POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

BAKALÁŘSKÁ PRÁCE

2023 MARTIN HRUBEŠ

POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostního managementu

Katedra managementu a informatiky

Informační kriminalita v České republice

Bakalářská práce

Information crime in the Czech Republic

Bachelor thesis

VEDOUCÍ PRÁCE
RNDr. Václav HNÍK, CSc.

AUTOR PRÁCE
Martin HRUBEŠ

PRAHA
2023

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpal, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Pardubicích, dne 1. 3. 2023

Martin HRUBEŠ

ANOTACE
Práce se zabývá problematikou informační kriminality, která je páchána na území České republiky se zaměřením na ta jednání, kde jsou informační technologie využívány jako nástroj k páchání trestné činnosti. Tedy trestnou činností páchanou v kyberprostoru, která je cílena proti osobám, a nikoliv proti informačním technologiím. Práce je rozdělena na dvě části, teoretickou a praktickou část. V teoretické části této práce jsou vymezeny základní pojmy, které souvisejí s řešenou problematikou. Dále se teoretická část zabývá právní úpravou a trestním řízením, v rámci kterého je tento druh trestné činnosti prověřován a vyšetřován. V praktické části je rozebrána případová studie konkrétního vyšetřovaného případu, resp. přečinu Podvodu dle § 209 odst. 1 trestního zákoníku, jenž vyšetřoval policejní orgán Odbor analytiky a kybernetické kriminality při Krajském ředitelství policie Pardubického kraje.

KLÍČOVÁ SLOVA
Informační kriminalita * kybernetická kriminalita * kyberkriminalita * informační technologie * právní úprava * počítačový systém * informace * kyberprostor * počítačová síť

ANNOTATION
The thesis deals with the issue of information crime committed in the Czech Republic, focusing on those acts where information technology is used as a tool to commit crime. That means criminal activities committed in cyberspace, which are targeted against persons and not against information technologies. The thesis is divided into two parts, a theoretical and a practical part. The theoretical part of this thesis defines the basic concepts related to the problem. Furthermore, the theoretical part deals with the legal regulation and the criminal proceedings within which this type of crime is examined and investigated. The practical part analyses a case study of a specific investigated case, i.e. the offense of Fraud according to § 209 (1) of the Criminal Code, which was investigated by the Police Department of Analytics and Cybercrime at the Regional Police Directorate of the Pardubice Region.

KEYWORDS
Information crime * cyber-crime * cybercrime * information technology * legislation * computer system * information * cyberspace * computer network

Obsah

Úvod

Informační technologie se staly všudypřítomnou součástí moderní společnosti. Rychlý rozvoj informačních technologií přinesl jednotlivcům a organizacím řadu příležitostí ke zlepšení jejich každodenního života a pracovních procesů, které poskytly nové způsoby pro komunikaci, zábavu, obchodování a uchovávání informací. Informační technologie se rozvinuly až do stavu, kdy se jim prakticky v současné společnosti nelze vyhnout. Na druhou stranu informační technologie, k nelibosti celé společnosti, poskytly také větší prostor k páchání trestné činnosti.

Právě tato nežádoucí činnost, definována jako informační kriminalita, je v současné době velmi skloňované a jinými synonymy nahrazované téma napříč celou společností. Důvodem patrně bude aktuálnost tohoto tématu, neboť pokud se na informační kriminalitu díváme jako na druh trestné činnosti, pak můžeme konstatovat, že se v současnosti jedná o nejvíce se rozvíjející formu trestné činnosti, jenž je páchána jak na území České republiky, tak i v jiných zemích. Dalším důvodem může být i vysoká společenská nebezpečnost, neboť páchání této trestné činnosti jsou způsobovány nemalé škody všeho druhu.

V minulosti se rozvíjela především informační kriminalita, při které bylo cílem pachatelů vyhledávat bezpečnostní mezery a následně útočit na softwarové vybavení informačních technologií, tedy na informační technologie samotné, což je především složitá sofistikovaná trestná činnost, která si na její pachatele nárokuje velmi vysoké znalosti v této oblasti, neboť musí překonat bezpečnostní opatření těchto technologií. V současnosti se vedle této sofistikované trestné činnosti mnohem rychleji rozvíjí ta informační kriminalita, kde pachatelé využívají neustále se zvětšující kyberprostor jakožto nástroj k páchání trestné činnosti, kdy za jeho užití cíleně útočí na osoby, které rovněž informační technologie používají, přičemž těží z „benefitů“ tohoto druhu trestné činnosti jako je anonymita, z toho vyplívající vysoká neobjasněnost a značně vysoké výnosy. Při páchání této trestné činnosti, je kladen již podstatně menší nárok na dovednosti pachatelů. Velkým bezpečnostním rizikem páchání tohoto druhu informační kriminality je také fakt, že se jim nelze zcela účinně bránit vývojem informačních technologií v oblasti

bezpečnosti, protože útoky jsou směřovány především proti osobám reálného světa.

Bakalářská práce si klade za cíl poukázat na problematiku informační kriminality s akcentem na ta jednání, jejímž předmětem útoku jsou právě osoby v reálném prostředí, jakožto v současnosti nejvíce se rozvíjející nežádoucí chování osob ve virtuálním prostředí, což se stalo také motivem výběru tohoto tématu. V teoretické části budou vysvětleny základní pojmy, které s touto problematikou úzce souvisí. Následně bude rozebrán vznik a vývoj této problematiky, zejména v České republice, a to na základě dostupných informací v odborné literatuře a statistických dat, která jednoznačně poukazují na stále rozvíjející se problematiku. Dále je práce zaměřena na jednotlivé projevy informační kriminality v uvedeném vymezení. Vzhledem ke skutečnosti, že se nacházíme v právním společenském uskupení, kde ostatně také vznikají následky této nežádoucí činnosti, není na místě jinak, než se tomuto druhu kriminality bránit zejména právními prostředky a preventivním působením. Značná část této práce bude věnována právní úpravě a prevenci, které spolu poskytují obranné mechanismy, pro efektivní boj s touto trestnou činností. V závěru teoretické části bakalářské práce budou zmíněny procesní a kriminalistická specifika v trestním řízení.

V praktické části se práce zabývá případovou studií reálného případu, který se odehrál v nedaleké minulosti a nachází se v mantinelech, kterými je tato práce vymezena. Jedná se o případ, který vyšetřoval policejní orgán Odbor analytiky a kybernetické kriminality, při Krajském ředitelství policie Pardubického kraje, pro přečin podvodu dle § 209 odst. 1 trestního zákoníku. Případ bude popsán z pohledu orgánů činných v trestním řízení, kdy případová studie bude popisovat všechny fáze trestního řízení od prověřování až po řízení před soudem. Na případové studii by měly být dále demonstrovány poznatky zjištěné v teoretické části této práce a tvořit tak ucelené poznání problematiky.

Metodologie

Teoretickou část předkládané práce tvoří primárně rešerše odborné literatury zabývající se informační kriminalitou a právními normami, sekundárně také analyzovaná statistická data. K vypracování této části bylo užito zejména bibliografie, kdy vzhledem k řešené problematice globálního rozsahu, byly užity jak české, tak i zahraniční publikace psané cizím jazykem, zpravidla anglickým. Rovněž bylo čerpáno z legislativních dokumentů, odborných článků a webových stránek organizací, které se touto problematikou zabývají.

Praktická část detailně zpracovává případovou studii konkrétního případu, který obsahově navazuje na teoretickou část, kdy na tomto případu budou demonstrovány poznatky zjištěné z teoretické části. Jedná se o případ, který vyšetřoval policejní orgán Odbor kybernetické kriminality, při Krajském ředitelství policie Pardubického kraje pro majetkovou trestnou činnost, která byla kvalifikována jako přečin podvodu dle § 209 odst. 1 trestního zákoníku. Studie tohoto případu byla vypracována na základě trestního spisu, který byl zapůjčen ze strany vyšetřujícího policejního orgánu.

Výsledkem je předkládaná bakalářská práce, která poskytuje dostatečné množství věrohodných a odborných informací, které souvisejí s řešenou problematikou. S aplikovanými poznatky na konkrétním reálném případu práce tvoří základní, ucelený, přehled o tomto druhu kriminality s akcentem na právní úpravu.

Teoretická část

1. Vymezení pojmů

Práce se zabývá výhradně informační kriminalitou, tedy odborným tématem, kdy zde budou řešeny primárně technické a právní aspekty již zmiňované problematiky. Pro rychlejší orientaci a pochopení obsahu práce, je nutné si některé základní pojmy a definice objasnit hned v úvodu. Vzhledem ke skutečnosti, že se práce zabývá aktuální problematikou, kterou vnímá i široká veřejnost, se mohou již některé pojmy jevit jako zcela jasné a pochopené. I přes tuto skutečnost jsou v této práci objasněny i základní, již obecně známé pojmy, neboť si je každý jedinec může subjektivně vykládat svým způsobem, a tedy ne vždy zcela správně tak, aby reflektovaly svůj význam. Je důležité podotknout, že význam jednotlivých pojmů, jako i pojmy samotné se v čase vyvíjí analogicky s řešenou problematikou, v tomto případě s informační kriminalitou, což je stále velice dynamické téma. Definice, i významy samotné tak mohou pozbývat platnosti, či být upravovány.

1.1. Informační kriminalita

Pro účely bakalářské práce je tento pojem stěžejní a má bezpočet definicí, kdy některé z nich v současnosti již ani neplatí. Toto platí i o pojmu samotném. Jak je uvedeno v úvodní části této kapitoly, pojem i samotné definice se v čase vyvíjely a v době kdy vznikaly, reflektovaly svůj význam na základě známých poznatků. Vývojem informačních technologií a nově zjištěnými poznatky však daný pojem a definice již nebyly schopny zahrnout všechny nově poznané skutečnosti, tedy pozbyly platnosti a již postrádají svůj význam.[1]

Na konci 20. století se pro informační trestnou činnost ustálil pojem „počítačová kriminalita“ (anglicky „computer crime“). Tento pojem v uvedené době obdržel několik definic. Jednu z nich ve své publikaci uveřejnil p. Smejkal, který uvedl, že *„pod pojmem počítačová kriminalita je třeba chápat páchání trestné činnosti, v níž figuruje počítač jako souhrn hardwarového a softwarového vybavení*

[1] *Kybernetická kriminalita – Příručka pro policisty* [online]. 1. vydání. Karlovy Vary: you connected, z.s., 2018 [cit. 16.02.2023]. Dostupné z: Intranet Policie ČR.

data nevyjímaje, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět této trestné činnosti, ovšem s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako movité věci, nebo jako nástroje trestné činnosti".[2]

Pojem „počítačová kriminalita" v současné době nelze považovat za zcela přesný a výstižný. Od této doby, došlo totiž k vývoji mikroprocesorů a některých dalších komponent, které byly rovněž postupem času minimalizovány. Díky tomu mohly vznikat i technická zařízení, která v mnoha oblastech nahradily úlohy počítačů. Dnešní výpočetní zařízení, která umožňují komunikaci mezi sebou a jejich uživateli navzájem, jsou daleko menších rozměrů a dosahují mnohonásobně vyšších výpočetních výkonů, než nejmodernější zařízení z konce 20. století. Přesto, že tato zařízení nenazýváme počítači, mohou být terčem nebo nástrojem k páchání trestné činnosti. Z tohoto důvodu se pojem již nepoužívá a nahradily ho pojmy „informační kriminalita" či „kybernetická kriminalita".[3] I přes tuto skutečnost se v mnoha nynějších publikacích tento pojem vyskytuje.

V odborné literatuře a publikacích najdeme několik definicí, kdy se jejich autoři snažili co nejpřesněji popsat a reflektovat pojem informační kriminality. Ani do dnešního dne nebyly definice sjednoceny a existuje jich hned několik. Například Policie ČR, jakožto policejní orgán, který se aktivním způsobem podílí na boji proti této kriminalitě, informační kriminalitu pro svou činnost definuje jako *„trestnou činnost, která je páchána v prostředí informačních a komunikačních technologií včetně počítačových sítí. Samotná oblast informačních a komunikačních technologií je buď předmětem útoku, nebo je páchána trestná činnost za výrazného využití informačních a komunikačních technologií jakožto významného prostředku k jejímu páchání."* [4]

Další definici lze nalézt například ve Výkladovém slovníku kybernetické kriminality, který uvádí, že informační kriminalita je *„trestná činnost, pro kterou je*

---

[2] SMEJKAL, Vladimír, Tomáš SOKOL a Martin VLČEK. *Počítačové právo*. Praha: C.H. Beck, 1995. ISBN: 80-7179-009-5.
[3] KOLOUCH, Jan. *CyberCrime* [online]. 1. vydání. Praha: CZ.NIC, 2016. [cit. 15.1.2023]. ISBN: 978-80-88168-15-7. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf
[4] *Kyberkriminalita - Policie České republiky* [online]. 2023 Policie ČR [cit. 06.02.2023]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

určující vztah k software, k datům, respektive uloženým informacím, respektive veškeré aktivity, které vedou k neautorizovanému ctění, nakládání, vymazaní, zneužití, změně nebo jiné interpretaci dat.“[5]

V některých publikacích je pojem „informační kriminalita“ často nahrazován pojmy „kybernetická kriminalita“ či zkráceně „kyberkriminalita“, ty pak vycházejí z pojmů „kybernetický prostor“, či opět zkráceně „kyberprostor“. Předchozím pojmům je však věnována zvláštní část této kapitoly, kde je uvedená samotná definice, která pojem reflektuje.[6] Obecně lze dovodit, že pojmy nesou obdobný význam.

1.2. Kybernetický prostor (virtuální prostor)

Kyberprostor poprvé pojmenoval autor sci-fi William Gibson ve svém románu „Neuromancer“ z roku 1984. V románu Gibson použil termín k popisu virtuální reality vytvořené pomocí počítačů, kde lidé mohli komunikovat se simulovaným prostředím.[7] Termín se od té doby stal široce přijatým a používá se k popisu internetu a dalších digitálních technologií.

Policie České republiky na svých webových stránkách popisuje kyberprostor jako virtuální prostředí, které nemá začátek a ani konec, nezná hranice národních států a nelze určit, jak rozsáhlý je.[8]

Z hlediska legální definice je pojem kyberprostor popsán v zákoně o kybernetické bezpečnosti, který uvádí, že se jedná o *„digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací“.*[9]

---

[5] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti* [online]. Praha: Národního úřad pro kybernetickou a informační bezpečnost, 2022. [cit. 07.02.2023]. Dostupné z: https://www.cybersecurity.cz/data/Slovnik_523el.pdf

[6] kapitola 1.2. Kybernetický prostor (virtuální prostor)

[7] GIBSON, William. *Neuromancer*. Vydání páté. Přeložil Josef RAUVOLF. Praha: Euromedia Group, 2019. ISBN: 978-80-7617-760-4.

[8] *Kyberkriminalita - Policie České republiky* [online]. 2023 Policie ČR [cit. 06.02.2023]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

[9] § 2 odst. 1 písm. a) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů

1.3. Počítačová síť

Počítačová síť je soubor vzájemně propojených zařízení, umožňující komunikaci a výměnu informací mezi počítači. Architektura a design počítačových sítí se staly nástrojem rozvoje internetu a dalších globálních sítí, které umožňují komunikaci a sdílení informací v celosvětovém měřítku. Možnost propojit počítače a další digitální zařízení má za následek revoluci ve způsobu, jakým pracujeme, komunikujeme a přistupujeme k informacím. Podle knihy „Počítačové sítě" od Andrewa S. Tanenbauma jsou počítačové sítě jednou z nejdůležitějších technologických inovací 20. století a výrazně ovlivnily společnost a ekonomiku.[10]

První počítačová síť vznikla v roce 1969 s názvem ARPANET, jenž byla vyvinutá ministerstvem obrany USA. Tato síť byla navržena tak, aby podporovala komunikaci mezi výzkumníky a vědci, kteří pracovali na různých projektech. ARPANET sloužil jako prototyp pro pozdější počítačové sítě a byl základem moderního internetu.[11]

V současnosti existuje několik typů počítačových sítí, z nichž každá má své vlastní jedinečné vlastnosti a použití. Mezi nejběžnější typy řadíme místní sítě (LAN), rozlehlé sítě (WAN), metropolitní sítě (MAN) a bezdrátové sítě. Sítě LAN se obvykle používají k připojení počítačů v malé geografické oblasti, např. v domácnostech, kancelářích, školách atd. Na druhé straně sítě WAN propojují sítě LAN a další sítě na velké geografické vzdálenosti, které často zahrnují více měst nebo dokonce zemí. MAN jsou podobné sítím WAN, ale jsou navrženy, aby obsluhovaly konkrétní metropolitní oblast. Bezdrátové sítě, jak název napovídá, využívají k připojení zařízení bezdrátová komunikační média, což umožňuje mobilitu a flexibilitu v přístupu k síti.[12] Všechny zmíněné sítě propojuje globální síť, kterou nazýváme internetem.

---

[10] TANENBAUM, Andrew. *Computer networks*. 4. vydání. New Jersey: Prentice-Hall, 2003. ISBN: 9780130661029.
[11] Tamtéž
[12] KUROSE, James F. a Keith W. ROSS. *Computer networking: a Top-down approach featuring the Internet*. 7. vydání. Boston: Addison-Wesley, 2017. ISBN 9780201477115.

1.3.1. Internet

Pojem internet pochází ze spojení slov „inter“ a „net“, v překladu „mezisít“ a vysvětluje se jako celosvětový systém navzájem propojených počítačových sítí s decentralizovanou strukturou *(žádná z těchto sítí není ostatním podřízená, či nadřízená a všechny vystupují ze stejné úrovně)*, které propojují tzv. síťové uzly. Uzlem pak může být přímo počítač, či zařízení se speciální síťovou funkcí, například router. Připojení k internetu zprostředkovávají svým zákazníkům, samozřejmě za smluvený poplatek, poskytovatelé internetového připojení (Internet Service Providers – ISP). Těmito poskytovateli jsou zpravidla velké telekomunikační společnosti vybavené rychlým připojením do zahraničí, přičemž toto připojení se svými zákazníky sdílejí. Český internetový provoz se z velké míry odehrává na českém území, kdy spolu velmi často komunikují počítače připojené do sítě některého z českých poskytovatelů internetu. Pokud by tato komunikace probíhala přes zahraničí, byl by přenos dat zbytečně zdlouhavý a drahý. Poskytovatelé internetu proto v každé zemi vytvářejí tzv. IXP (Internet Exchange Point - doslova bod výměny internetu). To jsou komunikační uzly propojující jednotlivé sítě poskytovatelů tak, aby data proudila co nejkratší a nejrychlejší cestou. Zatímco přenos dat do zahraničí bývá obvykle zpoplatněn dle skutečného objemu přenesených dat, připojení do IXP je za zlomkovou paušální cenu. Připojení IXP tedy přenos dat nejen zrychluje, ale i zlevňuje. Existence IXP však není nezbytně nutná. Pokud by v tomto bodě došlo k problémům, data si díky decentralizované struktuře najdou jinou cestu. To z internetu činí nejspolehlivější komunikační technologii současnosti.[13]

V České republice IXP provozuje nezávislá společnost NIX.CZ, která sdružuje přes 200 sítí s datovým tokem okolo 2 Tb/s (Terabajtů za sekundu), čímž se stává jednou z největších společností provozující IXP uzly v Evropě.[14]

Klíčovou funkci pro fungování celého internetu vykonávají TCP/IP protokoly, které zajišťují bezchybnou výměnu informací mezi správnými počítači,

---

[13] CZ.NIC, Akademie. *Jak na internet: Struktura internetu*. Metodický portál: Články [online]. 06. 10. 2014, [cit. 07.02.2023]. ISSN 1802-4785. Dostupné z: https://clanky.rvp.cz/clanek/19213/JAK-NA-INTERNET-STRUKTURA-INTERNETU.html

[14] Neutral Internet Exchange. *Technické informace* [online]. Praha: NIX.CZ, 1997 [cit. 16.02.2023]. Dostupné z: https://nix.cz/cs/technical

skrze zmíněnými uzly. Například zajišťují, aby email přišel na správnou adresu, po rozkliknutí odkazu se spustila patřičná webová prezentace/stránka apod.

Na internetu lze pak za užití těchto technologií provozovat několik služeb, kdy mezi ty hlavní a nejznámější řadíme:

- WWW stránky (zajišťují HTTP, HTTPS protokoly);
- E-maily (zajišťují IMAP, POP3, SMTP protokoly);
- Přenos souborů (zajišťují protokoly FTP, FTP/S);
- Internetovou telefonii (zajišťují protokoly VoIP);
- Šifrované přihlášení k jiným počítačům (zajišťují protokoly SSH);
- A další…

Z uvedených skutečností vyplývá, že internet je globální decentralizovanou infrastrukturou počítačových sítí a vytváří nejrozšířenější virtuální prostor, který sebou nese především výhodu v tom, že internet jako takový je velmi obtížné vyřadit z provozu a je obtížně regulovatelný ze strany politických a ekonomických zájmových skupin, jejichž působnost je vždy do určité míry územně omezená.[15]

Na druhou stranu, díky absenci centrální autority, která by internet řídila, nelze regulovat ani jednání společensky nežádoucí. Tím se internet stává také prostředím nebezpečným, kde často dochází k páchání trestné činnosti.

1.3.2. Peer-to-peer a klient-server sítě

Peer-to-peer je počítačová síť, pro kterou je charakteristický vztah počítačových uzlů, které si jsou zde rovné. To umožňuje přímou a decentralizovanou komunikaci mezi počítačovými systémy a jejich uživateli bez nutnosti nadřazeného počítačového systému (serveru). To má především za následek, že tento typ sítě nejde centrálně spravovat a kontrolovat jej. Zmíněný typ sítě je charakteristický také tím, že čím více je v této síti připojených počítačových systémů, tím rychlejší je datový přenos mezi nimi. Využívá se například ke sdílení souborů, systémových prostředků, aj.

---

[15] CZ.NIC, Akademie. *Jak na internet: Struktura internetu*. Metodický portál: Články [online]. 06. 10. 2014, [cit. 07.02.2023]. ISSN 1802-4785. Dostupné z: https://clanky.rvp.cz/clanek/19213/JAK-NA-INTERNET-STRUKTURA-INTERNETU.html

Oproti tomu síť typu klient-server je charakteristická nadřízeností a podřízeností počítačových systémů v síti, kdy klient většinou žádá o službu server, který služby vykonává, či zprostředkovává komunikaci apod. Zde pak platí opačné pravidlo, že čím více je k síti připojeno klientů, tím pomalejší je datový přenos mezi nimi a serverem, který musí zpracovávat více požadavků. Server vykonává funkci nadřízené autority, přičemž může síť ovlivňovat a řídit.[16]

1.4. Kryptoměny a další virtuální aktiva

Virtuální měny, také známé jako kryptoměny, jsou digitální formou peněz, které se nezávisle na státu nebo jakékoliv centrální autoritě šíří prostřednictvím internetu. Kryptoměny se neustále vyvíjejí a nabývají na popularitě, protože nabízejí mnoho výhod oproti tradičním měnám, jako je například vyšší míra anonymity, transparentnost samotných transakcí a celková bezpečnost celého systému, což zajišťuje technologie Blockchain. Na druhou stranu se kryptoměny vyznačují velmi vysokou volatilitou ceny, což znamená, že jejich hodnota může v krátkém časovém horizontu rychle stoupat, ale také klesat. Dále je nutno uvést, že kryptoměny jsou decentralizované a nejsou žádným způsobem regulovány ze strany státních mocností, ani jiné autority. To znamená že nad těmito měnami nemá nikdo ústřední moc a nemůže je nikdo zrušit, či do nich neoprávněně zasahovat. Tímto se kryptoměny odlišují od ostatních aktiv.[17]

V dnešní době existují stovky aktivních kryptoměn, se kterými se obchoduje. První kryptoměnou a zároveň nejrozšířenější kryptoměnou na světě je Bitcoin. Bitcoin jsou internetové peníze, se kterými se platí obdobně, jako běžnými penězi, akorát na internetu.

---

[16] KOLOUCH, Jan. *CyberCrime* [online]. 1. vydání. Praha: CZ.NIC, 2016. [cit. 15.1.2023]. ISBN: 978-80-88168-15-7. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf

[17] ZAVRŠNIK, Aleš. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7552-758-5.

1.4.1. Blockchain

Pro správné pochopení fungování kryptoměn a dalších virtuálních aktiv, je nezbytné přiblížit technologii Blockchain, na jejímž principu virtuální aktiva fungují.

Blockchain se dá vyjádřit jako decentralizovaná, řetězová databáze, která uchovává historii transakcí. Blockchain je tvořen z bloků, které obsahují několik transakcí a reference o předchozím bloku v řetězci. Bloky jsou šifrovány a navzájem propojeny tak, aby nebylo možno jakkoliv změnit jejich obsah. Celá technologie funguje na principu distribuovaného účetnictví, což znamená, že se informace o transakcích ukládají na všechny počítače v síti. Tyto počítače se nazývají uzly. Každý uzel má kopii celého blockchainu a spolupracuje při ověřování a potvrzování transakcí na základě konsenzu (vzájemného souhlasu) nadpoloviční většiny uzlů. Tento proces se nazývá těžba.

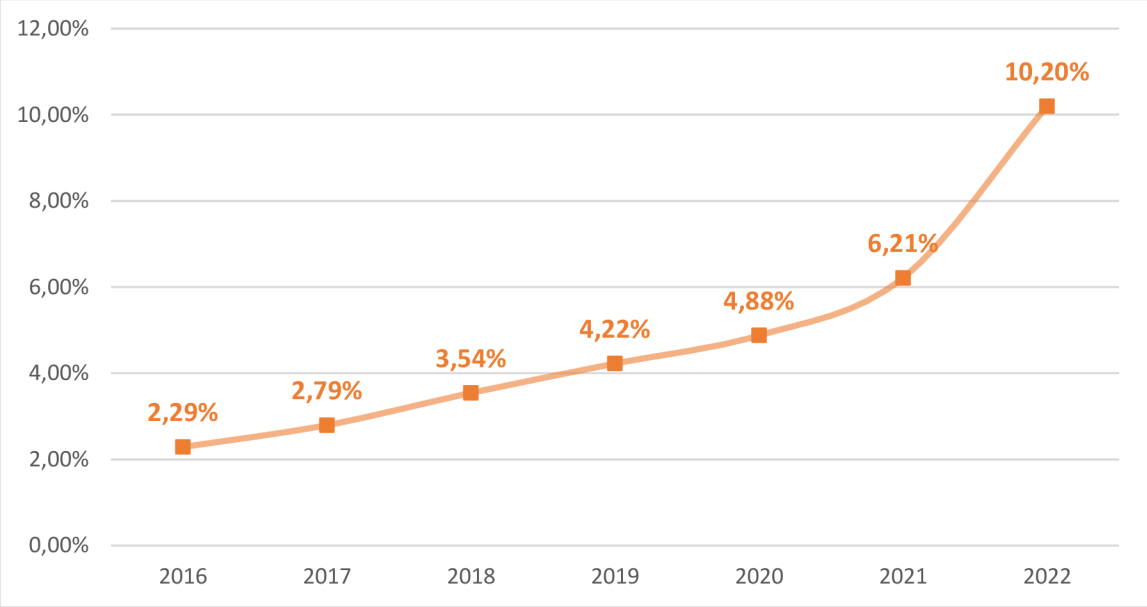
Blockchain je považován za velice bezpečnou technologii, protože žádný uzel nemá moc ovlivňovat nebo měnit již zapsaná data. Teoreticky lze ovlivnit již zapsaná a potvrzená data, ale pouze v případě, že dojde k ovlivnění nadpoloviční většiny uzlů v síti, což je prakticky nemožné. To znamená, že blockchain je odolný vůči útokům a manipulaci. Proto je vhodný pro řadu účelů, jako jsou například transakce s kryptoměny, dává ale zároveň základ pro decentralizované aplikace, jako jsou například systémy pro řízení dodavatelského řetězce, elektronické hlasování apod.[18]

[18] STROUKAL, Dominik a Jan SKALICKÝ. *Bitcoin: peníze budoucnosti: historie a ekonomie kryptoměn, stručná příručka pro úplné začátečníky*. Praha: Wolters Kluwer, 2015. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-87733-26-4.

2. Vývoj informační kriminality v České republice

V České republice je dlouhodobě evidován rostoucí trend registrované trestné činnosti, jenž je páchána ve virtuálním prostředí, čímž se potvrzuje předpoklad o postupném přesunu trestné činnosti do kyberprostoru. Důkazem tohoto tvrzení mohou být i statistická data z posledních let, která ukazují, že podíl informační kriminality na celkové kriminalitě meziročně dlouhodobě stoupá.

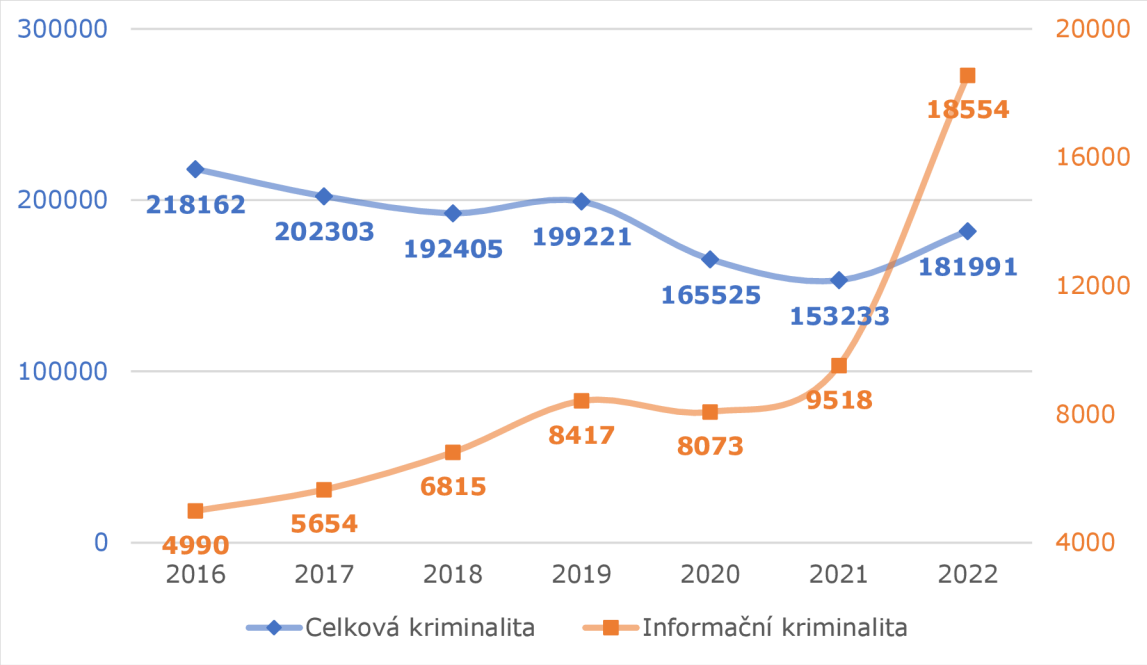
Největší podílový nárůst je evidován v roce 2022 oproti roku předchozímu. V roce 2022 tvořila informační kriminalita 10,2 % z celkové registrované trestné činnosti, v roce 2021 „pouze“ 6,21 %.[19]



Obrázek č. 1 – Podíl informační kriminality na celkové kriminalitě za období 2016 - 2022

[19] *Vývoj registrované informační kriminality - Policie České republiky* [online]. Praha: Policie ČR, 2023 [cit. 06.02.2023]. Dostupné z: intranet Policie ČR

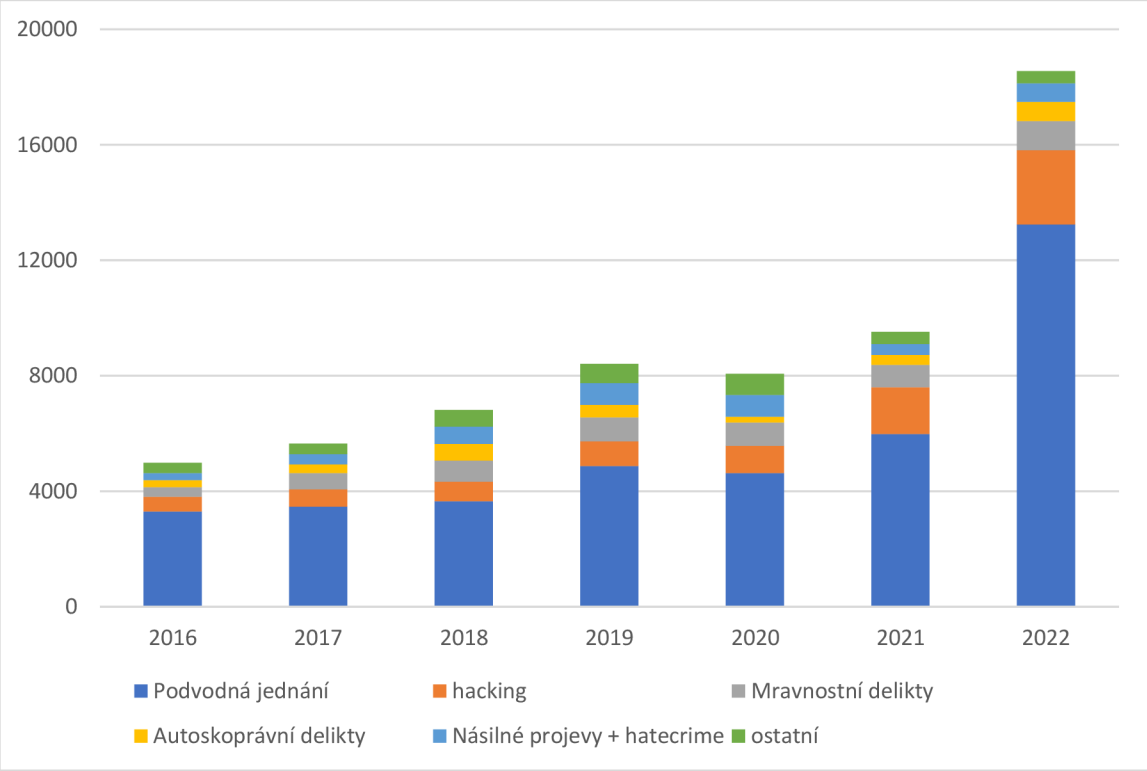
Na rapidní růst informační kriminality ukazují i počty registrovaných trestných činů tohoto druhu, které se dlouhodobě meziročně zvyšují. Od roku 2016 byl jediný, velmi mírný, pokles zaznamenán pouze v roce 2020, kdy jich bylo evidováno 8 073, o 344 trestných činů méně než v roce předchozím, což činí pokles o 4,26 %. Naopak nejvyšší meziroční nárůst byl zaznamenán v roce 2022, kdy registrovaných trestných činů informační kriminality bylo evidováno 18 554, o 9 036 trestných činů více než v roce předchozím, což činí nárůst o 94,4 %. Pro porovnání vývoje informační kriminality a celkové kriminality byl vypracován graf, ze kterého vyplývá, že kriminalita informační má rostoucí trend, přičemž kriminalita celková má kolísavý trend.[20]



Obrázek č. 2 – Vývoj celkové a informační kriminality
za období 2016 - 2022 (dle počtu evidovaných trestných činů)

[20] *Vývoj registrované informační kriminality - Policie České republiky* [online]. Praha: Policie ČR, 2023 [cit. 06.02.2023]. Dostupné z: intranet Policie ČR

Policie České republiky, pro účely vykazování trestné činnosti, celkovou kriminalitu rozděluje dle TSK (takticko-statistické klasifikace), která vychází převážně z právní kvalifikace právních předpisů a umožňuje tak lépe sledovat průběh páchání trestné činnosti o konkrétním druhu trestné činnosti, v konkrétním čase a místě, na což lze reagovat zvolením vhodných opatření, pro efektivní potlačování trestné činnosti. Tímto lze snadněji sledovat i vývoj jednotlivých druhů informační kriminality.[21]

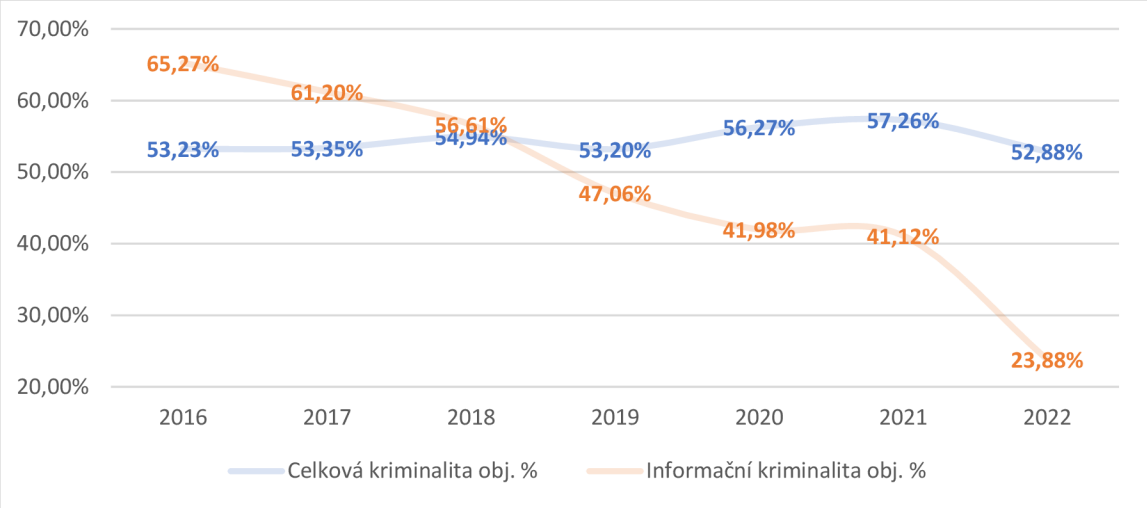


Obrázek č. 3 – Vývoj jednotlivých druhů informační kriminality za období 2016 – 2022

Z předložených dat vyplývá, že nejvyšší podíl na celkové informační kriminalitě dlouhodobě tvoří podvodná jednání. Nejvyšší podíl podvodných jednání je stejně jako u celkové informační kriminality evidován v roce 2022, kdy v tomto roce podvodná jednání tvoří tři čtvrtiny celkové informační kriminality.[22]

[21] *Vývoj registrované informační kriminality - Policie České republiky* [online]. Praha: Policie ČR, 2023 [cit. 06.02.2023]. Dostupné z: intranet Policie ČR
[22] Tamtéž

Ve zkoumaném období je rovněž sledována objasněnost jak celkové, tak informační kriminality. Z těchto dat vyplývá, že procentuální část všech objasněných trestných činů má opět kolísavý trend kdy, nejmenší procentuální část objasněných trestných činů byla zaznamenána v roce 2022, kde procentuální podíl objasněných trestných činů tvořil 52,88 %, oproti roku předchozímu byl zaznamenán pokles o 4,38 %. Oproti tomu objasněnost informační kriminality se od roku 2016 neustále snižuje. V roce 2016 tvořil podíl objasněných trestných činů informační kriminality 65,27 %. V roce 2022 bylo objasněno pouze 23,88 %. Největší meziroční pokles objasněnosti informační kriminality je zaznamenán mezi roky 2021 a 2022, kdy je evidován propad objasněnosti o 17,24 %.[23]



Obrázek č. 4 – Objasněnost celkové a informační kriminality za období 2016 – 2022

Předkládaná data poukazují na velmi závažný problém informační kriminality. Její rapidní meziroční nárust je alarmující i z hlediska velkého nárustů této kriminality v posledním roce. Pokud z těchto dat uměle predikujeme možný další vývoj tohoto druhu kriminality v následujících letech, který má v současnosti spíše exponenciální trend, mohla by být velkou měrou narušena celková bezpečnost celé společnosti. Objasněnost této kriminality postupně klesá, což může být zapříčiněno postupným zdokonalováním pachatelů, ale i zatížeností orgánů činných v trestním řízení.

[23] *Kriminalita - Policie České republiky* [online]. Praha: Policie ČR, 2023 [cit. 18.02.2023]. Dostupné z: https://www.policie.cz/statistiky-kriminalita.aspx

3. Rozdělení informační kriminality

Informační kriminalita je co do svého rozsahu velmi obsáhlou a rozmanitou problematikou, a proto je snahou tento způsob páchání trestné činnosti dále rozčlenit do několika skupin dle různých hledisek. Rozčlenění napomáhá v celkové kvalifikaci informační kriminality, přičemž jednotlivá vymezení často udávají, co spadá do problematiky a co nikoliv. I přes to existují taková rozdělení, která neobsahují komplexně celou problematiku, ale zahrnují pouze nějakou část jednání, která spadají do informační kriminality vyplývající z obecných definic. Jednotlivá rozdělení se liší dle sledovaného účelu, autorova pojetí, právního vymezení, kriminalisticko-taktického hlediska, či jiného relevantního důvodu. Neexistuje jediné rozdělení, ale existuje jich hned několik.

3.1. Podle Budapešťské úmluvy

Úmluva Rady Evropy o počítačové kriminalitě (viz. Kapitola 4.2.1.) rozděluje informační kriminalitu podle skutkových podstat na 4 základní kategorie a několik dalších podkategorií, které již spíše vymezují jednotlivé dílčí jednání, které mají být trestným činem v jednotlivých členských státech. Tato úmluva rozděluje informační kriminalitu na *„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.“* [24]

Dodatkový protokol k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů rozšiřuje Úmluvu o další skutková jednání, kterými jsou „Šíření rasistického a xenofobního materiálu skrze počítačový systém, Rasisticky a xenofobně motivovaná výhrůžka, Rasisticky a xenofobně motivovaná urážka a Popírání, hrubé zlehčování, schvalování nebo ospravedlňování genocidy nebo zločinů proti lidskosti.“[25]

---

[24] Sdělení č. 104/2013 Sb. m. s., Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě

[25] Sdělení č. 9/2015 Sb. m. s., Ministerstva zahraničních věcí o sjednání Dodatkového protokolu k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů

3.2. Podle kriminalistiky

Z kriminalistického hlediska je informační kriminalita kategorizována dle předmětu útoku. Z toho vycházeli i Zdeněk Konrád a kol., kteří ve své publikaci informační kriminalitu dělí na *„neoprávněný zásah do vstupních dat, neoprávněné změny v uložených datech, neoprávněné pokyny k počítačovým operacím, neoprávněné pronikání do počítačů, počítačového systému a jeho databází, napadení cizího počítače, jeho programového vybavení a souborů dat v databázích, informační trestná činnost“*.[26]

3.3. Další rozdělení

Další rozdělení na svém portále zveřejňuje i Policie České republiky, coby policejní orgán, co se aktivním způsobem podílí na boji proti této kriminalitě, kde uvádí jednotlivé druhy kyberkriminality. Informační kriminalita je v tomto případě rozdělována na *„Podvodná jednání, Hacking, Blagging, Podvodné e-shopy, Mravnostní trestné činy, Trestné činy proti autorskému právu a Násilné projevy + hate crime“*.[27]

Toto vymezení zahrnuje pouze část jednání, které spadají do oblasti informační kriminality, kdy vzhledem ke skutečnosti, že na konci článku je uveden graf znázorňující počty registrované kriminality v roce 2016, lze toto rozdělení považovat za výčet, v té době, nejaktuálnějších hrozeb informační kriminality, a ne za výčet komplexní jenž by zahrnoval všechna jednání spadající do informační kriminality.

Informační kriminalitu ostatně rozděluje i tato práce, která již v úvodu, při vymezení obsahu práce, informační kriminalitu dělí dle významu informačních technologií na jednání, kde informační technologie jsou nástrojem k páchání trestné činnosti a na jednání, kde informační technologie jsou cílem útoku při páchání trestné činnosti.

---

[26] KONRÁD, Zdeněk, Viktor PORADA, Jiří STRAUS a Jaroslav SUCHÁNEK. *Kriminalistika: kriminalistická taktika a metodiky vyšetřování*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7380-547-0.

[27] *Jednotlivé druhy kyberkriminality - Policie České republiky* [online]. Praha: Policie ČR, 2023 [cit. 06.02.2023]. Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx

4. Nejčastější projevy informační kriminality

4.1. Podvodná jednání

Podvodná jednání se dle Budapešťské úmluvy o počítačové kriminalitě podřazují pod trestné činy související s počítačem. V současnosti podvody v České republice tvoří většinovou část registrované informační kriminality.[28] V trestním zákoníku je trestný čin podvodu vymezen tak, že *„kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu…“*[29]

Páchaním trestného činu podvodu mnohdy dochází k souběhu s dalšími trestnými činy. Nejčastěji se jedná o trestný čin Neoprávněného přístupu k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací[30] a trestný čin Neoprávněné opatření, padělání a pozměnění platebního prostředku[31].

Trestný čin podvodu je páchán i mimo prostředí informačních technologií. Vznikl dávno před vznikem počítačových sítí, a i v současnosti dochází k páchání podvodů bez užití informačních prostředků. Ve virtuálním prostředí se jednání mající povahu podvodu označuje jako „scam“ v překladu „podvrh“.

Cílem pachatele při páchání trestné činnosti je se obohatit nezákonným způsobem na úkor jiné osoby. Za tímto účelem pachatelé využívají metody, jenž umožňují informační technologie, které dokáží zastřít úmysl, a tím snadněji dosáhnout svého cíle. Zmíněné metody pachatelé také často kombinují, aby vytvořily v oběti patřičnou důvěru k provedení nějaké činnosti, která vede k úspěšnému dokonání trestného činu.

4.1.1. Sociální inženýrství

Sociální inženýrství lze popsat jako ovlivňování, přesvědčování či manipulaci s lidmi za účelem donutit je provést určitou akci, či od nich získat informace mající pro pachatele určitou hodnotu, a které by jinak neposkytly.

---

[28] Kapitola 2. Vývoj informační kriminality
[29] § 209 Zákona č. 40/2009 Sb., trestní zákoník
[30] § 230 Zákona č. 40/2009 Sb., trestní zákoník
[31] § 234 Zákona č. 40/2009 Sb., trestní zákoník

Smyslem je přesvědčit oběť, že situace, v níž se nachází, je jiná, než ve skutečnosti je.

Hlavní myšlenkou sociálního inženýrství v informační kriminalitě je nepoužívat k dosažení kýženého cíle pouze technických postupů a nástrojů, ale například k získání informací, jako jsou hesla apod., využít oběť, která je ve srovnání s technickým zabezpečením mnohem slabším článkem.[32]

4.1.2. Phising

Phising se dá jednoduše vyjádřit jako podvodná jednání, jejichž účelem je získání informací o uživateli, jako jsou například uživatelská jména a hesla, čísla kreditních karet, pinů, CVC kódu a jiných údajů, které mají pro pachatele určitou hodnotu a se kterými může dále nakládat. Obecně se dá za Phishing označit jakékoliv podvodné jednání, které má v osobě vzbudit důvěru, snížit jeho ostražitost a celkově donutit akceptovat scénář, který je často ze strany pachatele předpřipraven. Při Phishingových útocích dochází k oklamání osoby.

Pod Phising pak lze zařadit několik specifických forem, které se odlišují dle způsobu provedení. **Vishing** je telefonický Phising a využívá se ve VoIP telefonii za účelem navedení osoby k nějakému úkonu. **Smishing** se využívá obdobně v rámci SMS zpráv, ve kterých je osoba vyzvána provést nějakou akci (kliknout na odkaz, zavolat na placenou linku apod.), **Pharming** je sofistikovanější forma Phisingu, která funguje na principu napadení DNS (Domain name system) serveru na kterém dochází k převodu doménových jmen (např. www.nic.cz) na IP adresu (např. 217.31.205.50). Poté proto nedojde k přesměrování na správnou webovou stránku, ale na podvrženou (s jinou IP adresou), která se svým vzhledem může jevit stejně, ale slouží k jinému účelu ve prospěch pachatele. **Spoofing**em rozumíme takové jednání pachatele, který se vydává za důvěryhodnou společnost, nebo za někoho komu potencionální oběť důvěřuje (banky, státní orgány apod.) tak, že napodobuje jejich kontakty (emaily, telefonní hovory, SMS

[32] KOLOUCH, Jan. *CyberCrime* [online]. 1. vydání. Praha: CZ.NIC, 2016. [cit. 15.1.2023]. ISBN: 978-80-88168-15-7. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf

zprávy), aby byla oběť přesvědčena o skutečnosti, že komunikuje se správnou osobou.[33]

4.1.3. Podvodné webové stránky

Pachatelé na internetu mnohdy vystavují podvodné webové stránky, které představují nějaký účel. Může to být například nabídka výhry, či prodej podceněného zboží. Následně využívají sociálního inženýrství, přičemž spoléhají na důvěřivost potencionálních obětí. Oběti na webových stránkách zadávají údaje o své osobě, platebních prostředcích apod., nebo přímo provádí platby na účet pachatele.[34]

4.2. Šíření závadového obsahu

Kyberprostor se stává stále významnějším prostředím pro sdílení informací a komunikaci, ale bohužel také pro šíření závadového obsahu, což řadíme mezi další projevy informační kriminality. Závadový obsah zahrnuje škodlivý a nebezpečný obsah, jako jsou pornografie, násilí, terorismus a dezinformace. Tyto druhy obsahu mají vliv na veřejné mínění a mohou mít vážné důsledky pro společnost.

Jedním z nejrozšířenějších typů závadového obsahu v kyberprostoru je pornografie. Internet a digitální technologie umožňují snadný a rychlý přístup k obrovskému množství pornografického materiálu. Tento druh obsahu může mít negativní dopady na psychické a sociální zdraví lidí, zejména na mladé lidi, kteří se mohou dostat do závislosti na pornografii. Mezi zakázané materiály pornografie řadíme například dětskou pornografii, násilnou pornografii a pornografii s urážlivým obsahem. Tyto formy pornografie jsou zakázány zákony mnoha zemí a jejich šíření je trestné.[35] Dalším druhem rozšířeného závadového obsahu v kyberprostoru je násilí a extremismus. Teroristické organizace a extremistické skupiny často využívají internet k šíření svých myšlenek a propagandy. Následkem toho může být vývoj radikalizace a růst násilí v reálném světě. Dále

---

[33] KOLOUCH, Jan. *CyberCrime* [online]. 1. vydání. Praha: CZ.NIC, 2016. [cit. 15.1.2023]. ISBN: 978-80-88168-15-7. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf
[34] Tamtéž
[35] § 191 a § 192 zákona č. 40/2009 Sb., trestní zákoník

mezi závadový obsah v kyberprostoru řadíme dezinformace. S množstvím informací, které jsou k dispozici na internetu, mohou lidé snadno narazit na nepravdivé nebo zavádějící informace. To může mít vliv na veřejné mínění a vytváření politických a společenských názorů. Například, dezinformace o pandemii COVID-19 může vést k šíření choroby a ohrožení zdraví lidí.[36] Rovněž je nutno neopomenout právo duševního vlastnictví, kdy v kyberprostoru ve velké míře dochází k šíření ilegálních kopií autorských děl, ať už to jsou díla audiovizuální, softwarová či jiná.[37]

Šíření závadového obsahu se z hlediska kriminalistiky vyznačuje vysokou latencí, neboť závadový obsah je šířen velmi rychle, anonymně a geograficky rozsáhle. Jako autor práce se domnívám, že vysoká latence tohoto projevu informační kriminality úzce souvisí se skutečností, že takovými projevy často nejsou způsobovány škody konkrétním osobám, či o nich nevědí. Vysoká míra latence se promítá ve statistikách registrované kriminality, kde podíl tohoto projevu tvoří pouze malou poměrnou část v komparaci s ostatními projevy[38], i když se lze domnívat, že skutečné počty této kriminality budou mnohonásobně vyšší.

---

[36] Odborný článek: *Dezinformace vítězí!?. Metodický portál* [online]. Praha: Národní pedagogický institut, 2023. [cit. 08.02.2023] Dostupné z: https://clanky.rvp.cz/clanek/s/Z/21175/DEZINFORMACE-VITEZI.html

[37] § 270 zákona č. 40/2009 Sb., trestní zákoník

[38] Viz kapitola č. 2 – Vývoj informační kriminality

5. Právní ochrana před informační kriminalitou

Na rychlý vývoj a nárůst informační kriminality musí v průběhu času reagovat i právní úprava pro efektivní boj s touto trestnou činností za účelem ochrany společnosti, neboť se do prostředí informačních technologií přesouvá stále větší množství společenských ale i ekonomických vztahů, čímž vyvstává potřeba určité právní regulace, jako je běžná v reálném prostředí.

Hned na úvod je nutné uvést, že kyberprostor je volně a snadno přístupný všem a *„…neplatí zde žádné zvláštní zákony a je třeba se řídit obecně závaznými normami.“*[39], z čehož plyne, že virtuální prostředí není regulováno žádnou centrální autoritou, která by zde uplatňovala speciální právní úpravy, jimiž by se všichni uživatelé řídili. Je zde nezbytné podotknout, že virtuální svět není od toho reálného odtržený, ale úzce spolu souvisí, neboť následky jednání v kyberprostoru vznikají ve světě reálném. Z tohoto důvodu je nezbytné i ve virtuálním prostředí řešit otázku právní odpovědnosti, a to za využití zmíněných obecně závazných právních norem.

Problém zde nastává v rozsáhlosti virtuálního prostředí, ve kterém vystupují osoby téměř všech zemí, kde se právní úpravy a samotná vymahatelnost práva liší. Do velké míry se proto v této problematice promítá také právo mezinárodní.[40]

5.1. Trestněprávní úprava

5.1.1. Trestní právo hmotné

V obecné rovině je základním účelem trestního práva hmotného ochrana nejdůležitějších právních statků (zájem společnosti, ústavní zřízení České republiky, práva a oprávněné zájmy fyzických a právnických osob) před trestnými činy taxativně vyjmenovanými v trestněprávních normách. Jedná se o nepřísnější právní prostředek a užívá se tam, kde jiné právní prostředky nepostačují, či jejich

---

[39] SMEJKAL, Vladimír a Jan SKALICKÝ. *Internet @ §§§: peníze budoucnosti: historie a ekonomie kryptoměn, stručná příručka pro úplné začátečníky*. Praha: Grada, 1999. Právní monografie (Wolters Kluwer ČR). ISBN 80-716-9765-6.

[40] KOLOUCH, Jan. *CyberCrime* [online]. 1. vydání. Praha: CZ.NIC, 2016. [cit. 15.1.2023]. ISBN: 978-80-88168-15-7. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf

užití by bylo neúčelné. Již ze samotného účelu trestního práva a jeho funkcí vychází několik zásad, kterými se trestní právo řídí. Jednou z nejvýznamnějších zásad vycházející již z ústavně-právní úrovně[41] je zásada „nullum crimen sine lege, nulla poena sine lege“ v překladu „žádný trestný čin bez zákona, žádný trest bez zákona“.[42]

Pokud jde o informační kriminalitu, tak již z této zásady můžeme konstatovat fakt, že pokud kybernetický útok, či jiné nežádoucí jednání páchané v kyberprostoru, nebude možné zařadit pod jednotlivá taxativně vyjmenovaná ustanovení zakotvená v trestněprávních normách, tak z tohoto jednání nelze vyvodit trestněprávní postih. Tímto však není vyloučen postih podle jiného práva, například správního, či občanského.[43]

Zákon č. 40/2009 Sb., trestní zákoník jakožto hlavní pramen trestního práva ve své zvláštní části stanoví konkrétní trestné činy, které je možno považovat za trestné a subsumovat tak jednotlivá jednání pod konkrétní ustanovení. Výčet vybraných trestných činů, k jejichž páchání mohou být užity prostředky informačních a komunikačních technologií jsou uvedeny v příloze[44].

5.1.2. Trestní právo procesní

Trestní právo hmotné se uplatňuje za užití trestního práva procesního, které ve svých předpisech upravuje postup orgánů činných v trestním řízení tak, aby trestné činy byly náležitě zjištěny a jejich pachatelé podle zákona spravedlivě potrestáni.[45]

Hlavním pramenem trestního práva procesního je zákon č. 141/1961 Sb., o trestním řízení soudním (dále jen jako „trestní řád“) jenž nabyl účinnosti dne 1. 1. 1962. V této době se informační technologie nacházely ve svém raném věku,

---

[41] Čl. 39, čl 40 Usnesení č. 2/1993 Sb., předsednictva České národní rady o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součástí ústavního pořádku České republiky
[42] JELÍNEK, Jiří. *Trestní právo hmotné: obecná část, zvláštní část*. 7. aktualizované a doplněné vydání. Praha: Leges, 2019. Student (Leges). ISBN 978-80-7502-380-3.
[43] KOLOUCH, Jan. *CyberCrime* [online]. 1. vydání. Praha: CZ.NIC, 2016. [cit. 15.1.2023]. ISBN: 978-80-88168-15-7. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf
[44] Příloha č. 1
[45] JELÍNEK, Jiří. *Trestní právo hmotné: obecná část, zvláštní část*. 7. aktualizované a doplněné vydání. Praha: Leges, 2019. Student (Leges). ISBN 978-80-7502-380-3.

nemluvě o počítačových sítí, které v této době ani neexistovali, neboť první počítačová síť vznikla až v roce 1969 (viz kapitola 1.3).

Od zmíněné doby prošel trestní řád několika novelami v rámci, kterých se reagovalo mimo jiné i na problematiku informačních technologií. První zásadní úpravy se trestní řád dočkal již brzy po roce 1989 v souvislosti se zásadními společenskými změnami, kdy byly odstraněny nejzávažnější nedostatky trestního řádu, které v nových podmínkách demokratického právního státu a tržního hospodářství nemohly obstát.[46] Na informační kriminalitu například reagovala novela[47], jenž nabyla účinnosti dnem 1. 1. 2002, kterou bylo do trestního řádu zakotveno ustanovení § 88a, upravující postup orgánů činných v trestním řízení při zjišťování údajů o uskutečněném telekomunikačním provozu.

V současnosti však přetrvává značné množství problémů, které brání efektivnímu průběhu trestního procesu. Z tohoto důvodu v roce 2014 vznikla pracovní Komise, která má za úkol úplnou rekodifikaci trestního řádu tak, aby došlo k jeho modernizaci a dosažení komplexní úrovně trestního řízení s ohledem na zrychlení trestního řízení, posílení kontradiktornosti řízení, posílení oportunních prvků, posílení koncentrace řízení, posílení práv poškozeného, snížení administrativní zátěže orgánů činných v trestním řízení a zjednodušení řízení, zefektivnění výkonu o trestní sankci a modernizace trestního řádu v návaznosti na technologický vývoj.

5.2. Mezinárodní právní úprava

Vzhledem k nadnárodnímu charakteru počítačových sítí (zejména internetu) závisí situace v oblasti boje proti kybernetickým incidentům velmi silně na mezinárodní spolupráci. Výraznějšího zlepšení situace je možné dosáhnout jen postupem, koordinovaným na mezinárodní úrovni, respektive vycházejícím z mezinárodních úmluv, při kterém by jednotlivé vnitrostátní právní úpravy

---

[46] *Rekodifikace trestního práva procesního – Justice* [online]. Praha: Ministerstvo spravedlnosti ČR, 2022 [cit. 16.02.2023]. Dostupné z: https://justice.cz/web/msp/rekodifikace-trestniho-prava-procesniho

[47] Zákon č. 265/2001 Sb. zákon, kterým se mění zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, zákon č. 140/1961 Sb., trestní zákon, ve znění pozdějších předpisů, a některé další zákony

navazovaly na mezinárodně koordinované úsilí o řešení konkrétních témat. Spolupráce mezi státy při stíhání pachatelů internetové kriminality se v současnosti uskutečňuje na základě mezinárodních úmluv, a to zpravidla za splnění podmínky oboustranné trestnosti.[48]

Největším problém kriminality ve virtuálním prostředí je určení jurisdikce, která by měla trestný čin vyšetřit a potrestat. Ve většině případů je příslušných více jurisdikcí, které se mohou přít o to, kdo daný případ vyšetří. Podle některých právních řádů může být dokonce jednání trestným činem, avšak podle jiných nikoliv. Problém ale nemusí být tak výrazný a často může být rozdílný pouze hrozící trest, či jiné okolnosti.

5.2.1. Úmluva o počítačové kriminalitě

Úmluva Rady Evropy o počítačové kriminalitě, známá také jako Budapešťská úmluva, si klade za cíl reagovat na některé z problémů informační kriminality na mezinárodní úrovni. Jejím hlavním cílem je sjednocení vybraných trestných činů v oblasti počítačové kriminality, uzákonění možnosti postihu právnických osob za informační kriminalitu, či zlepšení procesní spolupráce členských států Úmluvy. To v konečném důsledku pomáhá jednotně bojovat proti informační kriminalitě v mezinárodním měřítku.[49]

V současnosti je Úmluva jediným závazným mezinárodním nástrojem v této oblasti. V platnost vstoupila v roce 2004, ale Česká republika ji ratifikovala později, až v roce 2013. K dnešnímu dni ji podepsalo 53 členských států a slouží především jako závazný návod při tvorbě národní legislativy v oblasti informační kriminality a jako základ pro mezinárodní spolupráci mezi členskými zeměmi. K této Úmluvě se doplňuje také Dodatkový protokol o kriminalizaci činů rasistické a xenofobní povahy spáchaných v kyberprostoru a v současné době se projednává druhý

---

[48] *Mezinárodní spolupráce v boji proti informační kriminalitě - Ministerstvo vnitra České republiky* [online]. Praha: Ministerstvo vnitra ČR, 2009 [cit. 16.02.2023]. Dostupné z: https://www.mvcr.cz/soubor/cyber-vyzkum-studie-mezinarodni-pdf.aspx

[49] ZAHRADNÍČEK Jan. *Počítačová kriminalita: Mezinárodní úmluva je konečně závazná i pro Česko - Patria.cz* [online]. 2014 [cit. 16.02.2023]. Dostupné z: https://www.patria.cz/pravo/2694193/pocitacova-kriminalita-mezinarodni-umluva-je-konecne-zavazna-i-pro-cesko.html

dodatkový protokol, který hlouběji řešil mezinárodní spolupráci mezi členskými státy.[50]

Úmluva je strukturována do 4 kapitol. První kapitola pro její účely definuje základní pojmy, jakými jsou „počítačový systém“, „počítačová data“, „poskytovatel služby“ a „provozní data“. Druhá kapitola Úmluvy stanovuje opatření, která mají být přijata na vnitrostátní úrovni. Z hmotněprávního hlediska taxativně vyjmenovává jednání, která mají být považována za trestná a stanoví formy odpovědnosti a trestů. Stejně tak Úmluva stanoví opatření, která mají být přijata v oblasti procesního práva a soudní pravomoci. Třetí kapitola upravuje mezinárodní spolupráci všech členských států a ve čtvrté kapitole se nacházejí závěrečná ustanovení.[51]

5.2.2. Další mezinárodní dokumenty

Zmíněná Úmluva o počítačové kriminalitě, je sice jediným závazným právním aktem v oblasti mezinárodního práva, ale existují i jiné mezinárodní dokumenty v oblasti internetové kriminality. Tyto dokumenty mají informační a metodický charakter a rovněž napomáhají v boji proti tomuto druhu kriminality.

Na úrovni Evropské unie je to například Sdělení komise Evropskému parlamentu, Radě a Evropskému Výboru regionů k obecné politice v boji proti počítačové kriminalitě, kde je cílem sdělení posílit boj proti počítačové kriminalitě na vnitrostátní, evropské a mezinárodní úrovni za účelem zdokonalení bezpečnosti v oblasti počítačové techniky.[52]

Kybernetická kriminalita je zároveň řešena Organizací spojených národů, která v roce 1994 uveřejnila dokument „United nations manual on the prevention and control of computer-related crime“, v překladu „Manuál spojených národů o prevenci a kontrole zločinu spojeným s počítačem“. Účelem manuálu je pomoci při vývoji společenského rámce pro pochopení důsledků počítačové kriminality na

---

[50] *Výbor k úmluvě o počítačové kriminalitě T-CY – Justice* [online]. Praha: Ministerstvo spravedlnosti ČR [cit. 16.02.2023]. Dostupné z: https://justice.cz/web/msp/rada-evropy?clanek=vybor-k-umluve-o-pocitacove-kriminalite-t-cy-

[51] Sdělení č. 104/2013 Sb. m. s., Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě

[52] Sdělení komise Evropskému parlamentu, Radě a Evropskému Výboru regionů č. 267/2007, k obecné politice v boji proti počítačové kriminalitě

celém světě. V souladu s tím radí členským státům o povaze problému a reaguje na nedostatky současných zákonů v různých řešeních nebo návrzích opatření, které jsou doporučovány státům po celém světě. Manuál netrvá na tom, že by opatření musela být nutně přijata, ale spíše se snaží být pracovním dokumentem, jenž navrhuje vhodná opatření, která mohou členské státy, jenž čelí tomuto druhu kriminality, použít k lepšímu pochopení problematiky, seznámit se s některými řešeními, která jsou manuálem doporučena a na základě toho vyvinout vlastní reakci na řešení problému a podpořit tak mezinárodní spolupráci.[53]

5.3. Vnitrostátní úprava České republiky

Mimo trestněprávní úpravy existují i další vnitrostátní právní úpravy, které jsou nezbytné pro efektivní boj proti informační kriminalitě.

5.3.1. Zákon o kybernetické bezpečnosti

Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů ve znění pozdějších předpisů na vnitrostátní úrovni upravuje práva a povinnosti osob, jakožto i působnost a pravomoc orgánů veřejné moci, přičemž definuje i některé pojmy v oblasti kybernetické bezpečnosti, za účelem zvýšení bezpečnosti kybernetického prostoru zejména té části infrastruktury, která je pro fungování státu důležitá a jejíž narušení by vedlo k poškození nebo ohrožení zájmu České republiky. Zákon se však nevztahuje na informační nebo komunikační systémy, které nakládají s utajovanými informacemi.[54]

Zákon obecně stanoví, jak má být zajištěna kybernetická bezpečnost a rovněž určuje, jakým způsobem se má na kybernetické hrozby reagovat, nebo jakým způsobem se má řešit již nastalý incident. Dále stanoví provádění kontrol, nápravná opatření a přestupky na úseku tohoto zákona. Konkrétní způsoby realizace bezpečnostních opatření, a dále jakým způsobem se má komunikovat s kontaktními místy, jak vést bezpečnostní dokumentace. Kategorizaci

---

[53] *United nations manual on the prevention and control of computer-related crime - International review of criminal policy* [online]. New York: United Nations Digital Library Systém, 1994 [cit. 16.02.2023]. Dostupné z: https://digitallibrary.un.org/record/162804

[54] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů

kybernetických bezpečnostních incidentů určuje Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).[55]

5.3.2. Další vnitrostátní úprava

Jak již bylo uvedeno v úvodu, je v oblasti informační kriminality a virtuálního prostoru na místě postupovat dle obecných právních předpisů, neboť zde platí obdobná právní pravidla. Tato problematika se dotýká většiny zákonů a obecně platných právních norem v České republice. Nejvýznamnější právní předpisy na vnitrostátní úrovni pak jsou:

- Zákon č. 273/2008 Sb., o Policii České republiky, *který v oblasti informační kriminality poskytuje policistům některá oprávnění*[56],
- Zákon č. 110/2019 Sb., o zpracování osobních údajů,
- Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon),
- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů,
- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce,
- Zákon č. 12/2020 Sb. o právu na digitální služby,
- Zákon č. 250/2017 Sb. Zákon o elektronické identifikaci,
- a mnoho dalších…

5.4. Mimoprávní ochrana – prevence

Prevence kriminality je součástí trestní politiky, jenž obsahuje řadu nerepresivních opatření, která jsou realizována státem, veřejnými i soukromými subjekty za účelem přecházení trestné činnosti. Tato opatření zahrnují snahu o

---

[55] *NÚKIB – Legislativa* [online]. Praha: Národní úřad pro kybernetickou a informační bezpečnost [cit. 16.02.2023]. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/

[56] např. § 66 zák. č. 273/2008 Sb., o Policii České republiky

snížení rozsahu a závažnosti kriminality a jejích následků, jak prostřednictvím omezení příležitostí k trestné činnosti, tak prostřednictvím vlivu na potenciální pachatele a oběti kriminality.[57]

Prevence a preventivní opatření hrají v boji proti informační kriminalitě velmi významnou roli. Josef Kuchta ve svém odborném článku uvádí, že prevence a preventivní opatření v boji proti počítačové kriminalitě je dokonce důležitější než represe, neboť zabraňuje vysoké latenci této trestné činnosti a velmi vysokým škodám. Prevencí se pak šetří i kapacity orgánů činných v trestním řízení, což je pozitivní faktor, neboť vyšetřování a dokazování tohoto druhu trestné činnosti je velice náročné z časového i finančního hlediska, kdy ve většině případů z pohledu objasněnosti končí neúspěšně, tedy se jedná o značně neefektivní činnost.[58] Na vysokou neobjasněnost ostatně ukazují i statistická data[59].

5.4.1. Instituce zabývající se prevencí informační kriminality

V současnosti se prevencí na úseku informační kriminality zabývají jak mezinárodní, státní, tak i soukromé instituce, kdy vyvíjejí svou aktivitu za účelem potlačení tohoto druhu kriminality.

Nejvýznamnější institucí v oblasti prevence před kybernetickou kriminalitou je Ministerstvo vnitra, Odbor prevence, jejímž hlavním úkolem je tvorba a koordinace politiky v oblasti prevence kriminality na resortní i vládní úrovni. Výstupem této činnosti je Strategie prevence kriminality v České republice a její Akční plán. Tento resort rovněž poskytuje odbornou a metodickou podporu, dotace a jiné formy finančních příspěvků obcím, krajům, neziskovým organizacím i resortním subjektům na projekty zabývající se prevencí kriminality, a zároveň na pomoc a podporu obětem trestné činnosti.[60]

---

[57] *Prevence kriminality v České republice* [online]. Praha: Ministerstvo vnitra ČR, 2023. [cit. 16.02.2023]. Dostupné z: https://prevencekriminality.cz/prevence-kriminality/

[58] KUCHTA, Josef. *Časopis pro právní vědu a praxi: Aktuální problémy počítačové kriminality včetně její prevence* [online]. Praha: 24. Masarykova univerzita, Právnická fakulta, 2016 [cit. 16.02.2023]. ISSN 1805-2789. Dostupné z: https://journals.muni.cz/cpvp/article/view/5260

[59] Kapitola 2. Vývoj informační kriminality

[60] *Odbor prevence kriminality - Ministerstvo vnitra České republiky* [online]. Praha: Ministerstvo vnitra České republiky, 2023 [cit. 16.02.2023]. Dostupné z: https://www.mvcr.cz/clanek/odbor-prevence-kriminality.aspx

Prevence kybernetické kriminality je součástí „Strategie prevence kriminality v České republice na léta 2022-2027“, v rámci které pod svým strategickým cílem „G“ stanoví, že *„Česká republika aktivně, systémově a koordinovaně posiluje prevenci kybernetické kriminality a rizikového chování v kyberprostoru a poskytuje pomoc a podporu obětem v kyberprostoru.“* [61]

Ke splnění tohoto strategického cíle jsou určovány jednotlivé specifické cíle, které mají určitý charakter a na základě nich volí vhodná opatření, skrze nichž dojde k naplnění jednotlivých specifických cílů v určitém časovém období. Všechny cíle jsou uvedeny v Implantačním plánu této Strategie.[62] Kompletní Strategický cíl „G: Prevence kybernetické kriminality“ je přílohou[63].

[61] *Strategie prevence kriminality v České republice na léta 2022 až 2027* [online]. Praha: Ministerstvo vnitra ČR, 2023. [cit. 16.02.2023]. Dostupné z: https://www.mvcr.cz/clanek/strategie-prevence-kriminality-v-ceske-republice-na-leta-2022-az-2027.aspx
[62] Tamtéž
[63] Příloha č. 2 – Implementační plán Strategie prevence kriminality v ČR na léta 2022-2027

6. Procesní a kriminalistická specifika v trestním řízení

Vzhledem k charakteru informační kriminality, která se z velké části odehrává ve virtuálním prostředí, jsou vyžadována určitá procesní i kriminalistická specifika, jež jsou uplatňována v rámci trestního řízení, které je třeba zohlednit. Odhalování, prověřování a vyšetřování tohoto druhu kriminality je velice náročné z časového i finančního hlediska, neboť získávání informací často probíhá ze zahraničí, za úplatu, či za využití drahých softwarů, či informačních technologií. Vysoký nárok je kladen také na odbornost orgánů činných v trestním řízení, které se v rámci své činnosti potýkají s velkým počtem specifických situací i překážek, vyplývající ze samotných charakterových vlastností informační kriminality.

6.1. Kriminalistická metodika

Kriminalistika je samostatný vědní obor, který slouží k ochraně občanů a státu před trestnými činy tím, že objasňuje zákonitosti vzniku, shromažďování a využívání stop a soudních důkazů, jenž souvisejí s kriminalisticky relevantní událostí, přičemž vychází zejména z trestního práva a vypracovává metody, postupy, prostředky a operace k úspěšnému odhalování, vyšetřování a předcházení trestné činnosti. Metodika vyšetřování jednotlivých trestných činů tvoří zvláštní část kriminalistiky a zkoumá zákonitostí vzniku stop určitého druhu trestných činů a na jejich základě modifikuje obecné kriminalistické metody tak, aby vyhovovaly podmínkám odhalování, vyšetřování a prevenci jednotlivých druhů trestných činů.[64]

Z čehož vyplývá, že kriminalistická metodika se dá využít i v oblasti informační kriminality a efektivněji tak vést samotné vyšetřování tohoto druhu trestné činnosti.

6.1.1. Digitální stopy

Orgány činné v trestním řízení se pro stíhání informační musí v rámci trestního řízení potýkat s digitálními stopami, které mají operativní i důkazní

[64] VICHLENDA, Milan. *Studijní opora: Kriminalistika* [online]. Karvinná: Střední odborná škola ochrany osob a majetku, 2011 [cit. 16.02.2023]. Dostupné z: https://www.sosoom-zlin.cz/media/skripta/kriminalistika.pdf

charakter. Digitální stopy v oblasti kriminality nesou důkazní hodnotu, bez nichž by informační kriminalita zpravidla nešla vyšetřovat, natož prokazovat.

Z právního pohledu za elektronický důkaz považujeme *„produkt analogového zařízení nebo údaj v digitální podobě, který je vytvořen, upraven, uložen nebo spojen s jakýmkoliv zařízením, počítačem nebo počítačovým systémem, respektive se přenáší komunikačním systémem a je relevantní pro proces posuzování“.* Z hlediska technického digitální stopy tvoří série impulsů.

Pro digitální stopy je charakteristické, že je prvotně lidské smysly nevnímají, ale lze je přečíst až za pomoci počítačového vybavení (softwaru, hardwaru) a snáze se mění nebo upravují, a proto jsou zapotřebí speciální postupy pro zajištění jejich integrity, aby zůstaly nezměněny.[65]

Počítačovou stopu lze charakterizovat jako *„změnu na nosiči informací, vzniklou v souvislosti s trestným činem, při jehož páchání byla použita výpočetní technika a která je zjistitelná za pomoci současných metod, prostředků a operací. Digitální topy se nacházejí na pevném disku a vyměnitelných paměťových médiích*“.[66]

Digitální stopy jsou specifické, neboť jsou zpravidla značně objemné z hlediska velikosti dat, dynamické (nestálé) a rovněž se vyznačují tím, že se mohou nacházet kdekoliv v kyberprostoru, a ne například na místě činů, jak je tomu v případě běžných stop. Dynamičnost digitálních stop způsobuje, že jejich životnost může být velmi krátká a jakékoliv průtahy související s jejich zajištěním, mohou způsobovat jejich ztrátu. Dalším specifikem je reprodukovatelnost. Jak již víme, digitální stopy jsou vnímatelné až za využití výpočetního zařízení, zpravidla za využití speciálního softwaru. Každý tento software umí stejná data (digitální stopy) reprodukovat odlišným způsobem.

V rámci páchání informační kriminality dochází k zanechávání celé řady takovýchto stop. Mohou to být stopy na paměťových médiích počítačů, hard discích serverů jednotlivých poskytovatelů, či ve virtuálním prostředí samotném. Je nutné neopomenout skutečnost, že pácháním informační kriminality nedochází

---

[65] ZAVRŠNIK, Aleš. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7552-758-5.
[66] STRAUS, Jiří. *Kriminalistická metodika*. 2. rozšířené vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2008. ISBN 978-80-7380-124-3.

jen k vytváření digitálních stop, ale například dochází k vytváření stop ve vědomí osob (paměťových stop), které trestnou činnost vnímaly. Tyto stopy nesou významnou hodnotu v prvotních fázích trestního řízení.

Z hlediska trestního práva procesního není forma digitálního důkazu upravena a je subsumována pod ustanovení § 112 odst. 1, 2 trestního řádu, které vymezuje věcné a listinné důkazy. Jan Kolouch ve své publikaci dále dodává, že „subsumpce digitální stopy pod ustanovení dopadající na věcný či listinný důkaz není zcela vhodná, a ne vždy je touto subsumpcí možné postihnout veškerá specifika digitální stopy.“[67]

Správné procesní zajištění těchto dat je z procesní stránky mnohdy časově náročné. Jak již bylo předestřeno, elektronická data se vyznačují svou nestálostí, což by z hlediska jejich zajištění vyžadovalo rychlou reakci, aby nedošlo k jejich ztrátě, či změnění. Řešení této problematiky řeší institut tzv. „zmražení dat“, jenž je vymezen ustanovením § 7b trestního řádu, které stanoví, že *„je-li zapotřebí zabránit ztrátě, zničení nebo pozměnění dat důležitých pro trestní řízení, která jsou uložena v počítačovém systému nebo na nosiči informací, lze nařídit osobě, která uvedená data drží nebo je má pod svojí kontrolou, aby taková data uchovala v nezměněné podobě po dobu stanovenou v příkazu a učinila potřebná opatření, aby nedošlo ke zpřístupnění informace o tom, že bylo nařízeno uchování dat.“*

Elektronická data lze zajišťovat například

- Institutem dožádání dle § 8 odst. 1 až 5, dle § 88a trestního řádu apod.[68]
- Vydáním či odnětím věci dle § 78 a § 79 trestního řádu,
- Prohlídkami dle § 82 až § 85 trestního řádu, či
- Ohledáním dle § 113 trestního řádu.[69]

6.2. Problematika příslušnosti

U běžné kriminality, povětšinou není problém s určováním místní příslušnosti, resp. jaké orgány činné v trestním řízení, se danou událostí budou zabývat, neboť je povětšinou známo místo, kde došlo k naplnění skutkové

[67] KOLOUCH, Jan. *CyberCrime* [online]. 1. vydání. Praha: CZ.NIC, 2016. [cit. 15.1.2023]. ISBN: 978-80-88168-15-7. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf
[68] Dále obecně viz kapitola 6.3 Získávání informací
[69] Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád)

podstaty konkrétního jednání. Při určování místní příslušnosti v oblasti informační kriminality, jenž je páchána ve virtuální prostředí, však vzniká problém. Na otázku, kde došlo ke spáchání trestného činu asi odpovíme, že ve virtuálním prostředí. Pro určování místní příslušnosti se však vychází z trestněprávních předpisů, které žádné virtuální prostředí neznají. Z toho plyne, že místem trestného činu musí být místo v reálném prostředí, které lze geograficky vyjádřit.

Místní příslušnost upravuje trestní řád, který v prvé řadě stanoví, že *„řízení koná soud, v jehož obvodu byl trestný čin spáchán“*[70], za což považujeme místo, kde došlo k naplnění objektivní stránky skutkové podstaty trestného činu, tedy místo, kde pachatel jednal a místo kde došlo k jeho následku. V případě informační kriminality, za využití virtuálního prostoru, jsou tato místa zpravidla geograficky odlišná a mnohdy se nacházejí i v odlišných státech. V tomto případě hovoříme o tzv. distančním deliktu a za místo spáchání trestného činu je považováno i místo následku.[71] Jedná se o místo, kde oběť byla, za využití informačních technologií, v kontaktu s pachatelem v souvislosti kriminalisticky relevantní událostí. *„Nelze-li místo činu zjistit nebo byl-li čin spáchán v cizině, koná řízení soud, v jehož obvodu obviněný bydlí, pracuje nebo se zdržuje; jestliže se nedají tato místa zjistit nebo jsou mimo území České republiky, koná řízení soud, v jehož obvodu čin vyšel najevo.“*[72]

V oblasti informační kriminality často dochází k tomu, že pachatel útočí a poškodí zájmy více osob, byť i několika jednáními, na což zpravidla policejní orgány přichází v průběhu prověřování a vyšetřování této kriminality, na základě společných znaků, kterými může být telefonní číslo, přezdívka, IP adresa, doména apod. V tomto případě vzniká podezření, že se těchto všech zjištěných jednání dopustil tentýž pachatel, či organizovaná skupina, čímž je dán důvod pro vedení společného řízení ve všech těchto věcech. To však zakládá příslušnost několika soudů, kdy dle trestního zákoníku koná řízení ten soud *„… u něhož podal státní*

---

[70] § 18 odst. 1 Zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád)
[71] Usnesení Nejvyššího soudu ČR ze dne 19.11.2020 č. 7 Td 58/2020
[72] § 18 odst. 2 Zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád)

zástupce obžalobu, návrh na potrestání, návrh na schválení dohody o vině a trestu nebo jemuž byla věc přikázána nadřízeným soudem.“[73]

Policejní orgány místní příslušnost určují analogicky podle trestněprávních předpisů a v případě vedeného společného řízení, jej vede ten policejní orgán, který se o trestném činu dozvěděl jako první.[74]

Pro úplnost je nezbytné dodat, že výše uvedené postupy se nevtahují na trestní řízení ve věcech mládeže, kde se postupuje dle jiných kritérií.[75]

6.3. Získávání informací

Informace tvoří základ každého trestního řízení, bez nichž by ani samotné řízení nebylo možno vést. Stejně tomu je také v oblasti informační kriminality. Pro účely trestního řízení jsou významným zdrojem informací elektronická data, která byla zaznamenána v souvislosti se spácháním trestného činu. Mohou to být například IP adresy a přesné časy připojení počítačového systému do počítačové sítě, logovací soubory jednotlivých systémů apod.

Pro elektronická data je charakteristické, že jsou velice nestálá.[76] Tím zákon o elektronických komunikacích ukládá povinnost právnickým a fyzickým osobám zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací uchovávat provozní a lokalizační údaje po dobu 6 měsíců.[77] Tímto vzniká prostor pro orgány činné v trestním řízení tyto data získat. Získané informace mohou za určitých okolností sloužit i jako digitální stopa.[78]

Obecně se informace vyžadují dle § 8 odst. 1 trestního řádu, který stanoví, že *„Státní orgány, právnické a fyzické osoby jsou povinny bez zbytečného odkladu, a nestanoví-li zvláštní předpis jinak, i bez úplaty vyhovovat dožádáním orgánů činných v trestním řízení při plnění jejich úkolů.“*[79]

---

[73] § 20 Zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád)
[74] Pokyn policejního prezidenta č. 30/2009, o plnění úkolů v trestním řízení
[75] Zákon č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů
[76] Viz kapitola 6.1.1 Digitální stopy
[77] § 97 odst. 3 Zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů
[78] Viz kapitola 6.1.1 Digitální stopy
[79] § 8 Zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád)

Tímto způsobem se v odvětví informační kriminality realizují zpravidla dožádání adresovaná vnitrostátním institucím, pro vyžádání informací, na které se nevztahuje tajemství, která jsou stanovena jednotlivými právními úpravy, resp. zákony. Jedná se zejména o informace podléhající bankovnímu tajemství a tajemství dopravovaných zpráv, dříve telekomunikační tajemství.

Zákon o bankách stanoví, že bankovní tajemství se vtahuje na všechny bankovní obchody, peněžní služby bank, včetně stavů na účtech a depozit, kdy umožňuje podat zprávu o záležitostech týkajících se klienta, které jsou předmětem bankovního tajemství, na základě jeho žádosti nebo s jeho souhlasem.[80] Pokud je nezbytné pro účely trestního řízení zjistit informace, zejména k řádnému objasnění okolností nasvědčující tomu, že byl spáchán trestný čin, které podléhají bankovnímu tajemství, postupuje se dle § 8 odst. 2 trestního řádu. Tyto informace může vyžádat pouze státní zástupce, či po podání obžaloby nebo návrhu na potrestání také předseda senátu.[81]

Tajemství dopravovaných zpráv chrání dokonce trestní zákoník, ze kterého je patrné, že v souvislosti s informační kriminalitou se tajemství vztahuje na datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli, který zprávu přijímá, nebo na neveřejný přenos dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková data.[82] V případě zjišťování informací, jenž podléhají tajemství dopravovaných zpráv, se postupuje dle § 88a trestního řádu. Nutno však podotknout, že tohoto institutu je možno využít pouze u taxativně vyjmenovaných jednání v tomto ustanovení.

V případech informační kriminality se mnohdy vyskytuje mezinárodní prvek, kdy například pachatel páchá svou trestnou činnost v jednom státě, informační systém se nachází v druhém státě, až škoda vzniká ve státě třetím. V takových případech je pro získávání informací nutná úzká spolupráce na mezinárodní úrovni mezi policejními a justičními orgány. V tomto smyslu je kladen důraz na spolupráci rychlou a efektivní, neboť elektronické důkazy, které jsou nezbytné pro

---

[80] § 38 odst. 1 Zákona č. 21/1992 Sb., o bankách
[81] § 8 odst. 2 Zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád)
[82] § 182 Zákona č. 40/2009 Sb., trestní zákoník

účely trestního řízení často bývají volatilní. Obecně lze říci, že mezinárodní policejní spolupráce funguje častěji efektivněji než spolupráce justiční, neboť její realizace je méně byrokraticky zatížená, existují zde osobní vazby vyšetřovatelů kyberkriminality jednotlivých států, a je postavena na existenci mezinárodních organizacích, které jsou schopné takovou spolupráci zprostředkovat. Těmito organizacemi jsou například Europol či Interpol. Mezinárodní policejní spolupráce však nevede k produkci zákonných důkazů, a proto je nutno využívat mezinárodní justiční spolupráce. Ta je výrazně byrokratičtější a zatížena mezinárodní politikou a diplomatickými vztahy, což výrazně negativně ovlivňuje efektivitu a celkovou úspěšnost vyřízení takové spolupráce. Z hlediska informační kriminality je mezinárodní justiční spolupráce výrazně rychlejší a efektivnější, v případě že je vyžadována od států, které podepsaly Úmluvu o počítačové kriminalitě[83], která se mimo jiné zabývá i mezinárodní spoluprací, a států Evropské Unie.[84] Mezinárodní tuto spolupráci upravuje zákon, který *„upravuje postupy justičních, ústředních a jiných orgánů v oblasti mezinárodní justiční spolupráce ve věcech trestních (dále jen „mezinárodní justiční spolupráce“) a postavení některých subjektů působících v této oblasti, zapracovává příslušné předpisy Evropské unie1) a zároveň navazuje na přímo použitelné předpisy Evropské unie.“*[85] Z tohoto zákona plyne, že justiční orgány se stýkají s cizozemskými orgány prostřednictvím ústředních orgánů, zpravidla písemně diplomatickou cestou.

6.4. Zúčastněné subjekty

Důležité je také zmínit specifické postavení osob, které v trestním řízení vystupují jako pachatelé a oběti. I tyto subjekty se v oblasti informační kriminality vyznačují jistými specifikacemi.

6.4.1. Pachatelé

V současnosti se rapidním způsobem rozšiřuje okruh pachatelů, kteří se mohou informační kriminality dopustit, což zapříčiňuje neustále se zvětšující

---

[83] Viz kapitola 5.2.1. Úmluva o počítačové kriminalitě
[84] POLČÁK, Radim. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7598-045-8.
[85] Zákon č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních

virtuální prostor, rozšiřování a celková dostupnost informačních technologií, ale také vyšší vzdělanost a dovednost prakticky většiny obyvatelstva v této oblasti kriminality.

Charakteristické rysy pachatele informační kriminality nelze jednoznačně určit. Charakteristiku lze specifikovat a diferencovat až v konkrétních případech, na základě jeho motivace, osobních schopností a vlivu vnějšího okolí. Obecně lze ale vyjít z toho, že pachatelé informační kriminality bývají často vzdělanější, inteligentnější, ovládající nezbytné dovednosti s potřebnou mírou přizpůsobivosti. Tato charakteristika však není pravidlem, kdy pachatelem může být i osoba která nedisponuje ani jednou z typických charakteristik. Zde existuje vyšší předpoklad jejich dopadení, neboť jejich jednání bývá nedokonalé a prosté.

Osobnost pachatele se nikterak neodlišuje od většiny populace. Věkově se této trestné činnosti dopouštějí zpravidla mladší osoby, které vyrůstali společně s rozvojem informačních technologií. Není výjimkou, že se trestné činnosti dopouští i osoby mladistvé či nezletilé. Oproti tomu informační kriminalitu páchají i starší pachatelé, kteří získali znalosti v této oblasti a neustále si je obnovují.

U většiny registrované informační kriminality velkou měrou převažuje motivace touhy po zisku. Faktorů vedoucí pachatele k páchání tohoto druhu kriminality je však mnohem více, i když jejich míra není vysoká. Může to být například pomsta, euforie z pocitu beztrestnosti a nedostižitelnosti, touha po riziku a dobrodružství, soutěživost, či jen intelektuální výzva.

Informační kriminalita disponuje jistými výhody ve prospěch pachatele, které vycházejí již ze samotné charakteristiky virtuálního prostoru. Pachatel zde vystupuje zpravidla anonymně, s velmi nízkým rizikem, vysokou časovou flexibilitou a snáze překonává rozpaky, ostych a plachost. Pachatelé rovněž těží z faktu, že následky jejich trestné činnosti vznikají geograficky na zcela jiném místě kdekoliv po světě a po spáchání trestné činnosti ji již nemusí vnímat ve svém okolí. To také zapříčiňuje fakt, že vyšetřování této trestné činnosti probíhá povětšinou v místě následků a vyšetřovatelé tím ztrácejí výhodu jejich osobních znalostí, např. ze své předchozí činnosti.[86]

---

[86] KUCHTA, Josef. *Časopis pro právní vědu a praxi: Aktuální problémy počítačové kriminality včetně její prevence* [online]. Praha: 24. Masarykova univerzita, Právnická fakulta, 2016 [cit. 16.02.2023]. ISSN 1805-2789. Dostupné z: https://journals.muni.cz/cpvp/article/view/5260

Jirkovský ve své publikaci v roce 2007 představil tabulku, která srovnává průměrné loupežné přepadení a průměrný kybernetický útok ve vztahu k jejich pachatelů, kterou vytvořila FBI na základě dlouholetého sběru dat.

Srovnávací parametr	Průměrné Loupežné přepadení	Průměrný Kybernetický útok
Riziko	pachatel riskuje zranění či zabití	bez rizika fyzického zranění
Zisk	průměrně 3 až 5 tis. USD	od 50 až 500 tis. USD
Pravděpodobnost dopadení	dopadeno 50 až 60 % útočníků	dopadeno cca 10 % útočníků
Pravděpodobnost odsouzení	odsouzeno 95 % dopadených útočníků	z dopadených útočníků je pouze 15 % soudně projednáno a z nich je odsouzeno jen 50 %
Trest	průměrně 5 až 6 let, pokud pachatel někoho zranil	průměrně 2 až 4 roky

Tabulka č. 1 – Srovnání loupežného přepadení a kybernetického útoku[87]

Z tabulky vyplývá, že ve všech srovnávacích parametrech je pro pachatele mnohokrát výhodnější páchání kybernetického trestného činu.

6.4.2. Oběti

Obětmi informační kriminality se stávají zpravidla osoby, které využívají informačních technologií. Tyto technologie využívá i značná část osob staršího věku, kteří také tvoří významnou část všech obětí. Příčinou může být pouze okrajové povědomí o fungování informačních technologií, čehož pachatelé hojně využívají za užití technik sociálního inženýrství. Již zmíněné osoby disponují větším množstvím finančních prostředků, a proto jim jsou způsobovány největší finanční ztráty.

Rostoucí počet obětí je zaznamenán i u osob mladších 25 let. Tato nejmladší věková skupina si často uvědomuje rizika, která pachatelé informační

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

kriminality představují, ale nemá zkušenosti s přijetím seriózních opatření k ochraně svých zájmů. Nejmladší skupina osob se také často stává obětí mentality „to se mi nemůže stát“. Vzhledem k celkově nižším disponibilním finančním prostředkům, nejsou následky příliš vysoké. Jejich stále rostoucí zastoupení však dokazuje, že pokud jde o kybernetickou bezpečnost, nikdo není v úplném bezpečí.[88]

Je důležité si uvědomit fakt, že i oběť se může snadno stát pachatelem. Jedná se o tzv. „bílé koně“. Tyto osoby využívají pachatelé k praní peněz, jenž pocházejí z trestné činnosti. Často si oběti neuvědomují, že se dopouštějí nějaké nelegální činnosti, neboť pachatelé zpravidla zastírají svůj účel. I tak toto jednání může mít pro osobu trestně právní postih. Trestní zákoník činnost kvalifikuje jako Legalizaci výnosů z trestné činnosti, či Legalizaci výnosů z trestné činnosti z nedbalosti.[89] Z toho vyplývá, že pro naplnění skutkové podstaty trestného činu postačí pouze nedbalostní jednání. V tomto případě je také možná forma účasti na trestném činu pomocí.[90] [91]

Pachatelé získávají bílé koně za užití různých metod, kterými může být přímý kontakt buď osobní, nebo prostřednictvím e-mailu, či jiných komunikačních kanálů.

Por. Plíšek, komisař oddělení hospodářské kriminality pak na webových stránkách Policie České republiky uveřejňuje popis takového jednání: *„V praxi jde o to, že pachatel osloví jiného člověka s nabídkou např. přivýdělku, kdy oslovený poskytne zcela dobrovolně a bez znalosti účelu své osobní údaje nebo i aktivně vykoná nějakou činnost ve prospěch pachatele.“*[92]

---

[88] HARTLEY, Andrew. *Who Is Most Likely to Be a Victim of a Cybercrime?. LinkedIn* [online]. 2021 [cit. 16.02.2023]. Dostupné z: https://www.linkedin.com/pulse/who-most-likely-victim-cybercrime-andrew-hartley

[89] § 217, § 218 Zákona č. 40/2009 Sb., trestní zákoník

[90] § 24 odst. 1 písm. c) Zákona č. 40/2009 Sb., trestní zákoník

[91] *Preventivní publikace: Bílí koně*. Europol [online]. [cit. 16.02.2023]. Dostupné z: https://www.europol.europa.eu/sites/default/files/documents/cz_flyers.pdf

[92] *Problematika bílých koní - Policie České republiky* [online]. Praha: Policie ČR, 2023 [cit. 16.02.2023]. Dostupné z: https://www.policie.cz/clanek/problematika-bilych-koni.aspx

Praktická část

Podvodná jednání páchaná prostřednictvím informačních technologií, resp. na internetu v současnosti tvoří největší podíl internetové kriminality[93]. Způsobů, jak pachatelé realizují podvody, je vzhledem k možnostem informačních technologií, nepřeberné množství. Tato poměrně značná variabilita, klade vysoké nároky na vědomosti a časové dispozice orgánů činných v trestním řízení, které posléze trestnou činnost vyšetřují.

V praktické části bude probrána případová studie konkrétního případu, jenž byl vyšetřován pro trestný čin podvodu dle § 209 odst. 1 trestního zákoníku, ze strany policejního orgánu Odbor analytiky a kybernetické kriminality při Krajském ředitelství policie Pardubického kraje pod čj. KRPE-26494/TČ-2022-170079. Případ plně vystihuje zaměření bakalářské práce, které bylo vymezeno v úvodu. Jedná se o specifický případ, zejména z hlediska způsobu spáchání ale i osob, které byly na trestné činnosti zúčastněny.

Případová studie je vypracována z pohledu orgánů činných v trestním řízení, které se na odsouzení činu podílely, přičemž budou rozebrány všechny fáze trestního řízení od prověřování až po řízení před soudem, s akcentem na specifické procesní úkony, zejména na podkladě poskytnutého trestního spisu.

V rámci zpracované případové studie jsou uveřejňovány anonymizované originální texty písemností ze spisového materiálu.

[93] Viz kapitola č. 2. Vývoj informační kriminality v České republice

7. Popis případu

7.1. Skutkový děj

Studie se zabývá případem, v rámci kterého si pachatel začátkem roku 2022 v místě svého bydliště na svém počítači, za využití grafických programů a na internetu zveřejněných náhledů originálních obrázků, vytvořil falešné kopie NFT obrázků jedné originální kolekce, které opatřil digitálními tokeny a zveřejnil je na online tržišti s NFT soubory, kde je jako pravé nabízel k prodeji pod záminkou výhodné koupě originálních NFT obrázků, pomocí sociálních sítí a komunikační platformy navedl poškozeného ke koupi uvedených falešných a bezcenných NFT obrázků za celkovou částku 0,67 ETH (v té době 46.653 Kč), která ke dni spáchání trestného činu odpovídala hodnotě originálních obrázků, a tuto si nechal od poškozeného, prostřednictvím tržiště, po částech zaslat do své kryptoměnové peněženky a obdrženou virtuální měnu si ponechal pro svou vlastní potřebu.

7.2. Zúčastněné osoby

Pro účely případové studie budou zúčastněné osoby na trestním řízení anonymizovány. Totožnost uváděných osob, neodpovídá totožnostem skutečných osob. Pro účely studie je nezbytné uvést místa, kde k trestnému činu došlo. Vzhledem ke skutečnosti, že místa činu jsou shodná s bydlišti osob, budou uváděny pouze kraje, v nichž se místa nacházejí, které vyplývají ze samotných orgánů činných v trestním řízení, které se případem zabývaly. Na místě dat narození jednotlivých osob, je uváděn pouze ročník. Ostatní identifikovatelné údaje jsou anonymizovány zcela. Případovou studií proto nedochází k porušení práv na ochranu soukromí zúčastněných osob.

Pachatelem je v té době mladistvý dále uváděný jako Petr Dvořák, r. 2004, bytem v Pardubickém kraji, již v minulosti podmíněně trestaný (zvoleným opatřením) za majetkovou trestnou činnost, žijící v rodině se svými prarodiči, studující střední školu, ve společnosti nevýrazný a uzavřený.

Poškozený (oběť) zde uváděný jako Jan Novák, r. 2003, bytem ve Středočeském kraji, čerstvě plnoletý, studující střední školu a zajímající se o virtuální měny od roku 2021.

Svědek zde uváděný jako Daniel Svoboda, r. 2002, bytem v Moravskoslezském kraji, v tomto případě vystupující jako osoba s odbornými znalostmi v oblasti NFT souborů.

Shodně se výše uvedení, po určitou rozdílnou dobu, pohybují v oblasti virtuálních měn a aktiv.

8. Prvotní úkony

Dne 12.1.2022 se v ranních hodinách osobně na Obvodní oddělení Policie v Kolíně dostavil Jan Novák, za účelem podání trestního oznámení proti neznámé osobě, neboť se domníval, že se stal obětí podvodu. Uvedený policejní orgán oznamovatele Nováka vyzval dle § 158 odst. 6 trestního řádu k řádnému podání vysvětlení, ve kterém se vyjádřil ke všem jemu známým skutečnostem, které s věcí souvisí.

Úřední záznam o podaném vysvětlení – Jan Novák[94]

[Předchozí text vynechán]

„Na OOP v Kolíně jsem se dostavil, abych podal oznámení na neznámého pachatele, který mě podle mého názoru podvedl při zakoupení NFT obrázků. Podrobněji se vyjádřím níže. Cítím se zdráv, jsem schopen podání vysvětlení.

Když mi bylo asi 17 let, tak mi mí rodiče založili u České spořitelny účet [xxx]. Na tento účet mi rodiče průběžně zasílají peníze. I já sám si na účet zasílám peníze. Například, když dostanu peníze od starých rodičů, případně z brigád. Ke včerejšímu dni jsem měl na účtu [xxx] Kč. Dispoziční právo k účtu mám jenom já. Do účtu se přihlašuji přes internetové bankovnictví. Nikdy jsem nezaznamenal, že by mi někdo cizí neoprávněně vnikl na účet.

V dubnu 2021 jsem se začínal více zajímat o virtuální měnu. Konkrétně jsem se zajímal o měnu Bitcoin. Můj zájem spočíval v tom, že jsem začal sledovat kurzy této měny a i jsem si pouštěl videa na YouTube. Videa byla o vývoji měny a obchodování s měnou. [..text o jeho virtuální činnosti vynechán..] Dne 02.01.2022 jsem se přes IG seznámil s osobou, která na IG vystupuje pod uživatelským jménem [xxx] (dále [Petr]). Tato osoba se také zajímá o virtuální měnu a NFT obrázky. NFT obrázky jsou obrázky, které mají danou unikátní adresu (číselný kód). Tyto obrázky může vydat kdokoliv. Podle toho, kdo ty obrázky vydává, tak se i určuje jejich hodnota. Můžou je vydávat např. umělci, kteří se podíleli na hrách od firmy Marvel apod. V podstatě je můžu vydávat i já. Podle toho, kdo je vydává, tak se určuje i jejich hodnota. Každý vydavatel těchto NFT obrázků si pak založí svoji komunitu. Může to být na jakýchkoliv sociálních sítích. Tyto obrázky jsou po zakoupení zahalené a až po nějaké době (např. 14 dnech) se tyto obrázky odhalí. V tu chvíli já zjistím, co je na obrázcích. Já pak samozřejmě tyto obrázky mohu přeprodat dále, ale již odhalené. Když se vrátím k osobě [Petr], tak ten mi sdělil, že byly vydány kolekce od osoby, která vystupuje pod uživatelským jménem [anonymizováno]. Již dříve jsem měl v počítači prohlížeč se stránkami OpenSea a rozšíření do prohlížeče MetaMask. Následně jsem se dne

[94] Trestní spis čj. KRPE-26494/TČ-2022-170079.

11.01.2022 v čase kolem 20:15 hodin v počítači přihlásil do účtu OpenSea a ten [Petr] mi nadiktoval jméno vydavatele obrázků [anonymizováno]. Když jsem ho vyhledal, tak jsem na něho klikl a prohlížel jsem si obrázky. K tomu uvádím, že tyto obrázky jsou jednak označeny názvem Royal Cubs a doplněné o hashtag s číslem. Čím menší číslo, tak je pravděpodobné, že to bude mít větší raritu, tedy i větší hodnotu. Nejdříve jsem klikl na jeden obrázkem s číslem 4 a zakoupil. Po zakliknutí obrázku na mě vyskočilo dialogové okno MetaMask, tam jsem se přihlásil a propojil peněženku s OpenSea a zadal příkaz k nákupu. Platil jsem měnou Ethereum, kterou jsem měl v peněžence (MetaMask). Jelikož jsem v peněžence již neměl dostatek virtuální měny (Etherea), tak jsem se přihlásil do směnárny Binance, kam jsem si poslal peníze ze svého spořitelního účtu ve výši 37.666,50- Kč (1.500 Euro). Na Binance jsem obdržel eura, které jsem následně směnil za Ethereum. Když jsem měl dostatek této měny, tak jsem si je pak poslal na MetaMask. Pak jsem se zase přihlásil do MetaMask a následně na OpenSea zakoupil ještě dva zahalené obrázky (č. 1 a 2). Za všechny tři obrázky jsem zaplatil celkem 0,67 ETH (0,2 ETH, 0,2 ETH, 0,27 ETH). Poplatky šly pak zprostředkovateli platby. Tato částka odpovídá asi 1.910,84 Euro a to by mohlo odpovídat částce 46.653,20 Kč. Zakoupené obrázky mi přišly do aplikace OpenSea, kdy byly uložené v záložce Collected 3. K této transakci uvádím, že po celou dobu nákupu byl se mnou [Petr] spojený přes aplikaci Discord (komunikační aplikace). Já jsem s ním měl sdílenou obrazovku. Tedy viděl všechno, co jsem dělal při zakoupení obrázků. Pouze, když jsem zadával údaje k platbě, tak jsem sdílení vypnul. [text o jeho o komunikaci s Petrem, kde jej přesvědčuje o pravosti vynechán] Ještě bych uvedl, že když jsem se koukal na obrázky, které údajně měl zakoupit, tak jsem u těch obrázků nezjistil, že by je někdo zakoupil. Dnes jsem zjistil, že ten [Petr] skutečně zřejmě zakoupil dva obrázky s č. 17 a 96. Ten s č. 17 zakoupil před 12 hodinami a s č. 96 někdy 09:30 hodinami dnešního dne. Dokonce mi nabízel, že mi za špatný tip dá jeden svůj ověřený obrázek. Je mi to divné. Nechápu, že když jsem ho včera informoval o možném podvodu, tak proč on ty obrázky stejně na TRC zakoupil.

To, že jsem byl podvedený také dovozuji z toho, že na TRC je uvedeno, že mají vystaveno 866 obrázků, kdy 32 uživatelů si zakoupilo obrázky. Nejnižší cena obrázku je 0,2 ETH a jejich obrat je 0,67 ETH, což odpovídá mnou zaplacené částce. Já jsem to totiž porovnával i s jinými vydavateli, kdy jejich obraty za prodané obrázky jsou daleko větší.

[..text o důvodech, proč si myslí že byl podveden a informacích o profilových účtech Petra vynechán..]

Na OOP Kolín dodám screenshoty všeho, co se týká výše popsané transakce. Jsem poučen o tom, že vše ponechám i v elektronické podobě.“

Ve svém podání vysvětlení se poškozený vyjadřuje ke skutečnostem, které souvisejí s předmětným podvodem, kdy se i vyjadřuje k fungování NFT obrázků a kryptoměn. Uvádí přesný popis svého jednání, které uskutečnil za účelem domnělého výhodného nákupu NFT obrázků, tak jak mu to poradil Petr. Dále odůvodňuje, proč si myslí, že byl podveden. Společně s podáním vysvětlení oznamovatel ke spisovému materiálu doložil elektronické materiály, potvrzující jeho výpověď, pro účely dalšího řízení.

Uvedený policejní orgán, který s osobou prováděl podání vysvětlení, na základě zjištěných skutečností dospěl k závěru, že mohl být spáchán trestný čin podvodu dle § 209 odst. 1 trestního zákoníku, a proto ve věci dle § 158 odst. 3 trestního řádu zahájil úkony v trestním řízení. O tom sepsal záznam, ve kterém popsal zjištěný skutkový děj.

Záznam o zahájení úkonů trestního řízení[95]

*„Podle § 158 odstavec 3 trestního řádu byly dne **12.01.2022** na základě oznámení **od** [Jana Nováka] zahájeny úkony trestního řízení ve věci **NP PODVOD NA INTERNETU,** neboť na podkladě zjištěných skutečností je dostatečně odůvodněn závěr, že v době od 11.01.2022 07:01 hod. do 12.01.2022 07:01 hod.*
*mohl být (kým): **neznámý pachatel,***
*spáchán ve [Středočeském kraji] přečin **podvodu podle § 209 odst. 1 trestního zákoníku** tím, že přes aukční portál OpenSea nabízel pod uživatelským jménem [anonymizováno] k prodeji obrázky NFT (Non-fungible token) The Royal Cubs, označené Royal Cubs a doplněné # a pak i číslem, s tím, že se jedná o originály, kdy na uvedenou nabídku zareagoval 11.01.2022 poškozený [Jan Novák], který si prostřednictvím aplikace MetaMask zakoupil tři NFT obrázky s #1, 2 a 4, za které zaplatil 0,67 ETH, což odpovídá částce 46.653,- Kč, které si následně otevřel přes aplikaci OpenSea, přičemž dle poskytnutých údajů dospěl k závěru, že vzhledem k historii obrázků se zřejmě nejedná o originály, čímž měla být poškozenému [Janovi Novákovi] způsobena škoda 46.653,- Kč“*

Policejní orgán v rámci prvotních úkonů provedl zejména podání vysvětlení oznamovatele na základě čehož zjistil částečný skutkový děj, a poté bez dalšího zahájil úkony v trestním řízení.

Sofistikovaná trestná činnost, kterou se případ jistě vyznačuje, je zejména v rámci prvotních úkonů velice náročná jak pro orgány činné v trestním řízení, tak

[95] Trestní spis čj. KRPE-26494/TČ-2022-170079.

i pro osoby, které ji oznamují. Základní policejní útvary, které plní činnost policejních orgánů v rámci trestního řízení, plní široké spektrum jím uloženým úkolům, kdy se musejí potýkat se všemi druhy trestné činnosti. Policisté nejsou a ani nemohou být odborníky „na všechno“. U závažné trestné činnosti jsou proto ve výjimečných případech přítomni také odborníci z útvarů, zpravidla služby kriminální policie a vyšetřování, kdy případ takto vyhodnocen nebyl. Stejně tak jsou prvotní úkony náročné i pro oznamovatele, resp. poškozené osoby. Poškozené osoby se povětšinou na orgány obracejí, stejně jako v tomto případě, bezprostředně po spáchání trestného činu, čímž jsou často ovlivněny emocemi. Skutečnosti také způsobují, že prováděné úkony jsou zdlouhavé a neúplné. Podání vysvětlení oznamovatele, coby osoby poškozené trvalo bezmála 3 hodiny. Rovněž lze konstatovat, že uvedeným podáním vysvětlení nebyly zjištěny všechny skutečnosti pro účely dalšího prověřování. Absentují zde například čísla virtuálních peněženek, mezi kterými došlo k prováděným platbám. To může být zapříčiněno několika faktory. První faktor je, že se vyslýchající policista v problematice dostatečně neorientoval a poškozeného se na dostatečné množství informací nedotázal, druhým faktorem může být, že poškozený těmito informacemi nedisponoval v době podání vysvětlení, nebo se skutečnosti opomněly uvést. Nedostatky jsou rovnány v průběhu dalšího prověřování trestného činu, což je u takto sofistikované trestné činnosti běžnou praxí. I přes uvedené skutečnosti hodnotím prvotní podání vysvětlení velice kladně, kdy byl zjišťován jak detailní skutkový stav, tak i samotná funkce kryptoměn a NFT souborů, se kterými trestná činnost přímo souvisí. Stejně byly od poškozené osoby přijaty i digitální soubory, které potvrzovaly jeho výpověď. V souvislosti s předanými daty je pro úplnost nutno zmínit procesní úkon vydání věci dle § 78 odst. 1 trestního řádu.[96] V případě, že by data měla sloužit jako důkazní prostředek, měla být vydána dle tohoto ustanovení, o čemž je policejní orgán povinen sepsat protokol.

[96] Viz kapitola 6.1.1 Digitální data

9. Prověřování

Následně v rámci prověřování policejní orgán navázal opětovný kontakt s oznamovatelem, kdy jej vyzval k doplnění podání jeho předchozího vysvětlení, neboť zjistil další skutečnosti, které přímo souvisí s trestným činem. Doplnění vysvětlení bylo realizováno dne 18.1.2022.

Úřední záznam o doplnění podaného vysvětlení – Jan Novák[97]

„[Předchozí text vynechán]

Na OOP v Kolíně jsem se dostavil, abych doplnil svoji výpověď ze dne 12.01.2022. Nejprve bych chtěl uvést, že já vystupuji na OpenSea pod uživatelským jménem [anonymizováno].

*Dále jsem zjistil, že ty obrázky, které jsem kupoval, jsem kupoval z neoriginálních stránek. Originální stránky mají název The Royal Cubs a ty, ze které jsem je kupoval měly název The Royal**e** Cubs. To mě utvrzuje v tom, že jsem naletěl podvodníkovi. Kdo stojí za vytvořením stránek The Royale Cubs, tak to nevím. Mohu se pouze domnívat. Vytvoření takovýchto stránek není nic složité. [text ohledně popisu založení vynechán] Jak jsem uvedl 12.01.2022, tak jsem ty tři obrázky zakoupil přes OpenSea ze stránek The Royale Cubs, kdy autorem obrázků je osoba [anonymizováno]. K tomuto uvádím, že jsem dohledal adresu peněženky 0xeaf[…]7ead. Ke spisu přikládám profil osoby [anonymizováno]. Osobně si myslím, že ten, co vytvořil fiktivní stránky, tak si pouze propůjčil toto jméno a označil ho jako tvůrce obrázků.*

Od posledního podání vysvětlení se mi podařily zjistit nové skutečnosti. Nejprve k osobě [Petr Dvořák] mohu uvést, že jsem zjistil, že tento člověk bydlí v [Pardubickém kraji]. Je možné, že mu je 17 let. Tento údaj jsem zjistil v aplikaci TikTok v jeho biu. On tam má veřejně dostupná videa a i nějaké osobní údaje. To, že má profil na TikToku, tak jsem zjistil na IG v odkaze Linktr.ee. On si zřejmě na Linktree založil účet, kde vystupuje pod uživatelským jménem @[anonymizováno]. Jinak na TikToku vystupuje pod uživatelským jménem @[anonymizováno]. Také jsem na něho zjistil telefonní číslo a pak i adresu [Pardubický kraj]. Adresu jsem zjistil od kamaráda, který v [Pardubickém kraji] hraje fotbal a zná ho.

Dále bych chtěl uvést, že jsem se zkontaktoval přes IG s jistým [Danielem Svobodou], který na IG vystupuje pod uživatelským jménem [anonymizováno]. [text o tom, co mu poškozený poskytl vynechán..] Když jsem to všechno poskytl tomu [Danieli], tak ten mi řekl, že je to fake. On se spojil s tím [Petrem Dvořákem]. Nejprve mu telefonoval a pak

[97] Trestní spis čj. KRPE-26494/TČ-2022-170079.

s ním chatoval. Komunikaci mi zaslal. Tu přikládám ke spisu. Pak mi ještě poslal hlasovou zprávu, ze které jsem pochopil, že se ten [Dvořák] [Danielovi] doznal, že mě podvedl. Hlasovou zprávu od [Daniela] přikládám ke spisu.

Ke spisu jsem dále přiložil screenshoty, které jsem pořídil z OpenSea. Tam je zaznamenána aktivita osoby [anonymizováno]. V odkaze Activity a vyfiltrování Sales (prodej) jsou vidět pouze ty moje tři obrázky. Když kliknu na More (rozšíření), tak je vidět, že jsem je koupil.

[Text o popisu všech dodaných dat vynechán] Adresa peněženky osoby [profilový účet anonymizován] je 0xd2[anonymizováno]5c26. Jinak není problém si založit novou peněženku.

Ke spisu jsem mj. přiložil i videa, které měl [Dvořák] svém profilu Tik Tok. Ke spisu dále přikládám kopii profilu osoby [Daniela Svobody].“

Poškozený ve svém doplněném vysvětlení upřesnil skutečnosti o skutkovém ději, kdy uvedl detailní informace jak o možném pachateli, tak informace o své virtuální peněžence, kdy na základě zjištěných dat lze realizovat další úkony za účelem zjištění totožnosti případného pachatele. Rovněž doplnil, proč si myslí, že byl podveden a jakým způsobem k tomu dospěl. Zmínil další osobu, která se zapojila jako odborný prostředník do komunikace mezi ním a panem Dvořákem. Během komunikace mělo dojít k přiznání pana Dvořáka k uvedenému jednání, kdy se přiznal právě panu Svobodovi. Provedeným úkonem došlo k významnému zjištění, resp. přiznání osoby pachatele k předmětnému jednání. V současnosti má tato skutečnost spíše operativní charakter, neboť informace byly získány pouze podáním vysvětlení, které nelze považovat za důkazní prostředek. V tomto případě se jedná pouze o zprostředkované skutečnosti, které by z hlediska dokazování nemohly obstát.

Policejní orgán se v rámci prověřování rovněž zabýval věcnou a místní příslušností[98] k dalšímu prověřování. Z hlediska místní příslušnosti vycházel zejména z místa spáchání trestného činu, ke kterému muselo dojít na dvou místech. Na místě odkud pachatel jednal s poškozeným a na místě, kde došlo k následku. V tomto případě bylo zjištěno pouze místo následku, ke kterému došlo ve Středočeském kraji a místní příslušnost připadá orgánu, který dosud ve věci

[98] Viz kapitola 6.2. Problematika příslušnosti

prováděl úkony. Pro určení věcné příslušnosti je hlavním aspektem trestní sazba odnětí svobody, kterou lze uložit pro nejzávažnější trestný čin. Pro přečin podvodu dle § 209 odst. 1 trestního zákona je horní hranice sazby trestu odnětí svobody stanovena ve výši 2 let. Podle Pokynu policejního prezidenta č. 103/2013 je dána věcná příslušnost službě kriminální policii a vyšetřování trestných činů, kde horní hranice trestu odnětí svobody převyšuje hranici 5 let. Z toho pohledu by i věcná příslušnost připadala tomuto policejnímu orgánu. Zde policejní orgán, i přes uvedené důvody, dospěl k závěru, že ve věci není věcně příslušný, neboť případ vykazuje známky nové formy kybernetické kriminality, který se bude zřejmě vyznačovat složitostí zpracování a zřejmě i složitostí důkazní, což vyžaduje i hlubší znalosti v dané problematice.

Věc byla dne 19. 1. 2022 postoupena kompetentnímu policejnímu orgánu Odboru analytiky a kybernetické kriminality při Krajském ředitelství policie Středočeského kraje v souladu s Pokynem policejního prezidenta č. 103/2013 k provedení dalších úkonů.

Postoupený policejní orgán vyhodnotil všechna data, která ke spisovému materiálu dodal poškozený. Detailně se zabýval rozborem snímků obrazovky, kde je zaznamenána konverzace mezi osobami, profilové náhledy uživatele sociálních sítí možného pachatele, transakce virtuálních měn vč. náhledů kryptoměnových peněženek a stránky zobrazující vlastnictví NFT obrázků. Rovněž byla vyhodnocena videa umístěná na profilovém účtu sociální sítě Tik Tok možného pachatele. Na základě doložených elektronických dat policejní komisař provedl šetření v prostředí veřejné sítě internet.

Šetřením zjistil, že originální kolekce NFT je prezentována na stránkách https://www.theroyalcubs.com, falešná kolekce je nabízena na stránkách https://theroyalecubs.com. Porovnáním odkazů je zřejmé, že se liší pouze v písmeni "e", které je navíc u odkazu na falešnou kolekci https://theroyal"e"cubs.com/. Dále webové stránky porovnal a zjistil, že vykazují stejný vzhled s minimem rozdílů.

Z vyhodnocených zvukových stop, resp. hlasových zpráv, které poslal Petr Janovi vyplývá, že autor zprávy by rád poslal peníze zpět, ale zpanikařil a nevěděl co má dělat. V další hlasové zprávě uvádí, že *„peníze příjemce hlasové zprávy určitě uvidí, přiznává, že je to jeho chyba, že to neposlal rovnou; dále zmiňuje, že*

je ochoten sepsat čestné prohlášení a podepsat ho, kdy to můžou takto vyřešit i on-line.“

Rovněž na základě vyhodnocených dat, provedl šetření ke zjištěným adresám kryptoměnových peněženek, mezi kterými došlo k transakcím v souvislosti s tímto podvodem. Určil, že adresa 0x6f[…]A3fb je adresou kryptoměnové peněženky Ethereum, kterou využívá poškozený a z této adresy byly provedeny dne 11. 1. 2022 celkem 3 převody (0,2 ETH, 0,2 ETH a 0,27 ETH) ve prospěch adresy 0xA0[…]7C77. Adresa je však označena jako Polygon (Matic): Bridge, tzn. že slouží jako rozhraní pro přesun prostředků mezi uživateli. Další cesta prostředků zjištěna nebyla, neboť kriminalisté nedisponují žádným nástrojem pro trasování kryptoměny Ethereum. Jednotlivé kryptoměnové adresy nenesou žádné identifikační údaje o svém majiteli, síť uživatelů je decentralizovaná a neexistuje tak žádná centrální autorita ověřující transakce a uživatele. Anonymita je jednou z podstat kryptoměn a důvod, proč jsou užívány k nelegálním transakcím.

Z blockchainu kryptoměny Ethereum bylo zjištěno, že adresa 0xD2…5c26, která je uvedena u již neexistujícího profilu podezřelého na tržišti OpenSea, obchoduje s kryptoměnovou směnárnou Binance. Dožádáním společnosti Binance bylo zjištěno, že předmětné transakce provedl uživatel, který si účet založil dne 12. 05. 2021 a jako registrační údaje uvedl e-mail [adresa podezřelého]@gmail.com a jméno babičky podezřelého. Při založení účtu uživatel zaslal pro ověření totožnosti fotografie občanského průkazu č. [anonymizováno] vystaveného na jméno babičky podezřelého. Dále bylo zjištěno, že Ethereová adresa uživatele je 0x8c[…]65c4. Tímto byly zjištěny další adresy podezřelého, avšak nebylo zjištěno žádného dalšího poznatku, neboť nebyly spojeny s žádnou transakcí.

Ve věci byl rovněž sepsán protokol o ohledání profilových účtů na sociálních sítích dle § 113 trestního řádu, za účelem propojení podezřelého Petra Dvořáka s účty na různých sociálních sítích. Procesním úkonem došlo k propojení profilových účtů sociálních sítí Instagram, Twitter, Snapchat, TikTok, OpenSea, Spotify a Linktree. V rámci ohledání profilových účtů policejní orgán na profilovém účtu TikTok, ze zde uveřejněného videa, zjistil podobu pachatele a skutečnost, že uživatel má peněženku MetaMask s Ethereovou adresou 0xEAf...7ead. Toto bylo

zásadní zjištění, neboť tato část adresy byla shodná s adresou, kterou doložil poškozený jako podklad pro další prověřování a vypátrání osoby pachatele. V blockchainu Ethereum bylo zjištěno, že z předmětné adresy byl převeden ID token podvodných NFT obrázků na adresu kryptoměnové peněženky poškozeného.

Dále byl v souladu s ustanovením dle § 66 Zákona č. 273/2008 Sb. ztotožněn majitel telefonního čísla, který užíval podezřelý pan Dvořák. Postupem bylo zjištěno, že majitelem je babička podezřelého.

Následně policejní orgán identifikoval osobu pachatele na základě všech uvedených skutečností jako Petr Dvořák, r. 2004, bytem v Pardubickém kraji. Rovněž byl ztotožněn prostředník jako Daniel Svoboda, r. 2002, bytem v Moravskoslezském kraji.

Policejní komisař ve svém Úředním záznamu popsal funkci NFT souborů a souvisejících aspektů, neboť se jednalo o nový, pro většinu společnosti dosud nepoznaný, technologický trend.

Úřední záznam[99]

„OpenSea (URL:https://opensea.io) je jedno z největších online tržišť nezaměnitelných tokenů (NFT), které umožňuje prodej, nákup a aukce NFT. Společnost sídlím na adrese 105E 24th St #4d, New York, USA. NFT lze koupit přímo za předem stanovenou cenu, nebo v aukci, kdy lze daný NFT vydražit. Transakce obvykle probíhají přes kryptopeněženku MetaMask v kryptoměně Ethereum. Tržiště rovněž umožňuje vytvářet NFT, což mohou být obrázku, audionahrávky nebo 3D modely. Při vytváření těchto NFT je možné jejich podobu skrýt a ta se odhalí až tomu, kdo si NFT koupí. Vytvoření NFT (minting) znamená proces tokenizace digitálního soboru, jeho zašifrování a zanesení do blockchainu.

Obchod s NFT zažívá obrovský nárůst v řádu miliard amerických dolarů. To kromě investorů láká i podvodníky, takže v lednu 2022 bylo cca 80% NFT vytvořených na tržišti OpenSea padělaných.

Ačkoliv jsou NFT unikátní a nezměnitelné, lze vytvářet jejich duplikáty a padělky originálů, které sice mohou vypadat stejně, ale mají různé autory a Token ID. Neopatrní investoři mohou koupit padělek v domnění, že kupují originál.

[99] Trestní spis čj. KRPE-26494/TČ-2022-170079.

Vyhledáním řetězce "Royal Cubs" bylo nalezeno kromě originální kolekce "The Royal Cubs" na URL: https://opensea.io/collection/the-royal-cubs více než 70 dalších kolekcí.“

Zde provedeným prověřováním policejní orgán pojal důvodné podezření, že předmětného jednání se dopustil Petr Dvořák, který v době spáchání podvodu nedovršil věku plné zletilosti, a proto policejní orgán postupoval v souladu se zákonem č. 218/2003 o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže. Dle zákona v návaznosti na trestní zákoník a trestný řád je osoba podezřelá ze spáchání provinění[100] podvodu dle 209 odst. 1 trestního řádu. Rovněž zákon stanoví, že *„Řízení koná soud pro mládež, v jehož obvodu mladistvý bydlí, a nemá-li stálé bydliště, soud, v jehož obvodu se zdržuje nebo pracuje.“*[101], čímž se ve věci mění místní příslušnost pro další prověřování. Policejní orgán věc z uvedeného důvodu dne 16.3.2022 postoupil dle bydliště podezřelého příslušnému policejnímu orgánu - Odbor analytiky a kybernetické kriminality při Krajském ředitelství policie Pardubického kraje.

Postoupený policejní orgán po detailním nastudování trestního spisu vyzval k podání vysvětlení Daniela Svobodu. Ten se dne 20.4.2022 k celé věci vyjádřil, kdy s ním byl sepsán Úřední záznam o podaném vysvětlení.

Úřední záznam o doplnění podaného vysvětlení – Daniel Svoboda[102]

„[předchozí text vynechán]

Dlouhodobě se zajímám o oblast IT, studuju i střední školu se zaměřením na IT, kdy v letošním roce maturuji. V poslední době mě zejména zaujala technologie NFT světa, kdy se jedná vlastně o soubory opatřené digitálním tokenem, kdy každý soubor opatřený tímto digitálním tokenem je vlastně unikátní, jedinečný a autentický. Vlastnictví souboru je pak zapsáno do blockchainu, což je vlastně digitální databáze na internetu, kam se vlastnictví a převody tokenu zapisují. Takže např. jedna fotka (digitální obrazový soubor) je opatřena NFT tokenem (certifikátem) a pak již jde o jediný pravý originál, kdy vlastnictví takovéhoto souboru s tím tokenem je pak mnohem cennější než vlastnictví té fotky bez certifikátu. S těmito soubory se pak samozřejmě obchoduje zejména na internetu, kdy např. umělci nebo herci vydávají vlastní kolekce těchto unikátních souborů (fotek, videí, písní atd.), které jsou opatřeny NFT

[100] § 6 zákona č. 218/2003 o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže
[101] § 37 zákona č. 218/2003 o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže
[102] Trestní spis čj. KRPE-26494/TČ-2022-170079.

tokenem a zájemci je pak kupují a buď si je ponechávají ve vlastnictví, nebo je zase přeprodávají dále.

Tahle technologie NFT mě opravdu zaujala a nastudoval jsem si velmi podrobně, o co jde, jak to celé funguje. Jsem v téhle oblasti na internetu docela aktivní a dalším lidem jsem pak např. vysvětloval nebo radil na různých diskusních fórech na internetu, kde lze NFT soubory koupit a jak to celé funguje. Sám i nějaké takové NFT soubory vlastním. Také se na mě sem tam obrací i cizí lidé a chtějí s něčím poradit nebo něco vysvětlit. Dne 12. ledna 2022 se na mě pak obrátil i mně neznámý kluk jménem [Jan Novák], který se dotazoval taky na věci týkající se NFT souborů.

[text o komunikaci s poškozeným vynechán]

Otázka: Měl jste možnost prozkoumat NFT soubory, které zakoupil poškozený [Jan Novák]? Jedná se dle vašeho názoru o pravou NFT kolekci The Royal Cubs? Jak lze určit či poznat, zda je tato kolekce "originální" nebo "fake"?

Odpověď: Ano, NFT soubory [Jana] jsem prozkoumal a zjistil jsem, že se jedná o nepravé soubory, že nejde o originální kolekci The Royal Cubs. To jsem poznal podle toho, že přes oficiální stránku www.theRoyalCubs.com jsem zjistil, že [Janem] zakoupená kolekce v době kdy jí koupil ještě oficiálně nevyšla, nebyla vydána, nesedělo to o několik dní.

Otázka: Jak byste vysvětlil, že jde o "falešné“ NFT soubory?

Odpověď: Nesedělo tedy datum vydání, NFT byly ukradené z náhledů oficiální kolekce. Tyto soubory byly zkrátka bezcenné, neměly žádné využití oproti originálním NFT souborům.

Odpověď: Jak to podle Vás pachatel udělal? V čem přesně měl ten "podvod" spočívat?

Odpověď: Pachatel si propojil svoji peněženku Metamask s aukčním portálem Opensea, kam následně nahrál ukradené náhledy z originální kolekce The Royal Cubs z originálních stránek na Discordu. Dále se zřejmě přes komunikační platformu Discord zkontaktoval s [Janem], který mu uvěřil, že se jedná o pravou kolekci The Royal Cubs a navedl jej ke koupi falešných a bezcenných NFT obrázků. Platba za falešné NFT obrázky probíhala zřejmě přes aukční tržiště OpenSea, kde měl pachatel falešné obrázky nahrané a měl u nich stanovenou cenu. Obrázky byly zakoupeny digitální měnou Ethereum. [Jan] zřejmě nevěděl, že peníze (kryproměnu Ethereum) posílá do peněženky pachatele a ne do peněženky originální kolekce The Royal Cubs.

Otázka: Dle Vašeho názoru, s Vašimi technickými a IT znalostmi, šlo o legitimní obchod, nebo ten prodejce uvedl kupujícího v omyl?

Odpověď: Kupující byl prodejcem uveden v omyl.

Otázka: Dle tvrzení p. [Jana Nováka] jste měl o celém věci komunikovat i s tím prodejcem. Znáte ho, víte o koho se jedná?

Odpověď: Osobně jej neznám, komunikoval jsem s ním na žádost [Jana] přes Instagram. Chaty jsem předal dobrovolně policii. On při komunikaci v chatu na Instagramu vystupoval pod nickem [anonymizováno], kdy ale z jeho fotek a dalších informací které jsem měl je jasné že šlo o [Petra Dvořáka].

Otázka: Během komunikace s [Petrem Dvořákem] ohledně předmětné "FAKE" kolekce NFC obrázků, přiznal tento, že šlo o podvod a že peníze (platba) skončila u něj?

Odpověď: Ano, to připustil, přímo mi řekl (napsal) že mu ty peníze vrátí a že to na něj zkusil. Podle mě mu bylo jasné, že nejde o pravé (autentické) NFC obrázky, ale o jejich téměř bezcenné kopie. Já jsem si s [Petrem Dvořákem] psal vícekrát a on mi sliboval že [Janovi] peníze vrátí, když ho podvedl, kdy mi je jasné že musel vědět, že nejde o "běžný" obchod ale o boudu na toho kupujícího, který se v tom neorientoval a naletěl mu. Z komunikace s [Petrem Dvořákem] vyplynulo, že peníze (Ethereum) za NFT soubory obdržel on na svoji peněženku.

Já jsem se na něj na OpenSea nedávno díval - na [Petra Dvořáka] (na tržišti OpenSea vystupoval pod nickem [anonymizováno]) a na tom jeho profilu se dalo najít, že ty obrázky on sám přímo vytvořil, opatřil certifikátem (NFT) a pak je zveřejnil na FAKE profilu "[anonymizováno]" na tom OpenSea, ze kterého je dále ZDARMA přesunul na profil [anonymizováno]. Ale dnes je tohle (ta historie těch souborů) už skrytá, kdy tohle musel skrýt ten [Petr] (nikdo jiný k tomu nemá práva).

[další text vynechán]“

V podání vysvětlení pan Svoboda vysvětlil vztahy mezi ním, panem Dvořákem a panem Novákem. Rovněž popsal funkci kryptoměn a NFT technologie, kde se vyjádřil i k důvodům, proč si myslí, že byl pan Novák podveden ze strany pana Dvořáka a jak byl podvod realizován. Vyjádřil se rovněž ke skutečnosti, kdy se mu měl podezřelý k činu doznat. Bezprostředně po podaném vysvětlení policejní orgán Svobodu vyzval v souladu s § 78 odst. 1 trestního řádu k vydání dat, které zmiňuje ve svém vysvětlení.

Protokol o vydání věci[103]

„Dne 20.04.2022 v 13:05 hodin byl podle § 78 odst. 1 trestního řádu vyzván: [Daniel Svoboda, r. 2002, bytem v Moravskoslezském kraji]

k vydání:

komunikace vedená na Instagramu z profilu "[anonymizováno]" s dalšími osobami užívající profily na Instagramu s uživatelskými jmény "[anonymizováno]" a "[anonymizováno]"

jako věci, která může sloužit pro důkazní účely.

[text poučení vynechán]

Po poučení vyzvaná osoba uvádí:

Poučení jsem porozuměl, chápu svá práva i povinnosti, těmto jsem porozuměl a uvádím, že Policii ČR pro potřeby probíhajícího trestního řízení dobrovolně vydávám komunikaci vedenou mezi mnou a zájmovými osobami přes soc. síť Instagram. Můj profil na Instagramu je

[103] Trestní spis čj. KRPE-26494/TČ-2022-170079.

pod názvem "[anonymizováno]" a zájmové chaty jsou s osobami užívající profily na Instagramu s uživatelskými jmény "[anonymizováno]" a "[anonymizováno]".

Komunikace byla zajištěna tak, že se uživatel [Daniel Svoboda] přihlásil na svůj účet na Instagramu, vněm našel zájmové komunikace, tyto byly policistou následně nafoceny (screenshoty komunikace) a tyto screenshoty následně staženy do prac. notebooku PČR. Následně byly komunikace zpakovány do souboru s názvem "KRPE-26494-TC-2022-170079 komunikace [Daniel Svoboda].rar", který byl poté pro zajištění autenticity dat opatřen kontrolní sumou o velikosti MD5: 8cc2025331988394ef857f2342768154.

K tomu uvádím, že komunikace nežádám vrátit zpět, stále je vlastním na svém účtu. To je vše, co k věci uvádím.

[pokračování textu vynecháno]“

Protokolem o vydání věci policejní orgán procesně správně získal data od Daniela Svobody, která mohou být v trestním řízení považována za platný důkaz. Pro zachování integrity vydaných digitálních dat, byla data komprimována do souboru „.rar“ a soubor opatřen kontrolní sumou MD5. Kontrolní suma představuje pečeť dat a v případě, že by byla v budoucnu změněna, kontrolní suma změnu zaznamená a při jejím opětovném výpočtu bude rozdílná. Takto zajištěná data jsou bezpečná a nelze je v průběhu trestního řízení měnit, či s nimi jakkoliv manipulovat.

Policejní orgán vyzval k podání vysvětlení babičku podezřelého, která se jako zákonná zástupkyně mladistvého podezřelého k věci řádně vyjádřila. V úředním záznamu o podaném vysvětlení uvedla sociální poměry podezřelého Dvořáka a vyjádřila se k případu samotnému, kdy uvedla, že o podvodu ví, neboť ji o tom Petr řekl. Domluvili se spolu na úhradě škody, která se musí uhradit poškozenému Janovi. Petr ji však sdělil, že mu peníze vrátit nemůže, neboť je již investoval do oficiálních NFT obrázků, které ztratili na hodnotě a o peníze přišel. V závěru uvedla, že se s Janem dohodli o postupném splácení vzniklé škody.

10. Zahájení trestního stíhání

Na základě všech zjištěných skutečností v rámci celého prověřování policejní orgán dospěl k závěru, že jednání se dopustila určitá osoba, a proto ve věci zahájil trestní stíhání[104] osoby Petra Dvořáka pro spáchání provinění podvodu dle § 209 odst. 1 trestního zákoníku.

USNESENÍ o zahájení trestního stíhání[105]

„Policejní orgán Oddělení kybernetické kriminality Pardubice, Odbor analytiky a kyber. kriminality rozhodl takto:

Podle ustanovení § 160 odst. 1 trestního řádu, za použití § 6 odst. 1 zákona číslo 218/2003 Sb., se zahajuje trestní stíhání mladistvého

[Petra Dvořáka, r. 2004, bytem v Pardubickém kraji], jako obviněného ze spáchání provinění podvodu podle ustanovení § 209 odst. 1 trestního zákoníku,

kterého se měl dopustit tím, že

v období minimálně od 7.1.2022 do 11.1.2022, v místě svého bydliště, nejprve na svém počítači s využitím grafických programů a na internetu zveřejněných náhledů originálních obrázků kolekce The Royal Cubs, vytvořil falešné kopie NFT obrázků originální kolekce The Royal Cubs, které rovněž nechal opatřit digitálními tokeny a zveřejnil je na online tržišti s NFT soubory OpenSea (htttps://opensea.io) pod odkazem htttps://opensea.io/collection/theroyalecubs,

kde je jako pravé nabízel k prodeji a následně pod záminkou výhodné koupě originálních NFT obrázků kolekce The Royal Cubs pomocí sociálních sítí a komunikační platformy Discord i pomocí přesných internetových odkazů navedl poškozeného [Jana Nováka] ke koupi těchto tří bezcenných falešných NFT obrázků za celkovou částku 0,67 ETH (částka 0,67 virtuální měny Ethereum ke dni 11.1.2022 odpovídala částce 46.653,- Kč), kterou si od [Jana Nováka] nechal dne 11.1.2022 po částech zaslat do kryptoměnové peněženky s adresou 0xA0[..]7C77, kdy si obdrženou virtuální měnu ponechal pro vlastní potřebu, čímž způsobil poškozenému [Janu Novákovi] škodu ve výši 46.653,- Kč,

tedy

sebe nebo jiného obohatil tím, že uvedl někoho v omyl, využil něčího omylu nebo zamlčel podstatné skutečnosti a způsobil tak na cizím majetku škodu nikoli nepatrnou.

[část odůvodnění vynechána]“

---

[104] § 160 odst. 1 trestního řádu
[105] Trestní spis čj. KRPE-26494/TČ-2022-170079.

V odůvodnění usnesení policejní orgán shrnul všechny zjištěné skutečnosti v rámci prověřování. Usnesením o zahájení trestního stíhání osoby se trestní řízení přesouvá do fáze vyšetřování, ve které byly provedeny další úkony.

11. Vyšetřování

V rámci vyšetřování policejní orgán provedl opětovné podání vysvětlení s poškozenou osobou, která se vyjádřila zejména ke způsobené škodě. Bylo zjištěno, že obviněný pan Dvořák je v průběhu trestního řízení v kontaktu s poškozeným, kdy i nahradil část způsobené škody v české měně, převodem na bankovní účet. Postupně uhradil většinovou část způsobené škody ve výši 37.638 Kč. Zbývající částku 9.015 Kč neuhradil s odůvodněním, že už nemá žádné peníze. Výpovědí bylo zjištěno, že se pan Dvořák panu Novákovi neomluvil, ani neprojevil žádnou lítost. Poškozený se tak připojil k trestnímu řízení s jeho nárokem na náhradu způsobené škody, která mu po uhrazení poměrné částky vznikla ve výši 9.015 Kč.[106]

Po zjištění všech uvedených skutečností byl s obviněným sepsán protokol o jeho výslechu.

Protokol o výslechu obviněného[107]

„[předchozí text vynechán]

K usnesení, kterým bylo zahájeno trestní stíhání mé osoby pro provinění podvodu podle ustanovení § 209 odst. 1 trestního zákoníku a které mi bylo doručeno dne 25.7.2022, uvádím, že toto usnesení je pravdivé.

Je pravdou, že jsem dne 7.1.2022 v místě svého bydliště na adrese [Pardubický kraj] za využití grafického programu Adobe Photoshop a na internetu zveřejněných náhledů originálních obrázků kolekce The Royal Cubs, na svém tabletu Apple Ipad, vytvořil falešné kopie NFT obrázků originální kolekce The Royal Cubs a tyto obrázky jsem zveřejnil na online tržišti s NFT soubory OpenSea (htttps://opensea.io) pod odkazem htttps://opensea.io/collection/theroyalecubs, kde jsem je nabízel jako pravé k prodeji. Na sociální síti Instagram jsem se seznámil s [Janem Novákem], který chtěl koupit NFT obrázky a já jsem mu poslal odkaz na mnou vytvořenou falešnou kolekci obrázků The Royal Cubs. On tyto obrázky dne 11.1.2022 zakoupil a částku 0,67 Eth přes Opensea postupně poslal do mé kryptoměnové peněženky s adresou 0xA0[…]7C77. Za obdrženou virtuální měnu od [Jana Nováka] jsem si já následně zakoupil pravé obrázky kolekce The Royal Cubs, které však po čase pozbyly hodnoty a já jsem o celou investici přišel. Tímto jsem způsobil [Janu Novákovi] škodu ve výši 46.653,- Kč.

Sám si dále k věci vypovídat nepřeji, odpovím na otázky policejního komisaře.

---

[106] § 43 odst. 3 trestního řádu
[107] Trestní spis čj. KRPE-26494/TČ-2022-170079.

Otázka policejního komisaře: Jste v současné době v kontaktu s poškozeným [Janem Novákem]?

Odpověď: Ano jsem. Píšeme si spolu cca jednou týdně na Instagramu. Řešíme spolu náhradu škody.

Otázka policejního komisaře: Nahradil jste poškozenému celou vzniklou škodu? Jakou část vzniklé škody jste mu případně nahradil?

Odpověď: Celou škodu jsem mu nenahradil. Poslal jsem mu cca 80 procent částky. Mám mu ještě poslat 0,2 Eth. Tu částku co on chce, mu skutečně pošlu ale nevím kdy. Asi mu ještě dlužím 10.000,- Kč, přesně nevím.

Otázka policejního komisaře: Přejete si k věci ještě něco uvést? Odpověď: Asi ne.„

V protokolu o výslechu obviněného se pan Dvořák plně doznal ke svému jednání, kdy jeho výpověď plně koresponduje se zjištěným stavem věci. Obviněný také dostal prostor pro vyjádření své lítosti, čehož nevyužil a vyjádřil se pouze k jednání, které přímo souvisí se spáchaným podvodem. Jeho výslech na mě, jako na autora práce, subjektivně působí chladně s nezájmem o vyjádření lítosti, či uvědomění, že spáchal protiprávní jednání, kterým způsobil nikoliv nepatrnou škodu. Postupné vyrovnání způsobené škody je pozitivním faktorem, kdy poškozený obdržel zpět alespoň část finančních prostředků.

Policejní orgán ukončil vyšetřování a spisový materiál společně s návrhem na podání obžaloby proti obviněnému ke dni 4. 10. 2022 doručil státnímu zástupci.[108]

[108] V souladu s ust. § 166 odst. 3 trestního řádu

12. Řízení před soudem

Státní zástupce po prostudování spisového materiálu shledal zákonné podmínky pro podání obžaloby[109] na obviněného mladistvého Petra Dvořáka a obžalobu 17. 10. 2022 doručil příslušnému Okresnímu soudu ve věcech mládeže, kde navrhl uložení trestního opatření ve výměře pěti měsíců s podmíněně odloženým výkonem na zkušební dobu jednoho roku.

Okresní soud ve věcech mládeže po prostudování spisového materiálu shledal podmínky pro vydání trestního příkazu a rozhodl tak o vině a trestním opatření, přičemž se shodl s návrhem státního zástupce.

Trestní příkaz[110]

„Samosoudce Okresního soudu v Pardubicích jako soud pro mládež vydal dne 20. 10. 2022 podle § 314e odst. 1 tr. ř. následující trestní příkaz:

Obviněný

mladistvý [Petr Dvořák]

je vinen, že

v období minimálně od 7. 1. 2022 do 11. 1. 2022 v místě svého bydliště v [Pardubickém kraji] na svém počítači s využitím grafických programů a na internetu zveřejněných náhledů originálních obrázků kolekce The Royal Cubs vytvořil falešné kopie NFT obrázků originální kolekce The Royal Cubs, které nechal opatřit digitálními tokeny a zveřejnil je na online tržišti s NFT soubory OpenSea (htttps://opensea.io) pod odkazem htttps://opensea.io/collection/theroyalecubs, kde je jako pravé nabízel k prodeji, a následně pod záminkou výhodné koupě originálních NFT obrázků kolekce The Royal Cubs pomocí sociálních sítí a komunikační platformy Discord i pomocí přesných internetových odkazů navedl poškozeného [Jana Nováka] ke koupi těchto tří bezcenných falešných NFT obrázků za celkovou částku 0,67 ETH (částka 0,67 virtuální měny Ethereum ke dni 11. 1. 2022 odpovídala částce 46.653 Kč), kterou si od [Jana Nováka] nechal dne 11. 1. 2022 zaslat do kryptoměnové peněženky s adresou 0xA0[..]7C77, kdy si obdrženou virtuální měnu ponechal pro vlastní potřebu, čímž způsobil poškozenému [Janu Novákovi] škodu ve výši 46.653 Kč, tedy

sebe obohatil tím, že uvedl někoho v omyl, a způsobil tak na cizím majetku škodu nikoli nepatrnou,

čímž spáchal

provinění podvodu podle § 209 odst. 1 tr. zákoníku,

a odsuzuje se

---

[109] V souladu s ust. § 176 odst. 1 trestního řádu

[110] Trestní spis čj. KRPE-26494/TČ-2022-170079.

podle § 209 odst. 1 tr. zákoníku za použití § 31 odst. 1 zákona o soudnictví ve věcech mládeže k trestnímu opatření odnětí svobody v trvání 5 (pět) měsíců.

Podle § 81 odst. 1 tr. zákoníku, § 82 odst. 1 tr. zákoníku a § 33 odst. 1 zákona o soudnictví ve věcech mládeže se výkon uloženého trestního opatření podmíněně odkládá na zkušební dobu v trvání 1 (jeden) rok.

Podle § 228 odst. 1 tr. řádu je obviněný povinen nahradit škodu poškozenému [Janu Novákovi], ve výši 9 015 Kč.

Poučení:

Proti tomuto trestnímu příkazu lze do osmi dnů od jeho doručení podat u zdejšího soudu odpor. Právo podat odpor nenáleží poškozenému. Pokud je odpor podán včas oprávněnou osobou, trestní příkaz se ruší a ve věci bude nařízeno hlavní líčení. Při projednání věci v hlavním líčení není samosoudce vázán právní kvalifikací ani druhem a výměrou trestu obsaženými v trestním příkaze. Nebude-li odpor řádně a včas podán, trestní příkaz se stane pravomocným a vykonatelným. V případě, že obviněný odpor nepodá, vzdává se tím práva na projednání věci v hlavním líčení.“

V zákonné lhůtě proti trestnímu příkazu nebyl podán žádnou stranou odpor a trestní příkaz dne 9.11.2022 nabyl právní moci a je vykonatelný. Odsouzený přijal trestní příkaz, ve kterém mu byla vedle trestního opatření uložena i povinnost nahradit zbytek způsobené škody ve výši 9.015 Kč.

13. Zhodnocení

V závěru této kazuistiky zpracovávaného případu lze konstatovat, že případ ukázal, jakým způsobem mohou být jednotlivci ohroženy v souvislosti s informační kriminalitou. V popsaném případě byla užita technika sociálního inženýrství, čímž pachatel zmanipuloval svou oběť a přesvědčil ji o zdánlivě výhodném nákupu NFT souborů, přičemž ho k této činnosti krok po kroku naváděl. Oběť akceptovala předem připravený scénář, který za užití informačních technologií pachatel připravil. Tímto způsobem se pachatel mnohem jednodušeji dostal k finančnímu obnosu, nežli by překonal bezpečnostní zabezpečení informačních technologií, které poškozený využívá.

Zásadním bylo prozření poškozeného po spáchání trestného činu, kdy si téměř okamžitě začal zjišťovat informace u svých známých osob, které mu sdělily, že se stal obětí podvodu. To mělo za následek oznámení trestného činu hned následující den po jeho spáchání. Zároveň poškozený prohloubil své znalosti v oblasti technologie NFT souborů a aktivně se zapojil do objasňování tohoto činu. Jeho aktivní přístup pomohl orgánům činným v trestním řízení se v nové technologii rychleji orientovat.

Je nutné neopomenout skutečnost, že celé trestní řízení probíhalo téměř 9 měsíců i přes skutečnost, že totožnost pachatele byla známa téměř okamžitě. To především způsobuje složitost procesních úkonů a případu samotného. Případ byl celkem dvakrát postoupen mezi policejními orgány, následně předán státnímu zástupci k podání obžaloby a celý spis nakonec předložen soudu ke spravedlivému odsouzení. Jak kriminalisté, tak i státní zástupce a soudce se museli seznámit s technickými aspekty a fungováním celé technologie, aby mohlo dojít k poznání skutkového stavu. Dále se proces prodloužil z důvodu geologicky vzdálených míst pobytů všech zúčastněných osob, se kterými byly realizovány jednotlivé úkony.

Kazuistika ukazuje, jak snadno mohou být jednotlivci podvedeni, pokud nejsou dostatečně obezřetní. Připodobněním lze závěrem konstatovat, že v reálném případě potencionální oběti s největší pravděpodobností také nekoupí věc v tak vysoké hodnotě, jen protože jim to poradí cizí osoba na ulici. Stejně tak

je nezbytné přistupovat i v oblasti virtuálního prostředí a být co možná nejobezřetnější.

Závěr

Výskyt informační kriminality se v posledních letech výrazně zvyšuje a stává se závažným problémem pro celou společnost. Cílem bakalářské práce bylo provést čtenáře touto problematikou, s důrazem na ta jednání, u kterých je útok veden proti osobám využívající informační technologie.

V teoretické části bakalářské práce byly přiblíženy základní aspekty informační kriminality, jakožto v současnosti nejvíce rozvíjející se formu trestné činnosti. Úvodem byly vysvětleny pojmy, které jsou pro komplexní pochopení informační kriminality zásadní. Za účelem nastínění aktuálnosti řešené problematiky, byla zpracována statistická data vývoje informační kriminality v České republice. Data objektivně poukazují na její rapidní nárůst a postupný přesun celkové kriminality do virtuálního prostředí, upozorňující na sestupný trend objasněnosti a vymezující zastoupení jednotlivých projevů. V části obsahu je uvedeno rozdělení informační kriminality, dle různých hledisek, její nejčastější projevy a právní úprava, která vymezuje nežádoucí jednání ve virtuálním prostoru a reguluje podmínky jeho užívání. Závěr teoretické části je věnován procesním a kriminalistickým specifikům v trestním řízení, neboť se jedná o trestnou činnost, která se od ostatních v mnoha směrech odlišuje. Zmíněny jsou zvláštní způsoby dokazování, zajišťování stop, získávání informací a specifické postavení pachatelů a obětí.

Praktická část práce se věnovala případové studii, která zpracovala trestný čin podvodu, jenž byl spáchán v prostředí informačních technologií, přičemž cílem pachatele bylo oklamat poškozeného za účelem finančního zisku. Tím studie obsáhla jednak jednu z nejčastějších forem páchání informační kriminality, jednak vymezení této práce. Ze samotné studie vyplývá, že informační kriminalita se velkou měrou vyznačuje specifickou trestnou činností, která klade vysoké nároky na orgány činné v trestním řízení v oblasti znalostí informačních technologií, jejich neustálého rozvoje a velké rozmanitosti ve způsobu spáchání jednotlivých trestných činů. Studie akcentuje zvláštnosti při určování místní příslušnosti, vyžadování informací, zajišťování důkazů a elektronických dat, prováděného šetření a dalších specifických úkonů, přičemž demonstruje jejich aplikaci na zpracovaném případu.

Na případové studii jsou aplikovány poznatky z teoretické části v praxi, čímž předkládaná bakalářská práce tvoří ucelené poznání problematiky informační kriminality, která je páchána na území České republiky, přičemž plně zpracovává vymezené téma v jejím úvodu.

Vypracováním bakalářské práce jsem dospěl k názoru, že prevence je klíčovým faktorem pro efektivní boj s informační kriminalitou. Velmi důležitá je také edukace uživatelů informačních technologií tak, aby dokázali dostatečně včas odhalit nekalé praktiky útočníků informační kriminality a na ně vhodně reagovat stejně jako v reálném prostředí. I když bakalářská práce nese název „Informační kriminalita v České republice“, tak se jako autor práce neztotožňuji s faktem, že informační kriminalita je problémem České republiky, nýbrž se často jedná o trestnou činnost mezinárodního charakteru, přičemž národní právní rámce mohou být nedostatečné. Je proto třeba vyvíjet úsilí na mezinárodní úrovni, aby bylo možné efektivněji potlačovat tuto kriminalitu a účinně vymáhat tresty pro pachatele, v rámci čehož by měly být podporovány mezinárodní dohody a spolupráce mezi státy v oblasti boje proti informační kriminalitě.

Závěrem lze konstatovat, že informační kriminalita je velmi sofistikovanou a dynamickou problematikou, u které je třeba neustále sledovat její vývoj a volit včasná a vhodná opatření, stejně tak i prohlubovat vědomosti orgánů činných v trestním řízení, které se aktivně podílejí na jejím potlačování.

Seznam použité literatury

Monografie

[01] KOLOUCH, Jan. *CyberCrime* [online]. 1. vydání. Praha: CZ.NIC, 2016. [cit. 15.1.2023]. ISBN: 978-80-88168-15-7. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf

[02] SMEJKAL, Vladimír, Tomáš SOKOL a Martin VLČEK. *Počítačové právo*. Praha: C.H. Beck, 1995. ISBN: 80-7179-009-5.

[03] GIBSON, William. *Neuromancer*. Vydání páté. Přeložil Josef RAUVOLF. Praha: Euromedia Group, 2019. ISBN: 978-80-7617-760-4.

[04] TANENBAUM, Andrew. *Computer networks*. 4. vydání. New Jersey: Prentice-Hall, 2003. ISBN: 9780130661029.

[05] KUROSE, James F. a Keith W. ROSS. *Computer networking: a Top-down approach featuring the Internet*. 7. vydání. Boston: Addison-Wesley, 2017. ISBN 9780201477115.

[06] ZAVRŠNIK, Aleš. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7552-758-5.

[07] STROUKAL, Dominik a Jan SKALICKÝ. *Bitcoin: peníze budoucnosti: historie a ekonomie kryptoměn, stručná příručka pro úplné začátečníky*. Praha: Wolters Kluwer, 2015. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-87733-26-4.

[08] KONRÁD, Zdeněk, Viktor PORADA, Jiří STRAUS a Jaroslav SUCHÁNEK. *Kriminalistika: kriminalistická taktika a metodiky vyšetřování*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7380-547-0.

[09] SMEJKAL, Vladimír a Jan SKALICKÝ. *Internet @ §§§: peníze budoucnosti: historie a ekonomie kryptoměn, stručná příručka pro úplné začátečníky*. Praha: Grada, 1999. Právní monografie (Wolters Kluwer ČR). ISBN 80-716-9765-6.

[10] JELÍNEK, Jiří. *Trestní právo hmotné: obecná část, zvláštní část*. 7. aktualizované a doplněné vydání. Praha: Leges, 2019. Student (Leges). ISBN 978-80-7502-380-3.

[11] STRAUS, Jiří. *Kriminalistická metodika*. 2. rozšířené vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2008. ISBN 978-80-7380-124-3.

[12] POLČÁK, Radim. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7598-045-8.

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

Zákonná úprava a IAŘ

[14] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů v posledním znění

[15] Sdělení č. 104/2013 Sb. m. s., Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě v posledním znění

[16] Zákon č. 40/2009 Sb., trestní zákoník v posledním znění

[17] Usnesení č. 2/1993 Sb., předsednictva České národní rady o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součástí ústavního pořádku České republiky v posledním znění

[18] Zákon č. 141/1961 Sb., o trestním řízení soudním v posledním znění

[19] Usnesení Nejvyššího soudu ČR ze dne 19.11.2020 č. 7 Td 58/2020

[20] Pokyn policejního prezidenta č. 30/2009, o plnění úkolů v trestním řízení v posledním znění

[21] Zákon č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů v posledním znění

[22] Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů v posledním znění

[23] Zákon č. 21/1992 Sb., o bankách v posledním znění

[24] Zákon č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních v posledním znění

[25] Sdělení komise Evropskému parlamentu, Radě a Evropskému Výboru regionů č. 267/2007, k obecné politice v boji proti počítačové kriminalitě

[26] Sdělení č. 9/2015 Sb. m. s., Ministerstva zahraničních věcí o sjednání Dodatkového protokolu k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů

Webové stránky a elektronické zdroje

[27] *Kyberkriminalita - Policie České republiky* [online]. 2023 Policie ČR [cit. 06.02.2023]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

[28] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti* [online]. Praha: Národního úřad pro kybernetickou a informační bezpečnost, 2022. [cit. 07.02.2023]. Dostupné z: https://www.cybersecurity.cz/data/Slovnik_523el.pdf

[29] CZ.NIC, Akademie. Jak na internet: Struktura internetu. *Metodický portál: Články* [online]. 06. 10. 2014, [cit. 07.02.2023]. ISSN 1802-4785. Dostupné z: https://clanky.rvp.cz/clanek/19213/JAK-NA-INTERNET-STRUKTURA-INTERNETU.html

[30] Neutral Internet Exchange. *Technické informace* [online]. Praha: NIX.CZ, 1997 [cit. 16.02.2023]. Dostupné z: https://nix.cz/cs/technical

[31] *Vývoj registrované kriminality - Policie České republiky* [online]. Praha: Policie ČR, 2023 [cit. 06.02.2023]. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx

[32] *Jednotlivé druhy kyberkriminality - Policie České republiky* [online]. Praha: Policie ČR, 2023 [cit. 06.02.2023]. Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx

[33] *Rekodifikace trestního práva procesního – Justice* [online]. Praha: Ministerstvo spravedlnosti ČR, 2022 [cit. 16.02.2023]. Dostupné z: https://justice.cz/web/msp/rekodifikace-trestniho-prava-procesniho

[34] *Mezinárodní spolupráce v boji proti informační kriminalitě - Ministerstvo vnitra České republiky* [online]. Praha: Ministerstvo vnitra ČR, 2009 [cit. 16.02.2023]. Dostupné z: https://www.mvcr.cz/soubor/cyber-vyzkum-studie-mezinarodni-pdf.aspx

[35] ZAHRADNÍČEK Jan. *Počítačová kriminalita: Mezinárodní úmluva je konečně závazná i pro Česko - Patria.cz* [online]. 2014 [cit. 16.02.2023]. Dostupné z: https://www.patria.cz/pravo/2694193/pocitacova-kriminalita-mezinarodni-umluva-je-konecne-zavazna-i-pro-cesko.html

[36] *Výbor k úmluvě o počítačové kriminalitě T-CY – Justice* [online]. Praha: Ministerstvo spravedlnosti ČR [cit. 16.02.2023]. Dostupné z: https://justice.cz/web/msp/rada-evropy?clanek=vybor-k-umluve-o-pocitacove-kriminalite-t-cy-

[37] *United nations manual on the prevention and control of computer-related crime - International review of criminal policy* [online]. New York: United Nations Digital Library Systém, 1994 [cit. 16.02.2023]. Dostupné z: https://digitallibrary.un.org/record/162804

[38] *Národní úřad pro kybernetickou a informační bezpečnost – Legislativa* [online]. Praha: Národní úřad pro kybernetickou a informační bezpečnost [cit. 16.02.2023]. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/

[39] *Prevence kriminality v České republice* [online]. Praha: Ministerstvo vnitra ČR, 2023. [cit. 16.02.2023]. Dostupné z: https://prevencekriminality.cz/prevence-kriminality/

[40] KUCHTA, Josef. *Časopis pro právní vědu a praxi: Aktuální problémy počítačové kriminality včetně její prevence* [online]. Praha: 24. Masarykova univerzita, Právnická fakulta, 2016 [cit. 16.02.2023]. ISSN 1805-2789. Dostupné z: https://journals.muni.cz/cpvp/article/view/5260

[41] *Odbor prevence kriminality - Ministerstvo vnitra České republiky* [online]. Praha: Ministerstvo vnitra České republiky, 2023 [cit. 16.02.2023]. Dostupné z: https://www.mvcr.cz/clanek/odbor-prevence-kriminality.aspx

[42] *Kybernetická kriminalita – Příručka pro policisty* [online]. 1. vydání. Kralovy Vary: you connected, z.s., 2018 [cit. 16.02.2023]. Dostupné z: Intranet Policie ČR.

[43] *Strategie prevence kriminality v České republice na léta 2022 až 2027* [online]. Praha: Ministerstvo vnitra ČR, 2023. [cit. 16.02.2023]. Dostupné z: https://www.mvcr.cz/clanek/strategie-prevence-kriminality-v-ceske-republice-na-leta-2022-az-2027.aspx

[44] VICHLENDA, Milan. Studijní opora: Kriminalistika [online]. Karvinná: Střední odborná škola ochrany osob a majetku, 2011 [cit. 16.02.2023]. Dostupné z: https://www.sosoom-zlin.cz/media/skripta/kriminalistika.pdf

[45] HARTLEY Andrew, *Who Is Most Likely to Be a Victim of a Cybercrime?. LinkedIn* [online]. 2021 [cit. 16.02.2023]. Dostupné z: https://www.linkedin.com/pulse/who-most-likely-victim-cybercrime-andrew-hartley

[46] *Preventivní publikace: Bílí koně. Europol* [online]. [cit. 16.02.2023]. Dostupné z: https://www.europol.europa.eu/sites/default/files/documents/cz_flyers.pdf

[47] *Problematika bílých koní - Policie České republiky* [online]. Praha: Policie ČR, 2023 [cit. 16.02.2023]. Dostupné z: https://www.policie.cz/clanek/problematika-bilych-koni.aspx

[48] *Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY - Cybercrime* [online]. Strasbourg Cedex: Council of Europe, 2023 [cit. 18.02.2023]. Dostupné z: https://www.coe.int/en/web/cybercrime/parties-observers

[49] *Kriminalita - Policie České republiky* [online]. Praha: Policie ČR, 2023 [cit. 18.02.2023]. Dostupné z: https://www.policie.cz/statistiky-kriminalita.aspx

Přílohy

Příloha č. 1 – Výčet trestných činů, při jejichž páchání mohou být užity prostředky informačních a komunikačních technologií[111]

- § 180 neoprávněné nakládání s osobními údaji
- § 181 poškození cizích práv
- § 182 porušení tajemství dopravovaných zpráv
- § 184 pomluva
- § 191 šíření pornografie
- § 192 výroba a jiné nakládání s dětskou pornografií
- § 193 zneužití dítěte k výrobě pornografie
- § 193b navazování nedovolených kontaktů s dítětem
- § 205 krádež
- § 209 podvod
- § 213 provozování nepoctivých her a sázek
- § 214 podílnictví
- § 216 legalizace výnosů z trestné činnosti
- § 230 neoprávněný přístup k počítačovému systému a nosiči informací
- § 231 opatření a přechovávání přístupového zařízení a hesla k počítačovému systému
- a jiných takových dat
- § 234 neoprávněné opatření, padělání a pozměnění platebního prostředku
- § 236 výroba a držení padělatelského náčiní
- § 268 porušení práv k ochranné známce a jiným označením
- § 269 porušení chráněných průmyslových práv
- § 272 obecné ohrožení
- § 276 poškození a ohrožení provozu obecně prospěšného zařízení
- § 287 šíření toxikomanie
- § 316 vyzvědačství
- § 345 křivé obvinění
- § 348 padělání a pozměnění veřejné listiny
- § 353 nebezpečné vyhrožování
- § 354 nebezpečné pronásledování
- § 355 hanobení národa, rasy, etnické nebo jiné skupiny osob
- § 356 podněcování k nenávisti vůči skupině osob nebo k omezování práv a svobod
- § 357 šíření poplašné zprávy
- § 361 účast na organizované zločinecké skupině
- § 364 podněcování k trestnému činu
- § 365 schvalování trestného činu
- § 400 genocida
- § 403 založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka
- § 407 podněcování útočné války

[111] KOLOUCH, Jan. *CyberCrime* [online]. 1. vydání. Praha: CZ.NIC, 2016. [cit. 15.1.2023]. ISBN: 978-80-88168-15-7. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf

Strategický cíl G: Prevence kybernetické kriminality		**ČR aktivně, systémově a koordinovaně posiluje prevenci kybernetické kriminality a rizikového chování v kyberprostoru a poskytuje pomoc a podporu obětem v kyberprostoru**		Indikátor pro strategický cíl		Plnění specifických cílů	Výchozí hodnota	Viz hodnoty ISC	Cílová hodnota	Viz hodnoty ISC
Specifický cíl	Indikátor pro specifický cíl (ISC)	Výchozí hodnota ISC	Cílová hodnota ISC	Opatření	Popis opatření	Harmonogram realizace opatření	Kritérium splnění	Odpovědná instituce	Spolupracující subjekty	Nároky na financování a zdroj
G.1 Nastavit systém spolupráce a vzdělávání v oblasti prevence kybernetické kriminality na národní úrovni	Existující systémová koordinace a spolupráce v oblasti prevence kybernetické kriminality	ne	ano	G.1.1 Vytvořit pracovní skupinu / komisi v rámci RVPPK ke koordinaci aktivit a spolupráce v prevenci kybernetické kriminality	V rámci RVPPK vytvořit pracovní skupinu / komisi, která bude aktivně koordinovat oblast prevence kybernetické kriminality. Bude se podílet se na tvorbě a naplňování strategických dokumentů, zprostředkovávat dobrou praxi na všech úrovních působnosti (vertikální i horizontální). Podporovat silná a strategická partnerství, participativní formu spolupráce v oblasti prevence kybernetické kriminality na národní úrovni. Zabývat se, jak působit efektivně v oblasti vzdělávání a osvěty na všechny cílové skupiny s důrazem na odbornou veřejnost a skupiny zvlášť zranitelné v kyberprostoru.	2022 vznik pracovní skupiny / komise) 2022–2027 její působení	Existující pracovní skupina	MV	členové RVPKK (vč. NÚKIB), DigiKoalice, ÚV ČR NNO	V rámci vlastních rozpočtů
				G.1.2 Spolupracovat na vzdělávání i profesním rozvoji odborníků v oblastech zvyšování digitálních kompetencí, kyberbezpečnostních návyků; posilovat digitální vědomí společnosti v oblasti wellbeingu	Ve spolupráci se zapojenými subjekty vytvářet kvalitní odborné vzdělávací materiály zaměřené na profesní vzdělávání osob, které přichází do kontaktů s rizikovými skupinami (mj. policisté, učitelé, sociální pracovníci, pracovníci v justici, zaměstnanci veřejné správy, pracovníci NNO ad.). Vytvořit tak prostor pro kvalitní dlouhodobou práci těchto profesních skupin s rizikovými skupinami v oblasti prevence kybernetické kriminality. Vytvořit jednotnou platformu a postup pro oblast vzdělávání v kybernetické bezpečnosti tak, aby bylo dosaženo zvýšení odbornosti u pracovníků působících v oblasti prevence kybernetické kriminality a řešení nápadu i dopadu kybernetické kriminality. Spolupracovat na vzdělávání i profesním rozvoji odborníků v oblasti prevence kybernetické kriminality. U cílové skupiny širší veřejnosti podporovat osvětu i zvyšování digitálních kompetencí, posilovat digitální (digitálně-právní) vědomí společnosti, zvyšovat bezpečné chování koncových uživatelů v kyberprostoru.	2022–2027	Existující spolupráce, vydávané vzdělávací materiály, existence jednotné platformy	NÚKIB	Členové RVPPK, DigiKoalice, ÚV ČR - NNO	V rámci vlastních rozpočtů
				G.1.3 Vytvořit provázaný ekosystém na bázi bilaterální spolupráce v oblasti prevence kybernetické kriminality	Sdílet poznatky a dobrou praxi, sdílet případové studie z místní lokální praxe, přenášet ji do národního měřítka. Podporovat kooperaci v rámci sítě odborníků a komunit odborníků působících v oblasti prevence a vzdělávání v kyberprostoru.	2022–2027	Existující bilaterální spolupráce	Členové RVPPK	Kraje, obce, NNO	V rámci vlastních rozpočtů
G.2. Nastavit a podporovat systém policejní práce v oblasti řešení kybernetické kriminality / kriminality páchané prostřednictvím informačních technologií v rámci PČR	Existující funkční systém práce a vzdělávání na úrovni ÚSKPV PP ČR a KŘP	ne	ano	G.2.1 Nastavit a koordinovat systém v oblasti řešení kybernetické kriminality / kriminality páchané prostřednictvím informačních technologií, zejména na úrovni ÚSKPV PP ČR a KŘP	Bude vytvořen fungující, provázaný systém řešení kriminality páchané prostřednictvím informačních technologií v rámci PČR na celorepublikové i lokální úrovni. Fungující systém podpoří nejen činnost policistů, ale bude působit i ve vztahu k práci PČR s oběťmi a potenciálními oběťmi. Operativní a kvalifikované řešení případů bude mít vliv na snižování takového druhu kriminality a bude působit i preventivně. Správné nastavení jednání s oběti bude zvyšovat důvěru k policii, pocit bezpečí, a tím bude docházet ke zvyšování motivace oznamovat páchání těchto trestných činů. Poznatky z řešených případů a práce s oběťmi budou přenášeny do tvorby metodických a vzdělávacích materiálů a preventivních aktivit Policie ČR. Poznatky budou také dále sdíleny s partnery (RVPPK, samosprávy apod.). Příslušníci PČR budou průběžně vzdělávání.	2022 nastavení systému 2022–2026 fungování systému	Existující systém policejní práce a vzdělávání v této oblasti, vytvořená metodika postupu, existující koordinace systému vzdělávání a profesního rozvoje PČR	PČR		V rámci vlastních rozpočtů
				G.2.2 Posílit personální kapacity Policie ČR v oblasti řešení kybernetické kriminality / kriminality páchané prostřednictvím informačních technologií v rámci PČR na úrovni ÚSKPV a KŘP	Navýšit počty pracovníků (příslušníků) Policie ČR v oblasti řešení kybernetické kriminality / kriminality páchané prostřednictvím informačních technologií v rámci PČR, v souladu s již schválenými materiály vlády ČR.	2022	navýšené počty pracovníků	PČR		V rámci vládou ČR již schválených počtů navýšení příslušníků Policie ČR
				G.2.3 Realizovat školení v rámci Policie ČR zaměřené na genderově podmíněné kybernásilí	Na základě projektu nastavit systém vzdělávání a profesního rozvoje pracovníků Policie ČR v problematikách genderově podmíněného kybernásilí, a to a) pro metodiky a metodičky domácího násilí v rámci pořádkové a kriminální policie o tzv. nových formách sexuálního násilí v online prostoru; b) pro liniové vedení policie bude vytvořeno školení pro zvyšování odborných kompetencí policistů v uvedených problematikách kybernásilí, šíření dobré praxe, prevence, vzdělávání a osvěty mezi příslušníky PČR.	2022 zahájení a realizace projektu (samotné zahájení možné již 2021) 2024 vytvoření systému vzdělávání 2024–2027 realizace vzdělávání jako součást systému PČR	Realizovaný projekt, vytvořená vzdělávání (2 typy), realizovaná školení	ÚV ČR (realizace projektu), PČR (promítnutí výstupů projektu do systému vzdělávání)	MV	V rámci vlastních rozpočtů, realizace pilotního projektu s podporou Norských fondů
G.3 Aktivně působit v oblasti prevence a osvěty kybernetické kriminality na všechny cílové skupiny	a) Počet realizovaných kampaní a vzdělávání b) Existující celonárodní kampaň zahrnující též problematiku vlastní prezentace dětí v on-line prostoru	a) neeviduje se b) ne c) nevyhovující stav	a) vedený přehled, zapojení všech relevantních subjektů b) ano c) naplnění kritérií opatření G.3.4	G.3.1 Posílit prevenci rizikového chování v kyberprostoru u zvlášť zranitelných skupin obyvatel zejména dětí, mládeže a také seniorů	Systematicky a dlouhodobě působit v oblasti prevence a osvěty prostřednictvím nástrojů s masivním informačním dopadem. Působit také e-learningovými nástroji a sociálními platformami. Proškolovat odbornou veřejnost i širší veřejnost kurzem Bezpečně v kyber! a dalšími e-learningovými nástroji s celorepublikovým dopadem. Podporovat projekty zaměřené na prevenci rizikového chování a v kyberprostoru a prevenci sextingu i dalších nebezpečných online projevů dětí a mládeže v kyberprostoru (i s důrazem na genderové aspekty, věk, sexuální orientaci), např. online sexuální násilí a nátlak.	2022–2027	Realizované preventivně-vzdělávací a osvětové kampaně	Členové RVPPK (vč. NÚKIB)		V rámci vlastních rozpočtů

[112] *Strategie prevence kriminality v České republice na léta 2022 až 2027* [online]. Ministerstvo vnitra České republiky [cit. 18.02.2023]. Dostupné z: https://www.mvcr.cz/clanek/strategie-prevence-kriminality-v-ceske-republice-na-leta-2022-az-2027.aspx

s důrazem na skupiny zvlášť zranitelné v kyberprostoru, zejména děti a mládež	c)Posílená kyberbezpečnost na školách				Podporovat osvětové kampaně s celorepublikovým dopadem v oblasti bezpečného chování na internetu, včetně genderově specifických hrozeb (online sexuální násilí, sexistické nenávistné projevy, pořizování, zveřejňování a šíření intimních vizuálních materiálů bez souhlasu zobrazených osob, aj.).					
				G.3.2 V rámci preventivních, vzdělávacích a osvětových aktivit v oblasti prevence kybernetické kriminality se zaměřit i na prevenci potenciálního páchání kriminality a nežádoucího chování, zejména cestou zvyšování právního vědomí.	V rámci prevence kybernetické kriminality je nutné vedle potenciálních obětí se zaměřovat také na potenciální pachatele kybernetické kriminality a dalšího nežádoucího chování v kyberprostoru. Výzkumy ukazují, že lidé často ani nemají tušení (nebo jen velmi slabé povědomí), že svým jednáním v kyberprostoru mohou páchat něco nezákonného či si vůbec neuvědomují, jak velké a negativní dopady může jejich jednání mít na druhé. Proto je nutné předcházet kyberkriminalitě i cestou zvyšování právního vědomí či upozorňováním na dopady nevhodného chování v kyberprostoru na ostatní, včetně genderových aspektů této problematiky (online sexuální násilí, sexistické nenávistné projevy na internetu, pořizování, zveřejňování a šíření intimních vizuálních materiálů bez souhlasu zobrazených osob, ad,)	2022–2027	Realizované preventivně-vzdělávací a osvětové kampaně	Členové RVPPK (vč. NÚKIB)		V rámci vlastních rozpočtů
				G.3.3 Vytvořit kampaň zaměřenou na prevenci a zvyšování povědomí o online sexuálním zneužívání i nátlaku na děti a mladistvé v kyberprostoru. Kampaň se zaměří konkrétně také na problematiku zvýšení povědomí u cílové skupiny dětí a mladistvých o rizicích při jejich vlastní sebeprezentaci na internetu a v online prostoru a jak těmto rizikům předcházet. Rovněž podporovat kampaně s takovým zaměřením realizované jinými subjekty.	Vytvoření kampaně v problematice zvyšování povědomí i v oblasti prevence sexuálního online zneužívání a nátlaku, v důsledku rizikových komunikací a sextingu, jímž čelí děti a mladiství pořizující a následně sdílející vlastní intimní materiály – fotografie, videa. Uvedená kampaň bude sloužit také jako podpora wellbeingu a zvyšování povědomí u dětí a mladistvých i jako osvěta u širší veřejnosti v oblasti zvyšování digitálních kompetencí. Zejména jako prevence rizikového chování dětí a mládeže, a to specificky i při jejich vlastní prezentaci na internetu, a jako prevence online sexuálního zneužívání. Také v rámci existujících dotačních programů či formou odborné spolupráce podporovat obdobně zaměřené projekty realizované jinými subjekty.	2022–2027	Realizace preventivní kampaně „Jak se vidím na internetu a v online světě“, podpora dalších obdobně zaměřených aktivit	MV	MŠMT, NÚKIB, PČR, NNO, ÚV (RVRŽM, OEDA),	V rámci vlastních rozpočtů, případně s využitím mimorozpočtových zdrojů (fondů EU, Norských fondů apod.)
				G.3.4 Vytvořit systém zajištění infrastruktur zabezpečení ICT ve školách. Posílit bezpečnost ve školách v oblasti prevence kybernetické kriminality a kybernetické bezpečnosti. Koordinovat systém kyberbezpečnostních auditů ve školách.	Posílit kyberprevenci i kyberbezpečnost v oblasti vzdělávání a bezpečnosti dětí a mládeže – Nastavit systém kybernetické bezpečnosti a prevence kybernetické kriminality ve všech školách v ČR. Posílit tým prevenci i detekci v oblasti kybernetické kriminality u zvlášť zranitelné skupiny obyvatel – dětí a mládeže. Po vzoru bezpečnostních auditů na školách (realizovaných také v metodickou a finanční podporou MV) vypracovat systém kyberbezpečnostních auditů ve školách. Navázat na zajištění bezpečnosti ve školách školeními odborné veřejnosti a dlouhodobou vzdělávací i osvětovou kampaní pro odbornou i širší veřejnost k posilování digitálního vědomí a digitálních dovedností i důvěry jako součásti prevence před kybernetickou kriminalitou a součásti prevence bezpečného chování v online prostředí i pro zvýšení efektivity procesu digitalizace školství.	2022–2027	Vytvoření minimálního kyber bezpečnostního standardu pro školy, rámce zabezpečení ICT infrastruktur, systému vzdělávání v online prostoru na školách jako součást prevence před kybernetickou kriminalitou a rizikovým chováním. Osvětová kampaň na školách na podporu prevence před rizikovým chováním v online prostředí.	MŠMT	MPO, MV vč. PČR, NÚKIB, MPSV, další členové RVPKK, DigiKoalice	V rámci vlastních rozpočtů
G.4 Podporovat oběti kybernetické kriminality	a) Počet poradenských pracovišť b) Existující metodika pro práci a pomoc obětem kybernetické kriminality c) Míra latence kybernetické kriminality	a) 1 pracoviště (navíc lokální) b) ne c) není známo	a) 14 krajských pracovišť b) ano c) zaveden systém pravidelného sledování latence	G.4.1 Podpořit vznik sítě krajských poradenských a informačních center	Finančně a odborně podpořit vytvoření provázané sítě poradenských a informačních center na krajích, kde bude dostupný informační servis a poradenství (lze realizovat např. formou odborníků pomáhajících na telefonních linkách, mailech apod.) obětem kybernetické kriminality, kyberagrese a kybernetického násilí. Kraje mohou realizovat samostatně, vhodná by se ale jevila koordinace např. prostřednictvím MV podporovaného projektu KPBI.	2022–2027, z toho dobudování sítě do konce roku 2025	Podpora pro 14 nově zřízených krajských center	MV vč. PČR, MSp, MPSV	Kraje (zřízení center), ÚV, členové RVPPK (odborná, případně finanční pomoc)	V rámci stávajících rozpočtů
				G.4.2 Na základě analýzy viktimnosti v oblasti kyberkriminality vytvořit metodiku pro práci a pomoc obětem kybernetické kriminality s cílem snižovat latenci kybernetické kriminality	Vytvořit metodiku pro práci v oblasti pomoci obětem kybernetické kriminality, zejména se zaměřením na kybernetické násilí a kybernetickou agresi. Vytvořit doporučení postupu pro oběti kybernásilí, kyberagrese a kybernetické kriminality. Při tom vycházet z analýzy (např. z viktimologického výzkumu) v oblasti latence kybernetické kriminality, pocitu bezpečí a dostupnosti pomoci u obětí kybernetické kriminality, zvláště u tematik kybernásilí a stalkingu.	2022–2027	2023 analýza 2025 metodika	MV vč. PČR, IKSP	ÚV, další členové RVPKK, kraje, NNO	V rámci vlastních rozpočtů

G.5 Zajistit důsledné zohledňování problematiky genderově podmíněného kybernásilí v rámci koncepční činnosti, sběru dat a legislativy	a) Počet rezortních materiálů zohledňující problematiku genderově podmíněného kybernásilí b) Počet výzkumů zohledňující problematiku genderově podmíněného kybernásilí c) Počet ročních přehledů statistik kriminality zohledňujících problematiku genderově podmíněného kybernásilí	a) 2 b) 0 c) 0	a) 7 b) 3 c) 5	G.5.1 Zahrnout problematiku genderově podmíněného kybernásilí v rezortních materiálech	V rámci rezortních strategických, koncepčních a metodických materiálů pravidelně a důsledně zohledňovat problematiku genderově podmíněného kybernásilí.	2022–2027	Výčet koncepčních, strategických a metodických dokumentů, v nichž byla problematika zohledněna	MV, MPSV, MŠMT, MSp		V rámci vlastních rozpočtů
				G.5.2 Zohledňovat problematiku genderově podmíněného kybernásilí v rámci výzkumu	Zařadit téma genderově podmíněného kybernásilí do výzkumů v oblasti trestní politiky a prevence kriminality, pachatelů a obětí domácího a genderově podmíněného násilí, trendů kyberkriminality a navrhnout účinná opatření k vytváření odpovídajícího systému zacházení s pachateli genderově podmíněného kybernásilí. Již ve stávajících výzkumech bude toto téma dle možností zohledněno, širší uplatnění je však možné až na základě návrhu nového Střednědobého plánu výzkumných úkolů, jehož realizace bude probíhat od roku 2024.	2022–2027	Výzkumná zpráva zohledňující problematiku	MSp	IKSP	V rámci vlastních rozpočtů
				G.5.3 Zohledňovat problematiku genderově podmíněného násilí v rámci sběru statistických údajů kriminality v ČR	V rámci statistik kriminality zavést kategorie za účelem získání statistických údajů o trestných činech souvisejících s genderově podmíněným kybernásilím (např. kategorie pohlaví, kategorie, zda byl čin spáchán online formou) a zvážit jejich pravidelné zveřejňování.	2022–2027	Statistiky kriminality obsahující statistické údaje o genderově podmíněném kybernásilí	MV, MSp	PČR	V rámci vlastních rozpočtů

Příloha č. 3 – Seznam členských států Budapešťské úmluvy[113]

- Albánie
- Andorra
- Argentina
- Arménie
- Austrálie
- Rakousko
- Ázerbájdžán
- Belgie
- Bosna a Hercegovina
- Brazílie
- Bulharsko
- Kapverdy
- Kanada
- Chile
- Kolumbie
- Chorvatsko
- Kostarika
- Kypr
- Česká republika
- Dánsko
- Dominikánská republika
- Estonsko
- Finsko
- Francie
- Gruzie
- Německo
- Ghana
- Řecko
- Maďarsko
- Island
- Izrael
- Itálie
- Japonsko
- Lotyšsko
- Litva
- Lucembursko
- Malta
- Mauricius
- Monako
- Černá Hora
- Maroko
- Holandsko
- Nigérie
- Severní Makedonie
- Norsko
- Panama
- Paraguay
- Peru
- Filipíny
- Polsko
- Portugalsko
- Moldavsko
- Rumunsko
- San Marino
- Senegal
- Srbsko
- Slovensko
- Slovinsko
- Španělsko
- Srí Lanka
- Švédsko
- Švýcarsko
- Tonga
- Turecko
- Ukrajina
- Spojené království
- Spojené státy americké

---

[113] *Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY - Cybercrime* [online]. Strasbourg Cedex: Council of Europe, 2023 [cit. 18.02.2023]. Dostupné z: https://www.coe.int/en/web/cybercrime/parties-observers