https://doi.org/10.5817/RPT2023-2-2

VYŠETŘOVÁNÍ KYBERNETICKÉ KRIMINALITY A JEJÍ PŘEDPOKLÁDÁNÝ BUDOUCÍ VÝVOJ[1]

PAVLA STANKOVÁ[2]

ABSTRAKT

Článek představuje problematiku jedné z rapidně se vyvíjejících oblastí trestné činnosti – kriminalitu kybernetickou. Pozornost je zaměřena na její odhalování a následné vyšetřování kriminalistickým, ale i trestněprávním prismatem, zejména je poukázáno na nedostatky, se kterými se orgány činné v trestním řízení potýkají. Opomenut není rovněž ani mezinárodní boj s kyberkriminalitou, zejména pak přeshraniční instituty, které vyšetřování napomáhají. Článek pracuje se statistickými údaji, kdy je nastíněn současný, ale i předpokládaný budoucí vývoj kybernetické kriminality v České republice. Závěrem je zmíněna otázka budoucnosti České republiky v oblasti kybernetické bezpečnosti.

KLÍČOVÁ SLOVA:

Kyberkriminalita; vyšetřování kyberkriminality; statistické údaje v oblasti kybernetické kriminality; kyberbezpečnost České republiky; budoucí vývoj; covid-19 a jeho vliv na kyberzločin

---

[1] Tento text vychází z autorčiny diplomové práce s názvem “Kriminalizace útoků na informační systémy” , která byla zveřejněna v rámci digitálního repozitáře UK viz https://dspace.cuni.cz/handle/20.500.11956/179367. Diplomová práce byla zmíněna v sekci "Recenze závěrečných prací I/2023" v Revue pro právo a technologie č. 27, roč. 14, 2023.

[2] Mgr. Pavla Stanková je asistentkou soudce na Městském soudě v Praze. Kontaktní e-mail: padza.s@seznam.cz

ABSTRACT

The article presents the issue of one of the rapidly developing areas of crime - cybercrime. Attention is focused on its detection and subsequent investigation by criminalistic, but also criminal law view, in particular, it is pointed out the shortcomings that law enforcement authorities face. The international fight against cybercrime is also not neglected, in particular the cross-border institutes that facilitate the investigation. The article works with statistical data, outlining the current and projected future development of cybercrime in the Czech Republic. Finally, the question of the future of the Czech Republic in the field of cyber security is mentioned.

KEY WORDS:

Cybercrime; Cybercrime Investigation; Cybercrime Statistics; Cybersecurity of the Czech Republic; Future of Cybercrime; COVID-19 and its Impact on Cybercrime

1. ÚVOD

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. S ohledem na variabilitu a dynamičnost nelegálních aktivit v kyberprostoru, se musela kriminalistika, ale i trestní právo vypořádat s nedostatečností běžných institutů a vyšetřovacích metod.

Článek přibližuje problematiku vyšetřování kyberkriminality, kdy je pozornost koncentrována na digitální stopy včetně jejich zajišťování a není opomenuta ani nezastupitelná role znalce při zkoumání těchto stop. Je poukázáno na problematické aspekty vyšetřování, načež jsou představeny instituty trestního řádu a mezinárodní justiční spolupráce, které vyšetřování umožňují. Teoretické poznatky jsou podpořeny statistickými údaji. Variabilita kyberprostoru je demonstrována na koronavirové pandemii a rovněž na

probíhajícím ozbrojeném konfliktu na Ukrajině. Závěrem je představena situace České republiky v oblasti kybernetické bezpečnosti a nastíněn možný budoucí vývoj kyberkriminality.

2. DIGITÁLNÍ STOPY A JEJICH ZAJIŠŤOVÁNÍ

Pro vyšetřování kyberkriminality, potažmo pro účely následného trestního řízení, hrají nezastupitelnou roli digitální stopy. Přiléhavou definici nabídla 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“*.[3] 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.

Nezastupitelnou roli při zajišťování digitálních stop plní metody digitální forenzní analýzy (DFA). První metoda, kterou DFA aplikuje, je tzv. tradiční, někdy také klasická digitální forenzní analýza, která předpokládá 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

[3] PORADA, Viktor a Eduard BRUNA. Digitální svět a dokazování obsahu elektronických dokumentů. *Bezpečnostní technologie, systémy a management*. [online]. 2013. [cit. 24. 8. 2023], s. 3.

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 (tzv. 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.[4]

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. 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.

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:

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

- „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“*.[5]

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.[6]

3. ROLE ZNALCE

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.

[5] 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.

[6] Ibidem, s. 253.

Hlavní činnost znalce spočívá ve vypracování znaleckého posudku, ve kterém prostřednictvím svých odborných znalostí posuzuje skutečnosti mu předložené zadavatelem posudku. 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.

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. Nutno podotknout, že neodborné zásahy mohou vést ke ztrátě digitálních stop, a proto je účast znalce i v takových případech potřebná. Pakliže nepůjde zajistit celý počítačový systém nebo nosič informací, může znalec vytvořit na místě identickou bitovou kopii nosiče.[7] 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 znaleckého dokazování a znaleckých posudků z oblasti kyberkriminality, lze spatřovat ve vytvoření nového seznamu znaleckých oborů, jako je obor informační a komunikační technologie a kybernetická bezpečnost.[8]

4. PROBLEMATICKÉ ASPEKTY VYŠETŘOVÁNÍ A DOKAZOVÁNÍ KYBERKRIMINALITY

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

[7] KOLOUCH, Jan. *CyberCrime*. 1.vydání. Praha: CZ.NIC, z.s.p.o., 2016, s. 453.

[8] Seznam nových znaleckých oborů a odvětví byl zaveden do právního řádu zákonem č. 254/2019 Sb., resp. vyhláškou 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, a to s účinností od 1. ledna 2021.

důkazů se zvyšující časovou prodlevou značně 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.[9] 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. Možné řešení nabízí identifikace prostřednictvím metadat[10]. Někteří autoři nicméně poukazují na možné nedostatky vyvstávající při dokazování skrze přeceňovaná metadata 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 taktéž pozměnit.[11]

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. Praxe vyšetřování a stíhání kyberkriminality se nicméně potýká s jistými problémy i na straně vyšetřovatelů, kdy jde zejména o personální deficit pracovníků specializujících se na IT systémy. Podle autorů Požára a Hníka jde dále o nedostatečné softwarové vybavení a nevhodné organizační uspořádání specializovaných policejních pracovišť.[12]

---

[9] Srov. se zásadou nemo tenetur se ipsum accusare.

[10] Metadata jsou strukturovaná data poskytující informace o datech v digitalizovaných dokumentech.

[11] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018. s. 709–710.

[12] POŽÁR, Josef a Václav HNÍK. *Specifické problémy boje s kybernetickou kriminalitou* [online]. Praha: Policejní akademie ČR v Praze – Fakulta bezpečnostního managementu. [cit. 24. 8. 2023]. s. 23–24.

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.[13] 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).“*[14]

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. 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). Rovněž v neposlední řadě může orgánům činným v trestním řízení při vyšetřování pomoci i institut podpůrných operativně pátracích prostředků, zejména pak osoba informátora (taktéž konfidenta).

[13] PORADA, Viktor a Jiří STRAUS. *Kriminalistika (výzkum, pokroky, perspektivy)*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2014, s. 525.

[14] Ibidem, s. 523–524.

5. INSTITUTY TRESTNÍHO ŘÁDU NAPOMÁHAJÍCÍ VYŠETŘOVÁNÍ KYBERKRIMINALITY

5.1 DOMOVNÍ PROHLÍDKA

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.

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).[15] 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, konzultanta 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 přimě-*

[15] PORADA, Viktor a kolektiv. *Kriminalistika: technické, forenzní a kybernetické aspekty*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2016. s. 798–799.

řeně a dostatečně zdůvodněno.“[16] 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 neopakovatelnosti v příkazu nemusí nutně znamenat nezákonnost takové prohlídky.[17] *„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.“*[18]

5.2 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 (…)“*.[19] 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 taktéž velmi přísné podmínky pro jeho aplikaci.

Pozitivní úpravu daného institutu nalezneme v § 88 TŘ, kde 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

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

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

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

[19] 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.

(§ 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 činy.[20] 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.

V souvislosti s vyšetřováním kybernetické kriminality je v poslední době poměrně hojně diskutovaný recentní 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 (až na 90 dnů) a 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, tedy na základě zmíněného by bylo možné institut aplikovat i na obsah komunikace na sociálních sítích, ale taktéž na obsah emailové komunikace.[21] Zajímavé rovněž je i to, že daný institut nikterak nereflektuje zá-

[20] 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.

[21] 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.

važnost vyšetřovaného trestného činu, tedy lze jej de facto aplikovat na jakýkoliv trestný čin. Problematická se dle mého názoru taktéž jeví dikce zákona, která uvádí, že příkaz může být vydán policejním orgánem i bez předchozího souhlasu státního zástupce. Ačkoliv se z hlediska vyšetřování kyberkriminality zcela jistě jedná o institut, který má potenciál její vyšetřování urychlit i objasnit, je zapotřebí zamyslet se nad tím, zda aplikací tohoto institutu nedochází k obcházení jiných procesních institutů (jako je například odposlech), u kterých zákonodárce pragmaticky stanovil přísné podmínky jejich aplikace.

5.3 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.[22] Opačný názor zastává

[22] KOLOUCH, Jan. *CyberCrime*. 1.vydání. Praha: CZ.NIC, z. s. p. o., 2016, s. 443.

Dostál, který poukazuje na to, že pokud nějaká data mají být zajištěná, musí nejdříve vůbec existovat.[23] Ani judikatura však nezaujala shodný názor. V roce 2011 Nejvyšší soud jednoznačně potvrdil, že § 88 TŘ lze uplatnit do budoucna, kdežto § 88a TŘ nikoliv.[24] 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“*.[25]

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[26] (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, právní řády některých členských států příslušnou povinnost retence stále obsahují.[27] Současnou úpravu uchovávání dat vybraných členských zemí EU přibližuje následující tabulka.

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

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

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

[26] 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.

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

Země	**Povinnost retence dat**
Belgie	zrušena v roce 2021[28]
Česká republika	6 měsíců
Francie	12 měsíců
Itálie	30 měsíců
Polsko	12 měsíců

Tabulka 1 – Srovnání povinnosti uchovávání dat ve vybraných státech EU[29]

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[30] 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. Jsem toho názoru, že získávání dat na základě § 66 PolČR by nemělo prvotně sledovat získávání důkazů pro trestní řízení, neboť vzhledem k velmi specifickému okruhu podmínek stanovených dle PolČR bylo nejspíše snahou zákonodárce minimalizovat pokusy obcházení § 88a TŘ.

[28] BERTHÉLÉMY, Chloé. New Belgian data retention law: a European blueprint? In: *EDRi.* [online]. 2021 [cit. 24. 8. 2023] Dostupné z: https://edri.org/our-work/new-belgian-data-retention-law-a-european-blueprint/

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

[30] 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).

5.4 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[31] 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.[32] V neposlední řadě lze i v rámci kyberkriminality využít institutu použití agenta dle § 158e TŘ, a to za účelem infiltrace skupin na dark webu.[33]

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

[31] 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.

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

[33] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z. s. p. o., 2016, s. 451.

přeshraničního získávání důkazů nabídla členským státům několik možných nástrojů.

6.1 EVROPSKÝ VYŠETŘOVACÍ PŘÍKAZ (EVP)

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.

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.[34]

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 po-

[34] 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. 24. 8. 2023]. Dostupné z: https://eucrim.eu/media/issue/pdf/eucrim_issue_2019-01.pdf

psat 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.

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, 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.[35]

6.3 ALTERNATIVNÍ MECHANISMY KE STÁVAJÍCÍM INSTITUTŮM MEZINÁRODNÍ JUSTIČNÍ SPOLUPRÁCE

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.[36] Návrh nařízení reagoval na roztříštěné právní úpravy členských států a na rostoucí aktivitu páchání trestných činů v oblasti kyberprostoru. Nařízení mimo jiné vytváří dva zcela nové instituty, a to evropský předávací příkaz

[35] European Union Agency For Criminal Justice Cooperation. Joint investigation teams. In: *eurojust.europa.eu*. [online]. [cit. 24. 8. 2023]. Dostupné z: https://www.eurojust.europa.eu/judicial-cooperation/eurojust-role-facilitating-judicial-cooperation-instruments/joint-investigation-teams.

[36] Dne 25. ledna 2023 potvrdila Rada dohodu s Evropským parlamentem o návrhu nařízení a návrhu směrnice o přeshraničním přístupu k elektronickým důkazům.

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. Oba zmíněné instituty by pak měly zrychlit a zúčelnit přeshraniční přístup k případným elektronickým důkazům.

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. Důvod vzniku tohoto institutu 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 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.

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 přijetím 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.

7. KYBERKRIMINALITA – PROBLÉM MODERNÍ DOBY?

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 bylo odůvodňováno narůstajícími případy koronavirového onemocnění COVID-19, ale především spíše legislativní změnou trestního zákoníku[37], která mimo jiné posunula hranice škody nikoliv nepatrné z původních pěti tisíc na deset tisíc korun. Rok 2022 byl z hlediska nárůstu kyberkriminality zlomový, neboť bylo zaznamenáno 18 554 skutků, což je oproti roku 2021 nárůst o téměř 95 %. K nejčastěji páchaným trestným činům prostřednictvím kyberprostoru řadíme majetkovou trestnou činnost, zejména podvodná jednání, kdy signifikantní nárůst byl zaznamenán u inzertních podvodů (zejména podvody reverzní) a v neposlední řadě jsou ve větším množství páchány trestné činy podle § 230 TZ (neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací), § 231 TZ (opatření a přechovávání přístupového zařízení a hesla k počítačovému

[37] 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.

systému a jiných takových dat) a § 232 TZ (neoprávněný zásah do počítačového systému nebo nosiče informací z nedbalosti).

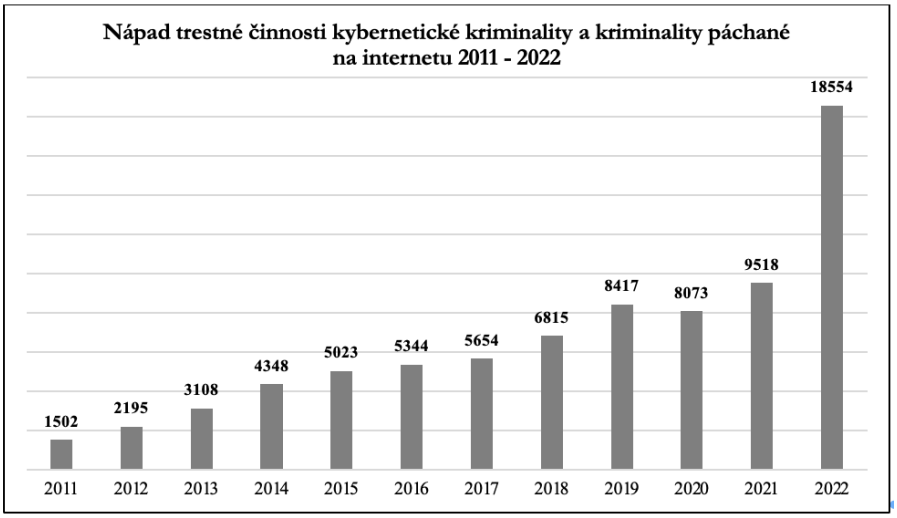
Mezi nejčastěji páchaným typem útoku za rok 2022 byl phishing a jeho různé podoby, kdy tyto útoky byly v České republice zpravidla realizovány zasíláním podvodných e-mailů. V menším měřítku útočníci využívali i podvodných telefonátů (tzv. vishing) či zasílání podvodných sms zpráv (tzv. SMiShing). Minulý rok byla na území České republiky zpozorována rovněž i nová phishingová technika s názvem Browser in the Browser (BitB).[38] Takový útok pak uživateli otevřel podvodné přihlašovací okno, které se zobrazilo jako součást běžného internetového prohlížeče a vybídlo uživatele k zadání přihlašovacích údajů.[39]

Podle oficiálních údajů z minulého roku tvoří nápad trestné činnosti kybernetické kriminality 10 % 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 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.

Nápad trestné činnosti kybernetické kriminality a kriminality páchané na internetu v České republice mezi lety 2011 až 2022 přibližuje následující graf.

[38] NÚKIB. Kybernetické incidenty pohledem NÚKIB [online]. 2022 [cit. 29.10.2023]. Dostupné z: https://nukib.cz/download/publikace/vyzkum/03-2022-Novinky.pdf

[39] GRUSTNIY, Leonid. Browser-in-the-browser attack: a new phishing technique. In: kaspersky.com. [online]. 25.5.2022. [29.10.2023]. Dostupné z: https://www.kaspersky.com/blog/browser-in-the-browser-attack/44163/



*Graf **1** – Nápad trestné činnosti kybernetické kriminality a kriminality páchané na internetu v letech 2011-2022*[40]

7.1 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. Pachatele v kyberprostoru po-

[40] Ministerstvo vnitra České republiky. *Statistiky kriminality – dokumenty (hodnocení bezpečnostní situace, statistiky kriminality)*. Zpráva o situaci v oblasti veřejného pořádku a vnitřní bezpečnosti na území České republiky. [online]. Poslední změna 17. 7. 2023. [cit. 24. 8. 2023]. Dostupné z: https://www.mvcr.cz/clanek/statistiky-kriminality-dokumenty.aspx

vzbudil též fakt, že se souvisejícími karanténami a prací z domova, došlo mezi zaměstnavateli k nárůstu přístupu BYOD *(Bring Your Own Device)*[41]. 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. Taktéž cíle kybernetických útoků velmi přiléhavě reagovaly na koronavirovou situaci, neboť touto dobou byl i největší nárůst útoků zaznamenán u nemocnic a jiných zdravotnických zařízení (příkladmo lze uvést útok na Fakultní nemocnici Brno či Psychiatrickou nemocnici Kosmonosy).

7.2 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 i nadále budou narůstat útoky na kritické informační a komunikační systémy. Vliv ozbrojeného konfliktu na český kyberprostor potvrzují i data poskytnutá NÚKIB za rok 2022, kdy byl zaznamenán zvýšený počet útoků (zejména DDoS) stran ruských hackerů převážně na české subjekty veřejného sektoru, což velmi pravděpodobně souviselo s podporou, kterou Česká republika vyjádřila Ukrajině.[42] Obecně byl taktéž

[41] BYOD je novým trendem na poli pracovněprávních vztahů, kdy zaměstnancům je ze strany zaměstnavatele umožněno přinést si do práce vlastní výpočetní techniku, kterou na pracovišti využívají pro výkon práce.

[42] NÚKIB. Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022. [online] 2023, s. 15. [cit. 28.10.2023]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2022.pdf

zaznamenán zvýšený počet kyberútoků od počátku války na cíle v členských zemí NATO až o 300 %.[43]

S ohledem na připravovanou digitalizaci veřejné správy lze mít za to, že kybernetická trestná činnost bude v budoucnu cílit na nejzranitelnější strategický cíl, jakým je veřejný sektor. Tuto domněnku rovněž podporuje i zpráva Agentury EU pro kybernetickou bezpečnost za rok 2022, která vyhodnotila, že sektor veřejné správy zaznamenal nejvyšší procento kybernetických incidentů.[44]

Možným řešením je posílení kybernetické bezpečnosti v kritických oblastech, jako je energetika, průmysl a zdravotnictví. Osobně se domnívám, že by pozornost měla být koncentrována na spolupráci mezi orgány působícími v oblasti kybernetické bezpečnosti, jako je PČR a NÚKIB (Národní úřad pro kybernetickou a informační bezpečnost), přičemž opomenuta by rovněž neměla zůstat spolupráce se soukromým sektorem. Je nutné zmínit, že jedním z nejdůležitějších prostředků v boji proti potenciální kriminalitě je bezpochyby posilování mezinárodní spolupráce mezi státy.

7.3 BUDOUCNOST ČESKÉ REPUBLIKY NA POLI KYBERNETICKÉ BEZPEČNOSTI

NÚKIB 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 obsahuje cíle a vize republiky v oblasti kybernetické

[43] Google Threat Analysis Group (TAG). Fog of War – How the Ukraine Conflict Transformed the Cyber Threat Landscape. In: services.google. [online]. 16. 2. 2023. [cit. 29. 10. 2023]. Dostupné z: https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf

[44] European Parliament. Cybersecurity: main and emerging threats. In: euparl.europa.eu. [online]. 21. 3. 2023. [cit. 30. 10. 2023]. Dostupné z: https://www.europarl.europa.eu/pdfs/news/expert/2022/1/story/20220120STO21428/20220120STO21428_en.pdf

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“*.[45]

Druhým dokumentem, určujícím aktuální směřování České republiky v oblasti kybernetické bezpečnosti, je Strategie prevence kriminality v České republice na léta 2022-2027. Strategie je vypracována Ministerstvem vnitra v součinnosti s Republikovým 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, které nejenom, že se stávají často oběťmi, ještě častěji se ale stávají jejími 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.

Srovnání vybraných cílů strategických dokumentů představuje následující tabulka.

[45] Národní úřad pro kybernetickou a informační bezpečnost. Národní strategie kybernetické bezpečnosti České republiky na období let 2021-2025. In: *NUKIB.cz*. [online]. 2. 12. 2020. [cit. 24. 8. 2023]. Dostupné z: Národní úřad pro kybernetickou a informační bezpečnost - Strategie / Akční plán (nukib.cz)

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 podmíněnéh o kybernásilí	podpora policejní spolupráce v oblasti řešení kyberkriminality

Tabulka 2 – Srovnání vybraných cílů strategických dokumentů v oblasti kybernetické bezpečnosti

Vyjma výše uvedených dokumentů determinují budoucnost České republiky na poli kybernetické bezpečnosti i legislativní akty EU, jmenovitě stojí za zmínku recentně přijatá NIS2 směrnie[46] (Network and Information Systems), jejíž požadavky mají být implementovány do českého právního řádu v druhé polovině roku 2024. Směrnice koncentruje pozornost zejména na oblasti jako je zdravotnictví, energetika, veřejný sektor, bankovnictví, poskytovatelé digitálních služeb, tedy ta odvětví, která jsou v současné době velmi náchylná ke kybernetickým incidentům a rozšiřuje tak okruh subjektů, které jsou povinny zabezpečovat své systémy. Povinné subjekty v daných odvětvích budou podrobeny přísnější regulaci z hlediska bezpečnostních opatření, kdy budou zajišťovat míru kybernetické bezpečnosti, identifikovat, vyhodnocovat rizika a zajišťovat bezpečnost IT infrastruktury. Požadavky směrnice představují takové stěžejní změny v oblasti kybernetické bezpečnosti, pročež bylo přistoupeno k vytvoření zcela nového návrhu zákona o kybernetické bezpečnosti.

[46] Směrnice Evropského parlamentu a Rady 2022/2555 ze dne 14. 12. 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii.

Bezpečnost v oblasti kyberprostoru je rovněž každoročně posilována účastí České republiky na mezinárodních bezpečnostních cvičeních s názvem Locked Shields, která jsou pořádána ve spolupráci s NATO, kdy primárním cílem je testovat obranu národních kritických infrastruktur fiktivních zemí v reálném čase, přičemž tyto útoky odpovídají závažným a sofistikovaným kybernetickým incidentům.[47]

Z výše zmíněného lze zpozorovat, že kybernetická bezpečnost v České republice postupně směřuje k vybudování pevné základny, která v budoucnu zajistí potřebnou míru takového zabezpečení, čímž bude zajištěna schopnost čelit nejrůznějším kybernetickým útokům.

8. 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.

Nutno dodat, že ani 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. Boj s kyberkriminalitou nikterak neulehčuje ani fakt, že velká část kybernetických útoků, není orgánům činným v trestním řízení vůbec oznámena. Trestní řád disponuje řadou procesních institutů, které vyšetřování kybernetické kriminality usnadňují, kdy se specificky jde jmenovat institut domovních prohlídek, od-

[47] CCDCOE. Locked Shields. Tallinn: CCDCOE. In: ccdcoe.org. [online]. [cit. 29. 10. 2023]. Dostupné z: https://ccdcoe.org/exercises/locked-shields/

poslechů a záznamů telekomunikačního provozu, vyžádání údajů o uskutečněném telekomunikačním provozu a operativně pátrací prostředky. Procesní nedostatek lze spatřovat v poměrně dlouhých lhůtách, se kterými trestní řád, potažmo zákon o mezinárodní justiční spolupráci, pracuje, což se z hlediska vyšetřování kybernetické trestné činnosti nemusí jevit vždy 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 digitálních stop, potažmo 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.

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 měla především měla cílit na rizikové skupiny, jako jsou děti a mládež. Nejen, že tyto skupiny bývají kvůli své důvěřivosti velmi často oběťmi útoků, ale stávají se mnohdy jejich samotnými pachateli. Klíčové pro boj s touto trestnou činností je rovněž 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 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. Klíčové pro objasňování kyberkriminality je rovněž zajištění proškolených odborníků na straně vyšetřovatelů. Zvyšující se nároky jsou mimo to kladeny i na samotný stát, který bude muset do budoucna být schopen zabezpečit kritické informační sys-

témy a infrastrukturu, neboť lze očekávat, kupříkladu z důvodu probíhající digitalizace veřejné správy, že bude docházet k nárůstu kybernetických útoků směřujících vůči státu. Závěrem je nutné dodat, že nicméně ty největší nároky v boji proti kyberkriminalitě leží na každém z nás.

9. SEZNAM POUŽITÝCH ZDROJŮ

[1] BERTHÉLÉMY, Chloé. New Belgian data retention law: a European blueprint? In: *EDRi*. [online]. 2021 [cit. 24. 8. 2023] Dostupné z: https://edri.org/our-work/new-belgian-data-retention-law-a-european-blueprint/

[2] CCDCOE. Locked Shields. Tallinn: CCDCOE. In: ccdcoe.org. [online]. [cit. 29. 10. 2023]. Dostupné z: https://ccdcoe.org/exercises/locked-shields/

[3] ČÁP, Jan, Lukáš BREU a Zdeněk PROKEŠ. Zajišťování, zpřístupňování a vyhodnocování digitálních stop. *Bezpečnostní teorie a praxe*. 2022. ISSN: 1801-8211.

[4] DOSTÁL, Otto. Zajišťování důkazů u počítačové kriminality – odposlech a údaje o komunikaci (2. díl). *Trestněprávní revue*. 2019, č. 4, s. 77–83. ISSN 1213-5313.

[5] European Parliament. Cybersecurity: main and emerging threats. In: euparl.europa.eu. [online]. 21.3.2023. [cit. 30.10.2023]. Dostupné z: https://www.europarl.europa.eu/pdfs/news/expert/2022/1/story/20220120STO21428/20220120STO21428_en.pdf

[6] European Union Agency For Criminal Justice Cooperation. Joint investigation teams. In: *eurojust.europa.eu*. [online]. [cit. 24. 8. 2023]. Dostupné z: https://www.eurojust.europa.eu/judicial-cooperation/eurojust-role-facilitating-judicial-cooperation-instruments/joint-investigation-teams.

[7] Google Threat Analysis Group (TAG). Fog of War – How the Ukraine Conflict Transformed the Cyber Threat Landscape. In: services.google. [online]. 16. 2. 2023. [cit. 29. 10. 2023]. Dostupné z: https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf

[8] GRUSTNIY, Leonid. Browser-in-the-browser attack: a new phishing technique. In: kaspersky.com. [online]. 25. 5. 2022. [29. 10. 2023]. Dostupné z: https://www.kaspersky.com/blog/browser-in-the-browser-attack/44163/

[9] 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. 24. 8. 2023]. Dostupné z: https://eucrim.eu/media/issue/pdf/eucrim_issue_2019-01.pdf

[10] HEJDUK, Marek. Kriminalistické aspekty odhalování, prověřování a vyšetřování počítačové mravnostní kriminality. *Bezpečnostní teorie a praxe*. 2021, č. 1. ISSN: 1801-8211.

[11] KOLOUCH, Jan. *CyberCrime*. 1. vydání. Praha: CZ.NIC, z.s.p.o., 2016, 524 s. ISBN 978-80-88168-18-8.

[12] Ministerstvo vnitra České republiky. *Statistiky kriminality – dokumenty (hodnocení bezpečnostní situace, statistiky kriminality)*. Zpráva o situaci v oblasti veřejného pořádku a vnitřní bezpečnosti na území České republiky [online]. Poslední změna 17. 7. 2023. [cit. 24. 8. 2023]. Dostupné z: https://www.mvcr.cz/clanek/statistiky-kriminality-dokumenty.aspx.

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

[14] Národní úřad pro kybernetickou a informační bezpečnost. Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025. In: *NUKIB.cz*. [online]. 26. 7. 2021. [cit. 24. 8. 2023]. Dostupné z: Národní úřad pro kybernetickou a informační bezpečnost - Strategie / Akční plán (nukib.cz).

[15] Národní úřad pro kybernetickou a informační bezpečnost. Národní strategie kybernetické bezpečnosti České republiky na období let 2021-2025. In: *NUKIB.cz*. [online]. 2. 12. 2020. [cit. 24. 8. 2023]. Dostupné z: Národní úřad pro kybernetickou a informační bezpečnost - Strategie / Akční plán (nukib.cz).

[16] NÚKIB. Kybernetické incidenty pohledem NÚKIB [online]. 2022 [cit. 29. 10. 2023]. Dostupné z: https://nukib.cz/download/publikace/vyzkum/03-2022-Novinky.pdf

[17] NÚKIB. Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022. [online] 2023, s. 15. [cit. 28. 10. 2023]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2022.pdf

[18] POLČÁK, Radim a kol. *Elektronické důkazy v trestním řízení*. 1. vydání. 2015. Brno: Masyrykova univerzita, Právnická fakulta, 2015. 253 s. Spisy Právnické fakulty Masarykovy univerzity, řada teoretická, Edice Scientia č. 542. ISBN 978-80-210-8073-7.

[19] PORADA, Viktor a Eduard BRUNA. Digitální svět a dokazování obsahu elektronických dokumentů. *Bezpečnostní technologie, systémy a management*. [online]. 2013. [cit. 24. 8. 2023]. Dostupné z: http://trilobit.fai.utb.cz/Data/Articles/PDF/37bacb88-3602-4ea7-b9c8-7864970f89e7.pdf

[20] PORADA, Viktor a Jiří STRAUS. *Kriminalistika (výzkum, pokroky, perspektivy)*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2014, 704 s. ISBN 978-80-7380-477-0.

[21] PORADA, Viktor a kolektiv. *Kriminalistika: technické, forenzní a kybernetické aspekty*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2016, 1024 s. ISBN 978-80-7380-589-0.

[22] POŽÁR, Josef a Václav HNÍK. *Specifické problémy boje s kybernetickou kriminalitou* [online]. Praha: Policejní akademie ČR v Praze - Fakulta bezpečnostního managementu. [cit. 24. 8. 2023]. Dostupné z: http://www.mvcr.cz/soubor/policejni-akademie.aspx

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

[24] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018, 936 s. ISBN 978-80-7380-720-7.

[25] Směrnice Evropského parlamentu a Rady 2022/2555 ze dne 14. 12. 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii.

[26] ŠÁMAL, Pavel, Jan MUSIL, Josef KUCHTA a kolektiv. *Trestní právo procesní*. 4. přepracované vydání. Praha: C. H. Beck, 2013, 1065 s. ISBN 978-80-7400-496-4.

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

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

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

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

[31] 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. 244-257. ISSN: 1805-4951.

[32] 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.
