti.

Zákon č. 254/2019 Sb., o znalcích, znaleckých kancelářích a znaleckých ústavech.

Zákon č. 273/2008 Sb., o Policii ČR.

Zákon č. 289/2005 Sb., o Vojenském zpravodajství.

Zákon č. 301/2005 Z.z., trestný poriadok.

Zákon č. 370/2017 Sb., o platebním styku.

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

Seznam použitých internetových zdrojů

BERTHÉLÉMY, Chloé. New Belgian data retention law: a European blueprint? In: *EDRi* [online]. 2021 [cit. 2022-03-19]. Dostupné z: https://edri.org/our-work/new-belgian-data-retention-law-a-european-blueprint/.

BRENT, Laura. NATO's role in cyberspace. In: *NATO Review* [online]. 12. února 2019 [cit. 2022-06-02]. Dostupné z: https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html.

CCDCOE. *Locked Shields* [online]. Tallinn: CCDCOE. [cit. 2022-06-02]. Dostupné z: https://ccdcoe.org/exercises/locked-shields/.

COUNCIL OF EUROPE. *Octopus 2021: Cooperation against Cybercrime*. Key messages [online]. 18. listopadu 2021 [cit. 2022-06-01]. Dostupné z: https://rm.coe.int/octopus-conference-2021-key-messages-v18nov2021/1680a494e6.

ENISA. About ENISA – The European Union Agency for Cybersecurity. *ENISA* [online]. [cit. 2022-05-31]. Dostupné z: https://www.enisa.europa.eu/about-enisa.

EUROPEAN CENTRAL BANK. *Virtual Currency Schemes – October 2012* [online]. Frankfurt am Main, 2012 [cit. 2022-05-28]. ISBN: 978-92-899-0862-7. Dostupné z: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

EUROPEAN COMMISSION. *Shaping Europe's digital future – The Digital Europe Programme* [online]. [cit. 2022-06-01]. Dostupné z: https://digital-strategy.ec.europa.eu/en/activities/digital-programme.

EUROPEAN PARLIAMENT. *Crypto assets: new rules to stop illicit flows in the EU* [online]. 31. března 2022 [cit. 2022-05-29]. Dostupné z: https://www.europarl.europa.eu/news/en/press-room/20220324IPR26164/crypto-assets-new-rules-to-stop-illicit-flows-in-the-eu.

EUROPEAN UNION AGENCY FOR CRIMINAL JUSTICE COOPERATION. Joint investigation teams. *The purpose of JITs* [online]. 2021 [cit. 2022-03-24]. Dostupné z: https://www.eurojust.europa.eu/judicial-cooperation/eurojust-role-facilitating-judicial-cooperation-instruments/joint-investigation-teams.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. *Data retention across the EU* [online]. 13. července 2017 [cit. 2022-03-19]. Dostupné z: https://fra.europa.eu/en/publication/2017/data-retention-across-eu.

EUROPOL. European Cybercrime Centre – EC3. In: *Europol* [online]. 1. března 2022 [cit. 2022-05-31]. Dostupné z: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

EVROPSKÁ UNIE. Evropský vyšetřovací příkaz, vzájemná právní pomoc a společné vyšetřovací týmy. In: *Portál evropské e-Justice* [online]. [cit. 2022-03-24]. Dostupné z: https://e-justice.europa.eu/92/CS/european_investigation_order_mutual_legal_assistance_and_joint_investigation_teams.

GILBERT, Nestor. 31 Crucial Insider Threat Statistics: 2022 Latest Trends & Challenges. In: *FinancesOnline* [online]. 2022 [cit. 2022-05-26]. Dostupné z: https://financesonline.com/insider-threat-statistics/.

GUERRA, José Eduardo a Christine JANSSENS. Legal and Practical Challenges in the Application of the European Investigation Order. In: *EUCRIM – The European Criminal Law Associations Forum* [online]. 2019, vol. 1, s. 48–49 [cit. 2022-03-24]. Dostupné z: https://eucrim.eu/media/issue/pdf/eucrim_issue_2019-01.pdf.

HAYES, Adam. 10 Important Cryptocurrencies Other than Bitcoin. In: *Investopedia* [online]. 2022 [cit. 2022-05-28]. Dostupné z: https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/.

HAYES, Adam. Dotcom Bubble. In: *Investopedia* [online]. 25. června 2019 [cit. 2022-05-28]. Dostupné z: https://www.investopedia.com/terms/d/dotcom-bubble.asp.

INTERPOL. *Cybercriminals can unknowingly use your computer to generate cryptocurrency* [online]. 2020 [cit. 2022-05-26]. Dostupné z: https://www.interpol.int/Crimes/Cybercrime/Cryptojacking.

JONES, Caitlin. *Phishing, Vishing, SMiShing, Whaling And Pharming: How To Stop Social Engineering Attacks* [online]. 19. ledna 2022 [cit. 2022-06-04]. Dostupné z: https://expertinsights.com/insights/phishing-vishing-smishing-whaling-and-pharming-how-to-stop-social-engineering-attacks/.

KREMEN, Stanley. Apprehending The Computer Hacker: The Collection and Use of Evidence. In: *Computer Forensics Online* [online]. 1998 [cit. 2022-05-22]. Dostupné z: http://www.shk-dplc.com/cfo/articles/hack.htm.

MATOCHA, Jakub. Virtuální měny a trestní právo. *Právní prostor* [online]. 2016 [cit. 2022-05-29]. Dostupné z: https://www.pravniprostor.cz/clanky/trestni-pravo/virtualni-meny-a-trestni-pravo.

MELL, Peter a Timothy GRANCE. *The NIST Definition of Cloud Computing* National Institute of Standards and Technology [online]. 2011 [cit. 2022-02-22]. Dostupné z: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

MINISTERSTVO VNITRA ČR. Statistiky kriminality – dokumenty. *Zpráva o situaci v oblasti veřejného pořádku a vnitřní bezpečnosti na území České republiky* [online]. [cit. 2022-02-22]. Dostupné z: https://www.mvcr.cz/clanek/statistiky-kriminality-dokumenty.aspx.

MINISTERSTVO VNITRA ČR. *Strategie prevence kriminality v České republice na léta 2022-2027* [online]. 5. října 2021 [cit. 2022-03-11]. Dostupné z: https://prevencekriminality.cz/wp-content/uploads/2021/10/04__spk-2022-2027_strategicka-cast.pdf.

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Kybernetické incidenty pohledem NÚKIB* [online]. 2022 [cit. 2022-06-04]. Dostupné z: https://nukib.cz/download/publikace/vyzkum/03-2022-Novinky.pdf.

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Národní strategie kybernetické bezpečnosti České republiky* [online]. 2020 [cit. 2022-03-11]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/.

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020* [online]. [cit. 2022-02-22]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf.

NATO Communications and Information Agency. *About the NCI Academy* [online]. [cit. 2022-06-02]. Dostupné z: https://www.ncia.nato.int/what-we-do/nci-academy/about-the-nci-academy.html.

NOHE, Patrik. What is an Air Gapped Computer? In: *hashedout by The SSL Store* [online]. 13. března 2018 [cit. 2022-06-11]. Dostupné z: https://www.thesslstore.com/blog/air-gapped-computer/.

PIROCH, Jan a Jan BUMBA. Studie: Dostupnost dětské pornografie snižuje sexuální násilí na dětech. In: *iRozhlas* [online]. 2010 [cit. 2022-06-09]. Dostupné z: https://www.irozhlas.cz/clovek/studie-dostupnost-detske-pornografie-snizuje-sexualni-nasili-na-detech_201012131955_jpiroch.

POLICIE ČR. Kriminalita – Statistické přehledy. In: *Policie.cz* [online]. [cit. 2022-06-15]. Dostupné z: https://www.policie.cz/statistiky-kriminalita.aspx.

POLICIE ČR. Skimming. In: *Policie.cz* [online]. [cit. 2022-06-05]. Dostupné z: https://www.policie.cz/clanek/ncoz-skimming.aspx.

POŽÁR, Josef a Václav HNÍK. *Specifické problémy boje s kybernetickou kriminalitou*. Praha: Policejní akademie ČR v Praze – Fakulta bezpečnostního managementu [online]. [cit. 2022-03-28]. s. 23–24. Dostupné z: https://slideplayer.cz/slide/11176990/.

RADA EVROPSKÉ UNIE. *Nařízení o přeshraničním přístupu k elektronickým důkazům: Rada se dohodla na svém postoji* [online]. 12. prosince 2018 [cit. 2022-03-25]. Dostupné z: https://www.consilium.europa.eu/cs/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/.

RODRIGUES, Katitza a Meri BAGHDASARYAN. UN Committee to begin negotiating new cybercrime treaty amid disagreement among states over its scope. In: *EFF* [online]. 15. února 2022 [cit. 2022-06-03]. Dostupné z: https://www.eff.org/deeplinks/2022/02/un-committee-begin-negotiating-new-cybercrime-treaty-amid-disagreement-among.

SENTINELONE, Inc. Ransomware Research Data Summary. In: *SentinelOne* [online]. 2016 [cit. 2022-03-28]. Dostupné z: https://go.sentinelone.com/rs/327-MNM-087/images/Data%20Summary%20-%20English.pdf.

SHEA, Sharon. 6 different types of hackers, from black hat to red hat. In: *Techtarget* [online]. 2019 [cit. 2022-05-25]. Dostupné z: https://www.techtarget.com/searchsecurity/answer/What-is-red-and-white-hat-hacking.

TUNGGAL, Tyas Abi. *What is Typosquatting (and how to prevent it)* [online]. 8. května 2022 [cit. 2022-06-05]. Dostupné z: http://www.upguard.com/blog/typosquatting.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. *Cybercrime Repository* [online]. 2020 [cit. 2022-06-03]. Dostupné z: https://www.unodc.org/unodc/en/cybercrime/cybercrime-repository.html.

Seznam jiných zdrojů

Důvodová zpráva k návrhu Rozhodnutí Rady č. 2021/0383 (NLE), kterým se členské státy zmocňují, aby v zájmu Evropské unie ratifikovaly druhý dodatkový protokol k Úmluvě o počítačové kriminalitě o posílené spolupráci a zpřístupňování elektronických důkazů.

Důvodová zpráva k zákonu č. 287/2018 Sb. kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a některé další zákony, č. 287/2018 Dz.

Důvodová zpráva k zákonu, kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a některé další zákony, sněmovní tisk 79/0.

Důvodová zpráva k návrhu zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, sněmovní tisk 385.

Důvodová zpráva k zákonu č. č. 254/2019 Sb., sněmovní tisk 72/0.

International Law Commission. Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries. Yearbook of the International Law Commission. 2001, vol. II, Part Two.

Mezinárodní vědecká konference: vliv nových technologií na právo. In: Youtube [online]. 24. března 2022 [cit. 2022-05-17]. Dostupné z: https://www.youtube.com/watch?v=5vL8Ye3xAKU. Kanál uživatele Právnická fakulta UK.

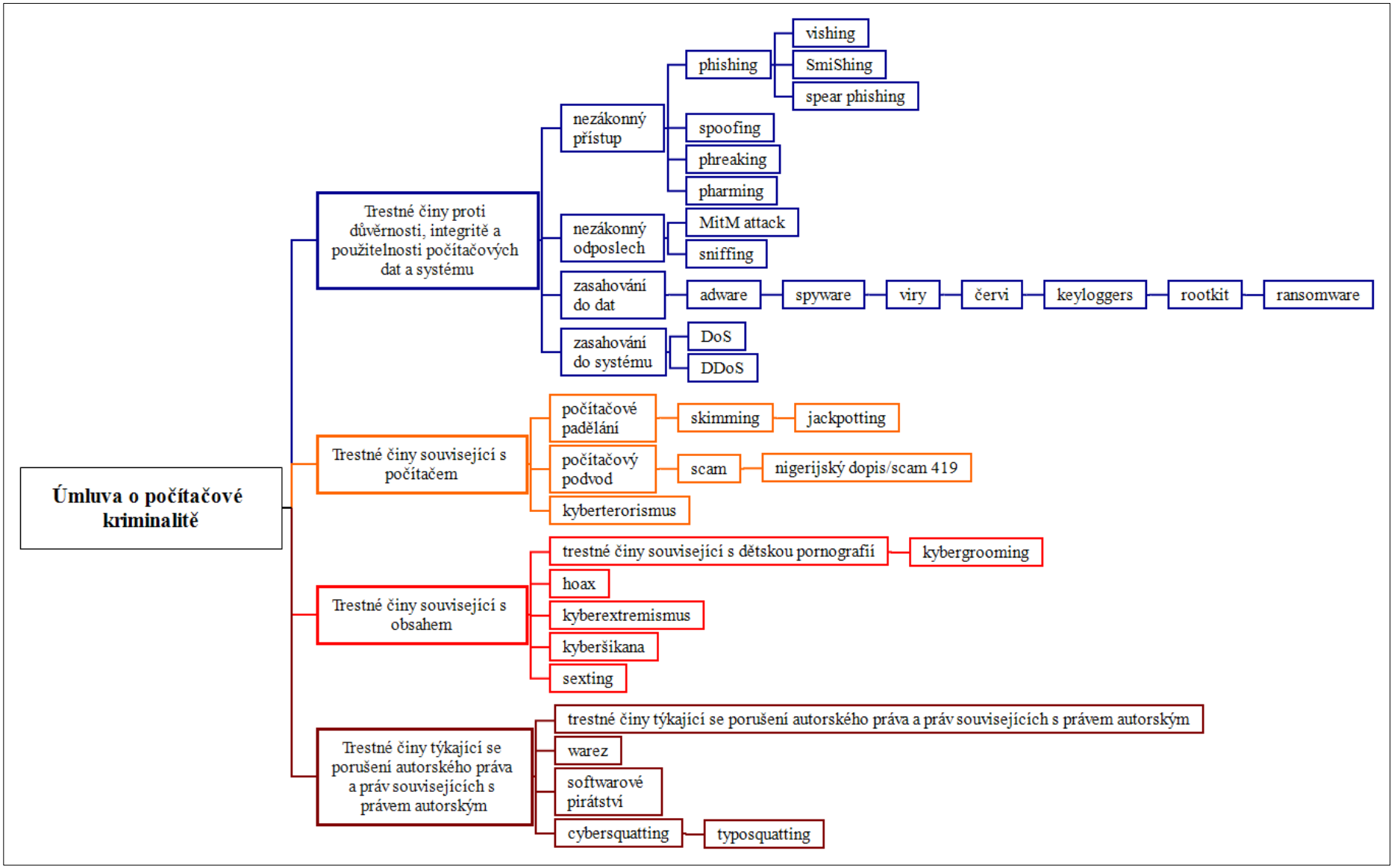
Návrh nařízení Evropského parlamentu a Rady o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech ze dne 17. 4. 2018, č.j.: 2018/0108 (COD).

Výkladové stanovisko poř. č. 1/2015 Sb. v. s. Nejvyššího státního zastupitelství ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek ze dne 26. ledna 2015, sp. zn. 1 SL 760/2014.

PŘÍLOHY

Seznam příloh

Příloha 1 – Schéma kybernetických útoků



NÁZEV DIPLOMOVÉ PRÁCE V ČESKÉM JAZYCE

Kriminalizace útoků na informační systémy

ABSTRAKT

Diplomová práce se zabývá problematikou kriminalizací útoků na informační systémy. Aktuálnost tématu je podržena rapidním vývojem informačních a komunikačních technologií a přesunem každodenních aktivit do virtuálního prostředí. V současné době kybernetická kriminalita představuje rostoucí nebezpečí nejenom pro jednotlivce, ale také pro stát. Cílem práce je představit kybernetické útoky a trestněprávně je klasifikovat. Dále je pozornost koncentrována na procesněprávní stránku útoků, zejména na jejich odhalování, vyšetřování a postup při mezinárodní spolupráci. Opomenut není ani nadnárodní a mezinárodní rámec v boji proti kybernetické kriminalitě. Snahou práce je zjistit jakým problematickým aspektům čelí tuzemská právní úprava a jaký budoucí vývoj v oblasti kyberzločinu lze očekávat.

Úvodní část objasňuje základní pojmy, se kterými práce hojně pracuje. Následně jsou představeny klíčové mezinárodní instrumenty v boji proti kybernetické kriminalitě. Těžiště je věnováno představení jednotlivých druhů kybernetických útoků a jejich následné trestněprávní klasifikaci. Navazující část přibližuje procesní rovinu problematiky, přičemž vymezená část obsahuje taktéž poznatky z kriminologie, jako je typologie pachatelů a jejich motivů. Zmíněna je taktéž problematika aktuálních trendů v kyberprostoru, jako jsou cloudová úložiště, virtuální měny a virtuální krádeže. Závěrem jsou představeny statistické údaje týkající se nápadu kybernetické trestné činnosti v České republice během posledních let a možného předpokládaného budoucího vývoje. Kapitola současně reflektuje i vývoj kybernetické trestné činnosti v souvislosti s koronavirovým onemocněním COVID-19 a probíhajícím válečným konfliktem na Ukrajině. Mimo to jsou prezentovány vize a cíle České republiky v oblasti kybernetické bezpečnosti.

KLÍČOVÁ SLOVA

kybernetická kriminalita, kyberútok, kyberprostor

NÁZEV DIPLOMOVÉ PRÁCE V ANGLICKÉM JAZYCE

The Criminalization of Cyberattacks on Information Systems

ABSTRACT

This master thesis deals with the issue of criminalization of attacks on information systems. The topicality of the topic is supported by the rapid development of information and communication technologies and the shift of everyday activities to the virtual environment. Nowadays, cybercrime poses a growing danger not only to individuals but also to the state. The aim of this thesis is to introduce cyberattacks and to classify them criminally. Furthermore, attention is concentrated on the procedural aspect of attacks, in particular on their detection, investigation and the procedure of international cooperation. The transnational and international framework in the fight against cybercrime is not omitted. The thesis seeks to identify what problematic aspects domestic legislation faces and what future developments in the field of cybercrime can be expected.

The introductory section explains the basic terms that are used extensively in the thesis. Subsequently, key international instruments in the fight against cybercrime are introduced. The focus is on introducing the different types of cyberattacks and their subsequent criminal classification. The subsequent part introduces the procedural level of the issue, while the defined part also includes findings from criminology, such as the typology of perpetrators and their motives. The issue of current trends in cyberspace such as cloud storage, virtual currencies and virtual theft is also mentioned. Finally, statistical data concerning the incidence of cybercrime in the Czech Republic in recent years and possible future developments are presented. At the same time, the chapter also reflects on the development of cybercrime in the context of the COVID-19 coronavirus disease and the ongoing war conflict in Ukraine. In addition, the vision and goals of the Czech Republic in the field of cyber security are presented.

KEYWORDS

cybercrime, cyberattack, cyberspace