POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostně právní

Katedra kriminální policie

Elektronické důkazy v trestním řízení

Diplomová práce

Electronic evidence in criminal proceedings

Master Thesis

VEDOUCÍ PRÁCE

doc. JUDr. Ladislav POKORNÝ, Ph.D.

AUTOR PRÁCE

Bc. Tomáš NOVOTNÝ

Praha

2023

Čestné prohlášení

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

V Ústí nad Labem, dne 23. 2. 2023

Bc. Tomáš Novotný

Poděkování

Tímto bych rád poděkoval panu doc. JUDr. Ladislavu Pokornému, Ph.D. za všechny připomínky, cenné rady, vstřícný a trpělivý přístup při konzultacích k této diplomové práci.

ANOTACE

Tématem diplomové práce jsou elektronické důkazy v trestním řízení. Práce se zaměřuje na principy využitelnosti elektronických dat jako důkazů pro trestní řízení. Dotýká se oblastí obecné podstaty dokazování v trestním řízení, důkazních prostředků a rozdělení důkazů. Dále provádí kritickou analýzu stavu dokazování pro vybrané druhy elektronických důkazů, přičemž sleduje vybrané fáze dokazování s důrazem na způsoby zajištění dat a hodnocení důkazů, které mohou vést k individuální identifikaci osob. Práce dále zpracovává analýzu statistických dat o vybraných registrovaných a objasněných trestných činech v ČR za období od roku 2016 do 2022. Závěry, doporučení a náměty *de le ferenda* jsou vyvozeny z analýzy právních norem, odborné literatury a internetových zdrojů.

KLÍČOVÁ SLOVA

dokazování * důkazní prostředek * důkaz * elektronická data * elektronický důkaz * zajištění a hodnocení důkazů * analýza kriminality

ANNOTATION

The topic of the thesis is electronic evidence in criminal proceedings. The thesis focuses on the principles of the usability of electronic data as evidence for criminal proceedings. It touches on the areas of the general essence of evidence in criminal proceedings, means of evidence and division of evidence. It also provides a critical analysis of the state of evidence for selected types of electronic evidence, while monitoring selected phases of evidence with an emphasis on methods of securing data and evaluating evidence that can lead to individual identification of persons. The thesis further processes the analysis of statistical data on selected registered and clarified criminal offenses in the Czech Republic for the period from 2016 to 2022. Conclusions, recommendations and themes *de le ferenda* are derived from the analysis of legal standards, professional literature and internet sources.

KEYWORDS

proving * means of evidence * evidence * electronic data * electronic proof * securing and evaluating evidence * crime analysis

Obsah

Úvod

V posledním desetiletí je zaznamenán obrovský technologický vývoj v oblasti komunikace a přenosu digitálních dat, který se přirozeně dotýká každého z nás nejen v osobním životě, ale také ve vztahu k orgánům veřejné moci. Tvrzení, že každý má svět na dosah ruky, je při pohledu na rychlost, kterou lze přenášet data a informace napříč celým světem neuvěřitelně pravdivá. Nejnovější technologie s sebou mimo výhod přináší také některá rizika, která se naplno projevují v oblasti bezpečnosti a trestné činnosti. Výpočetní technika se v oblasti kriminality objevuje nejen jako předmět, ale také jako prostředek k páchání trestné činnosti. V oblasti kyberkriminality se přítomnost výpočetní techniky přímo předpokládá, avšak elektronika a výpočetní technika má přesah také do obecné kriminality. Většina lidí u sebe v průběhu celého dne nosí některá elektronická zařízení, jejichž používání vytváří nesmazatelnou digitální stopu často i bez vědomí dotyčné osoby. Zároveň mnoho měst a soukromých subjektů vynakládá nemalé finance na to, aby zajistila bezpečnost ve své oblasti působnosti, což se projevuje také čím dál častějším využitím elektronických zařízení, která jsou schopna zaregistrovat a uchovat elektronická data, která jsou následně využitelná pro trestní řízení. Vývoj je v tomto směru tak rychlý, že legislativa často není schopna pružně a včasně reagovat na nové technologie, postupy, možnosti a způsoby páchání, tak aby dokázala sjednotit postup orgánů činných v trestním řízení (OČTŘ). Ty jsou nezřídka nuceny ohýbat právní normy a přizpůsobovat si postupy a možnosti zajišťování určitých důkazů často na hranici zákona, čímž se vytváří prostor pro obhajobu k tomu, aby se nesnažila pouze vyvrátit samotnou dokazovanou skutečnost, ale přímo napadat zákonnost zajištění či provedení takového důkazu, což může v důsledku vést k naprosté nepoužitelnosti takového důkazu. Podstata dokazování elektronickými důkazy je ve spoustě poměrech specifická a náročná. Značná část trestných činů, především kybernetické kriminality, zůstává neobjasněna a vzhledem k absenci adekvátních technických prostředků na straně OČTŘ také latentní. Autor této práce se nemůže zbavit dojmu, že OČTŘ v oblasti adekvátních právních norem i technických řešeních „ujíždí vlak“. Tato diplomová práce je zaměřena na popis vybraných elektronických dat, která jsou použitelná v trestním řízení jako důkaz. V úvodní části práce jsou objasněny pojmy týkající se obecného dokazování v trestním řízení podle

trestního řádu, zásady dokazování, důkazní prostředky a rozdělení druhů důkazů podle specifických charakteristik. V další části je uveden popis konkrétních elektronických důkazů, jejich pramenů a dále jsou objasňovány způsoby nakládání s takovými důkazy pro účely trestního řízení. Následuje část, ve které jsou vysvětlovány způsoby dokazování vybranými elektronickými důkazy (e-mailem; provozními a lokalizačními údaji; odposlechem; elektronickými dokumenty; daty z mobilních komunikačních zařízeních; daty z dohledových systémů kybernetické bezpečnosti) a jednotlivé fáze, které s tímto druhem dokazování souvisí, jako je zajištění dat, provedení důkazů a hodnocení důkazů. Po této části následuje analýza současného stavu právních norem, postupů a specifických problémů či nejasností, které se ke konkrétním způsobům dokazování vážou. V další části se práce soustředí na analýzu statistických dat vybraných trestných činů za období od 1. 1. 2016 do 31. 12. 2022 s cílem poukázat na skutečný stav registrovaných a objasněných trestných činů, ve kterých je předpokládána přítomnost elektronických dat, která jsou důležitá pro odhalení a objasnění těchto trestných činů. Analýza by měla zároveň potvrdit hypotézu, že kriminalita se čím dál více přesouvá do virtuálního světa, kde využití elektronických dat ve vybraných oblastech obecné kriminality napomáhá k vyšší objasněnosti. Zároveň možnost používání moderních technologií pachateli ve specifických případech majetkové trestné činnosti znesnadňuje odhalení a objasnění trestných činů. Práce si klade za cíl poukázat na nutnost změn některých nejasných právních norem a dále poskytnout zjednodušený náhled do této problematiky pro laickou veřejnost i pro kolegy Policie ČR, se zaměřením především na způsoby zajištění a analýzu dat, neboť se zajištěním dat jako jedním z prvotních úkonů, se setkávají nejen IT a analytičtí specialisté, ale mnohdy také policisté na obvodních odděleních nebo příslušníci Služby kriminální policie a vyšetřování (SKPV). Pro trestní řízení je důležité, aby právě činnost při zajištění dat, probíhala zákonným a co nejodbornějším způsobem tak, aby nedošlo ke znehodnocení dat a důkazů. Autor v práci zveřejňuje některé své poznatky, či názory, které by mohly sloužit k rozpoutání diskuse, čímž není myšleno vyvracování stanovisek či závěrů odborníků v tomto oboru. Při zpracování práce autor využil metody pozorování a obsahové analýzy právních předpisů, odborné literatury a internetových zdrojů, které se dotýkají oblasti práva a elektronických a informačních technologií.

1 Dokazování v trestním řízení

Před náhledem do problematiky elektronických důkazů, je vhodné, aby bylo objasněno několik pojmů týkajících se samotného procesu dokazování v rámci trestního řízení. Trestní řízení musí být vedeno v souladu se zákony. Mezi nejdůležitější právní normy pro trestní řízení patří Ústavní zákon č. 1/1993 Sb., Ústava České republiky, Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod, zákon č. 40/2009 Sb., Trestní zákoník (TZ) a zákon č. 141/1961 Sb., Trestní řád (TŘ).[1] Veškeré úkony provedené v rámci trestního řízení nesmí překračovat hranice zákonnosti a musí dodržovat další zásady trestního řízení.[2] Trestní řád se zabývá postupem OČTŘ, který má směřovat ke správnému zjištění trestných činů a potrestání pachatelů. Úkolem trestního řízení je pak předcházet a zamezovat trestné činnosti v mezích určených zákonem.[3] Trestní řád se také zabývá pojmem dokazování, což je velmi důležitá část trestního řízení, kterou je možno *„charakterizovat jako zákonem stanovený souhrn pravidel, která upravují postup OČTŘ a dalších subjektů při vyhledávání, zajišťování, provádění a hodnocení důkazů v trestním řízení.*“[4] Trestní řád nicméně neuvádí, jaký je rozdíl mezi základními pojmy, kterými jsou dokazování, důkaz a důkazní prostředek a v praxi bývají tyto pojmy často zaměňovány.[5] Laická veřejnost si pod těmito pojmy představí, že se jedná o prostředky sloužící k usvědčení pachatele z trestného činu nebo ospravedlnění podezřelého z trestného činu. V následujících podkapitolách budou tyto pojmy vysvětleny blíže.

1.1 Zásady dokazování v trestním řízení

Zákon č. 141/1961 Sb., Trestní řád (TŘ) se v Hlavě první v ustanovení § 2, věnuje základním zásadám trestního řízení. Jedná se o obecná ustanovení, kterými jsou OČTŘ povinny postupovat v rámci celého trestního řízení. Při vybočení z těchto zásad by se zcela jistě jednalo o nezákonný postup OČTŘ, který by měl za

---

[1] NOVOTNÝ, František a kol. *Trestní právo procesní*. 2. vyd. Plzeň: Aleš Čeněk, 2017, s. 16-17. ISBN 978-80-7380-677-4.
[2] Viz. § 2 zákona č. 141/1961 Sb., *Trestní řád* v posledním znění
[3] Viz. § 1 odst. 1 zákona č. 141/1961 Sb., *Trestní řád* v posledním znění
[4] NOVOTNÝ, František a kol. *Trestní právo procesní*. 2. vyd. Plzeň: Aleš Čeněk, 2017, s. 244. ISBN 978-80-7380-677-4.
[5] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 56. ISBN 978-80-210-8073-7.

následek zpochybnění a zneplatnění celého řízení. Ze základních zásad trestního řízení lze vybrat několik zásad, které se dotýkají přímo procesu dokazování, těmi jsou následující zásady:

- **Zásada presumpce neviny (§ 2 odst. 2 TŘ)**

Zásada presumpce neviny je jednou z nejdůležitějších zásad trestního řízení. Ta směřuje k osobě podezřelého (obviněného, obžalovaného), a má chránit jeho osobnost, neboť ukládá povinnost na tuto osobu pohlížet jako na nevinného, do doby pravomocného odsuzujícího rozsudku soudu, který ho uzná vinným.[6] V každém postavení má osoba možného pachatele různá práva a povinnosti. Pro příklad pouze podezřelý může být podroben výslechu podezřelého podle § 76 odst. 3 TŘ. Pouze proti obviněnému může být vedeno vazební zasedání podle § 73d TŘ Pouze obžalovaný má právo posledního slova v hlavním líčení před soudem. A pouze pravomocně odsouzenému lze uložit výkon trestu odnětí svobody.

- **Zásada vyhledávací (§ 2 odst. 5 TŘ)**

V souladu se zákonem jsou OČTŘ povinny zjišťovat *„skutkový stav věci, o němž nejsou důvodné pochybnosti, a to v rozsahu, který je nezbytný pro jejich rozhodnutí.“*[7] Doznání obviněného nezbavuje OČTŘ povinnosti vyhledat a přezkoumat další důkazy důležité pro rozhodnutí ve věci. Vyhledávat důkazy jsou oprávněny také strany v trestním řízení.[8]

- **Zásada volného hodnocení důkazů (§ 2 odst. 6 TŘ)**

V trestním řádu není jasně stanoveno, jaká má být potřebná síla důkazu pro rozhodnutí ve věci. Důležité je, aby důkaz souvisel s objasňovanou věcí. Trestní řád ponechává hodnocení důkazů na OČTŘ podle vlastního uvážení.[9]

---

[6] Viz. § 2 odst. 2 zákona č. 141/1961 Sb., *Trestní řád* v posledním znění
[7] Viz. § 2 odst. 5 zákona č. 141/1961 Sb., *Trestní řád* v posledním znění
[8] Tamtéž
[9] Viz. § 2 odst. 6 zákona č. 141/1961 Sb., *Trestní řád* v posledním znění

- **Zásada ústnosti (§ 2 odst. 11 TŘ)**

Dokazování a jednání před soudem je vedeno ústní formou, především v podobě výslechu. Listinné důkazy se při dokazování čtou. Elektronické důkazy ve formě zpráv, obrazů, dat, hlasových zpráv, se zpravidla vyhodnocují a přepisují do písemné podoby ve formě úředních záznamů, protokolů, znaleckých posudků a odborných vyjádření, popř. se přehrávají v originální formě.[10]

- **Zásada bezprostřednosti (§ 2 odst. 12 TŘ)**

Zásada bezprostřednosti je úzce spjata s předchozí zásadou ústnosti a říká, že soud může rozhodovat pouze na základě provedených důkazů souvisejících s objasňovanou skutečností.[11]

1.2 Dokazování

Pojem *„dokazování je možné charakterizovat jako zákonem stanovený souhrn pravidel, která upravují postup OČTŘ a dalších subjektů při vyhledávání, zajišťování, provádění a hodnocení důkazů v trestním řízení.“*[12] Zjednodušeně by se dalo říct, že dokazování je celý proces, při kterém OČTŘ získávají předepsaným postupem důkaz z (od) nositele informace prostřednictvím důkazních prostředků, až po hodnocení důkazu, které je důležité pro rozhodnutí ve věci samé.[13]

Příklad:

- Prostřednictvím **důkazního prostředku** výslechem svědka podle § 101 TŘ, získají OČTŘ důkaz (informaci) o tom, že se podezřelý nacházel na místě spáchání trestného činu.
- Výsledkem je **důkaz**, který je tvořen obsahem výpovědi svědka.
- Konkrétní svědek je v tomto případě **nositelem informace**.

---

[10] Viz. § 2 odst. 11 zákona č. 141/1961 Sb., *Trestní řád* v posledním znění
[11] Viz. § 2 odst. 12 zákona č. 141/1961 Sb., *Trestní řád* v posledním znění
[12] NOVOTNÝ, František a kol. *Trestní právo procesní*. 2. vyd. Plzeň: Aleš Čeněk, 2017, s. 244. ISBN 978-80-7380-677-4.
[13] NOVOTNÝ, František a kol. *Trestní právo procesní*. 2. vyd. Plzeň: Aleš Čeněk, 2017, s. 249-250. ISBN 978-80-7380-677-4.

- **Předmět dokazování**

Taxativní výčet okolností, které se týkají předmětu dokazování, se nachází v ustanovení § 89 odst. 1 TŘ. Jedná se o dokázání skutečností, které jsou důležité pro posouzení, zda se ve věci jedná o trestný čin, o určení a vymezení jeho skutkové podstaty, skutečností dokazujících, zda a jakým způsobem se čin stal a zda jej spáchala určitá osoba, co ji k tomu vedlo, o jak závažný čin se jedná, jaké jsou poměry obviněného (zda byl dříve trestán, zda má rodinu, zaměstnání, atd.), jaká byla činem způsobena újma nebo škoda, a okolnosti, které k činu vedly.[14]

- **Rozsah dokazování**

To, v jakém rozsahu je potřebné dokazovat skutečnosti důležité pro trestní řízení, závisí vždy na podmínkách a specifikách konkrétního případu a dále na konkrétní fázi, ve které se řízení koná.[15] Vzhledem k rozsahu a pestrosti trestné činnosti, nelze uvést přesný návod, co se rozsahu dokazování týká a OČTŘ si částečně sami stanovují, jaký okruh a v jaké kvalitě je nutné skutečnosti dokazovat, přičemž musí být zachovány základní zásady dokazování. Co se týká rozsahu dokazování v určitých fázích trestního řízení, tak pro postup v každé z fází je potřeba jiná kvalita a kvantita důkazů, např. poznatek o spáchané trestné činnosti může stačit pro zahájení trestního řízení. Konkrétní důkazy svědčící proti určité osobě jsou potřebné pro zahájení jeho trestního stíhání, ale pro jeho odsouzení je potřebná existence přímých důkazů popř. řetězce nepřímých důkazů, které jsou způsobilé usvědčit obviněného ze spáchání trestného činu v takovém rozsahu, aby ve věci nebylo možno rozhodnout jinak, neboť v souvislosti s trestním řízením je nutné respektovat právní zásadu „in dubio pro reo“, která říká, že pokud při rozhodování existují určité pochybnosti, je nutné rozhodnout ve prospěch obviněného.[16]

1.3 Fáze dokazování

Proces dokazování je možné rozfázovat na několik částí, které na sebe navazují a bez nichž by nebylo možné dosáhnout účelu dokazování. Nejprve je nutné

---

[14] Viz § 89 odst. 1 zákona č. 141/1961 Sb., *Trestní řád* v posledním znění
[15] NOVOTNÝ, František a kol. *Trestní právo procesní*. 2. vyd. Plzeň: Aleš Čeněk, 2017, s. 252. ISBN 978-80-7380-677-4.
[16] Viz. § 2 zákona č. 141/1961 Sb., *Trestní řád* v posledním znění

vhodným způsobem vyhledat prameny důkazů a zákonným způsobem je zajistit. Následuje fáze provedení důkazu a v závěru jeho hodnocení.[17]

- **Vyhledávání důkazu**

Na tuto fázi se přímo váže výše uvedená zásada vyhledávací, neboť aby bylo možno někomu dokázat vinu nebo prokázat jeho nevinu, je nejprve nutné vyhledat a obstarat informace/důkazy, které jsou způsobilé takovouto skutečnost prokázat. V praxi se jedná o ustanovení směřující k zajištění věcí důležitých pro trestní řízení, což může být aplikováno formou zasažením do majetkového práva osoby, či obstaráním takových věcí, informací, nebo záznamů, při kterém osobě nevzniká žádný zásah do majetkových práv, nicméně tím vznikají zásahy do jiných osobnostních práv, jako je právo na soukromí atd.

Příklad vybraných ustanovení TŘ směřujících k vyhledání důkazů:

§ 78 – povinnost k předložení nebo vydání věci,
§ 79 - odnětí věci,
§ 82 - 85c – důvody a podmínky domovních, osobních prohlídek a prohlídek jiných prostor a pozemků,
§ 86 - 87c – zadržení, otevření, záměna a sledování zásilky,
§ 88 – odposlech a záznam telekomunikačního provozu,
§ 88a – údaje o uskutečněném telekomunikačním provozu,
§ 158b - 158f – použití operativně pátracích prostředků.[18]

Trestní řád není jediným zákonem, který se věnuje možnostem vyhledávání informací důležitých pro trestní řízení. Zákon č. 273/2008 Sb., o Policii České republiky mimo jiné říká, že úkolem policie je působit preventivně v oblasti trestné činnosti, odhalovat, objasňovat trestné činy a dále provádět vyšetřování trestných činů. Při získávání poznatků ve věci, ve které doposud nebylo zahájeno trestní

[17] NOVOTNÝ, František a kol. *Trestní právo procesní*. 2. vyd. Plzeň: Aleš Čeněk, 2017, s. 246. ISBN 978-80-7380-677-4.
[18] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 73-74. ISBN 978-80-210-8073-7.

řízení, ale i v souvislosti s probíhajícím trestním řízením, jsou policisté podle ustanovení § 72 - 77 tohoto zákona oprávněni používat podpůrné operativně pátrací prostředky, kterými jsou informátor, krycí prostředky, zabezpečovací technika a zvláštní finanční prostředky.[19] Takto získané poznatky lze využít pro rozpracování případu a následné zahájení trestního řízení.

- **Zajištění a provádění důkazu**

Jedná se o proces využívání důkazních prostředků, pomocí kterých OČTŘ zjišťují a zajišťují informace důležité pro trestní řízení a dále je předepsaným způsobem zaznamenávají pro další fáze řízení především písemnou formou. Mohou mít formu úředních záznamů, protokolů, odborných vyjádření, znaleckých posudků, avšak důkazy mohou být také zajištěny a provedeny ve formě in natura. Příkladem provedení důkazu v původní formě mohou být zvukové či obrazové záznamy, ve kterých se nachází informace důležité pro trestní řízení, a které jsou při dokazování určité skutečnosti přehrány.[20]

Příklady vybraných ustanovení TŘ směřujících k zajištění a provedení důkazů:

§ 158/3 – postup OČTŘ před zahájením tr. stíhání – oprávnění vyžadovat vysvětlení, odborná vyjádření, obstarávat podklady, provádět ohledání, vyžadovat provedení zkoušky krve, nebo podobného úkonu, pořizovat zvukové a obrazové záznamy osob, snímat jejich daktyloskopické otisky, provádět prohlídku těla, omezovat osoby na svobodě, zajištovat věci důležité pro trestní řízení a dále s nimi nakládat a provádět neodkladné a neopakovatelné úkony,
§ 90 - 96 - výslech obviněného,
§ 97 – 104 - výslech svědka,
§ 104a – 104e - zvláštní způsoby dokazování (konfrontace, rekognice, vyšetřovací pokus, rekonstrukce, prověrka na místě),
§ 105 – 111 - činnost znalce v souvislosti s trestním řízením,
§ 111a - ustanovení o provádění výslechu za pomocí videokonference,

[19] Viz. § 72 až 77 zákona č. 273/2008 Sb., *o Policii České republiky* v posledním znění
[20] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 65-66. ISBN 978-80-210-8073-7.

§ 112 - ustanovení o věcných a listinných důkazech,
§ 113 – 118 - ohledání (ohledání věci, ohledání místa činu, prohlídka těla, prohlídka mrtvoly a její exhumace, vyšetření duševního stavu).[21]

- **Prověrka důkazů**

Prověrkou důkazů má být posouzeno, jak jsou důkazy kvalitní a spolehlivé. Důkazy jsou takto posuzovány samostatně a dále navzájem s ostatními důkazy, za účelem zjištění, zda jsou důkazy v souladu, nebo mezi nimi existují rozpory. Případné rozpory má prověrka důkazů za úkol, pokud možno odstranit. K tomu lze využít některé zvláštní způsoby dokazování, které byly uvedeny i v části získávání důkazů § 104a – 104e TŘ (konfrontace, rekognice, vyšetřovací pokus, rekonstrukce, prověrka na místě). Prověrka důkazů jde ruku v ruce s následující závěrečnou fází, kterou je hodnocení důkazů.[22]

- **Hodnocení důkazů**

Ustanovení § 89 odst. 2 TŘ říká, že *„Za důkaz může sloužit vše, co může přispět k objasnění věci…“*[23] Z tohoto tvrzení vyplývá nutnost vyhodnocení informací, které k objasnění věci opravdu mohou přispět. Je nutné vyhodnotit, zda tyto informace s věcí souvisí a jsou schopny přímo či nepřímo dokázat objasňovanou skutečnost (závažnost), zda pochází z věrohodného zdroje a jsou v souladu se skutečností (věrohodnost a pravdivost) a to, zda byly získány zákonným způsobem (zákonnost). Teprve takto zhodnocené zjištěné a zajištěné informace mohou sloužit k následnému rozhodnutí OČTŘ. Toto hodnocení provádí příslušný OČTŘ, před kterým zrovna fáze dokazování probíhá, přičemž hodnocení probíhá

[21] Viz. § 90 až 158 zákona č. 141/1961 Sb., *Trestní řád* v posledním znění
POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 65-66. ISBN 978-80-210-8073-7.
[22] NOVOTNÝ, František a kol. *Trestní právo procesní*. 2. vyd. Plzeň: Aleš Čeněk, 2017, s. 246. ISBN 978-80-7380-677-4.
POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 66. ISBN 978-80-210-8073-7.
[23] Viz. § 89 odst. 2 zákona č. 141/1961 Sb., *Trestní řád* v posledním znění

v souladu se zásadou volného hodnocení důkazů a nikde není uvedeno, že jeden důkaz má mít přednost před druhým.[24]

Příklad fází dokazování

OČTŘ vyzve podezřelého k předložení mobilního telefonu (**vyhledání**). Následným ohledáním mobilního telefonu zjistí a zajistí obsah komunikace, ve které podezřelý vyhrožuje poškozenému smrtí (**zajištění a provedení**). Následně OČTŘ prověří souvislost tvrzení z výpovědi poškozeného a podezřelého s touto vyhodnocenou komunikací a zhodnotí, zda a jakým způsobem získaná komunikace souvisí s prověřovaným případem ublížení na zdraví poškozeného. Tyto informace dále porovná s dalšími získanými důkazy (**prověrka**). Soudu poté přísluší vyhodnotit a rozhodnout, zda nebylo zajištění komunikace provedeno nezákonným postupem (**hodnocení**).

1.4 Důkazní prostředek

„Důkazní prostředek je postup (proces), kterým OČTŘ získávají důkazy (informace) z pramene (nositele) důkazu.“[25] Pramenem neboli nositelem informace mohou být živé či zemřelé osoby nebo věci, které disponují různými informacemi důležitými pro trestní řízení (vzpomínka v paměti poškozeného, bodné zranění na těle poškozeného, mechanické poškození věci, ulpění otisku papilárních linií osoby na věcném nosiči a další). OČTŘ prostřednictvím důkazních prostředků tyto informace zajišťují takovým způsobem, aby bylo možné výsledek této činnosti pokládat za důkaz. Trestní řád v ustanovení § 89 odst. 2 říká, že:
„Za důkaz může sloužit vše, co může přispět k objasnění věci, zejména výpovědi obviněného a svědků, znalecké posudky, věci a listiny důležité pro trestní řízení a ohledání. Každá ze stran může důkaz vyhledat, předložit nebo jeho provedení navrhnout. Skutečnost, že důkaz nevyhledal nebo nevyžádal orgán činný v trestním řízení, není důvodem k odmítnutí takového důkazu.“[26] Tím TŘ taxativně

---

[24] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 66-68. ISBN 978-80-210-8073-7.
[25] NOVOTNÝ, František a kol. *Trestní právo procesní*. 2. vyd. Plzeň: Aleš Čeněk, 2017, s. 249. ISBN 978-80-7380-677-4.
[26] Viz. § 89 odst. 2 zákona č. 141/1961 Sb., *Trestní řád* v posledním znění

vyjmenovává nejčastější důkazní prostředky. V ustanoveních § 91 – 118 TŘ pojednává o dalších důkazních prostředcích. Za nejčastější důkazní prostředky jsou považovány:

§ 91 - 96 - výslech obviněného,
§ 97 – 104 výslech svědka,
§ 104a – 104e - zvláštní způsoby dokazování (konfrontace, rekognice, vyšetřovací pokus, rekonstrukce, prověrka na místě,
§ 105 – 111 - činnost znalce v souvislosti s trestním řízením,
§ 112 - ustanovení o věcných a listinných důkazech,
§ 113 – 118 - ohledání (ohledání věci, ohledání místa činu, prohlídka těla, prohlídka mrtvoly a její exhumace, vyšetření duševního stavu).[27]

1.5 Důkaz

„Důkaz je přímý poznatek (informace) o předmětu dokazování, získaný v procesu dokazování pomocí důkazního prostředku.“[28] *„Důkaz musí mít vztah k objasňované věci a musí být způsobilý prokázat či vyvrátit dokazovanou skutečnost.“*[29] Důkazy lze rozdělovat z několika následujících hledisek.

- **Dělení důkazů podle trestního řádu**
  - **Listinné důkazy**

„Listinnými důkazy jsou listiny, které svým obsahem prokazují nebo vyvracejí dokazovanou skutečnost, vztahující se k trestnému činu nebo k obviněnému.“[30] Může se jednat o veřejné listiny vydané některým orgánem veřejné moci nebo listiny soukromé, což jsou všechny ostatní.[31]

---

[27] NOVOTNÝ, František a kol. *Trestní právo procesní*. 2. vyd. Plzeň: Aleš Čeněk, 2017, s. 249. ISBN 978-80-7380-677-4.
[28] Tamtéž.
[29] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 58. ISBN 978-80-210-8073-7.
[30] Viz. § 112 odst. 2 zákona č. 141/1961 Sb., *Trestní řád* v posledním znění
[31] Viz. § 565 až 569 zákona č. 89/2012 Sb., *Občanský zákoník* v posledním znění

- **Věcné důkazy**

„Věcnými důkazy jsou předměty, kterými nebo na kterých byl trestný čin spáchán, jiné předměty, které prokazují nebo vyvracejí dokazovanou skutečnost a mohou být prostředkem k odhalení a zjištění trestného činu a jeho pachatele, jakož i stopy trestného činu.“[32] Může se jednat např. o střelnou zbraň, kterou pachatel zastřelil poškozeného, počítač, ve kterém se nachází dětská pornografie, nebo tričko, které pachatel zapomněl na místě činu při vloupání do objektu. Příkladem věcného důkazu spojeného s listinou může být ulpění povýstřelových zplodin, nebo otisk papilárních linií prstů podezřelého na listině.

- **Dělení důkazů podle vztahu k předmětu řízení**
  - **Usvědčující**

Důkazy, které jsou způsobilé usvědčit podezřelého (obviněného, obžalovaného) a svědčí v jeho neprospěch.[33]

  - **Ospravedlňující**

Důkazy, které jsou způsobilé prokázat nevinu podezřelého (obviněného, obžalovaného).[34]

- **Dělení důkazů podle pramene důkazu**
  - **Původní**

Originální důkazy v původní podobě, kterými mohou být originální data, listiny nebo výpovědi přímých očitých svědků události (př. obsah výpovědi svědka, který viděl, jak pachatel zabodl oběť nožem).[35]

  - **Odvozené**

Může se jednat o kopie, duplikáty, klony dat, popř. výpověď nepřímého svědka, který sám předmětný čin nevnímal, ale informaci zná pouze zprostředkovaně od jiného zdroje (př. obsah výpovědi osoby, které se kamarád svěřil, že jeho kamarád zabodl oběť nožem).[36]

---

[32] Viz. § 112 odst. 1 zákona č. 141/1961 Sb., *Trestní řád* v posledním znění
[33] NOVOTNÝ, František a kol. *Trestní právo procesní*. 2. vyd. Plzeň: Aleš Čeněk, 2017, s. 255. ISBN 978-80-7380-677-4.
[34] Tamtéž
[35] Tamtéž
[36] Tamtéž

- **Dělení důkazů podle vztahu k dokazované skutečnosti**
  - **Přímé**

Důkazy, které přímo potvrzují nebo vyvracejí hlavní skutečnost, kterou je v trestním právu vina či nevina podezřelého (obviněného, obžalovaného), popř. to, zda se skutečnost stala nebo nestala. (př. obsah výpovědi svědka, který viděl, jak pachatel zabodl oběť nožem).[37]

  - **Nepřímé**

Důkazy, které dokazují vedlejší skutečnost, která musí být v příčinném vztahu s hlavní skutečností (př. obsah výpovědi svědka, který byl přítomen tomu, když pachatel vyhrožoval oběti zabodnutím nožem a tato oběť byla následně nalezena mrtvá). Nelze rozhodnout o vině podezřelého na základě jednoho nepřímého důkazu. Pro rozhodnutí je nutné více (i nepřímých) důkazů, které na sebe navazují a jsou způsobilé v konečném důsledku vyvodit jediný závěr o objasňované věci.[38]

- **Dělení důkazů podle použitelnosti důkazu**

V rámci fáze hodnocení důkazů může dojít k situaci, kdy je zjištěn nesoulad v postupu s právními předpisy (vady dokazování). Tyto vady mají význam z hlediska použitelnosti, respektive nepoužitelnosti důkazu v trestním řízení. Může se jednat o nepodstatné (formální vady) a podstatné (způsobilé ovlivnit rozhodnutí OČTŘ) vady.[39] Možné dělení důkazů s podstatnými vadami:

  - **Relativně neúčinné**

Důkazy, jejichž vady lze napravit. Např. bude-li proveden výslech svědka, který je povinen zachovávat mlčenlivost. K důkazu nelze přihlížet do doby, než bude zbaven povinnosti mlčenlivosti. Po takovém odstranění vady lze k důkazu vyplývajícím z takového výslechu přihlížet v rámci trestního řízení.[40]

---

[37] NOVOTNÝ, František a kol. *Trestní právo procesní*. 2. vyd. Plzeň: Aleš Čeněk, 2017, s. 256. ISBN 978-80-7380-677-4.
[38] Tamtéž
[39] NOVOTNÝ, František a kol. *Trestní právo procesní*. 2. vyd. Plzeň: Aleš Čeněk, 2017, s. 258. ISBN 978-80-7380-677-4.
[40] Tamtéž

- **Absolutně neúčinné**

Důkazy, jejichž vady nelze napravit, a ke kterým nelze přihlížet, i kdyby se jednalo o důkazy, které jsou způsobilé usvědčit obviněného. Jedná se např. o důkazy získané domovní prohlídkou bez příkazu soudu.[41]

[41] NOVOTNÝ, František a kol. *Trestní právo procesní*. 2. vyd. Plzeň: Aleš Čeněk, 2017 s. 258. ISBN 978-80-7380-677-4.

2 Elektronické důkazy v trestním řízení

Trestní řád se věnuje dokazování a důkazním prostředkům, ale konkrétně nepojednává o elektronických důkazech. Zároveň však nevylučuje jejich užití v rámci trestního řízení. Trestní předpisy se pouze zmiňují o pojmech jako je počítač, počítačový systém, data nebo nosič informací. V důsledku absence pojmu elektronických důkazů v trestním řádu, je proces dokazování ohýbán a přizpůsobován konkrétním podmínkám a skutečnostem. Vzhledem k tomu, že život se čím dál více přesouvá do virtuálního prostředí, každý z nás zanechává ve světě jistou digitální stopu, kterou často běžný uživatel elektronických zařízení ani nezaznamená (logy, metadata, údaje vznikající při registracích, atd.). Fenomén začlenění výpočetních a komunikačních technologií do běžných životů přináší mnoho výhod, mezi kterými lze vyzdvihnout především rychlost a přesnost přenesených informací. Současně s tím tento trend přináší také mnoho úskalí, které se v současnosti naplno projevují v kriminalitě. Aktuální účinné právní předpisy nepředpokládaly rychlost vývoje těchto technologií, které by v představách před pouhými 20 lety působily nereálně. Ačkoliv je 20 let z hlediska historie lidstva pouhým okamžikem, došlo za tuto dobu patrně k nerychlejšímu technologickému vývoji v historii. V počátku 21. století již existovaly mobilní telefony, pomocí kterých bylo možné uskutečňovat hovory a komunikovat pomocí SMS zpráv s jinými uživateli, ale jinak umožňovaly užívat pouze zlomek funkcí, které nabízí současné technologie. V dnešní době jsou mobilní telefony součástí životů prakticky všech lidí civilizovaného světa a jsou využívány při každodenních rutinních činnostech. Je samozřejmostí, aby mobilní telefony poskytovaly uživatelům takové funkce jako je budík, fotoaparát a videokamera, kalendář s možností zapisování schůzek a poznámek, aplikace pro sledování počtu kroků, aplikace pro sledování pohybu s lokalizací uživatele, nebo sledování tepu či spánku uživatele. Představa odemčení plochy telefonu na základě přiložení otisku prstu, či pohledu do čtečky obličeje, nebo placení přiložením telefonu k terminálu před pár lety působila jako scéna ze sci-fi filmu, ale dnes se jedná o běžnou funkci telefonu, kterou bereme jako samozřejmost. Virtuální svět má každý na dosah ruky a internetová síť nám umožňuje vyhledávat informace a komunikovat s celým světem pouze prostřednictvím několika pohybů prstem na pracovní ploše telefonu. Tyto technologie jsou naší černou skříňkou, neboť většina způsobů užívání těchto

technologií zanechává datový otisk, ze kterého lze zjistit mnoho informací o konkrétním uživateli a o jeho chování. Z toho vyplývá, že výpočetní technika může být nejen předmětem páchání trestné činnosti, ale také jeho skvělým prostředkem, přičemž nefiguruje pouze v tzv. kyberkriminalitě, ale běžně se vyskytuje také v obecné kriminalitě.

2.1 Prameny elektronických důkazů

Pramenem důkazu se rozumí osoba nebo věc, která disponuje informací důležitou pro trestní řízení. Osoby těmito informacemi mohou disponovat v podobě vzpomínek v paměti, nebo v podobě změn, které vznikly na těle osoby (např. řezná rána). Řeznou ránu na těle člověka lze spatřit na vlastní oči, ale vzpomínky jsou neviditelné. Totožně lze uvažovat o informacích spojených s užíváním věcí. Konkrétně informace, které se vážou k elektronice, lze vysvětlit na příkladu videozáznamu. Pramenem usvědčujícího videozáznamu je datový nosič (PC, mobilní telefon, flash disk, atd.), v jehož paměti je soubor se záznamem uložený v určeném formátu (.mp4, .avi, .mkv, atd.). Dříve než se k soudu dostane takový důkaz v podobě videozáznamu, musí uvnitř kamerového zařízení proběhnout mnoho procesů, které umožní záznam nahrát a uložit i s doplňujícími informacemi, které se k záznamu vážou. Samotný proces záznamu i podrobnosti takového videozáznamu, jsou pro laickou veřejnost mnohdy příliš odbornou oblastí na to, aby se jím zabývala, ale odborníci z nich za pomocí elektronických zařízení a speciálních programů dokáží vyčíst informace nejrůznějšího charakteru. Takovými informacemi mohou být například: délka záznamu, období, ve kterém byl záznam pořízen, informace o tom, v jakém formátu a pod jakým názvem byl záznam uložen, ale také to, zda byl tento záznam nějak pozměňován, což může být velmi zajímavé z hlediska důkazní hodnoty takového záznamu. V trestním řízení nemusí být vždy podstatný pouze obsah takového záznamu, ale i tyto doplňující informace. Videozáznam lze zjednodušeně přirovnat ke vzpomínce v paměti člověka. Pramen důkazu může také tvořit samotný nosič, tak jako lidské tělo v případě řezné rány. Obdobou řezné rány na těle člověka může být mechanické poškození nosiče, na kterém je záznam uložený. V případě přestřižení některých kovových částí kleštěmi dojde k jejich poškození, a tyto nosiče tak lze podrobit

mechanoskopickému zkoumání za účelem identifikace nástroje, kterým byl nosič poškozen. Prameny elektronických důkazů se rozumí taková zařízení, která produkují, nebo uchovávají data (informace), která jsou důležitá pro trestní řízení, a které mohou mít vliv na jeho průběh a rozhodnutí. Nerozšířenějšími prameny elektronických důkazů mohou být:

- Počítače, notebooky, tablety – jejich hardware (vstupní a výstupní zařízení, procesory, paměti) a software (systémové programy a doplňující programy),
- mobilní telefony a jejich součásti – software mobilního telefonu, paměťové karty, Sim karty,
- paměti - ve formě HDD disků, externích disků, CD, DVD, Blu-Ray,
- počítačové a telekomunikační sítě,
- cloudové úložiště,
- a další.[42]

2.2 Elektronická data jako důkaz

Užíváním počítačových a jiných elektronických systémů a sítí vznikají elektronická data. Tato data poté systém ukládá do určených formátů souborů, které o uživateli, jeho činnosti a životě mohou poskytnout mnoho informací. Pokud jsou tato data získána OČTŘ zákonným způsobem a reprodukována tak, aby poukazovala na určitou skutečnost, a při tom byla srozumitelná pro soud, mohou být užita jako důkaz v trestním řízení. Taková data lze rozdělit na data, která jsou vytvořena uživatelem, a data, která jsou vytvořena softwarem. Uživatel může svou činností v počítačovém prostředí sám vytvářet, upravovat, kopírovat, ale i mazat např. textové soubory, zprávy, obrazové soubory a videosoubory atd., a dále s takovými soubory manipulovat v rámci paměti počítače, jiných pamětí nebo v rámci sítě či síťového úložiště (Cloud). Softwarem bývají při činnosti uživatele vytvářena data, o kterých často běžný uživatel nemusí mít ani představu. Může se jednat o následující data:

[42] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 83-94. ISBN 978-80-210-8073-7.

- **Metadata**

Primárními daty mohou být např. textové soubory, obrazové, zvukové, nebo video soubory. K těmto primárním datům se vážou automaticky programově vytvořené informace tzv. metadata. Metadata jsou jakési podrobnosti o primárních datech. Z těchto podrobností lze právě např. zjistit, kdo je autorem dat, kdy byla data vytvořena, kdy byla změněna, a dále např. délku záznamu, počet stran atd.[43]

- **Provozní a lokalizační údaje**

Těmito daty se rozumí především údaje týkající se komunikačního přenosu, o kterém pojednává zákon č. 127/2005 Sb., o elektronických komunikacích (ZEK), který operátorům ukládá povinnost uchovávat po dobu 6 měsíců takové údaje o uživatelích těchto komunikací.[44] Z těchto údajů lze zjistit např. *„informace o tom, komu bylo voláno, s kým bylo voláno či jak dlouho hovor trval, obdobné informace u SMS a MMS služeb. Dále informace o typu internetového připojení, identifikátor uživatelského účtu, IP adresa, datum a čas připojení do sítě Internet atd.“*[45]

- **Logy**

Jedná se o textové záznamy informací, které vytváří program o své vlastní funkci a o událostech uvnitř programu. Pomocí tohoto procesu lze vysledovat např., kdy došlo k chybě programu, ale také kdo z jaké adresy program otevíral a dělal v něm poslední změny. V oboru editace softwarů a programů, soubor logů umožňuje analýzu a rekonstrukci dat v období, kdy v programu vznikla chyba. V rámci přenosu dat, lze ze souboru logů vyčíst například to, z jaké IP adresy se uživatel připojil k webové stránce, kdy se uživatel připojil a jakou dobu na serveru strávil. Tento soubor logů vygeneruje webový server.[46]

---

[43] POLANSKÝ, Petr. Co jsou metadata dokumentů?. *Exon* [online]. [cit. 9.10.2022]. Dostupné z: https://www.exon.cz/cs/blog/co-jsou-metadata-dokumentu

[44] Viz. § 97 odst. 3 zákona č. 127/2005 Sb., *o elektronických komunikacích* v posledním znění

[45] PŘÍKAZSKÁ, Lenka a Michal MOHELSKÝ. Současná právní úprava data retention je dle Ústavního soudu ústavně konformní a tedy přípustná. *epravo.cz* [online]. 16.10.2019 [cit. 9.10.2022]. Dostupné z: https://www.epravo.cz/top/clanky/soucasna-pravni-uprava-data-retention-je-dle-ustavniho-soudu-ustavne-konformni-a-tedy-pripustna-110069.html

[46] REHBERGER, Ivo. Obsahují webové logy bohatství?. *Lupa.cz* [online]. 30.1.2002 [cit. 9.10.2022]. Dostupné z: https://www.lupa.cz/clanky/obsahuji-webove-logy-bohatstvi/

- **Soubory cache a cookies**

Jedná se o soubory, které vznikají při prohlížení webových stránek. Servery tato data ukládají v uživatelském počítači. Soubory cache slouží k uložení zdrojů webových stránek a mají vliv na rychlejší načítání dat ze serverů, v případě opětovného otevření, tím že se nemusí data načítat znovu celá. Soubory cookies jsou data, vytvářená webovými stránkami za účelem usnadnění přístupu uživateli k již dříve navštíveným webovým stránkám, tím že se tato data ukládají v historii prohlížení a dále umožňují provozovatelům webových serverů např. sledovat uživatelské preference, na základě kterých cílí na uživatele s reklamou nebo zobrazovaným obsahem.[47]

Výše uvedená data se obvykle vyskytují v binárních kódech, programových jazycích, či číselných údajích. V případě použití těchto dat v rámci trestního řízení by měla mít větší důkazní hodnotu taková data, která jsou vytvářena při činnosti uživatele automaticky softwarem, a která nejsou tak snadno změnitelná než data, která uživatel sám vytvořil, a která lze snadno změnit. Jelikož se jedná o data, která jsou pro člověka v mnoha případech nesrozumitelná, je potřeba je před předložením soudu převést do srozumitelné formy v písemné podobě, což se obvykle děje za pomocí k tomu vytvořených programů. Tento proces převodu by v rámci trestního řízení měli mít na starosti analytičtí odborníci, popř. znalci, neboť neodborným jednáním může dojít v nejhorším případě ke smazání důležitých dat, k jejich poškození nebo pozměnění, které může mít za následek snížení jeho důkazní hodnoty. V praxi se vyhodnocováním těchto dat zabývají také policisté SKPV, nebo pokud jim případ náleží, také policisté zařazeni na obvodních odděleních policie.[48]

2.3 Nakládání s elektronickými důkazy

Použitelnost elektronických dat jako důkazů v trestním řízení závisí na dodržení obecných zásad dokazování, kdy je dán zvláštní důraz na otázku dodržení

---

[47] *Difference between Cache and Cookies*. Geeksforgeeks [online]. 5.7.2022 [cit. 9.10.2022]. Dostupné z: https://www.geeksforgeeks.org/difference-between-cache-and-cookies/

[48] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 94-97. ISBN 978-80-210-8073-7.

zákonnosti. K tomu se vyjadřuje ustanovení § 89 odst. 3 TŘ, které říká, že pro trestní řízení nelze použít takové důkazy, které by byly získány nezákonným donucením.[49] Nelze tak nutit podezřelého, aby vydal důkazy o své trestné činnosti, čímž však nejsou dotčena ustanovení, která se týkají vydání popř. odnětí věci a s tímto spojenými domovními a osobními prohlídkami, nebo prohlídkami jiných prostor a pozemků atd. V **kapitole 1.3 Fáze dokazování**, jsou popsány jednotlivé obecné fáze dokazování, které probíhají také v případě dokazování elektronickými důkazy, se specifiky, které vyplývají z podstaty těchto elektronických dat.

- **Opatřování elektronických dat**

Opatření elektronických dat je jedním z prvotních kroků vedoucích k úspěšnému využití těchto dat jako důkazu v trestním řízení. Trestní řád dle názoru autora práce nevěnuje dostatečnou pozornost problematice elektronických dat, což je mimo jiné zapříčiněno rychlostí vývoje výpočetní techniky. V důsledku toho OČTŘ často využívají analogie na procesní ustanovení nejvíce podobná těmto postupům a dále judikáty a stanoviska Nejvyššího státního zastupitelství, popř. vnitřní akty řízení. Samotné zajišťování elektronických dat může být mnohdy problematické, neboť nejenže se jedná o specifickou odbornou oblast, ale s mnoha daty se dá poměrně snadno manipulovat, ať už se jedná o pozměnění, nebo smazání. V několika okamžicích lze relativně snadno vymazat velké množství dat. Je nepochybně snadnější smazat usvědčující kompletní transakční listiny, než se zbavit těla zavražděného. To jen dokazuje, jak složité může být dokazování elektronickými důkazními prostředky. Další potíže mohou nastat v okamžiku, kdy jsou data zajišťována neodbornou manipulací ze strany Policie ČR, nebo ze strany majitele takového zařízení (př. stažení kamerových záznamů z prodejny potravin jejím pracovníkem), což může vést k částečnému nebo úplnému a nevratnému poškození takových dat. Elektronická data lze obecně opatřit pro účely trestního řízení následujícími způsoby.

[49] Viz. § 89 odst. 3 zákona č. 141/1961 Sb., *Trestní řád* v posledním znění

- ***„Zajištěním zařízení nebo datových nosičů, na kterých jsou počítačová data uchovávána.“***[50]

Nejčastějším úkonem souvisejícím s opatřováním věcí důležitých pro trestní řízení je dobrovolné vydání věci podle § 78 TŘ. V případě, že osoba, která takovou věc má a neuposlechne výzvy k jejímu vydání, musí počítat s tím, že ji může být uložena pořádková pokuta podle § 66 TŘ, a i přesto ji věc může být na základě rozhodnutí státního zástupce či policejního orgánu za splnění zákonných povinností odňata podle § 79 TŘ.[51] Postupy směřující k vydání a odnětí věcí se týkají také nosičů, na kterých mohou být uložena elektronická data. Takovými nosiči jsou např. počítače, mobilní telefony, paměťové karty, externí a pevné disky, atd. Trestní řád přitom nerozlišuje, zda se jedná o např. o služební externí disk, nebo soukromý mobilní telefon, čímž ponechává poměrně široké mantinely pro zajištění těchto nosičů, neboť každý z těchto nosičů může obsahovat informace různého charakteru ve vztahu k soukromí dotčené osoby. Zároveň tyto nosiče mohou disponovat různým stupněm zabezpečení.[52] Dalšími procesními úkony k opatření takových zařízení a nosičů mohou být domovní prohlídky a prohlídky jiných prostor a pozemků (§ 82 – 85c TŘ), ve kterých se mohou tato zařízení a nosiče nacházet. *„Nařídit domovní prohlídku je oprávněn předseda senátu a v přípravném řízení na návrh státního zástupce soudce.“*[53] Totožné platí i o provedení prohlídek jiných prostor a pozemků, s tím rozdílem, že v tomto případě lze prohlídku vykonat i bez příkazu, pokud věc nesnese odkladu. Policejní orgán musí o souhlas s prohlídkou dodatečně požádat, a pokud jej neobdrží, není možné výsledek prohlídky a zjištěné informace použít jako důkaz. Prohlídku jiných prostor a pozemků je možné vykonat bez příkazu také, pokud dotčená osoba písemně předem souhlasí s provedením prohlídky.[54] V případě zajištěných zařízení a nosičů kterýmkoliv z výše uvedených způsobů, je nutné do protokolu uvést co

---

[50] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 101. ISBN 978-80-210-8073-7.

[51] Viz § 78 až 79 zákona č. 141/1961 Sb., *Trestní řád* v posledním znění

[52] STUPKA, Václav, Jan PROVAZNÍK a Jakub VOSTOUPAL. Elektronické důkazy jako výzva pro trestní proces. *Právník. Teoretický časopis pro otázky státu a práva* [online]. 2022, roč. 161, č. 4. s. 332-349. [cit. 25.1.2023]. ISSN0231-6625. Dostupné z: https://www.ilaw.cas.cz/upload/web/files/pravnik/issues/2022/4/3_Stupka-Provaznik-Vostoupal_332-349_4_2022.pdf

[53] Viz § 83 odst. 1 zákona č. 141/1961 Sb., *Trestní řád* v posledním znění

[54] Viz § 83a zákona č. 141/1961 Sb., *Trestní řád* v posledním znění

nejvíce informací o zajišťované věci tak, aby ji nebylo možné zaměnit za jinou (výrobce, typ, barva, výrobní číslo, IMEI, poškození, atd.). Takto zajištěná zařízení a nosiče lze následně podrobovat zkoumání za účelem zjištění obsahu úložiště.

- ***„Získáním přímého přístupu k počítačovým datům uchovaným v počítačových systémech.“***[55]

Takovým způsobem je možné zajistit data, která nejsou přímo uložena v zařízení, ale která jsou se zařízením nějak propojena, respektive s pomocí zařízení se k nim lze „na dálku“ připojit. Pokud se jedná o volně dostupná data v síti, která nejsou ničím zabezpečena, neváže se na ně žádné omezení, co se týká jejich zajištění. Pro pořizování důkazů z těchto volně dostupných informací není třeba žádné povolení. Může se jednat např. o webové stránky, ze kterých lze vhodným způsobem vyčíst informace jen při samotném použití internetového prohlížeče. Internetové stránky nemusí být stálé, proto je doporučeno provést co nejvíce úkonů směřujících k zajištění co největšího množství dat, která lze v té době zajistit (videodokumentace, fotodokumentace, zdrojový kód stránky, atd.). K datům, která nejsou volně dostupná, ale jsou např. opatřena přístupovým jménem a heslem, si mohou OČTŘ zjednat přístup na základě dobrovolného sdělení těchto údajů a souhlasu s přístupem do tohoto prostoru od oprávněné osoby např. při podání vysvětlení podle § 158 odst. 6 TŘ. To, že dotčená osoba dobrovolně vydá OČTŘ přístupové údaje je ideální stav, nicméně ne vždy se lze spoléhat na to, že osoba je ochotna spolupracovat s OČTŘ. Pokud se tedy jedná o vzdálená data, která jsou uložená v jiných počítačových systémech, a která jsou zabezpečená přístupovými údaji, je pro jejich zajištění nutný jiný postup, než v případě volně dostupných dat. OČTŘ v takovém případě musí postupovat na základě oprávnění, které jim v určitých případech přiznává ustanovení § 158d odst. 3 TŘ o sledování osob a věcí, které mimo jiné pojednává o takovém způsobu sledování, při kterém má být zjišťován obsah písemností a záznamů uchovávaných v soukromí za použití technických prostředků. K takovému postupu je potřeba předchozího souhlasu soudce. Bez souhlasu nelze zahájit sledování a informace získané bez

[55] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 101. ISBN 978-80-210-8073-7.

souhlasu nelze použít v rámci trestního řízení, což může vést ke zmaření velké části případných důkazů. Může se jednat o případy, kdy policie zajistí počítač nebo jiné zařízení, ve kterém zůstane uživatel přihlášen k e-mailové schránce, nebo ve kterém jsou přístupové údaje do takové schránky přednastaveny. Fakt, že případný přístup do schránky by v takovém případě nepředstavoval žádné větší technické obtíže, nedává OČTŘ právo k tomu, aby bez povolení vstupovaly do soukromého prostoru a zajišťovaly z nich tato data.[56]

- ***„Získáním počítačových dat od poskytovatelů služeb.“***[57]

Tímto způsobem lze získat mnoho důkazů, aniž by uživatel, o jehož data se jedná, pojal jakékoliv podezření o zájmu policejního orgánu, což může být z hlediska taktického postupu významným činitelem. Tito poskytovatelé služeb se mohou orientovat na telekomunikační služby nebo informační služby. Pod telekomunikačními službami si lze představit provoz a zajišťování elektronické komunikační sítě a přiřazených prostředků (infrastruktura těchto sítí). Poskytovatelé těchto služeb jsou podle zákona č. 127/2005 Sb., o elektronických komunikacích (ZEK) povinni po dobu 6 měsíců uchovávat provozní a lokalizační údaje.[58] Naproti tomu na poskytovatele informačních služeb se taková povinnost nevztahuje a řídí se zákonem č. 480/2004 Sb., o některých službách informační společnosti. Informačními službami se rozumí poskytování služeb v rámci provozovaní elektronické komunikační sítě, které zpřístupňují uživatelům tyto služby (e-mail, cloudová úložiště, webové servery, webové vyhledávače, atd.).[59] Způsob zajištění dat se odvíjí od míry ochrany a zabezpečení těchto dat. Pokud se jedná o data, která nejsou nijak zabezpečena, a na něž se nevztahuje telekomunikační tajemství, je poskytovatel těchto služeb na žádost OČTŘ podle § 8 odst. 1 TŘ povinen takové údaje a data poskytnout pro účely trestního řízení.

---

[56] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 103-106. ISBN 978-80-210-8073-7.

[57] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 101. ISBN 978-80-210-8073-7.

[58] Viz. § 97 odst. 3 zákona č. 127/2005 Sb., *o elektronických komunikacích* v posledním znění

[59] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 106. ISBN 978-80-210-8073-7.

To se může týkat informací a dat nejrůznějšího charakteru. Pokud se jedná o data, která jsou chráněna např. přístupovým jménem a heslem, je pro zajištění těchto dat nutné postupovat v souladu s ustanovením § 158d odst. 3 TŘ. Příkladem může být zajišťování aktuálního stavu e-mailové schránky, neboť data a komunikace, která se nachází v této schránce, mají charakter jiných písemností a záznamů, která jsou uchovávána v soukromí, a to i přesto, že se jedná o virtuální komunikace a data, která nemají povahu klasických listin.[60] Pokud se jedná např. o obsah komunikací v reálném čase, nikoliv o obsah již přečtených zpráv a komunikací budoucí, musí OČTŘ postupovat v souladu s ustanovením § 88 TŘ, neboť takovýto zásah do komunikace uživatelů, by se dal přirovnat k provádění odposlechu. Totožný postup je nutný v případě, že se jedná o zjišťování obsahu elektronické komunikace, která má v budoucnu probíhat na již zajištěném nosiči (př. Policie ČR zajistí mobilní telefon v souladu ustanovením § 78 TŘ, a nová příchozí komunikace, se kterou se uživatel již nemohl seznámit, jsou OČTŘ oprávněny použít pouze za předpokladu splnění zákonného postupu tohoto ustanovení).[61] Zajištění provozních a lokalizačních údajů, na něž se vztahuje ZEK, je možné za využití ustanovení § 88a TŘ. Tímto postupem lze získat informace o proběhnuvší komunikaci, ale nikoliv o obsahu této komunikace.

- **Povinnost uchovávat data podle § 7b trestního řádu**

Mimo předchozí postupy stojí nový institut, který přijal zákon č. 287/2018 Sb., změna trestního zákoníku a některých dalších předpisů. Tento pozměňovací zákon se dotkl také trestního řádu, do kterého přidal ustanovení § 7b. To se poměrně ze široka vyjadřuje k povinnosti uchovávat data uložená v počítačovém systému nebo na jiném nosiči. Postup v souladu s tímto ustanovením umožňuje uložení dvou povinností dotčeným osobám. Lze takto nařídit prakticky komukoliv, aby uchoval v nezměněné podobě data důležitá pro trestní řízení, pokud je předpoklad, že by tato data mohla být ztracena, zničena či pozměněna. Dále lze v souladu s tímto ustanovením přikázat, aby dotčená osoba neumožnila přístup

[60] Výkladové stanovisko NSZ č. 1/2015 Sb., *ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů včetně obsahu e-mailových schránek*
[61] Tamtéž

k těmto datům dalším osobám. Tím má být dosaženo zabránění v pokračování nebo opakování trestné činnosti. Příkaz k uchování dat nebo k zamezení přístupu k takovým datům, je oprávněn vydat předseda senátu a v přípravném řízení také státní zástupce, nebo s jeho souhlasem policejní orgán. Policejní orgán nepotřebuje povolení státního zástupce, pokud věc nesnese odkladu a pokud nelze tohoto souhlasu předem dosáhnout. Je důležité zmínit, že ustanovení se vztahuje vždy jen na data, která již existují a dotčená osoba je povinna taková data uchovat, nebo k nim zamezit přístup na dobu uvedenou v příkazu, což může být maximálně 90 dnů.[62] Tento institut tedy nelze využít na data, která mají vzniknout až v budoucnosti a nelze tak hovořit o paralele k institutu sledování podle § 158d TŘ nebo odposlechu ve smyslu § 88 TŘ. Jedná se o předběžné opatření, které klade za úkol uchovat tato data do doby, než bude rozhodnuto o jejich zajištění pomocí dalších procesních úkonů (§ 78, § 79, § 158d TŘ a dalších). Toto opatření na rozdíl od jiných předběžných opatření nemusí směřovat jen proti podezřelému, ale může se týkat prakticky každého, kdo tato data má ve své moci. Měla by být dodržena zásada přiměřenosti a příkaz by měl směřovat pouze na data, která jsou důležitá pro trestní řízení. Tímto není dotčen postup týkající se zajišťování údajů o uskutečněném telekomunikačním provozu podle § 88a TŘ, neboť ten je dostatečně a podrobně popisován v samostatném ustanovení a nelze tedy tyto údaje poskytovat na základě ustanovení § 7b TŘ a tímto způsobem obcházet zákonný postup pro vydání takových údajů. Prakticky by postup podle ustanovení § 7b TŘ měl policejní orgán realizovat prostřednictvím Útvaru zvláštních činností služby kriminální policie a vyšetřování (ÚZČ SKPV), tak jako např. odposlechy, či vyžádání údajů o telekomunikačním provozu.[63]

- **Analýza dat**

To, že OČTŘ získá určitá data, o kterých předpokládá, že by mohla být důležitá pro trestní řízení, ještě neznamená, že opravdu bude možné tato data použít jako důkaz. Analýza dat je dalším podstatným krokem v procesu dokazování elektronickými důkazy, neboť mnoho zajištěných dat nemá žádnou souvislost

[62] Viz. § 7b zákona č. 141/1961 Sb., *Trestní řád* v posledním znění
[63] Stanovisko OBP Ministerstva vnitra ČR, *k aplikaci ustanovení § 7b trestního řádu* ve znění k 21. 8. 2019

s prověřovanou věcí a je nutné tato data vyhodnotit a vytřídit z nich ta, která by mohla mít povahu důkazu v trestním řízení. Problémem elektronických dat ve složitějších případech je, že do fáze analýzy často nelze v prvním okamžiku zcela jasně určit, která data budou v dalším procesu důležitá, a která ne. Dalším problémem může být samotný charakter dat, neboť některá elektronická data mohou být pro laika v původní formě nesrozumitelná. Naopak výhodou elektronických dat je možnost relativně rychlého a bezpečného kopírování dat, čímž osobě, o jejíž data se jedná, obvykle nevzniká žádná újma ve smyslu odebrání těchto dat. Úkolem analýzy dat je vytřídit podstatná data a následně je interpretovat tak, aby je bylo možné použít jako důkaz, což bývá zpracováno v listinné podobě ve formě úředního záznamu, protokolu, odborného vyjádření nebo znaleckého posudku. Nejčastějším postupem analýzy dat je tedy ohledání zařízení (popř. nosiče, e-mailové schránky, atd.), vypracování odborného vyjádření a znaleckého posudku.[64] Ohledání provádí policejní orgán za pomocí dostupných zařízení a prostředků (obvykle za pomocí PC a jeho ovládacích zařízení). V souvislosti s ohledáním zařízení je nutné postup řádně zaprotokolovat a vytvořit příslušnou dokumentaci. Touto dokumentací je myšlena videodokumentace a fotodokumentace, která však nemusí být vždy dostatečná a některá podstatná data mohou být i přesto přehlédnuta. Především v souvislosti se složitými případy je vhodné vytvořit bitovou kopii celého nosiče pomocí speciálních zařízení a softwarů, které jsou schopné přenést všechna data z nosiče, a to včetně skrytých dat. Při ohledání nosičů je nutné popsat postup, kterým byla data stažena a popsat cestu k místu v paměti zařízení, kde se data nacházela. Data je následně vhodné zkomprimovat pomocí programů (např. Winrar) a opatřit je tzv. kontrolním otiskem souborů tzv. „Hash kódem“ vytvářeným speciálním programem (např. CHK Hash Tool). Tento program dokáže pomocí speciálních algoritmů vytvořit textový kód složený z písmen a číslic, který v přenesené formě odpovídá přesně zálohovaným datům. V případě změny těchto dat, by se pozměnil i tento kód. Tímto postupem se zaručí, že s daty nebylo nijak manipulováno a jedná se o původní data.

---

[64] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 109-112. ISBN 978-80-210-8073-7.

Pro příklad lze uvést krátký hash kód hashovací funkce MD5, vytvořený programem Python, který dokazuje, jak rozdílný kód je vytvořen pro slova „koala“ a „kaola“.

*„python md5.py **"koala"***   *HASH MD5: **a564de63c2d0da68cf47586ee05984d7***   *VELIKOST: 32*   *python md5.py **"kaola"***   *HASH MD5: **ffd11199b517ddffb8070f7f7c77ddc6***   *VELIKOST: 32“*[65]

Takto získaná data může analyzovat a vyhodnocovat policejní orgán, který data zajistil, popř. přibraný znalec. Policejní orgán k tomu může využít nejrůznější postupy. Pokud se např. jedná o analýzu dat z mobilního telefonu, ve kterém by se měla nacházet dětská pornografie, může policejní orgán rovnou přistoupit k vyhodnocování pouze souborů v příslušných formátech, který se týká videozáznamů a obrazových záznamů (.jpg, .BMP, .avi, .mp4, atd.). Pokud je např. potřeba vyhodnotit komunikaci z poskytnutých screenshotů obrazovky telefonu od poškozeného, je vhodnější, aby se tímto zabýval policejní orgán než znalec. Pokud má znalec provést analýzu dat, je nutné ho přibrat opatřením podle § 105 TŘ. Přibrání znalce je vhodné zejména pokud má jít o technicky náročnou analýzu, neboť mnoho článků Policie ČR zkrátka nedisponuje potřebnými programy, zařízeními ani znalostmi pro hlubší analýzu těchto dat. Výhodou přibrání znalce je, že se odborně vyjádří k položeným otázkám, které se týkají vnějších částí nosičů či zařízení a dat, jejich technické stránce a obsahu. Znalecký posudek, který je výsledkem jeho činnosti lze použít u soudu jako důkaz. Znalci tuto činnost ale neprovádí bezplatně a zároveň obvykle vyhotovení znaleckého posudku trvá déle, než analýza a vyhodnocení, které vypracuje policejní orgán, což je další důvod, proč se znalci nepřibírají ke každému případu. Další možností analýzy dat je vyhotovení odborných vyjádření, která nejčastěji zpracovávají

[65] JAHUŇÁK, Petr. Šifry, kódy a hashovací funkce (1.část). *blog.hackerlab.cz* [online]. 16.1.2016 [cit. 19.10.2022]. Dostupné z: https://blog.hackerlab.cz/sifry-kody-a-hashovaci-funkce-1cast/

pracoviště Odborů kriminalistické techniky a expertizy Policie ČR (OKTE). Odborná vyjádření lze použít jako důkaz v trestním řízení, ale nedosahují takové právní síly, která je přikládána znaleckým posudkům.[66]

- **Provádění a hodnocení elektronických důkazů**

V souladu s dodržením zásad ústnosti a bezprostřednosti se obvykle důkazy provádějí před soudem ústní formou. Nejčastějším způsobem provedení důkazu je výslech a další možností provedením důkazu ústní formou, je přečtení listinných důkazů. Z toho důvodu je nutné elektronické důkazy často převádět do takové formy, aby mohly být před soudem provedeny, pokud je nelze provést v původní podobě. Elektronika je náročným technickým oborem, kterému do hloubky rozumí pouze odborníci, tak jako je to u každého jiného odvětví. Dokazování elektronickými důkazy v původní podobě před soudem je často nemožné, neboť soudy nedisponují potřebnými zařízeními a charakter mnoha důkazů zkrátka není možné interpretovat v původní podobě a vyžaduje zpracování a přenesení do srozumitelnější podoby takovým způsobem, aby nebylo možné tento postup napadnout pro pozměnění dat, k čemuž slouží právě ohledání, znalecké posudky, či odborná vyjádření, jak je uvedeno v předchozí kapitole. Některé soudy dávají přednost přečtení protokolu o ohledání před využitím původních dat, a to i přesto, že by je bylo možné bez problémů v původní podobě provést (soudce raději přečte protokol o ohledání datového nosiče, na kterém se nachází videozáznam s dětskou pornografií, místo přehrání takového videozáznamu). Vývoj forenzních technologií a procesní změna v tomto směru, by dle autora mohla mít kladný vliv na rychlost řízení, neboť vypracování znaleckých posudků obvykle trvá i několik měsíců a převádění původních dat do srozumitelné formy, často protahuje celé řízení. Podstatou důkazů je prokázat vinu či nevinu obviněného, popř. jiná tvrzení, která mají souvislost s trestním řízením. Při hodnocení elektronických důkazů je kladen důraz především na zjištění otázky zákonnosti při zajišťování a opatřování dat. Dalším neméně důležitým hlediskem souvisejícím s hodnocením

[66] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 109-112. ISBN 978-80-210-8073-7.

elektronických důkazů je ustanovení původního zdroje a autora těchto dat.[67] „*Hodnocení elektronických důkazů je závislé především na technických parametrech – na charakteru příslušných dat, jejich zdroji, metodě jejich získání a uchování, využitých interpretačních, analytických a forenzních nástrojích apod. Tyto faktory mohou ovlivňovat důkazy oběma směry: nejenže nevhodný postup při zajištění důkazů může způsobit jejich znehodnocení nebo snížení jejich důkazní síly, ale může nastat i opačná situace, kdy například využitý forenzní nástroj vygeneruje nespolehlivé nebo nesprávné výstupy.“*[68]

[67] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 112-114. ISBN 978-80-210-8073-7.

[68] STUPKA, Václav, Jan PROVAZNÍK a Jakub VOSTOUPAL. Elektronické důkazy jako výzva pro trestní proces. *Právník. Teoretický časopis pro otázky státu a práva* [online]. 2022, roč. 161, č. 4. s. 332-349. [cit. 25.1.2023]. ISSN0231-6625. Dostupné z: https://www.ilaw.cas.cz/upload/web/files/pravnik/issues/2022/4/3_Stupka-Provaznik-Vostoupal_332-349_4_2022.pdf

3 Dokazování e-mailem

Pojem e-mail (Electronic mail) lze přeložit jako elektronická pošta. E-mail je specifickým elektronickým prostředkem, který má podobu zabezpečené elektronické schránky, opatřené přístupovými údaji konkrétního uživatele, sloužící ke vzdálené komunikaci s dalšími uživateli. V současné době je v podstatě nemožné fungovat ve virtuálním světě, aniž by člověk vlastnit e-mail. Původně tyto e-mailové schránky sloužily k elektronické komunikaci, především za pomocí textových zpráv. V současnosti lze e-mailem rozesílat soubory různých formátů jako přílohu zprávy. Společnost Seznam.cz, která je největší tuzemskou společností poskytující tyto služby, uvádí, že maximální velikost přílohy na této platformě může být až 50 MB.[69] Pomocí e-mailu je možné zprávy psát, odesílat jiným uživatelům, přijímat a přeposílat. Mezi nejrozšířenější domény e-mailové patří Gmail, Outlook.com, email.cz, seznam.cz, centrum.cz a další. Tuto službu, zřizují poskytovatelé informačních služeb, na něž se vztahuje zákon č. 480/2004 Sb., o některých službách informační společnosti. Zřízením účtu si uživatel nejprve pojmenuje svou vlastní schránku tak, aby byla jedinečná a nepoužíval ji již jiný uživatel a následně je povinen tuto schránku zabezpečit zvoleným heslem. Některé společnosti již vyžadují, nebo nabízí také tzv. dvoufázové ověření uživatele, což znamená, že uživatel je povinen potvrdit přihlášení na dalším zařízení, obvykle na mobilním telefonu, na který je zaslán jednorázový kód, který slouží k ověření, zda se jedná o dotyčnou osobu, a nikoliv o program či jinou osobu. Jedná se o bezpečnostní nastavení. Totožný postup vyžadují např. také banky při přihlášení do internetových klientů. E-mailová schránka je nezbytná pro jakoukoliv činnost ve virtuálním světě. Její zadání je požadováno v případě nákupů přes internet, k ověření totožnosti uživatele, k možnosti instalace dalších softwarů do jiných zařízení, ale třeba již také pro zřízení bankovního účtu atd. Osobní e-mailový účet by se dal zjednodušeně přirovnat k internetovému občasnému průkazu, bez kterého sice lze prohlížet webová rozhraní, ale pokud uživatel chce využívat další funkce webů, či aplikací, zřízení e-mailové schránky se nevyhne. Adresa e-mailové schránky může mít

[69] *Práce s přílohami*. Seznam.cz [online]. [cit.19.10.2022]. Dostupné z: https://napoveda.seznam.cz/cz/prilozeni-prilohy/

následující podobu: TommmmNovotny@server.cz, přičemž „TommmmNovotny“ je v tomto případě jméno schránky zvolené uživatelem. „@server.cz“ je označení zařízení DNS, které je dostupné z internetu (Domain Name System), a na kterém probíhá služba MTA (Mail Transfer Agent), která slouží k zasílání zpráv mezi různými poštovními servery (Gmail.com, seznam.cz, atd.). Uživatel se do své zvolené e-mailové schránky může přihlašovat prostřednictvím webových serverů, nebo pomocí POP a IMAP protokolů, umožňující stažení klienta do svého zařízení. Pomocí těchto protokolů si může svou komunikaci stahovat do zařízení. Celý proces přenosu dat (odeslání zprávy) řídí protokol SMTP (Simple Mail Transfer Protocol), který má za úkol kontaktovat server MTA a předat mu data.[70] Z hlediska trestního řízení se často důležitá data nenachází jen v obsahu komunikace, ale také v hlavičce e-mailu, která skrývá mnoho doplňujících údajů o samotné komunikaci, ale také o uživateli. Příklad hlavičky doručeného e-mailu:

```
Received: from unknown ([::ffff:89.103.20.203])
        by email.seznam.cz (szn-ebox-5.0.26) with HTTP;
        Thu, 14 May 2020 13:21:28 +0200 (CEST)
From: Pavel <brabii03@seznam.cz>
To: <TommmmNovotny@seznam.cz>
Subject: =?utf-8?q?OP=C4=8C?=
Date: Thu, 14 May 2020 13:21:28 +0200 (CEST)
Message-Id: <9e0.EmZQ.6m2y{1GThIl.1UlIcu@seznam.cz>
Mime-Version: 1.0 (szn-mime-2.0.57)
X-Mailer: szn-ebox-5.0.26
Content-Type: multipart/mixed;
        boundary="=_60f420a87de8400f5ed3eba0=ad724210-a21b-5478-b7a3-
08ee1ead6136_="

--=_60f420a87de8400f5ed3eba0=ad724210-a21b-5478-b7a3-08ee1ead6136_=
Content-Type: text/plain;
        charset=utf-8
Content-Transfer-Encoding: quoted-printable


--=_60f420a87de8400f5ed3eba0=ad724210-a21b-5478-b7a3-08ee1ead6136_=
Content-Type: application/msword;
        name="statnice_opc_cela.doc"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
        size=869888;
        filename="statnice_opc_cela.doc"
Content-Id: <i00276335172801960 3>

--=_60f420a87de8400f5ed3eba0=ad724210-a21b-5478-b7a3-08ee1ead6136_=--
```

[70] PERNICA, Tomáš. Jak funguje mail. *Tomp.eu* [online]. 20.3.2008 [cit. 20.10.2022]. Dostupné z: https://www.tomp.eu/2008/03/20/jak-funguje-email/

Z uvedeného příkladu lze vyčíst následující informace.

Recieved: označení serverů, skrze které e-mail procházel. IP adresy od nejstarších (odesílatel) po nejnovější (příjemce) - IP adresa (Internet Protocol) je číslo, které odlišuje různá síťová rozhraní, na základě kterého lze s pomocí poskytovatelů informačních služeb zjistit geografické místo, kde bylo zařízení připojeno k internetové síti. Může mít podobu zvýrazněného čísla v hlavičce e-mailu (89.103.20.203),
From: e-mailová adresa odesílatele e-mailu,
To: e-mailová adresa příjemce,
Subject: předmět e-mailu,
Date: datum a čas odeslání e-mailu,
Message-Id: unikátní číslo zprávy (pro správce serveru),
X-Mailer: program, který byl použit pro odeslání mailu,
Content Type: kódovaný obsah e-mailu, popř přílohy a jejího formátu.[71]

3.1 Zajištění dat

Dokazování e-mailem není snadnou procedurou a postup OČTŘ pro zajištění těchto dat a informací z e-mailové schránky závisí na více faktorech. Data a komunikace, která se nachází v e-mailové schránce, jsou opatřena přístupovým jménem a heslem, tudíž je nutné k nim přistupovat jako k listinám, které jsou uchovávány v soukromí uživatele. Trestní řád neposkytuje přesný návod, jak při zajišťování obsahu e-mailové schránky postupovat a OČTŘ se musí spoléhat na výkladová stanoviska. Problematice se zajišťováním obsahu e-mailové schránky se podrobně věnuje Výkladové stanovisko Nejvyššího státního zastupitelství poř. č. 1/2015.[72] V souvislosti s trestním řízením se OČTŘ mohou setkat s různými druhy dat, uložených různým způsobem, které mají různý stupeň ochrany, přičemž může jít o následující data.

[71] *Jak číst hlavičku zprávy*. Seznam.cz [online]. [cit. 26.10.2022]. Dostupné z: https://napoveda.seznam.cz/cz/email/jak-cist-hlavicku-zpravy/
[72] Výkladové stanovisko NSZ č. 1/2015 Sb., *ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů včetně obsahu e-mailových schránek*

- **Elektronická data a obsah komunikace, která jsou uložená v zařízení** (v mobilním telefonu, počítači, na pevném disku, externím disku, atd.),
- **Elektronická data a obsah komunikace, která jsou uložená v jiném zařízení** (online) v e-mailové schránce, která je opatřena přístupovými údaji uživatele a zařízení je pouze přístupovým bodem ke schránce,
- **Doplňující informace** o e-mailové schránce a uživateli.[73]

- **Elektronická data a obsah komunikace, která jsou uložená v zařízení**

Některá zařízení a poskytovatelé e-mailových služeb nabízejí možnost provázání více e-mailových schránek různých poskytovatelů, kdy přes e-mailového klienta je tato pošta sjednocena v jednom programu, ve kterém je možné nastavit stahování kontaktů, obsahu komunikace a dalších doplňujících informací do paměti zařízení uživatele (Outlook). Tato zařízení a nosiče dat mohou být zajišťována jako věci důležité pro trestní řízení, čímž je myšlen postup následujícími způsoby: vydáním věci (§ 78 TŘ), odnětím věci (§ 79 TŘ), zajištěním při ohledání místa činu (§ 113 TŘ), nebo v souvislosti s prováděním domovní nebo osobní prohlídky, či prohlídky jiných prostor a pozemků (§ 82 – 85c TŘ).[74] K datům uloženým v těchto zařízeních, lze přistupovat dvěma způsoby, z hlediska toho, v jaké fázi bylo zařízení zajištěno.

- **Zajištění elektronických dat a obsahu komunikace uložené v zařízení, která proběhla před zajištěním zařízení**

Zajištěná zařízení a nosiče podle výše uvedených úkonů, lze následně podrobovat zkoumání bez dalších omezení ve smyslu povolení či příkazů soudu. To se dotýká také obsahu zpráv a komunikací uložených v těchto zařízeních či nosičích v době, kdy jsou zajištěny. To znamená, že pokud komunikace proběhla do doby zajištění a uživatel měl možnost se s obsahem seznámit, mohou k těmto datům OČTŘ přistupovat bez omezení.[75] Tím není dotčen přístup ke zprávám a komunikacím

---

[73] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 121-123. ISBN 978-80-210-8073-7.

[74] Viz. § 78 až 113 zákona č. 141/1961 Sb., *Trestní řád* v posledním znění

[75] Výkladové stanovisko NSZ č. 1/2015 Sb., *ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů včetně obsahu e-mailových schránek*

nacházejícím se v internetovém prostředí. Nelze tak přistupovat do vzdálených schránek i přesto, že na zařízení je např. neustále připojený e-mail klient, nebo pokud jsou přístupové údaje do takové schránky v zařízení vyplněny předem.[76]

- **Zajištění elektronických dat a obsahu komunikace uložené v zařízení, která proběhla po zajištění zařízení**

Je-li předpoklad, že po zajištění nosiče či zařízení bude probíhat další komunikace (příjem zpráv), která bude ukládána do paměti zařízení nebo nosiče, a má-li být tato komunikace důležitá pro trestní řízení, může OČTŘ zjišťovat obsah této komunikace pouze na základě příkazu předsedy senátu, nebo v přípravném řízení soudce, který jej vydá na základě předchozího návrhu státního zástupce podle ustanovení § 88 TŘ. Toto ustanovení TŘ hovoří o odposlechu a záznamu telekomunikačního provozu. Podstatnou podmínkou pro tento postup je, že oprávnění podle ustanovení § 88 TŘ lze využít, pouze pokud se jedná o trestní řízení v souvislosti s úmyslným TČ, na který zákon stanoví trest odnětí svobody s horní hranicí nejméně 8 let, nebo pro vyjmenované trestné činy v tomto ustanovení TŘ. Bez příkazu soudu, lze toto ustanovení využít v souvislosti s některými taxativně vyjmenovanými trestnými činy v TŘ, pokud s tím dotčený uživatel takového zařízení souhlasí. Může se jednat o případy, kdy je prováděna domovní nebo jiná prohlídka podle TŘ, při které jsou tyto nosiče zajištěny, a na kterých dále probíhá komunikace, se kterou se uživatel již nemohl seznámit, nebo dále v případě zadržení podezřelého atd.[77]

---

[76] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 104-105. ISBN 978-80-210-8073-7.

[77] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 123-125. ISBN 978-80-210-8073-7.
Výkladové stanovisko NSZ č. 1/2015 Sb., *ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů včetně obsahu e-mailových schránek*

- **Elektronická data a obsah komunikace, která jsou uložená v jiném zařízení (online) v e-mailové schránce, která je opatřena přístupovými údaji uživatele a zařízení je pouze přístupovým bodem ke schránce**

Jedná se o data, která nejsou ukládána do vnitřní paměti zařízení či datového nosiče, ale nachází se uložená ve virtuálním prostředí v e-mailových schránkách na serverech, cloudech atd. Přístup do tohoto prostředí je zabezpečen přístupovými údaji, a proto je nutné na taková data nahlížet jako na písemnosti a záznamy uchovávané v soukromí. Poskytovatelé e-mailových služeb nemají oprávnění uchovávat obsah komunikace uživatelů a poskytovat je OČTŘ a nelze tedy požadovat vydání takového obsahu např. na základě žádosti ve smyslu ustanovení § 8 odst. 1 TŘ. Také v případě zajišťování obsahu e-mailových schránek se postup OČTŘ bude lišit v závislosti na několika faktorech.[78]

- **Poskytnutí přihlašovacích údajů oprávněným uživatelem**

V ideálním případě při zajišťování elektronických dat a obsahu komunikací z elektronických schránek uživatele dojde k tomu, že sám oprávněný uživatel dobrovolně umožní OČTŘ přístup do schránky a poskytne přístupové údaje do takové schránky. To se obvykle týká oznamovatelů a poškozených, neboť se má za to, že vydání takové komunikace je v jejich prospěch a na základě těchto dat a informací, které uvedou v podání vysvětlení, lze zahájit úkony v trestním řízení. Jedná se o případy, kdy osoba vydá, nebo předloží nosič, podle § 78 TŘ popř. pouze sdělí přihlašovací údaje v podání vysvětlení podle § 158 odst. 6 TŘ, za účelem ohledání e-mailové schránky a zajištění obsahu komunikace, uložené v této schránce. OČTŘ v tomto případě nepotřebují žádné další povolení či příkaz k zajištění těchto dat. Může se stát, že takovéto údaje dobrovolně poskytne také podezřelý či obviněný, a to především v případech, kdy zdůrazňuje, že nemá před

---

[78] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 125-129. ISBN 978-80-210-8073-7.
Výkladové stanovisko NSZ č. 1/2015 Sb., *ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů včetně obsahu e-mailových schránek*

policií co skrývat, popř. že se ve schránce nachází komunikace či data, která by mohla vyvrátit podezření ze spáchání TČ a podpořit jeho tvrzení.[79]

- **Zajištění zařízení, které je přístupovým bodem k elektronické schránce**

Při postupu směřujícím k zajištění důležitých věcí pro trestní řízení (domovní prohlídky, prohlídky jiných prostor a pozemků, vydání, odnětí věci, ohledání místa činu atd.) bývají častým předmětem zajištění také elektronická zařízení, ze kterých se uživatel přihlašuje do své e-mailové schránky. Pokud je na takovém zařízení stále uživatel přihlášen pomocí e-mailového klienta, nebo pokud se v internetovém prohlížeči nachází předem uložené přístupové údaje do e-mailové schránky, neopravňuje to OČTŘ k přístupu k datům, která jsou v těchto schránkách uložená. Takový přístup do elektronické schránky nebo jiného vzdáleného úložiště, je bez zákonného oprávnění, narušením soukromí a takto získané údaje OČTŘ nemohou použít v trestním řízení jako důkaz. K takovým datům má policejní orgán právo přistoupit za účelem ohledání a vytvoření „datového otisku" elektronické schránky pouze za splnění podmínek ustanovení § 158d odst. 1 a 3 TŘ.[80] Toto ustanovení říká, že pro zásah do soukromí tímto způsobem, je potřeba předchozího souhlasu soudce. Bez takového souhlasu nelze zahájit „sledování" a takto získané informace nelze použít v rámci trestního řízení.[81] Tímto postupem lze zjistit obsah zpráv odeslaných, odstraněných (v koši), rozepsaných a doručených včetně těch, které si uživatel mohl přečíst, ale dosud nepřečetl. Takto zajistit obsah e-mailové schránky je policejní orgán oprávněn provést pouze za účelem provedení kopie (otisku) schránky komunikace, která již proběhla v minulosti, a která bude následně vyhodnocována a analyzována. Je nepřípustné, aby policejní orgán vstupoval do této schránky opakovaně, nebo aby na základě

---

[79] Výkladové stanovisko NSZ č. 1/2015 Sb., *ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů včetně obsahu e-mailových schránek*

[80] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 127-128. ISBN 978-80-210-8073-7.
Výkladové stanovisko NSZ č. 1/2015 Sb., *ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů včetně obsahu e-mailových schránek*

[81] Viz. § 158d odst. 3 zákona č. 141/1961 Sb., *Trestní řád* v posledním znění

povolení podle § 158d odst. 1 a 3 TŘ prováděl neustálé „sledování“ této schránky.[82]

- **Zajištění obsahu ukončené, probíhající a budoucí komunikace bez zařízení**

Pokud je nutné pro trestní řízení zjistit obsah komunikace v e-mailové schránce, bez zajištění nosiče, popř. zařízení, ve kterém je uložena, musí policejní orgán postupovat tak, jako v předchozím případě v souladu ustanovením § 158d odst. 1 a 3 TŘ, přičemž musí být uvedeny údaje o konkrétních zařízeních, na kterých má být „sledování“ provedeno. Pokud je třeba zjistit obsah právě probíhající nebo budoucí e-mailové komunikace, je k takovému zásahu do soukromí nutné postupovat podle ustanovení § 88 TŘ, které hovoří o odposlechu a záznamu telekomunikačního provozu, na základě příkazu předsedy senátu, nebo v přípravném řízení na příkaz soudce, který jej vydá na základě návrhu státního zástupce.[83] Zde si autor dovolí uvést, o jak nejasnou problematiku se jedná. Výkladové stanovisko Nejvyššího státního zastupitelství č. 1/2015 se k věci vyjádřilo výše uvedeným postupem, nicméně Odbor bezpečnostní politiky Ministerstva vnitra ČR dne 21. 8. 2019 vydalo stanovisko k aplikaci ustanovení § 7b TŘ, které se týká povinnosti uchovávat data, kde se autor stanoviska mimo jiné vyjadřuje následovně: *„O jinou situaci se však bude jednat v případě, kdy má být předmětem sledování teprve budoucí e-mailová komunikace (přestože bude využit stejný procesní institut § 158d odst. 3 tr. řádu) a příkaz podle § 7b tr. řádu by měl vést k jakémusi „překlenutí“ doby mezi žádostí a vydáním povolení soudce…“*[84] Z pohledu autora této práce nelze soudit, zda se ve stanovisku OBP jedná o administrativní chybu autora stanoviska, popř. zda si autor stanoviska skutečně stojí za tvrzením, že budoucí e-mailovou komunikaci lze zajišťovat podle § 158d odst. 3 TŘ. Autor práce tento rozpor mezi stanovisky Nejvyššího státního zastupitelství a Odboru bezpečnostní politiky Ministerstva

---

[82] Výkladové stanovisko NSZ č. 1/2015 Sb., *ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů včetně obsahu e-mailových schránek*

[83] Tamtéž

[84] Stanovisko OBP Ministerstva vnitra ČR, *k aplikaci ustanovení § 7b trestního řádu* ve znění k 21.8.2019

vnitra ČR v práci uvádí, aby poukázal na to, jak je současná právní úprava nedostatečná, nejasná a matoucí.

- **Doplňující informace o e-mailové schránce a uživateli**

V některých případech je před zjištěním nebo mimo zjištění samotného obsahu schránky důležité získat doplňující informace o schránce a jeho uživateli. Může také nastat situace, kdy je ohledáním jedné e-mailové schránky zjištěno, že z jiné schránky byla do ohledávané schránky zasílána závadová komunikace, jakou může být např. dětská pornografie. Policejní orgán se poté zabývá ztotožněním uživatele, který takový obsah rozesílá. Při tom se může obrátit na poskytovatele informačních služeb, kteří jsou povinni vyhovět žádosti OČTŘ podle § 8 odst. 1 TŘ o poskytnutí součinnosti ve smyslu vydání údajů vedených k takové schránce, čímž může policejní orgán získat důležité informace týkající např. data registrace schránky, informace o dalších provázaných e-mailových schránek, či tel. čísla uživatele, ale také podrobnosti o přístupu do schránky, IP adresách, ze kterých se do schránky uživatel přihlašuje, informace o poskytovateli internetového připojení, popř. osobní údaje, které o sobě uživatel uvedl v době registrace schránky, atd.[85]

3.2 Provádění a hodnocení důkazu z e-mailu

Hlavním úkolem při dokazování e-mailem je ustanovit skutečného autora či odesílatele zprávy, neboť to, že zpráva odešla ze schránky osoby, opravdu nemusí znamenat, že ji dotyčná osoba psala nebo poslala. Příkladem může být situace, kdy rodina vlastní jeden počítač, který využívají všichni členové domácnosti. Pokud jeden ze členů rodiny nechá přihlášeného svého e-mailového klienta v prohlížeči, nebo umožní prohlížeči uložení hesla, které při dalším přihlášení není nutné vyplňovat znovu, nic nebrání jinému členovi rodiny, se takto jedním klikem myši, přihlásit do e-mailové schránky dotyčného. V ideálním případě podezřelá osoba nezpochybňuje, že je jediným uživatelem schránky, ani nemá snahu napadat pravost e-mailu. Mohou ale také nastat opačné situace, kdy podezřelý uvádí, že předmětný e-mail nepsal, i přesto, že odešel z jeho schránky,

[85] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 107. ISBN 978-80-210-8073-7.

nebo z jeho zařízení a odvolává se na to, že do zařízení, nebo schránky měla přístup další osoba, jak bylo popsáno výše, popř. že mu byl zcizen nebo napaden účet a takto byl e-mail zaslán bez jeho vědomí. Důkazem toho, že e-mail skutečně zaslala dotyčná osoba, může být svědecká výpověď osoby, která dotyčného při odesílání viděla, nebo které se dotyčná osoba o odeslání svěřila. Dalším způsobem ztotožnění autora s majitelem schránky může být znalecký posudek, který je zaměřen na obsah textu, jeho formu, úpravu textu a způsob vyjadřování v písemném projevu. Obsah komunikace ale není jediná věc, která OČTŘ v trestním řízení zajímá. Jak již bylo řečeno, mnoho údajů se dá vyčíst také z hlavičky e-mailu. Jestliže je známa IP adresa při odeslání mailu a IP adresy, ze kterých se dotyčná osoba v minulosti přihlašovala, je možné IP adresy takto srovnat a v případě shody lze hovořit o dalším z nepřímých důkazů, který může vést ke ztotožnění pachatele. Pokud se dotyčný hájí tím, že do schránky a k zařízení mají přístup i další osoby, popř. že znají přístupová hesla, se kterými se do schránky mohou přihlásit z jiných zařízení, je důležité v rámci řízení tuto skutečnost vyvrátit, popř. potvrdit, neboť krádeže účtů, napadení a ovládnutí zařízení bez vědomí uživatele, mohou mít vážné důsledky i v jiných oblastech života této osoby. Známé jsou též případy, kdy jednu schránku používá více osob, což může ztěžovat dopadení skutečného pachatele, nicméně se předpokládá, že přístup do soukromé e-mailové schránky, ve které se nachází soukromá komunikace, je výsostní právo majitele této schránky, který schránku vytvořil a může s ní nakládat.[86]

3.3 Shrnutí poznatků

Častým problémem při ustanovení majitele schránky pomocí provozních údajů je, že zkušenější pachatelé využívají nástroje sloužící k šifrování IP adres, které skutečnou adresu pomocí VPN a proxy serverů přesměrují tak, že to vypadá, že uživatel do schránky přistupuje z jiné geografické lokality. Takové IP adresy bývají často přesměrovány do úplně jiné země a maskují skutečné informace o poloze uživatele. K tomu slouží mnoho bezplatných i placených programů společností

[86] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 132-137. ISBN 978-80-210-8073-7.

(ExpressVPN, bind2.com, anonymoX, atd.), jejichž výše anonymity a vůle spolupráce s OČTŘ se může lišit.[87] V takových případech bývá dopadení dosud neznámého pachatele problematické, pokud se nejedná o komunikaci mezi osobami, které se osobně znají, a známá osoba je ochotna pomoci s ustanovením neznámého pachatele, nebo pokud uživatel při registraci neuvedl další osobní informace.

[87] *Hackeři radí, jak ukrýt svoji identitu v online prostředí*. Citadelo.com [online]. 29.3.2018 [cit. 26.10.2022]. Dostupné z: https://citadelo.com/cz/blog/hackeri-radi-jak-ukryt-svoji-identitu-v-online-prostredi/

4 Dokazování provozními a lokalizačními údaji

Pojmu provozních a lokalizačních údajů (Data retention) se věnuje mimo TŘ především Zákon č. 127/2005 Sb., o elektronických komunikacích (ZEK), který podle ustanovení § 97 odst. 3 ukládá povinnost právnickým a fyzickým osobám, které zajišťují veřejnou komunikační síť, nebo poskytují veřejně dostupnou službu elektronických komunikací, uchovávat tyto údaje po dobu 6 měsíců. Poskytovatelé také mají povinnost takové údaje při splnění zákonných podmínek poskytnout OČTŘ pro účely trestního řízení a pokud je OČTŘ nevyžadovaly, jsou poskytovatelé po uplynutí této doby povinni údaje smazat.[88] Pod těmito právnickými a fyzickými osobami si lze představit např. telefonní operátory a poskytovatele internetového připojení. Provozními údaji jsou podle ustanovení § 90 ZEK *„jakékoli údaje zpracovávané pro potřeby přenosu zprávy sítí elektronických komunikací nebo pro její účtování.“*[89] Lokalizačními údaji jsou podle ustanovení § 91 ZEK *„jakékoli údaje zpracovávané v síti elektronických komunikací nebo službou elektronických komunikací, které určují zeměpisnou polohu telekomunikačního koncového zařízení uživatele veřejně dostupné služby elektronických komunikací.“*[90] Rozsah údajů, které mají poskytovatelé uchovávat, stanoví Vyhláška č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů. Těmito údaji mohou být např. telefonní čísla a identifikátory tel. SIM karty osoby volající a volané, datum, čas a délka hovoru, datum a čas odeslání SMS/MMS, použitá tel. služba a pokud jsou provozovateli známy, též jméno a příjmení osoby. U poskytovatelů internetových služeb také typ připojení, IP adresa, datum a čas připojení a další.[91] Tímto postupem tedy nelze zjistit obsah komunikace, ale pouze výše uvedené doplňující informace. Termínem „Data retention“ se také zabývala Směrnice Evropského parlamentu a rady č. 2006/24/ES, o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES, která ukládala povinnost výše uvedeným poskytovatelům služeb zemí Evropské Unie tyto údaje

[88] Viz. § 97 odst. 3 zákona č. 127/2005 Sb., *o elektronických komunikacích* v posledním znění
[89] Viz. § 90 odst. 1 zákona č. 127/2005 Sb., *o elektronických komunikacích* v posledním znění
[90] Viz. § 91 odst. 1 zákona č. 127/2005 Sb., *o elektronických komunikacích* v posledním znění
[91] Viz. § 2 vyhlášky č. 357/2012 Sb., *o uchovávání, předávání a likvidaci provozních a lokalizačních údajů* v posledním znění

uchovávat. Dne 8. 4. 2019 byla tato Směrnice zrušena Soudním dvorem Evropské Unie pro rozpory s čl. 7 a 8 Listiny základních práv EU. Od té doby již nejsou členské státy EU povinny vyžadovat po poskytovatelích služeb uchovávání těchto údajů. Česká republika v tomto směru dosud nepodnikla žádné změny a poskytovatelé těchto služeb mají stále povinnost tyto údaje uchovávat a poskytovat je OČTŘ pro potřeby trestního řízení. V minulosti byla problematika uchovávání těchto údajů posuzována Ústavním soudem. V roce 2019 skupina 58 poslanců požadovala zrušení této povinnosti z důvodu nepřiměřeného zásahu do zaručeného soukromí Ústavou, neboť jsou uchovávány údaje celé populace využívající tyto služby. Dne 14. 5. 2019 Ústavní soud ve věci rozhodl tak, že zákonný postup uchovávání a vydání těchto údajů podle TŘ a ZEK je v souladu s Ústavou.[92]

4.1 Zajištění dat

Zákonnému postupu při zajišťování provozních a lokalizačních údajů se věnuje TŘ. OČTŘ se v tomto směru nemohou spoléhat na obecnou žádost ve smyslu § 8 odst. 1 TŘ, neboť se jedná o údaje, kterým přísluší značná právní ochrana. TŘ je uvádí jako údaje, na něž se vztahuje telekomunikační tajemství nebo ochrana osobních a zprostředkovaných dat. Vydání těchto údajů OČTŘ od poskytovatelů služeb je možné pouze na základě dodržení postupu uvedeného v § 88a TŘ.[93] Příkaz k vydání těchto údajů nařizuje předseda senátu a v přípravném řízení soudce na návrh státního zástupce. Státnímu zástupci policejní orgán nejprve postoupí žádost k vydání takového návrhu. Příkaz k vydání údajů, na něž se vztahuje telekomunikační tajemství, nebo ochrana osobních a zprostředkovaných dat, je možné vydat pouze, pokud je ve věci vedeno trestní řízení (tento institut nelze použít před zahájením trestního řízení jako podpůrné operativně pátrací prostředky) pro úmyslný trestný čin, na který zákon stanoví trest odnětí svobody, jehož horní hranice je nejméně tři roky, nebo pro taxativně vyjmenované trestné činy v tomto ustanovení, nebo pro úmyslný trestný čin, který je stíhatelný podle

[92] PŘÍKAZSKÁ, Lenka a Michal MOHELSKÝ. Současná právní úprava data retention je dle Ústavního soudu ústavně konformní a tedy přípustná. *epravo.cz* [online]. 16.10.2019 [cit. 28.10.2022]. Dostupné z: https://www.epravo.cz/top/clanky/soucasna-pravni-uprava-data-retention-je-dle-ustavniho-soudu-ustavne-konformni-a-tedy-pripustna-110069.html

[93] Viz. § 88a zákona č. 141/1961 Sb., *Trestní řád* v posledním znění

mezinárodní smlouvy, která k tomu zavazuje Českou republiku. Aby mohl být takový příkaz vydán, musí být řádně odůvodněn, což platí i pro návrh státního zástupce potažmo žádost policejního orgánu. Za odůvodnění jsou považovány známé údaje o uživateli (jméno, tel. čísla, která užívá, IMEI telefonu, atd.), popř. zařízení, dále uvedení skutkových okolností trestného činu, pro které je řízení konáno i další okolnosti, které směřují k vydání příkazu, a které podtrhují důležitost tohoto vydání, včetně prokázání toho, že účelu, který sleduje vydání těchto údajů, nelze dosáhnout jiným způsobem, nebo by jeho dosažení bylo podstatně ztížené.[94] Tímto způsobem lze získat informace o uživateli, aniž by měl tušení o zájmu o jeho osobu ze strany policejního orgánu. Možnost vydání těchto údajů je také možné se souhlasem osoby, ke které se tyto údaje vztahují.[95] V praxi se může jednat o oznamovatele, poškozeného, ale také o prověřovaného, který chce souhlasem prokázat, že např. s poškozeným nebyl v kontaktu, nebo se nenacházel na místě činu. Policejní orgán je oprávněn žádat tyto údaje až 6 měsíců zpětně, a jejich vydání provádí Útvar zvláštních činností služby kriminální policie a vyšetřování (ÚZČ SKPV). Více k činnosti ÚZČ SKPV je uvedeno v **kapitole 5.2 Provádění a hodnocení důkazu odposlechem**.

4.2 Provádění a hodnocení důkazu provozními a lokalizačními údaji

Zajištěné provozní a lokalizační údaje jsou vydány státnímu zástupci nebo policejnímu orgánu v textové podobě. Obvykle se jedná o velké množství údajů, které je potřeba analyzovat, vyhodnotit a užít pouze taková data, která mají souvislost s předmětným činem. Prováděním dokazování tímto způsobem lze ztotožnit zařízení, které je původcem hovoru nebo zpráv, či jeho příjemcem. Individuální identifikace osoby je obtížná, ale ne nemožná. Ustanovit konkrétní osobu pomocí těchto údajů lze na základě více skutečností, které musí tvořit ucelený na sebe navazující řetězec. Osoba se např. může bránit tím, že hovor prováděl nebo zprávu posílal z jeho přístroje někdo jiný. Často se tedy jedná o nepřímé důkazy, které mají podporující a doplňující charakter a je potřeba prověřit

[94] Viz. § 88a odst. 1 zákona č. 141/1961 Sb., *Trestní řád* v posledním znění
[95] Viz. § 88a odst. 4 zákona č. 141/1961 Sb., *Trestní řád* v posledním znění

a objasnit i další skutečnosti, které by mohly vést k usvědčení pachatele, neboť, to že byl uskutečněn hovor z jeho telefonu, nemusí být dostatečným důkazem. Je důležité zjistit motiv k páchání této osoby a jiné doprovodné znaky jeho chování. Z hlediska hodnocení důkazu je opět nutné zdůraznit zákonnost a pravost důkazu, neboť nezákonně získané údaje nemohou být použity jako důkaz. Jiný postup než v souladu s ustanovením § 88a TŘ je neakceptovatelný a může vést ke zpochybňování dalších důkazů ze strany obviněného a jeho obhájce.

4.3 Shrnutí poznatků

Provozní a lokalizační údaje jsou v současné době hojně využívány v rámci dokazování v trestním řízení nejen v odvětví kyberkriminality, ale také při dokazování v souvislosti s obecnou kriminalitou. Autor práce se neztotožňuje s názorem laické i odborné veřejnosti, která tlačí zákonodárce ke změně týkající se uchovávání provozních a lokalizačních dat, jak je tomu v jiných zemích EU (Německo, Slovensko)[96] a domnívá se, že v době, kdy se kriminalita z velké části přenáší do virtuálního prostoru, by měla být zákonná možnost ke sledování tohoto prostoru, k čemuž svým způsobem mohou sloužit také provozní a lokalizační údaje, a sice za splnění přísných zákonných podmínek, které v současné době nejsou žádnou formalitou. Je nutné brát v potaz, kolik institucí tento proces musí schválit, než soud konečně nařídí vydání těchto údajů. Autor se neztotožňuje s názorem, že by uchováváním provozních a lokalizačních údajů bylo zasahováno nepřiměřeně do soukromí uživatelů, neboť možnost vydání těchto údajů je pro účely trestního řízení možné pouze v souvislosti s některými úmyslnými trestnými činy a nedotýká se tak automaticky každého trestného činu, pokud se nejedná o případ, kdy k vydání těchto údajů dá dotčený uživatel souhlas, což samo o sobě vyvrací omezení jeho práv. Soukromí osob je jedno ze základních lidských práv, nicméně autor práce se domnívá, že při znemožnění vydávání těchto údajů by pachatelům trestné činnosti byla poskytnuta další výhoda spojená s užíváním moderních technologií, přičemž objasnění některého druhu trestných činů by bez

[96] PŘÍKAZSKÁ, Lenka a Michal MOHELSKÝ. Současná právní úprava data retention je dle Ústavního soudu ústavně konformní a tedy přípustná. *epravo.cz* [online]. 16.10.2019 [cit. 28.10.2022]. Dostupné z: https://www.epravo.cz/top/clanky/soucasna-pravni-uprava-data-retention-je-dle-ustavniho-soudu-ustavne-konformni-a-tedy-pripustna-110069.html

těchto údajů nebylo možné (internetové podvody, šíření dětské pornografie a jiné) a v mnoha případech se právě díky těmto údajům daří posunout prověřování či vyšetřování vpřed. Kritici namítají, že se tímto způsobem neuchovávají jen důležitá data pro trestní řízení, avšak autor má za to, že tak jako v jiných oblastech dokazování, ve kterých se nachází mnoho nesouvisejících informací a dat, je potřeba i v tomto případě údaje analyzovat a určit, která jsou důležitá pro trestní řízení. Tyto údaje poté mohou být důležitým důkazem v trestním řízení a zároveň mohou uchovávat informace o osobním životě a kontaktech dotyčné osoby, jejichž vyzrazení mimo mantinely trestního řízení je neospravedlnitelné. Příslušníci Policie ČR, kteří se s těmito údaji seznamují, a kteří je vyhodnocují, jsou podle zákona č. 273/2008 Sb., o Policii České republiky povinni zachovávat mlčenlivost o skutečnostech, které se dozví v souvislosti s jejich povoláním a dle osobního názoru autora, policisté při výkonu služby přichází do styku s často zajímavějšími a detailnějšími informacemi o osobách, než mohou tyto údaje poskytnout.[97] Příkladem může být provedení domovní prohlídky, kde policisté prohledávají každou část bytu (koš s odpadky, ložnici, skříně a šuplíky s osobními věcmi či spodním prádlem atd.), ve kterém se nachází mnoho choulostivých informací o životě dotyčné osoby, ale je nepředstavitelné, aby při takové prohlídce policisté nepřišli do styku s osobními věcmi a informacemi, které nijak nesouvisí s trestním řízením. I zde policisté musí vyhodnotit, co je věcí důležitou pro trestní řízení. Paradoxem je, že oba instituty mají podobný charakter, při vydání příkazů soudem. Další zajímavostí je, že pokud jsou vydány údaje o uskutečněném telekomunikačním provozu policejnímu orgánu a jedná se o případ, kdy poškozený má pachatelovo tel. číslo v zařízení zablokováno, a ten se mu snaží dovolat, tyto údaje se nezaznamenávají v telekomunikačním provozu i přesto, že poškozený může na svém telefonu zjistit, že se mu pokoušelo dovolat zablokované číslo. To může způsobit potíže např. konkrétně u trestného činu nebezpečného pronásledování (§ 354 TZ), kdy se z těchto pokusů o kontakt poškozeného stanovuje četnost tohoto jednání. Zároveň v případě, pokud je proti pachateli již vedeno trestní stíhání na svobodě, a ten i přes poučení o důvodech vazby takto dál zkouší kontaktovat poškozeného, nelze dokazování postavit na

[97] Viz. § 115 odst. 1 zákona č. 273/2008 Sb., *o Policii České republiky* v posledním znění

základě takových údajů od poskytovatelů telekomunikačního provozu, ale je nutné důkaz zajistit jiným způsobem, kterým může být např. předložení mobilního telefonu (§ 78 TŘ) za účelem vytvoření snímků obrazovky s historií blokovaných hovorů, ze kterých lze potvrdit, že pachatel i přes poučení dále páchá trestnou činnost a z toho důvodu jsou dány podmínky pro vazební trestní stíhání.

5 Dokazování odposlechem

Odposlechem se v rámci trestního řízení rozumí zjištění obsahu komunikace, na kterou se váže telekomunikační tajemství. Původním záměrem zákonodárců bylo stanovit podmínky, které by opravňovaly odposlouchávat hovory mezi účastníky, především pomocí telefonů, vysílaček a podobných zařízení. S postupným vývojem komunikačních prostředků, lze do této sféry zahrnout všechna zařízení, která jsou schopná komunikovat prostřednictvím telekomunikačních sítí a sítí elektronických komunikací.[98]

5.1 Zajištění dat

Zajistit odposlech a záznam telekomunikačního provozu je možné pouze v souladu s ustanovením § 88 TŘ na základě písemného příkazu předsedy senátu a v přípravném řízení na příkaz soudce, jemuž podává návrh k vydání příkazu státní zástupce. Policejní orgán obvykle ještě před vydáním návrhu státního zástupce zpracuje a doručí státnímu zástupci žádost o vydání takového návrhu. Předseda senátu nebo soudce může nařídit odposlech a záznam telekomunikačního provozu, pokud je zahájeno trestní řízení pro zločin, na který zákon stanoví trest odnětí svobody, jehož horní hranice je nejméně osm let, nebo pro taxativně vyjmenované trestné činy v tomto ustanovení, nebo pro úmyslný trestný čin, který je stíhatelný podle mezinárodní smlouvy, která k tomu zavazuje Českou republiku. Aby mohl být takový příkaz vydán, musí být řádně odůvodněn, což platí i pro návrh státního zástupce potažmo žádost policejního orgánu. V odůvodnění je potřeba uvést skutkové okolnosti činu, známé údaje o uživateli (jméno, tel. čísla, která užívá, IMEI telefonu, atd.) a dobu, po kterou má být odposlech prováděn. Tato doba nesmí být delší než 4 měsíce, ale lze ji na základě vyhodnocení opakovaně prodloužit vždy maximálně o 4 měsíce. Prodloužení schvaluje soudce vyššího soudu a v přípravném řízení na návrh státního zástupce soudce Krajského soudu. Podstatnou okolností pro vydání příkazu je předpoklad, že odposlechem budou získány důležité skutečnosti pro trestní řízení a sledovaného účelu nelze dosáhnout jiným způsobem, nebo by jeho dosažení bylo

[98] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 181. ISBN 978-80-210-8073-7.

podstatně ztížené. Bez tohoto příkazu může být odposlech a záznam proveden pouze v řízení o zákonem stanovených trestných činech (Obchodování s lidmi § 168 TZ, Vydírání § 175 TZ, Nebezpečné vyhrožování § 353 TZ, atd.), pokud s tím dotyčná osoba souhlasí.[99]

5.2 Provádění a hodnocení důkazu odposlechem

Odposlech a záznam telekomunikačního provozu provádí výhradně Policie České republiky pro všechny OČTŘ. Konkrétně se o provádění odposlechu a záznamů telekomunikačního provozu stará ÚZČ SKPV. Jedná se o celorepublikový útvar, který má v rámci krajů zřízené své expozitury. ÚZČ SKPV mimo odposlechů provádí také např. sledování osob a věcí. Konkrétní činnost a postup, jakým toto ÚZČ SKPV provádí je však utajován veřejnosti.[100] To, jakým způsobem ÚZČ SKPV postupuje společně s poskytovateli telekomunikačních služeb, se po technické stránce zabývá Vyhláška č. 336/2005 Sb., o formě a rozsahu informací poskytovaných z databáze účastníků veřejně dostupné telefonní služby a o technických a provozních podmínkách a bodech pro připojení koncového telekomunikačního zařízení pro odposlech a záznam zpráv. Jedná se o vyhlášku vztahující se k ZEK. V té je uvedeno, že zahájení odposlechu je možné provést následujícími způsoby.

„a) aktivací odposlechu u zájmové uživatelské adresy, čímž se síť nebo služba uvede do stavu, ve kterém se informace o každé aktivitě zájmové uživatelské adresy přenáší na výstup, nebo

b) instalací zařízení oprávněného orgánu v připojovacím bodě a jeho aktivací.“[101]

To, zda důvody pro odposlech a záznam telekomunikačního provozu trvají, je policejní orgán povinen průběžně vyhodnocovat a zjistí-li, že již netrvají důvody k této činnosti, je povinen odposlech a záznam telekomunikačního provozu ihned ukončit a informovat o tom osoby, které odposlech nařídili. Pokud mají být

---

[99] Viz. § 88 zákona č. 141/1961 Sb., *Trestní řád* v posledním znění

[100] *Útvar zvláštních činností služby kriminální policie a vyšetřování*. Policie České republiky [online]. © 2022 [cit. 28.10.2022]. Dostupné z: https://www.policie.cz/clanek/utvar-zvlastnich-cinnosti-sluzby-kriminalni-policie-a-vysetrovani-716842.aspx

[101] Vyhláška č. 336/2005 Sb., *o formě a rozsahu informací poskytovaných z databáze účastníků veřejně dostupné telefonní služby a o technických a provozních podmínkách a bodech pro připojení koncového telekomunikačního zařízení pro odposlech a záznam zpráv* v posledním znění

výsledky odposlechu a záznamu telekomunikačního provozu použity u soudu jako důkaz, je policejní orgán povinen k tomuto vytvořit protokol, který musí splňovat funkcionality uvedené v ustanovení § 55 TŘ (místo, čas, způsob provedení, obsah, označení pořizujícího orgánu). Pokud je vyhodnocováním zjištěno, že obviněný komunikuje se svým obhájcem, je policejní orgán povinen takový odposlech a záznam ukončit, přičemž nesmí zjištěné informace použít a záznam s takovým odposlechem musí zákonným způsobem zničit. O zničení je povinen také sepsat protokol.[102] Důkaz odposlechem a záznamem telekomunikačního provozu může být před soudem proveden přečtením protokolu, ve kterém je popsané doslovné znění hovoru, popř. přehráním originální formy záznamu. Tak jako u ostatních důkazů, je třeba hodnotit pravost a zákonnost takto získaných důkazů. Odposlech a záznam je realizován tak, že je zaznamenáván hlasový, či písemný projev odposlouchávané osoby, tedy konkrétně jeho zařízení. I při tomto dokazování nastává problém se ztotožněním konkrétní osoby, přestože jsou známy údaje o tom, kdo zařízení či účastnické telefonní číslo užívá, může se tato osoba bránit tím, že se na záznamu nejedná o ní, a že nikdy takový hovor neprovedla. Ke ztotožnění konkrétní osoby může být použita technologie umožňující srovnání hlasového projevu např. za pomocí programu Phonexia. Programy pro srovnání hlasového projevu využívají znalci při zpracování znaleckých posudků, které mohou být před soudem použity jako důkaz. Srovnání hlasů se provádí na základě vybraných preferencí (jazyk, emoce, rozpoznání pohlaví a věku, rychlost řeči, atd.) Podstatným kritériem pro ztotožnění konkrétní osoby je kvalita zkoumané nahrávky.[103] Dalšími způsoby, které mohou sloužit k ustanovení konkrétní osoby, jsou svědecké výpovědi osob, které v době komunikace viděly osobu manipulovat se zařízením, popř. slyšely její hovor, či viděly zprávy dotyčné komunikace. K ustanovení konkrétního uživatele může vést také výpověď druhé osoby zúčastněné v takové komunikaci, případně lze využít

[102] Viz. § 88 zákona č. 141/1961 Sb., *Trestní řád* v posledním znění
[103] MICHÁLEK, Luděk a kol. *Kriminální zpravodajství jako nástroj kontroly trestné činnosti a zajišťování vnitřní bezpečnosti*. 1. vyd. Praha: Policejní akademie České republiky v Praze, 2020, s. 106. ISBN 978-80-7251-506-6.

provozní a lokalizační údaje o telekomunikačním provozu, použité IP adresy, IMEI komunikujících zařízení, či jiné identifikátory, elektronické podpisy atd.[104]

5.3 Prostorový odposlech

Vedle klasického odposlechu čili získávání informací z telekomunikačního provozu, stojí tzv. prostorový odposlech, který není zmiňován v § 88 TŘ. Pojem prostorový odposlech trestní řád vůbec nevysvětluje a lze si pod ním představit postup, při kterém se skrytě za pomocí technických prostředků pořizují záznamy o osobách. Takové technické prostředky mohou být nainstalovány prakticky kdekoliv, kde je dán předpoklad nezákonného jednání, pro které je prostorový odposlech povolován (v autě, kanceláři, garáži, fotbalové šatně, atd.). Jelikož TŘ nehovoří o prostorovém odposlechu, je tento postup realizován podle ustanovení § 158d TŘ, které se dotýká sledování osob a věcí. Postup v pořizování prostorových odposlechů lze analogicky přiřadit pod 2. a 3. odstavec tohoto ustanovení.[105] Postup podle § 158d TŘ je přiblížen v **kapitole 2.3 Nakládání s elektronickými důkazy**. Povolení lze získat na základě písemné a odůvodněné žádosti na dobu maximálně 6 měsíců. Tuto dobu je možné na základě vyhodnocení a nové žádosti prodloužit o dalších 6 měsíců. Zásadním rozdílem mezi klasickým a prostorovým odposlechem je, že v případě odposlechu podle § 88 TŘ se získávají pouze informace o uživateli zařízení a jeho komunikaci s jiným uživatelem. Dalším podstatným rozdílem je to, že ustanovení § 88 TŘ stanoví okruh trestných činů, pro které je možné takový odposlech nařídit, přičemž i taxativně vyjmenovává určité trestné činy. Naproti tomu ustanovení § 158d TŘ o sledování nic takového neuvádí. Běžným odposlechem a záznamem telekomunikačního provozu i prostorovým odposlechem je zasahováno do soukromí nejen dotčené osoby. Prostorový odposlech sleduje prostor, ve kterém probíhá komunikace dotyčné osoby s ostatními, kteří nemusí mít s trestnou činností, pro kterou byl odposlech nařízen, nic společného. Zajímavé je, že pokud je při odposlechu podle § 88 TŘ zjištěn jiný trestný čin, lze záznam z tohoto

---

[104] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 193-194. ISBN 978-80-210-8073-7.

[105] Viz. § 158d odst. 2 a odst. 3 zákona č. 141/1961 Sb., *Trestní řád* v posledním znění

odposlechu použít jako důkaz, pokud je v této věci vedeno trestní stíhání a jedná-li se o okruh trestných činů, pro které je možné odposlech nařídit, nebo pokud s tím dotyčný uživatel souhlasí. V případě prostorových odposlechů podle § 158d TŘ je věc jiná v tom, že informace získané podle odstavce 2, je možné použít jako důkaz také v případech, kdy je v jiné věci vedeno trestní řízení o úmyslném trestném činu, ale TŘ už nehovoří o možnosti takového užití v případech odstavce 3, kdy má být odposlech prováděn v soukromí.[106] To by mohlo být nešťastné, pokud by například byl teoreticky prováděn prostorový odposlech v bytě podezřelého pro trestný čin podplácení podle § 332 TZ a byly by tímto odposlechem zjištěny důkazy o jiném úmyslném trestném činu, pro který je vedeno trestní řízení (např. že se podezřelý s jinou osobou baví o skutkových okolnostech spáchané vraždy, pro kterou je vedeno trestní řízení). V takovém případě by teoreticky nebylo možné použít tyto důkazy v trestní věci vraždy, což se jeví nelogické vzhledem ke způsobu povolení takového sledování a závažnosti činu.[107] V otázce prostorových odposlechů ve smyslu § 158d odst. 3 TŘ a jejich využitelnosti pro jinou trestnou činnost, než byly povoleny, vznikají právní spory, kdy se část odborné veřejnosti domnívá, že z hlediska analogie lze informace zjištěné v soukromí prostorovým odposlechem podle § 158d odst. 3 TŘ použít jako důkaz i v jiné trestní věci ve smyslu § 158d odst. 10 TŘ a druhá strana toto tvrzení odmítá s názorem, že pokud by zákonodárce uvažoval o možnosti použití těchto důkazů v jiné věci, jistě by takovou možnost uvedl v trestním řádu, neboť sledování podle § 158d odst. 2 TŘ není tak invazivní a neprolamuje právo na soukromí v takové intenzitě jako § 158d odst. 3 TŘ. Dne 16. 12. 2020 v této věci udělal jasno Nejvyšší soud, jehož Trestní kolegium přijalo do Sbírky rozhodnutí Nejvyššího Soudu usnesení ze dne 25. 8. 2020, sp. zn. 8 Tdo 647/2020 a usnesení ze dne 1. 9. 2020, sp. zn. 7 Tdo 865/2020, která se zabývala právě možností využití prostorových odposlechů v jiné trestní věci, a která se shodla na jasném závěru.[108] *„Záznamy o sledování osob a věcí uvedené v § 158d odst. 2 tr. ř. a připojené protokoly tedy lze použít jako důkazní prostředky i v jiné trestní věci,*

[106] Viz. § 158d zákona č. 141/1961 Sb., *Trestní řád* v posledním znění
[107] Tamtéž
[108] *Trestní kolegium Nejvyššího soudu ukončilo „spor o odposlechy" z jiné věci*. Advokatnidenik.cz [online]. 17.12.2022 [cit. 6.11.2022]. Dostupné z: https://advokatnidenik.cz/2020/12/17/trestni-kolegium-nejvyssiho-soudu-ukoncilo-spor-o-odposlechy-z-jine-veci/

než je ta, v níž bylo povoleno sledování, je-li i v této věci vedeno řízení o úmyslném trestném činu nebo souhlasí-li s tím osoba, do jejíž práv a svobod bylo sledováním zasahováno (§ 158d odst. 10 tr. ř.). To platí jak v případech, kdy bylo sledování povoleno státním zástupcem (§ 158d odst. 2 tr. ř.), tak i tehdy, kdy bylo sledování povoleno soudcem (§ 158d odst. 3 tr. ř.).“[109] S tímto tvrzením se ztotožňuje také autor této práce, který se zároveň domnívá, že prostorové odposlechy mohou být významným zdrojem informací v trestním řízení a jako takové by si zasloužily své vlastní zákonné znění, které by jasně definovalo možnosti použití takových odposlechů, místo toho, aby tento institut musel být užíván na základě výkladu jiných ustanovení a rozhodnutí soudu. Autor má dále za to, že právní spory týkajících se takto nejasně popsaných ustanovení, kterými je zásadním způsobem zasahováno do základních lidských práv, poskytují příležitosti a prostor obhajobě k napadání zákonného postupu všech OČTŘ při zajišťování důkazů s odkazem právě na takové nesrovnalosti v zákoně, což nemá dosah pouze na soudce a státní zástupce, kteří jsou přítomni hlavnímu líčení, ale také na policisty, kteří jsou obvykle prvním článkem při zajišťování takových důkazů. Tématu začlenění prostorových odposlechů do trestního řádu se také věnoval prof. JUDr. Jiří Jelínek, CSc. již v roce 2018 v jeho odborném příspěvku na portálu Bulletin-advokacie.cz, kde se snažil poukázat na důležitost zpracování prostorových odposlechů do trestního řádu pod samostatným ustanovením, přičemž současnou úpravu prostorových odposlechů označil za závažný nedostatek trestního řádu, s čímž se ztotožňuje i autor této práce.[110]

5.4 Shrnutí poznatků

I při splnění všech zákonných podmínek, které jsou uvedené v přechozích podkapitolách, je na místě zmínit současný trend a problém v problematice odposlechů z pohledu OČTŘ, kterým je využívání komunikačních aplikací a softwarů, které svým klientům nabízí koncové šifrování (tzv. end-to-end). Toto šifrování je využíváno především v chatovacích aplikacích, přes které

[109] Usnesení Nejvyššího soudu ČR ze dne 25. 8. 2020, sp. zn. 8 Tdo 647/2020
Usnesení Nejvyššího soudu ČR ze dne 1. 9. 2020, sp. zn. 7 Tdo 865/2020
[110] JELÍNEK, Jiří. K chybějící právní úpravě tzv. prostorového odposlechu v trestním řádu. *Bulletin-advokacie.cz* [online]. 22.9.2018 [cit. 25.1.2023]. Dostupné z: http://www.bulletin-advokacie.cz/k-chybejici-pravni-uprave-tzv.-prostoroveho-odposlechu-v-trestnim-radu

uživatelé mohou komunikovat pomocí textových, obrazových, či zvukových zpráv. Tyto aplikace také umožňují hovor jednoho účastníka s druhým, nebo celé skupiny uživatelů mezi sebou. Šifrován není jen obsah zprávy, ale také přílohy a informace o zprávě. V některých aplikacích je toto šifrování automaticky užíváno, v jiných si ho může uživatel aplikace zapínat a vypínat dle libosti. Toto šifrování prakticky funguje tak, že odesílaná zpráva je zašifrována pomocí různě silného šifrovacího klíče (algoritmem), poté pokračuje sítí až ke koncovému uživateli, jehož aplikace dešifrovacím kódem umožní zobrazení originální formy této zprávy. Toto zabezpečení způsobí to, že obsah není čitelný ani pro poskytovatele této služby a skutečný obsah v původní formě je možné přečíst pouze na přístroji odesílatele a příjemce.[111] Některé aplikace dále nabízí možnost tzv. automatického smazání komunikace, které způsobí, že odeslaná či přijatá zpráva, po nastavené době od přečtení nadobro zmizí a není možné ji nikde vyhledat. Totožné platí i u uskutečněných hovorů v aplikaci, kdy stejným způsobem zmizí všechny údaje o provedeném hovoru. Takové zprávy a informace o hovoru se neukládají ani do zařízení, skrze které uživatelé komunikují. Jediný způsob možnosti zachování takové zprávy je poté možnost vytvoření snímku obrazovky zařízení, který se uloží do paměti zařízení.[112] Tyto aplikace tedy neztěžují pouze provádění odposlechu, ale také možnosti získání komunikací a dat např. po zajištění mobilního telefonu podle § 78 TŘ. Úspěšnost chatovacích aplikací je dána tím, kolik lidí skrze ně komunikuje. V současné době je patrné, že spousta uživatelů, kteří mají pocit, že jejich komunikace není dostatečně soukromá skrze běžné služby poskytované operátory a běžnými komunikačními nástroji (SMS, tel. hovor, Facebook, E-mail), přechází na tyto šifrované aplikace ve snaze skrýt obsah své komunikace. To lze tvrdit také o činnostech spojených s kriminalitou. Pachatelé jsou si dobře vědomi skutečnosti, že je bezpečnější komunikovat na těchto platformách než pomocí běžných telekomunikačních prostředků. To, jak se s touto problematikou vypořádají zákonodárci potažmo OČTŘ, bude v následujících letech dle autora

---

[111] JELIČ, Pavel. Co je to end-to-end šifrování. *Letem světem applem* [online]. 23.2.2020 [cit. 27.10.2022]. Dostupné z: https://www.letemsvetemapplem.eu/2020/02/23/co-je-to-end-to-end-sifrovani/

[112] PALYZA, Jiří. Chaty ve WhatsAppu se mažou automaticky: nová funkce by měla řešit velký problém. *chip.cz* [online]. 20.5.2021 [cit. 27.10.2022]. Dostupné z: https://www.chip.cz/novinky/chaty-ve-whatsappu-se-mazou-automaticky-nova-funkce-by-mela-resit-velky-problem/

práce klíčové v oblasti dokazování elektronickými důkazy, které jsou získávány z komunikace uživatelů.

6 Dokazování elektronickými dokumenty

Pojem dokument vysvětluje definice uvedená v ustanovení § 2 písm. e) zákona č. 499/2004 Sb., o archivnictví a spisové službě, která říká, že dokumentem se rozumí *„každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace, ať již v podobě analogové či digitální, která byla vytvořena původcem nebo byla původci doručena.“*[113] Z této definice vyplývá, že se může jednat o informace nejrůznějšího charakteru, které bývají uložené na různých nosičích. Z hlediska elektronických dokumentů lze hovořit o elektronických nosičích, kterými mohou být CD, DVD a Blu-ray disky, HD disky a vnitřní paměti zařízení, paměťové karty, externí disky, servery, cloudy atd. Je logické, že se technologický pokrok a digitalizace dotýká také písemností, které jsou již nějaký čas hojně využívány v elektronické podobě na různých úrovních právních vztahů, a lze předpokládat, že tento trend se bude v budoucnu projevovat v běžném životě každého z nás čím dál častěji. Přednostmi užití dokumentů v elektronické podobě může být především rychlost přenosu informací a pohodlí při vytváření dokumentu, neboť velkou část dokumentů lze vytvořit pouze za použití notebooku, mobilního telefonu, tabletu či jiného obdobného zařízení z pohodlí domova. V neposední řadě je nutné zmínit možnost uchovávání takových dokumentů, pro které není nutné disponovat prostory, kde by se hromadily stohy papírů, ale postačí pouze vhodný datový nosič, na kterém je dokument uložen. Naproti tomu je nutné také uvést některé aspekty, které v tomto ohledu brzdí technologický pokrok. Autor se domnívá, že se jedná o „problém“ různých generací, kde jsou na jedné straně mladší uživatelé, a proti nim starší generace uživatelů. Mladí jsou otevřenější k užívání nejnovějších technologií, které jim umožní ulehčit jakoukoliv práci. Starší generace v tomto ohledu zastává často konzervativnější přístup a mnohdy nedá dopustit na papírovou podobu dokumentace. Dále je nutné zmínit problematiku identifikace autora. V tomto směru mohou dokumenty v listinné podobě obsahovat některé znaky, které umožňují snadnější identifikaci osoby. Základními údaji mohou být uvedení jména, příjmení, podpisu, data a místa podepsání. Vyšší stupeň zabezpečení může představovat ověření takové listiny ověřenými podpisy nebo ověření listiny

[113] Viz. § 2 písm. e) zákona č. 499/2004 Sb., *o archivnictví a spisové službě* v posledním znění

notářem. Vlastnoručně psané listinné dokumenty lze také podrobit grafické expertize ručního písma, která umožňuje individuálně identifikovat pisatele. Také elektronické dokumenty nabízí několik druhů opatření směřující k prokázání totožnosti původce, ať už samotný fakt, že tyto dokumenty prochází e-mailovou či datovou schránkou konkrétní osoby. Použití těchto služeb předpokládá zabezpečení přístupu před jinými uživateli přístupovými údaji či jinými technickými prostředky (chipy, přístupové karty, atd.). Jako další způsob k prokázání totožnosti autora dokumentu může sloužit opatření dokumentu elektronickým podpisem, časovým razítkem nebo elektronickou pečetí. Listinné dokumenty lze také převádět do digitální formy několika způsoby v závislosti na tom, zda má být prokázána autenticita tohoto dokumentu, k čemuž se používá autorizovaná konverze. Pokud není nutné prokazovat tuto autenticitu, může být využit prostý sken dokumentu. Stejným způsobem lze převádět dokumenty také opačným směrem.

- **Obrazové a zvukové dokumenty**

Obrazovými dokumenty jsou informace znázorněné grafickými prvky, které lze rozdělit na statické dokumenty (fotografie, malby, obrázky atd.) a dynamické, což mohou být videozáznamy, popř. audiovizuální záznamy, které jsou obohaceny také o zvukovou stopu.[114] Obrazové dokumenty vznikají za použití mnoha nástrojů, kterými mohou být samotná zařízení jako fotoaparáty, mobilní telefony, tablety nebo za pomocí programů, které umožňují tvorbu obrazových dokumentů (Malování, Photoshop, Corel Draw, Adobe Illustrator, atd.). Statické obrazové dokumenty se nejčastěji vykytují ve formátu typu .jpeg, .BMP, .PNG, .PDF, atd. Dynamické obrazové dokumenty mohou mít formáty typu .GIF, .mp4, .mkv, .avi atd. K záznamu a vytvoření zvukových dokumentů bývají používány mikrofony a jiná nahrávací zařízení. Může se jednat o samostatné mikrofony nebo součást a jednu z funkcí víceúčelových zařízení, kterými jsou mobilní telefony, notebooky, tablety atd. Zvukové dokumenty mívají odlišný formát oproti výše uvedeným. Obvykle se jedná o soubory formátu .mp3, .WAV, .FLAC atd. Obrazové a zvukové

[114] *Obrazový dokument vizuální dokument, ikonický dokument*. Česká terminologická databáze knihovnictví a informační vědy [online]. © 2012 [cit. 20.11.2022]. Dostupné z: http://aleph.nkp.cz/publ/ktd/00000/09/000000912.htm

dokumenty mohou být v rámci přenosu informací samostatným prvkem, popř. mohou být přílohou písemného elektronického dokumentu, pro kterou bývají nejčastěji využívány statické obrazové dokumenty. Výše uvedené dokumenty mohou být uloženy na nejrůznějších nosičích.

- **Písemné dokumenty**

Z hlediska práva je jednou z podstatných skupin dokumentů skupina písemných dokumentů, která má prokazovat písemný projev vůle autora. Písemný dokument může mít podobu klasické listiny, kdy je tento projev zachycen v „papírové podobě“ nebo podobu elektronické písemnosti uložené na datovém nosiči v příslušném elektronickém formátu.[115] Elektronické písemnosti mohou být vytvářeny nejrůznějšími nástroji a softwary. Některé z těchto softwarů jsou přístupné uživatelům zdarma, nebo se může jednat o zpoplatněné programy, které nejsou součástí základního vybavení zařízení. Obvyklými formáty písemných elektronických dokumentů jsou formáty typu .doc, .docx, nebo .odt. Vytváření, prohlížení a editování dokumentů v těchto formátech umožňují programy jako Microsoft Word, OpenOffice, atd. Každý z těchto programů má své vlastní typické rozhraní. Dalším často používaným formátem je formát typu .txt, pro který je využíván program Microsoft NotePad. Dokumenty tohoto formátu jsou oproti výše uvedeným formátům strohé a nepříliš vhodné pro vytváření delších dokumentů. Jako další lze zmínit formáty .htm a .html sloužící pro tvorbu zdrojových kódů webových stránek. Pro následný přenos informací původního elektronického písemného dokumentu jinému uživateli je vhodné takový dokument převést ze základního formátu (.doc, .docx, .odt, .txt, atd.) do formátu .PDF, což umožňuje např. program Adobe Acrobat. Tento formát je schopný zachovat nastavení a formátování dokumentu nezávisle na tom, v jakém programu byl dokument vytvořen, což je rozdíl oproti textovým programům typu Microsoft Word a OpenOffice, kdy stejný dokument otevřený v jiném druhu programu může mít rozdílnou podobu. Převedené dokumenty ve formátu .PDF dále na rozdíl od

[115] PODANÝ, Jan. Podepisování soukromých listin včera, dnes a zítra. *Advokátní deník* [online]. 4.5.2020 [cit. 20.11.2022]. Dostupné z: https://advokatnidenik.cz/2020/05/04/podepisovani-soukromych-listin-vcera-dnes-a-zitra/

dokumentů formátu .doc, .docx, atd. nelze po převodu editovat či pozměňovat a lze je označit elektronickými daty pro identifikaci autora.[116]

6.1 Zajištění dat

Postup pro zajišťování elektronických dokumentů je závislý především na tom, na jakém nosiči je tento dokument uložen. V případě uložení dokumentu na běžném datovém nosiči jako CD, DVD, HDD, SD kartě či v paměti zařízení, lze využít instituty vydání či odnětí věci ve smyslu § 78 a 79 TŘ, popř. ustanovení týkající se provádění prohlídek (§ 82 – 85c TŘ). Dalším způsobem může být zajištění takového nosiče při ohledání místa činu, nebo při ohledání samotného nosiče (§ 113 TŘ). V případě, že došlo k přenosu takového dokumentu za pomocí e-mailové komunikace, může policejní orgán pro zajištění takového dokumentu postupovat tak, jak je uvedeno v **kapitole 3 Dokazování e-mailem**. Datové schránky byly v minulosti určeny především ke komunikaci právnických osob, případně fyzických osob s orgány veřejné moci, ale v současnosti je možné datové schránky užívat také ke komunikaci mezi fyzickými osobami, které si tuto službu zřídí. Přenos dat je šifrován a není možné zjistit obsah datových zpráv jinak, než v oprávněném přístupu do datové schránky pomocí přístupových údajů. Jedinými údaji o komunikaci, které informační systém datových zpráv dokáže zpřístupnit, jsou údaje na obálce datové schránky (údaje o odesílateli a příjemci). Datové zprávy mohou obsahovat také doručenku, která odesílateli potvrdí přijetí takové zprávy příjemcem. Datové zprávy jsou na stejné právní úrovni jako doručování listovních zásilek do vlastních rukou. Nicméně se jedná o placenou službu a v komunikaci mezi fyzickými osobami převládá komunikace pomocí e-mailových schránek, jejichž používání v základní formě je zdarma. Zároveň jsou datové schránky zřizovány konkrétním osobám a se schránkami jsou provázána také jejich osobní údaje.[117] Z toho důvodu se způsob páchání trestné činnosti za využití datových zpráv jeví jako nesmyslný, neboť datové schránky pachatelům nenabízí prakticky žádnou míru anonymity ve smyslu identifikace odesílatele

[116] *Adobe Acrobat*. Adobe.com [online]. © 2022 [cit. 20.11.2022]. Dostupné z: https://www.adobe.com/cz/acrobat/online/convert-pdf.html

[117] *Nejčastější dotazy*. Datové schránky [online]. © 2022 [cit. 8.12.2022]. Dostupné z: https://info.mojedatovaschranka.cz/info/cs/1028.html

zprávy (tím není dotčen obsah zpráv, který je pro provozovatele služby šifrovaný), oproti e-mailovým schránkám nebo chatovacím aplikacím. Některé z e-mailových a chatovacích služeb částečně stále nabízí možnost vytvoření profilu s falešnými údaji, neboť uvedené údaje v těchto službách obvykle nejsou při vytváření profilu blíže ověřovány.

6.2 Provádění a hodnocení důkazu elektronickými dokumenty

Provedení důkazů z elektronických dokumentů je možné jak v jeho původní podobě např. přehráním video nebo audio dokumentu, případně zobrazením obrazového dokumentu nebo přečtením písemného dokumentu v zařízení, které přehrání nebo zobrazení takového dokumentu umožňuje. Dalšími způsoby provedení důkazu elektronickými dokumenty může být ohledání nosiče, či dokumentu samotného (§ 113 TŘ), odborné vyjádření či znalecký posudek (§ 105 TŘ), zaměřený na konkrétní otázky týkající se takového dokumentu. V úvahu také připadá výslech svědka (§ 101 TŘ), který může být taktéž nositelem informací, týkajících se vzniku, změny nebo odstranění důležitého dokumentu pro trestní řízení.[118] Hodnocení důkazu se v případě elektronických dokumentů zabývá především správností a platností dokumentu a dále možností autentizace konkrétní osoby, jejíž jednání s dokumentem nějak souvisí, což objasňuje následující podkapitola.

6.2.1 Autentizace elektronických dokumentů

Digitální komunikace není aktuálním termínem pouze mezi fyzickými osobami a orgány veřejné správy, ale také ve sféře obchodní mezi právnickými osobami, bankovními a jinými institucemi s jejich klienty a také mezi fyzickými osobami navzájem. Komunikace a agenda v digitálním prostředí nabízí mnoho výhod pro všechny zúčastněné strany, avšak zároveň klade zvýšené nároky na zabezpečení technického řešení a také na autentizaci skutečně oprávněných osob k tomuto jednání. V souvislosti se zajištěním identifikace autora dokumentu a jeho vůle s úkonem podpisu takového dokumentu bylo v minulosti vydáno několik právních

[118] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 73-81. ISBN 978-80-210-8073-7.

norem, které se mimo jiné zaměřují na autentizaci a bezpečnost v problematice elektronických dokumentů. Pro příklad lze zmínit následující 2 předpisy:

Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, kterým byl zrušen zákon č. 227/2000 Sb., o elektronickém podpisu.

Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (eIDAS).

Ve zkratce by se o opatřeních sloužících k identifikaci autora dalo říci, že se jedná o specifická elektronická data, kterými jsou primární data (dokumenty) označena. Těmi mohou být elektronické podpisy, elektronické pečetě, certifikáty pro elektronické podpisy a pečetě a časová razítka.[119]

- **Datová konverze dokumentů**

V problematice písemných dokumentů a jejich následnému přenosu a právní použitelnosti je nutné zmínit formu, v jaké je konečný dokument přenášen, popř. archivován. V tomto ohledu lze zmínit několik způsobů, které slouží k převodu dokumentů. Dokumenty lze převádět z listinné podoby do elektronické, ale také opačným směrem z elektronické podoby do listinné. Nejobyčejnějším způsobem převodu písemného dokumentu může být prostý sken listinného dokumentu, respektive prostý tisk elektronického dokumentu. V takovém případě nejsou dokumenty opatřovány žádnými autorizačními znaky a jejich využitelnost pro případné řízení je sporné, pokud vyplynou námitky o jeho správnosti, neboť při převodu se blíže nezjišťuje, zda cílový dokument skutečně odpovídá původnímu. I při takovém převodu, nebo při vytvoření nového elektronického dokumentu, vznikají určitá elektronická data, která jsou použitelná pro trestní řízení. Zmínit lze např. vytvoření metadat a doplňujících informací o elektronickém dokumentu, ze kterých lze vyčíst mnoho podrobnosti o samotném dokumentu (velikost souboru, jeho název, datum a čas vzniku, případně změny a název zařízení, ve kterém byl

[119] Viz. § 5 až 12 zákona č. 297/2016 Sb., *o službách vytvářejících důvěru pro elektronické transakce* v posledním znění

dokument vytvořen). Při převodu elektronického dokumentu bez konverze do listinného dokumentu mohou zůstávat v použitých zařízeních (počítač, tiskárna) metadata týkající se tisku dokumentu. Dalším způsobem převodu dokumentu, který popisuje zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, je právě autorizovaná konverze dokumentu. Zákon říká, že takto převedený dokument, který je opatřen doložkou, má stejné právní účinky, jako původní dokument, neboť se jedná o totožný obsah dokumentu, který je ověřen na kontaktním místě veřejné správy.[120] Kontaktní místa veřejné správy provádí konverzi na základě žádosti a jedná se např. o notáře, krajské, matriční a obecní úřady, určené zastupitelské úřady, držitele poštovní licence, banky, pojišťovny a další instituce. Kontaktní místa veřejné správy mohou být označena názvem Czech POINT (Český Podací Ověřovací Informační Národní Terminál).[121] Tato místa bývají zřízená ve výše uvedených institucích a umožnují snadnější komunikaci s orgány veřejné správy, ověřování listin a získávání dat z různých informačních systémů. Smyslem kontaktních míst je snížení byrokratického zatížení občanů, tím že umožňují vyřízení široké palety žádostí na jednom místě, bez nutnosti návštěvy více úřadů.[122] Obsah doložky dokumentu se liší podle toho, zda je dokument převáděn z listinné nebo digitální formy a v závislosti na tom obsahuje název provádějícího orgánu, pořadové číslo, potvrzení o totožnosti obsahu, informace o počtu stran, datum vyhotovení, a dále jméno, příjmení a kvalifikovaný elektronický podpis osoby provádějící konverzi. V případě, že se jedná o konverzi do listinné podoby, obsahuje též údaje o tom, zda byl elektronický dokument opatřen elektronickým podpisem či jiným obdobným prvkem a datum a čas takového opatření a další.[123]

- **Elektronické podpisy**

Občanský zákoník uvádí, že pokud má mít právní jednání písemnou formu, je k platnosti takové písemnosti nutné připojit také podpis dotyčné osoby. Dále

---

[120] Viz. § 22 zákona č. 300/2008 Sb., *o elektronických úkonech a autorizované konverzi dokumentů* v posledním znění
[121] Viz. § 8a zákona č. 365/2000 Sb., *o informačních systémech veřejné správy* v posledním znění
[122] *Co je Czech POINT?*. Czechpoint [online]. © 2022 [cit. 8.12.2022]. Dostupné z: https://www.czechpoint.cz/public/statistiky-a-informace/co-je-czech-point/
[123] Viz. § 25 zákona č. 300/2008 Sb., *o elektronických úkonech a autorizované konverzi dokumentů* v posledním znění

odkazuje na možnosti využití mechanických prostředků k podpisu a v případě elektronických dokumentů na využití elektronických podpisů.[124] Elektronické podpisy, respektive dokumenty opatřené takovými podpisy mají určitou dobu platnosti. Obvykle se jedná o 1 rok. Připojením elektronického časového razítka, kterým je dokument označen, lze ale tuto dobu platnosti dokumentu dále prodlužovat (při prvním užití razítka o 5 let).[125]

- **Prostý elektronický podpis**

Jedná se o nejběžnější a o nejméně náročný způsob podepisování elektronických dokumentů. Takový podpis není ověřen žádným certifikátem jako následující uvedené způsoby. V praxi se může jednat o napsání podpisové doložky na závěr dokumentu jako např. „s úctou, Tomáš Novotný“. Dále se může jednat o některé způsoby potvrzení souvisejících s obchodními podmínkami webových stránek apod. Dalším příkladem prostého elektronického podpisu může být naskenovaný vlastnoruční podpis, který je přiložen k dokumentu. Prostý elektronický podpis je hojně využíván v soukromoprávní oblasti, kde není zákonem vyžadován jiný kvalifikovanější způsob podepisování. Jako takový bez dalších opatření poskytuje nejmenší jistotu ve smyslu identifikace konkrétní osoby a formy prostého elektronického podpisu nejsou vyjádřeny v zákoně.[126]

- **Zaručený elektronický podpis**

Tomuto termínu se věnuje eIDAS, který ukládá požadavky pro vytvoření a užívání zaručeného elektronického podpisu. Ten by měl být spojený s určitou osobou, která jako jediná s tímto druhem elektronických dat může nakládat. Dále by měl zaručený elektronický podpis umožňovat identifikaci této osoby, ale při tom není vytvořen na základě bezpečnostního certifikátu jako následující způsob elektronického podepisování. Zabezpečení těchto podpisů musí umožňovat

[124] Viz. § 561 odst. 1 zákona č. 89/2012 Sb., *Občanský zákoník* v posledním znění
[125] *Časová razítka*. Česká pošta [online]. © 2022 [cit. 22.11.2022]. Dostupné z: https://www.ceskaposta.cz/sluzby/certifikacni-autorita-postsignum/casova-razitka
[126] KUČERA, Roman. Používání různých podpisů. *Magazín Egovernment 1/2021* [online]. © 2022 [cit. 22.11.2022]. Dostupné z: https://www.egovernment.cz/inpage/podpisy-1-2021/

zjištění kterékoliv následné změny dat.[127] Dle některých odborníků se jedná o chybu v překladu, přičemž tento druh elektronického podpisu není reálně způsobilý k tomu, zjistit skutečného autora, jelikož neklade žádné další nároky na vytvoření takového podpisu, ve smyslu ztotožnění skutečné osoby před vytvořením podpisu a jeho výhodou oproti prostému elektronickému podpisu je pouze to, že umožňuje zjistit pozdější změnu dat.[128]

- **Zaručený elektronický podpis na základě kvalifikovaného certifikátu (uznávaný)**

Uznávaný elektronický podpis je možné vytvořit na základě několika bezpečnostních opatření, která na rozdíl od předchozích způsobů umožňují opravdu individuálně identifikovat jeho autora. Jedná se o data, která jsou schválena některou ze společností, představující kvalifikované poskytovatele služeb vytvářejících důvěru a poskytované kvalifikované služby vytvářející důvěru. Mezi tyto společnosti lze řadit např. První certifikační autorita, a. s., Česká pošta, s. p., eIdentity a. s., Software602 a.s., Správa základních registrů, SEFIRA spol. s.r.o., TECHNISERV IT, spol. s.r.o.[129] Tyto společnosti mají certifikační akreditaci sloužící k zaručení toho, že použitý podpis je skutečně spojen s osobou, pro kterou jsou tato data vytvořena. Zákon č. 297/2016 Sb. vyžaduje použití minimálně uznávaného elektronického podpisu nebo podpisu s vyšším zabezpečením v případě zasílání elektronických dokumentů veřejné správě, pokud fyzická osoba nevlastní datovou schránku.[130] V praxi se může jednat o různé žádosti, potvrzení, smlouvy a jiné písemnosti, sloužící ke komunikaci s úřady.

---

[127] Viz. článek 26 Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 *o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu* v posledním znění

[128] HANÁK, Jakub a Lukáš PRUŠKA. Elektronický podpis pohledem aktuální právní úpravy. *epravo.cz* [online]. 22.1.2020 [cit. 1.12.2022]. Dostupné z: https://www.epravo.cz/top/clanky/elektronicky-podpis-pohledem-aktualni-pravni-upravy-110560.html

[129] *Seznam kvalifikovaných poskytovatelů služeb vytvářejících důvěru a poskytovaných kvalifikovaných služeb vytvářejících důvěru*. Ministerstvo vnitra České republiky [online]. 19.10.2022 [cit. 1.12.2022]. Dostupné z: https://www.mvcr.cz/clanek/seznam-kvalifikovanych-poskytovatelu-sluzeb-vytvarejicich-duveru-a-poskytovanych-kvalifikovanych-sluzeb-vytvarejicich-duveru.aspx

[130] HANÁK, Jakub a Lukáš PRUŠKA. Elektronický podpis pohledem aktuální právní úpravy. *epravo.cz* [online]. 22.1.2020 [cit. 1.12.2022]. Dostupné z: https://www.epravo.cz/top/clanky/elektronicky-podpis-pohledem-aktualni-pravni-upravy-110560.html

- **Kvalifikovaný elektronický podpis**

Jedná se o elektronický podpis, který zaručuje nejvyšší míru zabezpečení a autentizace s konkrétní osobou. eIDAS takovému elektronickému podpisu dává váhu, jako by se jednalo o vlastnoruční podpis konkrétní osoby. Zabezpečení před zneužitím či zfalšováním takového podpisu zabraňují jednak hashovací algoritmy ve formě časových razítek, která umožňují zjistit případnou pozdější změnu dat v podpisu, a dále elektronické pečetě a kvalifikovaný prostředek, bez kterého nelze podpis vytvořit a použít. Tím může být prostředek ve formě dat, uložených na externím datovém nosiči. Ten může mít podobu přístupové karty, chipu, tokenu, nebo např. USB disku s aplikací. Pouze v případě držení a použití takového nosiče lze vytvořit kvalifikovaný elektronický podpis.[131]

- **Kvalifikované časové razítko**

Tímto pojmem jsou myšlena data, která slouží k potvrzení toho, že dokument, podpis či jiná data existovala v době jejich opatření tímto razítkem. Nejčastěji se tedy jedná o doplňující prvek elektronických podpisů, který má za úkol předejít pochybnostem o tom, že byl dokument uměle vytvořen s jiným datem, než ve kterém mohl skutečně vzniknout. Časová razítka vydávají uznávané certifikační společnosti (např. PostSignum) na základě žádosti osoby a tato razítka prodlužují platnost elektronického dokumentu.[132]

- **Kvalifikovaná elektronická pečeť**

Zákon č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce udává organizacím povinnost při zasílání elektronických dokumentů připojit kvalifikovanou elektronickou pečeť. Elektronický podpis má za účel prokázat, že dokument vytvořila konkrétní osoba, zatímco elektronická pečeť má za úkol prokázat, že se jedná o data, která jsou původní, a která jsou vytvořená konkrétní právnickou osobou (např. úřadem). Elektronických pečetí je také více druhů

---

[131] HANÁK, Jakub a Lukáš PRUŠKA. Elektronický podpis pohledem aktuální právní úpravy. *epravo.cz* [online]. 22.1.2020 [cit. 1.12.2022]. Dostupné z: https://www.epravo.cz/top/clanky/elektronicky-podpis-pohledem-aktualni-pravni-upravy-110560.html

[132] *Kvalifikovaná časová razítka PostSignum*. Elektronický podpis.cz [online]. [cit. 5.12.2022]. Dostupné z: https://www.elektronickypodpis.cz/kvalifikovana-casova-razitka/

v závislosti na jejich zabezpečení, nicméně Evropská Unie ukládá státům povinnost uznání právě kvalifikované elektronické pečeti, která je tak v celé Evropské Unii považována za nejvhodnější způsob pečetění elektronických dokumentů.[133]

6.3 Shrnutí poznatků

Problematika elektronických dokumentů se dotýká každého, kdo využívá moderní technologie. Rozdílný charakter těchto dat je dán účelem, za jakým jsou data vytvořena. Kapitola se po většinu času věnovala formě elektronických písemných dokumentů, které jsou v současnosti hojně využívány v oblastech soukromoprávní i veřejnoprávní povahy. Vzhledem ke směru vývoje této oblasti, je jisté, že tyto dokumenty budou v budoucnu čím dál častějším prostředkem v právní komunikaci fyzických i právnických osob s veřejnými orgány, a zároveň v soukromoprávním prostoru mezi fyzickými a právnickými osobami. Zajišťování těchto dat v souvislosti s trestním řízením nečiní přílišné problémy, avšak podstatnou okolností v dokazování těmito dokumenty je možnost identifikace původce takového dokumentu. K tomu slouží především technické nástroje umožňující označení dokumentu elektronickými daty, které náleží konkrétní osobě, po prokázání její totožnosti. V možnosti vytvoření elektronického dokumentu, který má stejnou první váhu jako listinný dokument, autor práce vidí obrovský potenciál. Užívání písemných elektronických dokumentů by v budoucnu mohlo vést ke snížení byrokratického zatížení, které je spojené s jednáním s orgány veřejné moci. V této oblasti byl za poslední roky učiněn značný pokrok. Správně označené elektronické dokumenty technickými prostředky dále mohou poskytovat dostatečnou jistotu fyzickým i právnickým osobám komunikujícím mezi sebou v otázce prokázání skutečné totožnosti jednající osoby.

---

[133] *Elektronická pečeť dle eIDAS – jak a co vlastně pečetit?*. ProID [online]. [cit. 6.12.2022]. Dostupné z: https://proid.cz/elektronicka-pecet-dle-eidas-jak-a-co-vlastne-pecetit/

7 Dokazování daty z mobilních komunikačních zařízení

Mobilními komunikačními zařízeními jsou mobilní telefony, vysílačky atd. Ty prošly v historii značným technickým vývojem a ve srovnání s původními mobilními telefony dnes nabízí nepředstavitelné možnosti. Nejprodávanějšími mobilními telefony jsou zařízení společností Apple iPhone, Samsung, Xiaomi, Honor, Vivo, Huawei atd. Ty disponují operačním systémem, který je závislý na jejich výrobci (iPhone užívá vlastní systém - iOS, a např. Samsung, Xiaomi a Huawei užívají univerzální systém smartphonů - Android).[134] Mobilní telefony jsou opatřeny vlastní vnitřní pamětí, do které lze ukládat data nejrůznějšího charakteru, jako jsou aplikace (některé základní aplikace se v mobilech nachází již v továrním nastavení), kontakty, zprávy nejrůznějších komunikačních aplikací (SMS, MMS, zprávy z chatovacích aplikací, e-maily, atd.), které mohou mít také podobu textovou, datovou, či zvukovou, dále data v obrazových formátech (.jpeg, .PNG, .BMP, .GIF, atd.), zvukové stopy (ve formátech .mp3, .mp4, .FLAC, .waw, atd.), videa (ve formátech .mp4, .mkv, .avi, .wmv, atd.). Mobilní telefony za pomocí svého technického rozhraní a aplikací, umožňují jejich uživatelům vytvářet data nejrůznějšího charakteru, která lze ukládat do paměti zařízení, cloudů a na další nosiče. Mobilní telefony obvykle disponují vlastním fotoaparátem, kterým lze vytvářet obrazové soubory, dále videokameru, kterou lze zaznamenávat video záznamy a hlasový záznamník, kterým lze vytvářet hlasové záznamy. Textovým rozhraním mobilního telefonu lze vytvářet textové soubory, či zprávy a komunikovat tak s ostatními uživateli. Mobilní telefony a jejich aplikace při používání také vytváří mnoho dat, o kterých uživatel často ani neví (data aplikací, metadata, logy, atd.). Totožnou funkci jako má vnitřní paměť mobilu, mohou plnit vložené paměťové karty, které jsou z pohledu práva součástí, či příslušenstvím takového mobilního telefonu. Může jít o karty typů SD, microSD a dále vzdálená úložiště v podobě cloudů.[135] Pro optimální a plnohodnotnou funkci mobilních telefonů je vyžadováno, aby byla do mobilního zařízení vložena SIM karta. K SIM

---

[134] SMEJKAL, Petr. Nejprodávanější mobily Apple, Samsung, Xiaomi, Honor, Vivo a Huawei. *Testado.cz* [online]. 29.8.2022 [cit. 9.11.2022]. Dostupné z: https://www.testado.cz/nejprodavanejsi-mobilni-telefony/?gclid=EAIaIQobChMIvrb3tbag-wIVFobVCh2xpwZsEAAYAyAAEgKQiPD_BwE

[135] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 197-198. ISBN 978-80-210-8073-7.

kartě je přiloženo účastnické číslo s mezinárodní předvolbou (v ČR +420). Následuje devítimístné číslo (př. 606 123 321). Toto číslo je originální a vždy může být aktivní pouze jedna karta s takovým číslem. Používáním SIM karty v mobilu lze skrze služby operátora provádět komunikaci s ostatními uživateli a využívat síťové služby (volání, SMS, MMS, GPS, internet). Zároveň i SIM karty umožňují ukládání některých dat přímo na kartu, přičemž se jedná především o uložené kontakty. Velikost paměti SIM karty zdaleka není srovnatelná s paměťovou kartou, která může mít paměť o velikosti stovek Gigabytů. I přes totožného výrobce, výrobní postupy a součásti zařízení, je každý mobilní telefon originální a lze ho individuálně identifikovat, k čemuž slouží především IMEI kód (International Mobile Equipment Identity), který je tvořen číselnou řadou konkrétního zařízení. Tento kód se někdy nachází přímo na štítku zařízení, případně jej lze zobrazit klávesovým příkazem ve tvaru *#06# - příklad IMEI: 364551823325481/16. Mobilní telefony umožňují síťové připojení, pomocí kterého mohou uživatelé užívat také funkce online skrze internetové připojení zajišťované operátorem, či Wi-fi připojením k jiné síti. Tím není myšleno pouze užívání internetového prohlížeče (Google Chrome, Mozilla Firefox, atd.), ale také použití rozšiřujících funkcí, jako jsou cloudové služby (iCloud, Google disk, atd.), e-mailové komunikace nebo chatovací aplikace a sociální sítě (Facebook, Messenger, Instagram, Whatsapp, Signal, Telegram, atd.). Skrze chatovací aplikace a sociální sítě lze komunikovat s ostatními uživateli a sdílet s nimi různé datové soubory. Mobilní zařízení dále umožňují spárování s dalšími zařízeními, či platebními kartami. Pomocí technologie NFC je možné provádět platby debetní či kreditní kartou přiložením telefonu k terminálu.[136] Z výše uvedeného vyplývá, že funkcí a možnosti užívání mobilních zařízení je opravdu spousta a není divu, že díky rozsáhlým možnostem použití a malé velikosti, se mobilní telefony staly součástí života lidí na celém světě. Zároveň umožňují propojení a komunikaci lidí přes různé kontinenty. Je pochopitelné, že mobilní telefony jsou v dnešní době součástí také oblasti trestné činnosti, kde mohou mít zásadní vliv na proces dokazování, neboť se jedná o zařízení, ve kterém se často nachází velké množství dat o jeho uživateli. V rámci

[136] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 198-206. ISBN 978-80-210-8073-7.

trestního řízení mohou být mobilní telefony předmětem (odcizený mobilní telefon) nebo prostředkem (mobilní telefon, pomocí kterého podezřelý vydírá poškozeného) trestné činnosti.

7.1 Zajištění dat

Na otázku, jak zajišťovat data z mobilních telefonů není jednoznačná odpověď, neboť se jedná o tak obsáhlou problematiku, a takové množství různých dat, kterým zákon poskytuje různý stupeň ochrany, že zkrátka jeden způsob zajištění není dostatečný. Princip zajišťování dat z mobilního telefonu či vzdáleného úložiště je stejný jako v případě jiných elektronických důkazů a je důležité, aby OČTŘ tyto úkony prováděly podle zákona, s co nemenším omezením práv dotčených osob a zároveň co nejodborněji, aby nemohla být zpochybněna pravost a správnost získaného důkazu, což se dotýká především policejního orgánu, který data zajišťuje. Způsoby zajištění dat z mobilního telefonu lze rozdělit na několik základních skupin podle charakteru dat, která jsou tímto úkonem dotčena.

- **Zajištění dat, která se nachází v paměti mobilního telefonu**

Nejčastějším úkonem v souvislosti se zajišťováním dat, která se nachází v mobilním telefonu, jsou úkony TŘ, která pojednávají o postupu při zajišťování věcí, jako vydání nebo předložení věci (§ 78 TŘ), odnětí věci (§ 79 TŘ), postup při provádění prohlídek (§ 82 – 85c TŘ) a ohledání (§ 113 TŘ), přičemž povinnost vydat věc důležitou pro trestní řízení neplatí pouze pro obviněného, ale může se dotknout osob v kterémkoliv postavení trestního řízení. Pokaždé není nutné zajišťovat celé zařízení, ale lze využít součinnosti uživatele, který může zařízení na výzvu policejního orgánu pouze předložit podle § 78 TŘ pro následné ohledání a zajištění potřebných dat do jiného úložiště. Po tomto úkonu se mu zařízení ihned vrací a nejedná se tedy o tak invazivní prostředek, kterým by bylo vydání zařízení a následné zkoumání, které by trvalo podstatně delší dobu. V souvislosti s takovým zajištěním mobilního telefonu policejní orgán dále nepotřebuje žádné povolení či příkaz k analýze dat, která se nachází uvnitř zařízení, čímž je myšlena vnitřní paměť zařízení, včetně příslušenství, kterým mohou být SIM karty nebo paměťové karty. Zařízení musí být řádně popsáno v protokolu, včetně takového

popisu, který znemožní záměnu za jiné zařízení a umožní tak jeho individuální identifikaci. Podstatným prvkem je zaznamenání IMEI kódu telefonu. Tímto způsobem lze z mobilních telefonů vytěžovat data nejrůznějšího charakteru (obrazové, zvukové, video, textové soubory a informace o nich, kontakty nebo obsah doručených zpráv SMS, zpráv chatovacích aplikací, informace týkající se nainstalovaného softwaru a aplikací v mobilním telefonu atd.). Je nutné si uvědomit, že data uložená v mobilních telefonech jsou nestálá a při zajišťování takových dat je nutné postupovat, pokud možno co nejodborněji, aby nedošlo k nechtěnému pozměnění, či vymazání důležitých dat. Zároveň je vhodné celý proces zajištění řádně zadokumentovat a postupovat co nejrychleji, neboť mobilní telefony umožňují propojení s dalšími zařízeními a hrozí tak odstranění dat pomocí vzdáleného přístupu k zařízení. Celá problematika zabezpečení dat před pozměněním, či odstraněním, je složitější a závisí na míře spolupráce uživatele. Ideálním způsobem, jak zajistit nemožnost změn, je zařízení vypnout a odpojit baterii, což ale může způsobit obtíže při následném zapnutí zařízení, které může být opatřeno PIN kódem SIM karty, nebo heslem, zvoleným gestem, či otiskem prstu uživatele, pro zpřístupnění mobilního telefonu. Pokud je uživatel ochotný spolupracovat, může policejnímu orgánu poskytnout PIN kódy, hesla, gesta a údaje, ke zpřístupnění obsahu v zařízení, jinak platí, že ho nelze nutit k tomu, aby takové údaje vydal. V případě že dotyčná osoba odmítá spolupracovat, nezbývá policejním orgánu, aby se pokusil do zákonně zajištěného mobilního telefonu dostat jiným způsobem. Zabezpečení SIM karty PIN a PUK kódem, může policejní orgán prolomit v součinnosti s operátorem, kterého je třeba oslovit s žádostí ve smyslu § 8 odst. 1 TŘ o vydání PUK kódu, který nemůže uživatel sám měnit. V případě, že se do zařízení nelze otevřeně dostat kvůli jinému zabezpečení, policejnímu orgánu nezbývá, než se pokusit kontaktovat výrobce, za účelem prolomení zabezpečení. Další možností je poskytnout zařízení znalci, ke znaleckému zkoumání, či odborným pracovištím policie OKTE. Prolomení zabezpečení ale není možné v každém případě. Prolomení zabezpečení znalcem, je časově a finančně náročné. Z toho důvodu jsou v jednodušších případech spíše

upřednostňovány jiné způsoby zajištění důkazů než znaleckým posudkem.[137] Pokud nastane situace, že je zajištěn telefon, na kterém dále probíhá komunikace, se kterou se dotčený uživatel již nemohl před zajištěním seznámit, nemůže k takovým informacím policejní orgán přistupovat, jak se mu zlíbí, ale je povinen opatřit si příkaz k odposlechu podle § 88 TŘ.[138] (viz. **kapitola 5 Dokazování odposlechem**). Samotné zajištění dat z telefonu lze provést několika způsoby, přičemž nejzákladnějším, je připojení mobilního telefonu ke služebnímu počítači pomocí rozhraní USB, ze kterého je následně kopírován obsah dat do úložiště policejního orgánu, čímž nejsou nijak poškozena data na primárním úložišti dotčené osoby. To lze provést jako ohledání věci (§ 113 TŘ), při kterém se kopírují pouze data, o kterých je předpoklad, že by mohla být důležitá pro trestní řízení. U ohledání je v ideálním případě přítomná také dotčená osoba, či nezúčastněná osoba, která svým podpisem protokolu potvrdí, že postup policie probíhal tak, jak je v protokolu uvedeno. Dále je doporučeno zajištěná data zkomprimovat do souboru .Zip, který je následně opatřen „hash kódem" (více ke komprimaci a hash kódu je uvedeno v **kapitole 2.3 Nakládání s elektronickými důkazy**), který zaručuje, že se zajištěnými daty nebylo dále nijak manipulováno. Celý proces zajištění je zaznamenán do protokolu o ohledání věci, který může být následně přečten v hlavním líčení před soudem. Takto zajištěná data mohou být následně vyhodnocována a podrobena zkoumání. Dalším způsobem je vyhledání podstatných dat přímo v rozhraní mobilního telefonu a následné ofocení jeho displeje (např. vyfocení obrázku z displeje telefonu). Tento způsob je časově méně náročný, ale na druhou stranu neposkytuje tolik informací (místo uložení v paměti, datu a čas vytvoření, atd.), jako právě celá kopie dat. Další možností je využití forenzních nástrojů pracovišť OKTE, které umožňují získání kompletních dat z paměti, včetně zdánlivě smazaných dat, která ještě nebyla přepsána jinými novými daty.[139] Jedná se např. o programy UFED, EnCase Forensic, MOBILedit

[137] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 201-206. ISBN 978-80-210-8073-7.

[138] Výkladové stanovisko NSZ č. 1/2015 Sb., *ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů včetně obsahu e-mailových schránek*

[139] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 206-209. ISBN 978-80-210-8073-7.

Forensic.[140] Další možností je využití soukromých znalců v oboru elektroniky, IT a elektrotechniky, jejichž metody jsou však náročné z časového i finančního hlediska. Metody znaleckého zkoumání mohou mít také destruktivní charakter a mohou vést k částečnému nebo úplnému poškození dat v zařízení, nebo dokonce celého zařízení, které je při provádění destruktivních metod někdy nutné „rozebrat na části".[141]

- **Zajištění dat z jiného úložiště, ke kterému je přistupováno ze zajištěného mobilního telefonu**

Mobilní telefony umožňují využívat internetovou síť a instalovat do zařízení různé klienty a přístupové aplikace k úložištím mimo toto zařízení (e-mail, cloudové úložiště, atd.). Pokud policejní orgán zamýšlí zajištění také takových dat, nemůže k nim skrze mobilní telefon přistupovat bez povolení, či příkazu soudu, neboť na taková data se pohlíží jako na záznamy uchovávané v soukromí a vztahuje se na ně přísnější zákonná ochrana. Pokud má jít o data, popř. obsah komunikace, která proběhla v minulosti a nachází se na vzdáleném úložišti (cloud, e-mailová schránka, atd.), musí policejní orgán při zajišťování takových dat postupovat v souladu s ustanovením § 158d odst. 3 TŘ. Při splnění těchto podmínek má policejní orgán oprávnění vytvořit kopii tohoto úložiště a následně může data zkoumat a vyhodnocovat, ale neopravňuje ho to přistupovat k takovému úložišti opakovaně, nebo sledovat úložiště či komunikaci v budoucnosti. Pokud se má jednat o obsah komunikace probíhající, nebo budoucí, je nutné, aby si policejní orgán obstaral soudní příkaz k odposlechu takové komunikace podle § 88 TŘ.[142]

- **Odposlech a provozní a lokalizační údaje mobilního telefonu**

V mobilních telefonech jsou obvykle vloženy SIM karty s telefonním číslem uživatele, které jim umožňují komunikovat ve smyslu telekomunikačního provozu

---

[140] MICHÁLEK, Luděk a kol. *Kriminální zpravodajství jako nástroj kontroly trestné činnosti a zajišťování vnitřní bezpečnosti.* 1. vyd. Praha: Policejní akademie České republiky v Praze, 2020, s. 105. ISBN 978-80-7251-506-6.

[141] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 208. ISBN 978-80-210-8073-7.

[142] Výkladové stanovisko NSZ č. 1/2015 Sb., *ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů včetně obsahu e-mailových schránek*

s jinými účastníky. Pokud policejní orgán potřebuje zjistit obsah takové komunikace v budoucnosti, je nutné dodržet zákonný postup podle § 88 TŘ řádu, o odposlechu a záznamu telekomunikačního provozu. Více se této problematice věnuje **kapitola 5 Dokazování odposlechem**. Mimo obsahu takové komunikace bývají leckdy stejně důležité také údaje o uskutečněném telekomunikačním provozu, ve smyslu provozních a lokalizačních údajů, které lze získat postupem podle § 88a TŘ, čemuž se blíže věnuje **kapitola 4 Dokazování provozními a lokalizačními údaji**.

7.2 Provádění a hodnocení důkazu daty z mobilních komunikačních zařízení

Postup při provádění a hodnocení důkazů získaných odposlechem či provozními a lokalizačními údaji, je blíže popsán v samostatných kapitolách konkrétní problematiky. Tato kapitola se bude spíše zabývat daty, která se nachází přímo v mobilním telefonu. Provést důkaz z dat mobilního telefonu je v některých případech možné v jeho původní formě, čímž není dotčen postup, který má za úkol získání takového důkazu zdokumentovat (protokol o vydání, protokol o ohledání, odborné vyjádření, znalecký posudek). Jestliže se např. jedná o obrázek, videozáznam, či hlasovou zprávu, není z pohledu autora důvod, aby soud nemohl přistoupit k provedení dokazování v jeho původní podobě. Přesto však policejní orgán taková data vyhodnocuje a záleží na soudu, zda bude dokazování probíhat tímto způsobem, nebo ve formě přečtení protokolu jako listinného důkazu. Spousta dat se v mobilních telefonech nachází v nesrozumitelné formě a je nutné je vyhodnotit, k čemuž slouží forenzní nástroje specializovaných pracovišť či soukromých znalců, kteří k těmto datům vytváří odborná vyjádření či znalecké posudky. Následně může být proveden důkaz výslechem znalce (§ 108 TŘ), přičemž všechny úkony směřující k zajištění a provedení důkazu musí být provedeny v souladu se zákonem, tak jak je uvedeno v části o zajištění dat. Tak jako v případě jiných elektronických důkazů, je nutné ustanovit osobu, která se zařízením manipulovala v době vzniku těchto dat. Běžně se jedná o jediného uživatele takového zařízení, avšak ten se může bránit tím, že takové zařízení nikdy neměl, data nevytvářel, nikomu nepsal, či nevolal atd. Z druhého pohledu

existují případy, ve kterých pachatel využil mobilního telefonu jiné osoby k páchání trestné činnosti, buď s jejím vědomím, nebo po získání přístupu k zařízení jiným způsobem. Tato zařízení obsahují takové množství doplňujících dat a údajů, že obvykle nebývá problém s prokázáním činnosti uživatele. Současně důkazy z dat mobilních telefonů, mohou být podpořeny jinými získanými důkazy a společně jsou způsobilé utvořit ucelený řetězec nepřímých důkazů, na základě kterých lze vyslovit vinu či nevinnu podezřelého. Důkazy z dat v mobilních telefonech nemusí jen vést k přímému prokázání viny v hlavním líčení, ale mohou být použity např. v přípravném řízení za účelem získání doznání nebo naopak vyvrácení lživé výpovědi.[143]

7.3 Shrnutí poznatků

Jelikož jsou mobilní telefony nejrozšířenějším elektronickým zařízením sloužícím ke komunikaci, je z pohledu policejního orgánu zajišťování dat z úložiště mobilního telefonu patrně tím nejčastějším úkonem v rámci zajišťování elektronických důkazů. Mobilní telefony hrají čím dál větší roli ve většině oblastí trestné činnosti. Mobilní telefon je dle názoru autora práce nejhlubším nositelem elektronických informací o jeho uživateli a v trestním řízení se zajišťováním dat z těchto zařízení setkávají policisté na všech úrovních, od obvodních odděleních policie po celorepublikové útvary policie. Autor si v tomto směru z vlastních zkušeností dovoluje poukázat na fakt, že tak, jak se často liší úroveň zpracování spisů na jednotlivých článcích policie, lze totožné tvrdit i v souvislosti se zajišťováním dat z mobilních telefonů. Je pochopitelné, že policisté na obvodních odděleních nebudou zpracovávat hloubkovou analýzu paměti mobilního telefonu tak, jak je tomu v nezávažnějších trestných činech, nicméně základní postup při zajišťování zařízení, či dat, která se v tomto zařízení nacházejí, by v tomto směru měl být sjednocen. Tím se lze vyhnout tomu, aby bylo provedeno zajištění a zadokumentování dat nedostatečným způsobem, který vytváří prostor ke zpochybňování pravosti důkazu či zákonnosti zajištění těchto dat. Vzhledem k tomu, že analýza dat ze zařízení pomocí OKTE či znalců je časově a v případě

[143] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 209-219. ISBN 978-80-210-8073-7.

znalců i finančně náročná, je dán ze strany policejních orgánů důraz na to, aby co největší množství dat bylo zajišťováno a analyzováno již na organizačních článcích policie, které vedou spis. Tak jako v případě jiné výpočetní techniky, se i vývoj mobilních telefonů posouvá vpřed vysokou rychlostí. Tento rychlý vývoj může mít za následek ztížení manipulace a zajištění dat především u starších policistů, kteří nejnovější technologie v běžném životě nevyužívají. Důsledkem toho může být nedostatečné zajištění důležitých dat nikoliv z vědomého jednání policistů, ale zkrátka z důvodu jejich neodbornosti v tomto směru. Zajistit v příštích letech dostatečnou odbornost při manipulaci s mobilními telefony a jejich daty, by mělo být dle autora práce pro Policii ČR klíčovou prioritou, neboť pokud se Policie ČR není schopná orientovat v současných technologických trendech nyní, tak s rychlostí vývoje a přesunu do virtuálního prostředí, tento faktor může v budoucnosti představovat obrovské bezpečnostní riziko pro celou společnost.

8 Dokazování daty z dohledových systémů kybernetické bezpečnosti

Kyberprostor neboli virtuální svět tvořící elektronickou síť je prostorem, který nabízí mnoho možností a také informací. Do této sféry se přesouvá čím dál více oblastí života. Trestná činnost se tak jako jiné oblasti života vyvíjí a pachatelé se snaží využívat všech dostupných prostředků k naplnění svých cílů. Klasických trestných činů, jako jsou loupeže bankovních institucí, vydírání atd. ubývá, a naopak je patrných více trestných činů, spáchaných v tomto virtuálním světě (Podvod § 209 TZ, Výroba a jiné nakládání s dětskou pornografií § 192 TZ, Legalizace výnosů z trestné činnosti § 216 TZ, Neoprávněný přístup k počítačovému systému a nosiči informací § 230 TZ, Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat § 231 TZ a další). Spáchané činy v tomto prostředí mají i přes svůj virtuální děj značný dopad na skutečný život lidí, neboť se může jednat o útoky na citlivá osobní data, přístupové údaje, klíčovou infrastrukturu a také finance prostřednictvím počítačových sítí. Kyberprostor je pro moderní zločinecké organizace lákavým prostředím už jen díky míře anonymity, kterou nabízí a takové organizace jsou jedním z největších globálních bezpečnostních rizik, které se mohou dotknout všech subjektů využívajících moderní technologie v soukromém i veřejném prostoru. Kybernetické bezpečnosti se věnuje především zákon č. 181/2014 Sb., o kybernetické bezpečnosti (ZKB) a zákon č. 127/2005 Sb., o elektronických komunikacích (ZEK). V souvislosti s touto problematikou je klíčové přiblížení pojmů - Kybernetický útok, Kybernetická bezpečnostní událost a incident.

- **Kybernetické útoky**

Kybernetické útoky jsou taková jednání pachatelů, která jsou páchána v kyberprostoru a mohou směřovat proti kterémukoliv uživateli elektronických sítí. Největším rizikem pro společnost jsou však tzv. DDoS útoky profesionálních hackerských týmů, které mohou směřovat proti národním a nadnárodním firmám, za účelem získání obrovského množství osobních dat, firemního know-how, nebo znepřístupnění služeb, což s sebou nese riziko poškození obrovského množství

klientů společností. Mohou mít také podobu útoků na důležité státní instituce či infrastrukturu státu (energetické a chemické společnosti, dopravní společnosti, bankovní sektor, zdravotní zařízení, vodní hospodářství, nebo digitální infrastruktura). Takové útoky mohou probíhat právě za použití infikovaných zařízení malwary běžných uživatelů, kteří nemusí nic tušit.[144]

- **Malware**

Jedná se o škodlivý program, který je nainstalován v zařízení uživatele, aniž by o něm věděl, a který umožňuje pachateli přístup do takového zařízení. Je mnoho druhů malwarů (viry, trojské koně, atd.). Malwary jsou užívány za různými účely, jakými jsou např. získání osobních či přístupových údajů, krádež peněz či zablokování přístupu do zařízení. Tyto programy jsou nejčastěji šířeny pomocí internetové sítě v různých podobách. Může se např. jednat o přílohu mailu, různých souborů nebo programů stažených z webu, kdy po otevření takového souboru je naistalován škodlivý program do zařízení uživatele.[145]

- **Spyware**

Jeden z druhu malwaru, který má za úkol špehovat uživatele při činnosti se zařízením. Spyware se současně pokouší získat přístup k osobním datům, údajům internetového bankovnictví, nebo sleduje činnost uživatele na internetu.[146]

- **Phishing**

Pod tímto pojmem se skrývá současný fenomén rozesílání falešných e-mailů nebo jiných zpráv, které se snaží vyvolat interakci uživatele. Tyto zprávy mohou působit, jako by je odesílaly skutečné společnosti (banky, pojišťovny, atd.) nebo jiní uživatelé. Phishingové útoky mohou mít podobu například upomínky za fakturu, upozornění o výhře, nebo se mohou jevit jako běžné zprávy uživatelů sociálních sítí, které lákají uživatele k otevření odkazu, který se v takové zprávě či mailu

---

[144] *Co je DDoS útok a jaká je ochrana?*. Eset.com [online]. [cit.10.11.2022]. Dostupné z: https://www.eset.com/cz/ddos-utok/

[145] *Malware*. Avast.com [online]. [cit. 10.11.2022]. Dostupné z: https://www.avast.com/cs-cz/c-malware

[146] *Spyware*. Avast.com [online]. [cit. 10.11.2022]. Dostupné z: https://www.avast.com/cs-cz/c-spyware

nachází. Po kliknutí na odkaz je uživatel přesměrován na falešné webové stránky. Tyto webové stránky jsou často velmi propracované a mohou mít podobu webu internetové banky, popř. platební brány, kam uživatel následně uvádí údaje o bankovní kartě či přístupové údaje do internetové banky. Vyplněním údajů uživatel nevědomě poskytuje přihlašovací údaje pachateli. Weby působí opravdu autenticky a často je pouze nepatrný rozdíl v URL adresy, kde může přebývat nebo chybět písmenko, popř. se může jednat o jinou doménu (.cm místo .com).[147]

- **Vishing**

Jedná se o podvodné vylákání přístupových údajů uživatele, které obvykle probíhá telefonickým hovorem. Pachatelé se mohou vydávat např. za pracovníky banky, policisty, nebo lékaře a pod smyšlenou legendou se snaží tlačit na majitele účtu, aby jim poskytl své osobní údaje, údaje o platební kartě, bankovním účtu atd. Při tomto jednání často dochází za součinnosti poškozeného k odčerpání peněz z jeho bankovního účtu a k následnému přeposlání na účet pachatele do zahraničí. Množí se také případy, kdy pachatelé navedou poškozeného k výběru co největšího obnosu hotovosti z banky, přičemž se pachatelé vydávají za zaměstnance banky nebo policisty, kteří mají informace o tom, že v bance nejsou peníze poškozeného v bezpečí. Poté přesvědčí poškozeného k vložení těchto peněz do Bitcoinmatů (automaty na vkládání hotovosti do virtuální měny). Takto vložené peníze už jsou následně nedohledatelné a odchází na účet pachatelů. Pachatelé jsou zároveň schopni přesměrovat telefonní hovor tak, že působí, jako by volali ze skutečného čísla policie nebo bankovní instituce. Při zpětném volání na toto číslo se však poškození nedovolají pachateli, ale opravdu na policii nebo do banky.[148]

- **Dos a DDoS útoky**

Útoky, které mají za úkol vyřadit nebo znepřístupnit službu nebo systém jeho uživatelům. Napadenou službou či systémem mohou být e-shopy, webové

[147] *Phishing*. Avast.com [online]. [cit. 10.11.2022]. Dostupné z: https://www.avast.com/cs-cz/c-phishing

[148] DOBROZENSKÝ, Dominik. Phishing: definice phishingu, jak jej rozpoznat a jak na phishingový útok vyzrát. *Cnews.cz* [online]. 3.3.2022 [cit. 10.11.2022]. Dostupné z: https://www.cnews.cz/co-je-phishing-a-jak-se-branit

stránky, či online služby a systémy. Útoky Dos probíhají pouze z jednoho zařízení, kdežto DDoS útoky probíhají z více infikovaných zařízení současně (botnetová síť). Tyto útoky mohou mít různé cíle, jako je generování zisku vydíráním poškozené společnosti, vyřazení a poškození konkurenčních společností, ale k útokům také dochází z ideologických a aktivistických důvodů. DDoS útoky mohou také sloužit pouze jako zástěrka, přičemž primárně se pachatelé mohou pokoušet o špionáž či sabotáž společností.[149]

- **Kybernetická bezpečnostní událost, incident a trestný čin**

Těmto pojmům se věnuje § 7 ZKB:

„(1) Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.

(2) Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.

(3) Orgány a osoby uvedené v § 3 písm. b) až f) jsou povinny detekovat kybernetické bezpečnostní události v jejich významné síti, informačním systému kritické informační infrastruktury, komunikačním systému kritické informační infrastruktury, informačním systému základní služby nebo významném informačním systému.“[150]

Kybernetický bezpečnostní incident je stav (událost), který jsou některé napadené společnosti povinné hlásit národnímu nebo vládnímu pracovišti CERT v závislosti na provozovaných službách dotčené společnosti. Pracoviště CERT tento stav (událost) zhodnotí a posoudí, zda došlo k ohrožení bezpečnosti. V případě podezření ze spáchání trestného činu, se teprve událost stává kybernetickým bezpečnostním incidentem, který následně pracoviště CERT oznamuje Policii ČR. Národní a vládní pracoviště CERT i Policie ČR mají k dispozici pouze data, která

[149] *Co je DDoS útok a jaká je ochrana?.* Eset.com [online]. [cit.10.11.2022]. Dostupné z: https://www.eset.com/cz/ddos-utok/

[150] Viz. § 7 zákona č. 181/2014 Sb., *o kybernetické bezpečnosti* v posledním znění

se nachází v takovém oznámení. Policie ČR může zahájit úkony trestního řízení na základě informací v tomto oznámení.[151]

8.1 Dohledová pracoviště kybernetické bezpečnosti CERT (Computer Emergency Response Team)

Mimo zkratky CERT mohou být tato pracoviště nazývána zkratkami CSIRT (Computer Security Incident Response) nebo CIRC (Computer Incident Response Capability). Dohledová pracoviště mají za úkol zabezpečovat bezpečnost sítí, předcházet a reagovat na kybernetické bezpečnostní incidenty a v případě vzniku incidentu minimalizovat vzniklé a hrozící škody. V souvislosti s touto činností spolupracují s ostatními pracovišti, Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB) a Policií ČR. Dále mohou provádět mezinárodní spolupráci.[152] Dohledová pracoviště lze rozdělit na zákonem stanovená (vládní a národní) a jiná.

- **Vládní dohledové pracoviště kybernetické bezpečnosti**

Oblast činností vládního CERT pracoviště stanoví ustanovení § 20 ZKB, které v úvodu zmiňuje, že vládní CERT je součástí NÚKIB. Tuto funkci plní společnost GovCERT.cz. Tento bezpečnostní tým je zaměřen především na řešení kyberneticky bezpečnostních incidentů, které jsou způsobilé ohrožovat bezpečnost státu a služeb, které poskytuje. Vládní CERT může představovat interní tým, který má možnost přímo zasahovat v případě potřeby.[153] Ten konkrétně koordinuje postup při řešení incidentů a poskytuje podporu týmům dotčené společnosti. Poskytuje dále služby za účelem analýzy incidentu a jeho řešení, případně provádí konzultace a předávání informací o bezpečnostním incidentu mezi týmy v mezinárodním měřítku. Dále provádí preventivní opatření a testování zabezpečení institucí na základě smlouvy. Odborníci týmu mohou provádět analýzu bezpečnostního incidentu a vyhledávat škodlivé kódy

[151] VÁGNER, Michal. *Management na místě činu kybernetického bezpečnostního incidentu*. Praha, 2021. Disertační práce. Institut forenzních, bezpečnostních studií a managementu, s. 29-30.
[152] Tamtéž
[153] KROPÁČOVÁ, Andrea. CERT/CSIRT týmy a jejich role. *Root.cz* [online]. 6.5.2013 [cit. 14.11.2022]. Dostupné z: https://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/

v systému, přičemž také mohou institucím poskytovat podporu ve formě zajištění důležitých dat k takové analýze ve formě kopií, či obrazů paměti. V rámci své činnosti dále vládní CERT poskytuje vzdělávací a školící programy zaměřené na kybernetickou bezpečnost a na postupy týkající se bezpečnostních incidentů, k čemuž vytváří doporučující dokumenty pro společnosti, instituce a uživatele informačních technologií.[154]

- **Národní dohledové pracoviště kybernetické bezpečnosti**

Oblast činností národního CERT pracoviště stanoví § 17 ZKB. V České republice zastává funkci národního pracoviště společnost CSIRT.cz. Národní CERT na rozdíl od vládního či interních týmů nemají kontrolu nad infrastrukturou a slouží jako prostředník, na kterého se mohou instituce obracet v případě potřeby koordinace více složek při bezpečnostním incidentu, popř. za účelem předání kontaktů a informací mezi jednotlivými týmy. Většina incidentů bývá vyřešena přímou komunikací s bezpečnostními týmy dotčených institucí. CSIRT.cz v rámci své činnosti dále provádí vzdělávací osvětu, zaměřenou na kybernetickou bezpečnost pro veřejnost nebo instituce, které mají za úkol podpořit vznik dalších pracovišť daných institucí za účelem zabezpečení této kritické infrastruktury.[155] Vznik a funkci národního pracoviště CERT sice ukládá zákon ZKB, nicméně se jedná o společnost soukromoprávní povahy, která díky tomuto postavení může pružněji a rychleji reagovat, než tomu bývá v případě veřejnoprávních institucí. [156]

- **Jiná dohledová pracoviště kybernetické bezpečnosti**

Mimo výše uvedené druhy dohledových pracovišť existují další dohledová pracoviště, jako například interní pracoviště institucí, bank, školských zařízení, výzkumných pracovišť, komerčních institucí atd. Ta jsou zřizována na základě soukromoprávní smlouvy. Právě tato pracoviště jsou základním prvkem ve struktuře dohledových pracovišť, neboť jsou společně se správci sítí první, na

---

[154] *Poskytované služby*. Národní centrum kybernetické bezpečnosti [online]. [cit. 14.11.2022]. Dostupné z: https://www.govcert.cz/cs/vladni-cert/poskytovane-sluzby/

[155] KROPÁČOVÁ, Andrea. CERT/CSIRT týmy a jejich role. *Root.cz* [online]. 6.5.2013 [cit. 14.11.2022]. Dostupné z: https://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/

[156] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 223-224. ISBN 978-80-210-8073-7.

koho by se měl uživatel obrátit, pokud bylo jeho zařízení napadeno. Tato pracoviště také mohou být prvním článkem, který bezpečnostní incident zaznamená. Tato pracoviště mají za úkol chránit konkrétní infrastrukturu či síť před bezpečnostními riziky a kyberútoky. Vzhledem k tomu, že jejich činnost je úzce svázána právě s dotčenou institucí, jsou oprávněny v této infrastruktuře provádět bezpečnostní opatření za účelem odstranění nebezpeční (odpojení zařízení od sítě, provádění změn v nastavení, zastavování poskytované služby, popř. aplikovaní obranných mechanismů atd.), a dále se snaží minimalizovat ztráty a napravovat škody vzniklé při těchto incidentech a kybernetických útocích. V souvislosti s napadením uchovávají data, která mohou následně sloužit k zahájení trestního řízení a incidenty konzultují s národním CERT pracovištěm, které takovou možností přímého zásahu v institucích nedisponuje.[157] Tato jiná pracoviště by se dala dále rozdělit na následující 3 kategorie:

- **Pracoviště, která jsou součástí subjektu**, **jemuž § 3 ZKB ukládá povinnosti** v souvislosti s kybernetickou bezpečností (instituce zajišťující kritickou informační infrastrukturu či významnou síť, atd.)[158]

- **Pracoviště, která nejsou součástí subjektu, kterému § 3 ZKB neukládá povinnosti v** souvislosti s kybernetickou bezpečností, **ale zároveň** se jedná o subjekty, které **poskytují služby podle ZEK**, jímž ukládá povinnosti v souvislosti s jejich činností právě ZEK[159] (*„Podnikatelé zajišťující veřejné komunikační sítě nebo poskytující veřejně dostupné služby elektronických komunikací jsou povinni zajistit technicky a organizačně důvěrnost zpráv a s nimi spojených provozních a lokalizačních údajů…“*)[160]

---

[157] KROPÁČOVÁ, Andrea. CERT/CSIRT týmy a jejich role. *Root.cz* [online]. 6.5.2013 [cit. 14.11.2022]. Dostupné z: https://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/

[158] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 226. ISBN 978-80-210-8073-7.

[159] Tamtéž

[160] Viz. § 89 odst. 1 zákona č. 127/2005 Sb., *o elektronických komunikacích* v posledním znění

- **Pracoviště, která nejsou součástí subjektu, jemuž § 3 ZKB ukládá povinnosti** v souvislosti s kybernetickou bezpečností **a zároveň subjekt není podnikatelem v poskytování služeb podle ZEK**[161]

8.2 Zajištění dat

Způsob, jakým lze zajistit data z kybernetického bezpečnostního incidentu, díky kterým by bylo možné zahájit úkony v trestním řízení, je dán především charakterem dotčené instituce a jejího vztahu k ZKB a ZEK, jak je popsáno výše. Jelikož se jedná o specifickou problematiku, je jen těžko představitelné, že by v případě kybernetických bezpečnostních incidentech docházelo ke klasickému ohledání místa činu, tak jako v případě obecné trestné činnosti, neboť důležitá data se nachází ve virtuálním prostoru a jsou často zašifrována a opatřena heslem. Nelze se také spoléhat na vydání či odnětí zařízení jako věci důležité pro trestní řízení a jeho další podrobování znaleckému zkoumání či ohledávání, neboť se často jedná o zařízení, jejichž poloha nemusí být pro policejní orgán dost dobře známa. Policejní orgán se tak často musí spoléhat pouze na data, která mu jsou od dotčených společností dobrovolně poskytována. Pochopit strukturu sítě za účelem zajištění potřebných dat, by představovalo obrovskou časovou zátěž, a dále by také takové odpojení a odebrání zařízení pro účely trestního řízení mohlo představovat riziko vzniklých vysokých škod společností, kterých se takový zásah týká.[162]

- **Zajištění dat od pracovišť, která jsou součástí subjektu, jemuž § 3 ZKB ukládá povinnosti v souvislosti s kybernetickou bezpečností**

Ustanovení § 3 ZKB vymezuje oblasti poskytujících služeb subjektů, kterým ukládá určité povinnosti v souvislosti s touto činností. Takovou povinností je mimo jiné podávat hlášení v případě zjištění bezpečnostního incidentu ve svěřené síti či systému infrastruktury. To, zda incidenty hlásí národnímu či vládnímu pracovišti CERT stanoví § 8 ZKB, který uvádí, že orgány a osoby uvedené

[161] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 226. ISBN 978-80-210-8073-7.
[162] VÁGNER, Michal. *Management na místě činu kybernetického bezpečnostního incidentu*. Praha, 2021. Disertační práce. Institut forenzních, bezpečnostních studií a managementu, s. 44-45.

v § 3 písm. c) až f) jsou povinné hlásit zjištěné bezpečnostní incidenty přímo NÚKIB čili vládnímu pracovišti CERT, který zajišťuje společnost GovCERT.cz. Pracovišti národního CERT, který zajišťuje společnost CSIRT.cz, jsou takové incidenty povinny hlásit osoby a orgány uvedené v § 3 písm. b) a h) tohoto zákona.[163] Tyto údaje je z hlediska trestního řízení možné vyžadovat na základě žádosti podle § 8 odst. 1 TŘ a v hlášení by měly být uvedené informace o IP adresách souvisejících s bezpečnostním incidentem.[164]

- **Zajištění dat od pracovišť, která nejsou součástí subjektu, jemuž § 3 ZKB ukládá povinnosti v souvislosti s kybernetickou bezpečností, ale zároveň se jedná o subjekty, které poskytují služby podle ZEK**

Taková pracoviště nejsou ze zákona (ZKB) povinny podávat národnímu či vládnímu pracovišti CERT hlášení o zjištěných bezpečnostních incidentech, ale zároveň takové hlášení není ze zákona vyloučeno. Možnost podávat hlášení o bezpečnostních incidentech národními či vládnímu CERT pracovišti stanoví § 8 odst. 6 ZKB.[165] Na poskytovatele služeb podle ZEK se vztahuje povinnost uchovávat provozní a lokalizační údaje po dobu 6 měsíců podle ustanovení § 97 odst. 3 ZEK.[166] Provozními a lokalizačními údaji jsou myšleny také IP adresy, které jsou běžně součástí hlášení národnímu či vládnímu CERT pracovišti. Jelikož se jedná o orgány a osoby, které by měly postupovat podle jiného zákona než v prvním případě, je nutné k těmto údajům přistupovat z hlediska ZEK. V souvislosti s trestním řízením je možné tyto údaje vyžadovat na základě příkazu podle § 88a TŘ.[167]

---

[163] Viz. § 3 a § 8 zákona č. 181/2014 Sb., *o kybernetické bezpečnosti* v posledním znění
[164] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 226. ISBN 978-80-210-8073-7.
[165] Viz. § 8 odst. 6 zákona č. 181/2014 Sb., *o kybernetické bezpečnosti* v posledním znění
[166] Viz. § 97 odst. 3 zákona č. 127/2005 Sb., *o elektronických komunikacích* v posledním znění
[167] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 226. ISBN 978-80-210-8073-7.

- **Zajištění dat od pracovišť, která nejsou součástí subjektu, jemuž § 3 ZKB ukládá povinnosti v souvislosti s kybernetickou bezpečností a zároveň subjekt není podnikatelem v oblasti poskytování služeb podle ZEK**

Těmto soukromým bezpečnostním pracovištím nejsou ukládány povinnosti ani z jednoho z uvedených zákonů. V souvislosti s trestním řízením je tedy možné od nich získávat informace či údaje na základě obecné žádosti podle § 8 odst. 1 TŘ, čímž ovšem není vyloučena případná nepoužitelnost pro dokazování takovými daty v trestním řízení. Těmito daty mohou být IP adresy, které se v jiných případech považují za provozní a lokalizační údaje. Je logické, že se dotčené společnosti zajímají o bezpečnost svých údajů, sítě či infrastruktury, nicméně sledování a uchovávaní takových údajů nesmí být nepřiměřené a v rozporu se zákonem.[168]

8.3 Provádění a hodnocení důkazu z dat z dohledových systémů kybernetické bezpečnosti

Bezpečnostní pracoviště provádějí monitoring svěřených sítí a infrastruktur za pomocí vhodné kombinace hardwarových a softwarových zařízení, kterými mohou být nástroje kategorie SIEM (Security Information and Event Management), které mají za úkol automaticky monitorovat, zaznamenávat a analyzovat případné bezpečnostní události a incidenty či jiná bezpečnostní nebezpečí v reálném čase. Tím poskytují možnost včasné reakce na tyto hrozby, které jsou tato zařízení schopná detekovat a částečně či úplně eliminovat. Umožňují také zmírnit dopady bezpečnostní události či incidentu, z jejichž zaznamenávání vznikají reporty o události či incidentu.[169] Jako příklad softwarových služeb typu SIEM lze uvést nástroje SolarWinds, Datadog, Splunk, McAfee ESM, Alienvault USM, Logrythm

---

[168] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 226-227. ISBN 978-80-210-8073-7.

[169] KŘÍŽ, Lukáš. SIEM: Náročná cesta k pokročilému zajištění kybernetické bezpečnosti. *Hospodářské noviny* [online]. 20.6.2019 [cit. 17.11.2022]. Dostupné z: https://ictrevue.hn.cz/c3-66593380-0ICT00_d-66593380-siem-narocna-cesta-k-pokrocilemu-zajisteni-kyberneticke-bezpecnosti

nebo ArcSight.[170] Jak bylo uvedeno výše, nelze se v této oblasti spoléhat na ohledání nebo vydání věci důležité pro trestní řízení a dokazovaní tak probíhá na základě zajištěných dat, které poskytují dotčené společnosti pracovištím CERT a následně policejnímu orgánu. Tato data by měla být součástí reportu o bezpečnostním incidentu v takové formě, aby nevznikly pochybnosti o tom, že se jedná o původní data, která dále nebyla nijak pozměňována, čímž je myšleno vytvoření bitové kopie těchto dat a opatření algoritmickou funkcí tzv. „hash kódem“ (viz. **kapitola 2.3 Nakládání s elektronickými důkazy**). V procesu dokazování a hodnocení důkazu se nelze spoléhat pouze na informace získané z takových reportů. I kdyby se podařilo ustanovit IP adresu zařízení, které bylo příčinou incidentu, neprokazuje to úmysl v jednání uživatele a je nezbytné provádět další procesní úkony za účelem obstarání dalších důkazů o tom, že zařízení užívala konkrétní osoba. Dále je nutné zjistit způsob a důvod jeho používání, tak jako v případě dokazování e-mailem nebo při dokazování provozními a lokalizačními údaji.[171]

8.4 Shrnutí poznatků

Páchání trestné činnosti v kyberprostoru nahrává současný trend, který byl mimo jiné poznamenán celosvětovou pandemií Covid-19, v rámci které bylo mnoho firem a institucí nuceno přejít na systém home office, při kterém značná část zaměstnanců pracovala z pohodlí domova. To s sebou jistojistě přineslo mnoho výhod nejen pro zaměstnance, ale také pro zaměstnavatele, kteří by v této době nebyli schopni jiným způsobem zajišťovat svou činnost. Zároveň tento způsob pomohl rychlejšímu zvládnutí pandemie, která by při běžném setkávání osob v zaměstnání mohla trvat delší dobu a způsobila by tak větší ekonomické potíže v celosvětovém měřítku. Z toho důvodu se tyto instituce zaměřily na častější využívání online funkcí a sdílených úložišť, což s sebou nese také určitá rizika. Zaměstnanci si byli „nuceni brát práci domů“, čímž se instituce vystavily vyššímu

---

[170] *Top 11 Nejlepší SIEM Nástrojů v roce 2021 Pro Real-Time Reakce na incidenty a Bezpečnostní*. Constant reader [online]. 11.11.2020 [cit. 17.11.2022]. Dostupné z: https://theconstantreader.com/cs/top-11-nejlepsi-siem-nastroju-v-roce-2021-pro-real-time-reakce-na-incidenty-a-bezpecnostni/

[171] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 231-232. ISBN 978-80-210-8073-7.

riziku kybernetických útoků, jelikož musely umožnit přístup k důležitým údajům a informacím vzdáleným způsobem, kdy se k těmto datům zaměstnanci dostávali z pracovních, či soukromých zařízeních obvykle za použití své domácí sítě, nebo veřejné sítě. Takový způsob připojení nemusí být vždy dostatečně zabezpečen oproti kvalifikovaným bezpečnostním postupům a zabezpečením uvnitř instituce. Dalším problémem může být vědomé či nevědomé infikování zařízení přímo zaměstnancem (např. otevřením přílohy e-mailu, vložením flash disku a spuštění infikovaného souboru, atd.). Šíření takového škodlivého kódu vnitřní sítí může vést k vysokým škodám dotčené instituce. Autor je toho názoru, že po ukončení pandemie spojené s Covid-19 není nutné vracet všechny postupy do stavu, který této pandemii předcházel, ale naopak je žádoucí zaměřit se na inovace spojené se zabezpečením vzdálených přístupů a sdílením dat a informací. V problematice kybernetické bezpečnosti pravděpodobně nelze zajistit 100% bezpečnost a největší prevencí v oblasti kybernetické bezpečnosti se tak jeví pravidelné a kvalitní školení a osvěta nejen zaměstnanců, ale společnosti obecně. Velká část uživatelů informačních technologií stále podceňuje zabezpečení svých účtů a zařízení, kdy pro přístup ke svým účtům používá hesla typu „123456“ nebo „qwertz“, atd. Taková hesla uživatelé často používají jak ve svém osobním životě, tak v souvislosti s využíváním pracovních účtů, což může vést ke snadnějšímu prolomení hesla ze strany pachatele a následnému odcizení důležitých dat. Jako optimální postup se jeví využití složitějších a delších hesel, která jsou složená z různých písmen a číslic jako např. „3Nd45ReT91Ku“. K tomuto bodu lze uvést, že mnoho institucí si již závažnost síly přístupových údajů uvědomuje a nepovoluje založení účtů s jednoduchými hesly. Současně informační technologie používá také mnoho starších osob, které si neuvědomují, jakou zbraní v tomto ohledu může jejich zařízení či účet být. Je tedy nezbytné, aby se zákonodárci, OČTŘ a bezpečnostní kybernetická pracoviště snažila co nejvíce zamezit protiprávnímu jednání a případně minimalizovat způsobené škody, ale největší tíhu by měla na bedrech nést právě společnost běžných uživatelů, o jejichž bezpečnost jde v tomto případě především, a která je svým jednáním a rozhodováním schopná zabránit vzniku takových událostí a incidentů.

9 Analýza statistických dat vybraných trestných činů, u kterých se předpokládá dokazování elektronickými důkazy

Předpoklad před analýzou statistických dat je takový, že elektronická data využívaná v trestním řízení u obecné kriminality napomáhají k vyšší objasněnosti činů, odhalení a potrestání pachatelů. Zároveň se vývoj a použití technických nástrojů promítá v páchání podvodů a jiné trestné činnosti ve virtuálním prostředí, kde tyto prostředky poskytují vyšší míru anonymity a prostor k uniknutí spravedlnosti, neboť OČTŘ v současnosti zkrátka nedisponují tak kvalitními technickými prostředky, vědomostmi a právními normami, které by umožnily účinný boj s tímto druhem kriminality. Elektronické důkazy hrají v takovém případě klíčovou a nezastupitelnou roli, zejména v případech, kde jiné důkazy neexistují. Analýza vychází ze statistických údajů od 1. 1. 2016 do 31. 12. 2022 o registrovaném a objasněném stavu kriminality. Tato data pravidelně zveřejňuje Policie České republiky na svých webových stránkách www.policie.cz. Toto období bylo autorem zvoleno, neboť v roce 2016 došlo k zásadní změně evidování kriminality spojené s využíváním nových hardwarových i softwarových zařízeních a programů policie. Ze statistik Policie ČR nevyplývá, kolik trestných činů bylo způsobeno běžným způsobem a kolik v rámci virtuálního prostředí, tudíž se analýza dotýká všech registrovaných trestných činů nezávisle na způsobu spáchání, avšak autor se snažil vybrat takové oblasti kriminality, kde se přítomnost důkazů vycházejících z elektronických dat předpokládá, aby měla analýza určitou vypovídající hodnotu pro tuto práci.[172] Analýza statistických dat byla vytvořena pro následující oblasti trestné činnosti, přičemž zvláštní pozornost bude věnována podvodům:

- **Nebezpečné vyhrožování** (§ 353 TZ)
- **Nebezpečné pronásledování** (§ 354 TZ)
- **Vydírání** (§ 175 TZ)
- **Nedovolená výroba a jiné nakládání s omamnými a psychotropními látkami a s jedy** (§ 283 TZ)
- **Podvod** (§ 209 TZ)

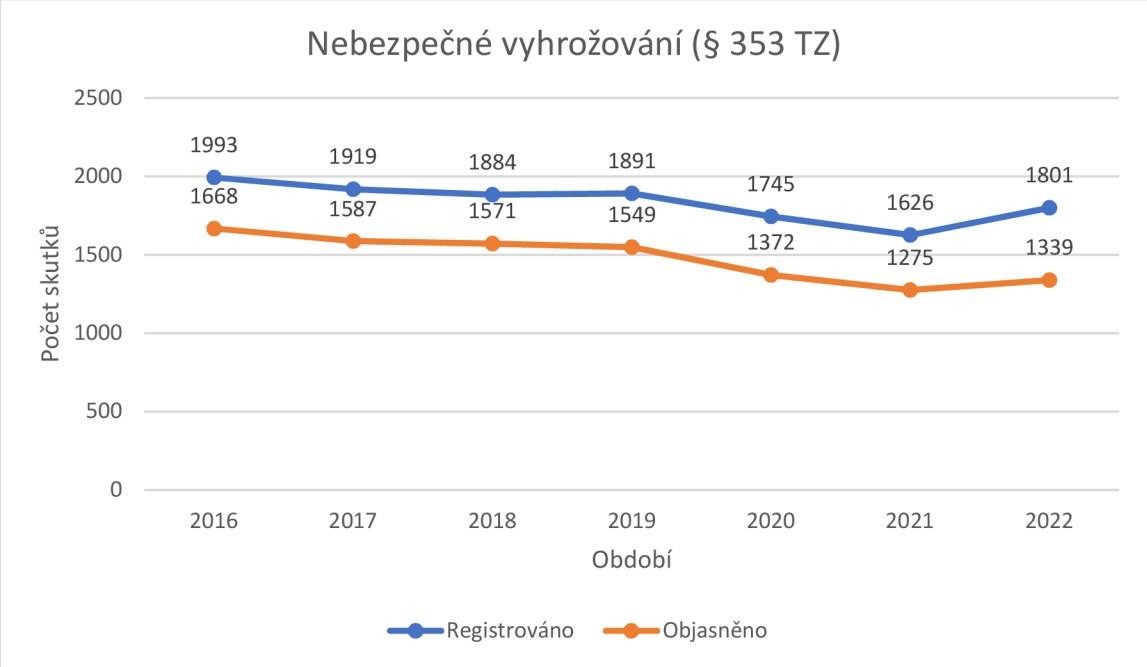
[172] *Statistické přehledy kriminality za rok 2022*. Policie České republiky [online]. © 2022 [cit. 30.12.2022]. Dostupné: https://www.policie.cz/clanek/statisticke-prehledy-kriminality-za-rok-2022.aspx

9.1 Nebezpečné vyhrožování (§ 353 TZ)

Základní skutková podstata:

„Kdo jinému vyhrožuje usmrcením, těžkou újmou na zdraví nebo jinou těžkou újmou takovým způsobem, že to může vzbudit důvodnou obavu, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti.“[173]

Analýza statistických dat:



Období	2016	2017	2018	2019	2020	2021	2022
Registrováno	1993	1919	1884	1891	1745	1626	1801
Objasněno	1668	1587	1571	1549	1372	1275	1339
Objasněnost	83,7%	82,7%	83,4%	81,9%	78,6%	78,4%	74,4%
Škoda v tisících Kč	2	21	45	0	0	0	0

Vyhrožování může mít povahu trestného činu pouze v případě, že vzbudí důvodnou obavu o způsobení výše uvedené újmy, většina takového jednání nesplňuje právě tuto podmínku a je vedeno jako přestupek proti občanskému soužití podle § 7 zákona č. 251/2016 Sb., o některých přestupcích.[174] Počet registrovaných skutků má v posledních letech více méně konstantní tendenci, přičemž se vymykají roky 2020 a 2021, kde se na nižším počtu registrovaných

[173] Viz. § 353 odst. 1 zákona č. 40/2009 Sb., *Trestní zákoník* v posledním znění
[174] Viz. § 7 zákona č. 251/2016 Sb., *o některých přestupcích* v posledním znění

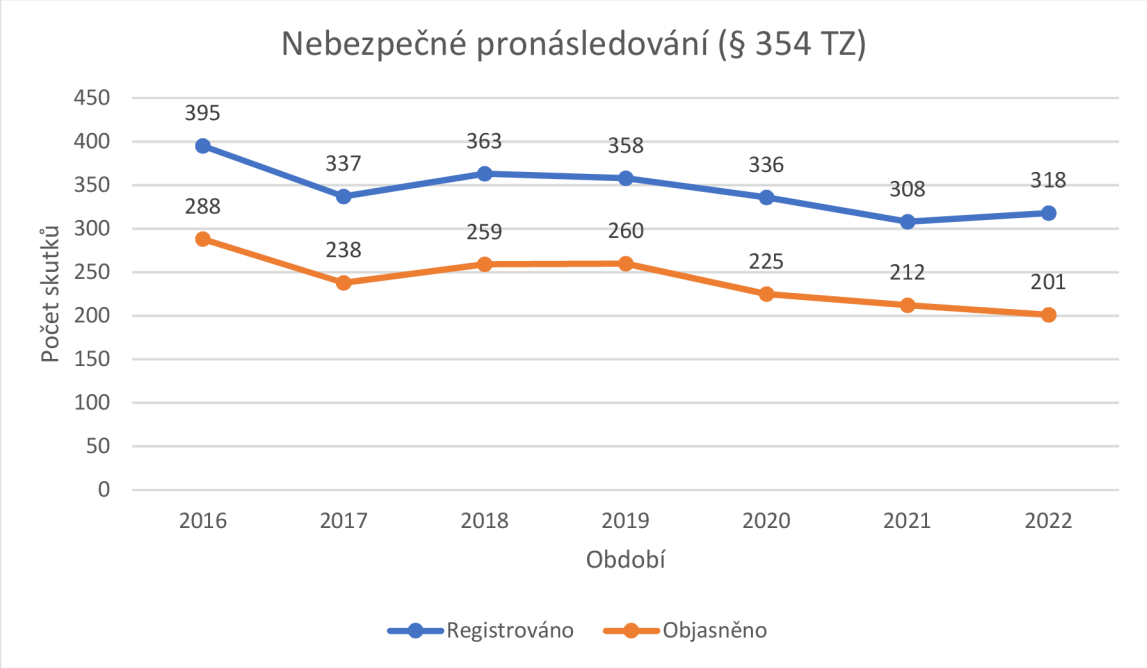
trestných činů mohla podílet opatření spojená s pandemií Covid-19, při které bylo omezeno setkávání osob. Míra objasněnosti se stále drží na vysoké úrovni. To je dáno mimo jiné tím, že se jedná o čin, při kterém je často mezi pachatelem a poškozeným vztah, což usnadňuje odhalení pachatele, neboť není nutné pátrat po neznámé osobě. Pachatelé mohou svým obětem vyhrožovat osobně, nebo za použití komunikačních zařízení. Vyhrožování za pomocí komunikačních zařízení umožňuje získání a použití elektronických dat, která jsou způsobilá prokázat dokazovanou skutečnost lépe než v případě chybějících důkazů při osobním vyhrožování, kterému nejsou přítomné další osoby v postavení svědků. Také v případě osobního vyhrožování přichází v úvahu využití provozních a lokalizačních údajů ve smyslu § 88a TŘ k prokázání skutečnosti, že se osoba nacházela na místě, kde mělo k vyhrožování docházet, popř. dalších elektronických důkazů.

9.2 Nebezpečné pronásledování (§ 354 TZ)

Základní skutková podstata:

„Kdo jiného dlouhodobě pronásleduje tím, že a) vyhrožuje ublížením na zdraví nebo jinou újmou jemu nebo jeho osobám blízkým, b) vyhledává jeho osobní blízkost nebo jej sleduje, c) vytrvale jej prostřednictvím prostředků elektronických komunikací, písemně nebo jinak kontaktuje, d) omezuje jej v jeho obvyklém způsobu života, nebo e) zneužije jeho osobních údajů za účelem získání osobního nebo jiného kontaktu, a toto jednání je způsobilé vzbudit v něm důvodnou obavu o jeho život nebo zdraví nebo o život a zdraví osob jemu blízkých, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti.“[175]

Analýza statistických dat:



Období	2016	2017	2018	2019	2020	2021	2022
Registrováno	395	337	363	358	336	308	318
Objasněno	288	238	259	260	225	212	201
Objasněnost	72,9%	70,6%	71,4%	72,6%	67,0%	68,8%	63,2%
Škoda v tisících Kč	0	0	0	0	0	0	0

Nebezpečné pronásledování bývá označováno za stalking, který znesnadňuje a znepříjemňuje život oběti. Oběť stalkingu je v důsledku chování pachatele často

[175] Viz. § 354 odst. 1 zákona č. 40/2009 Sb., *Trestní zákoník* v posledním znění

nucena doslova měnit své životní návyky a reálně se pouze snaží vyhnout pachateli, čímž jsou zásadně dotčena její základní práva. Podstatné je, že aby toto jednání naplňovalo skutkovou podstatu trestného činu, musí být způsobilé vzbudit obavu oběti o svůj život, zdraví nebo o život a zdraví osob blízkých takové oběti.[176] Převážná část takového jednání zůstává jako v případě vyhrožování kvalifikována jako přestupek proti občanskému soužití.[177] Zároveň může být nebezpečné pronásledování prováděno nejrůznějšími způsoby, kde není nutný pouze osobní kontakt a vyhledávání oběti, ale také kontaktování elektronickými prostředky. Při vyhodnocování, zda se jedná o trestný čin nebo přestupek, je důležité stanovit četnost a dlouhodobost takového jednání, ke kterému judikáty uvádí, že četnost musí dosahovat alespoň 10 pokusů o kontaktování oběti a za dlouhodobost je považována doba nejméně 4 týdnů.[178] Statistiky neuvádí příliš vysoké počty registrovaných skutků, ale objasněnost tohoto druhu kriminality je také na vysoké, i když klesající úrovni. Vyšší míra objasněnosti je stejně jako v předchozím případě zapříčiněna častým předchozím vztahem mezi pachatelem a obětí. Elektronická data vznikající při pokusech kontaktování oběti, jsou v trestním řízení hojně využívána v podobě důkazů. Tím mohou být dotčeny prakticky všechny způsoby dokazování uvedené v této práci, pomineme-li dokazování daty z elektronických dohledových pracovišť, které je charakteristickým postupem spíše pro jiné druhy trestné činnosti.

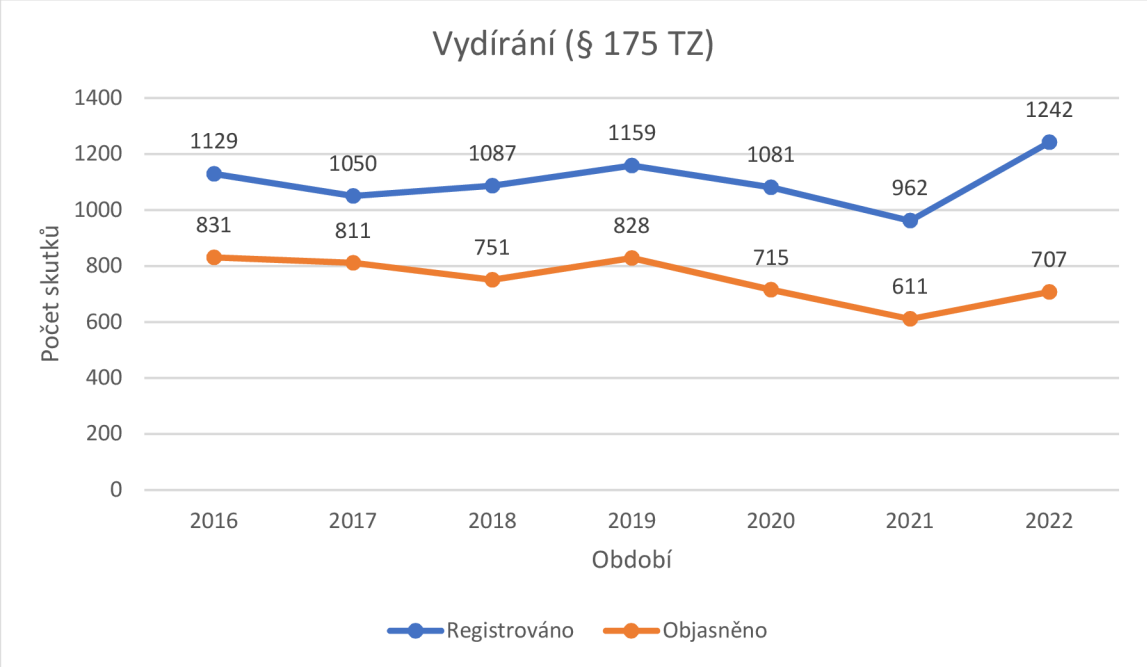
[176] Viz. § 354 odst. 1 zákona č. 40/2009 Sb., *Trestní zákoník* v posledním znění
[177] Viz. § 7 zákona č. 251/2016 Sb., *o některých přestupcích* v posledním znění
[178] JAKOUBKOVÁ, Barbora. Nebezpečné pronásledování (stalking). *Advokátní kancelář Grinacová* [online]. 10.8.2020 [cit. 31.12.2022]. Dostupné z: https://www.akgr.cz/nebezpecne-pronasledovani

9.3 Vydírání (§ 175 TZ)

Základní skutková podstata:

„Kdo jiného násilím, pohrůžkou násilí nebo pohrůžkou jiné těžké újmy nutí, aby něco konal, opominul nebo trpěl, bude potrestán odnětím svobody na šest měsíců až čtyři léta nebo peněžitým trestem.“[179]

Analýza statistických dat:



Období	2016	2017	2018	2019	2020	2021	2022
Registrováno	1129	1050	1087	1159	1081	962	1242
Objasněno	831	811	751	828	715	611	707
Objasněnost	73,6%	77,7%	69,1	71,4	66,1%	63,5%	56,9%
Škoda v tisících Kč	12 382	48 248	67 493	23 356	9 157	24 753	115 883

Počty registrovaných skutků vydírání mají proměnlivou tendenci, což může být v posledních letech zapříčiněno světovou epidemií Covid-19, která částečně znemožnila osobní setkávání osob. Velká část obchodních jednání se přesunula do virtuálního světa a stejně tak i pachatelé čím dál častěji vyhledávají jiný a bezpečnější způsob páchání trestné činnosti. K vydírání mnohdy dochází mezi osobami, které se znají, ale běžný je také způsob vydírání oběti neznámým pachatelem, který má o oběti určité informace. K vydírání může docházet z mnoha

[179] Viz. § 175 odst. 1 zákona č. 40/2009 Sb., *Trestní zákoník* v posledním znění

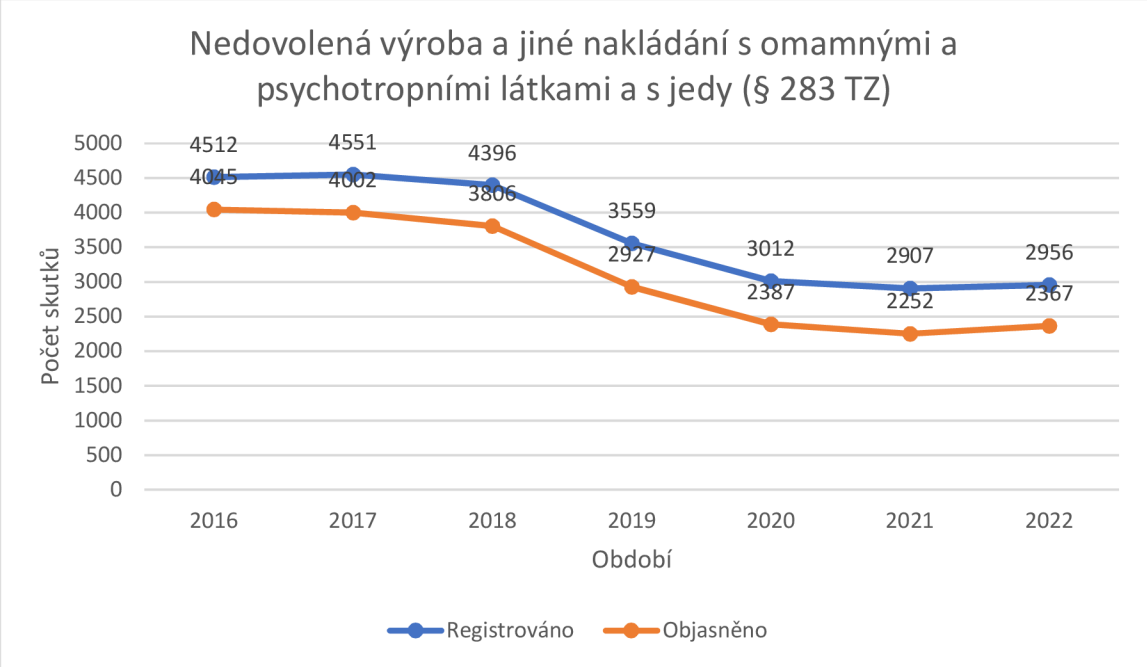
důvodů, jako jsou mezilidské vztahy, snaha získávání určité výhody plynoucí z postavení poškozeného, ale také ze zištných důvodů za účelem získání peněz nebo nemovitých či movitých věcí. Výše způsobené škody závisí na konkrétních případech a je logické, že škoda není meziročně konzistentní. V souvislosti s používáním moderních technologií, lze zaznamenat některé změny ve způsobu páchání této trestné činnosti. Pachatelé využívají e-mailových zpráv, SMS zpráv, telekomunikačních hovorů a komunikací v nejrůznějších chatovacích aplikacích, za účelem působení na poškozeného, čímž mohou nevědomě usnadnit práci OČTŘ, neboť za sebou často zanechávají spoustu elektronických dat využitelných pro trestní řízení a lze v tomto smyslu využít většinu způsobů dokazování, o kterých pojednává tato práce.

9.4 Nedovolená výroba a jiné nakládání s omamnými a psychotropními látkami a s jedy (§ 283 TZ)

Základní skutková podstata:

„Kdo neoprávněně vyrobí, doveze, vyveze, proveze, nabídne, zprostředkuje, prodá nebo jinak jinému opatří nebo pro jiného přechovává omamnou nebo psychotropní látku, přípravek obsahující omamnou nebo psychotropní látku, prekursor nebo jed, bude potrestán odnětím svobody na jeden rok až pět let nebo peněžitým trestem.“[180]

Analýza statistických dat:



Období	2016	2017	2018	2019	2020	2021	2022
Registrováno	4512	4551	4396	3559	3012	2907	2956
Objasněno	4045	4002	3806	2927	2387	2252	2367
Objasněnost	89,7%	87,9%	86,6%	82,2%	79,3%	77,5%	80,1%
Škoda v tisících Kč	0	0	0	0	0	0	0

Celkový počet registrovaných skutků v posledních letech klesá, což není zapříčiněno nutně pouze tím, že by nedocházelo k výrobě a následnému prodeji omamných a psychotropních látek, ale mění se způsob, kterým jsou tyto látky vyráběny a prodávány a také prostředí, ve kterém k tomu dochází. V důsledku

[180] Viz. § 283 odst. 1 zákona č. 40/2009 Sb., *Trestní zákoník* v posledním znění

těchto změn zůstává mnoho činů latentních. Některé způsoby pěstování a držení drog v malém množství jsou posuzovány jako přestupky podle zákona č.167/1998 Sb. o návykových látkách.[181] Část takového jednání je Policií ČR prošetřována, aniž by byly zahájeny úkony v trestním řízení, nebo je rozpracována. Rozpracováním je myšlen postup při získávání poznatků o trestné činnosti a pachatelích, na základě kterých je možné zahájit úkony v trestním řízení, potažmo trestní stíhání. Rozpracování takových případů může trvat řadově i několik měsíců, než dojde k trestnímu stíhání určité osoby. Touto trestnou činností zpravidla nebývá primárně způsobena škoda, ale důsledky jsou vážnější, neboť drogová závislost se dotýká spousty obyvatel a rodinných příslušníků závislých osob, jímž v souvislosti se sekundární drogovou kriminalitou, vznikají škody na majetku a také na rodinných vztazích. Drogová závislost způsobuje značné výdaje daňových poplatníků, z jejichž daní jsou pro závislé také placeny programy a kontaktní centra. Klesající tendenci registrovaných činů je také možné přičíst způsobu páchání této trestné činnosti, jelikož osoby vyrábějící a prodávající omamné látky přechází na složitější způsoby komunikace, při které častěji mění předplacené SIM karty, nebo využívají šifrované chatovací služby a aplikace, které umožňují vyšší míru anonymity před OČTŘ. Tyto aplikace také mohou umožňovat data o proběhnuvší komunikaci ihned odstranit, čímž znesnadňují rozpracování a trestní řízení jednotlivých případů, zejména při využití oprávnění odposlechu a záznamu telekomunikačního provozu podle § 88 TŘ.

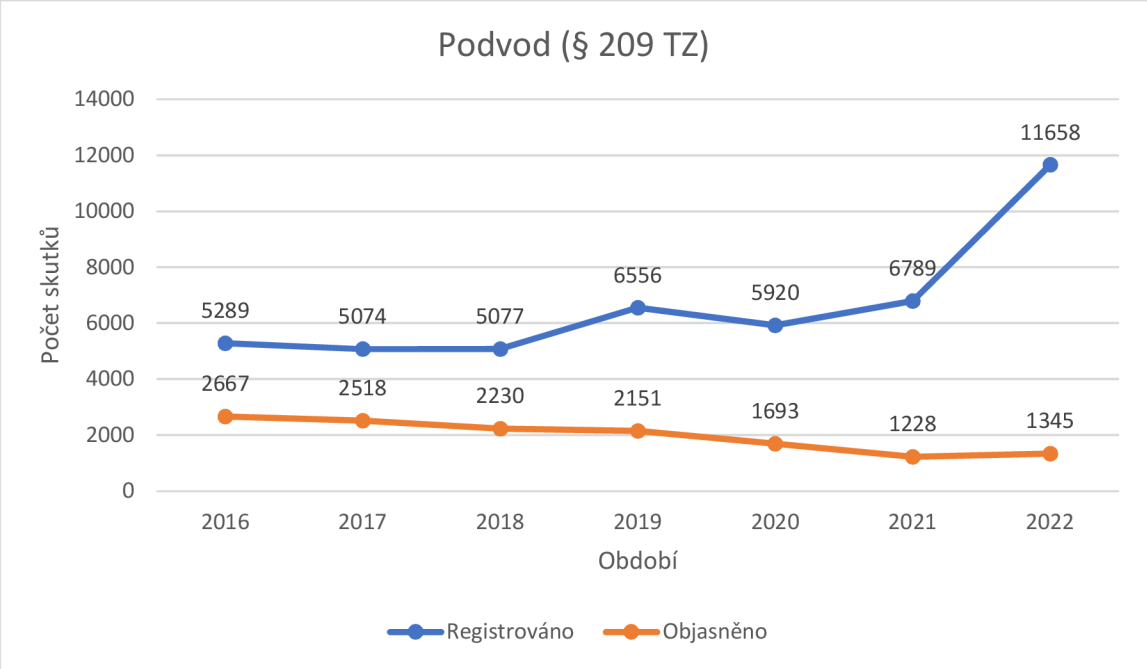
[181] Viz. § 39 odst. 1 až 4 zákona č. 167/1998 Sb., *o návykových látkách* v posledním znění

9.5 Podvod (§ 209 TZ)

Základní skutková podstata:

„Kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.“[182]

Analýza statistických dat:



Období	2016	2017	2018	2019	2020	2021	2022
Registrováno	5289	5074	5077	6556	5920	6789	11658
Objasněno	2667	2518	2230	2151	1693	1228	1345
Objasněnost	50,4%	49.6%	43,9%	32,8%	28,6%	18,1%	11,5%
Škoda v tisících Kč	951 771	939 896	1 575 965	1 664 887	1 690 240	2 143 577	3 516 346

Všeobecný tlak na společnost, který je zaměřen na oblast komunikace a výměnu informací v digitální podobě, má za důsledek, že výpočetní techniku používají také osoby, které neznají základní funkce takových zařízení či jejich technického řešení a při používání takových zařízení, si mnohdy počínají naivně a neopatrně. Digitalizace se stejně jako ostatních oborů dotýká bankovních služeb, kde nabízí možnost přesunů vysokých finančních částek, sjednávání půjček a spravování

[182] Viz. § 209 odst. 1 zákona č. 40/2009 Sb., *Trestní zákoník* v posledním znění

jiných žádostí pouze za použití mobilního telefonu. Během několika minut lze tímto způsobem převádět mezi účty v různých státech milionové částky, což je na jednu stranu významné pozitivum v obchodním styku, ale na druhou stranu tyto možnosti představují značné riziko právě u osob, které si s moderními technologiemi příliš nerozumí. Toho v posledních několika letech využívají pachatelé a zločinecké organizace, které se zaměřují na majetkovou trestnou činnost. Pachatelé těchto podvodů bývají technicky tak zdatní, že dokážou napodobit technická řešení, která jsou na první pohled nerozeznatelná od původních. Příkladem může být použití falešné webové stránky nebo platební brány, která se od originálu odlišuje pouze zdrojovým kódem. Pachatelé také často disponují komunikativními dovednostmi a využívají naivity poškozených, ze kterých pod propracovanou falešnou legendou získávají přístupové údaje k jejich účtům, ze kterých okamžitě vyčerpají všechny možné finanční prostředky, které následně převádí na neznámé účty do zahraničí. V horším případě pachatelé ještě stihnou sjednat jménem poškozeného půjčku a odčerpají i tyto prostředky. Jiným postupem pachatelé mohou poškozeného přimět k tomu, aby finanční obnos z jeho účtu sám vybral a vložil do Bitcoinmatu za účelem výhodného investování. Se záminkou výhodné investice mohou také poškozené přesvědčit o instalaci investičního programu do jejich počítačů. Tento program pouze umožňuje vzdálené ovládání zařízení. Následně pomocí takového programu obdobným způsobem odčerpají finance z účtu. Většina těchto činů je páchána za přímé účasti poškozené osoby, která nevěnuje dostatečnou pozornost varovným signálům a pachatelům dobrovolně poskytuje své přístupové údaje do internetového bankovnictví, nebo údaje o platební kartě. Poškození také v rámci spolupráce v dobré víře pachatelům umožňují na dálku ovládat svá zařízení, přičemž vlastně v přímém přenosu pouze sledují, jak jim z účtu mizí úspory. Jak dokazují statistická data, registrovaných činů skokově přibývá a objasněnost je nejhorší za sledované období. Ve statistice kriminality Policie ČR není uvedeno, jaká část z celkového počtu registrovaných podvodů, je páchána za použití výpočetní techniky. Výše způsobených škod se každoročně zvyšuje a představuje tak opravdu velký problém pro běžnou společnost, která je tímto jednáním nejvíce dotčena. Trestní řád umožňuje zajištění nástrojů trestné činnosti a výnosů z trestné činnosti podle § 79a TŘ. Toto ustanovení dává policejnímu orgánu

možnost vydat usnesení o zajištění peněžních prostředků na účtu vedeného v ČR, které musí být bance doručeno spolu s dalšími dokumenty a banka následně může zastavit odčerpání finančních prostředků.[183] Bohužel v mnoha případech dochází k pozdnímu oznámení těchto podvodů, což je jedním z důvodů, proč se nedaří zajistit peníze poškozených, které takto následně míří na neznámé zahraniční bankovní účty. Autor se domnívá, že snížení počtu těchto činů by mohla pomoci výraznější informovanost veřejnosti, cílená na prevenci při používání internetového bankovnictví a plateb kartou online. Především je vhodné dbát zvýšené opatrnosti a používání selského rozumu při jednání spojených s bankovními transakcemi ve virtuálním prostředí.

[183] Viz. § 79a zákona č. 141/1961 Sb., *Trestní řád* v posledním znění

10 Závěr

Diplomová práce se zaměřila na vybrané elektronické důkazy a na jejich využitelnost v trestním řízení. Ze strany autora byl dán důraz především na způsoby zajištění elektronických dat a jejich hodnocení v souvislosti s identifikací osoby, která tato data vytvořila. Diplomová práce představuje zjednodušený náhled do této obsáhlé problematiky, ze kterého by mohly čerpat především kolegové z řad Policie České republiky, kterým by práce mohla přiblížit, jakým způsobem lze nakládat s elektronickými daty v souvislosti s trestním řízení. Elektronická data nás obklopují při každodenní činnosti. Způsob zajišťování a další nakládání s takovými daty je závislý na konkrétním charakteru dat a na úrovni zabezpečení, která jim je ze zákona přisuzována. Aby byla data využitelná pro účely trestního řízení, je nutné je zajišťovat a nakládat s nimi především v souladu se zákonem č. 141/1961 Sb., trestní řád a s dalšími zákony, které se k těmto datům vážou. Mnoho právních norem nepředpokládalo tak rychlý vývoj elektronických a informačních technologií a možnosti zajišťování elektronických dat tak v tomto důsledku mohou působit nejasně a krkolomně, což dokazuje fakt, že v některých případech se odborná veřejnost liší s názory na podmínky a povinnosti při nakládání s takovými daty. Autor je toho názoru, že ze strany Policie ČR stále není dán dostatečný důraz ve smyslu proškolení příslušníků Policie ČR k tomu, jak s elektronickými daty nakládat, čímž je vytvářen prostor pro pochybení, která mohou vést ke ztrátě podstatných důkazů. Při analýze statistických dat byly vybrány oblasti obecné kriminality, ve kterých je předpokládána využitelnost některých z uvedených způsobů dokazování. Ze zjištěných údajů vyplývá, že počet registrovaných trestných činů některých druhů obecné kriminality má kolísavou či klesající tendenci z mnoha důvodů, přičemž toto tvrzení neplatí o trestném činu podvodu (§ 209 TZ), při kterém se naplno projevují rizika spojená s digitalizací a přesunem oblastí lidské činnosti do virtuálního prostředí. Počet registrovaných podvodů a nízká objasněnost, se stává závažným celorepublikovým problémem, při kterém v součtu vznikají miliardové škody běžným občanům. Přitom se zdá, že pachatelé jsou stále napřed před orgány činnými v trestním řízení a prognóza v tomto směru není příliš optimistická. Z pohledu vývoje kriminality bude nesmírně zajímavé, jak se s tímto problémem zákonodárci, OČTŘ a společnost jako taková vypořádá. Otázkou zůstává, kterým

směrem se tento druh trestné činnosti bude dále vyvíjet, neboť pachatelé jsou velmi přizpůsobiví a virtuální prostředí jim nabízí opravdu mnoho možností. Konkrétně při páchání podvodů bývají elektronická zařízení obvyklým prostředkem k páchání trestné činnosti, při kterém je patrný markantní rozdíl ve znalostech tohoto oboru mezi pachatelem, poškozeným a OČTŘ. Elektronické důkazy by v tomto směru měly hrát klíčovou roli, neboť se často jedná o jediné důkazy, které lze v tomto směru zajistit. Jako další překážku, která souvisí s odhalováním a objasňováním trestných činů, lze v oblasti užívání moderních technologií zmínit přechod pachatelů od klasického telekomunikačního provozu na chatovací aplikace, které umožňují šifrování přenášených zpráv a hovorů. Tyto aplikace dále umožňují automatické mazání doručených zpráv, čímž prakticky znemožňují provádění odposlechů a získávání informací ze zajištěných zařízeních, ve kterých se taková komunikace předpokládá.

Doporučení a náměty *de le ferenda*

- **Povinnost uchovávat data podle § 7b trestního řádu**

Této problematice se věnuje práce v **kapitole 2.3 Nakládání s elektronickými důkazy.** Určité právní postupy v souvislosti se zajišťováním elektronických dat jsou minimálně nejasné a přináší do této složité problematiky více otázek, než odpovědí. Ustanovení § 7b TŘ hovoří o nakládání s daty, která jsou uložená v počítačovém systému nebo na nosiči informací a dále o povinnosti tato data na příkaz uchovat, či znepřístupnit jiné osobě po dobu 90 dnů. Pozitivní je, že se problematika spojená s elektronickými daty začleňuje do trestního řádu, nedostatkem ovšem je, že § 7b TŘ se blíže nezmiňuje o charakteru dat, mimo to, že se musí jednat o data důležitá pro trestní řízení, a že se mají nacházet v počítačovém systému nebo na nosiči informací. Teoreticky se tak může jednat o všechna elektronická data, která jsou takto uložena (metadata, komunikace, elektronické dokumenty, provozní a lokalizační údaje, atd.). Tak, jak se liší charakter takových dat, se liší také úroveň právní ochrany těchto dat. Tento postup má mít formu předběžného opatření příkazem. Ustanovení dále nerozlišuje, kterým osobám lze tento příkaz uložit, ani nekonkretizuje způsob uchování těchto dat. Zároveň neuvádí důsledek toho, že by osoba takového příkazu neuposlechla.

Ustanovení § 66 TŘ se zmiňuje o možnosti uložení pořádkové pokuty až do výše 50 000,- Kč tomu, kdo neuposlechne příkaz podle TŘ. Autor se domnívá, že TŘ by měl blíže specifikovat, na jaká konkrétní data se toto ustanovení může vztahovat a jakým způsobem by měla být tato data uchována, nebo znepřístupněna. Z taktického hlediska je jistě vhodnější volit přímo způsoby sloužící k zajištění a vydání takových dat, nebo celých nosičů. V případě, že by dotčená osoba byla do trestného činu zainteresována a policejní orgán by o tom nevěděl a vydal ji příkaz pouze k uchování dat důležitých pro trestní řízení, mohlo by dojít k úmyslnému zničení důležitých dat. V takovém případě se případná pokuta do 50 000,- Kč nejeví jako příliš vysokým postihem ve srovnání s důsledky odsouzení. Lze si tak představit, že pachatel raději smaže data a zaplatí pokutu do 50 000,- Kč, než aby čekal na to, jakým způsobem policejní orgán přikročí k zajištění důkazů.

- **Údaje o uskutečněném telekomunikačním provozu (§ 88a TŘ)**

Další oblastí zasluhující zmínku v doporučeních, jsou údaje o uskutečněném telekomunikačním provozu, které se zajišťují podle § 88a TŘ. Tato problematika je přiblížena v **kapitole 4 Dokazování provozními a lokalizačními údaji**. Autor je toho názoru, že současná právní úprava je dostatečná a s námitky odborné veřejnosti, že se jedná o zbytečný zásah do soukromí celé populace, která využívá telekomunikační služby, nesouhlasí. Skutečností sice je, že operátoři jsou povinni po dobu 6 měsíců uchovávat všechna data, z nichž je jen část využitelná pro trestní řízení, ale jejich vydání policejnímu orgánu musí být dostatečně odůvodněno a schváleno několika nezávislými orgány, přičemž možnost vyžádání takových údajů, se týká pouze vybraných trestných činů. Policisté se při objasňování závažné trestné činnosti často setkávají s mnohem osobnějšími informacemi o dotčených osobách, než poskytují tyto údaje. Autor se domnívá, že vzít nebo omezit tento nástroj z rukou OČTŘ, by vedlo ke zhoršení objasněnosti závažné trestné činnosti, při které hrají důležitou roli.

- **Prostorový odposlech a data z e-mailových schránek**

Prostorovému odposlechu se věnuje **kapitola 5.3 Prostorový odposlech**. O provádění odposlechu se zmiňuje trestní řád v ustanovení § 88, zatímco zmínka

o prostorovém odposlechu v trestním řádu chybí a policejní orgán je tímto nucen přizpůsobovat si jiná ustanovení, v důsledku čehož prostorový odposlech provádí podle § 158d odst. 2 a 3 TŘ. Doporučením vycházejícím z této práce je implementovat do trestního řádu ustanovení, které by se dotýkalo konkrétně prostorového odposlechu, kterým by byl objasněn samotný postup a podmínky, týkající se schvalování a provádění prostorového odposlechu. Dále by bylo vhodné, aby byla v trestním řádu uvedena zmínka o možnosti použitelnosti prostorového odposlechu prováděného v soukromí pro jiný trestný čin, než pro který je odposlech nařízen. V současné době se lze opřít o již uskutečněná rozhodnutí Nejvyššího Soudu, která uznávají zákonnost takto pořízených důkazů. Podobně by bylo vhodné sjednotit postup v souvislosti se zajišťováním dat z e-mailových schránek, čemuž se věnuje **kapitola 3 Dokazování e-mailem**. Jedná se o obtížnou proceduru, při které je v rámci trestního řízení postupováno podle několika paragrafových znění v závislosti na charakteru dat, jejich právní ochraně, nosiči, na kterém se data nachází a také na tom, zda se jedná o data již existující nebo budoucí. V tomto ohledu by nebylo od věci, kdyby úkony prováděné v prostředí e-mailových schránek, zaujímalo v rámci trestního řádu vlastní ustanovení, které by tuto problematiku podrobně zakotvilo.

- **Závěrečná doporučení**

Závěrečné doporučení se týká celkového způsobu zajišťování elektronických důkazů, kde by bylo vhodné základní články policie a SKPV na úrovni Územních odborů policie vybavit dostatečnými technickými prostředky, které by umožňovaly a usnadňovaly práci s elektronickými daty, neboť stav zařízení, na kterých mají být takové úkony činěny, je leckdy žalostný a softwarové vybavení je neodpovídající. Pro přehrání a zajištění souborů mnoha formátů elektronických dat, se musí volit složité způsoby, které obchází doporučená nastavení zařízení, přičemž prvotně se k zajišťování těchto dat dostanou právě policisté ze základních článků a SKPV Územních odborů policie. V budoucnu se jeví jako důležitá častější a aktuálnější osvěta policistů ke způsobům zajišťování elektronických dat. Tím lze docílit správného procesního i technického provedení takového zajištění, což by umožnilo zamezit případnému znehodnocení dat. Zvýšení vzdělanosti policistů v tomto ohledu, by také mohlo odstranit překážku nepoužitelnosti důkazů, kvůli

nedodržení zákonných postupů. Nad rámec policie, by mělo být prioritou pro celou společnost, zintenzivnit preventivní činnost, zaměřenou na seznamování veřejnosti s nejnovějšími trendy ve způsobech páchání majetkové trestné činnosti, ke které dochází prostřednictvím výpočetní techniky.

11 Seznam použitých zkratek

eIDAS - Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu

NÚKIB - Národní úřad pro kybernetickou a informační bezpečnost

OČTŘ – Orgán činný v trestním řízení

OKTE – Odbor kriminalistické techniky a expertiz

SKPV – Služba kriminální policie a vyšetřování

TČ – trestný čin

TŘ – zákon č. 141/1961 Sb., Trestní řád

TZ – zákon č. 4/2009 Sb., Trestní zákoník

ÚZČ SKPV – Útvar zvláštních činností služby kriminální policie a vyšetřování

ZEK – zákon č. 127/2005 Sb., o elektronických komunikacích

ZKB – zákon č. 181/2014 Sb., o kybernetické bezpečnosti

12 Použitá literatura

- MICHÁLEK, Luděk a kol. *Kriminální zpravodajství jako nástroj kontroly trestné činnosti a zajišťování vnitřní bezpečnosti.* 1. vyd. Praha: Policejní akademie České republiky v Praze, 2020. ISBN 978-80-7251-506-6.
- Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 *o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu* v posledním znění
- NOVOTNÝ, František a kol. *Trestní právo procesní*. 2. vyd. Plzeň: Aleš Čeněk, 2017. ISBN 978-80-7380-677-4.
- POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015. ISBN 978-80-210-8073-7.
- Stanovisko OBP Ministerstva vnitra ČR, *k aplikaci ustanovení § 7b trestního řádu* ve znění k 21. 8. 2019
- Usnesení Nejvyššího soudu ČR ze dne 1. 9. 2020, sp. zn. 7 Tdo 865/2020
- Usnesení Nejvyššího soudu ČR ze dne 25. 8. 2020, sp. zn. 8 Tdo 647/2020
- VÁGNER, Michal. *Management na místě činu kybernetického bezpečnostního incidentu*. Praha, 2021. Disertační práce. Institut forenzních, bezpečnostních studií a managementu.
- Vyhláška č. 336/2005 Sb., *o formě a rozsahu informací poskytovaných z databáze účastníků veřejně dostupné telefonní služby a o technických a provozních podmínkách a bodech pro připojení koncového telekomunikačního zařízení pro odposlech a záznam zpráv* v posledním znění
- Vyhláška č. 357/2012 Sb., *o uchovávání, předávání a likvidaci provozních a lokalizačních údajů* v posledním znění
- Výkladové stanovisko NSZ č. 1/2015 Sb., *ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů včetně obsahu e-mailových schránek*

- Zákon č. 127/2005 Sb., *o elektronických komunikacích* v posledním znění
- Zákon č. 141/1961 Sb., *Trestní řád* v posledním znění
- Zákon č. 167/1998 Sb., *o návykových látkách* v posledním znění
- Zákon č. 181/2014 Sb., *o kybernetické bezpečnosti* v posledním znění
- Zákon č. 251/2016 Sb., *o některých přestupcích* v posledním znění
- Zákon č. 273/2008 Sb., *o Policii České republiky* v posledním znění
- Zákon č. 297/2016 Sb., *o službách vytvářejících důvěru pro elektronické transakce* v posledním znění
- Zákon č. 300/2008 Sb., *o elektronických úkonech a autorizované konverzi dokumentů* v posledním znění
- Zákon č. 365/2000 Sb., *o informačních systémech veřejné správy* v posledním znění
- Zákon č. 40/2009 Sb., *Trestní zákoník* v posledním znění
- Zákon č. 499/2004 Sb., *o archivnictví a spisové službě* v posledním znění
- Zákon č. 89/2012 Sb., *Občanský zákoník* v posledním znění

Internetové zdroje:

- *Adobe Acrobat*. Adobe.com [online]. © 2022 [cit. 20.11.2022]. Dostupné z: https://www.adobe.com/cz/acrobat/online/convert-pdf.html
- *Co je Czech POINT?*. Czechpoint [online]. © 2022 [cit. 8.12.2022]. Dostupné z: https://www.czechpoint.cz/public/statistiky-a-informace/co-je-czech-point/
- *Co je DDoS útok a jaká je ochrana?.* Eset.com [online]. [cit.10.11.2022]. Dostupné z: https://www.eset.com/cz/ddos-utok/
- *Časová razítka*. Česká pošta [online]. © 2022 [cit. 22.11.2022]. Dostupné z: https://www.ceskaposta.cz/sluzby/certifikacni-autorita-postsignum/casova-razitka
- *Difference between Cache and Cookies*. Geeksforgeeks [online]. 5.7.2022 [cit. 9.10.2022]. Dostupné z: https://www.geeksforgeeks.org/difference-between-cache-and-cookies/

- DOBROZENSKÝ, Dominik. Phishing: definice phishingu, jak jej rozpoznat a jak na phishingový útok vyzrát. *Cnews.cz* [online]. 3.3.2022 [cit. 10.11.2022]. Dostupné z: https://www.cnews.cz/co-je-phishing-a-jak-se-branit
- *Elektronická pečeť dle eIDAS – jak a co vlastně pečetit?*. ProID [online]. [cit. 6.12.2022]. Dostupné z: https://proid.cz/elektronicka-pecet-dle-eidas-jak-a-co-vlastne-pecetit/
- *Hackeři radí, jak ukrýt svoji identitu v online prostředí*. Citadelo.com [online]. 29.3.2018 [cit. 26.10.2022]. Dostupné z: https://citadelo.com/cz/blog/hackeri-radi-jak-ukryt-svoji-identitu-v-online-prostredi/
- HANÁK, Jakub a Lukáš PRUŠKA. Elektronický podpis pohledem aktuální právní úpravy. *epravo.cz* [online]. 22.1.2020 [cit. 1.12.2022]. Dostupné z: https://www.epravo.cz/top/clanky/elektronicky-podpis-pohledem-aktualni-pravni-upravy-110560.html
- JAHUŇÁK, Petr. Šifry, kódy a hashovací funkce (1.část). *blog.hackerlab.cz* [online]. 16.1.2016 [cit. 19.10.2022]. Dostupné z: https://blog.hackerlab.cz/sifry-kody-a-hashovaci-funkce-1cast/
- *Jak číst hlavičku zprávy*. Seznam.cz [online]. [cit. 26.10.2022]. Dostupné z: https://napoveda.seznam.cz/cz/email/jak-cist-hlavicku-zpravy/
- JAKOUBKOVÁ, Barbora. Nebezpečné pronásledování (stalking). *Advokátní kancelář Grinacová* [online]. 10.8.2020 [cit. 31.12.2022]. Dostupné z: https://www.akgr.cz/nebezpecne-pronasledovani
- JELIČ, Pavel. Co je to end-to-end šifrování. *Letem světem applem* [online]. 23.2.2020 [cit. 27.10.2022]. Dostupné z: https://www.letemsvetemapplem.eu/2020/02/23/co-je-to-end-to-end-sifrovani/
- JELÍNEK, Jiří. K chybějící právní úpravě tzv. prostorového odposlechu v trestním řádu. *Bulletin-advokacie.cz* [online]. 22.9.2018 [cit. 25.1.2023]. Dostupné z: http://www.bulletin-advokacie.cz/k-chybejici-pravni-uprave-tzv.-prostoroveho-odposlechu-v-trestnim-radu

- KROPÁČOVÁ, Andrea. CERT/CSIRT týmy a jejich role. *Root.cz* [online]. 6.5.2013 [cit. 14.11.2022]. Dostupné z: https://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/
- KŘÍŽ, Lukáš. SIEM: Náročná cesta k pokročilému zajištění kybernetické bezpečnosti. *Hospodářské noviny* [online]. 20.6.2019 [cit. 17.11.2022]. Dostupné z: https://ictrevue.hn.cz/c3-66593380-0ICT00_d-66593380-siem-narocna-cesta-k-pokrocilemu-zajisteni-kyberneticke-bezpecnosti
- KUČERA, Roman. Používání různých podpisů. *Magazín Egovernment 1/2021* [online]. © 2022 [cit. 22.11.2022]. Dostupné z: https://www.egovernment.cz/inpage/podpisy-1-2021/
- *Kvalifikovaná časová razítka PostSignum*. Elektronický podpis.cz [online]. [cit. 5.12.2022]. Dostupné z: https://www.elektronickypodpis.cz/kvalifikovana-casova-razitka/
- *Malware*. Avast.com [online]. [cit. 10.11.2022]. Dostupné z: https://www.avast.com/cs-cz/c-malware
- *Nejčastější dotazy*. Datové schránky [online]. © 2022 [cit. 8.12.2022]. Dostupné z: https://info.mojedatovaschranka.cz/info/cs/1028.html
- *Obrazový dokument vizuální dokument, ikonický dokument*. Česká terminologická databáze knihovnictví a informační vědy [online]. © 2012 [cit. 20.11.2022]. Dostupné z: http://aleph.nkp.cz/publ/ktd/00000/09/000000912.htm
- PALYZA, Jiří. Chaty ve WhatsAppu se mažou automaticky: nová funkce by měla řešit velký problém. *chip.cz* [online]. 20.5.2021 [cit. 27.10.2022]. Dostupné z: https://www.chip.cz/novinky/chaty-ve-whatsappu-se-mazou-automaticky-nova-funkce-by-mela-resit-velky-problem/
- PERNICA, Tomáš. Jak funguje mail. *Tomp.eu* [online]. 20.3.2008 [cit. 20.10.2022]. Dostupné z: https://www.tomp.eu/2008/03/20/jak-funguje-email/
- *Phishing*. Avast.com [online]. [cit. 10.11.2022]. Dostupné z: https://www.avast.com/cs-cz/c-phishing

- PODANÝ, Jan. Podepisování soukromých listin včera, dnes a zítra. *Advokátní deník* [online]. 4.5.2020 [cit. 20.11.2022]. Dostupné z: https://advokatnidenik.cz/2020/05/04/podepisovani-soukromych-listin-vcera-dnes-a-zitra/
- POLANSKÝ, Petr. Co jsou metadata dokumentů?. *Exon* [online]. [cit. 9.10.2022]. Dostupné z: https://www.exon.cz/cs/blog/co-jsou-metadata-dokumentu
- *Poskytované služby*. Národní centrum kybernetické bezpečnosti [online]. [cit. 14.11.2022]. Dostupné z: https://www.govcert.cz/cs/vladni-cert/poskytovane-sluzby/
- *Práce s přílohami*. Seznam.cz [online]. [cit.19.10.2022]. Dostupné z: https://napoveda.seznam.cz/cz/prilozeni-prilohy/
- PŘÍKAZSKÁ, Lenka a Michal MOHELSKÝ. Současná právní úprava data retention je dle Ústavního soudu ústavně konformní a tedy přípustná. *epravo.cz* [online]. 16.10.2019 [cit. 9.10.2022]. Dostupné z: https://www.epravo.cz/top/clanky/soucasna-pravni-uprava-data-retention-je-dle-ustavniho-soudu-ustavne-konformni-a-tedy-pripustna-110069.html
- PŘÍKAZSKÁ, Lenka a Michal MOHELSKÝ. Současná právní úprava data retention je dle Ústavního soudu ústavně konformní a tedy přípustná. *epravo.cz* [online]. 16.10.2019 [cit. 28.10.2022]. Dostupné z: https://www.epravo.cz/top/clanky/soucasna-pravni-uprava-data-retention-je-dle-ustavniho-soudu-ustavne-konformni-a-tedy-pripustna-110069.html https://www.epravo.cz/top/clanky/soucasna-pravni-uprava-data-retention-je-dle-ustavniho-soudu-ustavne-konformni-a-tedy-pripustna-110069.html
- REHBERGER, Ivo. Obsahují webové logy bohatství?. *Lupa.cz* [online]. 30.1.2002 [cit. 9.10.2022]. Dostupné z: https://www.lupa.cz/clanky/obsahuji-webove-logy-bohatstvi/

- *Seznam kvalifikovaných poskytovatelů služeb vytvářejících důvěru a poskytovaných kvalifikovaných služeb vytvářejících důvěru*. Ministerstvo Vnitra České republiky [online]. 19.10.2022 [cit. 1.12.2022]. Dostupné z: https://www.mvcr.cz/clanek/seznam-kvalifikovanych-poskytovatelu-sluzeb-vytvarejicich-duveru-a-poskytovanych-kvalifikovanych-sluzeb-vytvarejicich-duveru.aspx
- SMEJKAL, Petr. Nejprodávanější mobily Apple, Samsung, Xiaomi, Honor, Vivo a Huawei. *Testado.cz* [online]. 29.8.2022 [cit. 9.11.2022]. Dostupné z: https://www.testado.cz/nejprodavanejsi-mobilni-telefony/?gclid=EAIaIQobChMIvrb3tbag-wIVFobVCh2xpwZsEAAYAyAAEgKQiPD_BwE
- *Spyware.* Avast.com [online]. [cit. 10.11.2022]. Dostupné z: https://www.avast.com/cs-cz/c-spyware
- *Statistické přehledy kriminality za rok 2022*. Policie České republiky [online]. © 2022 [cit. 30.12.2022]. Dostupné: https://www.policie.cz/clanek/statisticke-prehledy-kriminality-za-rok-2022.aspx
- STUPKA, Václav, Jan PROVAZNÍK a Jakub VOSTOUPAL. Elektronické důkazy jako výzva pro trestní proces. *Právník. Teoretický časopis pro otázky státu a práva* [online]. 2022, roč. 161, č. 4. s. 332-349. [cit. 25.1.2023]. ISSN0231-6625. Dostupné z: https://www.ilaw.cas.cz/upload/web/files/pravnik/issues/2022/4/3_Stupka-Provaznik-Vostoupal_332-349_4_2022.pdf
- *Top 11 Nejlepší SIEM Nástrojů v roce 2021 Pro Real-Time Reakce na incidenty a Bezpečnostní*. Constant reader [online]. 11.11.2020 [cit. 17.11.2022]. Dostupné z: https://theconstantreader.com/cs/top-11-nejlepsi-siem-nastroju-v-roce-2021-pro-real-time-reakce-na-incidenty-a-bezpecnostni/
- *Trestní kolegium Nejvyššího soudu ukončilo „spor o odposlechy" z jiné věci*. Advokatnidenik.cz [online]. 17.12.2022 [cit. 6.11.2022]. Dostupné z: https://advokatnidenik.cz/2020/12/17/trestni-kolegium-nejvyssiho-soudu-ukoncilo-spor-o-odposlechy-z-jine-veci/

- *Útvar zvláštních činností služby kriminální policie a vyšetřování*. Policie České republiky [online]. © 2022 [cit. 28.10.2022]. Dostupné z: https://www.policie.cz/clanek/utvar-zvlastnich-cinnosti-sluzby-kriminalni-policie-a-vysetrovani-716842.aspx