**Univerzita Hradec Králové**
**Fakulta informatiky a managementu**
**Katedra managementu**

# Kybernetická kriminalita proti zařízením ICT

Bakalářská práce

Autor: Lukáš Dyntar
Studijní obor: Informační management

Vedoucí práce: Mgr. Tomáš Ledvinka, Ph.D.

Hradec Králové březen 2024

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 22. 3. 2024

Lukáš Dyntar

Poděkování:

Děkuji vedoucímu bakalářské práce Mgr. Tomášovi Ledvinkovi, Ph.D. za metodickou podporu, praktické rady a odborné vedení práce.

# Abstrakt

Tato bakalářská se zaměřuje na podrobný rozbor kybernetické kriminality proti zařízením informačních a komunikačních technologií („ICT“) na území České republiky. Metodologie kombinuje rešerši literárních pramenů, případovou studii a analýzu soudních rozhodnutí ve věcech kybernetické trestné činnosti. Teoretická část práce definuje klíčové pojmy, zkoumá právní úpravu a věnuje se vybraným druhům kybernetických trestných činů. Praktická část obsahuje detailní rozbor zvolených případů s podrobným rozborem skutkové stránky a právní kvalifikace. Výsledky práce nabízejí ucelený pohled na kybernetickou kriminalitu v České republice, přičemž vyvozená doporučení se zaměřují na posílení právní ochrany a prevenci v oblasti kybernetické bezpečnosti. Tato práce je příspěvkem k pochopení a řešení rostoucích kybernetických hrozeb v kontextu praxe a moderní společnosti.



# Abstract

## Title: Cybercrime against ICT devices

This bachelor thesis focuses on a detailed analysis of cybercrime against information and communication technology ("ICT") devices in the Czech Republic. The methodology combines literature research, a case study and an analysis of court decisions in cybercrime cases. The theoretical part of the thesis defines key concepts, examines the legal framework and focuses on selected types of cybercrime. The practical part contains a detailed analysis of selected cases with a thorough analysis of the facts and legal qualification. The results of the work offer a comprehensive view of cybercrime in the Czech Republic, while the recommendations drawn focus on strengthening legal protection and prevention in the field of cyber security. This thesis is a contribution to understanding and addressing the growing cyber threats in the context of practice and modern society.

**Klíčová slova:** kybernetická kriminalita, trestní právo, počítačové trestné činy, rozbor soudních rozhodnutí, kyberprostor

**Key words:** cybercrime, criminal law, computer crime, analysis of court decisions, cyberspace

# Obsah

# 1 Úvod

V současné éře technologické revoluce se naše životy stále více propojují s digitálním světem, čímž vzniká nová sféra, kterou může ovlivnit neviditelný a někdy neuchopitelný nepřítel – kybernetická kriminalita. Tato hrozba se stala nedílnou součástí našeho každodenního života, zasahuje do osobní i obchodní sféry, veřejné správy i do soukromí jednotlivce a našich domovů. Jednou z oblastí, která je přímo spojena s informačními technologiemi, které se zde vyskytují spíše jako cíl než jako nástroj, je kriminalita zaměřená na zařízení informačních a komunikačních technologií (ICT). Tato bakalářská práce se snaží přinést strukturovaný pohled na právní problematiku kybernetické kriminality v rámci České republiky, prostřednictvím zevrubného teoretického zkoumání této problematiky a dále analýzy vybraných případů a detailního zkoumání trestních rozhodnutí soudů.

Volba tématu této práce nevychází pouze z aktuálních trendů či bezprostředního ohrožení naší digitální společnosti. Motivací autora je také spojení dvou odlišných světů – světa informačních technologií a práva. Jako student právnické fakulty se snažím propojit oba tyto obory a přinést tak komplexní pohled na kybernetickou kriminalitu. Tato práce tak nespojuje pouze teoretické znalosti z oblasti informačních technologií a práva, ale také praktický přístup prostřednictvím případové studie a analýzy judikatury.

V rámci této práce bude v teoretické části věnována pozornost definici základních pojmů spojených s kybernetickou kriminalitou. Následně bude rozebrána právní úprava na vnitrostátní i mezinárodní úrovni, aby byl čtenář seznámen s nástroji, východisky a zásadami, se kterými se v rámci boje proti kybernetické kriminalitě setkáváme. S důrazem na detail budou také prezentovány vybrané fenomény z pestré škály druhů kybernetické kriminality. Teoretická část bude uzavřena kapitolou věnovanou procesním nástrojům a aspektům, které jsou klíčové a specifické při stíhání kybernetické kriminality.

Kybernetická kriminalita je jevem, který nepoznává hranice. V době globalizace a raketového rozvoje nových technologií se stáváme svědky neustálé evoluce tohoto jevu. Pachatelé operují ve virtuálním prostoru s promyšlenými motivy a rafinovanými metodami. Tato práce se snaží vrhnout světlo na temné kouty

kybernetické kriminality, přispět k lepšímu porozumění této komplexní problematiky a upozornit čtenáře na její výskyt blíže k jeho prahu, než by se mohlo některým zdát.

# 2 Cíl a metodika práce

## *2.1 Cíl práce*

Cílem práce je zanalyzovat a poskytnout přehled o kybernetické kriminalitě proti zařízením ICT v České republice.

V teoretické části budou vymezeny jednotlivé pojmy související s kybernetickou kriminalitou, které jsou důležité pro pochopení celé problematiky a bude tak stanoven definiční základ pro zbytek této práce. Následovat bude popis legislativní situace, a to jak se zaměřením na právo vnitrostátní (zejména trestní zákoník a trestní řád) tak na mezinárodní a unijní právo, a to i s ohledem na jejich implementaci a promítnutí do národní úpravy. Těžiště teoretické části leží na analýze jednotlivých vybraných druhů kybernetických trestných činů, které budou přiblíženy jak v rovině obecné, tak i technické a především právní. V této části budou jednotlivé fenomény více rozebrány i z hlediska právní kvalifikace a subsumpce pod konkrétní ustanovení trestních předpisů a s tím souvisejících problémů. Práce se naopak nebude do podrobností zabývat obecnou částí trestního zákoníku a pouze pokud to bude na daném místě vhodné bude stručněji vysvětlena daná právní úprava.

V druhé, praktické, části práce budou rozebrány konkrétní případy kybernetické trestné činnosti, a to jak skutkově, tak především právně. Zpracováno bude celkem 7 případů tematicky rozdělených do kapitol dle jednotlivých §§ trestního zákoníku. Na případech bude konkrétně zkoumána daná právní kvalifikace a další trestněprávní a tresněprocesní instituty a vztahy.

Trestní právo představuje svébytné právní odvětví v právním systému České republiky, nikoliv však jediné. Pro účely této práce jsou ale právo civilní, občanské, a jeho nástroje, stejně tak jako veřejnoprávních postih správního práva atp., ponechány stranou a nejsou předmětem této práce.

Práce si klade za cíl poskytnout komplexní přehled kybernetické kriminality, zejména s ohledem na zařízení informačních a komunikačních technologií, v republice. Hlavním záměrem je podrobně prozkoumat kybernetické trestné činy, se zaměřením na vybrané případy, které budou podrobně rozebrány v rámci případové studie. Důraz bude kladen na analýzu trestních rozhodnutí soudů v těchto

konkrétních případech, což by mělo přinést bližší vhled do stíhání kybernetické kriminality v České republice.

Celkovým cílem práce není pouze poskytnout vhled do kybernetické kriminality v České republice, ale také přispět k diskusi o možnostech novelizace právních norem, kvalifikace jednání obviněných jako kybernetické kriminality a ukládání trestů za ně. Práce by měla přinést nejen teoretický vhled, ale i praktické poznatky a doporučení, které mohou být relevantní pro odbornou veřejnost zabývající se danou problematikou. V praktické části budou také stanoveny konkrétní výzkumné otázky, na které bude po provedení rozborů rozhodnutí odpovězeno.

V době globalizace, nových technologií a neustálého vývoje kybernetických hrozeb je takový pohled nezbytný pro pochopení a efektivní boj proti této moderní formě kriminality.

## *2.2 Metodika*

Tato kapitola popisuje metodiku výzkumu, kterou autor zvolil pro dosažení stanovených cílů bakalářské práce. Metodika je klíčovým prvkem výzkumu, neboť poskytuje strukturu a návod, jak sbírat, analyzovat a interpretovat data. Tato práce kombinuje prvky deskripce a případové studie.

Deskriptivní přístup bude využit k poskytnutí přehledu o kybernetické kriminalitě v České republice zejména v první části práce. V teoretické části bylo užito několik výzkumných metod. Provedena byla analýza konkrétních legislativních dokumentů a jejich shrnutí, rozsáhlá literární rešerše, a to jak právních norem, tak i doktrinálních a jiných sekundárních zdrojů. V případě analýzy právních norem bylo užito metod interpretace práva, a to jak metod standardních, tak i nadstandardních (viz dále).

Interpretace práva je postup, jehož cílem je přispět k pochopení, porozumění a vysvětlení obsahu právních norem. Výklad práva je důležitým nástrojem právního systému a je nezbytný pro proces aplikace práva, kde zajišťuje účinné vymáhání právních norem v zákonodárcem předvídaných situacích – jednoduchých případech, ale při použitích tzv. „nadstandardních“ interpretačních metod pomáhá

řešit i složité, obtížné, sporné a nejasné situace a problémy – tzv. „*hard cases*“ [1 s. 115–122].

Interpretace práva může být také dělena, co do svého významu a dle autora, který jej provádí. Pro využití v této práci jsou dle Knappova dělení [2 s. 169–170] podstatné výklady soudní a doktrinální.

V případě soudního výkladu jsou rozlišovány dvě formy. První formou je výklad vrcholových soudů sloužících ke sjednocení judikatury a rozhodovací praxe soudů. Tyto stanoviska nejsou přímo právně závazná, ale utvářejí výklad práva mírou své přesvědčivosti, argumentace a autority soudu. Druhá forma jsou soudní rozhodnutí ve věci samé, které působí mezi účastníky řízení a jsou pro ně závazná bez dalšího.

Doktrinální výklad je tvořen právní vědou a obvykle má velkou váhu při tvorbě obecného právního názoru autoritativních subjektů pohybující se v právním systému a jejich interpretace práva. Tento výklad je většinou podáván předními právními osobnostmi a mohou jím být typicky právě právní komentáře a články.

K dosažení porozumění obsahu právního textu se využívají různé metody interpretace. Tyto metody představují metodologické direktivy pro výklad práva a obvykle se v kontinentálním právním kontextu rozdělují na standardní a nadstandardní. Mezi standardní metody patří jazykový, logický a systematický výklad, zatímco mezi nadstandardními nalezneme historický, teleologický a komparativní výklad [k tomu více např. 3 s. 134–135].

Další metoda zahrnuje literární rešerši týkající se kybernetické kriminality, právní úpravy, doktrinálních a jiných sekundárních zdrojů. Cílem je získat hluboký teoretický základ a pochopení aktuálního stavu dané problematiky.

Dalším krokem bude analýza právních dokumentů, zejména trestních rozhodnutí soudů v případech kybernetické kriminality. Tato analýza bude prováděna s cílem zhodnotit postih pachatelů a přístup soudů k těmto případům.

V praktické části budou autorem provedeny rozbory vybraných případů kybernetické kriminality. Bude se zaměřovat na konkrétní činy, vyhodnocovat způsoby útoků a analyzovat soudní rozhodnutí.

Případová studie je specifickou metodou kvalitativního výzkumu, kdy je podrobně analyzován jeden nebo více případů [4] za účelem užití získaných poznatků při dalších diskusích a úvahách.

Při tvorbě případové studie bylo užito jak deskriptivního výzkumného přístupu, tak i holistického [5]. Případová studie je tzv. popisnou případovou studií, která se zabývá popisem procesu právní kvalifikace a interpretace jednotlivých ustanovení právních norem, v tomto případě pak tedy odůvodněními soudů v dané trestní věci [6 s. 54].

Případy kybernetické kriminality budou vybírány na základě jejich relevance k předmětným ustanovení trestního zákoníku a v rámci cílů této práce. Důraz bude kladen na různorodost případů, aby bylo možné získat co nejkomplexnější pohled na kybernetickou kriminalitu v České republice, ale demonstrovány budou i opakující se a podobné znaky jednotlivých případů

Pro kvantitativní analýzu dat budou využity statistické výstupy soudních a policejních dat a popisy trendů a vzorů v kybernetické kriminalitě. Pro kvalitativní analýzu, zejména při studiu případů, bude použita obsahová analýza k identifikaci klíčových témat a vzorců.

Při psaní této práce je vycházeno z platné právní úpravy ke dni 1. 10. 2023.

# 3 Trestní právo v kyberprostoru

V této kapitole se bude vypořádáno s otázkou definice některých důležitých pojmů, se kterými bude dále pracováno. Práce si neklade za cíl zcela přesně (precizně) vymezit následující termíny, ale poskytnout přesvědčivou a relevantní formulaci, která zachytí hlavní pojmové znaky a vlastnosti a vystavět základní rámec, ve kterém s nimi bude tato bakalářská práce dále pracovat a případně nabídne širší pohled na jednotlivé problémy, které jsou s nimi spjaty nebo které je provází.

## *3.1 Kyberprostor*

Pojem kybernetického prostoru, kyberprostoru (z anglického *cyberspace*), poprvé použil americko-kanadský kyberpunkový spisovatel William Gibson, který v jedné ze svých kratších vědeckofantastických povídek „*Burning Chrome*“ v roce 1982 užívá označení maticového simulačního systému „*Ono-Sendai Cyberspace VII*“ (neboli *Cyberspace Seven*) [7]. V samotné příběhu je toto jediné místo, kde se termín vyskytuje, a proto je pro rozšíření pojmu zásadnější vydání jeho světoznámého románu „Neuromancer“ o dva roky později, v roce 1984, kdy vešel pojem *cyberspace* v širokou známost, uchytil se a vyvolal v mnohých technicích touhy po vytvoření takového prostředí.

*„Konsenzuální halucinace prožívaná denně miliardami legitimních operátorů, v každém národě, dětmi, které se učí matematickým pojmům... grafické zobrazení dat abstrahovaných z pamětí každého počítače v lidské společnosti. Nepředstavitelná komplexita. Linie světla rozprostírající se v neprostoru mysli, klastry a konstelace dat. Jako světla velkoměsta, vzdalující se..." [8]*

Gibsonova představa o kyberprostoru se však od dnešní podoby a chápání značně liší a je spíše metaforickým pojetím autorovy představy, které však dalo základ vývoji tohoto označení v dalších desítkách let a je, dle mého názoru, stále věrným zachycením samotné podstaty, autorovy doby a vyjádřením až s filosofickými přesahy do 21. století.

Dnešní definice kybernetického prostoru je samozřejmě mnohem techničtější a s přihlédnutím k technologiím a možnostem současného světa i poměrně široká.

*„Kyberprostor je globální a vyvíjející se doména popisovaná užíváním elektrických sítí a elektromagnetického spektra, jejíž smysl je vytvářet, uchovávat, upravovat, vyměňovat, sdílet, vybírat, používat či vymazávat informace. Kyberprostor zahrnuje: a) fyzická i telekomunikační zařízení, která umožňují spojení technologií a komunikaci sítí systému, chápáno obecně (SCADA zařízení, smartphony/tablety, počítače, servery, atd..), b) počítačové systémy a komplementární software, který zaručuje spojení a funkčnost systému, c) spojení počítačových sítí, d) uživatelské vstupy a uzly zprostředkovatelů spojení, e) informace – uživatelská data.“ [9]*

Tato formulace patří v současnosti k jedné z nejcitovanějším a vyčerpávajícím způsobem vymezuje kyberprostor z mnoha hledisek.

Další velmi významnou definici lze nalézt v normách Mezinárodní organizace pro normalizaci (ISO), která je narozdíl od předchozí mnohem jednodušší a srozumitelnější, a to přitom s ponecháním vlastnosti velmi dobré použitelnosti v praxi.

*„komplexní prostředí, které je výsledkem interakce lidí, softwaru a služeb na internetu prostřednictvím technologických zařízení a sítí k němu připojených a které neexistuje v žádné fyzické podobě“ [10 sek. 4.21]*

V této práci bude tedy primárně vycházeno z této definice, která je plně dostačující, kdy faktické vymezení kyberprostoru nebude ve většině případů hlavním ohniskem zkoumané materie. Klíčovým pojmem souvisejícím s kyberprostorem je také Internet, kterým se rozumí celosvětový systém počítačových sítí, které jsou vzájemně propojeny a které slouží k výměně dat (někdy bývá označován jako „síť sítí“) [11 s. 47]. Internet je hlavní platformou naprosté většiny interakcí v kyberprostoru.

Aplikace práva v kyberprostoru s sebou přináší mnohá úskalí (např. určení rozhodného práva nebo jurisdikce, relativně vysoká míra anonymity uživatelů,

identifikace pachatele trestné činnosti, odhalování trestné činnosti jako takové, problematika platnosti právních jednání a zajištění důkazních prostředků jak pro civilní, tak trestní proces a mnohé další), které často vycházejí z tradiční právní úpravy, která zcela přirozeně nepružně reaguje na nové trendy a extrémně dynamický vývoj v odvětvích jako jsou informační a komunikační technologie.

Kromě kybernetické trestné činnosti je kybernetický prostor důležitým aspektem také v kybernetické bezpečnosti a mezinárodních konfliktech, kdy představuje novou linii vedení války a bojů - tzv. hybridní válku, ale samozřejmě i každodenních právních jednání právních subjektů, pracovních a studijních povinností, trávení volného času nebo komunikaci s rodinou a přáteli.

## 3.2 ICT zařízení

S novelou trestního zákoníku zákonem č. 130/2022 Sb.[1] byl přidán do výkladových ustanovení nový § 136a, který v návaznosti na implementaci směrnic Evropského parlamentu a Rady o útocích na informační systémy[2] definuje počítačový systém takto:

*„Počítačovým systémem se rozumí zařízení anebo skupina vzájemně propojených nebo přidružených zařízení, z nichž jedno nebo více provádí na základě programu automatické zpracování dat. Počítačovým systémem se rozumí i data uložená, zpracovaná, opětovně vyhledaná nebo přenesená tímto zařízením anebo skupinou zařízení za účelem jeho nebo jejich provozu, použití, ochrany a údržby.“* [3]

Na tuto definici lze pohlížet jako na vysoce formální, kdy se snaží velmi normativně zachytit velmi pestrou škálu hardwarového a softwarového vybavení nejenom počítače, jejich vztah a provázanost a funkcionalitu do jednoho celku. V kontextu této definice je užito dokonce i právní fikce, a to ve větě druhé, kdy jsou

[1] Zákon č. 130/2022 Sb. kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, zákon č. 45/2013 Sb., o obětech trestných činů a o změně některých zákonů (zákon o obětech trestných činů), ve znění pozdějších předpisů, a některé další zákony
[2] Směrnice Evropského parlamentu a Rady 2013/40/EU ze dne 12. srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV
[3] Zákon č. 40/2009 Sb., trestní zákoník

za počítačový systém vydávána i určitá data. Tento přístup je předmětem drobné kritiky některých odborníků, kdy je viděn jako poměrně násilný pokus o vymezení něčeho s čím praxe už dlouho dobu pracovala a užívala jako notorietu [12 s. 26].

Autorem zvolený název ICT zařízení je reflexí nepřeberného množství přístrojů a jejich součástí, které mohou plnit funkce počítače, tak jak si jej běžný uživatel představí. Zařízením ICT tedy bude cokoliv, co je schopno provést naprogramovaný seznam instrukcí, reagovat na vnější pokyny, pracovat s daty a zpravidla komunikovat pomocí vstupních a výstupních zařízení. Do této kategorie tedy demonstrativně spadá vše od běžného stolního počítače, přes servery, složité stroje jako letadla, automobily až po nejdrobnější domácí spotřebiče jako jsou lednice, kávovary, televize, zařízení *IoT*[4] atp. [12 s. 35; 13 s. 2016; 14 sek. abstract]. Může jít jak o samostatnou funkční jednotku, nebo o soubor několika vzájemně propojených jednotek (počítačová síť) a *de facto* i o Internet jako takový, který je velmi komplexní počítačovou sítí, respektive počítačovým systémem [13 s. 58].

## 3.3 Pojem a předmět kybernetické kriminality

Pro pochopení problematiky kybernetické kriminality, které se tato práce věnuje, je v prvé řadě důležité si vymezit pojem a předmět kybernetické kriminality.

Vymezení kybernetické kriminality nelze považovat za lehký úkol s jednoznačným závěrem. Autoři mnoha publikací, ale i zákonodárce při tvorbě různých právních norem často užívají mnohá označení a často také chápou rozdílně obsahovou složku těchto pojmů.

První pojmovým znakem, který je třeba ozřejmit je kriminalita samotná. Co se tedy kriminalitou rozumí? Odpovědí na tuto otázku pro účely této práce budiž definice z trestněprávní perspektivy kriminologie tedy, že jde o *„souhrn všech jednání, která lze podřadit pod některou skutkovou podstatu, upravenou trestním zákonem.“* [15 s. 21–22]. Tato definice je pro svoji výstižnost a jednoduchost vhodná právě i pro oblast trestných činů v prostředí informačních a komunikačních technologií.

[4] Internet of Things, překl. internet věcí

Zdánlivě synonymní označení jako počítačová kriminalita, počítačová trestná činnost (*cybercrime*), *computer-related-crime*, kybernetická trestná činnost a další svědčí o komplikovanosti samotného, přesného, označení a jeho poměrně velmi dynamickém vývoji.

Dobrým příkladem pojmové nejasnosti je např. Smejkalova poznámka v úvodu jeho monografie [12 s. 21], kdy popisuje spor s vydavatelem o pojmenování této publikace, tj. jestli má být použito výrazu „kybernetická kriminalita" nebo „počítačová kriminalita". K tomuto se hodí poznamenat, že i Smejkal, který patří mezi zakladatele oborů počítačové právo a kybernetická kriminalistika v České republice, ve své knize v roce 1995 píše stále o kriminalitě počítačové [16 s. 99]. V tomto ohledu lze tedy sledovat vývoj označení tohoto fenoménu a nutnou reakci na vývoj nových technologií i v kontextu jednoho autora.

V dnešní době, kdy je možné si pod slovem počítač představit různě širokou množinu zařízení [blíže např. 13 s. 32], jsou však pravděpodobně nejpřesnější a nepřesvědčivější označení jako kybernetická kriminalita [12], kybernetická trestná činnost [13] nebo v zahraničních zdrojích *cybercrime* [17, 18], které na rozdíl od označení s různými adjektivy odvozenými od počítače zachycují přesněji povahu a prostor, kde je tato kriminalita páchána, tedy kyberprostor.

Na vývoj samotného označení bezprostředně navazuje i další problematika pokusu o definici kybernetické kriminality, a to totiž otázka vlastního obsahu a předmětu.

Jak již bylo nastíněno v úvodu této kapitoly, existuje mnoho různých definic kyberkriminality a vymezení obsahu a předmětu, které toto jednání zahrnuje. Pro účely této práce bude proveden letmý exkurs názory různých autorů a institucí a na tomto základě bude stanoven rámec, ve kterém se práce bude pohybovat.

Profesor univerzity v Cambridge Johnathan Clough přidává k výčtu synonymních pojmů, které již zde byly zmiňovány taky pojem „*high technology*" *crime*, který reaguje na stále se rozvíjející a všeprostupující digitální technologie, když dále pokračuje v úvaze o nejpřiléhavějším označení [18 s. 9–10]. Jedním z možných dělení, na kterém dle Clougha panuje shoda je rozdělení kyberkriminality na „*cyber-dependent*" a „*cyber-enabled*". „*Cyber-dependent*" (nebo také tzv. „*true cyber crimes*") jsou takové trestné činy,

které lze spáchat pouze za využití ICT zařízení a kde je taková technologie obvykle předmětem tohoto trestného činu. Trestnými činy tzv. „*cyber-enabled*“ se potom rozumí, „tradiční“ trestné činy k jejichž spáchání bylo použito zařízení ICT. Jako příklad je uváděno šíření a výroba dětské pornografie, nebezpečné pronásledování, porušení autorského práva nebo podvod – zde je hlavním rozlišovacím znakem fakt, že tyto trestné činy mohou být spáchány i bez využití informačních technologií [18 s. 11; shodně také 19 s. 542].

Starší vymezení z českého prostředí, rozděluje kyberkriminalitu (resp. kyberzločiny) do třech kategorií.

Prvními jsou „trestné činy ohrožující ICT“ [20 s. 35], tedy trestný čin proti integritě ICT zařízení často označován jako kybernetický trestný čin v úzkém pojetí, dále „trestné činy využívající ICT ke spáchání tradičních trestných činů“ [20 s. 35] a „trestné činy vztahující se k obsahu počítačových dat“ [20 s. 35].

Naopak velmi širokou a pro účely této práce obtížně uchopitelnou definici poskytuje oficiální Výkladový slovník kybernetické bezpečnosti vydávaný pod záštitou Národního bezpečnostního úřadu a Národního centra kybernetické bezpečnosti, který pod kybernetickou kriminalitu zahrnuje všechny služby nebo aplikace, které jsou v kyberprostoru cílem nebo nástrojem trestněprávního jednání nebo kdy je kyberprostor jako takový zdrojem, nástrojem, předmětem nebo místem spáchání trestného činu [21 s. 98].

Tato práce bude pracovat s pojmem kybernetické kriminality v jejím úzkém pojetí, tzn. že se bude zaměřovat na trestné činy proti zařízením ICT, tedy zejména §§ 230, 231 a 232 trestního zákoníku, které zákonodárce označuje jako „počítačové trestné činy“. Jde tedy o „ryze počítačové“ [12 s. 637] trestné činy, kde *„figuruje určitým způsobem počítač jako souhrn technického a programového vybavení včetně dat, nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě“* [12 s. 33] a to *„a) jako předmět této trestné činnosti, ovšem s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité“* [12 s. 33]. Podobně, avšak trochu více schematicky, vymezuje kyberkriminalitu i Kolouch [13 s. 34], dále, co se zahraniční doktríny týče, tomuto označení odpovídá i již zmiňovaný pojem *cyber-dependent*

*crime* a v neposlední řadě lze shrnout, že ve stejném smyslu jej nalézáme i v rozhodnutí Rady Evropské unie[5] či ve veřejných materiálech Policie ČR [22].

Problematika kybernetické kriminality se nevyčerpává pouze veřejnoprávním odvětvím práva trestního, ale je úzce provázána na další oblasti práva, zejména práva ICT (právo informačních a komunikačních technologií), kde jde zejména o odpovědnost poskytovatelů internetových služeb (tzv. ISP[6]), resp. poskytovatelů služeb informační společnosti[7], spolupráci ISP při zajišťování elektronických důkazů a jejich případná trestní spoluodpovědnost či oblast správního práva v otázkách kybernetické bezpečnosti [19 s. 543]. Těmito oblastmi práva jako takovými se tato práce více nezabývá.

# 4 Prameny právní úpravy

## *4.1 Mezinárodní dokumenty a právní úprava Evropské unie*

Tato kapitola si klade za cíl poskytnout základní pohled na mezinárodní a evropskou reakci na kybernetickou kriminalitu a přiblížit čtenáři klíčové právní dokumenty a normy v boji proti těmto novým formám hrozeb v digitálním prostoru.

V době rychlé globalizace, digitalizace a vzrůstající závislosti na informačních technologiích čelí společnost novým výzvám spojeným s kybernetickou kriminalitou. Bezpečnostní hrozby v kyberprostoru neznají hranice států a vyžadují proto globální spolupráci a komplexní právní úpravu. Tato kapitola se zaměřuje na analýzu mezinárodních dokumentů a právních předpisů i východisek Evropské unie, které reagují na narůstající problémy kybernetické kriminality.

V první části je věnována pozornost úsilí Organizace spojených národů (OSN) o úpravu trestněprávních aspektů kybernetické kriminality. Od historického Manuálu OSN pro prevenci a kontrolu počítačového zločinu v roce 1994 až po současné snahy o mezinárodní regulaci.

---

[5] Rámcové rozhodnutí Rady 2005/222/SVV ze dne 24. února 2005 o útocích proti informačním systémům, které je Rámcové rozhodnutí Rady 2005/222/SVV ze dne 24. února 2005 o útocích proti informačním systémům

[6] angl. *internet service provider*

[7] Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti)

Dále se kapitola zevrubně zaobírá „Úmluvou o kybernetické kriminalitě" přijatou Radou Evropy, která představuje komplexní úpravu s cílem sjednotit národní legislativu v oblasti kyberkriminality. Důraz klade na implementaci nástrojů pro postih trestných činů v kyberprostoru a zajištění efektivní mezinárodní spolupráce.

Poslední část se zaměřuje na právní rámec Evropské unie, která reaguje na výzvy kybernetické kriminality prostřednictvím směrnic, nařízení, rámcových rozhodnutí a judikatury Soudního dvora Evropské unie. S ohledem na Strategii kybernetické bezpečnosti a klíčové dokumenty, jako je směrnice Evropského parlamentu a Rady „o útocích na informační systémy". Evropská unie aktivně usiluje o harmonizaci trestních normativů a posílení ochrany informačních systémů.

### 4.1.1 OSN

Snahy o zakotvení základních trestněprávních aspektů kyberkriminality v rámci platformy Organizace spojených národů se objevují na poli mezinárodního práva mezi prvními. Jedním z prvních pokusů o regulaci v reakci na první velké kybernetické zločiny a útoky v roce 1986 (i v reakci na vytvoření prvních osobních počítačů Apple Mac) vydání Manuálu OSN pro prevenci a kontrolu počítačového zločinu v roce 1994.

V současnosti však v rámci OSN nevznikla žádná mezinárodní úmluva, která by se konkrétně týkala kybernetické kriminality, a to i přes poměrně velkou snahu některých států. V dopisu generálnímu tajemníkovi OSN ze září 2011 se Ruská federace společně Čínou, Tádžikistánem a Uzbekistánem navrhují přijetí „Mezinárodních pravidel chování v kyberprostoru" [23 s. 3]. Problematika kybernetické bezpečnosti a kriminality spadá do kompetence Mezinárodní telekomunikační unie při OSN, která vypracovala rámcový dokument „*Global Cybersecurity Agenda"*.

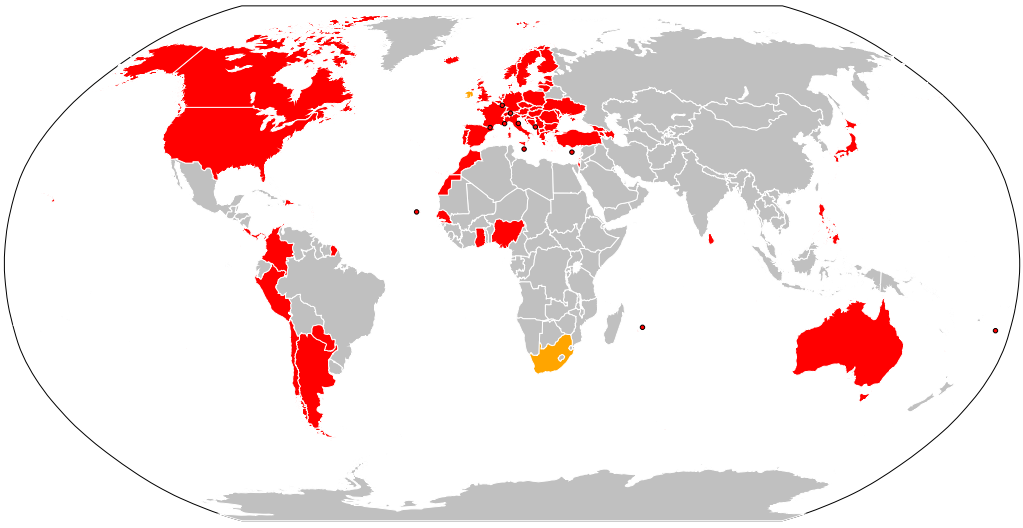
### 4.1.2 Úmluva o kybernetické kriminalitě

Za jednu z prvních komplexních úprav a úmluv o kybernetické kriminalitě v mezinárodním prostoru je považována „Úmluva o kybernetické kriminalitě" (anglicky „*Convention on Cybercrime"*), kterou jsem již zmínil. Byla přijata Radou

Evropy pod číslem 185 v listopadu 2001 v Budapešti. Ratifikační proces této úmluvy je však velmi pomalý a řada státu ji stále neratifikovala. Česká republika ratifikovala tuto úmluvu až v roce 2013[8].

Hlavním cílem a smyslem Úmluvy o kybernetické kriminalitě je sjednocení (harmonizace) dosud roztříštěných národních právních úprav v této oblasti [20 s. 162]. K tomuto Úmluva stanoví signovaným subjektům povinnost implementovat do svých právních úprav příslušné nástroje k možnému postihnu tohoto druhu kriminality. Text Úmluvy se snaží důkladně (a jednotně) vymezit skutkové podstaty kybernetických trestných činů pro provedení v národních řádech, kdy právě jednotnost úpravy je klíčem k efektivnímu vymáhání práva, zejména v naplnění požadavku oboustranné trestnosti, na mezinárodním poli, kdy je teritoriální působnost často rozprostřena po celém světě.

Kromě dalšího obsahuje Úmluva i požadavek na trestní odpovědnost právnických osob. Kromě otázek hmotného práva se dokument věnuje také úpravě společných postupů proti pachatelům kybernetické trestné činnosti v celosvětovém boji proti kyberzločinu – mezinárodní spolupráce, extradice apod. K Úmluvě k listopadu 2023 přistoupilo zatím 68 smluvních stran, a to i z řad států mimo Radu Evropy (např. Spojené státy americké, Austrálie, Japonsko nebo Kanada).



Obr. 1 Země, které ratifikovali Úmluvu o kybernetické kriminalitě.
Zdroj: PALOSIRKKA, *Wikimedia Commons* [24]

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

Další sjednocování a rozšiřování mezinárodní úpravy v oblasti kyberkriminality je prováděno pomocí dodatkových protokolů, které rozvíjí internetovou trestní jurisdikci a postupně se zaměřují na další specifické trestné činy a přestupky v kyberprostoru [25 s. 16].

Takovým je například Dodatkový protokol Rady Evropy č. 189 k Úmluvě o kybernetické kriminalitě, který se věnuje trestným činům v oblasti šíření závadného obsahu s rasistickým, xenofobní nebo jinak nesnášenlivým kontextem.

Závazky plynoucí pro Českou republiku z Úmluvy implementuje zákonodárce v příslušných předpisech vnitrostátního práva, v oblasti hmotného práva zejména v trestním zákoníku.

### 4.1.3 Právo Evropské unie

Evropská unie, která stojí na principech vzájemné spolupráce, která má být, pokud možno co nejefektivnější harmonizuje trestní normy v oblasti kybernetické kriminality samozřejmě také. Přijímané předpisy EU mají za cíl poskytnout podobnou míru ochrany daných objektů a umožnit větší efektivitu postihu daných protiprávních jednání. Hlavními nástroji k prosazování tohoto záměru jsou přirozeně směrnice, nařízení a rámcová rozhodnutí Evropské unie.

Politika a rámcová právní úprava kybernetického prostoru v Evropské unii vychází z dokumentu Strategie kybernetické bezpečnosti přijaté v roce 2013, která vyjadřuje mimo jiné závazek Evropské komise podporovat a zajišťovat spolupráci mezi Evropským centrem pro boj proti kyberkriminalitě a Europolem [26].

Ohnisko unijní právní úpravy leží především ve směrnici Evropského parlamentu a Rady „o útocích na informační systémy“. Cílem směrnice je sblížení trestněprávních ustanovení v jednotlivých členských státech a zlepšení vzájemné spolupráce i s výše zmíněnými agenturami, centry a jinými unijními institucemi. V rámci tohoto cíle poskytuje směrnice i implementační rámec pro výkladová ustanovení národního trestního práva.

Dalšími podstatnými dokumenty sekundárního práva Evropské unie jsou například rámcové rozhodnutí Rady 2000/375/JHA ze dne 29. 5. 2000 o boji proti dětské pornografii na internetu a směrnice 2000/31/EC ze dne 8. 6. 2000

o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu.

## 4.2 Česká právní úprava

Jak jsem již naznačil, hlavním prostorem, ve kterém se práce při zkoumání kybernetické kriminality pohybuje je přirozeně odvětví práva trestního. Při podání přehledu pramenů trestního práva je zde vycházeno z řazení dle právní síly.

Základní dělení právních norem je na normy ústavní, zákonné a podzákonné, které dohromady tvoří právní řád, který je jedním z předpokladům demokratického právního státu. Kritérium právní síly je klíčové pro správnou aplikaci právních norem, kdy platí, že norma nižší právní síly musí být v souladu (resp. nesmí odporovat) normě vyšší právní síly. Když tedy jdeme tzv. pyramidou právních předpisů směrem dolů musí být vždy vycházeno z výše postavených předpisů, a i při interpretaci nižších norem vždy zachován tento soulad [3 s. 49–51].

Prameny trestního práva v České republice tedy jsou: ústavní zákony - zejména Ústava České republiky[9], Listina základních práv a svobod[10], mezinárodní smlouvy dle čl. 10 Ústavy a další zákony (viz dále), amnestijní rozhodnutí prezidenta republiky a rozhodnutí Ústavního soudu normativní povahy.

Právní řád České republiky vychází ze základních zásad kontinentální právní kultury *nullum crimen, nulla poena sine lege*[11], tedy že trest je možno ukládat toliko a jen na základě zákona pro takové jednání, které je v něm vymezeno jako trestné a zásady subsidiarity trestní represe, kdy trestní právo je užívána jako prostředek ochrany práv až tehdy pokud jiné právní prostředky (typicky řízení ve věcech občanskoprávních nebo správní postih) jsou nevhodné nebo zjevně neúčinné, tedy jako tzv. prostředek *ultima ratio*.

Pramenem právní úpravy počítačové kriminality a jejího postihu může být tedy jen a pouze zákon – základním hmotně právním trestním předpisem je zákon

[9] Ústava České republiky, zákon č. 1/1993 Sb.
[10] Listina základních práv a svobod, republikována jako usnesení č. 2/1993 Sb.
[11] z lat. překl. žádný zločin, žádný trest bez zákona; viz § 12 odst. 1 trestního zákoníku, nález Ústavního soudu ČR sp. zn. II. ÚS 1152/17 a Listina základních práv a svobod čl. 39

č. 40/2009 Sb., („trestní zákoník“), v procesní rovině je to potom zákon č. 141/1961 Sb. o trestním řízením soudním („trestní řád“).

Nicméně existuje i celá řada dalších právních norem, které jsou pro danou problematiku relevantní.

Na sdíleném prvním místě je jistě vhodné uvést nejprve zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, který zakotvuje a blíže specifikuje trestní odpovědnost právnických osob, kde je kromě dalšího kruciální § 7 tohoto zákona, kde najdeme taxativní negativní výčet trestných činů, které mohou právnické osoby, při splnění dalších podmínek tohoto zákona, spáchat (velmi podstatnou novelou je zde zákon č. 183/2016 Sb., který nahradil původní pozitivní výčet trestných činů stávající podobou, kdy jsou zde pouze uvedeny výjimky trestných činů, které, většinou z povahy věci, nemůže právnická osoba spáchat). Druhým velmi důležitým zákonem je zákon č. 218/2003 Sb., o soudnictvích ve věcech mládeže, který upravuje řízení a postih ve věcech mládeže při spáchání provinění, trestného činu nebo činu jinak trestného.

Dále následuje pouhý nevyčerpávající výčet dalších předpisů: zákon č .121/2000 Sb., autorský zákon; zákon č. 441/2003 Sb., o ochranných známkách; zákon č. 14/1993 Sb., o opatřeních na ochranu průmyslového vlastnictví; zákon č. 527/1990 Sb., o vynálezech, průmyslových vzorech a zlepšovacích návrzích; zákon č. 127/2005 Sb., o elektronických komunikacích; zákon č. 480/2004 Sb., o některých službách informační společnosti; 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. 160/1999 Sb., o svobodném přístupu k informacím; zákon č. 181/2014 Sb., zákon o kybernetické bezpečnosti; zákon č. 89/2012 Sb., občanský zákoník; zákon č. 101/2000 Sb., o ochraně osobních údajů a zákon č. 273/2008 Sb., o Policii České republiky.

### 4.2.1 Trestní zákoník

Jak již bylo řečeno, zákon č. 40/2009 Sb., trestní zákoník je hlavním a nejdůležitějším hmotněprávním předpisem trestního práva. Trestní zákoník ve své obecné části kupříkladu stanovuje společná ustanovení, která jsou společná

všem trestným činům nebo, zejména ve výkladových ustanovení, vymezuje některé pojmy a znaky důležité pro některé trestné činy, dále upravuje například vznik a zánik trestní odpovědnosti, okolnosti vylučující protiprávnost, ukládání trestů a ochranných opatření, kdo je to pachatel, druhy trestných činů, působnosti trestního zákoníku a v neposlední řadě také základní zásady trestního práva.

V části zvláštní potom taxativně a katalogicky vymezuje jednotlivé trestné činy, které jsou dle objektu trestného činu, tj. společenského zájmů chráněných trestním právem rozděleny do 13 hlav a řazeny dle své společenské škodlivosti. Kybernetické trestné činy jsou řazeny v hlavě V. „Trestné činy proti majetku". Pro aplikaci a porozumění trestnímu zákoníku je třeba pracovat s obecnou i zvláštní částí dohromady a správně užívat propojovat jednotlivá ustanovení obou částí.

„Nový" trestní zákoník s účinností od 1. ledna 2010 přinesl oproti jeho předchůdci, trestnímu zákonu č. 140/1961 Sb. („starý trestní zákon") mnoho změn. Jedná se o výsledek rozsáhlého a náročného rekodifikačního procesu, který provázeli významné odborné diskuse nad jeho podobou. Trestní zákoník z roku 2009 opouští formálně-materiální princip a je vystaven na formálním principu s materiálními prvky (resp. materiálním korektivem), kdy je jednání považováno za trestné, pokud naplňuji všechny znaky skutkové podstaty (formální princip) a zároveň naplňuje určitou míru společenské škodlivosti (materiální prvek), kdy už nepostačí uplatnění ochrany práv jinými nástroji (zásada *ultima ratio*).

Trestní právo v České republice, na rozdíl od angloamerického právního systému, neuplatňuje sčítání trestů a pachatel je potrestán jen za ten nejzávažnější (viz § 43 odst. 1 trestního zákoníku).

Jen na okraj zde budou vymezeny znaky skutkové podstaty trestného činu, a to sice znaky obligatorní – objekt, objektivní stránka (jednání, následek a příčinná souvislost mezi jednáním a následkem), subjekt a subjektivní stránky (pachatel a vnitřní psychický stav pachatele k protiprávnímu jednání čili zavinění, které může být ve formě úmyslu, nebo nedbalosti[12]) a znaky fakultativní, které se mohou nebo

[12] Trestní zákoník vyžaduje k trestní odpovědnosti zavinění ve formě úmyslu, pokud nestanoví výslovně, že pro daný trestný čin postačuje nedbalost. To je stanoveno v § 13 odst. 2 trestního zákoníku.

nemusí vyskytovat nicméně jsou vyžadovány, v případě, když jsou vyjádřeny v konkrétní skutkové podstatě [K tomu více např. , 27].

Dále bude věnována pozornost změnám, které trestní zákoník přináší oproti nahrazenému trestnímu zákonu v oblasti kybernetické kriminality. První patrnou změnou je rozšíření úpravy kybernetických trestných činů, kdy oproti starému zákonu, který obsahoval takový trestný čin jeden, a sice „poškození a zneužití záznamu na nosiči informací“ dle § 257a, rozšiřuje škálu trestných činů na 3 paragrafová znění osahující 4 základní skutkové podstaty (§ 230 odst. 1 - „neoprávněný přístup k počítačovému systému“, § 230 odst. 2 - „neoprávněný zásah do počítačového systému“, § 231- „opatření a přechovávání přístupového zařízení a hesla“ a § 232 – „neoprávněný zásah do počítačového systému z nedbalosti“) [K tomu více 12 s. 640–645]. Zavedením nových skutkových podstat se výrazně zvýšila postižitelnost jednání pachatelů, kdy ve srovnání s aplikací § 257a starého trestního zákonu, kdy je uváděno, že v letech 1999-2004 bylo za tento trestný čin pravomocně odsouzeno 19 pachatelů, tak pro nové trestné činy je toto číslo, zejména díky § 230 trestního zákoníku v řádech stovek ročně [28 s. 308].

Druhou změnou, kterou přináší trestní zákoník č. 40/2009 Sb., je posun terminologie, kdy je místo výrazu „informace“ užíván termín „data“ [29].

Závěrem je zde uvedena novela trestního zákoníku zákonem č. 130/2022 Sb., která v oblasti kybernetické kriminality přináší změny jak v obecné části, kde ve výkladových ustanovení přidává již blíže rozebíraný § 136a, tak ve zvláštní části změnou znění textu § 230. Jednotlivé změny jsou zevrubněji probírány na konkrétních tematických místech této práce, kde jsou zmíněny, jsou dále vysvětlovány a je s nimi pracováno, s přihlédnutím k relativní čerstvosti této novely, zejména k překlenutí a aktualizaci původních závěrů před novou právní úpravou a v kontrastu k ní.

Trestní zákoník České republiky v oblasti kybernetické kriminality implementuje znění Úmluvy o kybernetické kriminalitě. Naplnění požadavků Úmluvy co do vlastního textu bývá však řadou odborníků kritizováno jako slepé přejímání, které je nekoncepční a zcela neodpovídá klasickým formulacím skutkových podstat v trestním zákoníku [28 s. 313].

### 4.2.2 Trestní řád

Zákon o trestním řízením soudním č. 141/1961 Sb., pro který se vžilo zkrácené označení „trestní řád“ je bazálním pramenem trestního práva procesního, který upravuje kromě jiného trestní řízení. Trestní řád, na rozdíl od trestního zákoníku, neprošel od svého přijetí v roce 1961 komplexním rekodifikačním procesem a patří tedy mezi jeden z nejdéle účinných zákonů v našem právním řádu. Přesto prošel zákon významnými novelizacemi souvisejícími zejména se změnou politického režimu v roce 1989, kdy bylo potřeba uzpůsobit jej potřebám nového právního státu postaveného na respektu k lidským právům jednotlivce a spravedlivém soudním procesu.

Trestní řád je ucelenou úpravou trestního práva procesního, který upravuje zejména základní zásady trestního řízení, práva a povinnosti osob zúčastněných na řízení, náležitosti úkonů v trestním řízení, postupy, povinnosti a práva při zajišťování osob a věcí, dokazování, vyšetřování a postupy orgánů činných v trestním řízení, práva a povinnosti osob proti kterým se řízení vede (a potrestání pachatelů), svědků, obhájců, tlumočníků, znalců a další důležité body a otázky. Systematicky je dělen do 5 částí.

# 5 Druhy kybernetické kriminality

V této kapitole je nahlíženo do rozmanitého světa trestné činnosti, která proniká do kyberprostoru – kybernetické kriminality. Cílem této kapitoly není systematické vymezení všech trestných činů spojených s kybernetickým prostředím, nýbrž se zaměřuje na klíčové aspekty, jež formují charakter této specifické formy kriminality, a to v rozsahu zejména §§ 230–232 trestního zákoníku. Zvolený přístup je pak zaměřen na podrobné vysvětlení vybraných fenoménů a problematik, které nejsou zdaleka vyčerpány, přičemž důraz je kladen na přiblížení celkové podstaty každého druhu kybernetické kriminality.

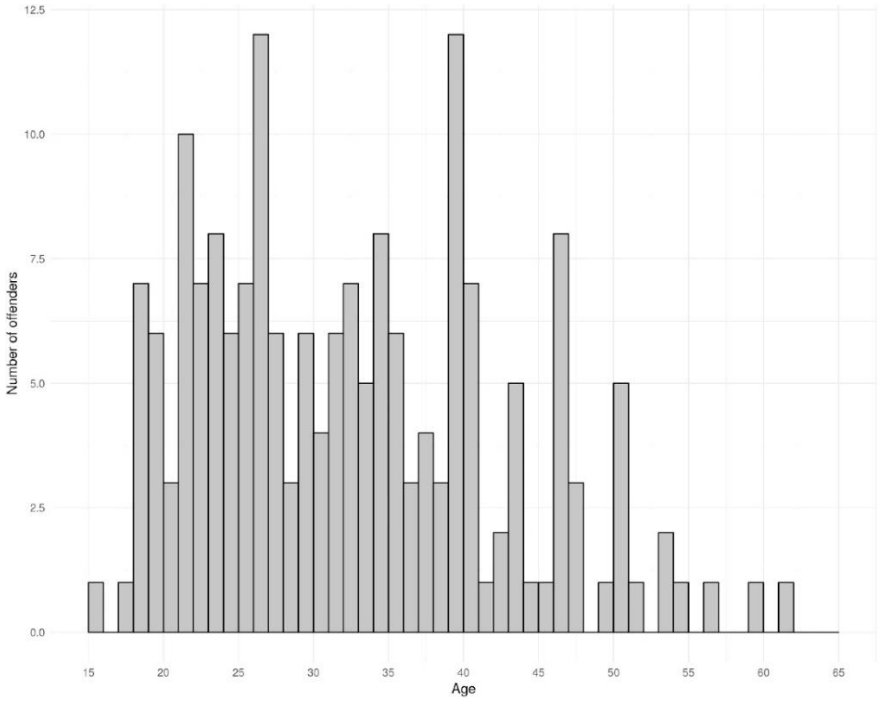
Kapitola se tak oprošťuje od klasického vymezení trestných činů postupně dle jednotlivých paragrafů a místo toho sleduje individuální pohled na vybraná jednání a fenomény. Zvolená struktura postavena na základě detailního rozebírání jednotlivých jevů, jako jsou DDoS útoky, hacking, malware a k doplnění i nedbalostní

§ 232 trestního zákoníku, s cílem poskytnout komplexní pohled na různé formy kybernetické trestné činnosti. Některé analyzované jevy se vzájemně prolínají a v praxi se spolu často vyskytují a souvisí.

Z dělení podle objektu trestných činů hlavy V. (Trestné činy proti majetku) trestního zákoníku řadíme počítačové trestné činy mezi tzv. poškozovací trestné činy [27 s. 746]. Kromě majetku jsou u počítačových trestných činů vymezených v §§ 230–232 trestního zákoníku chráněny i další zájmy jako ochrana počítačového systému a dat před neoprávněnými přístupy [27 s. 787–788]. Kromě hmotných věcí (hardware) je ale chráněn i nehmotný obsah a zprostředkovaně i další právní statky jako autorská díla, soukromí osob, osobní údaje, obchodní tajemství a další.

Předtím, než budou více rozebrány jednotlivé trestněprávní fenomény hodí se poznamenat několik závěrů v obecné rovině.

Analýza případů z let 2008–2016 provedená v České republice [30] ukazuje vysokou míru latence kybernetických trestných činů, kdy za sledované období byl odsouzen pouze zlomek pachatelů (konkrétně 229). Z analýzy také vyplývá, že věkové rozložení pachatelů kybernetické kriminality se překvapivě nikterak neliší od pachatelů jiných druhů trestné činnosti.




Graf. 2 Věkové rozložení pachatelů kybernetické kriminality.
Zdroj: GŘIVNA, DRÁPAL, *Attacks on the confidentiality, integrity and availability of data and computer systems in the criminal case law of the Czech Republic* [30]

V souvislosti s vysokou mírou latence vyplynula také významná potřeba výrazně zlepšit efektivitu odhalování a vyšetřování těchto trestných činů a orgány činné v trestném řízení by měli být schopny lépe a efektivněji zachycovat a vyšetřovat tyto útoky.

## 5.1 DoS, DDoS, Botnet

Útoky pachatelů v kyberprostoru jejichž cílem je znemožnění přístupu k internetovým službám, omezení nebo zabránění provozu na informační a komunikační infrastruktuře jsou v různé míře intenzity každodenním problémem mnoha poskytovatelů a provozovatelů těchto služeb. Jednání sledující tyto cíle se nazývá DoS (*Denial of Services*[13]) a jehož zvláštním druhem je DDoS (*Distributed Denial of Services*[14]) a jeho častým cílem jsou webové servery v síti Internet.

V případě DDoS je využíváno tzv. botnetů, které pomocí kontroly jednotlivých „*zombies*" (botů) – zařízeních zapojený do takové sítě, provádí činnost dle příkazů správce [13 s. 193] – útočníka (anglicky *bot herder)*. Útoky pomocí botnetů bývají také nabízeny jako tzv. *crime-as-a-service* [31], kdy objednavatel poptává využití již vytvořeného botnetu (většinou pomocí malwarem infikovaných ICT zařízení) k vlastnímu útoku případně je nabízeno i využití botnetu jako nástroje pro běh vlastního „zatěžujícího" skriptu nebo pouze specifikace požadavku takového útoku (*„script kiddies"*) [12 s. 923].

Typově mohou být infikovaná zařízení opravdu rozmanitá což znovu podtrhuje problematické pojmové vymezení celé kybernetické kriminality, tak jak se s ním bylo vypořádáno v přechozích kapitolách, jako netradiční a až poněkud „humorný" může být uveden případ z roku 2014, kdy malwarem infikovaná chytrá lednice vybavena TCP/IP konektivitou zapojena do rozsáhlého botnetu rozeslala před 750 000 emailů [32, 33].

Mechanismem tohoto druhu útoků je zasílání požadavků (*requests*) serveru poskytujícího nějakou službu nebo infrastruktuře ICT v takové míře a intenzitě, že dojde k jeho zahlcení, kdy přestává standardně fungovat a může docházet

[13] Překl. odepření služeb
[14] Překl. distribuované odepření služeb

k prodloužení odezvy, pomalému zpracovávání dat a dalších požadavků nebo až k úplnému znefunkčnění celé služby – server tzv. „spadne“. Dalším specifikem tohoto druhu útoků je fakt, že jeho cíl zůstává nepoškozen, tedy že po opadnutí zátěže vyvolané útočníkem může systém fungovat dále. Ne vždy je ale systém schopen se z takového útoku zotavit sám a je třeba dalších zásahů.

Z hlediska právního vymezení DoS/DDOS útoků je třeba primárně vycházet z toho, jakou technikou byl útok proveden a *de facto* jaká byla celá geneze takového útoku. Pro důslednou, a hlavně také účinnou kvalifikaci (viz dále) je třeba rozdělit DDoS jednání na několik fází. Zde je vycházeno z předpokladu jakéhosi komplexně vybaveného útočníka.

Prvním krokem pro zahájení DDoS útoku je vytvoření samotného botnetu. Nejčastěji bude tato fáze záležet v distribuci a instalaci malware k ovládaní daného ICT zařízení. Toto jednání je možné podřadit pod § 230 trestního zákoníku („Neoprávněný přístup k počítačovému systému“) odst. 2 písm. d) a dále dle okolností připadají v úvahu kvalifikované skutkové podstaty dle odst. 3 - zde v písm. a) zejména v podobě úmyslu způsobit újmu[15] nebo získat prospěch, a dále lze sledovat podobnou optikou odst. 4 a 5, které cílí na intenzivnější projevy tohoto skutku ať už do rozsahu (škody, prospěchu apod.), tak způsobu spáchání např. v organizované skupině. Dále je vhodným poznatkem, jak uvádí Kolouch, i aplikace § 207 odst. 1 alinea 1 trestního zákoníku (Neoprávněné užívání cizí věci), který by mohl být naplněn, ale zároveň zde poukazuje na velice nepravděpodobné využití téhož ustanovení v alinee 2, kdy opět nedochází ke vzniku právně relevantní škody [13 s. 204]. Toliko by bylo relativně přesvědčivě právně kvalifikováno jednání pachatele směřující k vytvoření botnetu kompromitací zombie zařízení.

Praktické problémy však způsobuje kvalifikace DoS jednání, které spočívá v zasílání velkého množství požadavků na službu (např. webový server) jako trestného. V následujících odstavcích jsou stručně představeny dosavadní poznatky

[15] Problematika škody je v tomto případě složitější a k širší diskusi. Ze samotné podstaty DoS útoku nelze vyvozovat úmysl způsobit škodu (ať už na zařízení, které slouží jako článek botnetu tak na cílovém serveru) naopak na cílech útoku není zpravidla způsobena žádná (trvalá) škoda. [k tomu blíže 44 s. 317]

doktríny a komentářové literatury, které dobře ilustrují velký interpretační prostor dotčených právních norem a názory různých autorů.

Navzdory Kolouchově dosavadnímu podrobnému rozboru se zdá, že jeho přístup k právní kvalifikaci DoS v současném kontextu zůstává spíše zdrženlivý a omezuje se hlavně na první fázi, tak jak bylo popsáno výše a dodává jenom zamyšlení úvahy „podle budoucího zákona“[16] k § 230 odst. 3 trestního zákoníku, kde by mohla být doplněna nová okolnost a to sice: *„úmyslně připojí počítačový systém do počítačové sítě s úmyslem spáchat trestný čin, či jej v této síti se stejným úmyslem užije.“* [13 s. 204], která by jistě pokrývala dané jednání.

Smejkal již v první části své analýzy vylučuje užití § 231(„opatření a přechovávání přístupového zařízení a hesla“) trestního zákoníku z důvodu nepřijatelnosti analogie v neprospěch pachatele[17] v trestním právu [K tomu více např. 35 s. 54] v dané situaci. Dále se věnuje aplikaci ustanovení § 230 trestního zákoníku zejména v odst. 2 a 3 ve znění, kdy je dle jeho názoru výkladem dojít k závěru, kdy by se jednalo o naplnění znaků skutkové podstaty trestného činu, je ale třeba vyčkat, jak se k tomuto problému postaví judikatura soudů [12 s. 932-933]. Interpretaci jednotlivých znaků těchto skutkových podstat je možné opřít i o názor z období přípravy nového trestního zákoníku a znění a smysl úpravy v Úmluvě Rady Evropy o kybernetické kriminalitě [12 s. 933]. Nejasnosti při subsumpci v § 230 („neoprávněný přístup k počítačovému systému a zásah do počítačového systému“) vedou i k úvahám o jiných trestných činech [K tomu blíže 12 s. 934], ale ty nejsou primárním předmětem zkoumání této práce.

Podobný názor, který svědčí o vážných pochybách při aplikaci § 230 zastává také Čep, který z logických důvodů vylučuje odst. 1 toho paragrafu, kdy není splněn již primární předpoklad této základní skutkové podstaty, a to překonání bezpečnostního opatření [34 s. 320–321]. Zároveň lze také jen stěží hovořit o neoprávněném přístupu ve formě zasílání zcela legitimních a *de facto* (jaký je jinak smysl webového serveru nabízejícího službu) žádoucích požadavků.

---

[16] lat. *de lege ferenda*
[17] lat. *in malam parte*

K potíže způsobujícímu znaku „získání přístupu“ ve vztahu k § 230 odst. 2 najdeme zmínky i v právních komentářích, které rozumějí tímto *„jednání, které umožní pachateli volnou dispozici s počítačovým systémem nebo nosičem informací a využití jeho informačního obsahu.“* [36]. Z tohoto vymezení je zřejmé, že takové míry toto jednání nedosahuje.

Další interpretační problémy pojmů jako „potlačí data“, „učiní data neupotřebitelnými“ nebo „neoprávnění vloží data“ Čep shrnuje, když píše až o možném vyvození trestní neodpovědnosti z důvodu nenaplnění těchto kvalifikačních znaků zmíněných skutkových podstat [34 s. 323; obdobně také 37].

Celkově považuji za nezbytné zmínit, že názory výše zmiňovaných autorů vychází z právní úpravy před účinností novely č. 130/2022 Sb., která ve vztahu k problematice § 230 mění kromě dalšího v odst. 2 slova „získá přístup…“ na „zasáhne do…“. Důvodová zpráva k této novele sice uvádí, že kromě dalšího je smyslem změny těchto slov i postih právě DoS a DDoS útoků [38], nicméně realita a praxe zůstávají stejné, tedy s velkým otazníkem a na výpovědní hodnotě se dle nové terminologie příliš nemění. Již při přípravě znění této novely někteří autoři vyjadřovali pochybnosti nad dostatečností úprav těchto skutkových podstat a jejich znakům, resp. jejich nedostatečností [12 s. 27; 34 s. 325–326]. Lze tedy shrnout, že naplnění skutkové podstaty § 230 odst. 2 v podobě DDoS útoku je setrvale obtížné a nejasné [12 s. 27] a je tedy stále velkou měrou otázka interpretace a posouzení daného soudce, jak bude v takovém případě rozhodovat – více bude tato materie rozebírána v praktické části.

## 5.2 Hacking

Pojem hacking zahrnuje mnoho nejrůznějších činností, ať už legálních nebo nelegálních. Společným znakem je vysoká technická znalost a schopnosti v oblasti informačních a komunikačních technologií a programování jednajícího – hackera. V této kapitole bude na problematiku hackingu pohlíženo převládající optikou vykreslovanou hromadnými sdělovacími prostředky veřejnosti, totiž jako na *„jakoukoliv činnost osoby směřující k získání nelegálního přístupu k cizímu systému či osobnímu počítači“* [13 s. 269].

Než budou více analyzovány trestně relevantní projevy hackingu bude ve stručnosti pojednáno také o různých, dalších, aspektech hackingu a druzích hackerů.

Nejprve je vhodné vyjasnit rozdíl mezi termínem *hacker* a *cracker*. Cracker je označení pro hackery ze skupiny tzv. Black Hats (viz níže), kteří pronikají do systémů s cílem způsobit škodu, neoprávněně získat informace nebo získat majetkový prospěch [13 s. 276]. Nejčastěji je cracking spojen s porušováním autorských práv ve vztahu k softwaru a jiných předmětů autorskoprávní ochrany, kde je většinou překonáván technický prostředek k jejich nelegálnímu užití nebo rozmnožování [39 s. 73]. Výrazy hacker a cracker však často splývají především v běžné řeči a vnímaní veřejnosti, a také někteří autoři příliš nelpí na rozlišení těchto označení, kdy se jedná v zásadě o podmnožinu hackerů. Toto rozlišení je spíše formalismem a často se větší rozlišení nachází spíše v hackerské komunitě, kdy hackeři (ve smyslu ICT odborníků) mají potřeba se vymezovat a jasně odlišit od jejich kolegů s nižší morální integritou [20 s. 38–43]. Pro účely této práce není nutné dbát striktního odlišení těchto dvou skupin, kdy je primární zaměření na pachatele trestné činnosti, a proto bude užíván pojem hacker v širokém slova smyslu.

Jak hackeři, tak crackeři mají obecně společný cíl spočívající v obstarání si neoprávněného přístupu do počítačového systému. V minulosti byla hlavním zdrojem motivace především zvědavost, jak systémy fungují a jak mohou být vylepšeny. Hranice zvědavosti a neoprávněného přístupu je však velmi tenká a často se tak hacking stával neetickým až trestným jednáním. Rozvoj organizovaného zločinu a rozmach kyberprostoru však do značné míry zúžily důvody hackování, a to velmi často na obstarávání majetkového či jiného prospěchu pro sebe nebo další osoby [17 s. 34–35].

Běžně používaným kritériem při dělení hackerů je důvod opatření přístupu k počítači nebo počítačovému systému. Tato kauza, která většinou určuje jejich motivace, způsoby přístupu a nakládání s daty nebo přístupy v rámci zařízení dává základy pro základní dělení do tří skupin[18]:

> 1) *White Hats* – někdy označování jako etičtí hackeři [40], získávají přístup do zařízení a systémů skrz jejich bezpečnostní slabiny a zranitelnosti, a to právě s cílem odhalit tyto bezpečnostní mezery. Odhalení takových zranitelností může být velmi cenné při vytvoření (opravě) opatření systému k prevenci „dalších" takových průniků.
>
> Těmito White Hat hackery jsou většinou vlastní zaměstnanci společnosti provozující tyto technologie nebo externí subjekty, které se na činnost penetračního testování zaměřují. Tyto subjekty, které zkouší odolnost zabezpečení systémů svým opatřením přístupu nezpůsobují újmu (zejména škodu) a nezneužívají dále tohoto přístupu [13 s. 273]. Většinou se průniky do systémů uskutečňují na základě předchozího souhlasu společnosti provozující dané zařízení, ale nejsou výjimečné i případy, kdy je tato činnost prováděna i bez takového souhlasu a tito hackeři následně pouze notifikují obchodní společnost o mezerách v jejich kybernetickém zabezpečením a jelikož nedochází k způsobení žádné újmy je obvykle toto oznámení, i po prvotním rozrušení a nedůvěře, kvitováno a kompenzováno finanční odměnou. V případě, kdy je prověřovací činnost probíhá na smluvním nebo jiném základě s předchozím souhlasem je nesporná legálnost takového jednání. Komplikovanější je posouzení v druhé zmiňované situaci, kdy se v zásadě jedná

[18] Jednotlivé skupiny hackerů jsou označovány anglickým výrazem odkazují na barvu jejich „klobouku" a obvykle nebývají překládány do češtiny. Odkazy na barvy, v uvedeném pořadí – bílá, černá, šedá, jsou referencí zejména na etický faktor jejich zásahu do systémů, kdy podobně jako v jiných odvětvích (např. „šedá ekonomika") označují „čistotu" (bílá barva) takového jednání.

o neoprávnění přístup (neexistuje k němu legitimní právní titul), ale z hlediska trestního práva by se mohlo jednat o případ nenaplnění materiálního znaku trestní odpovědnosti, totiž oné „míry společenské škodlivosti“ [28 s. 307].

2) *Black Hats* – druhou skupinou jsou hackeři, kteří jsou definičně přesným opakem předešle jmenovaných. Sem patří typicky pachatelé kybernetické trestné činnosti proti zařízením ICT, kdy motivací pro spáchání skutku je získání majetkového či jiného prospěchu anebo zneužití neoprávněně zpřístupněných dat [13 s. 273].
3) *Gray Hats* – na pomezí obou skupin stojí tzv. Gray Hats hackeři, kteří představují v tomto dělení zbytkovou kategorii. Při jejich činnosti může docházet k porušování práva nebo morálních principů, ale jejich cílem není primárně způsobení škody [13 s. 273]. Již výše byli zmínění etičtí hackeři, kteří jednají bez předchozí souhlasu a zařazení právě do této skupinu by mohlo být předmětem důvodné diskuse.

Hackeři při své činnosti užívají specifické techniky a nástroje, těmito jsou většinou prolamovače hesel (např. tzv. *brute-force* nebo slovníkové), vylákávání přístupových údajů pomocí podvodných zpráv apod. (tzv. *phishing*), malware (a jiný škodlivý software), sociální inženýrství, krádeží identity, *backdoors*, skenery, *sniffery,* a další [17 s. 35; 41 s. 59–67].

Pod souhrnný pojem hacking lze tedy podřadit celou řadu různých jednání. Trestněprávně relevantní však budou zejména ty, jejichž cílem je získání majetkového [12 s. 655] či jiného prospěchu. Hackerský útok může mít mnoho podob a forem, což bude zásadní při právní kvalifikace takového činu, kdy různá jednání mohou být subsumovány pod různé skutkové podstaty (nebo se může, a poměrně často tomu tak bude, jednat o souběh více trestných činů), příkladmo lze uvést – cracking (prolamování hesel a ochrany), sociální inženýrství, infikaci malware nebo jiným škodlivým kódem, instalaci „zádních vrátek“, odposlech komunikace v kyberprostoru nebo vylákávání přístupových údajů do systémů pomocí nejrůznějších podvodů [11 s. 93–94; 13 s. 274; 17 s. 29; 18 s. 31].

Nyní k trestněprávní kvalifikaci. Obecně si lze hackerský útok rozdělit na dvě formy – „základní“ a „pokročilou“ (kdy jsou využita i taková jednání, která mohou sama o sobě naplnit jinou skutkovou podstatu trestného činu – např. § 182 porušení tajemství dopravovaných zpráv, § 209 podvod, § 180 neoprávněné nakládání s osobními údaji nebo § 181 poškození cizích práv).

V případě základní formy se jedná o neoprávněný přístup k počítačovému systému a nosiči informací dle § 230 trestního zákoníku. Podřazení toto ustanovení se užije u hackingu, narušování dat, narušování systému a zneužívání zařízení [42].

V případech dle § 230 odst. 1 trestního zákoníku postačí ke spáchání trestného činu překonání bezpečnostních opatření, a tak získání neoprávněného přístupu do počítačového systému.

Dle odst. 2. § 230 trestního zákoníku spáchá trestný čin také pachatel, který získá přístup k počítačovému systému či nosiči informací (zde se ji nevyžaduje, aby byl tento přístup neoprávněný) a data takto získaná neoprávněně užije, nebo s nimi nějakým jiným způsobem neoprávněně naloží – zničí, pozmění, učiní neupotřebitelnými, nebo naopak neoprávněně vloží data nová. Za neoprávněné lze považovat především takové užití, které je v rozporu s právní normou, nebo v rozporu se stanoveným účelem nebo jsou jinak např. bez vědomí nebo souhlasu dotčené osoby zneužita. Toto ustanovení se použije i při využití malware (k infikování počítače [13 s. 276]).

Vznik škody a jiné újmy není vyžadován ani u jednoho z předešlých trestných činů a v případě, že újma vnikne může to být důvodem pro aplikaci kvalifikovaných skutkových podstat zejména odst. 3, 4 a 5.

S trestním jednání hackerů jsou spojené další jevy, jakým je přirozeně i nakládání s „hackerský vybavením a nástroji“. Trestnost tohoto počínání je zakotvena v § 231 trestního zákoníku, který upravuje situaci, kdy dojde k opatření a přechovávání přístupového zařízení nebo jeho součásti, postupu, nástroje, počítačového programu, nebo hesla či kódů k počítačovému systému [12 s. 692-694]. Trestní odpovědnost za tento trestný čin, ale může vzniknout jen v případě, kdy je tak činěno v úmyslu užít jich při spáchání trestného činu dle § 182 odst. 1 písm. b) nebo c) trestního zákoníku (porušení tajemství

dopravovaných zpráv) nebo § 230 trestního zákoníku (neoprávněný přístup k počítačovém systému…).

Trestný čin dle § 231 trestního je řazen mezi tzv. předčasně dokonané trestné činy [27 s. 791], to znamená, že trestní zákoník kriminalizuje i takové jednání, které běžně odpovídá stádiu přípravy. Jinak je přípravné jednání trestné jen u zvláště závažných zločinů dle § 20 odst. 1 trestního zákoníku. Normotvůrce, zda tak stanoví přísnější postih, kdy „posouvá“ míru jednání potřebné ke spáchání takového činu. Příprava „přípravy“ (resp. přípravné jednání ke spáchání trestného činu dle § 231) trestná nebude [12 s. 694], protože se nejedná i zvláště závažný zločin dle § 14 odst. 3 věta za středníkem.

Co se týče souběhu trestných činů dle §§ 230 a 231 trestního zákoníku je souběh těchto trestných činů vyloučen z důvodu subsidiarity [27 s. 792] a pachatel bude potrestán pro trestný čin dle § 230 (případně i § 182 odst. 1) pokud se čin stal – a to buď jako pachatel (§ 22 trestního zákoníku), nebo účastník dle § 24 trestního zákoníku, a pokud nedošlo k dokonání trestného činu dle § 230 potom jeho jednání bude posouzeno jako § 231 [12 s. 694] - jedná se o faktickou konsumpci [43 s. 344-346].

## *5.3 Malware*

Pro kybernetické trestné činy je často společným znakem využívání škodlivého kódu ať už samostatně, nebo ve spojení s dalším jednání anebo jako prostředek ke spáchání dalších skutkových podstat. Označení malware vzniklo složením anglických slov *malicious* (překl. škodlivý, zákeřný) a software [11 s. 96]. Jedná se o škodlivý kód (software), který je využíván k neoprávněnému omezení běžné funkčnosti ICT zařízení, získání dat nebo přístupu do počítačového systému. [13 s. 204] Jako rozlišovací znak takového software je uváděn také úmysl spáchat trestný čin nebo způsobit škodu [11 s. 96]. Také je třeba oddělit software, který je pouze nevyžádaný nebo nechtěný od toho škodlivého, který je způsobilý neoprávněně vniknout do počítačového systému [18 s. 38].

Malware obvykle zastává také více funkcí, kromě samotného obstarání neoprávněného přístupu do ICT zařízení může také sám sebe replikovat a šířit

prostřednictvím Internetu, *peer-to-peer* sítí, napadat připojená zařízení a odcizovat data.

Škodlivý software se dále dělí podle druhu hlavní činnosti nebo účelu, který program vykonává. Také označení jednotlivých druhů malware většinou vychází z jejich podstaty, a tak bývá zřejmé, jak konkrétně škodí [13 s. 205]. Jako příklad je možno uvést velmi rozšířený ransomware, což je druh malware, který po infiltraci do počítavého systému uzamkne nebo odcizí uživatelská a systémová data a za jejich zpřístupnění požaduje zaplacení peněžité částky – výkupného (z angl. *ransom*). Tento druh útoku je v českém prostředí poměrně častý a nezřídka cílí na veřejně prospěšné instituce jako jsou například nemocnice – viz „útok na Benešovskou nemocnici“ [44]. Dalšími mohou být *adware*, *spyware*, viry, červy, trojské koně nebo *rootkity* [13 s. 205; 18 s. 38].

Z hlediska trestněprávní kvalifikace bude útok pomocí malware postihnutelný dle § 230 (typicky odst. 2) trestního zákoníku, kdy instalace takové software bude představovat zásah do počítačového systému a další činnosti programu poté možná neoprávněná užití.

Skutkovou podstatu § 231 trestního zákoníku však naplní i pouze držení malware v úmyslu spáchat trestný čin dle § 182 nebo § 230. Kromě držení (resp. přechovávání) jsou trestnými i další jednání uvedená v § 231 (výroba, distribuce atp.). U některých zvláště závažných zločinů, kterými v této souvislosti mohou být dle § 311 teroristický útok, § 316 vyzvědačství nebo ohrožení utajované informace dle § 317 trestního zákoníku může být postihnuto i přípravné jednání [13 s. 221].

## 5.4 Nedbalostní § 232

Závěrem této kapitoly je výčet trestních fenoménů v oblasti kybernetické kriminality posledním z trestných činů upravené trestním zákoníkem a to § 232 (Neoprávněný zásah do počítačového systému nebo nosiče informací z nedbalosti). Zavedení této skutkové podstaty jde, na rozdíl od předcházejících §§ počítačových trestných činů, nad rámec Úmluvy o kybernetické kriminalitě [12 s. 695; 28 s. 312].

Zavedení tohoto trestného činu do českého trestního kodexu je v důvodové zprávě [45 s. 266] odůvodněno požadavkem z praxe. Tento důvod však neobstojí

v porovnání se statistikou, kdy za rok 2019 nebyl za tento trestný čin odsouzen ani jeden pachatel [28 s. 312]. Kriminalizace toho jednání je stále předmětem odborné diskuse [srov. 12 s. 695; 13 s. 377–378; 28 s. 312], kdy je scénář úmyslného jednání, ve kterém pravděpodobně selhávají orgány činné v trestním řízení v prokázání úmyslu nahrazen nedbalostním zaviněním [28 s. 312].

Spáchání trestného činu dle § 232 se lze dopustit jak konáním, tak i opomenutím (komisivně i omisivně), ale pouze speciálním subjektem vyplývající z vymezení v odst. 1. Vyžadována je hrubá nedbalost pachatele (dle § 16 odst. 2 trestního zákoníku) a způsobení škody alespoň značné (tj. nejméně 1 000 000 Kč – dle § 138 odst. 1 písm. d) trestního zákoníku).

# 6 Trestně-procesní aspekty

Závěrem teoretické části se tato práce bude zabývat stručným pohledem na problematiku odhalování a dokazování kybernetických trestných činů v České republice, které představují specifickou výseč trestního práva procesního.

Trestní právo České republiky nespočívá pouze ve stanovení sankcí pro trestné činy, ale také v zakotvení základních principů trestního řízení. Klíčovými dokumenty jsou Listina základních práv a svobod a trestní zákony (trestní zákoník a trestní řád). K jedním z nejdůležitějších principů, které mají zásadní význam pro dokazování, nejenom, kybernetické kriminality je „v pochybnostech ve prospěch obžalovaného“[19].

Orgány činné v trestním řízení, především policie, před sebou mají nelehký úkol spočívající v zajištění dostatečného množství dostatečně kvalitních důkazů (přičemž za důkaz může, ve velké zjednodušenosti, dle § 89 odst. 2 trestního řádu „sloužit vše, co může přispět k objasnění věci“), aby obžalovaný v trestním řízení mohl být usvědčen ze spáchání trestného činu (shledán vinným v dané věci a odsouzen) a to ve standardu tzv. „bez důvodných pochybností“ (§ 2 odst. 5 trestního řádu).

[19] lat. *in dubio pro reo*

Specifické výzvy přináší orgánům činným v trestním řízení digitální věk a kyberprostor, kdy právě prokázání spáchání kyberzločinu je často velmi složité. Při dokazování se vyžaduje prokázání viny konkrétní osobě, což při nástrojích o postupech, které používají pachatelé tohoto druhu trestné činnosti – jako jsou anonymizační programy, proxy servery, virtuální sítě apod. a účinné zametání stop v napadeném zařízení (mazání logů atp.) je někdy velmi náročné až nemožné.

Pokud se již podaří orgánům činným v trestní řízení prokázat původ trestného jednání většinou se jedná pouze o abstraktní identifikaci (IP adresu) zařízení ICT, ze kterého bylo učiněno. Toto zjištění však není dostatečným důkazem k prokázání viny konkrétní fyzické nebo právnické osoby. Okruh podezřelých však bývá alespoň z části zúžen a ve spojení s dalšími kriminalistickými metodami a svědeckými výpověďmi je možné v některých případech provést přesvědčivé určení pachatele.

Virtuální prostředí, ve kterém se kybernetická kriminalita odehrává, si vyžaduje od vyšetřovatelů nejenom podstatné technické znalosti, ale i schopnost rychle reagovat na neustále se měnící taktiky pachatelů. Dynamika digitálního světa klade na orgány činné v trestním řízení stále nové výzvy, přičemž odhalování počítačových trestných činů se stává složitějším a komplexnějším úkolem.

Zásada *in dubio pro reo* v digitálním prostředí zvláštní význam. Identifikace pachatele v kybernetickém prostoru je obtížná, a proto je tato zásada klíčovým prvkem spravedlivého soudního procesu.

Určitým drobným usnadněním, kromě tradičních institutů k zajištění důkazu, mohou být pro orgány činné v trestním řízení nástroje ve vztahu ke kyberprostoru a digitálním důkazům, které jim dávají trestní řád např. § 88a a zákon č. 127/2005 Sb., o elektronických komunikací v § 97 odst. 3 při vyšetřování trestných činů s horní hranicí trestní sazby alespoň 3 roky obecně a pro vyčtené trestné činy bez požadavku na výši trestní sazby zjistit údaje o telekomunikačním provozu. V těchto případech se však jedná pouze údaje provozně-lokalizačního charakteru, ne však obsah samotné komunikace.

Oproti tomu mohou orgány činné v trestním řízení využít při vyšetřování některých závažných trestných činů s horní hranicí trestní sazby nejméně 8 let a u vyjmenovaných trestných činů i bez stanovení minimální horní hranice trestní

sazby, odposlechu nebo záznamu telekomunikačního provozu dle § 88 trestního řádu, kdy je předmětem zajišťovaného důkazu obsah sledované komunikace.

Odhalování a dokazování kybernetických trestných činů je stále velkou výzvou pro moderní trestní právo. S nástupem digitální éry a komplexností kyberprostoru se stává identifikace pachatelů obtížnou, a to i navzdory nástrojům poskytovaným trestním právem. Zajištění dostatečných důkazů prokazujících vinu zůstává pro orgány činné v trestním řízení náročným úkolem.

# 7 Praktická část

V dnešní digitální době, charakterizované rychlým technologickým pokrokem a rozvojem internetových komunikačních prostředků, se kybernetická kriminalita stává stále významnějším fenoménem. Tato forma trestné činnosti využívá moderní technologie k nelegálním činnostem, čímž se stává závažným problémem pro společnost, ekonomiku a bezpečnost jednotlivců i institucí. Bakalářská práce se v této části zaměřuje na důkladnou analýzu kybernetické kriminality prostřednictvím konkrétní případové studie. Praktická část je rozdělena na kapitoly věnující se jednotlivým skutkovým podstatám tzv. „počítačových trestných činů“ obsažené v trestním zákoníku. Konkrétně se jedná o § 230 („neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému“), který obsahuje dvě základní skutkové podstaty v odst. 1 a v odst. 2 a každé z nich je věnována vlastní kapitola obsahující několik analyzovaných případů a dále § 231 („opatření a přechovávání přístupového zařízení a hesla“). Kvalifikované skutkové podstaty uvedených trestných činů jsou ponechány stranou, ale lze k nim obecně uvést, že zahrnují znaky v podobě kvalifikovaného úmyslu - např. způsobit škodu nebo získat prospěch, omezit funkčnost počítačového systému, vyšší kvantifikace škody dle § 138 trestního zákoníku, spáchání činu coby člen organizované skupiny nebo například útok na klíčovou infrastrukturu státu.

Trestní zákoník také zahrnuje trestný čin dle § 232 (neoprávněný zásah do počítačového systému nebo nosiče informací z nedbalosti), pro který však, jak již bylo pojednáno v teoretické části, neexistuje dohledatelný případ odsouzení za tento trestný čin. Webová aplikace jaktrestame.cz, která vychází z dat Ministerstva

spravedlnosti, které ji společně s Nejvyšším státním zastupitelstvím neuvádí ve svých datech od roku 2016 žádný případ odsouzení. Veřejně dostupné části databází soudních rozhodnutí soudů různých stupňů neposkytují pro toto ustanovení žádná data, stejně tak jako prověřené právní informační systémy.

Cílem této části práce je představit a analyzovat vybrané případy kybernetické kriminality, identifikovat specifika těchto případů v kontextu platných právních předpisů a demonstrovat účinnost a vhodnost právních nástrojů v boji proti této formě trestné činnosti. K tomu bude využito kombinace právního zkoumání a analýzy konkrétních případů, které poskytnou pohled na různorodé projevy kybernetické kriminality.

Při analýze těchto případů budou klíčovým prvkem otázky spojené s ustanovením § 230 odst. 1, § 230 odst. 2 a § 231 trestního zákoníku, které se týkají například definice a rozsahu popisovaných trestných činů, sankcí, procesních pravidel a dalších aspektů s trestním řízením spojených.

Při analýze případů je v naprosté většině vycházeno z rozhodnutí (usnesení) Nejvyššího soudu, které je vrcholovým soudem obecné soustavy soudů a jednotným místem rozhodováním o mimořádných opravných prostředcích trestního procesu, kterými jsou dovolání. Tato usnesení jsou dostatečným pramenem pro provedení podrobné případové studií, zejména proto, že shrnují dosavadní průběh soudního řízení u soudu 1. a 2. stupně, rekapitulují skutkovou stránku posuzované trestní věci, obsahují argumentaci obviněných a to jak ve vztahu k odvolacímu, tak i dovolacímu řízení a vyjádření zástupce veřejné (ob)žaloby – příslušného státního zástupce a především posouzení věci (formálně do rozsahu dovolacích námitek, ale v praxi i *de facto* k meritu věci) a vyslovení právních vět a názorů Nejvyššího soudu. Tato rozhodnutí jsou narozdíl od rozhodnutí okresních a krajských soudů poměrně dobře dohledatelná pro jejich spolehlivé zveřejňování a dostupnost.

Praktická část si pro jednotlivé kapitoly a případovou studii klade dále uvedené výzkumné otázky, na které budou poskytnuty odpovědi a východiska v rámci jednotlivých analýz případů.

> 1) Jaký je relevantní právní rámec kybernetické kriminality v českém trestním právu? Jak jsou vymezeny jednotlivé trestné činy? 2) Jaká jsou specifika jednotlivých trestných činů a čím se od sebe jednotlivé skutkové

podstaty odlišují? 3) Jak ve zjednodušené podobě probíhá trestní soudní proces? 4) Na jaká úskalí nebo s jakými specifickými otázkami se musely soudy v řízení vypořádat? 5) Jaké hodnoty chrání ustanovení trestního zákoníku o počítačových trestných činech? 6) Jakým způsobem se mění povaha kybernetické kriminality a aplikace práva soudem s postupem technologického vývoje?

Tyto výzkumné otázky budou sloužit jako základ pro analýzu a zhodnocení specifik kybernetické kriminality v kontextu uvedených právních norem, přičemž cílem bude přispět k lepšímu pochopení a poskytnout vhled do problematiky trestních řízení s pachateli kybernetické kriminality.

## 7.1 Rozbor rozhodnutí k § 230 odst. 1 trestního zákoníku

Tato kapitola se věnuje hlubšímu zkoumání § 230 odst. 1 trestního zákoníku v kontextu konkrétní případové studie. Tato právní norma s sebou nese významné implikace, které otevírají diskusi o zásazích do integrity a důvěrnosti dat a ochrany soukromí. § 230 odst. 1 trestního zákoníku se zaměřuje na neoprávněný přístup k počítačovému systému a nosiči informací překonáním bezpečnostního opatření[20]. Jedná se o ustanovení, které chrání důvěrnost dat a osobní bezpečnost v digitálním světě. Předmětem zkoumání je nejen samotný text právní normy, ale i jeho praktická aplikace v reálném soudním řízení a jeho skutkové vymezení, a přitom se bude zaměřovat i na důsledky neoprávněného přístupu k počítačovým systémům a závažnost tohoto jednání ve světle trestněprávní odpovědnosti.

Představení konkrétního případu, který nám poslouží jako studijní materiál k případové studii, nabídne pohled na současnou praxi soudů při řešení a úvahách daného projevu kybernetické kriminality. K analýze případu je využito usnesení Nejvyššího soudu 7 Tdo 1134/2020-445 ze dne 4. 11. 2020.

---

[20] § 230 Neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací

(1) Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.

*(zákon č. 40/2009 Sb., trestní zákoník)*

### 7.1.1 Shrnutí soudního řízení

Obviněný Š. H. byl 17. 12. 2019 v řízením před soudem 1. stupně – okresním soudem v Českých Budějovicích, uznán vinným zločinem týrání osoby žijící ve společném obydlí dle § 199 odst. 1, 2 písm. b), d) a přečinem neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 odst. 1 trestního zákoníku a byl mu uložen úhrnný trest odnětí svobody v délce 3 let s podmíněním odložením na zkušební dobu v délce 5 let se stanovením dohledu (tzv. „podmíněný trest odnětí svobody“). Proti tomuto rozsudku podali obviněný i státní zástupce odvolání ke krajskému soudu v Českých Budějovicích, jež odvolání zamítl jako nedůvodná. Obviněný podal proti zamítavému usnesení krajského soudu dovolání k Nejvyššímu soudu, který jej pro zjevnou neopodstatněnost odmítl. Z usnesení Nejvyššího soudu v rozsahu týkajících se kybernetické kriminality. tj. přečinu dle § 230 odst. 1 trestního zákoníku je pro tuto případovou studii vycházeno.

### 7.1.2 Skutková podstata

Skutková podstata spočívala v tom, že obviněný Š. H. dlouhodobě fyzicky a psychicky týral poškozenou A. Š., což kromě jiných naplněných skutkových podstat trestných činů (ty nejsou předmětem této studie) eskalovalo i ke spáchání trestného činu §230 odst. 1 trestního zákoníku, kdy Š. H. překonal bezpečnostní opatření neoprávněným užitím přístupového hesla k emailové schránce poškozené. Následně využil duplikátu telefonní SIM karty, kterou si nechal vyhotovit bez souhlasu poškozené, a po jejím vložení do svého telefonu získal neoprávněný přístup i k účtu poškozené na sociální síti Facebook pomocí vygenerování nového hesla. Dále na těchto účtech změnil bez souhlasu a vědomí poškozené přístupová hesla, čímž A. Š. znemožnil přístup a používání těchto účtu.

### 7.1.3 Argumentace obviněného

Obviněný namítl, že nemohl spáchat přečin neoprávněného přístupu, neboť sám zakládal daný počítačový účet, měl k němu přístup a znal heslo. Argumentoval tedy tím, že nepřekonal žádná bezpečnostní opatření, neboť všechny potřebné informace měl v rámci svých oprávnění. Na druhou stranu, soud dospěl k závěru, že použitím duplikátu SIM karty a následným blokováním přístupu poškozené

k vlastním účtům, obviněný překonal bezpečnostní opatření a neoprávněně pronikl do jejího „virtuálního obydlí“.

### 7.1.4 Překonání bezpečnostního opatření jako znak skutkové podstaty trestného činu

Státní zástupkyně ve svém stanovisku zdůraznila, že § 230 odst. 1 trestního zákoníku primárně sankcionuje narušení důvěrnosti dat neoprávněným přístupem k počítačovému systému. Zde je klíčové definovat, co přesně představuje „překonání bezpečnostního opatření“. Soudní rozhodnutí potvrzuje, že i využití duplikátu SIM karty může být považováno za překonání bezpečnostního opatření, ačkoliv pachatel nemusel překonávat technické bariéry, jako je heslo. Toto tvrzení je o to přesvědčivější v porovnání s názorem okresního soudu, kterému mu dal Nejvyšší soud plně za pravdu, že překonání bezpečnostního opatření, jako jeden z klíčových předpokladů pro naplnění skutkové podstaty dle § 230 odst. 1 trestního zákoníku, lze spatřovat i v samotném neoprávněném užití hesla k přístupu, byť jej obviněný znal z dřívějška.

Závěr prvoinstančního soudu potvrzeným shodným stanoviskem soudu Nejvyššího je také v souladu s relevantními doktrinálními právními komentáři [46, 47].

### 7.1.5 Virtuální prostor jako „obydlí“

Státní zástupkyně předložila zajímavé přirovnání, ve kterém virtuální prostor, zejména sociální média, byl přirovnán k „obydlí“. Toto srovnání zdůrazňuje, že i virtuální svět má svá soukromí a práva a že neoprávněný přístup k těmto účtům může být srovnatelný s neoprávněným vstupem do fyzického obydlí, kdy taktéž nemusí být užito „násilí“ ke vstupu, ale narušení soukromé sféry může být způsobeno např. i shodným klíčem k zámku. Důležité je, že se jedná o překonání zamýšlené překážky k zamezení přístupu (dveře, heslo – a to, jakkoliv triviální, kdy lze snadno tipnout/uhádnout, známé útočníkovi nebo složité a bezpečné k jehož překonání jsou potřebné speciální technické prostředky a náročné postupy). Poškozená svědčila o tom, jak obviněný zablokoval její účty a manipuloval s jejím osobním prostorem. To naznačuje, že neoprávněný přístup nejen narušuje

technologickou bezpečnost, ale má také reálné dopady na osobní život a soukromí jednotlivce.

### 7.1.6 Dopady případu

Podobná rozhodnutí o neoprávněném přístupu k počítačovému systému otevírá otázky ohledně vymezení a interpretace bezpečnostních opatření v digitálním prostoru. Jak technologie postupuje, soudy a právní systémy budou muset neustále aktualizovat své pojetí bezpečnostních opatření, aby efektivně reagovaly na nové kybernetické hrozby. Narušování důvěrnosti dat není doménou pouze „hackerů“ a útočníků coby 3. osob. Velmi často se jedná o neoprávněné přístupy nebo narušení soukromí v úzkém rodinném kruhu nebo mezi partnery, kdy nerespektování hranic soukromí druhého překonáním nastaveného přístupového hesla, PIN kódu, gesta nebo čím dál častějších biometrických bezpečnostních opatření může vést až trestní odpovědnosti pachatele za tento trestný čin.

Přestože zde pravděpodobně nejde hovořit o „dobrém úmyslu“ pachatele, a to zejména v případě, kdy se jedná o přístup bez vědomí a svolení poškozeného, bude pro většinu pachatelů překvapující závažnost a trestněprávní relevantnost jejich jednání. Motiv pachatele pro toto jednání bude v domácím prostředí většinově pramenit ze společnosti méně závažněji vnímané partnerské či jiné žárlivosti nebo zvědavosti, kdy kromě hrozící trestního postihu dochází hlavně, a především k narušení morální integrity pachatele, zavrženíhodnosti jeho chování či narušení mezilidského vztahu – to bude ve většině případů jediná sankce. Jinak tomu však bude při vzniku konfliktů ve vztahu a jejich další eskalaci, kdy tyto skutečnosti často vyplývají na povrch. Omezování a narušování přístupu v kombinaci s domácím násilím a psychickým týráním je také častým jevem, jak může být demonstrováno na aktuálním případu, na který autor narazil právě při psaní tohoto textu [48], nebo ve skutkové stránce studovaného rozhodnutí.

## *7.2 Rozbor rozhodnutí ve vztahu k § 230 odst. 2 trestního zákoníku*

Právní úprava obsažena v § 230 odst. 2[21] trestního zákoníku je další základní skutkovou podstatou § 230 postihujícím kybernetické trestné činy.

Tato kapitola si klade za cíl představit na podrobné analýze čtyřech konkrétních případů, kde byly osoby trestně stíhány za spáchání tohoto trestného činu, možné způsoby spáchání přečinu, pestrou škálu postihovaných jednání, které lze pod skutkovou podstatu subsumovat, argumentace obviněných a judikaturní závěry soudů, které poskytují další výkladová pravidla a vodítka pro jiné případy.

### 7.2.1 Případ 1 – „Špionáž ve schránce“

V této části studie bude představen případ J. F., příslušníka Policie ČR, obviněného z neoprávněného přístupu k e-mailové schránce Bc. J. Z. čím se měl dopustit spáchání trestného činu dle § 230 odst. 2 trestního zákoníku. Kromě základních skutkových okolností a analýzy soudního řízení bude pozornost věnována také otázce nutnosti způsobení škody pro naplnění skutkové podstaty tohoto trestného činu a jak je na ni pohlíženo optikou soudů. Základním zdrojem poznání je v tomto případě usnesení Nejvyššího soudu 6 Tdo 1479/2012 ze dne 12. 12. 2012.

---

[21] § 230 Neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací

(1) Kdo zasáhne do počítačového systému nebo nosiče informací tím, že

a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,
b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,
c) padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo
d) neoprávněně vloží nebo přenese data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítačového systému nebo jiného technického zařízení pro zpracování dat, bude potrestán odnětím svobody až na tři léta, zákazem činnosti nebo propadnutím věci.

*(zákon č. 40/2009 Sb., trestní zákoník)*

#### 7.2.1.1 Shrnutí soudního řízení

Rozsudek Okresního soudu v Břeclavi ze dne 30. 3. 2012 obviněného uznal vinným přečinem neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 2 písm. a) trestního zákoníku. Obviněný byl odsouzen k trestu odnětí svobody v trvání šesti měsíců, s podmíněným odložením na zkušební dobu jednoho roku. Rozsudek Krajského soudu v Brně ze dne 1. 8. 2012 potvrdil tuto vinu, když zamítl odvolání obviněného a jeho matky.

Obviněný však proti rozsudku odvolacího soudu podal dovolání k Nejvyššímu soudu, tvrdíce, že motiv jeho jednání by mohl snižovat společenskou škodlivost skutku a že by jeho čin mohl být posuzován jako přestupek. Dovolání bylo podáno s návrhem na zrušení rozhodnutí Krajského soudu v Brně a vrácení věci k novému projednání. Obhajoba zdůraznila, že údajný trestný čin nelze subsumovat pod konkrétní ustanovení trestního zákoníku, a vyzvala Nejvyšší soud k novému posouzení případu.

Nejvyšší soud případ prozkoumal a následně dovolání jako zjevně neopodstatněné odmítl.

#### 7.2.1.2 Skutková podstata

V květnu 2011 se obviněný J. F., příslušník Policie ČR, dopustil neoprávněného vstupu do e-mailové schránky Bc. J. Z., kde přistupoval a manipuloval s obsahem zpráv (daty). Přístupem k e-mailové schránce poškozené pomocí svého notebooku získal intimní korespondenci poškozené J. Z. s J. B., kterou následně bez vědomí a souhlasu (neoprávněně) vytiskl a v listinné podobě zaslal manželovi poškozené (R. Z.) a dále tyto informace o obsahu korespondence sdělil manželce J. B. (paní L. B.). Toto vedlo k vznesení obvinění podle § 230 odst. 2 trestního zákoníku.

#### 7.2.1.3 Posouzení případu

V rámci vyšetřování se prokázalo, že obviněný získal přístup k e-mailovému účtu prostřednictvím neoprávněně získaného hesla. I přes možnost, že měl k dispozici heslo poskytnuté obětí, mu byl vytýkán úmysl získat kontrolu nad

e-mailovou schránkou bez legitimního oprávnění. Vědomí tohoto záměru podtrhuje závažnost obvinění podle § 230 odst. 2 písm. a) trestního zákoníku.

Obviněný argumentoval v dovolání tím, že jeho motivy snižují společenskou škodlivost činu a měl by být posuzován jako přestupek. Poukázal na to, že obdržel přístup k e-mailové schránce od poškozené a používal ji s předpokladem, že má její svolení. Argumentoval také tím, že e-mailová korespondence probíhala v pracovní době na počítači zaměstnavatele, což by mohlo snižovat její právní ochranu. Obviněný tvrdil že tím, že předmětná korespondence byla vytvořena na počítači zaměstnavatele, v pracovní době a že když zaměstnavatel provádí „screening výpočetního systému“, pak nemohou tyto data požívat ochranu trestním právem.

Námitka, že jednání obviněného nedosahuje potřebné míry společenské škodlivosti byla uznána za relevantní, avšak k ní Nejvyšší soud zdůrazňuje, že trestní zákoník vymezuje trestné činy na základě protiprávního jednání, splňujícího stanovená kritéria. Samotná společenská škodlivost není samostatným právním znakem trestného činu, nýbrž slouží jako jedno z kritérií pro uplatňování zásady subsidiarity trestní represe podle § 12 odst. 2 trestního zákoníku. Dále vyvodil (v návaznosti na předchozí judikaturu) obecné pravidlo, že jakékoli jednání odpovídající definici trestného činu uvedeného v trestním zákoníku, je považováno za trestný čin, a nelze ho obecně označit za neškodné ve společnosti. Závěr, že trestný čin může být posouzen co do nedostatečné společenské škodlivosti činu lze vyvodit pouze v mimořádných situacích, kdy není vhodné uplatňovat trestní represi z určitých důvodů, a za podmínky, že závažnost daného jednání neodpovídá ani těm nejlehčím a běžně se vyskytujícím trestným činům dané právní kvalifikace.

Soud zdůraznil, že obviněný, jakožto příslušník Policie ČR, měl ze všech osob obzvláště dbát povinnosti dodržovat zákonná ustanovení a chránit bezpečnost elektronických dat občanů. Jeho neoprávněný vstup do e-mailové schránky byl považován za vážné porušení této povinnosti a zneužití důvěry spojené s jeho profesním postavením.

Rozhodujícím momentem byl také úmysl obviněného porušit bezpečnostní opatření a proniknout do soukromé elektronické komunikace. Jak vyplývá z důkazů a vyšetřování, obviněný si byl vědom následků svého jednání, přičemž nejenom

vstoupil do e-mailové schránky, ale též získal kontrolu nad obsahem a informacemi v ní obsaženými, které dále zneužil (neoprávněně užil).

Soud zdůraznil, že naplnění skutkové podstaty nespočívalo pouze v neoprávněném získání hesla, ale i v následném zneužití elektronických dat a tím byla naplněna základní skutková podstata dle § 230 odst. 2 trestního zákoníku.

#### 7.2.1.4 Škoda jako znak skutkové podstaty trestného činu

Nejvyšší soud ve svých závěrech také hovoří o škodě jako (ne)obligatorním znakem skutkové podstaty dle § 230 odst. 2 trestního zákoníku. V případě trestného jednání dle tohoto ustanovení tedy není obsažen znak úmyslu způsobit škodu, jinou újmu nebo získat prospěch a ani se nevyžaduje, aby k takovému účinku došlo. Zákon chrání počítačová data a programy před neoprávněnými zásahy, které by mohly ovlivnit existenci, kvalitu nebo správnost dat. Trestný čin se vztahuje k neoprávněnému získání přístupu a následnému neoprávněnému užití dat.

#### 7.2.1.5 Závěrem

Na spáchaný trestný čin zle pohlížet v kontextu ochrany soukromí a bezpečnosti elektronických komunikací jako na závažné porušení těchto chráněných hodnot. Případ J. F. poskytuje vhled do problematiky kybernetické kriminality a ochrany dat, kdy může docházet k neoprávněnému přístupu k datům a jejich neoprávněnému užití s různými motivy pachatele.

Soud také rekapituluje závěry ustálené judikatury Nejvyššího soudu, z nichž vyplývá že:

*„Získáním přístupu se zde rozumí takové jednání, které umožní pachateli volnou dispozici s počítačovým systémem nebo nosičem informací a využití jeho informačního obsahu. Získat přístup k počítačovému systému nebo nosiči informací lze neoprávněně, ale i oprávněně. Nezáleží ani na důvodu, který vedl k získání přístupu (může to být náhoda, plnění pracovních úkolů, využití počítače pro zábavu, odcizení nosiče informací atd).*

*Neoprávněným užitím dat (neboli počítačovou špionáží) je jakákoli nedovolená manipulace s daty uloženými v počítačovém systému nebo na nosiči informací, pokud*

*nejde o případy b) až d). Neoprávněné bude takové užití, které je v rozporu s právní normou … nebo je činěno v rozporu se stanoveným účelem, popř. bez vědomí či souhlasu oprávněné osoby. Neoprávněným užitím je též nedovolené kopírování na jiný nosič informací, který pak má většinou pachatel ve své dispozici.“ (6 Tdo 1479/2012)*

V úvahách o právní kvalifikaci případu lze přemýšlet také o aplikaci § 182 trestního zákoníku (Porušení tajemství dopravovaných zpráv), který chrání spíše datové zprávy jako takové a jejích integritu, kdežto u § 230 odst. 2 trestního zákoníku není příliš reflektován zdroj neoprávněně užitých dat jako právě jejich protiprávní užití.

### 7.2.2 Případ 2 – „Padělání elektronických dokumentů“

Tento rozbor se zaměřuje na případ R. H., která byla obviněna z neoprávněného přístupu k datové schránce společnosti A. I. C., s. r. o. dle § 230 odst. písm. c) trestního zákoníku. V roce 2016 byla uznána vinnou za padělání dat v této schránce a odsouzena k šesti měsícům odnětí svobody s podmíněným odkladem. Po neúspěšném odvolání se obrátila dovoláním na Nejvyšší soud, který její dovolání zamítl.

Kromě otázky viny a naplnění skutkové podstaty včetně precizního odůvodnění jednotlivých znaků se usnesení soudu zabývá také podstatnou problematikou aplikace trestních norem počítačové kriminality v oblasti datových schránek. Analyzované rozhodnutí usnesení Nejvyššího soudu 8 Tdo 266/2017 ze dne 15. 8. 2018 je zcela klíčovým v oblasti kybernetické kriminality a stanovuje výkladový rámec pro další případy a trestní řízení a bylo publikováno i ve Sbírce soudních rozhodnutí Nejvyššího soudu 23/2020.

#### 7.2.2.1 Shrnutí soudního řízení

Obvodní soud pro Prahu 1 uznal 14. 7. 2016 obviněnou R. H. vinnou z přečinu neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 2 písm. c) trestního zákoníku, kterého se měla dopustit padělám dat (dokumentů) v datové schránce poškozené obchodní společnosti A. I. C., s. r. o., se sídlem v Praze.

Za tento trestný čin byla obviněná odsouzena k trestu odnětí svobody v délce trvání 6 měsíců s podmíněným odloženým na zkušební dobu v trvání 1 roku.

Proti rozsudku Okresního soudu se obviněná i státní zástupkyně odvolaly k Městskému soudu v Praze, který usnesením ze dne 26. 10. 2016 (sp. zn. 44 To 385/2016) obě odvolání zamítl.

Proti tomuto rozhodnutí obviněná R. H. podala dovolání k Nejvyššímu soudu, dle § 265b odst. 1 písm. g) a l) trestního řádu, kde soudům z dotčeného trestního řízení vytýká nesprávnou právní kvalifikaci a dostatečné neaplikování zásady subsidiarity trestní represe.

Nejvyšší soud dovolání R. H. zamítl dle § 265j trestního řádu jako nedůvodné.

#### 7.2.2.2 Skutková podstata

Obviněná R. H. se dopustila trestného činu dle § 230 odst. 2 písm. c) trestního zákoníku tím, že v březnu 2014 zneužila datovou schránku společnosti A. I. C., s. r. o., ke které měla přístup dle platně uzavřené smlouvy o poskytování poradenských služeb ze dne 21. 12. 2012. Toto zneužití spočívalo v tom, že obviněná neoprávněně užila datovou schránku k elektronické komunikaci se svojí vlastní datovou schránkou. V rámci této komunikace obviněná zaslala do své datové schránky dokumenty, které obsahovaly uznání dluhu za práce, které měly být vyfakturovány obviněnou. P. V. jako jednatelka společnosti A. I. C. odmítla uhradit tyto faktury jako nedůvodné, neboť podle ní nebyly služby vyžádány ani provedeny.

Další částí popisu jednání obviněné bylo opakované zaslání dalších dokumentů z datové schránky společnosti A. I. C. do datové schránky R. H. Tyto dokumenty obsahovaly opětovné uznání dluhu a ukončení smlouvy. Důležitým prvkem skutkové podstaty je, že všechny zmíněné dokumenty obviněná sama vytvořila, vložila do počítačového systému a podepsala je jménem jednatelky společnosti P. V.

Obviněná tedy využila svůj přístup k datové schránce společnosti A. I. C. k vytvoření a odeslání falešných dokumentů, které obsahovaly nesprávné informace o dluhu a ukončení smlouvy. Celý proces měl za následek nesrovnalosti mezi obviněnou a P. V., která odmítla uznat a uhradit tyto faktury, a to s odůvodněním, že

nebyly vyžádány ani provedeny. Skutková podstata tedy spočívá v neoprávněném a klamavém užití datové schránky k vytváření a zasílání falešných dokumentů.

#### 7.2.2.3 Argumentace obviněné

Obviněná R. H. podala dovolání proti usnesení odvolacího soudu s odvolacími důvody podle § 265b odst. 1 písm. g) a l) trestního řádu a dovolání podkládala tvrzeními, že soudy nižších stupňů nesprávně právně kvalifikovaly její jednání, které označily jako přečin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 2 písm. c) trestního zákoníku, a že nepřihlédly k ustanovení § 12 odst. 2 trestního zákoníku.

V dovolání obviněná poukázala na to, že skutek popsaný v rozsudku Obvodního soudu není dle jejího názoru možné kvalifikovat jako přečin neoprávněného přístupu k počítačovému systému podle § 230 odst. 2 písm. c) trestního zákoníku. Tvrdila, že získala přístup k počítačovému systému v rámci svých práv (oprávněně), která jí udělila jednatelka společnosti A. I. C., a že neprovedla žádné padělání či pozměnění dat v počítačovém systému. Argumentovala, že vytvořila dokumenty související s řešením závazků ze smlouvy o poskytování poradenství, a tyto dokumenty odeslala jednatelce P. V. k odsouhlasení.

Obviněná upozornila na to, že data vytvořených dokumentů nebyla nikde použita a že nebyla jejich autorem a že tak ani učinit nemohla. Tvrdila, že zcela chybí úmysl k padělání dat, protože dokumenty nebyly nikdy použity ani vydávány za pravé. Celé její jednání spočívalo pouze ve vytvoření dokumentů, které posléze odeslala k odsouhlasení.

R. H. rovněž argumentovala, že z výsledků provedeného dokazování nevyplynulo, že by manipulovala s datovou schránkou poškozené nebo ji použila k odeslání nepravých dokumentů a že soudy nevěnovaly dostatečnou pozornost skutečnosti, že skutková zjištění postrádají podklad k závěru, že byla ona tou, kdo odeslal dokumenty prostřednictvím datové schránky. Zpochybnila výpovědi jednatelky P. V. ohledně přístupu k datové schránce a upozornila na možnost, že i další osoby mohly mít přístup k údajům.

Dále obhajoba kritizovala závěr odvolacího soudu, že odeslala dokumenty s úmyslem vyvolat mylný dojem o souhlasu jednatelky. Dokládala, že žádnou datovou zprávu o uznání dluhu za jednatelku P. V. neodesílala, a že takový krok musela udělat sama jednatelka nebo jiná pověřená osoba. Obviněná namítala, že soudy nevyhověly jejím požadavkům na znalecký posudek z oboru kybernetiky, který měl objasnit, zda jednatelka či jiná pověřená osoba seznámila s dokumenty zaslanými z datové schránky.

Soudy dle názory dovolatelky nesprávně posoudily škodlivost jejího jednání ve smyslu zásady uvedené v § 12 odst. 2 trestního zákoníku. Byla toho přesvědčení, že postačuje uplatnění odpovědnosti podle jiného právního předpisu, například stavovského předpisu nebo zákona o přestupcích k čemuž odkázala na stanovisko trestního kolegia Nejvyššího soudu ze dne 30. 1. 2013, sp. zn. Tpjn 301/2012, a tvrdila, že soudy způsobily nepřípustnou kriminalizaci závazkového vztahu (soukromoprávní vztahu) a z něj vyplývajících práv a povinností.

V závěru dovolání obviněná navrhla zrušení rozhodnutí napadeného dovoláním a přikázání věci k dalšímu projednání Obvodnímu soudu pro Prahu 1.

#### 7.2.2.4 Stanovisko státního zástupce

Státní zástupce Nejvyššího státního zastupitelství ve svém vyjádření k dovolání obviněné R. H. potvrdil správnost právní kvalifikace skutku, kterou přijal odvolací soud. Podle státního zástupce jsou klíčové tři okolnosti, které odvolací soud správně vyhodnotil. První okolností je definice padělání jako úplného vyhotovení nepravých dat s úmyslem vytvořit dojem, že jsou pravá, což obviněná spáchala v případě dokumentů vložených do systému datových schránek. Druhá okolnost se týká samotného trestného jednání v podobě padělání dat, aniž by bylo nutné, aby je pachatel fakticky využil k uvádění někoho v omyl. Třetí okolnost se týká rozsahu oprávnění obviněné k nakládání s datovou schránkou poškozené, kde státní zástupce zpochybnil tvrzení obviněné o faktickém předání všech práv na datovou schránku.

Státní zástupce dále rozvinul teorii tzv. „datového dvojníka“, kterým se obviněná stala v důsledku lehkovážného chování jednatelky P. V. Podle něj však úkony tohoto „datového dvojníka“ nelze považovat za úkony poškozené, a tedy

dokumenty, které se zdánlivě jeví jako úkony poškozené, ve skutečnosti nebyly jejími úkony.

Státní zástupce odmítl výhrady obviněné ohledně zásady podle § 12 odst. 2 trestního zákoníku a neshledal v činu žádné výjimečné znaky, které by snižovaly jeho společenskou škodlivost. Naopak zdůraznil, že padělaný dokument obsahoval údaje, které by mohly být v budoucnu využitelné ve prospěch obviněné a na úkor poškozené.

Celkově státní zástupce navrhl, aby Nejvyšší soud odmítl dovolání obviněné, protože je podle něj zjevně neopodstatněné.

#### 7.2.2.5 Posouzení případu

Nejvyšší soud přezkoumával dovolání obviněné, ve kterém se vypořádal s její argumentací a důvody, které spojovala s nutností zrušení rozsudku nižších soudů.

Dovolací soud v odůvodnění dovolání uvedl, že vytýkané nedostatky ve skutkových zjištění neodpovídají průběhu skutku, jak byly dostatečně zjištěny soudy a obviněná si vytvořila vlastní skutkovou verzi průběhu činu se kterou brojí v dovolacím řízení.

K námitce R. H. o neprovedení znaleckého posudku z oboru kybernetiky poznamenal Nejvyšší soud, že znalecké místo mají v řízení místo pouze tehdy pokud je potřeba objasnění odborných aspektů souvisejících s trestním řízením. V tomto případě však soud zohlednil návrh na doplnění dokazování znaleckým posudkem jako nadbytečný, jež by vedl k průtahům v řízení a neposkytlo by soudu žádné další poznatky potřebné pro rozhodnutí. Soud vyhodnotil že prostým výkladem empirických informací dožádaných od Ministerstva vnitra, coby správce služeb datových schránek, který poskytl údaj o IP adrese, ze které došlo k přístupu do datové schránky poškozené a informací od poskytovatel internetového připojení vedou k přesvědčivé identifikaci jednající osoby. Znalec by ve svém posudku musel užít stejného postupu a pro následnou interpretaci není potřeba jeho odborných znalostí.

Nejvyšší soud dále upozorňuje, že obviněné nebylo kladeno za vinu, že neoprávněně získala přístup k datové schránce poškozené, ale že použila její datovou schránku k odeslání nepravdivých dokumentů a že se tím snažila vytvořit

klamavý dojem, že jednatelka P. V. souhlasí s obsahem dokumentů a že zasláním dokumentů z datové schránky je jednatelka společnosti podepsala.

Ustanovení § 230 odst. 2 trestního zákoníku chrání integritu a dostupnost počítačových dat a systémů a poskytovaná ochrana zde dopadá na neoprávněné zásahy, které mohou mít vliv na existenci, kvalitu a správnost dat. Čin vymezený v písm. c) slouží právě k ochraně proti falšování údajů souvisejících s počítači a daty.

Soud však souhlasí s námitkou R. H., že k zpřístupnění datové schránky poškozenou předáním přístupového uživatelského jména a hesla došlo protiprávně. Jednatelka společnosti porušila povinnost dle § 9 zákona č. 300/2008 Sb., zákona o elektronických úkonech a autorizované konverzi dokumentů, kdy byla povinna zacházet s přístupovými údaji tak, aby nemohlo dojít k jejich zneužití a takovému nakládání, kdy dojde ke ztrátě faktické kontroly.

Statutární představitelka poškozené však dle názoru soudu absolutně nepochopila smysl ani význam datové schránky – tento závěr soud podložil skutečnostmi, že neplatila poplatky za provoz datové schránky, nepřistupovala k datové schránce a ani nevěděla, jak následně zbavit obviněnou přístupu). Z dokazování také vyplynulo, že obviněná byla v dané době jediná, která dokázala datovou schránku obsluhovat.

Fakt, že došlo k zřízení přístupu k datové schránce v rozporu s právem, ale nemá vyznám pro trestněprávní odpovědnost dovolatelky, kdy je podstatné, že takový přístup měla, nikoliv jak k němu přišla.

Po přezkoumání případu dospěl Nejvyšší soud k závěru, že v dovolání obviněné R. H. nespatřuje žádný relevantní důvod se kterým by se nižší soudy nevypořádaly a že dle zjištěného stavu došlo k naplnění skutkové podstaty § 230 odst. 2 písm. c) trestního zákoníku a tím spácháním za vinu kladeného trestného činu. Pro nedůvodnost toto dovolání Nejvyšší soud zamítl.

#### 7.2.2.6 Datová schránka

Nejvyšší soud se v rozebíraném usnesení věnuje také otázkám spojených s datovou schránkou.

Dle zákona č. 300/2008 Sb. je datová schránka vymezena jako elektronické úložiště k dodávání dokumentů osob fyzických tak právnických. Dále uvádí

podrobnou technickou argumentaci, ze které vyvozuje závěr, že informační systém datových schránek je bez pochyby počítačovým systémem ve smyslu § 136a trestního zákoníku. Datovou zprávou bude potom tedy elektronický dokument v podobě datové zprávy nebo i elektronický nosič této datové zprávy, tj. obálka nebo tzv. „kontejner".

Mimo jiné na základě výše uvedeného formuloval Nejvyšší soud v tomto usnesení následující právní větu:

*„Za přečin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 2 písm. c) tr. zákoníku lze považovat jednání spočívající ve vyhotovení takové nepravdivé informace, která se stane obsahem datové zprávy a je zaslána jako příjemci jiné osobě do jí zpřístupněné datové schránky, neboť má povahu padělaného elektronického dokumentu. Jde o falšování údajů souvisejících s počítačovým systémem, které představuje obdobu padělání listin (nejen veřejných). U datové zprávy je třeba považovat za data uložená v počítačovém systému nejen vlastní odesílaný text obsažený v datové zprávě, ale veškeré informace, které se v rámci datové zprávy přepravují a doručují do datové schránky, a tedy i informaci, která je zřejmá z tzv. detailu zprávy (tzv. kontejneru, obálky).“* (Usnesení Nejvyššího soudu 8 Tdo 266/2017 ze dne 15. 8. 2018)

#### 7.2.2.7 Ústavní stížnost

V té samé věci podala odsouzená R. H. ústavní stížnost s cílem zrušit odsuzující rozhodnutí týkající se obvinění ze neoprávněného přístupu k počítačovému systému. Stěžovatelka argumentovala, že rozhodnutí obecných soudů, včetně Nejvyššího soudu, porušilo její základní právo na spravedlivý proces dle čl. 36 odst. 1 Listiny základních práv a svobod a dle čl. 6 odst. 1 Úmluvy o ochraně lidských práv a základních svobod.

V ústavní stížnosti stěžovatelka tvrdila, že rozhodnutí obecných soudů bylo v extrémním rozporu s principy spravedlnosti, projevovalo znaky svévole a porušilo její ústavně zaručené právo na spravedlivý proces. Jako další důvod uvedla také překvapivé rozhodnutím Nejvyššího soudu, který zamítl dovolání, i když provedl

výklad některých právních pojmů a doplnil argumentaci vztahující se k subjektivní stránce trestného činu.

Ústavní soud však odmítl ústavní stížnost s tím, že jeho pravomoc spočívá pouze v přezkumu rozhodnutí z hlediska dodržení ústavnosti. Nepřísluší mu zasahovat do hodnocení důkazů nebo skutkových zjištění provedených obecnými soudy. Stěžovatelka nenaznačila žádné zjevné nedostatky v rozhodnutích obecných soudů a opakovala argumenty, kterými se soudy již zabývaly. Ústavní soud rovněž zdůraznil, že není oprávněn provádět kasaci obecných soudů bez zjevných důvodů, což v tomto případě nebylo splněno. Ústavní soud ČR tak svým usnesením ze dne 14. 5. 2019 sp. zn. II.ÚS 3852/18 rozhodl o odmítnutí ústavní stížnosti a dal tak za pravdu soudům předchozích instancí.

### 7.2.3 Případ 3 – „Hacker z kamionu“

Předmětem této studie případ řidiče nákladního vozidla R. Š. obviněného z přečinu neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 2 písm. d) trestního zákoníku. Soudní řízení se odehrálo před Okresním soudem v Havlíčkově Brodě, který věc postoupil k projednání v přestupkovém řízení. Státní zástupkyně však byla přesvědčena o potřebě trestního postihu tohoto jednání, a proto věc byla řešena u nadřízeného krajského soudu v Hradci Králové, a nakonec u příslušného správního orgánu. Případ se věnuje problematice ochrany hodnot a společnosti prostředky trestního práva a trestněprávní kvalifikace deliktů souvisejících s manipulací s digitálními tachografy v silniční dopravě. Blíže je případ popsán v usnesení Krajského soudu v Hradci Králové 13 To 416/2017 ze dne 17. 10. 2017.

#### 7.2.3.1 Shrnutí soudního řízení

Okresní soud v Havlíčkově Brodě rozhodl usnesením o postoupení věci trestně stíhaného R. Š. pro přečin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 2 písm. d) trestního zákoníku k Městskému úřadu v Havlíčkově Brodě, odboru dopravy, protože posuzovaný čin by měl dle názoru soudu projednán jako přestupek.

Proti tomuto usnesení podala státní zástupkyně stížnost a věcí se tak zabýval nadřízený krajský soud v Hradci Králové. Usnesením Krajského soudu ze dne 17. 10. 2017, sp. zn. 13 To 416/2017, byla věc postoupena správnímu orgánu s poukazem na posouzení jako přestupek podle § 23 odst. 1 písm. f) zákona č. 200/1990 Sb., zákona o přestupcích. Krajský soud odmítl stížnost státní zástupkyně, která trvala na tom a argumentovala, že čin by měl být považován za trestný přečin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 2 trestního zákoníku.

#### 7.2.3.2 Skutková podstata

Obviněný R. Š., řidič nákladní soupravy byl obžalován ze spáchání trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 odst. 2 písm. d) trestního zákoníku, kterého se měl dopustit dne 27. 5. 2017 v čase od 12:19 do 13:29 hodin vložením karty jiného řidiče, konkrétně J. M. do digitálního tachografu. K tomu došlo po vyčerpání maximální povolené doby jízdy a s cílem zakrýt nedodržení bezpečnostní přestávky.

Při silniční kontrole byla z digitálního tachografu vyjmuta karta řidiče č. 00000000057OH000, vedená na jméno J. M., a došlo k uložení nepravdivých údajů o jízdě na tuto kartu. Tímto jednáním porušil obviněný nařízení Evropského parlamentu a Rady (EU) č. 165/2014[22], které upravuje tachografy v silniční dopravě a stanoví pravidla pro dodržování bezpečnostních přestávek.

#### 7.2.3.3 Stanovisko státní zástupkyně

Státní zástupkyně ve své stížnosti předložila rozsáhlou argumentaci ke svému stanovisku, že čin obviněného, který spočíval v neoprávněném vložení karty jiného řidiče do digitálního tachografu, by měl být považován za trestný přečin podle § 230 odst. 2 trestního zákoníku

[22] Nařízení Evropského parlamentu a Rady (EU) č. 165/2014 ze dne 4. února 2014 o tachografech v silniční dopravě, o zrušení nařízení Rady (EHS) č. 3821/85 o záznamovém zařízení v silniční dopravě a o změně nařízení Evropského parlamentu a Rady (ES) č. 561/2006 o harmonizaci některých předpisů v sociální oblasti týkajících se silniční dopravy Text s významem pro EHP

Státní zástupkyně zdůraznila význam dodržování předpisů týkajících se bezpečnostních přestávek při řízení nákladních vozidel. Tvrdila, že porušování těchto ustanovení právních norem zvyšuje riziko nehod a ohrožuje bezpečnost ostatních účastníků silničního provozu. Její názor spočíval v tom, že tato skutková podstata měla chránit zájem společnosti na tom, aby nedocházelo k neoprávněným zásahům do počítačových systémů a nosičů informací v nákladních vozidlech.

Dále zástupkyně obžaloby předložila soudu svou interpretaci digitálního tachografu jako počítačového systému *sui generis*[23] a karty řidiče jako nosiče informací. Argumentovala, že obviněný získal neoprávněný přístup ke kartě jiného řidiče a vložil ji do tachografu, což vedlo k nesprávným záznamům o jízdě. Takový krok podle ní splňoval znaky skutkové podstaty přečinu neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 odst. 2 písm. d) trestního zákoníku.

Státní zástupkyně zdůraznila, že skutková podstata trestného činu podle § 230 odst. 2 trestního zákoníku neobsahuje znak v podobě úmyslu způsobit škodu, jinou újmu nebo získat prospěch. Tvrdila, že tato skutková podstata má primárně chránit před neoprávněnými zásahy do počítačových systémů a nosičů informací, což je v souladu s principem subsidiarity trestní represe.

V dalším bodě se státní zástupkyně odvolala na rozhodnutí Nejvyššího soudu ze dne 19. 1. 2011, sp. zn. 5 Tdo 17/2011, kde je uvedeno, že závěr o nedostatečné společenské škodlivosti činu je možno učinit pouze výjimečně. Tento argument podporovala tím, že v případech, kdy není vhodné uplatňovat trestní represi, může být společenská škodlivost pouze jedním z hledisek pro rozhodnutí o trestní odpovědnosti (pozn. autora: procesně nelze zásada subsidiarity trestní represe aplikovat, ale musí dojít k rozhodnutí o tom, že daný skutek není trestným činem. Míra společenské škodlivosti musí být posouzena z hlediska kritérií obsažených v § 39 odst. 2 trestního zákoníku).

Závěrem upozornila na fakt, že obviněný zavinil vytvoření nesprávných záznamů o době jízdy, což mělo bezprostřední dopad na bezpečnost silničního

[23] z lat. překl. „svého druhu“

provozu, které není pouze otázkou dodržování právních norem a pravidel provozu na pozemních komunikací, ale i ochrany života a majetku účastníků silničního provozu.

Celkově vzato, státní zástupkyně formulovala zdůvodnění, které zdůrazňovalo závažnost jednání obviněného a jeho potenciální dopady na bezpečnost silničního provozu.

#### 7.2.3.4 Problematika aplikace § 230 odst. 2 trestního zákoníku u digitálních tachografů

Ústřední otázkou v tomto soudním procesu byla interpretace § 230 odst. 2 trestního zákoníku v kontextu digitálních tachografů. Krajský soud zdůraznil, že neoprávněné vložení karty jiného řidiče do tachografu není tak závažným činem, aby vyžadoval trestní postih.

Dále soud podotkl, že i když digitální tachograf může být vnímán jako specifický technologický systém, každý zásah do něj nemusí nutně splňovat kritéria pro trestní odpovědnost. Soud také zdůraznil, že tak jednoduchý způsob nesprávné obsluhy, jako je vložení karty jiného řidiče, není dostatečně sofistikovaným zásahem, aby oprávněně vyvolal trestní odpovědnost nebo naplnění skutkové podstaty obviněnému za vinu kladenému konkrétního trestného činu.

Rozsudek krajského soudu potvrzuje, že společenská škodlivost jednání obviněného nemusí automaticky vést k uplatnění trestní odpovědnosti. Přestože obviněný porušil pravidla bezpečnostních přestávek, jeho jednání bylo posouzeno jako přestupek. Projednáním a rozhodnutím v přestupkovém řízení lze zajistit dostatečné potrestání případně spáchaného přestupku a trestní právo by vždy mělo představovat prostředek *ultima ratio*.

Tento případ jasně ukazuje složitost aplikace trestního práva v kontextu moderních technologií a ukazuje na nutnost přizpůsobení právního rámce novým výzvám v oblasti silniční dopravy.

Na podobnou praxi a problematiku, kdy jsou za podobné manipulace s tachografy odsuzováni pachatelé dle úmyslných trestných činů § 230 odst. 2 upozorňuje i „Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky“ vydávaná Ministerstvem vnitra České republiky [49 s. 51].

Ta ve zprávě za rok 2022 udává, že komparativní analýza trestních spisů v oblasti počítačových trestných činů v roce 2015 v porovnání s rokem 2019 ukazuje, že počet kybernetické kriminality neroste tak rychle jak se předpokládalo a že byť statistické údaje vykazují nárůst počítačové kriminality až v desítkách procent ročně jedná se více než v polovině případů právě pachatelů odsouzených dle § 230 trestního zákoníku za manipulace s digitálním tachografem.

### 7.2.4 Případ 4 – „Sourozenecká pře“

Případ, který je podroben analýze, se zabývá trestním stíháním v kontextu neoprávněného přístupu k počítačovému systému a neoprávněného užití dat. Tento případ osvětluje soudní rozhodnutí Nejvyššího soudu, usnesení Nejvyššího soudu 7 Tdo 731/2015 ze dne 30. 9. 2015, kde byla posuzována obvinění v souvislosti s nedovoleným vstupem do facebookového profilu a manipulací s obsahem, včetně rozeslání soukromé korespondence poškozené, sestry obviněného. Soudní argumentace se zaměřuje na objektivní a subjektivní stránku trestného činu, zohledňuje námitky obhajoby a analyzuje, zda bylo splněno kritérium společenské škodlivosti v souladu se zásadou subsidiarity trestní represe. Představený rozbor případu tak přináší detailní pohled na právní aspekty spojené s kybernetickým porušením soukromí jednice a následným soudním projednáním.

#### 7.2.4.1 Shrnutí soudního řízení

Nejvyšší soud rozhodoval v neveřejném zasedání o dovolání obviněného praporčíka Bc. J. S. proti usnesení druhoinstančního soudu, Krajského soudu v Praze v trestní věci obžalovaného vedeného u Okresního soudu v Příbrami.

Obviněný byl shledán vinným přečinem neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 2 písm. a), b) trestního zákoníku. Rozsudek byl vynesen dne 25. listopadu 2014 a obviněný byl odsouzen k trestu odnětí svobody v trvání 3 měsíců, s podmíněným odložením výkonu trestu na zkušební dobu 12 měsíců.

Rozhodnutí Okresního soudu bylo následně potvrzeno Krajským soudem, který zamítl odvolání obviněného. Proti tomuto rozhodnutí podal obviněný dovolání k Nejvyššímu soudu s odvoláním na porušení zásady subsidiarity trestní

represe. Nejvyšší soud však dovolání obviněného pro zjevnou neopodstatněnost odmítl.

#### 7.2.4.2 Skutková podstata

Obviněný se provinil tím, že v listopadu 2013 neoprávněně vstoupil do facebookového profilu a emailové schránky své sestry, Ing. T. S., a provedl různé manipulace s daty, včetně změny přístupového hesla, nahrazení profilové fotografie logem hnutí „ANONYMUS“ (pozn. správně „Anonymous“) a rozeslání části její soukromé korespondence dalším uživatelům (nejméně 130 osobám - tzv. „přátelům“ poškozené) sítě Facebook. Toto jednání bylo motivováno disharmonickými vztahy v rodině. Trestného činu se dopustil z místa svého zaměstnání, jimž byl toho času dopravní inspektorát Policie ČR prostřednictvím proxy serveru Ministerstva vnitra ČR, kdy heslo k přístupu na email poškozené natipoval.

#### 7.2.4.3 Argumentace obviněného

J. S. argumentoval tím, že soudy nepřihlédly k okolnostem provázejícím skutek, zejména k jeho vztahu k poškozené, která byla jeho sestra. Tvrdil, že momentální konfliktní situace v rodině a vzájemné nedorozumění vedlo k neoprávněnému přístupu na její facebookový profil, podle něj toto jednání bylo spíše nedorozuměním než úmyslným trestným činem. Tvrdil, že společenská škodlivost jeho jednání byla minimální, a že soudy porušily zásadu subsidiarity trestní represe tím, že mu uložily trest odnětí svobody. Sestra obviněného podala trestní oznámení z důvodu, že se obávala útoku 3. osoby (nikoliv svého bratra) na její facebookový účet.

Obviněný v dovolání navrhoval soudu, aby rozhodnutí soudů prvého a druhého stupně zrušil a postoupil věc Městskému úřadu v Příbram k projednání v řízení o přestupku.

#### 7.2.4.4 Posouzení případu

Státní zástupce Nejvyššího státního zastupitelství ve svém vyjádření k dovolání tvrdil, že soudy již v odvolání věnovaly dostatečnou pozornost námitkám obviněného. Zdůvodňoval to tím, že trestný čin neoprávněného přístupu

k počítačovému systému není podmíněn souhlasem poškozené, a že v tomto případě byly splněny objektivní a subjektivní znaky trestného činu. Státní zástupce namítal, že skutek obviněného vedl k narušení internetového soukromí poškozené a trest odnětí svobody byl spravedlivý.

Nejvyšší soud se při zkoumaní případu zaměřil na dovolací důvod obviněného podle § 265b odst. 1 písm. g) trestního řádu, kterým tvrdil, že rozhodnutí soudu spočívá na nesprávném právním posouzení skutku nebo jiném nesprávném hmotně právním posouzení.

Dle usnesení Nejvyššího soudu byla objektivní stránka trestného činu naplněna, když pachatel získal přístup k počítačovému systému nebo nosiči informací a zároveň naplnil alespoň jednu z dalších okolností uvedených v § 230 odst. 2 trestního zákoníku.

Dalšími okolnosti bylo dle rozsudku soudu naplnění ustanovení písm. a), které spočívalo v neoprávněném užití uložených dat konkrétně korespondence poškozené, která byla jinak uchovávána v soukromí (neveřejně) a písm. b), zejména změnou přístupového hesla a změnou profilové fotografie.

Soud připomněl, že získání přístupu je definováno jako jednání umožňující pachateli volnou dispozici s počítačovým systémem nebo nosičem informací a využití jeho informačního obsahu. Získání může být neoprávněné nebo oprávněné, a nemá význam, z jakého důvodu k němu došlo.

Následně odmítl relevanci námitek obviněného ohledně toho, že mu poškozená sama poskytla přístupové údaje. To je proto, že obviněnému není kladeno za vinu neoprávněné získání přístupu, ale neoprávněné užití dat uložených v počítačovém systému. K tomu upřesnil a vysvětlil, že neoprávněné užití dat zahrnuje jakoukoli nedovolenou manipulaci s daty, například změnu, zkreslení, nebo rozeslání korespondence bez souhlasu oprávněné osoby.

Celkově soud dospěl k závěru, že obviněným spáchaný čin byl v souladu s trestním zákoníkem, a že společenská škodlivost byla dostatečně závažná na to, aby byla trestní odpovědnost uplatněna. Dále zdůraznil, že společenská škodlivost se posuzuje individuálně vzhledem ke všem okolnostem případu, a v tomto konkrétním případě byla vyhodnocena jako dostatečně významná.

Nejvyšší soud konstatoval, že dovolací námitky obviněného jsou opakováním již předložených argumentů, a že nepředkládá nové skutečnosti nebo právní názory, které by nebyly již projednány nižšími soudy. Dále vyřkl názor, že v případě trestního činu neoprávněného přístupu k počítačovému systému není podstatné, zda obviněný měl k poškozené nějaký osobní vztah, a že skutek byl naplněn v okamžiku neoprávněného vstupu na její facebookový profil.

Pokud jde o dovolací námitky týkající se údajného nedorozumění, Nejvyšší soud shledal, že soudy se námitkám obviněného věnovaly a řádně je posoudily a že soudy měly dostatek důkazů pro posouzení viny obviněného. Není tedy na místě zasahovat do jejich skutkového posouzení. Nejvyšší soud dospěl k závěru, že dovolání obviněného není opodstatněné, a proto jej zamítl.

Tím bylo rozhodnuto, že obviněný zůstává odsouzen k trestu odnětí svobody ve výši 3 měsíců s podmíněným odložením výkonu trestu na zkušební dobu 12 měsíců.

### 7.2.5 Závěrem k § 230 odst. 2 trestního zákoníku

Výše analyzované případy přinášejí komplexní pohled na otázky spojené s různými aspekty právní kvalifikace dle § 230 odst. 2 trestního zákoníku, kdy obecně lze za hlavní společný znak těchto kauz považovat zapojení moderních technologií při páchání trestné činnosti a reakci právního sytému České republiky na nové výzvy a problémy spojené s aplikací práva v digitálním prostoru.

Soudy při svém přezkumu zdůraznily důležitost ochrany integrity a dostupnosti dat jako jeden se sekundárních objektů, které ustanovení § 230 odst. 2 trestního zákoníku chrání a společenskou škodlivost neoprávněného zásahu do počítačového systému nebo nosiče informací.

První a čtvrtý případ pak obzvláště akcentovaly potřebu chránit digitální soukromí jednotlivců, a to konkrétně v daných případech zpřístupňování soukromé korespondence poškozených dalším osobám.

Dále se soudy opakovaně zabývaly otázkou naplnění požadavku způsobení škody nebo jiné újmy, nebo i možné ohrožení tímto účinkem a dospěly k závěru, který byl několikrát potvrzen Nejvyšším soudem, že pro naplnění tohoto trestného činu není tento znak obligatorní.

Případ druhý potom kromě dalšího reaguje na problematiku širokého spektra zařízení a systémů, které mohou naplňovat výkladové definice počítačového systému vyjádřené ve skutkové podstatě přečinu což bylo demonstrováno na informačním systému datových schránek.

Ve dvou z uvedených případů byli obvinění příslušníci útvarů Policie ČR což jenom potrhovalo společenskou závažnost jejich jednání a soudem k tomu bylo přihlédnuto. Vyvozovat další závěry o míře podobné kriminality u policistů však z provedených studií nelze.

Častým argumentem obviněných v odvolacím či dovolacím řízení byla nedostatečná aplikace § 12 odst. 2 trestního zákoníku, tedy zásady subsidiarity trestní represe. Soudy však aplikaci této zásady však podmiňují velmi specifickými a konkrétními okolnostmi, které její aplikaci dostatečně odůvodňují. Trestnost trestného činu je vyjádřena obsažením skutkové podstaty v trestním zákoníku, a právě toto je hlavním kritériem pro určení trestnosti. Jak ale ukázal případ manipulace s tachografy, soud zde stanovuje pomyslnou limitu, kdy je třeba vyzdvihnout užití prostředků trestního práva jako *ultima ratio*, kdy je třeba zvážit možné sankce dle jiných právních předpisů – především veřejnoprávních a dostatečnost projednání deliktního jednání v nich.

Celkově byla v analyzovaných případech ukázána nutnost ochrany dat a systémů, ale i adaptabilita právního rámce. Přestože obvinění někdy argumentovali technickou jednoduchostí či absencí úmyslu, soudy ve svých rozsudcích zdůraznily, že efektivní právní rámec by měl reflektovat dynamiku moderních technologií a udržovat se aktuální v reakci na nový vývoj a trendy.

## 7.3 Rozbor rozhodnutí k § 231 trestního zákoníku

Jedním z relevantních ustanovení trestního zákoníku v oblasti kybernetické kriminality je § 231[24].

[24] § 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

Tato kapitola se zaměřuje na analýzu § 231 trestního zákoníku, zejména v kontextu dvou konkrétních případů kybernetických trestných činů. V následujících odstavcích budou rozebrány skutkové podstaty obou případů, právní posouzení ustanovení § 231, a také argumentace obviněných a soudů ve světle příslušných soudních rozhodnutí. Kapitola tak poskytne hlubší vhled do praktické aplikace § 231 trestního zákoníku v konkrétních soudních případech a přispěje k porozumění právnímu prostředí v oblasti kybernetické kriminality v České republice.

### 7.3.1 Případ 1 – „Kybernetické vydírání Andreje Babiše“

Tato podkapitola se zaměří na analýzu soudního procesu, který se týkal obviněného Romana H. a jím spáchaných kybernetických trestných činů v období od července do listopadu 2016. Státní zástupce obvinil Romana H. z vydírání, neoprávněného přístupu k počítačovému systému a nosiči informací a opatření a přechovávání přístupového zařízení a hesla. Studie se zaměřuje na průběh soudního řízení, skutkovou podstatu případu a klíčové otázky spojené s místní příslušností soudu při kybernetických trestných činech. V kontextu rozhodnutí o příslušnosti soudu a skončení případu výrokem Okresního soudu v Ostravě bude demonstrováno, jak se právní systém vyrovnává s výzvami představovanými

---

(2) Kdo vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává

a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části nebo k neoprávněnému zásahu do počítačového systému nebo nosiče informací, nebo
b) počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části,

v úmyslu, aby jej bylo užito ke spáchání trestného činu porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b) nebo c) nebo trestného činu neoprávněného přístupu k počítačovému systému a neoprávněného zásahu do počítačového systému nebo nosiče informací podle § 230 odst. 1 nebo 2, bude potrestán odnětím svobody až na dvě léta, propadnutím věci nebo zákazem činnosti.

*(zákon č. 40/2009 Sb., trestní zákoník)*

sofistikovanými kybernetickými delikty a jaké důsledky měly tyto činy pro obviněného a postižené subjekty, včetně známého politika Andreje Babiše.

Rozbor vychází z usnesení Nejvyššího soudu 7 Td 28/2018-7 ze dne 30. 5. 2018 a připojených mediálních článků.

#### 7.3.1.1 Shrnutí soudního řízení

Obžaloba proti obviněnému Romanovi H. podaná státním zástupcem Obvodního státního zastupitelství pro Prahu 4 k Obvodnímu soudu pro Prahu 4. Obviněnému je kladeno za vinu, že se dopustil přečinu vydírání dle § 175 odst. 1 trestního zákoníku a přečinu neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 2 písm. b), odst. 3 písm. b) trestního zákoníku, ve formě účastenství a přečinu opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat podle § 231 odst. 1 písm. a) trestního zákoníku.

Obvodní soud pro Prahu 4 se obrátil usnesením ze dne 30. 4. 2018 na Nejvyšší soud, coby nejblíže společný nadřízený soud k rozhodnutí o místní příslušnosti (resp. nepříslušnosti) soudu, kdy překládající soud dospěl k názoru, že není k projednání věci místně příslušný a že by věc měla být řešena u Okresního soudu v Ostravě, nebo Obvodního soudu pro Prahu 1, případně Okresního soudu Praha-Západ, v jehož obvodě měl poškozený Andrej Babiš toho času trvalé bydliště. Nejvyšší soud se v předmětném rozhodnutí zabývá stručně skutkovou stránkou případu v rovině k potřebné k posouzení místní příslušnosti. Výsledkem řízením před Nejvyšším soudem dle § 24 odst. 1 trestního řádu je usnesení 7 Td 28/2018-7 ze dne 30. 5. 2018, kdy se soud usnesl je k projednání věci je příslušný Okresní soud v Ostravě a to dle § 18 odst. 1 trestního řádu, kdy vyplynulo, že právě v jeho obvodu byl trestný čin spáchán.

#### 7.3.1.2 Skutková podstata

Skutková podstata případu pojednává o sérii kybernetických trestných činů, kterých se obviněný Roman H. hlásící se k celosvětové hackerské skupině Anonymous dopustil v období od července do listopadu 2016.

Prvním činem bylo vydírání (§ 175 odst. 1 trestního zákoníku) tehdejšího ministra financí Andreje Babiše prostřednictvím nátlaku na zrušení určitých ustanovení zákona o hazardních hrách. Obviněný nejprve zveřejnil výhrůžné vzkazy na hackerských facebookových skupinách (Anonymous#Opdestruction) vystupující pod přezdívkou M. A. S., obsahující výzvy k zrušení konkrétních zákonů a ustanovení doplněné fotografiemi manželky a dětí Andreje Babiše Dále následovala hrozba zveřejnění osobních údajů a fotek dcery Andreje Babiše, které měly být získány nabouráním se do jejího facebookového profilu, na pornografickém serveru Pinkmeth.

Druhým trestným činem (§ 230 odst. 2 písm. b), odst. 3 písm. b) trestního zákoníku) byla organizace kybernetického útoku typu DDoS. Obviněný Roman H. vyzval na sociálních médiích k provedení útoku na několik vládních a vojenských webových stránek (konkrétně: www.vlada.cz, www.mfcr.cz, www.vlada.gov.sk, www.finance.gov.sk, www.army.cz, www.mil.sk, www.naseslovensko.net) a následně tento útok koordinoval důsledkem čehož došlo k výpadku na internetových stránkách Úřadu vlády ČR.

Třetím trestným činem (§ 231 odst. 1 písm. a) trestního zákoníku) bylo šíření (distribuce) škodlivého software určeného právě k provedení v předchozím odstavci popsaných kybernetických útoků. Obviněný sám nainstaloval škodlivý software a dále jej nabízel ke stažení zájemcům, kteří se chtěli účastnit kybernetických útoků. Tímto jednáním naplnil skutkovou podstatu ustanovení § 231 trestního zákoníku.

Celý případ odhaluje sofistikované a nebezpečné chování obviněného, který využil internetové platformy k vydírání a organizaci kybernetických útoků a distribuci škodlivého software, nástrojů a postupů k provedení DDoS útoku na vybrané cíle.

#### 7.3.1.3 Místní příslušnosti soudu u kybernetických trestných činů

Místní příslušnost soudu pro projednání trestného činu je zásadním aspektem v každém trestním řízení. V případě obviněného Romana H. bylo rozhodnuto, že trestné činy byly spáchány v místě jeho trvalého bydliště v Ostravě, což stanovuje místní příslušnost soudu dle § 18 odst. 1 trestního řádu.

Obviněný se měl dopustit tří trestných činů, z nichž všechny byly úzce spojeny s jeho počítačem a kybernetickými aktivitami. Tím, že měl obviněný ve svém počítači nainstalovaný software umožňující kybernetické útoky, bylo místo trvalého bydliště rozhodujícím prvkem pro předložení věci soudu, který má místní příslušnost. Kdy daný hardware a software byl fakticky tím místem, kde byla trestná činnost páchána. V tomto konkrétním případě měl být trestný čin spáchán v obvodu Okresního soudu v Ostravě, kde bylo zajištěno trvalé bydliště Romana H. Místní příslušnost byla rovněž uvažována pro případ projevů následků trestného činu, které se týkaly též Ministerstva financí ČR a Úřadu vlády ČR s adresou na Praze 1 (Obvodní soud pro Prahu 1). Vzhledem k distančnímu charakteru většiny činů v kyberprostoru, kdy může být místo, kde následek nastal, odlišné od místa, kde došlo k samotnému jednání, bylo nutné brát v úvahu i místo, kde následek měl nastat.

Celkově lze konstatovat, že v případech kybernetických trestných činů může být místní příslušnost složitější na určení, zejména pokud se jedná o distanční delikty, kde jednání a následky nejsou fyzicky spojeny. Rovněž je zde důležité zohlednit, kde obviněný trvale žije a kde měl svůj počítač, ze kterého činy spáchal. V případě, kdy se nepodaří naplnit požadavky místní příslušnosti § 18 odst. 1 trestního řádu je nutné postupovat kaskádovitě dle odst. 2 téhož ustanovení.

#### 7.3.1.4 Skončení případu

Po určení místní příslušnosti Okresního soudu v Ostravě byl případ projednán v neveřejném zasedání, kde bylo rozhodnuto o vině a trestu obviněného trestním příkazem, ve kterém mu byl stanoven podmíněný trest odnětí svobody v délce trvání 1 roku se zkušební dobou v délce 2 let. Vedle hlavního trestu byl Romanovi H. uložen i vedlejší trest propadnutí věci – osobního počítače, dle § 70 trestního zákoníku. Případ byl vzhledem k dotčení známého politika a představitele vlády sledován i v mediálních článcích, kde se poškozený Andrej Babiš a orgány činné v trestním řízení opakovaně vyjadřovali k danému případu i na další související podobné kybernetické útoky a kauzy [50–52].

### 7.3.2 Případ 2 – „Mladistvý hacker“

V případu „Mladistvý hacker“ je analyzováno soudní řízení, jehož hlavní postavou je mladistvý X obviněný z kybernetických trestných činů. Soudní proces se týkal neoprávněného přístupu k počítačovému systému a nosiči informací, resp. pokusu o tento přístup a opatření a přechovávání přístupových údajů. Tato analýza se zaměří na různé aspekty konkrétního trestního procesu, skutkovou podstatu obvinění a argumentaci obviněného, který se snažil vyvrátit rozhodnutí soudu. Pro tuto studii je vycházeno z usnesení Nejvyššího soudu, soudu pro mládež, 8 Tdo 100/2019-35 ze dne 13. 2. 2019.

#### 7.3.2.1 Shrnutí soudního řízení

Mladistvý X byl obviněn z provinění neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, odst. 3 písm. b) trestního zákoníku ve stadiu pokusu podle § 21 odst. 1 trestního zákoníku a opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat podle § 231 odst. 1 písm. a) trestního zákoníku, za což byl rozsudkem Okresního soudu v Rychnově nad Kněžnou, soudu pro mládež, ze dne 30. dubna 2018 podle § 230 odst. 3 trestního zákoníku ve spojení § 31 odst. 1 zákona č. 218/2003 Sb., o soudnictví ve věcech mládeže a § 43 odst. 1 trestního zákoníku odsouzen k úhrnnému trestnímu opatření odnětí svobody v trvání osmi měsíců s podmíněným odložením na zkušební dobu v trvání dvaceti měsíců. Vedle hlavního trestního opatření mu bylo uloženo vedlejší trestní opatření spočívající v propadnutí věci představující veškeré vnitřní vybavení v zajištěném stolním počítači.

Mladistvý X se proti rozsudku Okresního soudu odvolal, avšak Krajský soud v Hradci Králové, soudu pro mládež, dne 26. září 2018 odvolání zamítl jako nedůvodné. Mladistvý se následně podal dovolání k Nejvyššímu soudu, soudnímu orgánu pro mládež, který ve svém neveřejném zasedání dne 13. února 2019 rozhodl o odmítnutí dovolání mladistvého pro jeho nedůvodnost.

#### 7.3.2.2 Skutková podstata

Ve věci trestného jednání mladistvého X byla soudem zkoumána rozsáhlá skutková podstata, která zahrnovala několik klíčových prvků a aktivit.

Prvním důležitým aspektem byla instalace škodlivého software na počítač mladistvého. Tento software, který obviněný nainstaloval, sloužil k provedení různých forem kybernetických útoků. Mezi jeho hlavní funkce patřilo neoprávněné získávání přístupu k cílovým počítačovým systémům a nosičům informací.

Jedním z konkrétních útoků spojených s obviněním byl DDoS útok ze dne 16. 6. 2016 v 12:32 na internetové stránky České strany sociálně demokratické (ČSSD) – www.cssd.cz za užití výše uvedeného software. Tento útok měl za cíl zahlcovat server strany velkým objemem falešných požadavků, což mělo vést k omezení dostupnosti webových stránek. Správcům internetové stránky se však podařilo tento útok odvrátit a webová stránka tedy zůstala po celou dobu funkční a nevznikla žádná přímá škoda.

Dalším bodem obvinění bylo provádění SQL Injection útoků. Mladistvý byl podezřelý ze vkládání škodlivého SQL kódu do vstupních polí webových formulářů nebo URL adres. Tímto způsobem se snažil obejít bezpečnostní opatření a získat neoprávněný přístup k databázovým systémům, s cílem manipulovat s elektronickými daty.

Obviněnému bylo rovněž kladeno za vinu používání nástrojů na prolomení hesel. Tyto nástroje mu umožňovaly neoprávněný přístup k chráněným účtům a systémům. Kombinací těchto nástrojů a technik mladistvý systematicky obešel zabezpečení a získal přístup k citlivým informacím.

Naplněním skutkové podstaty § 231 trestního zákoníku spočívající v přechovávání přístupových zařízení a hesel k počítačovým systémům prokázal nejen své schopnosti v kybernetickém prostoru, ale i ochotu a připravenost (úmysl) užít tyto prostředky k dlouhodobému neoprávněnému přístupu k systémům a sítím, tj. spáchat trestné činy dle § 182 nebo § 230 trestního zákoníku, kdy v druhém uvedeném byl dokonce shledán vinným ve formě pokusu.

#### 7.3.2.3 Argumentace obviněného

Obviněný ve svém dovolání a vyjádření k němu, které předložil Nejvyššímu soudu, argumentoval několika klíčovými body, které se týkaly právního posouzení skutku, provedeného důkazního řízení a následně i samotného rozsudku.

V prvním sledu byla obhajoba mladistvého X. postavena na nesprávné právní kvalifikaci skutku, kdy obviněný tvrdil, že soudy nesprávně kvalifikovaly jeho jednání jako trestný čin, respektive provinění neoprávněného přístupu k počítačovému systému. Argumentoval tím, že skutek měl být posouzen ve § 226 písm. a) trestního řádu, tedy že na základě předložených důkazů nebylo prokázáno, že se skutek stal.

Dále obviněný zdůrazňoval, že ve své obhajobě u prvoinstančního soudu poukázal na možnost, že do jeho počítačového systému se mohla nabourat jiná osoba. Tuto možnost podporoval tvrzením, že to sám vypracovaný znalecký posudek zcela nevylučuje a že soudy dostatečně nereflektovaly tuto možnost a řádně se s ní nevypořádaly. Ve vtahu ke znaleckému posudku bylo X upozorňováno na údajnou zaujatost znalce Ing. Jiřího Bergera, MBA, který vypracoval znalecký posudek. Tvrdil, že jeho vyjádření bylo příliš kritické a neobjektivní. Zpochybňoval serióznost posudku a tvrdil, že znalec nespravedlivě kritizoval jeho jednání, a dokonce se jej snažil „mentorovat“ a poučovat.

Nesprávná právní kvalifikace skutku podle § 230 trestního zákoníku záležela dle obhajoby v tom, že soudy nesprávně aplikovaly ustanovení § 230 trestního zákoníku při kvalifikaci jeho jednání. Tvrdil, že programy nalezené v jeho počítači mohly být využity i k legitimním a legálním účelům, tj. ochraně vlastního počítače před podobnými útoky.

Obviněný trval na tom, že soudy měly respektovat zásadu *in dubio pro reo*, což znamená, že v případě pochybností by mělo být rozhodnuto ve prospěch obviněného. Argumentoval tím, že jeho obhajoba nebyla dostatečně zvážena a že soudy nerespektovaly tuto zásadu.

Celkově vzato, obviněný se snažil přesvědčit Nejvyšší soud o tom, že původní soudní rozhodnutí trpělo vážnými procesními a právními vadami.

#### 7.3.2.4 Vyjádření k dovolání

Nejvyšší soud se s argumentací obviněného mladistvého neztotožnil a v jeho dovolání nenalezl žádný z přípustných dovolacích důvodů, a to, jak ten, který dovolatel sám uvádí, tak kterýkoliv jiný.

Nejvyšší soud, coby soud dovolací nesouhlasí s tvrzením obhajoby, že se s jí předloženými argumenty nebylo dostatečně vypořádáno a že zde nevidí žádný, a už vůbec ne, extrémní rozpor mezi skutkovými zjištěními soudů v daném trestním řízení a provedenými důkazy. Naopak vyzdvihl precizní odůvodnění soudu odvolacího, proč k zamítnutí odvolání přistoupil a že z provedených důkazů – mimo jiné oznámením o kybernetickém útoku, zprávou poskytovatele internetového připojení k identifikaci IP adresy pachatele, vypracovaným znaleckým posudkem a výslechem znalce, skutkový stav jasně vyplývá.

K obhajobou označovanému nestandardnímu vyjadřování znalce Nejvyšší soud zdůraznil, že v trestním řízení ve věci mladistvých je toto zcela akceptovatelné, a to zejména pro výchovný účel tohoto řízení.

*Obiter dictum*[25] soud vyslovil názor, že skutková zjištění popsaná v rozsudcích prvoinstančního a odvolacího soudu přesvědčivě naplňují znaky provinění, které jsou mladistvému kladeny za vinu.

### 7.3.3 Závěrem k § 231 trestního zákoníku

Oba případy poskytují pohled na páchání trestného činu podle § 231 trestního zákoníku. Skrze tyto případy lze identifikovat vzorce chování pachatelů, včetně konkrétního využívání kybernetických nástrojů a technik – „hackerských nástrojů“ pro účely páchání další kriminality. Skutkové podstaty obou případů jasně (avšak v odlišnostech) demonstrují definici trestného činu podle § 231 trestního zákoníku a jeho výskyt v souběhu s jinými trestněprávně relevantními činy.

Lze říci, že případy páchání trestného činu podle § 231 trestního zákoníku ilustrují potřebu zakotvení takovéto právní úpravy k boji s kybernetickou

[25] z lat. překl. „řečeno na okraj“ – jedná se o neautoritativní část rozhodnutí soudu, která slouží k dokreslení odůvodnění anebo jako vodítko pro další obdobné situace.

kriminalitou. A zároveň je nezbytné dodatečně a včasně modernizovat a posilovat tyto a podobné právní nástroje, tak aby postih kriminality v kyberprostoru byl efektivní a možný.

# 8 Shrnutí a diskuse výsledků

## *8.1 Shrnutí hlavních výsledků*

Provedená případová studie kybernetické kriminality zaměřující se na ustanovení § 230 odst. 1, § 230 odst. 2 a § 231 trestního zákoníku přináší podrobný pohled na problematiku kybernetických trestných činů v prostředí České republiky a popisuje reakce právního systému na tyto nové formy kriminality v kyberprostoru.

### 8.1.1 Závěry k § 230 odst. 1

Analýza trestné činnosti dle § 230 odst. 1 odhalila, že neoprávněný přístup k počítačovým systémům a narušení soukromí mohou být motivovány nejen obvyklými cíli profesionálních hackerů, ale i osobními konflikty a žárlivostí v soukromém životě. Také hovoří o možných způsobech zabezpečení počítačových systémů a dat a možnostech jejich překonání, které mohou představovat porušení norem trestního práva.

Získané výsledky poukazují na to, že narušování důvěrnosti dat není omezeno pouze na profesionální „hackery“ a útočníky třetích stran. Často se jedná o případy neoprávněných přístupů a narušení soukromí v osobních vztazích nebo rodinném kruhu. Překonání bezpečnostních opatření, jako jsou hesla, PIN kódy nebo biometrická data, může vést k trestní odpovědnosti pachatele.

Výzkum potvrzuje, že narušování přístupu může být spojeno s domácím násilím a psychickým týráním, což zdůrazňuje významné sociální a morální aspekty kybernetické kriminality v kontextu § 230 odst. 1 trestního zákoníku.

### 8.1.2 Závěry k § 230 odst. 2

Rozbor případů k § 230 odst. 2 trestního poskytuje komplexní pohled na právní kvalifikaci trestné činnosti dle tohoto ustanovení.

Soudy zdůrazňují důležitost ochrany integrity a dostupnosti dat jako které jsou chráněny právě § 230 odst. 2 trestního zákoníku.

Dále soudy opakovaně rozebírají otázku požadavku na způsobení škody nebo jiné újmy, přičemž judikují, že pro naplnění trestného činu podle § 230 odst. 2 není tento znak přítomen. Případ druhý rozšiřuje pohled na různá zařízení a systémy, které mohou spadat pod definici počítačového systému, což bylo demonstrováno na případu informačního systému datových schránek.

Soudy se rovněž zabývaly argumenty obviněných týkajících se nedostatečné aplikace zásady subsidiarity trestní represe podle § 12 odst. 2 trestního zákoníku. Výsledky naznačují, že soudy podmiňují aplikaci této zásady konkrétními a specifickými okolnostmi, které její uplatnění zdůvodňují.

### 8.1.3 Závěry k § 231

Provedená analýza § 231 trestního zákoníku na základě dvou případů poskytuje důkladný pohled na páchání trestné činnosti spojené s kyberprostorem. Tyto případy umožňují identifikovat vzorce chování některých pachatelů a specifické metody, které využívají při spáchání trestného činu, včetně užívání „hackerských nástrojů“ pro další formy kriminality.

Skutkové podstaty obou případů jasně ilustrují definici trestného činu podle § 231 trestního zákoníku a ukazují jeho souběh s dalšími trestnými činy. Tato zjištění podtrhují potřebu a důležitost právní úpravy v oblasti kybernetické kriminality, která by měla být neustále modernizována a posilována tak, aby byla schopná efektivního postihu pachatelů v kyberprostoru.

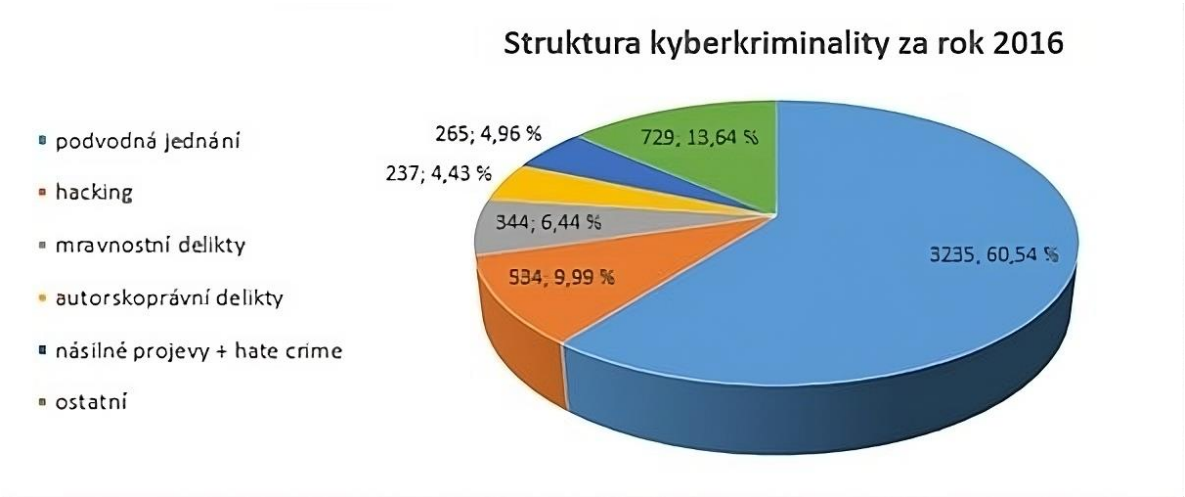
## *8.2 Trestních postih trestných činů dle § 230 odst. 1, odst. 2 a § 231 trestního zákoníku v praxi*

Před tím, než budou předložena konkrétní data k jednotlivým paragrafům trestního zákoníku lze na kybernetickou kriminalitu pohlédnout více obecně – tedy jako na souhrn všech trestných činů páchaných v kyberprostoru. Podkladem pro tento pohled může být zpráva o „Vývoji registrované kriminality v roce 2022“ ze 13. ledna 2023 uveřejněná na webu Policie ČR [53]. Zde je třeba v prvé řadě uvést, že registrovaná kriminalita vyjadřuje počet skutků, které Policie ČR na území

země zaznamenala, nejčastěji tedy takové, o kterých se dozvěděla a zahájila prošetřovací úkony z úřední povinnosti nebo na základě podaných trestních oznámení. Nejedná se tedy o počet vyjadřující počet objasněných případů, naplňující znaky trestného činu anebo počet odsouzených v těchto trestní věcech. Vymezení kybernetické kriminality, se kterou zpráva pracuje je také podstatně širší než vymezení kybernetických trestných činů v této práci, i přes to však dobře poslouží pro ilustraci celkových trendů.

Kriminalita páchaná v kyberprostoru již dlouhodobě dosahuje vysokého meziročního růstu a konkrétně pro rok 2022 tvořila 10,2 % celkové registrované kriminality celkem s 18 554 skutky. Více než 53 % meziroční nárůst byl zaznamenán v oblasti tzv. „hackingu".

Pro srovnání lze uvést i graf struktury kyberkriminality za rok 2016, kdy počet takto klasifikované registrované kriminality představoval 5 401 skutků.




Obr. 3 Struktura kyberkriminality za rok 2016.
Zdroj: POLICIE ČR, *Jednotlivé druhy kyberkriminality* [42]

Pokud budou dále uvedeny konkrétní informace o počtu odsouzených a druzích a délce ukládaných trestů je opět vycházeno z dat projektu jaktrestame.cz a to v nejvíce širokém nastavení filtru, které ale zachycuje naplnění skutkových podstat daných trestných činů, to znamená: sledované období let 2016-2022, s jakýmkoliv počtem předchozích odsouzení vč. „prvopachatelů", v souběhu s jinými trestnými činy i bez a bez rozlišení pohlaví odsouzených.

K § 230 odst. 1 uvádí statistika celkem 32 odsouzených, kdy v 19 případech byl uložen podmíněný trest odnětí svobody, u 7 odsouzených uložen peněžitý trest, ve 3 případech byl uložen trest obecně prospěšných prací a pouze 1 pachatel byl odsouzen k trestu odnětí svobody.

U odst. 2 § 230 je zaznamenáno celkem 528 případů odsouzení, kdy ve více než polovině případů byl uložen podmíněný trest odnětí svobody, druhým nejčastějším trestem byl trest peněžitý. Nepodmíněné tresty odnětí svobody (vč. tzv. „s dohledem“) byly uloženy 48 pachatelům.

Statistický výstup k postihu dle § 231 není v aplikaci dostupný. To může být pravděpodobně způsobeno tím, že pachatelé, kteří páchají trestný čin dle tohoto paragrafu jsou často odsouzeni ve formě souběhu více trestných činů, často právě dle § 230 odst. 2, kdy podle pravidla obsaženého v § 43 odst., kdy je trest ukládán za trestný čin, který je nejpřísněji trestný a souběžné trestné činy se projeví jako přitěžující okolnost ve smyslu § 42 písm. n). V tomto případě tak budou ukládány tresty dle § 230 odst. 2, což se ve statistice odsouzených za jednotlivé trestné činy jejich tresty projeví právě vyprázdněním této množiny.

## *8.3 Odpovědi na výzkumné otázky*

**1) Jaký je relevantní právní rámec kybernetické kriminality v českém trestním právu?** Trestní právo je v České republice upraveno v základních dvou zákonech, a to: trestním zákoníku, kde je upraveno právo hmotné, a trestním řádu, kde je upraveno právo procesní. Tyto zákony tvoří základní rámec a specifické případy, jako je třeba trestní odpovědnost právnických osob, jsou upraveny ve zvláštních zákonech. Kybernetická kriminalita a její hmotněprávní vymezení je obsaženo v trestním zákoníku, konkrétně v §§ 230–232, kdy tato ustanovení představují kromě dalšího i implementací závazků vyplývající z mezinárodních právních dokumentů, zejména Úmluvy o kybernetické kriminalitě.

**2) Jak jsou vymezeny jednotlivé trestné činy a jaká jsou specifika jednotlivých trestných činů a čím se od sebe jednotlivé skutkové podstaty odlišují?** Vymezení jednotlivých trestných činů je obsaženo v textu ustanovení 230-232 trestního zákoníku, kde je vymezena celá právní norma perfektně, tj. včetně hypotézy, dispozice i sankce.

Trestné činy vyjádřené § 230 v odst. 1 cílí na kybernetickou trestnou činnost spočívající v překonávání bezpečnostních opatření zařízení ICT, v odst. 2 neoprávněné nakládání s zařízeními ICT a daty, § 231 obsahuje postih vztahující se k „hackerským nástrojům“ a § 232 směřuje na nedbalostní trestné činy spojené především s porušením jiné právní povinnosti.

3**) Jak ve zjednodušené podobě probíhá trestní soudní proces?** Po podání obžaloby státním zástupcem je věc projednávána v hlavním líčením u soudu prvního stupně, proti rozsudku tohoto soudu lze podat řádný opravný prostředek (podaný před právní mocí rozhodnutí) – odvolání. Odvoláním obžalovaného se zabývá soud vyšší instance, což je v soustavě obecných soudů v České republice v případě soudů okresních soud krajský a v případě soudů krajských soud vrchní.

Proti rozhodnutí odvolacího soudu je přípustný ještě přípustný mimořádný opravný prostředek (podaný po právní moci rozhodnutí, který je bez suspenzivního účinku) – tak jak byl v analyzovaných případech většinově uplatňován, dovolání. Dovolání je prostředek s centralizovaným devolutivním účinkem, kdy o věci rozhoduje Nejvyšší soud, které může být podáno pouze státním zástupcem nebo prostřednictvím obhájce. Jak pro odvolání, tak dovolání je potřebné naplnit důvody a požadavky těchto úkonů, které jsou stanoveny v zákoně. Pravomoc odvolacích a dovolacích soudů, včetně formy a znění možného rozhodnutí o věci je blíže upraveno v trestním řádu.

**4) Na jaká úskalí nebo s jakými specifickými otázkami se musely soudy v řízení vypořádat?** Jedním z klíčových aspektů byla technická komplexnost kybernetických trestných činů. Soudy se musely vypořádat s náročným úkolem interpretace technických detailů a důkazů, zejména v případech, kde šlo o složité mechanismy kybernetických útoků na počítačové systémy.

Další výzvou bylo stanovení správné právní kvalifikace trestných činů. Soudy byly konfrontovány s otázkou, zda skutková podstata daného případu odpovídá definici kybernetického trestného činu podle příslušných paragrafů, například § 230 odst. 1, § 230 odst. 2, nebo § 231 trestního zákoníku. Tato otázka vyžadovala pečlivé zhodnocení konkrétních okolností každého případu a naplnění znaků skutkových podstat.

V případech trestních činů podle § 230 odst. 2 byla posuzována škoda nebo újma způsobená kybernetickým útokem. Soudy podrobně zkoumaly, zda je právě toto právní kvalifikační kritérium – znak skutkové podstaty.

Zásada subsidiarity trestní represe (§ 12 odst. 2) může být vnímána jako další komplexní téma pro soudní orgány. Soudy musely posoudit, zda byla správně aplikována tato právní zásada v kontextu konkrétních skutkových okolností a argumentů stran. Důkladná analýza materiálu z trestních spisů byla nezbytná pro spravedlivé rozhodnutí soudu.

Celkově lze říci, že soudní řízení v oblasti kybernetické kriminality přináší specifické výzvy, které vyžadují komplexní a inovativní přístup k právu. Soudy se musí neustále adaptovat na nový technologický a právní vývoj s cílem zajistit spravedlivá a účinná rozhodnutí v rámci digitálního prostoru.

**5) Jaké hodnoty chrání ustanovení trestního zákoníku o počítačových trestných činech?** Z výsledků případové studie vyvstává otázka, zda chráněné objekty skutkových podstat, tak jak jsou vyjádřeny v trestním zákoníku odpovídají skutečnosti a praxi v soudním rozhodováním. Ochrana majetku, vyplývající z doktríny, teoretické části této práce a systematickému výkladu trestního zákoníku a příslušných hlav nemusí být převládající chráněnou hodnotou. Pří výkladu právních norem a v odůvodnění rozhodnutí se opakovaně objevují názory, kdy je společenským zájmem ochrana soukromí, integrita, dostupnost dat a legitimní a legální přístup k nim. Zájmy vztahující se k datům a jejich užití mohou být jistě vykládána i v souladu s majetkovým objektem, byť škoda nebo jiná újma se u nich nevyžaduje, ale ochrana soukromí spadá systematicky spíše do hlavy II. „trestné činy proti svobodě a právům na ochranu osobnosti, soukromí a listovního tajemství“.

**6) Jakým způsobem se mění povaha kybernetické kriminality a aplikace práva soudem s postupem technologického vývoje?**

Prvním významným prvkem je exponenciální rozvoj moderních technologií a ICT, které přináší nové formy kybernetických hrozeb. Nové technologie, které sice nebyly obsaženy v analyzovaných rozhodnutích, ale jejich uvedení je nabíledni, jako jsou umělá inteligence, blockchain, a internet věcí (IoT), posouvají hranice možností jak pro kybernetické pachatele, tak pro právní systém. Soudy se musí vypořádat

s technickou komplexitou kybernetických trestných činů a rychle se adaptovat na nové formy trestné činnosti v kyberprostoru.

Globalizace kybernetické kriminality se stává stále výraznějším trendem. Pachatelé mohou operovat na globální úrovni a kdekoliv na světe, což zvyšuje obtížnost vyšetřování a soudního stíhání. Soudy a policejní orgány tak musí čelit výzvám spojeným s extrateritoriální jurisdikcí a potřebou mezinárodní spolupráce při řešení kybernetických případů.

Dalším klíčovým prvkem je rostoucí sofistikovanost útoků. Pachatelé neustále zdokonalují své techniky a využívají pokročilé nástroje k utajení svých aktivit. Soudy musí být schopny porozumět a správně interpretovat tyto složité technologické útoky, což může zahrnovat spolupráci s technickými odborníky - znalci, kterých je nedostatek již v současné době.

Ochrana osobních údajů a kybernetická bezpečnost jsou dnes záležitostmi rostoucího významu. Soudy se stávají arénou pro řešení případů týkajících se porušení soukromí a krádeže citlivých informací. Jejich role spočívá v nalezení rovnováhy mezi ochranou individuálních práv a potřebou efektivního postihu kybernetických pachatelů.

## 8.4 Limitace provedeného výzkumu

Důkladná analýza představovaná provedeným výzkumem přináší poznatky o specifických aspektech právních postihů v oblasti kybernetické kriminality podle českého trestního zákoníku. Zjištění zdůrazňují, že právní kvalifikace trestných činů podle § 230 odst. 1, § 230 odst. 2 a § 231 není pouhým formálním procesem, ale vyžaduje důkladné zhodnocení skutkových podstat a právních argumentů v rámci každého případu. Přítomnost podrobností o skutkových podstatách obsažených v použitých rozhodnutí soudů v analýze umožňuje lépe porozumět kontextu, v němž kybernetické trestné činy probíhají, a identifikovat možné vzory chování pachatelů.

Zároveň je třeba uvést limitace v podobě omezené vzorkové velikosti studie a specifičnosti vybraných případů, kterých nemůže být bez dalšího použito k vyvození obecných zákonitostí, znaků a projevů těchto jevů – celkově zobecnění. Dalším omezením, které je nutné brát v úvahu je, že v rámci širšího spektra kybernetické kriminality mohou existovat možnosti a projevy, které nebyly

zahrnuty do této analýzy. Důležitým poznatkem z výzkumu je také fakt, že informace získané z trestních rozsudků jsou pouze jednou stránkou celého soudního procesu, a nemohou plně zohlednit všechny aspekty soudního rozhodování a právní kvalifikace.

Nicméně, i přes výše zmíněná omezení, jsou závěry výzkumu klíčové pro diskusi o interpretaci a aplikaci právních norem v oblasti kybernetické kriminality a poskytují právním expertům, akademikům a tvůrcům právních norem cenný materiál pro přemýšlení o úpravách a posilování právního rámce kybernetické kriminality v reakci na neustále se vyvíjející povahu kybernetických hrozeb. Důraz na konkrétní případy trestních rozsudků umožňuje zapojení praktických aspektů práva do úvah o kybernetické kriminalitě, čímž studie přispívá k lepšímu pochopení celé problematiky, kterou se tato práce zaobírá a přiblížení právního prostředí čtenáři neprávníkovi a napříč obory, což může přispět k efektivnější ochraně kyberprostoru, objektů trestných činů a společnosti jako celku.

## 8.5 Závěry a doporučení

Bakalářská práce se zaměřila na téma kybernetické kriminality proti zařízením ICT v České republice a přináší komplexní vhled do této dynamické a rychle se rozvíjející oblasti. Cílem této práce bylo analyzovat a poskytnout přehled o různých projevech kybernetické kriminality, zejména s důrazem na vyhotovenou případovou studii, analýzu soudních rozhodnutí, obsahovou analýzu právních dokumentů včetně jejich interpretace, literární rešerši a kombinaci kvalitativního a kvantitativního výzkumu.

V teoretické části práce bylo provedeno důkladné vymezení základních pojmů spojených s kybernetickou kriminalitou, vymezení relevantní právní úpravy, představeny jednotlivé fenomény kybernetické kriminality a pojednáno bylo i o vybraných procesněprávních nástrojích trestního práva.

V rámci praktické části byla provedena případová studie vybraných případů kybernetické kriminality v České republice. Rozbory příkladů k jednotlivým skutkovým podstatám byly pečlivě strukturovány a obsahovaly popis incidentu, analýzu skutkového stavu, dopad na oběti a hodnocení právního postihu pachatelů. Tyto analýzy poskytly konkrétní a hluboký pohled na realitu kybernetických útoků v naší zemi.

Právní úprava, zejména trestní rozhodnutí soudů, byla analyzována a interpretována s cílem porozumění postupu právního systému při stíhání kybernetických deliktů. Kombinací soudního a doktrinálního výkladu byl podán hlubší pohled na interpretaci práva v kontextu kybernetické kriminality.

Kombinace kvalitativní analýzy obsahových dat a kvantitativního hodnocení statistických trendů umožnila získat komplexní pohled na kybernetickou kriminalitu v České republice

V závěrečných kapitolách práce byly prezentovány klíčové závěry a doporučení odvozená z provedeného výzkumu. Tyto poznatky mají potenciál ovlivnit nejen teorii kybernetické kriminality, ale také praktická opatření v oblasti prevence a stíhání těchto trestných činů.

Z hlediska možných doporučení z provedeného výzkumu je zdůraznit potřebu udržovat znění skutkových podstat trestního zákoníku v souladu

s mezinárodními dokumenty a závazky, které z nich České republice plynou, ustálení judikatury v oblasti rozhodovávání o kybernetické kriminalitě napříč soustavou obecných soudů. Při analýze rozhodnutí vyvstala otázka objektu těchto trestných činů, které by bylo vhodné jednoznačněji definovat, například ve formě přijetí *soft-law* dokumentů, což by vedlo k větší jednoznačnosti a předvídatelnosti trestního postihu, právních kvalifikací a celkové větší míře spravedlnosti vymáhání práva v těchto skutkových případech.

Dále považuji za vhodné, byť to explicitně nebylo doposud zmíněno, zaměřit se na informační osvětu široké veřejnosti ve vztahu ke kybernetické bezpečnosti a efektivně podporovat vzdělávání v této oblasti. Nejedná se pouze o občany jako jednotlivce, ale i právnické osoby, firmy a veřejné instituce, kde se často lze setkat s tím, že chybí vypracovaný odpovídající *compliance* program. Nejedná se jen o samotné vytvoření souladných politik uvnitř firmy z formálního hlediska, ale i jejich praktické a efektivní nasazení, které by mělo zajistit větší odolnost proti kybernetickým útokům z venku i zevnitř společnosti ale i omezení případné trestní odpovědnosti právnické osoby (zejména ve vztahu k § 8 odst. 5 zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim).

Celkově lze konstatovat, že tato bakalářská práce přispívá k rozvoji poznání v oblasti kybernetické kriminality v České republice a poskytuje základ pro další výzkum a diskuzi v této dynamické oblasti. Její výsledky mohou sloužit jako podklad pro tvorbu strategií boje proti kybernetické kriminalitě a zároveň nabízí ucelený pohled na tuto stále se rozvíjející hrozbu.

Dalšími navazujícími tématy na tuto práci může být kybernetická kriminalita zaměřená na širší rozsah popisovaných trestných činů jako jsou například stále narůstající podvodné e-shopy, phishing, mravnostní trestné činy, tzv. *hate crime* nebo trestné činy proti autorskému právu.

# 9 Seznam použité literatury


[1] MARŠÁLEK, Pavel. Metodologie interpretace práva: legitimní cíl nebo fixní idea? In: A. GERLOCH, Jan TRYZNA a Jan WINTR, ed. *Metodologie interpretace práva a právní jistota*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o, 2012. ISBN 978-80-7380-388-9.

[2] KNAPP, Viktor. *Teorie práva*. 1. vyd. Praha: Beck, 1998. Právnické učebnice. ISBN 978-80-7179-028-0.

[3] GERLOCH, Aleš. *Teorie práva*. 6., aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2013. ISBN 978-80-7380-454-1.

[4] KOSAŘ, David a Jan PETROV. Jak vybrat „případy" do případové studie pracovat s nimi v právu: poznatky z výzkumu na pomezí práva a politologie. *Jurisprudence*. 2016, **2016**(6), 21–30. ISSN 1802-3843.

[5] MAREŠ, Jiří. Tvorba případových studií pro výzkumné účely. *Pedagogika*. nedatováno, **2015**(2), 113–142. ISSN 0031-3815.

[6] MCCONVILLE, Michael a Wing Hong CHUI, ed. *Research methods for law*. Second edition. Edinburgh: Edinburgh University Press, 2017. Research methods for the arts and humanities. ISBN 978-1-4744-0321-4.

[7] GIBSON, William. *Burning chrome: all-new introduction from the author*. Nachdr. New York: Eos, 2003. ISBN 978-0-06-053982-5.

[8] GIBSON, William. *Neuromancer*. [Praha]: Laser-books (Laser), 2019. Sprawl. ISBN 978-80-7617-760-4.

[9] MAYER, Marco, Pablo Andrés MAZURIER a Luigi MARTINO. How would you define Cyberspace? [online]. nedatováno [vid. 2023-11-01]. Dostupné z: https://www.academia.edu/7096442/How_would_you_define_Cyberspace

[10] *ISO/IEC 27032:2012(en), Information technology — Security techniques — Guidelines for cybersecurity* [online]. [vid. 2023-11-01]. Dostupné z: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

[11] KREMLING, Janine a Amanda M. Sharp PARKER. *Cyberspace, cybersecurity, and cybercrime*. First Edition. Los Angeles: SAGE Publications, 2018. ISBN 978-1-5063-4725-7.

[12] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2022. ISBN 978-80-7380-849-5.

[13] KOLOUCH, Jan. *CyberCrime*. 1. vydání. Praha: CZ.NIC, z.s.p.o, 2016. Edice CZ.NIC, 14. publikace. ISBN 978-80-88168-15-7.

[14] HUTH, M., C. VISHIK a R. MASUCCI. 8 - From Risk Management to Risk Engineering: Challenges in Future ICT Systems. In: Edward GRIFFOR, ed. *Handbook of System Safety and Security* [online]. Boston: Syngress, 2017 [vid. 2023-11-01], s. 131–174. ISBN 978-0-12-803773-7. Dostupné z: doi:10.1016/B978-0-12-803773-7.00008-5

[15] GŘIVNA, Tomáš, ed. *Kriminologie*. 4., aktualizované vyd. Praha: Wolters Kluwer, 2014. ISBN 978-80-7478-614-3.

[16] SMEJKAL, Vladimír, Tomáš. SOKOL a Martin VLČEK. *Počítačové právo*. Vyd. 1. Praha: C.H. Beck : SEVT, 1995. ISBN 978-80-7179-009-9.

[17] WATTERS, Paul A. *Cybercrime and Cybersecurity*. Milton: Taylor & Francis Group, 2023. ISBN 978-1-00-099236-6.

[18] CLOUGH, Jonathan. *Principles of cybercrime*. Second edition. Cambridge, United Kingdom: Cambridge University Press, 2015. ISBN 978-1-107-03457-0.

[19] POLČÁK, Radim, ed. *Právo informačních technologií*. Vydání první. Praha: Wolters Kluwer, 2018. Právní monografie. ISBN 978-80-7598-045-8.

[20] GŘIVNA, Tomáš a Radim POLČÁK, ed. *Kyberkriminalita a právo*. Vydání první. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4.

[21] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. 5. Praha: Centrum kybernetické bezpečnosti, z.ú., 2022. ISBN 978-80-908388-4-0.

[22] *Nejčastější projevy kybernetické kriminality s odkazem na trestní zákoník - Policie České republiky* [online]. [vid. 2023-10-31]. Dostupné z: https://www.policie.cz/clanek/nejcastejsi-projevy-kyberneticke-kriminality-s-odkazem-na-trestni-zakonik.aspx

[23] MAURER, Tim. *Cyber norm emergence at the United Nations - An Analysis of the Activities at the UN Regarding Cyber-security* [online]. B.m.: Belfer Center for Science and International Affairs Harvard Kennedy School. listopad 2011. Dostupné z: https://www.un.org/en/ecosoc/cybersecurity/maurer-cyber-norm-dp-2011-11.pdf

[24] PALOSIRKKA. *Countries that have ratified Convention on Cybercrime* [online]. 17. prosinec 2020 [vid. 2023-11-09]. Dostupné z: https://commons.wikimedia.org/wiki/File:Ratified_Convention_on_Cybercrime.svg

[25] POLČÁK, Radim, ed. *Právo na internetu: spam a odovednost ISP*. Brno: Computer Press, 2007. ISBN 978-80-251-1777-4.

[26] JONÁŠOVÁ, Eliška. Aktuální kybernetické hrozby a odpovídající právní úprava v Evropské unii a v Kanadě. *Bezpečnostní teorie a praxe* [online]. 2018, **2018**(3), Odborné periodikum Policejní akadamie České republiky v Praze. ISSN 2571-4589. Dostupné z: https://veda.polac.cz/wp-content/uploads/2019/04/032018_Aktuální-kybernetické-hrozby-a-odpovídající-právní-úprava-v-Evropské-unii-a-v-Kanadě.pdf

[27] ŠÁMAL, Pavel, Tomáš GŘIVNA, Oto NOVOTNÝ, Jiří HERCZEG a Marie VANDUCHOVÁ, ed. *Trestní právo hmotné*. 9., přepracované vydání. Praha: Wolters Kluwer, 2022. ISBN 978-80-7598-764-8.

[28] PELC, Vladimír. Trestné činy proti počítačovým systémům. In: Tomáš GŘIVNA, Martin RICHTER a Hana ŠIMÁNOVÁ, ed. *Vliv nových technologií na trestní právo*. Praha: Auditorium, 2022. ISBN 978-80-87284-95-7.

[29] ŠÁMAL, Pavel a a kol. *Trestní zákoník. 2: § 140 - 421*. 1. vyd. Praha: Beck, 2010. Velké komentáře. ISBN 978-80-7400-178-9.

[30] GŘIVNA, Tomáš a Jakub DRÁPAL. Attacks on the confidentiality, integrity and availability of data and computer systems in the criminal case law of the Czech Republic. *Digital Investigation* [online]. 2019, **28**, 1–13. ISSN 1742-2876. Dostupné z: doi:10.1016/j.diin.2018.12.002

[31] EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION. *Cyber-attacks: the apex of crime as a service.* [online]. LU: Publications Office, 2023 [vid. 2023-10-31]. Dostupné z: https://data.europa.eu/doi/10.2813/30058

[32] *Fridge caught sending spam emails in botnet attack* [online]. [vid. 2023-10-23]. Dostupné z: https://www.cnet.com/home/kitchen-and-household/fridge-caught-sending-spam-emails-in-botnet-attack/

[33] REALITY, Open. Fridge SPAMs Thousands in Botnet Attack! *Open Reality* [online]. 25. březen 2015 [vid. 2023-11-13]. Dostupné z: https://www.openreality.co.uk/blog/fridge-spams-thousands-in-botnet-attack/

[34] ČEP, David. Trestní (ne)odpovědnost za DDoS útoky. In: Tomáš GŘIVNA, Martin RICHTER a Hana ŠIMÁNOVÁ, ed. *Vliv nových technologií na trestní právo*. Praha: Auditorium, 2022. ISBN 978-80-87284-95-7.

[35] KOŽELUHA, Patrik. Užití analogie legis v judikatuře českých soudů. nedatováno.

[36] GŘIVNA, Tomáš. Komentář k § 230. In: Pavel ŠÁMAL a kol.*Trestní zákoník: komentář II, § 140-421*. 2. vyd. Praha: Beck, 2012. ISBN 978-80-7400-428-5.

[37] ŠŤASTNÝ, Jakub. Trestní postih DoS/DDoS útoků. *EPRAVO.CZ* [online]. 20. duben 2020 [vid. 2023-11-14]. Dostupné

z: https://www.epravo.cz/top/clanky/trestni-postih-dosddos-utoku-110941.html

[38] VLÁDA ČR. *Důvodová zpráva k zákonu č. 130/2022 Sb., kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, zákon č. 45/2013 Sb., o obětech trestných činů a o změně některých zákonů (zákon o obětech trestných činů), ve znění pozdějších předpisů, a některé další zákony* [online]. 6. prosinec 2021. Dostupné z: https://www-beck-online-cz.ezproxy.is.cuni.cz/bo/chapterview-document.seam?documentId=oz5f6mrqgizf6mjtgbpwi6q&rowIndex=0

[39] MATĚJKA, Michal. *Počítačová kriminalita*. Praha: Computer Press, 2002. ISBN 80-7226-419-2.

[40] SAHU, Prabhat Kumar a Biswamohan ACHARYA. A REVIEW PAPER ON ETHICAL HACKING. *International Journal of Advanced Research in Engineering and Technology (IJARET)* [online]. 2020, **2020**(11), 163–168. ISSN 0976-6499. Dostupné z: doi:10.34218/IJARET.11.12.2020.018

[41] JÍROVSKÝ, Václav. *Kybernetická kriminalita*. Praha: Grada Publishing, 2007. ISBN 978-80-247-1561-2.

[42] *Jednotlivé druhy kyberkriminality - Policie České republiky* [online]. [vid. 2023-11-15]. Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx

[43] KRATOCHVÍL, Vladimír. *Kurs trestního práva. Trestní právo hmotné. Obecná část.* 1. vyd. Praha: Beck, 2009. Kurs trestního práva, 74. ISBN 978-80-7400-042-3.

[44] ČESKÁ TELEVIZE. Útok na benešovskou nemocnici způsobil šedesátimilionovou škodu. Policie případ odložila. *ČT24 - Nejdůvěryhodnější zpravodajský web v ČR - Česká televize* [online]. [vid. 2023-11-20]. Dostupné z: https://ct24.ceskatelevize.cz/domaci/3164067-utok-na-benesovskou-nemocnici-zpusobil-sedesatimilionovou-skodu-police-pripad

[45] VLÁDA ČR. *Sněmovní tisk 410/0, část č. 1/9 Vl.n.z. trestní zákoník - EU* [online]. [vid. 2023-11-20]. Dostupné z: https://www.psp.cz/sqw/text/tiskt.sqw?o=5&ct=410&ct1=0

[46] GŘIVNA, Tomáš a Marek DVOŘÁK. § 230 [Neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací]. In: Pavel ŠÁMAL a a kol.*Trestní zákoník. Komentář.* 3. vydání. Praha: C. H. Beck, 2023, s. s. 2957-2958. ISBN 978-80-7400-893-1.

[47] KANDOVÁ, Katarína a David ČEP. § 230 [Neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací]. In: Filip ŠČERBA a a kol.*Trestní zákoník*. 1. vydání (2. aktualizace). Praha: C. H. Beck, 2022. ISBN 978-80-7400-807-8.

[48] HRADIL, Miloslav. Neopětovala jeho city. Tak ji fackoval, kopal do hlavy a naboural se do jejího profilu - Novinky. *Novinky.cz* [online]. 8. prosinec 2023 [vid. 2023-12-08]. Dostupné z: https://www.novinky.cz/clanek/krimi-neopetovala-jeho-city-tak-ji-fackoval-kopal-do-hlavy-a-naboural-se-do-jejiho-profilu-40453581

[49] VLÁDA ČR. *Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky v roce 2022* [online]. B.m.: Ministerstvo vnitra, odbor bezpečnostní politiky. 12. červenec 2023. Dostupné z: https://www.mvcr.cz/soubor/zprava-o-situaci-v-oblasti-verejneho-poradku-a-vnitrni-bezpecnosti-na-uzemi-ceske-republiky-v-roce-2022.aspx

[50] ČESKÁ TISKOVÁ KANCELÁŘ. Vydíral Babiše, posílal mu fotky jeho rodiny. Hacker z Ostravy za to dostal dvouletou podmínku | Domov. *Lidovky.cz* [online]. 23. srpen 2018 [vid. 2023-12-09]. Dostupné z: https://www.lidovky.cz/domov/hacker-z-ostravy-dostal-podminku-za-dva-roky-stare-vydirani-babise.A180823_140618_ln_domov_ele

[51] NOHL, Radek. *Hacker vyhrožoval Babišovi a jeho rodině. Soud ho teď neveřejně odsoudil - Seznam Zprávy* [online]. 23. srpen 2016 [vid. 2023-12-09]. Dostupné z: https://www.seznamzpravy.cz/clanek/hacker-vyhrozoval-babisovi-a-jeho-rodine-soud-ho-ted-neverejne-odsoudil-54533

[52] HRUBEŠ, Karel. Policie zatkla hackera, který vydíral ministra Babiše - Seznam Zprávy. *Seznam Zprávy* [online]. 15. listopad 2016 [vid. 2023-12-09]. Dostupné z: https://www.seznamzpravy.cz/clanek/policie-zatkla-hackera-ktery-vydiral-ministra-babise-3760

[53] POLICIE ČR. Vývoj registrované kriminality v roce 2022. *Policie.cz* [online]. 13. leden 2023 [vid. 2023-12-13]. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx

## 9.1 Seznam použitých právních předpisů

- **Listina základních práv a svobod**, republikována jako usnesení č. 2/1993 Sb.
- **Nařízení Evropského parlamentu a Rady (EU) č. 165/2014** ze dne 4. února 2014 o tachografech v silniční dopravě, o zrušení nařízení Rady (EHS) č. 3821/85 o záznamovém zařízení v silniční dopravě a o změně nařízení Evropského parlamentu a Rady (ES) č. 561/2006 o harmonizaci některých předpisů v sociální oblasti týkajících se silniční dopravy s významem pro EHP.
- **Rámcové rozhodnutí Rady 2005/222/SVV** ze dne 24. února 2005 o útocích proti informačním systémům, nahrazené Rámcovým rozhodnutím Rady 2005/222/SVV ze dne 24. února 2005 o útocích proti informačním systémům.
- **Rozhodnutí Rady ze dne 29. května 2000 o boji proti dětské pornografii na internetu.**
- **Sdělení č. 104/2013 Sb. m. s.**, Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě.
- **Směrnice 2000/31/EC** ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu.
- **Směrnice Evropského parlamentu a Rady 2013/40/EU** ze dne 12. srpna 2013 o útocích na informační systémy, nahrazující rámcové rozhodnutí Rady 2005/222/SVV.
- SPOLEČNÉ SDĚLENÍ EVROPSKÉMU PARLAMENTU, RADĚ, EVROPSKÉMU HOSPODÁŘSKÉMU A SOCIÁLNÍMU VÝBORU A VÝBORU REGIONŮ: **Strategie kybernetické bezpečnosti Evropské unie** – Otevřený, bezpečný a chráněný kyberprostor.
- **Ústava České republiky**, zákon č. 1/1993 Sb.
- **Zákon č. 127/2005 Sb.**, o elektronických komunikacích.
- **Zákon č. 130/2022 Sb.**, kterým se mění zákon č. 40/2009 Sb., trestní zákoník ve znění pozdějších předpisů, zákon č. 45/2013 Sb., o obětech trestných činů a o změně některých zákonů (zákon o obětech trestných činů) ve znění pozdějších předpisů, a některé další zákony.
- **Zákon č. 140/1961 Sb.**, trestní zákon.
- **Zákon č. 141/1961 Sb.**, o trestním řízením soudním.
- **Zákon č. 183/2016 Sb.**, kterým se mění zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim.
- **Zákon č. 200/1990 Sb.**, o přestupcích.

- **Zákon č. 218/2003 Sb.**, o soudnictvích ve věcech mládeže.
- **Zákon č. 300/2008 Sb.**, o elektronických úkonech a autorizované konverzi dokumentů.
- **Zákon č. 40/2009 Sb.**, trestní zákoník.
- **Zákon č. 40/2009 Sb.**, trestní zákoník.
- **Zákon č. 418/2011 Sb.**, o trestní odpovědnosti právnických osob a řízení proti nim.
- **Zákon č. 480/2004 Sb.**, o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti).

## *9.2 Seznam použitých soudních rozhodnutí*

- Usnesení Městského soudu v Praze **sp. zn. 44 To 385/2016** ze dne 26. 10. 2016
- Stanovisko trestního kolegia Nejvyššího soudu **sp. zn. Tpjn 301/2012** ze dne 30. 1. 2013
- Usnesení Krajského soudu v Hradci Králové **sp. zn. 13 To 416/2017** ze dne 17. 10. 2017
- Usnesení Nejvyššího soudu, soudu pro mládež, **sp. zn. 8 Tdo 100/2019-35** ze dne 13.2.2019
- Usnesení Nejvyššího soudu **sp. zn. 5 Tdo 17/2011** ze dne 19. 1. 2011
- Nález Ústavního soudu ČR **sp. zn. II. ÚS 1152/17** ze dne 11. 6. 2018
- Usnesení Ústavního soudu ČR **sp. zn. II.ÚS 3852/18** ze dne 14. 5. 2019
- Usnesení Nejvyššího soudu **sp. zn. 7 Td 28/2018-7** ze dne 30. 5. 2018
- Usnesení Nejvyššího soudu **sp. zn. 8 Tdo 266/2017** ze dne 15. 8. 2018
- Usnesení Nejvyššího soudu **sp. zn. 7 Tdo 731/2015** ze dne 30. 9. 2015
- Usnesení Nejvyššího soudu **sp. zn. 7 Tdo 1134/2020-445** ze dne 4. 11. 2020
- Usnesení Nejvyššího soudu **sp. zn. 6 Tdo 1479/2012** ze dne 12. 12. 2012

# Zadání práce z IS (eVŠKP)

Univerzita Hradec Králové
Fakulta informatiky a managementu

## Zadání bakalářské práce

| | |
|---|---|
| **Autor:** | **Lukáš Dyntar** |
| Studium: | I2100121 |
| Studijní program: | B0688A140001 Informační management |
| Studijní obor: | Informační management |
| **Název bakalářské práce:** | **Kybernetická kriminalita proti zařízením ICT** |
| Název bakalářské práce AJ: | Cybercrime against ICT devices |

**Cíl, metody, literatura, předpoklady:**

**Cíl práce:**

Cílem práce je analýza kybernetické kriminality proti ICT zařízením. Teoretická část se zaměří na některé trestné činy proti zařízením ICT a v praktické části budou rozebrány projevy tohoto druhu počítačové kriminality.

**Osnova**

1. **Úvod** – motivace, cíl práce, metodika zpracování
2. **Teoretická část** – definice, prameny právní úpravy, druhy počítačové kriminality, trestněprocesní aspekty
3. **Praktická část** – případové studie, nebo statistické zpracování (bude upřesněno)
4. **Závěr**


SMEJKAL, Vladimír. Kybernetická kriminalita. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. ISBN 978-80-7380-849-5.

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

GŘIVNA, Tomáš; RICHTER, Martin a ŠIMÁNOVÁ, Hana (ed.). Vliv nových technologií na trestní právo. Praha: Auditorium, 2022. ISBN 978-80-87284-95-7.

CLOUGH, Jonathan. Principles of Cybercrime. 2nd edition. Cambridge University Press, 2015. ISBN 978-1-107-69816-1.

WATTERS, Paul A. Cybercrime and Cybersecurity. CRC Press, 2023. ISBN 978-10-0099-236-6.


| | |
|---|---|
| Zadávající pracoviště: | Katedra managementu,<br>Fakulta informatiky a managementu |
| Vedoucí práce: | Mgr. Tomáš Ledvinka, Ph.D. |

Datum zadání závěrečné práce: 15.10.2021