UNIVERZITA KARLOVA

Právnická fakulta

Daniela Ševčíková

Elektronický důkaz v trestním řízení

Diplomová práce

Vedoucí diplomové práce: JUDr. Martin Richter, Ph.D.

Katedra trestního práva

Datum vypracování práce (uzavření rukopisu): 16.5.2024

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

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 129 255 znaků včetně mezer.

Daniela Ševčíková

V Praze, dne 16.5.2024

Děkuji za odbornou pomoc, konzultace a vedení diplomové práce JUDr. Martinovi Richterovi, Ph.D.

Dále děkuji rodičům, sestrám a partnerovi za podporu, kterou mi poskytovali během psaní diplomové práce a během celého studia.

Obsah

Úvod

Dokazování je procesní postup, který tvoří klíčovou součást trestního řízení.[1] Podstatou dokazování je získávání podkladů pro objasnění relevantních skutečností tak, aby mohlo být ve věci spravedlivě rozhodnuto. Trestní řád to, co může být takovým podkladem, taxativně nevymezuje – platí, že jím může být „vše, co může přispět k objasnění věci“[2]. Orgány činné v trestním řízení tak musí při dokazování použít všechny vhodné a zákonem umožněné prostředky. Ač lze z trestního řádu dovodit některé druhy důkazních pramenů, důkazních prostředků i důkazů, které zákonodárce předpokládá nebo se kterými alespoň počítá, je možné konstatovat, že způsoby, kterými lze rozhodné skutečnosti dokázat, se neustále rozšiřují. Zásadní podíl na tomto rozšiřování má především vznik a rozvoj nových technologií, který v současnosti probíhá bezprecedentní rychlostí.

Nové technologie zasahují do všech oblastí lidské činnosti a není tak překvapivé, že ovlivňují i dokazování. Nové technologie mají v rámci dokazování vysoký potenciál – jak uvádím v práci níže, lze dokonce elektronické důkazy, získané za jejich pomoci, považovat za jakési „důkazy třetí generace“. Nové technologie však mají mnoho specifik a tradiční právní instituty, používané v souvislosti s dokazováním, nemusí odpovídat jejich zvláštní povaze. Hypotézou, ze které vycházím při psaní této práce tak budiž to, že trestní řád, tato specifika dostatečně nereflektuje a v praxi tak dochází k tomu, že jsou v souvislosti novými technologiemi používány tradiční instituty, jejichž správnost či vhodnost je přinejmenším diskutabilní. Cílem této diplomové práce je tak charakteristika elektronického důkazu, popis toho, jakým způsobem je s ním v rámci dokazování zacházeno a dále též právní analýza vybraných problematických aspektů související především se zajišťováním elektronických dat.

Účelem této práce naopak není rozbor toho, jak probíhá dokazování elektronickými důkazy po technické stránce (ač tuto problematiku velmi stručně zmiňuji), ani komplexní popis dokazování jako celku, ačkoliv pro kontext tématu elektronického důkazu v trestním řízení považuji zahrnutí některých obecných výkladů za nezbytné. S ohledem na rozsah práce ani neaspiruji na komplexní popsání problematiky elektronického důkazu vzhledem k tomu, že existuje nepřeberné množství druhů nosičů dat, elektronických zařízení a elektronických dat a aplikační problémy s nimi související se zdají být bezbřehými.

[1] Ač lze v poslední době vidět tendenci zákonodárce k tomu, aby bylo dokazování prováděno o něco méně (např. v institutu prohlášení viny podle §206c TrŘ nebo institutu nesporných skutečností §206d TrŘ) platí, že dokazování musí v rámci trestního řízení vždy, alespoň v nějaké formě, proběhnout.
[2] §89, odst. 2 TrŘ.

1 Dokazování, jeho vývoj a právní úprava

1.1 Pojem dokazování

Každé meritorní rozhodnutí v trestním řízení je činěno ohledně skutečností, které se staly v minulosti, zásadně tedy před tím, než vůbec došlo k zahájení úkonů trestního řízení.[3] Orgány činné v trestním řízení, kterými je podle §12, odst. 1 TrŘ soud, státní zástupce a policejní orgán[4], tak nebyly relevantním skutečnostem, kvůli nímž se trestní řízení vede přítomné, a samy je nevnímali, ale musí je pro účel vydání meritorního rozhodnutí co nejvěrněji poznat[5], což je činěno především prostřednictvím dokazování.[6] Dokazováním se tedy rozumí zákonem regulovaná činnost, kterou vykonávají zejména orgány činné v trestním řízení,[7] za účelem zjištění relevantního skutkového stavu tak, aby o jeho povaze nebyly důvodné pochybnosti.[8]

Dokazování se neomezuje pouze na to, zda byl spáchán trestný čin a kdo je jeho pachatelem, ale je třeba dokazovat další skutečnosti, jako třeba okolnosti důležité pro uložení trestu (např. osobní majetkové poměry pachatele) nebo procesní záležitosti (např. zda je důvod k tomu, aby svědek odmítl vypovídat).[9] V každém případě platí, že dokazování by mělo ve svém souhrnu vést ke kvalifikovanému rozhodnutí ve věci a k naplnění účelu trestního řízení, kterým je podle §1, odst. 1 TrŘ to, aby trestné činy byly náležitě zjištěny a jejich pachatelé byli podle zákona spravedlivě potrestáni. Považuji za důležité zdůraznit, že pro to, aby mohli být pachatelé spravedlivě potrestáni nestačí, aby trestní řízení skončilo spravedlivým výsledkem, ale je rovněž třeba, aby i postup, který k němu vedl, byl spravedlivý, tedy aby se při něm postupovalo v souladu se zásadami trestního řízení, byla chráněna základní lidská práva před nepřiměřenými zásahy a v neposlední řadě, aby byly dodržovány zákony.[10]

---

[3] Výjimkou může být situace kdy ten, proti němuž se řízení vede, spáchá další trestný čin. Pak může být i tento „další trestný čin“ projednán v rámci společného řízení podle §20 a násl. TrŘ – z čistě formalistického hlediska se tak bude v trestním řízení projednávat i trestný čin, k jehož spáchání došlo až po zahájení trestního řízení.

[4] K pojmu policejního orgánu viz §12, odst. 2 TrŘ.

[5] Nutnost „nejvěrnějšího poznání“ je částečně omezena např. u dohody o vině a trestu – rozhodnutí se opírá o přiznání obviněného za předpokladu, že to, k čemu se obviněný přiznal dostatečně prokazují výsledky vyšetřování. Viz §175a a násl. TrŘ.

[6] FENYK, Jaroslav a Jan PROVAZNÍK. Hlava XIII Obecné výklady o důkazech. In: *Trestní právo procení*. Praha: Wolters Kluwer ČR, 2019, s. 343.

[7] Dle §89, odst. 2 TrŘ se na určitých fázích dokazování (vyhledání, předložení a provedení důkazu) se mohou podílet i osoby odlišné od orgánů činných v trestním řízení, zejména procesní strany. Hodnocení důkazů ale vždy přísluší pouze orgánům činným v trestním řízení.

[8] §2, odst. 5 TrŘ.

[9] Srov. kapitola 2.3.

[10] *Nález ÚS ze dne 12. 10. 1994, sp. zn. Pl. ÚS 4/94*.

1.2 Stručný historický vývoj dokazování

Dokazování, jakožto právní institut, je neodmyslitelně spjato se soudním řízením a s procesním právem. Lze tedy konstatovat, že vývoj dokazování do jisté míry reflektuje historický vývoj samotného soudního řízení, ale i vývoj státu, společnosti a vývoj technologií. V období prvobytně pospolné společnosti neexistovala právní ochrana v moderním smyslu slova. Společnost se spoléhala na svépomoc, která představovala jediný způsob řešení bezpráví – dokazování v dnešním pojetí tak v té době nemělo opodstatnění. Od 11. století zastávala roli jakési rané soudní moci církev. Důkazní možnosti tehdejší doby byly značně limitované, a proto se soudci ve svých rozhodnutích často spoléhali na zjištění vycházející z víry v boží vůli, mnohdy o tzv. ordály[11].[12]

Ordálem se rozumí jakási zkouška, které se účastní strany řízení, při níž se předpokládá zásah nadpřirozených sil. Výsledek zkoušky je i výsledkem řízení. I když průběh ordálu někdy nahrazoval trestní řízení samotné a jeho výsledek byl často zároveň i trestem,[13] lze ordál pro jeho důkazní charakter, stejně jako později používanou torturu (tj. mučení při výslechu, jehož cílem je získat přiznání) řadit mezi tzv. iracionální důkazní prostředky, jejichž výsledkem jsou iracionální důkazy, tedy důkazy absurdní, nemající spolehlivý, kolikrát ani rozumný, základ. Ordály byly na našem území oficiálně zakázány ve 14. století, ale tortura byla oficiálně zakázána až v 18. století. Vedle iracionálních důkazů se paralelně rozvíjelo používání i tzv. racionálních (tj. rozumných) důkazů ze kterých se, v určité podobě vychází i dnes – šlo například o písemnosti, zemské desky (což jsou jacísi předchůdci zápisů v katastru nemovitostí), výsledek ohledání nebo výpověď soka (tedy svědka).[14]

Vzhledem k výše uvedenému lze konstatovat, že institut dokazování prošel značným vývojem. V minulosti bylo někdy potřebné spoléhat se na projevy boží vůle, na to, co sdělí domnělý pachatel při mučení nebo na jiné nedokonalé či nepřesné metody. I když tradiční důkazy, jako výpověď svědka, obsah listiny a výsledek ohledání dodnes hrají v procesu dokazování nezastupitelnou roli, dochází stále častěji k užívání jiných důkazů, a to zejména v reakci na vznik a vývoj nových technologií. Každá činnost prováděná za pomoci

[11] Na našem území zakotvovala použití ordálů např. Dekreta Břetislavova. Viz např. ADAMOVÁ, Karolina a Ladislav SOUKUP. *Prameny k dějinám práva v českých zemích*. Plzeň: Aleš Čeněk s.r.o., 2010, s. 21–22.
[12] VLČEK, Eduard. *Dějiny trestního práva v českých zemích a v Československu*. Brno: Masarykova univerzita Brno – Právnická fakulta, 2007, s. 3–18.
[13] POLČÁK, Radim. I. Důkaz a Informace. In: *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015, s. 22.
[14] VLČEK, Eduard. *Dějiny trestního práva v českých zemích a v Československu*, s. 18–27.

elektronických zařízení, které zpracovávají, předávají nebo uchovávají data, za sebou zanechává záznamy o své činnosti, tedy digitální stopy, které mohou posloužit jako důkazy v trestním řízení.[15] Orgány činné v trestním řízení tak v souvislosti s rozvojem technologií za prvé získávají nové a široké spektrum stop, které jim můžou usnadnit jejich činnost a za druhé získávají i nové nástroje k odhalování trestných činů. Dalo by se tak říci, že s rozvojem technologií přichází jakási „třetí generace důkazů"[16], tedy skupina důkazů, která je nová, má vysoký potenciál a může mít vysokou vypovídající hodnotu, ale s ohledem na její specifický charakter, přináší též nové výzvy.

1.3 Kyberkriminalita, „třetí generace důkazů" a Budapešťská úmluva

Stejně, jako se za pomoci nových technologií vyvinula jakási „třetí generace důkazů", vyvinul se za pomoci technologie i nový druh trestné činnosti, kterou lze označit jako kyberkriminalitu. Kyberkriminalitou se rozumí kriminalita, která je spáchána v kyberprostoru a pod níž spadá *„široká škála různých druhů trestné činnosti, jejichž primárním nástrojem nebo cílem jsou počítače a informační systémy"*[17]. Pod kyberkriminalitu tak spadají jak „nové trestné činy" (tedy trestné činy, které vzniky až v souvislosti s rozvojem technologií), tak nové způsoby páchání tradičních trestných činů. Například ten, kdo nelegálně provozuje online kasino, se dopouští přečinu neoprávněného provozování hazardní hry podle §252, odst. 1 TZ, který, ač je běžně „tradičním trestným činem", je v tomto případě možné považovat za trestný čin z oblasti kyberkriminality.[18]

Považuji za důležité zdůraznit, že ačkoliv je fakt, že při dokazování trestné činnosti z oblasti kyberkriminality budou „důkazy třetí generace" hojně používané, platí, že je nelze spojovat výlučně s tímto typem trestné činnosti. Třeba výpověď svědka, může být při vyšetřování kyberkriminality stejně důležitá jako „důkaz třetí generace". Analogicky pak lze dojít k závěru, že k dokazování trestných činů z jiných oblastí kriminality, než je ta kybernetická, budou používány „důkazy třetí generace" stejně jako kterékoliv jiné.

Ačkoliv nelze „důkazy třetí generace" spojovat pouze s kyberkriminalitou, myslím si, že právě kyberkriminalita je jedním hlavních hybatelů toho, proč tyto důkazy neustále nabírají na důležitosti. Také platí, že právní úprava „důkazů třetí generace" často vzniká

[15] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o, 2022, s. 825.
[16] První generací jsou myšleny důkazy iracionální, druhou generací důkazy racionální (oba pojmy vysvětleny v textu).
[17] *Společné sdělení Evropskému parlamentu, Radě, Evropskému hospodářskému výboru a sociálnímu výboru a Výboru regionů; Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor*. 2013. CELEX 52013JC0001.
[18] SMEJKAL, Vladimír. *Kybernetická kriminalita*, s. 31–34.

právě v souvislosti s právní úpravou kyberkriminality. Nejdůležitějším mezinárodním dokumentem upravujícím „důkazy třetí generace“ je Budapešťská úmluva, někdy též označována jako Úmluva o kyberkriminalitě, kterou Česká republika podepsala v roce 2005 a ratifikovala v roce 2013. Budapešťská úmluva je mezinárodní smlouva vypracovaná Radou Evropy, jejíž signatáři se z hmotněprávního hlediska zejména zavázali kriminalizovat některé druhy trestné činnosti a z procesněprávního zejména zavést procesní nástroje související s různými druhy dat.[19]

1.4 Úprava dokazování v českém vnitrostátním právu

V souvislosti s dokazováním je někdy používán termín „důkazní právo“, kterým se rozumí určitá výseč z trestního práva procesního, jež se skládá z jednotlivých právních norem, upravujících dokazování.[20] Co se týče českého vnitrostátního práva k roku 2024, je výchozí právní úprava dokazování v trestním řízení obsažena v páté části první hlavy trestního řádu, tedy zákona č. 141/1961 Sb. Úprava dokazování v této části není zcela vyčerpávající a lze ji najít jednak na jiných místech trestního řádu,[21] jednak v jiných zákonech, jako je třeba zákon č. 218/2003 Sb. (o soudnictví ve věcech mládeže). Obecný zákon trestního práva procesního, tedy trestní řád pocházející z šedesátých let minulého století, byl mnohokrát novelizovaný a s ohledem na jeho stáří není překvapivé, že se o jeho rekodifikaci diskutuje již několik (desítek) let. Ačkoliv existují návrhy jeho očekávaného nového znění,[22] je s praktickou jistotou možné říci, že je jeho přijetí do konce roku 2025 vyloučeno, a to zejména s ohledem na to, že se současnému složení Poslanecké sněmovny nedaří na jeho finální znění nalézt shoda. Rekodifikace trestního práva procesního tak bude pravděpodobně muset počkat minimálně do příštího volebního období.[23]

Při práci se stávající právní úpravou je tak třeba mít na paměti, že proces tvorby zákonů je složitý, každá jeho změna trvá určitý čas a zároveň to, že se momentálně nacházíme se v časovém období, ve kterém probíhá rozvoj technologií bezprecedentní rychlostí. Dynamičnost technologického pokroku v kombinaci se složitostí legislativních

[19] STUPKA, Václav. Kyberkriminalita. In: *Právo informačnich technologií*. Praha: Wolters Kluwer ČR, 2018, s. 548–550.
[20] FENYK, Jaroslav a Jan PROVAZNÍK. *Hlava XIII Obecné výklady o důkazech*, s. 345.
[21] Mimo pátou část první hlavy TrŘ nelze zejména opomenout úpravu zásad trestního řízení (včetně dokazování) v §2 TŘ. Speciální úprava dokazování se dále nachází v ustanoveních týkajících se jednotlivých stadií trestního řízení.
[22] Nejaktuálnější zveřejněný návrh ke dni 5.4.2024 je k 14. 10. 2022.
[23] Informace získána na základě dotazu zaslaného na Ministerstvo spravedlnosti ČR, Odbor legislativní, Oddělení trestně právní legislativy. DSarman@msp.justice.cz. 2024-04-05. Ministerstvo Spravedlnosti ČR – k dotazu na rekodifikaci trestního řádu. E-mail [osobní komunikace].

procesů, vede k tomu, že právo reaguje na technologie s určitým zpožděním. Celkově tak lze konstatovat, že ačkoliv se legální zakotvení dokazování, jak uvádím výše, v českém právním řádu nachází, v souvislosti s novými technologiemi trestní řád stále určité normy postrádá. Právní praxe tak si často musí poradit kreativním výkladem procesních institutů, které původně s existencí elektronických důkazů nepočítaly. Právní úprava používaná v souvislosti s „třetí generací důkazů", tak může být roztříštěná, neintuitivní a do jisté míry se může i zdát být neodpovídající, právě proto, že je potřeba skutečnost subsumovat pod právní institut, který s existencí elektronických dat původně nepočítal.[24] Ač legislativní nezakotvenost může být někdy úmyslem zákonodárce, myslím, že v tomto případě tomu tak není, a to zejména s ohledem na to, že lze očekávat, že detailnější právní úprava bude v této oblasti v budoucnu přijata.

Považuji za příhodné v této souvislosti zmínit, že trestní zákoník, který je obecným hmotněprávním trestním předpisem, na nové technologie reaguje o něco lépe. Větší aktuálnost trestního zákoníku lze přičítat zejména tomu, že k jeho rekodifikaci došlo poměrně nedávno,[25] a tak se při jeho tvorbě již počítalo jak se zněním Budapešťské úmluvy, tak s dalšími evropskými i mezinárodními závazky,[26] které bylo možné v jeho znění lépe reflektovat. V jeho zvláštní části lze nalézt několik „nových skutkových podstat trestných činů" z oblasti kyberkriminality a je také možné si povšimnout, že trestní zákoník pracuje s pojmy jako jsou data, počítačový systém či nosič informací[27].[28]

Ačkoliv trestní řád je předpisem procesněprávním a trestní zákoník je předpisem hmotněprávním platí, že specifikem trestního práva je to, že obě odvětví jsou na sebe napojena takovým způsobem, který v zásadě neumožňuje, aby se trestní právo hmotné realizovalo bez svého procesního protějšku. Bez trestního práva procesního by trestní právo hmotné existovalo pouze jakožto žádným způsobem nevynutitelná hrozba trestní odpovědnosti a sankce. Trestní právo hmotné i procesní tak stojí neodlučně vedle sebe a vychází ze stejných právních principů. Jelínek dokonce považuje postup zákonodárce, při kterém došlo k rekodifikaci trestního práva hmotného, ale nikoliv procesního,

[24] STUPKA, Václav. *Kyberkriminalita*, s. 572–573.
[25] Trestní zákoník nabyl účinnosti 1. 1. 2010.
[26] Např. se závazky ze směrnice Evropského parlamentu a Rady č. 2013/40/EU ze dne 12. 8. 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV a závazky z Úmluvy o ochraně dětí proti sexuálnímu vykořisťování a pohlavnímu zneužívání ze dne 25. 10. 2007 (č. 59/2016 Sb. m. s.) GŘIVNA, Tomáš a Marek DVOŘÁK. §230 Neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací. In: *Trestní zákoník. Komentář.* Praha: C. H. Beck, 2023, s. 2953.
[27] Pojem počítačového systému a nosiče informací se dostal do §7b TrŘ k tomu viz kapitola 4.5.
[28] JAKUB, Klein. *Dokazování elektronickými důkazními prostředky. Procesní aspekty v trestním řízení*. 2019, Diplomová práce, Univerzita Karlova, Právnická fakulta, s. 75.

za nesprávný, právě kvůli tomu, jak jsou na sebe obě odvětví navázána.[29] I když byly do trestního řádu včleněny procesní instituty předvídané Budapešťskou úmluvou, lze argumentovat, že správné splnění mezinárodních závazků by vyžadovalo rekodifikaci celého trestního práva, tedy jak trestního zákoníku, tak trestního řádu.[30]

1.5 Shrnutí

Aby mohly orgány činné v trestním řízení meritorně rozhodnout ve věci, musí získat informace o skutku, o kterém se trestní řízení vede – zejména, nikoli však výlučně, musí zjistit, zda došlo ke spáchání trestného činu a kdo je jeho pachatelem. Proces získávání těchto informací se označuje jako dokazování. V souvislosti s rozvojem technologií se orgánům činným v trestním řízení rozšiřují možnosti, jak tyto informace získat, a to proto, že za sebou pachatelé zanechávají kromě běžných stop i digitální stopy a také proto, že orgány činné v trestním řízení mají nové nástroje, jak stopy, ať už digitální či nikoliv, odhalit. Vznik a rozvoj technologií vede ale i k tomu, že pachatelé páchají trestné činy nové, případně páchají tradiční trestné činy novým způsobem (které lze souhrnně označit za trestné činy z oblasti kyberkriminality). Budapešťská úmluva je doposud nejdůležitějším mezinárodním pramenem, který upravuje jak kyberkriminalitu, tak problematiku související s dokazováním elektronickými důkazy. Budapešťská úmluva byla transponována do českého právního řádu, zejména do trestního zákoníku a částečně i do trestního řádu, který je základním trestně procesním předpisem a který obsahuje výchozí českou právní úpravu dokazování. S ohledem na to, že trestní řád ještě neprošel rekodifikací tak, jako trestní zákoník, lze tvrdit, že některá jeho ustanovení, související zejména s novými technologiemi, se v aplikační praxi setkávají s určitými potížemi.

[29] JELÍNEK, Jiří. I. Pojem trestního práva, jeho funkce, zásady trestního práva. In: *Trestní právo hmotné. Obecná část. Zvláštní část.* Praha: Leges, 2022, s. 21.
[30] STUPKA, Václav. *Kyberkriminalita*, s. 548.

2 Nové technologie v kontextu trestního řízení

2.1 Počítačový systém, nosič informací a data

Vzhledem k úzké provázanosti trestního práva hmotného a procesního platí, že nevymezuje-li trestní řád některé pojmy, které jsou z hlediska praxe či teorie potřebné, lze v rámci trestního řízení alespoň částečně vycházet z pojmů definovaných v trestním zákoníku.[31] Novelou trestního zákoníku z roku 2022[32] byla mezi výkladová ustanovení přidána definice pojmu počítačový systém v následujícím znění: „*Počítačovým systémem se rozumí zařízení anebo skupina vzájemně propojených nebo přidružených zařízení, z nichž jedno nebo více provádí na základě programu automatické zpracování dat. Počítačovým systémem se rozumí i data uložená, zpracovaná, opětovně vyhledaná nebo přenesená tímto zařízením anebo skupinou zařízení za účelem jeho nebo jejich provozu, použití, ochrany a údržby.*“[33] Pojem počítačového systému tak trestní zákoník vykládá poměrně široce a řadí pod zařízení či skupinu zařízení propojených kabelově i opticky, veškerý jejich hardware i software, základní jednotky i periferie a zejména pod něj také řadí v zásadě jakákoliv data existující v souvislosti s tímto zařízením či s těmito zařízeními.[34]

Myslím si, že tato definice počítačového systému je poměrně extenzivní a je vhodná při popisu skutkových podstat trestných činů, a to s ohledem na to, že dokáže postihnout širokou škálu společensky nežádoucích činů. I když se pojem počítačového systému na jednom místě v trestním řádě v souvislosti s procesněprávními instituty[35] objevuje (viz kapitola 4.5) jsem toho názoru, že pro účely trestního práva procesního a zejména pak pro účely této diplomové práce, je výše uvedená definice počítačového systému příliš široká.

O něco vhodnější mi pak přijde používání a odlišování pojmů data, počítačový systém (v užším slova smyslu) a nosič informací, se kterým trestní zákoník (možná trochu nedůsledně) pracuje v §183, odst. 1 (trestný čin porušení tajemství listin a jiných dokumentů uchovávaných v soukromí), kde je uvedeno sousloví „*data uložená v počítačovém systému nebo na nosiči informací*“.

---

[31] Pro úplnost dodávám, že trestní řád používá například pojmu „technické prostředky“ (§158d). Pod technické prostředky nicméně spadají i věci nevyužívající elektřinu, jako je třeba dalekohled, a nelze tak pojem technického prostředku a elektronického zařízení považovat za synonymní. ŠÁMAL, Pavel a Miroslav RŮŽIČKA. §158d. In: *Trestní řád: komentář*. Praha: C. H. Beck, 2013, s. 2004.

[32] Tedy zákonem č. 130/2022 Sb., kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, zákon č. 45/2013 Sb., o obětech trestných činů a o změně některých zákonů (zákon o obětech trestných činů), ve znění pozdějších předpisů, a některé další zákony.

[33] §136a TZ.

[34] GŘIVNA, Tomáš a Marek DVOŘÁK. § 136a Počítačový systém. In: *Trestní zákoník. Komentář.* Praha: C. H. Beck, 2023, s. 1828–1829.

[35] Pojem počítačového systému se v trestním řádu objevuje i v §88a TrŘ – tam se nicméně jedná pouze o odkaz na hmotněprávní úpravu.

Počítačový systém tak v kontextu §183, odst. 1 TZ lze restriktivně chápat pouze ve smyslu první věty jeho definice v §136a TZ, tedy jako „*zařízení anebo skupinu vzájemně propojených nebo přidružených zařízení, z nichž jedno nebo více provádí na základě programu automatické zpracování dat"*. Automatickým zpracováním dat se rozumí to, že zařízení, bez jakéhokoliv lidského zásahu, na data v něm obsažená působí prováděním počítačového programu.[36] Domnívám se že to, co je „propojeným nebo přidruženým zařízením", je třeba vykládat restriktivně – extenzivním, možná až absurdním výkladem, by totiž bylo možné dojít k závěru, že všechna elektronická zařízení, jež jsou napojena na internet, jsou propojena.

Nosičem informací může být obecně cokoliv, z čehož lze získat informace (tedy i například smlouva, dopis, dopravní značka). V souvislosti s výše uvedeným ustanovením (§183, odst. 1 TZ), je nosičem informací pravděpodobně myšlen především nosič (elektronických) dat, tedy cokoliv, do čeho lze data zaznamenat a zároveň je z toho lze následně získat zpět (např. CD-R, USB flash disk, pevný disk...). Platí, že počítačový systém, a to i v užším vymezení podle předchozího odstavce, může být zároveň i nosičem dat. Nosič dat se od počítačového systému v užším vymezení liší především v tom, že slouží především jako jakési skladiště dat a pokud není napojený na elektronické zařízení, neprobíhá v něm *a priori* automatické zpracování dat. *Largo sensu* může být nosičem dat i vzdálené úložiště, které však na elektronické zařízení bude napojeno v zásadě vždy a automatické zpracování dat tam pravděpodobně probíhat bude.[37]

Data, pak lze chápat jako „*surovinu, z níž se tvoří informace*"[38]. Takové pojetí dat v zásadě odpovídá i pojetí počítačových dat v Budapešťské úmluvě, ve které stojí, že „*počítačová data znamenají jakékoli vyjádření faktů, informací nebo pojmů ve formě vhodné pro zpracování v počítačovém systému, včetně programu způsobilého zapříčinit provedení funkce počítačovým systémem*".[39]

K výše uvedenému bych ještě doplnila, že mi použití přídavného jména „počítačový" ve vztahu k systému ani k datům nepřijde vhodné, a to zejména proto, že dle mého názoru u většiny populace evokuje přídavné jméno „počítačový" osobní počítač, což může být matoucí. Definice počítačového systému podle trestního zákoníku totiž sedí například i na mobilní telefon a pojetí počítačových dat v Budapešťské úmluvě zase odpovídá i datům,

[36] GŘIVNA, Tomáš a Marek DVOŘÁK. *§ 136a Počítačový systém*, s. 1828.
[37] GŘIVNA, Tomáš a Marek DVOŘÁK. *§230 Neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací*, s. 2960.
[38] GŘIVNA, Tomáš a Marek DVOŘÁK. *§ 136a Počítačový systém*, s. 1830.
[39] Čl. 1, písm. b. Budapešťské úmluvy.

jež mobilní telefon obsahuje. Ač je zřejmé, že mobilní telefon je „počítačem“, tedy výpočetní technikou, která provádí automatické zpracování dat, myslím si, že je příhodnější používat namísto „počítačový“ širší přídavná jména, například „elektronický“ nebo „digitální“ anebo přídavná jména v souvislosti s daty či systémem nepoužívat vůbec.

Pro zjednodušení a pro účely této diplomové práce jsem se tak rozhodla pracovat především s pojmem nosič dat, ve výše vymezeném smyslu a s pojmy elektronické zařízení (vycházející z první věty definice počítačového systému uvedené v §136a TZ) a elektronická data (vycházející z druhé věty definice počítačového systému uvedené v §136a TZ), v níže vymezeném významu.

Elektronickým zařízením se v této diplomové práci rozumí:

a) hmotná věc či skupina vzájemně propojených hmotných věcí,
b) využívající elektřinu pro svůj provoz,
c) zpravidla provádějící automatické zpracování dat,
d) sloužící v rámci dokazování především jako pramen důkazu a
e) jsoucí nosičem elektronických dat (tj. nosičem, v němž jsou data „fyzicky“ uložena) nebo alespoň prostředkem pro jejich čtení (tj. prostředkem, který má k datům přístup).

Elektronickými daty se v této diplomové práci rozumí:

a) nehmotná věc či skupina nehmotných věcí mající specifickou povahu,
b) získávaná z elektronického zařízení, popř. ze softwaru fungujícího v elektronickém zařízení,
c) u níž platí, že její existence a trvání může, ale nemusí být závislá na existenci elektrického zařízení[40] a
d) a která je způsobilá poskytnout nějakou informaci, resp. nějaký poznatek.

2.2 Elektronické zařízení a elektronická data

Elektronická zařízení a elektronická data nezřídka hrají zásadní roli jak v procesu dokazování, tak v trestním řízení jako celku. I prosté využití počítače pro doručení písemnosti do datové schránky,[41] lze chápat jako způsob, kterým elektronické zařízení

[40] Např. data, uchovávaná na vzdáleném úložišti, nezaniknou, bude-li zničen počítač, prostřednictvím kterého má uživatel k datům přístup. Nicméně, k tomu, aby bylo k datům možné získat přístup, bude vždy potřeba nějakého elektronického zařízení.
[41] Doručování písemností do datové schránky předpokládá §62 TrŘ.

vstupuje do trestního řízení. Elektronické zařízení může být dále použito například postupem podle §111a TrŘ, který upravuje výslech prostřednictvím videokonferenčního zařízení.

Elektronické zařízení může být předmětem útoku trestného činu, stejně jako jakákoliv jiná věc. Například odcizení televizoru může naplňovat skutkovou podstatu trestného činu krádeže podle §205 TZ a rozbití displeje objednávacího kiosku ve fastfoodu lze kvalifikovat jako přečin poškození cizí věci podle §228, odst. 1 TZ. V uvedených případech pachatel zpravidla působí na elektronická zařízení pro jejich hmotnou podstatu, nikoliv jejich obsah, tedy zejména nikoliv pro data, která obsahují.[42] Nicméně, pokud pachatel alespoň věděl, nebo vědět měl a mohl, že se v elektronickém zařízení nachází softwarové vybavení a elektronická data, bude minimálně z hlediska náhrady škody odpovědný i za to, co elektronické zařízení obsahuje. Toto tvrzení lze podpořit usnesením NS ze dne 15. 3. 2005 sp. zn. 5 Tdo 291/2005, ve kterém došel Nejvyšší soud k závěru, že součástí škody způsobené odcizením počítače je nejen cena hardwaru počítače, ale i cena softwarového vybavení, které počítač obsahuje, a to i když poškozený obdržel softwarové vybavení zdarma.

Protiprávní čin však může být spáchán na elektronickém zařízení vyloženě pro elektronická data, jež obsahuje (což trestní zákoník výslovně předpokládá - např. přečin neoprávněného zásahu do počítačového systému nebo nosiče informací z nedbalosti dle §232 TZ), prostřednictvím elektronického zařízení (např. při vydírání emailem naplňujícím skutkovou podstatu stanovenou v §175 TZ), za pomoci elektronického zařízení (např. využitím mobilního telefonu ke rozdělení úkolů mezi členy organizované zločinecké skupiny podle §129 TZ), případně se může elektronické zařízení nacházet v místě, kde se odehrály události důležité pro trestní řízení. Pro trestní řízení pak budou důležitá především elektronická data, vzniknuvší či existující v souvislosti s výše uvedenými okolnostmi.

Při páchání trestné činnosti, i při následném trestním řízení, může být důležité elektronické zařízení pro svou hmotnou podstatu anebo může jeho důležitost ustoupit elektronickým datům, která obsahuje nebo se kterými se lze jeho prostřednictvím seznámit. Platí však, že elektronická data i elektronické zařízení budou často součástí dokazování. Pro lepší demonstraci toho, jakou roli v dokazování zastávají, považuji za důležité vymezit níže uvedené pojmy, které nemají legální definici, ačkoli jsou v souvislosti s dokazováním často používány. Jedná se zejména o pojem předmětu dokazování, pramenu důkazu, důkazního prostředku a důkazu samotného.

[42] CHOCHOLATÝ, Jan. Využití mobilního telefonu v trestním řízení. *Časopis pro právní vědu a praxi*. 2005, roč. 13, č. 1, s. 71.

2.3 Předmět dokazování

Pod pojmem „předmět dokazování“ lze rozumět okolnost důležitou pro trestní řízení, která má být zjištěna a na níž zpravidla přímo nebo nepřímo závisí rozhodnutí ve věci samé.[43] Okolnostmi, na kterých závisí rozhodnutí, mohou být například takové okolnosti, které nasvědčují tomu, že obviněný je pachatelem trestného činu, že pachatel spáchal trestný čin určitým způsobem nebo i okolnosti, které osvědčují pohnutky, jež pachatele ke spáchání trestného činu vedly. Předmětem dokazování však mohou být i okolnosti, které jsou relevantní z hlediska práva procesního – třeba zda existuje důvod pro přerušení trestního stíhání podle §224 TrŘ.[44] Co je předmětem dokazování demonstrativně vymezuje §89, odst. 1 TrŘ.

S ohledem na zásadu *iura novit curia* (soud zná právo) nebudou pod předmět dokazování zásadně spadat otázky právní. Dále sem nebudou spadat skutečnosti, které se předpokládají (například právní domněnky a fikce) a skutečnosti, které jsou obecně známé (notoriety) a skutečnosti známe soudu z jeho úřední činnosti (oficiality), nevznikne-li o nich pochybnost[45]. Dokazovat se tedy bude zejména zbylá kategorie skutečností, a to tzv. skutečnosti prokazatelné. U skutečností prokazatelných je navíc třeba vymezit ty, které jsou pro dané trestní řízení relevantní tak, aby řízení nebylo zdlouhavé a nehospodárné.[46]

Ačkoliv nelze jednoznačně a komplexně vymezit okolnosti, k jejichž dokazování budou zásadně používána elektronická zařízení, elektronická data, resp. informace z nich získané, existují studie ohledně některých elektronických zařízení, které se snaží nalézt alespoň nějaké statistické souvislosti. Příkladem lze uvést studii z roku 2013, prováděnou na University of Glasgow, zabývající se mobilním telefonem jako pramenem důkazu, ve které dospěli autoři k závěru, že existuje souvislost mezi druhy trestných činů, ohledně kterých se trestní řízení vede a typy elektronických dat, které jsou v takových řízeních často využívány. Podle této studie se v řízeních, které se týkají tzv. drogových trestných činů často používají jako důkazy obsahy textových zpráv, v řízení se sexuálním podtextem jsou často relevantní videa a fotografie pořízené mobilním telefonem nebo jiným elektronickým zařízením a při

[43] FENYK, Jaroslav a Jan PROVAZNÍK. *Hlava XIII Obecné výklady o důkazech*, s. 350–353.
[44] PÚRY, František. §89 Obecná ustanovení. In: *Trestní řád: komentář*. Praha: C. H. Beck, 2013, s. 1319.
[45] Např. V trestním řízení může být důležitou skutečností to, kde se nachází srdce oběti. Notorietou je, že se srdce člověka nachází vlevo, u malého procenta lidí se však nachází vpravo – vznikne-li pochybnost o tom, kde se skutečně nachází srdce poškozeného, bude i taková známá skutečnost předmětem dokazování.
[46] POLČÁK, Radim. *I. Důkaz a Informace*, s. 41–44.

vyšetřování organizované trestné činnosti se zase často využívá záznamů telefonních hovorů.[47]

Domnívám se, že provedení obdobné studie v českém právním prostředí by bylo velmi obtížné, a to zejména s ohledem na přísné podmínky, které stanoví §65 TrŘ osobám k tomu, aby mohly nahlížet do spisu. Informace o elektronických pramenech důkazů, které byly použity v daném soudním řízení, tak může nezainteresovaná osoba (míněno osoba, se kterou nepočítá §65 TrŘ) v zásadě nalézt pouze ve zveřejněném rozhodnutí. Jsem však toho názoru, že i přestože je studie již více než 10 let stará, a i přesto že pochází ze Spojeného království, pokud by se přeci jen obdobná studie prováděla v českém právním prostředí dnes, byly by její výsledky obdobné.

2.4 Pramen důkazu a důkazní prostředek

Pramenem důkazu je zdroj, z něhož orgán činný v trestním řízení čerpá důkazy. Jedná se tedy v o nějakého (živého) nositele či o nějaký (neživý) nosič důkazu, který může mít nejrůznější podobu. V kontextu nových technologií a v kontextu toho, co je výše uvedeno, tak bude pramenem důkazu především nosič dat, resp. elektronické zařízení, které je zároveň i nosičem dat (typicky stolní či přenosný počítač, chytré hodinky a jiné wearables či mobilní telefon). Vzhledem k neustále se rozšiřujícímu množství chytrých zařízení, nelze vyloučit, že jako pramen důkazu může posloužit i takové elektronické zařízení, u kterého není na první pohled zřejmé, že v sobě obsahuje relevantní elektronická data, jako je třeba televize, elektrický vysavač[48] nebo lednička. Chytrá lednička totiž může zaznamenávat a uchovávat informace například o Bluetooth zařízeních, které se vyskytnou v její blízkosti, vizuální záznamy o předmětech, které jsou v ní umístěny nebo geolokační data.[49] Množství elektronických zařízení, které je možné použít jako pramen důkazu, se s ohledem na nárůst různých druhů chytrých zařízení neustále rozšiřuje.

Od pramenu důkazu je třeba odlišovat důkazní prostředek, což je „*způsob, jímž orgán činný v trestním řízení důkazy čerpá*“[50]. Důkazním prostředkem je podle tohoto pojetí například výslech, ohledání, ale i třeba vyšetřovací pokus, ačkoliv platí, že vyšetřovací

[47] MCMILLAN, Jack E. R., William B. GLISSON a Michael BROMBY. *Investigating the Increase in Mobile Phone Evidence in Criminal Activities*. Wailea, HI, USA: IEEE, 2013, s. 4904.
[48] Více viz např. GUO, Elieen. A Roomba recorded a woman on the toilet. How did screenshots end up on Facebook? In: *MIT Technology Review*. 19. 12. 2022.
[49] RYAN-MOSELY, Tate. How to hack a smart fridge. In: *MIT Technology Review*. 8. 5. 2023.
[50] FENYK, Jaroslav a Jan PROVAZNÍK. *Hlava XIII Obecné výklady o důkazech*, s. 346.

pokusy nejsou příliš v souvislosti s informačními technologiemi prováděny, vzhledem k tomu, že orgány činné v trestním řízení většinou upřednostňují využití znalce.[51]

2.5 Důkaz a elektronický důkaz

Důkazem je nějaká konkrétní informace, která je získána z pramene důkazu, v kontextu nových technologií především z elektronických dat, a která umožňuje přímý poznatek o tom, co je předmětem dokazování. Hlavním úkolem důkazu je vyvrácení či potvrzení určité skutečnosti. Přestože trestní řád demonstrativně vyjmenovává, co může být použito jako důkaz platí, že je-li důkaz získán zákonným způsobem, může jím být „*vše, co může přispět k objasnění věci*“[52].

Ačkoliv se elektronický důkaz, ani žádný synonymní pojem do demonstrativního výčtu důkazů nedostal, mezi „něco, co může přispět k objasnění věci“ jistě spadá. S ohledem na to, co bylo výše řečeno, lze dojít k závěru, že elektronickým důkazem je informace, mající původ v elektronickém zařízení, vycházející z elektronických dat, která umožňuje přímý poznatek o tom, co je předmětem dokazování. Zároveň platí, že bylo-li elektronické zařízení užito orgány činnými v trestním řízení pouze v souvislosti se zajišťováním jiného důkazu či důkazního pramenu, tedy v situaci, kdy elektronické zařízení bylo nástrojem, který pomáhá v procesu dokazování (např. záznam provádění úkonu nebo výslech svědka prostřednictvím telekomunikačního zařízení), není vhodné takto získaný důkaz řadit pod elektronický důkaz.

Aby bylo možné použít nehmotná elektronická data jako elektronický důkaz, je třeba, aby z nich byla vytvořena informace, která existuje v objektivně vnímatelné podobě, a to i vzhledem k tomu, že všechny relevantní důkazy musí být před soudem provedeny. Pojem elektronických dat tak nelze vnímat jako synonymum pojmu elektronického důkazu – pouze taková data, která jsou vyjádřena v podobě, kterou lze vnímat lidskými smysly, a které poskytují nějakou konkrétní informaci, mohou být elektronickým důkazem.[53]

Ačkoliv existence digitální stopy člověka s sebou nese i určitá (zejména bezpečnostní) rizika, je možné tvrdit, že z pohledu trestního vyšetřování je digitální stopa spíše žádaným fenoménem a její absence může naopak vést k paralýze trestního

[51] SMEJKAL, Vladimír. *Kybernetická kriminalita*, s. 821–822.
[52] §89, odst. 2 TrŘ.
[53] GŘIVNA, Tomáš a Martin RICHTER. Zajištění elektronického důkazu a související koncepční otázky. In: *Vliv nových technologií na trestní právo*. Praha: Auditorium, 2022, s. 14–15.

vyšetřování.[54] Rada Evropské unie dokonce uvádí, že se elektronické důkazy používají až v 85 % trestních vyšetřování.[55] Elektronické důkazy mají svá specifika a charakteristické znaky, se kterými se při jejich používání musí v rámci trestního řízení počítat. Jedná se zejména o problematiku zachycení dat v objektivně vnímatelné podobě, rozdílné povahy elektronických dat, metadat, spojení virtuální identity s konkrétním člověkem a problematiku nadnárodního charakteru elektronických dat.[56]

2.5.1 Zachycení elektronických dat v objektivně vnímatelné podobě

Jak je uvedeno výše, esenciálním rozdílem mezi elektronickými daty a elektronickým důkazem je to, že elektronický důkaz musí být zachycen ve formě, kterou lze objektivně vnímat. Jak je rovněž uvedeno výše, elektronická data lze vnímat prostřednictvím elektronického zařízení. Je-li elektronický důkaz proveden za použití elektronického zařízení, bude se jednat o věcný důkaz podle §112, odst. 1 TrŘ. Soudy ale často nebudou takovým elektronickým zařízením vybaveny nebo nemusí být použití takového elektronického zařízení při provádění důkazů vhodné. V některých případech mohou být elektronická data převedena do formy listinného důkazu podle §112, odst. 2 TrŘ. Například obsah emailové zprávy je možné zjistit prostřednictvím elektronického zařízení, tj. mobilního telefonu, počítače nebo tabletu, ale lze jej také vytisknout, čímž dostane listinnou, neelektronickou formu. Na druhou stranu je třeba myslet na to, že změnou formy může dojít ke ztrátě cenných dat (zejména metadat – viz níže). K procesu převádění do neelektronické formy je třeba vždy přistupovat s opatrností tak, aby nebyla elektronická data žádným způsobem narušena, aby byla uchována jejich vypovídající hodnota a aby z nich bylo možné získat co nejvíce informací. Samotné převádění může být komplikované i z důvodu potřebnosti odborných znalostí z oblasti informačních a komunikačních technologií. Může být a často i bude nařízen znalecký posudek, který provede osoba s odpovídající kvalifikací.[57]

---

[54] Na podporu tohoto tvrzení lze uvést případ vraždy Philipa Welshe z amerického Marrylandu, který ve svém soukromém životě nepoužíval žádná elektronická zařízení. Ačkoliv okolnosti vraždy nasvědčují tomu, je se jednalo o úmyslnou a plánovanou vraždu, nebyl doposud vrah dopaden, a to z části i kvůli úplné nepřítomnosti elektronických důkazů. GOODISON, Sean E., Robert C. DAVIS a Brian A. JACKSON. *Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence*. RAND Corporation, s. 2–3.

[55] Lepší přístup k elektronickým důkazům pro boj proti trestné činnosti. 2023.

[56] Specifika elektronických dat vybraná v této kapitole jsou jen zjednodušením celé problematiky. Zejména se omezuji na to, co je relevantní k dalším výkladům. Více ke specifikům elektronických dat viz např. SMEJKAL, Vladimír. *Kybernetická kriminalita*, s. 826.

[57] PEJČOCHOVÁ, Alena a Tomáš ELBERT. VIII. Dokazování daty z mobilních komunikačních zařízení. In: *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015, s. 209.

2.5.2 Nadnárodní charakter elektronických dat

Jednou z charakteristik elektronického zařízení, kterou uvádím výše[58] je, že elektronické zařízení je (1) nosičem elektronických dat (tj. nosičem, v němž jsou data „fyzicky" uložena) nebo alespoň (2) prostředkem pro jejich čtení (tj. prostředkem, který má k datům přístup). V prvním případě se jedná o situaci, kdy elektronická data důležitá pro trestní řízení jsou uložena přímo v elektronickém zařízení jako v nosiči dat. Budou-li taková data zajišťována, bude tak činěno především prostřednictvím jejich nosiče (srov. kapitola 4.1.1). V druhém uvedeném případě, tedy má-li elektronické zařízení pouze k elektronickým datům přístup, je situace o něco komplikovanější. Platí totiž, že i data uložená na vzdáleném úložišti, budou vždy závislá na nějakém fyzickém úložišti a mají-li být zajišťovaná data získána kompletně, tedy zejména včetně metadat, je třeba elektronická data získat z přímo z takového úložiště. Takové fyzické úložiště se může nacházet v České republice, ale i kdekoliv na světě a data mohou mezi těmito úložišti různě přecházet (v případě dat uložených v cloudu dochází k přecházení i bez účasti člověka, v závislosti na vytížení konkrétního úložiště)[59]. Úložiště budou navíc často vlastněna soukromými osobami. Teritoriální působnost orgánů činných v trestním řízení je však až na výjimky limitována na území České republiky. Budou-li orgány činné v trestním řízení potřebovat komplexně zajistit data, nacházející se na zahraničním úložišti, budou závislé na spolupráci soukromých osob, jež daná úložiště vlastní či provozují, nebo na spolupráci místních justičních orgánů.

2.5.3 Povaha elektronických dat a právo na soukromí

Pro demonstraci toho, proč je důležité zabývat se v souvislosti s elektronickými daty právem na soukromí mi přijde příhodná citace z případu Riley v. California, kde soud uvádí, že „*v době předcházející digitálnímu věku u sebe lidé většinou jen tak nenosili skříňku obsahující jejich citlivé osobní informace. Dnes, osoba, která ji nenosí, je výjimkou.*"[60]. Právo na soukromí je jedním ze základních konceptů demokratického právního státu. Zaručuje jej Listina, a to především v čl. 7 a v čl. 10. a lze jej chápat v následujícím pojetí: „*Právo na ochranu osobního soukromí je právem fyzické osoby rozhodnout podle vlastního uvážení zda, popř. v jakém rozsahu a jakým způsobem mají být skutečnosti jejího osobního soukromí zpřístupněny jiným subjektům a zároveň se bránit (vzepřít) proti neoprávněným zásahům do této sféry ze strany jiných osob*."[61]

[58] Srov. kapitola 2.2.
[59] SMEJKAL, Vladimír. *Kybernetická kriminalita*, s. 855.
[60] *Riley v. California, decided on 29. 4. 2014, 573 U.S. 373*. Překlad autorky.
[61] *Nález ÚS ze dne 1. 3. 2000, sp. zn. II. ÚS 517/99*.

Elektronická data mohou být soukromá – mohou obsahovat citlivé informace, o osobním, rodinném či jinak soukromém životě, a při zásahu do nich, resp. při jejich získávání by mělo být dbáno jejich zvláštní povahy. Existují však i elektronická data nesoukromá, například data anonymizovaná, u nichž není zvláštní ochrany třeba. Tento rozdíl lze demonstrovat na příkladu e-mailové zprávy – zpráva od osoby blízké o tom, že došlo narození dítěte v rodině bez pochyby bude chráněna právem na soukromí, nicméně zpráva o aktualizaci všeobecných obchodních podmínek e-shopu právem na soukromí chráněna nebude. Každopádně platí, že pokud je zde alespoň potencialita toho, že jsou elektronická data soukromá, a tudíž i pod ochranou práva na soukromí, měla by taková skutečnost být brána na zřetel a zejména orgány činné v trestním řízení by měly takovou skutečnost reflektovat.

2.5.4 Metadata

Naprostá většina elektronických dat obsahuje vedle primární informace i informace sekundární, kdy tyto sekundární informace jsou označovány jako tzv. metadata. Zatímco primární informace, která je výsledkem získaným z elektronických dat, jež jsou zamýšleným výsledkem činnosti osoby (tj. fotografie, videozáznam, text emailu…), metadata jsou „*strukturovaná data, která nesou informace o primárních datech*“[62]. Legální definici metadat lze nalézt v §3a, odst. 4 zákona č. 106/1999 Sb., o svobodném přístupu k informacím, které pro účely tohoto konkrétního zákona metadata popisuje jako „*data popisující souvislosti, obsah a strukturu zaznamenaných informací a jejich správu v průběhu času*“. Metadata tak v každém případě poskytují doplňující informace o primárních datech a o elektronickém zařízení, v němž je primární informace vyjádřena, které jej vytváří automaticky, protože v něm probíhá automatické zpracování dat[63] – například se jedná o datum a místo vytvoření primární informace, její úpravy a detaily týkající se softwaru, ve kterém primární informace vznikla.

Primární informace mohou být relativně snadno falzifikovány či jinak upraveny, a i když jsou metadata rovněž upravitelná, bude taková úprava zpravidla o něco složitější – navíc na ně často osoba, která se snaží o úmyslnou úpravu dat, které by mohly posloužit jako důkaz, zapomíná. V rámci metadat se někdy odlišuje samostatná podkategorie „pomocných dat“, které vytváří elektronické zařízení bez ohledu na to, zda je v něm primární informace vytvářena či nikoliv proto, aby mohlo samo fungovat nebo fungovat lépe. Jedná se například

[62] CELBOVÁ, Ludmila. Metadata. In: *KTD: Česká terminologická databáze knihovnictví a informační vědy (TDKIV)*. 2003. Praha: Národní knihovna ČR.
[63] Viz výše definice počítačového systému nebo elektronického zařízení.

o dočasné soubory a obsah mezipaměti (resp. cache), což jsou malé soubory, které se do elektronického zařízení ukládají pro to, aby fungovalo rychleji. Pomocné soubory aplikací ve většině případů nebude možné upravit, ale bude je možné smazat.[64]

2.5.5 Spojení virtuální identity s konkrétní osobou

Trestní řád nepočítá s trestním stíháním osoby neznámé – trestně stíhána může tedy být jen taková osoba, jejíž totožnost je známa. Elektronické důkazy používané za účelem prokázání viny či neviny je tak třeba vždy „přiřadit" k dané osobě. Nebude-li možné důkaz ztotožnit s takovou osobou, nebude možné důkaz jako takový, ve prospěch či v neprospěch takové osoby, použít. Pro přiřazení virtuální informace k osobě bude někdy třeba použít dalších, zejména nepřímých důkazů.

Pro příklad lze uvést fiktivní situaci, kdy při trestním řízení bylo jako důkaz v neprospěch obžalovaného použito znění emailové zprávy, poslané z emailové schránky prokazatelně patřící obžalovanému. Obžalovaný v takové situaci může tvrdit, že danou zprávu neodeslal, že se mu musel někdo dostat do počítače a odeslat zprávu místo něj. Pokud se prokáže, že se obžalovaný do emailové schránky přihlašoval výlučně z počítače, který měl ve své uzamčené domácí kanceláři, že emailová schránka byla zaheslována, obžalovaný používal dvoufázové ověření, a navíc zde nejsou žádné důvody pro to se domnívat, že došlo k dálkovému (hackerskému) útoku, zpochybnění přiřazení elektronického důkazu k obžalovanému zásadně nebude možné.

Ačkoliv je výše uvedený příklad fiktivní, lze tvrdit, že právě to, že virtuální identita nepatří tomu, v jehož neprospěch má být elektronický důkaz použit, se nabízí jako argument pro vyvrácení pravdivosti elektronického důkazu.[65] Soud se s touto argumentací musí vždy vypořádat a posoudit, zda bylo dostatečně prokázáno, že elektronický důkaz lze přiřadit k dané osobě. Takovou obranu používal obviněný při dovolání k Nejvyššímu soudu[66], který jako vlastník a administrátor domény www.serialycesky.cz metodou embeddingu sděloval veřejně díla v rozporu s autorským zákonem.[67] Nejvyšší soud v takovém případě konstatoval, že nenašel žádné logické vysvětlení pro to, proč by vlastníkem domény, kterou

[64] STUPKA, Václav. III. Data jako důkaz v trestním řízení. In: *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015, s. 95–96.
[65] Viz např. *Nález ÚS ze dne 30. 10. 2014, sp. zn. III. ÚS 3844/13*.
[66] *Usnesení NS ze dne 12. 11. 2014, sp. zn. 5 Tdo 1136/2014*.
[67] Konkrétně šlo o rozpor s § 12, § 30 a § 80 zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů.

má obviněný zaregistrovanou, byla jiná osoba, kterou navíc obviněný není schopen určit a proč by tato jiná osoba, posílala veškerý zisk z reklam na bankovní účet obžalovaného.[68]

2.6 Shrnutí

Ač trestní zákoník výslovně definuje pojem počítačového systému[69], domnívám se, že při teoretickém popisu toho, jakou funkci zastávají nové technologie v rámci trestního řízení, a především pak v rámci dokazování, je vhodnější používat pojmy jiné. Vymezení počítačového systému je totiž velmi široké a nerozlišuje mezi daty a jejich nosičem. Za vhodnější tak považuji používat pojmy elektronické zařízení a elektronická data, přičemž elektronické zařízení lze pro zjednodušení chápat ve smyslu první věty uvedené v definici počítačového systému (§136a TZ) a elektronická data zase ve smyslu věty druhé. Z hlediska dokazování bude elektronické zařízení především pramenem důkazu, tedy tím, z něhož orgány činné v trestním řízením získávají důkazy. Elektronická data přetvořená do objektivně vnímatelné podoby a získaná z elektronického zařízení jsou pak elektronickým důkazem, který lze užít k prokázání toho, co je předmětem dokazování. Způsob, jakým se důkaz získává z pramenu dokazování, lze označit jako důkazní prostředek. Elektronický důkaz je hojně používanou podkategorií „klasických důkazů“, jejíž specifičnost lze vidět v několika ohledech. Především v tom, že k tomu, aby elektronická data mohla vůbec sloužit jako důkaz, je třeba je přeměnit do objektivně vnímatelné podoby, též v tom, že se elektronická data často nacházejí na vzdálených úložištích a při jejich získávání bude potřeba spolupráce zahraničních justičních orgánů, dále v tom, že kromě primární informace mohou obsahovat i sekundární informace (tj. metadata) a konečně i v tom, že pro jejich využití při dokazování je bude zpravidla potřebné spojit s konkrétní osobou. Mají-li elektronická data soukromou povahu, měly by orgány činné v trestním řízení při nakládání s nimi tuto povahu respektovat.

[68] *Usnesení NS ze dne 12. 11. 2014, sp. zn. 5 Tdo 1136/2014*.
[69] §136a TrŘ.

3 Průběh dokazování

3.1 Trestní právo, základní práva a svobody a zásahy do nich

Trestní právo je jedním z nejdůležitějších nástrojů, kterým stát disponuje k zajištění ochrany jednotlivců před nejzávažnějšími zásahy do ústavně zaručených lidských práv. Samotná existence trestního práva a hrozba trestní sankce, může mnohdy stačit k odrazení potenciálního pachatele od spáchání trestného činu. Aby trestní právo mohlo tuto preventivní, potažmo ochrannou funkci zastávat, je třeba, aby hrozba trestní represe byla hrozbou reálnou, tedy aby skutečně mohla nastat. Proto je třeba, aby celý trestněprávní systém fungoval efektivně a aby byl nastaven způsobem zaručujícím, že uskutečněné a trestním zákonem upravené zásahy do základních práv budou odhaleny a spravedlivě potrestány. Odhalování a trestání takových zásahů, se však mnohdy neobejde bez dalších zásahů do základních práv, nikoliv ze strany pachatele ale ze strany státu, resp. orgánu činného v trestním řízení. Do práva na svobodu pohybu se zasahuje institutem vazby nebo při výkonu trestu odnětí svobody, do práva na soukromí je zasahováno při provádění domovních prohlídek či odposlechů telekomunikačního zařízení a do vlastnického práva je zasahováno při odebrání věci nebo při výkonu trestu propadnutí majetku.[70]

Stát je tak staven do na první pohled paradoxní situace, kdy k tomu, aby mohl základní práva chránit, musí do nich i zasahovat. Klíčovým je tak nalezení rovnováhy mezi zájmy společnosti na odhalení a potrestání pachatele a individuálními zájmy osoby, do jejíž práv se zasahuje – jinak řečeno, každý zásah do práv a svobod musí být především proporcionální. Lze však konstatovat, že orgány činné v trestním řízení mají nástroje, kterými mohou v zájmu dosažení spravedlivého výsledku řízení, zasahovat do lidských práv. Každý takový zásah má zákonná omezení (lze jej vykonat jen za určitých podmínek, z určitých důvodů, jen s určitým souhlasem…) a navíc je proti většině z nich možná procesní obrana, zejména je možné uplatnit některý z opravných prostředků.[71] I přes zákonná omezení může dojít k nepřiměřenému zásahu a také nelze zaručit 100% správnost či spravedlnost opravného rozhodnutí a také platí, že i když je pochybení později napraveno, mohlo již způsobit nenapravitelnou škodu či újmu. Obecnou pojistkou je i to, že orgány

[70] KLÍMA, Karel. Trestněprocesní rizika možného zákonného vstupu do ústavněprávních lidských hodnot. In: *Ochrana základních práv a svobod v trestním řízení*. Praha: Leges, 2020, s. 16.

[71] Jsou-li vyčerpané zákonné opravné prostředky, má osoba, jež se domnívá, že došlo k zásahu do jejích práv a svobod, zaručených ústavním pořádkem, možnost podat ústavní stížnost k Ústavnímu soudu. Je-li vyčerpána i tato možnost a jedná-li se o práva, která jsou zaručena EÚLP, má osoba, do jejíchž práv bylo zasaženo, možnost podat stížnost k Evropskému soudu pro lidská práva. JIRÁSEK, Jiří a Jiří MULÁK. II. Ochrana ústavně zaručených práv a svobod v trestním řízení. In: *Trestní právo procesní*. Praha: Leges, 2021, s. 50–59.

činné v trestním řízení musí postupovat v souladu se zásadou zdrženlivosti, jež je upravena v §52 TrŘ následovně: „*Při provádění úkonů trestního řízení se musí jednat s osobami na úkonu zúčastněnými tak, jak to vyžaduje význam a výchovný účel trestního řízení; vždy je nutno šetřit jejich osobnosti a jejich ústavou zaručených práv.*“[72].

3.2 Dokazování jako součást trestního řízení

Trestní řízení je postup, který začíná odhalením a zjištěním trestněprávně relevantního skutku, pokračuje identifikováním pachatele, hmotněprávním zhodnocením skutku a končí uložením trestní sankce, opatření, popř. jiným způsobem.[73] V rámci tohoto komplexního procesu, probíhají další dílčí procesy, bez kterých se trestní řízení neobejde a které mají své vlastní fáze.[74] Jedním z nejdůležitějších dílčích procesů, který je s trestním řízením úzce a neoddělitelně provázán, je proces dokazování – je to právě dokazování, prostřednictvím kterého je získáván podklad pro to, aby mohlo být ve věci meritorně rozhodnuto. Dokazování probíhá ve všech fázích trestního řízení a je zároveň nejvíce časově náročnou činností, kterou orgány činné v trestním řízení vykonávají. Dokazování má standardizované a chronologicky uspořádané fáze,[75] které se od sebe vzájemně odlišují především tím, jaké úkony jsou v jejich rámci vykonávány (také tím, kdo dané procesní úkony vykonává či kdo k nim dává souhlas či příkaz), ale i tím, jaké zásady se během nich uplatňují. Platí však, že ač lze jednotlivé fáze od sebe oddělit, nelze je úplně izolovat, protože probíhají v časové blízkosti a také jsou vzájemně provázané.[76]

3.3 Vyhledávání

První etapu dokazování lze označit jako fázi vyhledávání. I když není vyloučeno, aby vyhledávání důkazů probíhalo v pozdějším stadiu trestního řízení (v řízení před soudem), platí, že důkazy budou především vyhledávány na samotném začátku trestního řízení, tedy v rámci přípravného řízení. Přípravné řízení totiž slouží k tomu, „*aby se zjistilo, zda má být podána obžaloba a věcí se tedy má zabývat soud, či zda má být od dalšího trestního stíhání upuštěno*“[77]. K tomu, aby bylo takového zjištění dosaženo, musí orgány činné v trestním

[72]Zásada zdrženlivosti vychází i z čl. 8 EÚLP.
[73] JELÍNEK, Jiří. I. Úvodní výklady. In: *Trestní právo procesní*. Praha: Leges, 2021, s. 26.
[74] Za další dílčí procesy lze považovat například rozhodování o předběžné otázce, rozhodování o vazbě nebo o ustavování obhájce.
[75] Trestní řád fáze dokazování výslovně nepojmenovává – v naučné literatuře se tak mohou objevovat různé názvy jednotlivých fází, případně mohou být fáze spojovány či rozdělovány.
[76] JELÍNEK, Jiří. XV. Obecné výklady o důkazech. In: *Trestní právo procesní*. Praha: Leges, 2021, s. 428–431.
[77] JELÍNEK, Jiří. XX. Přípravné řízení. In: *Trestní právo procesní*. Praha: Leges, 2021, s. 529.

řízení pátrat po tom, jaké existují prameny důkazů, jež bude možné později využít pro získání důkazů samotných. Jsou to tedy právě orgány činné v trestním řízení na kterých leží, v souladu se zásadou vyhledávací, povinnost důkazy (resp. jejich prameny) vyhledávat a to i pokud jsou strany řízení (či jejich zástupci) nečinné.[78]

3.3.1 Účast osob odlišných od orgánů činných v trestním řízení na dokazování

Ačkoliv povinnost vyhledávat důkazy mají orgány činné v trestním řízení, chtějí-li procesní strany vyhledávat, předkládat a případně i provádět důkazy, trestní řád jim to umožňuje.[79] V trestním řízení se navíc obecně neuplatňuje zásada koncentrace řízení[80] a důkazy mohou být navrhovány v přípravném řízení, v řízení před soudem nebo i při odvolacím řízení.[81] I pro procesní strany, stejně jako pro orgány činné v trestním řízení, ale platí, že vyhledání a získávání důkazů, resp. důkazních pramenů, musí proběhnout v souladu se zákonem. Důkazy získané nezákonným způsobem nebude možné použít v trestním řízení jako důkaz, resp. budou takové důkazy neúčinné (srov. 3.6.1). Obviněný tak nemůže například svévolně vstoupit na sousedovu zahradu s odůvodněním, že se jen snažil zjistit, zda tam náhodou nemá bezpečnostní kameru, protože pokud by ji tam měl, mohl by její záznam použít k prokázání své neviny. Nejen, že by takto získaný důkaz nebyl získaný v souladu se zákonem, ale obviněný by se navíc pravděpodobně dopustil přečinu porušování domovní svobody podle §178 TZ.[82]

Orgánu činnému v trestním řízení dává trestní řád nástroje, kterými může důkazy vyhledat i zajistit (např. může využít operativně pátracích prostředků nebo zajišťovacích institutů). Osoba odlišná od orgánu činného v trestním řízení nicméně takovými prostředky nedisponuje. Prakticky tak mohou v souvislosti s vyhledáváním důkazů, které provádí osoba odlišná od orgánů činných v trestním řízení, nastat dvě situace. Za prvé, procesní strana má důkaz (resp. jeho pramen) k dispozici, může jej sama získat a předložit. Ačkoliv je tato situace pro procesní stranu do jisté míry náročnější, protože sama koná k tomu, aby mohla předložit důkazy, je zároveň pro procesní stranu i lepší, protože se nemusí spoléhat na součinnost orgánů činných v trestním řízení, jako v situaci druhé. Druhou situací tedy je, že procesní strana ví či předpokládá, že je důkaz v dispoziční sféře jiné osoby a je odkázána na

[78] CÍSAŘOVÁ, Dagmar a Tomáš GŘIVNA. Hlava IV Základní zásady trestního řízení. In: *Trestní právo procení*. Praha: Wolters Kluwer ČR, 2019, s. 109–110.
[79] 89, odst. 2 TrŘ.
[80] S výjimkou §43, odst. 3 TrŘ.
[81] VANTUCH, Pavel. Kdy může obhajoba důkazy vyhledat, kdy předložit a kdy jen navrhnout jeho provedení. *Bulletin advokacie*. 2013, s. 27–32.
[82] PÚRY, František. II. Dokazování v trestním řízení. In: *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015, s. 68–69.

pomoc orgánů činných v trestním řízení při vyhledání či zajištění takového důkazu. Správným postupem obviněného, který se domnívá, že sousedův dům obsahuje důležitý pramen důkazu, by pak bylo položení dotazu sousedovi a požádání o jeho vydání (první situace) či obrácení se na orgán činný v trestním řízení s žádostí o to, aby jej zajistil (druhá situace).

Navrhne-li procesní strana vyhledání, zajištění či provedení důkazu, má orgán činný v trestní řízení možnost odmítnout. Odmítnutí musí být vždy odůvodněné a důvodem nesmí být čistě jen to, že jej navrhla procesní strana. Bylo-li například navrženo vyhledání kamerového záznamu, který nebyl orgánem činným v trestním řízení nalezen, jedná se o zákonné odmítnutí navrhovaného důkazu.[83] Za další legitimní důvody odmítnutí lze považovat to, že důkaz nemá souvislost s tím, co se dokazuje, nemá vypovídací hodnotu nebo je nadbytečný, tj. má prokazovat či vyvracet to, co již bylo prokázáno či vyvráceno.[84]

3.3.2 Operativně pátrací prostředky

Ve vyhledávací fázi dokazování, tedy pro zjištění či zajištění pramenů důkazů, jsou často využívány operativně pátrací prostředky, což je podle trestního řádu[85] souhrnné označení pro předstíraný převod (§158c TrŘ), sledování osob a věcí (§158d TrŘ) a použití agenta (§158e TrŘ). O operativně pátracích prostředcích platí, že představují zásah do základních práv a svobod a mají být zásadně použity subsidiárně, tedy není-li možné zamýšleného účelu dosáhnout jinak nebo podstatně ztíženě.[86] Je možné je použít jen v souvislosti s odhalováním úmyslné trestné činnosti, nikoli tedy při vyšetřování trestných činů spáchaných z nedbalosti.[87] Je-li při použití operativně pátracích prostředků postupováno plně v souladu se zákonem, lze záznamy získané při použití operativně pátracích prostředků použít jako důkaz.[88] Předstíraným převodem se rozumí předstírání koupě, prodeje nebo jiného převodu „závadné věci“, tedy věci uvedené v §158c, odst. 1 TrŘ. Použitím agenta se pak rozumí vystupování příslušníka Policie České republiky, který plní úkoly, jež mu ukládá řídící policejní orgán a který zastírá skutečný účel své činnosti. Ač v souvislosti s využitím těchto operativně pátracích prostředků může dojít k získání

[83] *Usnesení ÚS ze dne 21. 2. 2024, sp. zn. IV. ÚS 2750/23*.
[84] PÚRY, František. *II. Dokazování v trestním řízení*, s. 71–72.
[85] §158b, odst. 1 TrŘ.
[86] §158b, odst. 2 TrŘ.
[87] §158b, odst.1 TrŘ.
[88] §158b, odst. 3 TrŘ.

důkazních pramenů, které můžou později sloužit jako elektronické důkazy,[89] nepovažuji za důležité je v této diplomové práci dále rozvádět. Naopak považuji za důležité věnovat zvláštní pozornost poslednímu z operativně pátracích prostředků, totiž sledování osob a věcí, u něhož trestní řád do jisté míry počítá s využitím elektronických zařízení a ve výsledku i se získáním elektronického důkazu a který je v souvislosti se zajišťováním elektronických dat hojně využíván.

3.3.3 Sledování osob a věcí podle §158d TrŘ

Sledování osob a věcí je proces *„získávání poznatků o osobách a věcech prováděné utajovaným způsobem technickými nebo jinými prostředky“*[90]. §158d TrŘ rozlišuje v odstavci 1, 2 a 3 tři typy sledování které probíhají v zásadně odlišných režimech:

1) Prosté sledování, u kterého není pořizován záznam podle §158d, odst. 2 TrŘ ani není zasahováno do základních práv a svobod uvedených v odst. §158d, odst. 3;
2) Sledování, při němž jsou pořizovány zvukové, obrazové nebo jiné záznamy, ale není zasahováno do základních práv a svobod uvedených v §158d, odst. 3 TrŘ;
3) Sledování, kterým se zasahuje do ústavně chráněných práv a svobod a jsou při něm používány technické prostředky.[91]

Prosté sledování, podle §158d, odst. 1 TrŘ, podléhá nejmírnějšímu povolovacímu režimu – není potřeba žádného povolení a je plně v kompetenci pověřeného policejního orgánu. Naopak sledování podle §158d, odst. 3 TrŘ, kterým se zasahuje do základních ústavně chráněných práv a svobod, tedy konkrétně do nedotknutelnosti obydlí, do listovního tajemství, popř. je zjišťován obsah písemností a záznamů uchovávaných v soukromí, podléhá nejpřísnějšímu režimu a nelze jej provést bez předchozího povolení soudce.[92] Sledování podle odst. §158d, odst. 2 TrŘ pak leží na pomezí těchto dvou režimů a jeho uskutečnění povoluje státní zástupce.[93]

Pod pojem technického prostředku, který je využíván při sledování osob a věcí, bezpochyby spadá i elektronické zařízení nicméně nelze jej s elektronickým zařízením vnímat synonymně, a to s ohledem na to, že technickým prostředkem podle tohoto

[89] Podle §158e, odst. 5 TrŘ platí, že agent nepotřebuje dalšího povolení ke sledování osob a věcí podle §158, odst. 2 TrŘ, kde se výslovně předpokládá pořizování zvukových, obrazových nebo jiných záznamů – takové záznamy zpravidla budou pramenem elektronického důkazu.
[90] §158d, odst. 1 TrŘ.
[91] ŠÁMAL, Pavel a Miroslav RŮŽIČKA. *§158d*, s. 2004.
[92] Ibid., s. 2006.
[93] Více k povolovacím režimům a procesním „pojistkám“ ochrany základních práv a svobod viz Tabulka č. 1, jež tvoří přílohu diplomové práce.

ustanovení může být i klasický dalekohled.[94] Institutu sledování osob a věcí je využíváno v souvislosti s zajišťováním dat bez současného zajištění jejich nosiče (viz kapitola 4.1.2), se získáváním hesel a přístupových údajů (viz kapitola 4.3) a též v souvislosti s instalací sledovacího softwaru, resp. při využívání tzv. prostorových odposlechů (viz kapitola 4.2).

3.4 Zajištění

Jsou-li důkazní prameny vyhledané, tedy ví-li se o jejich existenci ať už byla jejich existence zjištěna za pomocí operativně pátracího prostředku či nikoliv, nastává fáze zajištění, kdy je třeba důkazní prameny zajistit, tedy dostat je do dispoziční sféry orgánů činných v trestním řízení. Ač bude často důkaz zajištěn ihned po tom, co se o jeho existenci orgán činný v trestním řízení dozví, není vyloučeno, aby byla mezi těmito dvěma fázemi časová prodleva. Není-li pramen důkazu nebo důkaz samotný vydán dobrovolně osobou, jež jej má k dispozici, popř. není-li žádoucí, aby taková osoba věděla o tom, že jej má orgán činný v trestním řízení k dispozici a lze-li jej považovat za věc důležitou pro trestní řízení, bude zpravidla zajištěn orgánem činným v trestním řízení, a to za využití některého z níže uvedených zajišťovacích institutů. Průběh zajišťování bude zaznamenáván v protokolu a často u něj též budou prováděny obrazové, zvukové nebo jiné záznamy. Užívají-li se zajišťovací instituty pro zajišťování elektronických dat, platí určitá specifika, kterým se detailněji věnuji v kapitole 4.[95]

Při zajišťování důkazních pramenů zpravidla bude, stejně jako při využívání operativně pátracích prostředků, zasahováno do práv a svobod jednotlivce. Při užívání zajišťovacích institutů, je tak též třeba dbát na to, aby všechny zásahy byly proporcionální. Poznámkou na okraj budiž to, že i když jsou operativně pátrací prostředky formálně oddělovány od zajišťovacích institutů, jsou si zajišťovací instituty a operativně pátrací prostředky materiálně velmi podobné.

3.4.1 Zajištění věci podle trestního řádu

§67 a násl. TrŘ upravuje procesní instituty, které mohou orgány činné v trestním řízení využít k zajištění osob a věcí důležitých pro trestní řízení. S ohledem na téma diplomové práce, kterým je elektronický důkaz v trestním řízení, se nebudu zabývat zajišťováním osob[96], ač při těchto úkonech mohou být též využita nejrůznější elektronická zařízením, zejména pro záznam takového úkonu.

[94] ŠÁMAL, Pavel a Miroslav RŮŽIČKA. *§158d*, s. 2004–2005.
[95] PÚRY, František. *II. Dokazování v trestním řízení*, s. 65.
[96] Tj. zejména §67 až §77a TrŘ.

Podle §77b TrŘ je možné zajišťovat čtyři kategorie věcí – věci, které jsou nástrojem trestné činnosti, výnosem z trestné činnosti, náhradní hodnotou za předchozí dvě kategorie věcí, a především[97] pak věci, které mohou sloužit k důkazním účelům. Pojem věci trestní řád nedefinuje, nicméně lze vycházet z definice věci uvedené v občanském zákoníku, která stanoví, že věcí je „*vše, co je rozdílné od osoby a slouží potřebě lidí*“[98], přičemž věci mohou být hmotné, ale i nehmotné, kdy nehmotnými věcmi je třeba rozumět „*práva, jejichž povaha to připouští, a jiné věci bez hmotné podstaty“*[99]. Pod věc lze tedy řadit jak elektronická zařízení, tak elektronická data. V souvislosti se získáváním elektronických důkazů tak připadá v úvahu procesní institut odnětí věci (§79 TrŘ), osobní prohlídky (§82 a §83b TrŘ), domovní prohlídky (§82 a §83 TrŘ), prohlídky jiných prostor a pozemků (§82 a §83a TrŘ), zadržení zásilky (§86 TrŘ), otevření zásilky (§87 TrŘ) a odposlech a záznam telekomunikačního provozu (podle §88 a §88a TrŘ).

Platí, že při užití zajišťovacích institutů téměř vždy dochází k zásahu do ústavou zaručených práv a svobod, zejména do vlastnického práva či práva na soukromí, a proto jsou u každého zajišťovacího institutu upraveny mechanismy, kterými se má zásah buď minimalizovat nebo alespoň zajistit jeho proporcionalita s ohledem na účel, ke kterému má zajišťovaná věc sloužit. Ač považuji za vhodné jednotlivé zajišťovací instituty alespoň stručně vymezit, jsem toho názoru, že zahrnout do textu této diplomové práce informace o tom, který orgán činný v trestním řízení úkon přikazuje, dává k němu souhlas a jaké jsou další „zákonné pojistky chránící lidská práva a svobody“, by bylo zdlouhavé a nepřehledné, a tak jsem pro nejdůležitější informace zvolila formát tabulky, která tvoří přílohu této práce (viz Tabulka č.1). Tabulka č. 1 též zahrnuje operativně pátrací prostředek sledování osob a věcí podle §158d TrŘ a tzv. urychlené zajištění dat třetí osobou podle §7b TrŘ.

Na základě informací uvedených v Tabulce č. 1 lze konstatovat, že při provádění úkonů hrají nezastupitelnou roli policejní orgány, které jsou ve většině případů tím, kdo samotný zajišťovací úkon provádí. Na druhou stranu, s výjimkou výzvy k předložení nebo vydání věci a v některých případech i s výjimkou situace, kdy se jedná o věc, která nesnese odkladu, potřebují policejní orgány k provedení zajišťovacího úkonu vždy souhlas či příkaz státního zástupce nebo soudu. Státní zástupce může většinou přikázat provedení zajišťovacích úkonů, zejména pak v rámci přípravného řízení, nicméně provedení těch zajišťovacích úkonů, kterými se nejzásadněji zasahuje do ústavně zaručených práv a svobod,

[97] Zajištění věci pro důkazní účely má dle §77b, odst. 3 TrŘ prioritu.
[98] §489 OZ.
[99] §496 OZ.

může pouze navrhnout soudu. Soud[100] pak představuje nejvyššího garanta zákonného a spravedlivého postupu. Soud může přikázat provedení všech zajišťovacích úkonů i operativně pátracích prostředků a zároveň jako jediný orgán činný v trestním řízení může nařídit takové procesní úkony, které představují nejzásadnější zásah do ústavně zaručených lidských práv, za které lze považovat domovní prohlídku, odposlech a záznam telekomunikačního provozu, popř. sledování osob a věcí podle §158d, odst. 3 TrŘ.

3.4.2 Popis jednotlivých zajišťovacích institutů

Povinnost věc předložit či vydat (někdy označováno jako ediční povinnost) je obecně nejmírnějším prostředkem, kterým disponují (všechny) orgány činné v trestním řízení k tomu, aby věc důležitou pro trestní řízení získaly. Ačkoli má povinnost vydat věc každý, existují určité výjimky – pokud věc obsahuje záznamy, o nichž platí zákaz výslechu[101] nebo pokud by důkaz mohl sloužit proti osobě, jež má věc u sebe nebo proti jeho osobě blízké (ovšem prosté konstatování, že se na danou věc uplatňuje výjimka bude zpravidla nedostatečné a to, že je tu důvod pro odmítnutí výpovědi, bude třeba dokázat)[102]. Nebyla-li věc vydána, aniž by tu existoval důvod pro odmítnutí jejího vydání, je možné jednak uložit osobě, jež má věc u sebe, pořádkovou pokutu[103] a jednak je možné věc odejmout.[104]
Odnětí věci může být vykonáno samostatně nebo v rámci jiných zajišťovacích institutů, např. při osobní prohlídce, v rámci domovní prohlídky nebo prohlídky jiných prostor a pozemků. Příkaz k osobní i domovní prohlídce i prohlídce jiných prostor a pozemků v sobě zahrnuje i příkaz k odnětí věci – není tedy třeba vydávat příkazy dva.

Tyto tři typy prohlídek se v souvislosti se zajišťováním důkazů nařizují, je-li důvodné podezření, že osoba má u sebe věc důležitou pro trestní řízení nebo že takovou věc obsahuje určitý (fyzický) prostor. Rozdíl mezi domovní prohlídkou a prohlídkou jiných prostor a pozemků tkví v tom, zda se jedná o obydlí, či nikoliv. Obydlím se podle §133 TZ „*rozumí dům, byt nebo jiná prostora sloužící k bydlení a příslušenství k nim náležející.*“ Považuji za důležité zmínit, že pojem obydlí je soudy dlouhodobě vykládán extenzivně jako „*vše, co slouží člověku k bydlení a poskytuje mu soukromí*“[105]. Zahrnuje tak studentskou kolej

[100] V přípravném řízení soudce, v řízení před soudem zpravidla předseda senátu či samosoudce.
[101] Tedy informace utajované podle zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti či informace, na kterou platí zákonem uznaná povinnost mlčenlivosti. STUPKA, Václav. *Kyberkriminalita*, s. 573.
[102] Tento přístup potvrdil Ústavní soud např. v *nálezu ÚS ze dne 28. 3. 2002, sp. zn. IV. ÚS 2/02*.
[103] Podle §66 TrŘ.
[104] GŘIVNA, Tomáš a Václav MANDÁK. Hlava XII Zajištění osob, věcí a jiných majetkových hodnot důležitých pro trestní řízení. In: *Trestní právo procení*. Praha: Wolters Kluwer ČR, 2019, s. 321.
[105] ŠÁMALOVÁ, Milada. §133 Obydlí. In: *Trestní zákoník. Komentář.* Praha: C. H. Beck, 2023, s. 1799.

i hotelový pokoj, a dokonce ani nemusí být takové místo, které daná osoba užívá jako obydlí, užívané v souladu s právními předpisy.[106] Jinými prostory a pozemky je tak třeba rozumět místa, která nejsou veřejně přístupná[107] a zároveň se nejedná o obydlí.[108]

Trestní řád obsahuje ustanovení o zadržení a otevření zásilek, jejich záměně a sledování (§86 až §87c TrŘ). Zásilkou se rozumí přepravovaný předmět, bez ohledu na to, jakým způsobem je přepravován. Potom, co je přeprava ukončena, se už o zásilku nejedná.[109] Ač by teoreticky šlo na základě těchto ustanovení zadržet, otevřít, zaměnit či sledovat „zásilky" zasílané elektronickou poštou (např. e-mailem), platí, že prakticky to možné nebude. Elektronický přenos zpráv je zpravidla okamžitý nebo trvá několik málo sekund. Takový časový prostor není dostatečný k tomu, aby mohla být taková zásilka např. zajištěna a použití tohoto institutu tak při zajišťování elektronických zpráv zpravidla nebude vhodné, a proto nepovažuji za důležité se těmto institutům dále věnovat.[110]

3.4.3 Odposlech a záznam telekomunikačního provozu

Odposlech a záznam telekomunikačního provozu je dnes už poměrně tradičním institutem – i když při se při jeho tvorbě nepočítalo s „tak chytrými elektronickými zařízeními", které existují dnes, myslím si, že je dobře použitelný i v souvislosti s novými, resp. nejnovějšími technologiemi. Odposlech a záznam telekomunikačního provozu je bezpochyby velmi efektivním způsobem, kterým lze získat velké množství důkazů, ale zároveň se, z hlediska práva na soukromí, jedná o jeden z nejinvazivnějších zajišťovacích institutů. Tomu odpovídají i poměrně přísné podmínky, za kterých lze tento institut použít (viz Tabulka č.1). Zdůraznit lze to, že jeho provedení může nařídit pouze soud a je možné jej nařídit jen je-li trestní řízení vedeno pro zločin, na který trestní zákoník stanoví trest odnětí svobody s horní hranicí nejméně 8 let, jedná-li se o jeden z taxativně vyjmenovaných trestných činů nebo pokud tak stanoví mezinárodní smlouva.[111] Pod pojmem odposlechu a záznamu lze rozumět *„soudem aprobovaný postup orgánů činných v trestním řízení, které v reálném čase sledují a zachycují probíhající telekomunikační provoz za účelem získání informací důležitých pro trestních řízení."*[112]. Ač je odposlech a záznam telekomunikačního

[106] Ibid.
[107] K prohlídce veřejně přístupných míst není třeba žádného příkazu.
[108] GŘIVNA, Tomáš a Václav MANDÁK. *Hlava XII Zajištění osob, věcí a jiných majetkových hodnot důležitých pro trestní řízení*, s. 322, 325–328.
[109] ŠÁMAL, Pavel a Miroslav RŮŽIČKA. §87c. In: *Trestní řád. Komentář.* Praha: C. H. Beck, 2013, s. 1191.
[110] KOLOUCH, Jan. *CyberCrime*. CZ.NIC, 2016, s. 422.
[111] §88, odst.1 TrŘ.
[112] STUPKA, Václav. VII. Dokazování odposlechem. In: *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015, s. 182.

provozu řazen mezi zajišťovací instituty, nelze popřít, že svou povahou má blízko k operativně pátracím prostředkům.[113] Nejvyšší soud opakovaně konstatoval, že pro to, aby mohl být nařízen odposlech, musí být alespoň určitá míra jistoty o tom, že jsou splněny podmínky pro jeho přikázání, tedy zejména že je důvodné podezření, že byl spáchán trestní čin v §88, odst. 1 TrŘ. Presumpce takové informace, není možná. [114]

Pojem telekomunikačního provozu je tradičně vykládán poměrně široce – může se jednat o telefonní hovor, SMS zprávy či jakoukoliv jinou komunikaci prostřednictvím nejrůznějších platforem, kdy pod komunikaci se řadí i zaslané soubory, tedy například videa, dokumenty nebo obrázky. Telekomunikačním provozem je ale též veškerý provoz, který probíhá mezi komunikačními zařízeními, ať už jej činí člověk nebo je elektronické zařízení vykonává samo. Podle zavedené praxe platí, že pomocí §88 TrŘ lze získávat informace pouze *pro futuro*.[115] Po tom, co jsou data uložena v elektronickém zařízení, už se nejedná o data komunikačního provozu.[116]

3.4.4 Zjišťování údajů o uskutečněném telekomunikačním provozu

Zjišťování údajů o uskutečněném telekomunikačním provozu se od odposlechu a záznamu telekomunikačního provozu odlišuje především tím, že nepůsobí *pro futuro*, ale týká se již uskutečněného telekomunikačního provozu.[117] V rámci tohoto institutu nedochází k zajišťování obsahu komunikace, ale k zajišťování jiných vedlejších informací – zejména provozních a lokalizačních údajů. Provozním údajem lze rozumět *„údaje zpracovávané pro potřeby přenosu zprávy sítí elektronických komunikací nebo pro její účtování“*[118] a lokalizačním údajem pak *„údaje zpracovávané v síti elektronických komunikací nebo službou elektronických komunikací, které určují zeměpisnou polohu telekomunikačního koncového zařízení“*[119]. Provozní a lokalizační údaje jsou důležitou elektronickou stopou, která poskytuje orgánům činným v trestním řízení cenné informace, aniž by došlo k zásahu do důvěrnosti komunikace.[120]

---

[113] SKALICKÁ, Veronika. Není odposlech jako odposlech. *Trestněprávní revue*. roč. 2022, č. 1, s. 20–32.
[114] Viz např. *Usnesení NS ze dne 13. 12. 2023, sp. zn. 5 Pzo 10/2023*.
[115] TLAPÁK NAVRÁTILOVÁ, Jana a Ingrid GALOVCOVÁ. Uchovávání dat uložených v počítačovém systému – poskytování součinnosti, nebo nahrazování činnosti orgánů činných v trestním řízení? *Bulletin advokacie*. roč. 2019, č. 11, s. 36–39.
[116] *Usnesení ÚS ze dne 3. 10. 2013, sp. zn. ÚS 3812/12*.
[117] TLAPÁK NAVRÁTILOVÁ, Jana a Ingrid GALOVCOVÁ. *Uchovávání dat uložených v počítačovém systému – poskytování součinnosti, nebo nahrazování činnosti orgánů činných v trestním řízení?*
[118] §90 ZEK.
[119] §91 ZEK.
[120] *Nález ÚS ze dne 14. 5. 2019, sp. zn. PL. ÚS 45/17*.

Provozní a lokalizační údaje mají k dispozici především podnikatelé, zajišťující veřejnou komunikační síť nebo podnikatelé, poskytující veřejně dostupnou službu elektronických komunikací (tj. zejména mobilní operátoři a poskytovatelé internetového připojení). Povinnost uchovávat takové údaje trvá 6 měsíců.[121]

3.4.5 Zajišťování elektronických důkazů ze zahraničí

Jak zmiňuji v kapitole 2.5.2 platí, že v souvislosti se zajišťováním elektronických dat bude mnohdy potřebná mezinárodní justiční či jiná spolupráce. Existence elektronických dat, ke kterým má elektronické zařízení přístup, aniž by bylo zároveň jejich nosičem, totiž zpravidla závisí na existenci nějakého vzdáleného úložiště, které bude často fyzicky umístěno v zahraničí. Mají-li být získávány důkazy z jiných členských států Evropské unie, je hojně používaným nástrojem evropský vyšetřovací příkaz, který je zakotven v zákoně o mezinárodní justiční spolupráci.[122] Evropský vyšetřovací příkaz funguje na principu vzájemného uznávání rozhodnutí, což v zásadě znamená, že pokud vykonávající stát takový příkaz obdrží, je povinen jej za podmínek stanovených směrnicí (popř. ve vnitrostátním právním předpise) uznat a vykonat stejně, jako kdyby daný úkon vykonával pro potřeby vlastního státu. Lhůta pro provedení takového úkonu je však poměrně dlouhá (v celku může trvat až 120 dnů), což pro účely zajišťování elektronických důkazů nemusí být příliš praktické.[123]

Na poli Evropské unie bylo dále přijato nařízení o evropském vydávacím příkazu a evropském uchovávacím příkazu[124], jež má být plně účinné od 18.8.2026. Toto nařízení poskytuje definici elektronických důkazů, které definuje jako „*údaje o účastníkovi, údaje o provozu nebo údaje o obsahu uložené poskytovatelem služeb nebo jeho jménem v elektronické podobě v době doručení certifikátu evropského vydávacího příkazu nebo certifikát evropského uchovávacího příkazu*.“[125] Ač se jedná o jednu z prvních definic elektronického důkazu v závazných právních předpisech vůbec, je zřejmé, že taková definice nebude použitelná univerzálně, ale pouze v souvislosti s tímto nařízením. Toto nařízení především dává možnost justičním orgánům jednoho členského státu požadovat od

[121] §97, odst. 3 ZEK.
[122] Jedná se o transpozici Směrnice Evropského parlamentu a Rady 2014/41/EU ze dne 3. dubna 2014 o evropském vyšetřovacím příkazu v trestních věcech.
[123] STUPKA, Václav. *Kyberkriminalita*, s. 550–553.; Evropská komise. *Evropský vyšetřovací příkaz, vzájemná právní pomoc a společné vyšetřovací týmy*. E-justice.europa.eu. 25.11.2019.
[124] Nařízení (EU) 2023/1543 o evropském vydávacím příkazu a evropském uchovávacím příkazu pro elektronické důkazy v trestním řízení a pro výkon trestu odnětí svobody po skončení trestního řízení.
[125] Čl. 3, odst. 8 Nařízení (EU) 2023/1543 o evropském vydávacím příkazu a evropském uchovávacím příkazu pro elektronické důkazy v trestním řízení a pro výkon trestu odnětí svobody po skončení trestního řízení.

poskytovatelů některých služeb (především služeb elektronických komunikací, služeb názvů internetových domén a dalších služeb, umožňujících vzájemnou komunikaci), nacházejících se v jiném členském státě, aby předložili elektronické důkazy anebo aby takové důkazy zachovávaly. Lhůty pro vykonání požadované činnosti jsou přitom mnohem kratší než v případě evropského vyšetřovacího příkazu.[126]

Výše uvedené instituty jsou použitelné pouze na určitou výseč získávání elektronických dat ze zahraničí. Získávání elektronických dat ze zahraničí se dále může řídit například dvoustrannou mezinárodní smlouvou.[127] V této souvislosti lze zmínit i Budapešťskou úmluvu, která dává signatářům povinnost zakotvit ve vnitrostátních právních řádech určité instituty, které mají umožnit a zjednodušit mezinárodní spolupráci při zajišťování elektronických dat, jež mají později sloužit jako elektronické důkazy.

3.5 Provedení

Po tom, co je pramen důkazu vyhledán a zajištěn, tedy je v dispoziční sféře orgánů činných v trestním řízení, následují kroky vedoucí k tomu, aby důkazními prostředky byl z důkazního pramene získán samotný důkaz. Zatímco fáze vyhledávání a fáze zajišťování důkazu jsou typické pro počáteční stádia trestního řízení, provádění důkazů a jejich hodnocení bude často probíhat až při hlavním líčení. Pramen elektronického důkazu bude v rámci jeho provádění tzv. vytěžován (např. budou přehrávány audiovizuální záznamy)[128] a bude prováděna jeho analýza, kdy surová elektronická data budou převáděna na vypovídající informaci.[129] Někteří autoři v souvislosti s prováděním důkazu ještě odlišují fázi prověrky, tedy fázi, kdy dochází ke zjištění kvality, spolehlivosti a bezpečnosti důkazu.[130] Provádění elektronických důkazů může představovat určitou výzvu pro subjekty, jež tak činí, a to s ohledem na technickou náročnost, při které jsou zpravidla používány nástroje forenzní analýzy. Při provádění elektronických důkazů je třeba vybrat vhodný způsob s ohledem na to, jak byla data získána a na to, aby byla zachována metadata, pokud je elektronická data obsahují. V souvislosti s elektronickými důkazy bude často podáváno odborné vysvětlení nebo znalecký posudek.

---

[126] *Elektronické důkazy v trestním řízení – vydávací a uchovávací příkaz*. eur-lex.europa.eu. Online. 30.5.2023.

[127] Viz např. Sdělení č. 40/2000 Sb. m. s.Sdělení Ministerstva zahraničních věcí o sjednání Smlouvy mezi Českou republikou a Spojenými státy americkými o vzájemné právní pomoci v trestních věcech.

[128]ŠČERBOVÁ, Veronika. Zamyšlení nad skutečně aktuálními problémy právní úpravy tzv. prostorových odposlechů. Státní zastupitelství. roč. 2019, č. 4, s. 25.

[129] STUPKA, Václav. *Kyberkriminalita*, s. 581.

[130] PÚRY, František. *II. Dokazování v trestním řízení*, s. 66.

Znalecký posudek je jediným pramenem důkazu, který je explicitně upraven v souvislosti s právem procesní strany důkaz vyhledat, zajistit a předložit. Splňuje-li znalecký posudek formální náležitosti uvedené v §110a TrŘ a není-li důvod pro to, aby jej soud odmítl, bude se s ním v trestním řízení nakládat stejně, jako by jej opatřil orgán činný v trestním řízení. Jsou-li splněny předpoklady stanovené v §151a může stát navíc nést náklady, které jsou s obstaráním takového znaleckého posudku spojené.[131]

3.6 Hodnocení

Vyvrcholením a závěrečnou fází celého procesu dokazování je hodnocení důkazů. V rámci trestního řízení, se tato fáze objevuje ve dvojí formě, a to jako hodnocení důkazu a hodnocení důkazů. Hodnocení (jednotlivého) důkazu, bude vždy třeba provést záhy po tom, co byl důkaz proveden, nicméně platí, že takové zhodnocení nemusí být definitivní, a to s ohledem na to, že všechny důkazy je třeba hodnotit samostatně, ale i ve vzájemné souvislosti. Vyhledáním, zajištěním a provedením nového důkazu tak může dojít k „přehodnocení" již jednou zhodnoceného důkazu. Konečné zhodnocení jednotlivých důkazů a stanovení výsledku dokazování, tak nastane až po tom, co budou provedeny všechny důkazy. Výsledek dokazování bude obsažen v odůvodnění meritorního rozhodnutí a závěr, ke kterému se došlo na základě tohoto dokazování, se bude nacházet ve výroku.[132]

Při hodnocení důkazů je klíčovým principem zásada volného hodnocení důkazů, uvedená v §2, odst. 6 TrŘ, která říká, že „*Orgány činné v trestním řízení hodnotí důkazy podle svého vnitřního přesvědčení založeného na pečlivém uvážení všech okolností případu jednotlivě i v jejich souhrnu*.". Zásadu volného hodnocení důkazů nelze vykládat tak, že orgány činné v trestním řízení hodnotí důkazy libovolně – každé hodnocení důkazů musí být výsledkem logického a přezkoumatelného myšlenkového postupu. Orgány činné v trestním řízení hodnotí důkazy z několika hledisek, a to z hlediska zákonnosti (zda byly získány zákonným způsobem), pravdivosti (zda odpovídají skutečnosti), a závažnosti (jak relevantní poznatky přináší k dokazované skutečnosti). V souvislosti s hodnocením elektronických důkazů bude též klíčové ztotožnění (viz kapitola 2.5.5) důkazu a osoby. K tomu může být například využito neelektronických důkazů (např. výpověď svědka), ale i dalších elektronických důkazů (např. metadat, vč. provozních a lokalizačních údajů).[133]

[131] STUPKA, Václav. *Kyberkriminalita*, s. 583–584.
[132] CÍSAŘOVÁ, Dagmar a Tomáš GŘIVNA. *Hlava IV Základní zásady trestního řízení*, s. 116.; PÚRY, František. *II. Dokazování v trestním řízení*, s. 66.
[133] STUPKA, Václav. *VII. Dokazování odposlechem*, s. 193–1934.

3.6.1 Procesní důsledky porušení důkazního práva a použitelnost soukromých záznamů

V rámci procesu dokazování musí být postupováno v souladu s důkazním právem, a to i s ohledem na §89, odst.3 TrŘ, který stanoví, že „*důkaz získaný nezákonným donucením nebo hrozbou takového donucení nesmí být použit v řízení s výjimkou případu, kdy se použije jako důkaz proti osobě, která takového donucení nebo hrozby donucení použila.*“. Při hodnocení důkazu je zákonnost prvním zkoumaným aspektem, protože není-li důkaz získán způsobem, který zákon umožňuje, povede to k tomu, že je buďto nutné proces dokazování ve vztahu ke konkrétnímu důkazu zopakovat (pak jde o relativní neúčinnost) anebo konkrétní získaný důkaz není možné vůbec použít, resp. jeho použití nebude účinné (pak jde o absolutní neúčinnost).

Absolutně neúčinným důkazem bude například důkaz získaný orgány činnými v trestním řízení na základě zvukového záznamu, ke kterému nebyly použity odpovídající zajišťovací instituty[134] – tedy pokud orgány činné v trestním řízení pořídili záznam, aniž by pro takové pořízení byly splněny zákonné požadavky, nebo pokud bylo použití odpovídajících zajišťovacích prostředků obejito.[135]

Jednoznačnou odpověď však nelze podat na otázku, jakým způsobem má být zacházeno se záznamy, které pořídí soukromé osoby z vlastní iniciativy. Z judikatury lze dovodit, že použitelnost takových záznamů bude vždy záležet na konkrétním případě a nelze tak generálně konstatovat účinnost či neúčinnost soukromých záznamů.[136] Použití soukromých záznamů tak bude zpravidla podrobeno testu proporcionality, přičemž nejdůležitějšími zkoumanými hledisky bude to, zda byl pořízením sledován legitimní cíl[137], co bylo zaznamenáno, za jakým účelem, zda byl takový důkaz použit samostatně nebo společně s dalšími důkazy[138] a k jaké trestné činnosti se takový záznam vztahuje.[139]

Procesní postupy při vyhledávání, zajišťování a provádění elektronických důkazů jsou zákonem zpravidla upraveny zřídka anebo nejsou upraveny vůbec. Vyvstává tak otázka, co lze považovat za zákonný postup získání elektronického důkazu. Ač praxe určité postupy

---

[134] Např. postup podle §88 TrŘ nebo podle §158d TrŘ.
[135] *Usnesení ÚS ze dne 20. 10. 2011, sp. zn. II. ÚS 143/06*.
[136] Například v rozhodnutí *ÚS 191/05 ze dne 13. 9. 2006* Ústavní soud konstatoval porušení práva na ochranu tajemství doručovaných zpráv tím, že byl proveden důkaz přečtením záznamu telefonických hovorů pořízeného soukromou osobou, aniž by k tomu dotčená strana dala souhlas. Na druhou stranu to, že použití soukromého záznamu nelze a priori vyloučit, konstatoval Ústavní soud např. v *usnesení NS ze dne 3. 5. 2007, sp. zn. 5 Tdo 459/2007*.
[137] Viz např. *Usnesení ÚS ze dne 8. 2. 2010, sp. zn IV. ÚS 2425/09*.
[138] Viz např. *Usnesení NS ze dne 3.5.2007, sp. zn. Tdo 459/2007*. 2007.
[139] TIBITANZLOVÁ, Alena a Petra ZAORALOVÁ. K použitelnosti soukromých záznamů jako důkazu v trestním řízení. *Bulletin advokacie*. roč. 2023, č. 9, s. 14–23.; STUPKA, Václav. *VII. Dokazování odposlechem*, s. 182–183.

zavedla platí, jak uvádím v následující kapitole, že takové postupy nejsou přijímány bezvýhradně. Při zajišťování pramenů elektronických důkazů jsou tak orgány činné v trestním řízení částečně udržovány v určité nejistotě, a to s ohledem na to, že neví, jestli jimi zvolený postup nebude později shledán soudem za nezákonný.[140]

3.7 Shrnutí

Dokazování je neoddělitelnou součástí trestního řízení a platí, že má své standardizované fáze, které jsou vzájemně propojeny. Při vyšetřování orgány činné v trestním řízení zjišťují, jaké prameny důkazů jsou k dispozici a někdy tak činí i za využití operativně pátracích prostředků. Pokud mají orgány činné v trestním řízení představu o tom, jaké prameny důkazů existují, musí je pro účely trestního řízení zajistit. K zajišťování mají orgány činné v trestním řízení k dispozici nejrůznější nástroje, které se liší s ohledem na to, co je jak zajišťováno, ale i tím, jaký zásah do ústavně chráněných práv a svobod představují a jaké jsou podmínky k jejich nařízení. Zajištěné prameny důkazů se později analyzují či tzv. vytěžují a informace, která je tímto způsobem získána, musí být později zhodnocena soudem. Na procesu dokazování se mohou podílet i jiné osoby než orgány činné v trestním řízení, ale platí, že hodnocení náleží vždy jen soudu.

Celý proces musí zejména proběhnout v souladu se zákonem, protože pokud důkaz nebude získán zákonným způsobem, nebude účinný. S ohledem na to, že proces, který má být použit v souvislosti se zajišťováním elektronických důkazů, není vždy detailně upraven, hrozí, že bude postup, kterým byl elektronický důkaz získaný, později shledán nezákonným, a získaný důkaz neúčinným. S elektronickými zařízeními či s elektronickými daty počítají instituty sledování osob a věcí (podle §158d TrŘ) a odposlech a záznam telekomunikačního provozu (podle §88 a §88a TrŘ), kterých je v souvislosti s elektronickými důkazy často využíváno a jejichž použití je dále popisováno v následující kapitole.

[140] STUPKA, Václav. *Kyberkriminalita*, s. 572–573.

4 Zajišťování a uchovávání elektronických důkazů a jejich pramenů

4.1 Právní a technické způsoby zajišťování elektronických dat

To, jakým způsobem, ať už technickým nebo právním, budou zajišťována elektronická data (a ve výsledku i jakým způsobem z nich budou získány elektronické důkazy), se odvíjí od několika faktorů, zejména od toho:

1) zda se společně s elektronickými daty zajišťuje i elektronické zařízení či nikoliv;
2) zda se zajišťuje vypnuté elektronické zařízení či elektronické zařízení v provozu;
3) zda jsou elektronická data, která se zajišťují, stálá nebo proměnlivá; a od toho
4) jaký je charakter zajišťovaných dat.

4.1.1 Zajišťování elektronických dat za současného zajištění elektronického nosiče

Zajišťuje-li se elektronické zařízení, lze v zásadě využít všech zajišťovacích institutů popsaných v předchozí kapitole, které slouží k zajištění (hmotné) věci. Po technické stránce se jeví být relativně jednoduchým zajišťování elektronických dat, za současného zajištění nosiče dat, na kterém se data nacházejí, jež není připojen na elektronické zařízení (například zajištění elektronických dat na CD či flashdisku). Zajišťovaná data, která se nachází na takovém zajišťovaném nosiči dat, budou zpravidla neměnná – při jejich zajištění je jistota, že je zajištěna jejich konečná a pravá podoba. U takových dat nepřipadá v úvahu, aby měly proměnlivou povahu, tedy ani povahu telekomunikačního provozu, z čehož vyplývá, že se nebudou zajišťovat postupem podle §88 TrŘ. Takový nosič dat se zpravidla zapečetí a je-li to možné a vhodné, vytvoří se též jeho bitová kopie (tedy kopie obsahující nejen primární elektronická data, ale i metadata). Je-li pro trestní řízení relevantní to, že se nosič dat jakožto pramen důkazu nacházel na daném místě, musí orgány činné v trestním řízení při zajišťování dbát na to, aby bylo možné takovou skutečnost zpětně prokázat (je tedy zejména třeba zajištění řádně zdokumentovat, popř. přibrat nezúčastněnou osobu).[141]

Komplikovanější situace nastává, je-li pramen důkazu v provozu, popř. je-li napojen na elektronické zařízení, které je v provozu. Z technického hlediska může odpojení či vypnutí vést ke kompromitaci elektronických dat, k jejich zašifrování nebo ke ztrátě přístupu k datům, uloženým na vzdáleném úložišti. Při zajišťování je tak třeba posoudit, zda může k takovému znehodnocení dojít a zajišťování konkrétního pramenu důkazu tomu

[141] GŘIVNA, Tomáš a Martin RICHTER. *Zajištění elektronického důkazu a související koncepční otázky*, s. 7.; SMEJKAL, Vladimír. *Kybernetická kriminalita*, s. 825–826.; STUPKA, Václav. *Kyberkriminalita*, s. 573–575.

přizpůsobit. Platí, že je možné zajistit pouze nosič dat (tedy například SSD disk v notebooku) či nosič dat včetně elektronického zařízení, s nímž je propojen (tedy například celý notebook). Při rozhodování o tom, co všechno bude zajišťováno, musí orgány postupovat v souladu se zásadou zdrženlivosti[142] a dbát na to, aby do práv osob nebylo neúměrně zasahováno.[143]

Bude-li zajištěno elektronické zařízení podle předchozího odstavce, je pravděpodobné, že se v něm budou vyskytovat takzvaná proměnlivá data. Technicky pak bude zajišťování důkazu v takovém případě probíhat delší dobu „v živém přenosu", tedy neustálým monitorováním a zálohováním. Každá záloha tak bude představovat stav dat jako určitému časovému momentu. Z právního hlediska tak vyvstává otázka, k jakým datům může orgán činný v trestním řízení po zajištění takového elektronického zařízení přistupovat. Podle stávající praxe platí, že data, která jsou uložena přímo v elektronickém zařízení, tedy nikoli data, ke kterým má elektronické zařízení pouze dálkový přístup, může orgán činný v trestním řízení použít jako důkaz bez dalšího. Objeví-li se však na elektronickém zařízení po jeho zajištění elektronická data mající povahu elektronické komunikace (tedy telekomunikačního provozu), nesmí k nim orgán činný v trestním řízení podle momentální praxe přistoupit, aniž by byly splněny podmínky stanovené pro záznam a odposlech telekomunikačního provozu v §88 TrŘ, tedy zejména pro přístup k takovým datům potřebují předchozí souhlas soudce.[144]

4.1.2 Zajišťování elektronických dat bez současného zajištění elektronického nosiče

Elektronická data mohou být též zajišťována, aniž by současně s nimi bylo zajišťováno elektronické zařízení, prostřednictvím kterého má k nim jejich vlastník přístup. Po technické stránce platí, že taková data mohou též být zajišťována vytvořením kopie. Oproti bitové kopii pořizované ze zajištěného elektronického zařízení je však větší riziko, že kopie „původního důkazu" nebude obsahovat všechna data, protože některá data (především metadata) mohou zůstat skryta a nemusí do kopie dostat. Také platí, že nacházejí-li se taková data na úložišti, které je fyzicky umístěno v zahraničí, bude zpravidla potřebná součinnost osob, jež takové úložiště vlastní nebo provozují, či bude potřebná součinnost justičních orgánů daného států (srov. kapitola 3.4.5).[145]

[142] Zakotvené v §2, odst. 4 TrŘ.
[143] STUPKA, Václav. *Kyberkriminalita*, s. 573–575.
[144] SMEJKAL, Vladimír. *Kybernetická kriminalita*, s. 826–828.; *Výkladové stanovisko Nejvyššího státního zastupitelství č.1/2015 ze dne 26. 1. 2015, sp. zn. 1 SL 760/2014*. 2015, s. 12.
[145] SMEJKAL, Vladimír. *Kybernetická kriminalita*, s. 828.

Právní postup zajišťování takových dat bude záležet na povaze dat, která mají být zajišťována. Elektronická data, která jsou potřebná za účelem získání elektronického důkazu mohou být volně dostupná (např. webová internetová stránka). Pro jejich získání nebude třeba používat zajišťovacích institutů – bude nicméně třeba dodržovat pravidla stanovená pro ohledání věci[146], zejména je třeba sepsat protokol a pořizovat vhodnou dokumentaci, kterou může být například pořizování tzv. *printscreenů* (snímků obrazovky), často s časovým razítkem.[147]

Nebude-li se jednat o veřejně dostupná data, pak budou orgány činné v trestním řízením pro jejich zákonné získání muset postupovat jiným způsobem. Pokud jsou taková data elektronickou komunikací, která má teprve proběhnout, je nepochybné, že se pro jejich zajištění bude postupovat podle ustanovení o odposlechu a záznamu telekomunikačního provozu podle §88 TrŘ a pokud budou taková data metadata související s proběhlou elektronickou komunikací, bude se postupovat podle §88a TrŘ. Jakákoliv jiná soukromá data, ať už se jedná o již zaslané emailové zprávy nebo nejrůznější dokumenty uložené na vzdálených úložištích, se pak v praxi zajišťují postupem stanoveným pro sledování osob a věcí, kterým se zasahuje do vyjmenovaných ústavně zaručených práv a svobod podle §158d TrŘ.[148]

4.1.3 Veřejná data uchovávaná v soukromí

Problematiku získávání elektronických dat, u nichž současně nedochází k zajištění elektronického zařízení, lze demonstrovat na získávání dat, která lze označit jako veřejná data uchovávaná v soukromí – tedy data, která nelze jednoznačně označit za veřejná ani za soukromá. Do této kategorie zejména spadají data na sociálních sítích, kdy si míru veřejnosti upravuje každý uživatel sám. Pro příklad lze uvést sociální síť Facebook, kterou lze užívat pro komunikaci s konkrétními osobami (v rámci chatu – Messenger), ale také jako platformu pro komunikaci s neomezeným okruhem osob či omezeným okruhem dalších uživatelů, a to prostřednictvím osobní profilové stránky nebo prostřednictvím profilových stránek jiných uživatelů.[149]

To, jakým způsobem budou získávány důkazy ze sociálních sítí, se bude lišit podle konkrétního nastavení soukromí daného uživatele. Bude-li pro trestní řízení důležité zajistit data veřejná, tedy taková, u nichž není soukromí uživatelem žádným způsobem omezeno,

[146] §113 a násl. TrŘ.
[147] STUPKA, Václav. *Kyberkriminalita*, s. 575.
[148] GŘIVNA, Tomáš a Martin RICHTER. *Zajištění elektronického důkazu a související koncepční otázky*, s. 19.
[149] *Nález ÚS ze dne 30. 10. 2014, sp. zn. III. ÚS 3844/13*.

může je orgán činný v trestním řízení získat stejně, jako kterákoliv jiná veřejná elektronická data, volně přístupná na internetu, tedy nemusí využívat žádného zajišťovacího institutu. Bude-li chtít orgán činný v trestním řízení získat přístup k soukromé komunikaci (k chatu), která teprve proběhne či která probíhá, lze jej získat za splnění podmínek stanovených pro odposlech a záznam telekomunikačního provozu podle §88 TrŘ. Ústavní soud dále dovodil možnost získání důkazů za užití podpůrných operativně pátracích prostředků podle zákona č. 273/2008 Sb, o Policii České republiky.[150] Lze tak předpokládat, že důkazy budou použitelné i pokud budou získány za využití operativně pátracích prostředků, tedy zejména postupem podle §158d TrŘ, ale není vyloučeno ani získání dat za použití agenta podle §158e TrŘ. Z jiného rozhodnutí Ústavního soudu se lze dále domnívat, že je-li neveřejná informace ze sociální sítě zpřístupněna z vlastní iniciativy osobou, která má k takové informaci přístup (tedy například se jedná o „přítele" takové osoby), nelze *a priori* vyloučit použitelnost dat získaných tímto způsobem (viz kapitola 3.6.1).[151]

4.1.4 Zajišťování osobních elektronických zařízení

Výše uvedené lze též demonstrovat na osobním elektronickém zařízení. Osobní elektronická zařízení, tedy mobilní telefon, notebook, chytré hodinky nebo jiná podobná zařízení, představují soukromý prostor a digitální otisk svého uživatele. Obsahují obrovské množství dat – jednak ta, která jsou v něm uložena jako v datovém nosiči (tj. fotografie, poznámky, sms zprávy, kontakty…), jednak data, ke kterým má zařízení přístup (zejména lze uvést sociální sítě, ale i třeba fotografie uložená na vzdáleném úložišti). Trendem poslední doby je navíc mít vícero vzájemně propojených elektronických zařízení, která obsahují v zásadě stejná, nebo velmi podobná elektronická data. Elektronických zařízení, které představují soukromý prostor a digitální otisk svého uživatele, tak bude každá osoba mít zpravidla více.

Každé z těchto osobních zařízení lze zajistit jako hmotnou věc, tedy stejným způsobem, kterým by se zajišťovala třeba zbraň, kus oblečení nebo jakákoliv jiná věc důležitá pro trestní řízení. Porovnáme-li zajištěné osobní zařízení se zajištěným kusem oblečení, je na první pohled zřejmé, že penzum informací, která je každá z těchto věcí způsobilá poskytnout, je diametrálně rozlišné a i zásah do práv, ke kterým v důsledku zajištění věci dojde, je nesrovnatelný. Přesto se v obou situacích uplatní stejné procesní postupy. Podle stávající praxe totiž platí, že ke všem elektronickým datům, jež jsou uložena

[150] *Nález ÚS ze dne 28. 5. 2019, sp. zn. III. ÚS 3564/18*.
[151] *Nález ÚS ze dne 30. 10. 2014, sp. zn. III. ÚS 3844/13*.

přímo v osobním zařízení (kdy osobní zařízení je nosič dat), má orgán činný v trestním řízení přístup bez dalšího (pokud se postupuje podle §79 TrŘ není tak třeba ani příkazu státního zástupce). Nicméně platí, že pokud elektronická data nebudou fyzicky uložena v osobním zařízení, ale bude se jednat o data, ke kterým má dané zařízení přístup musí orgány činné v trestním řízení pro jejich zajištění postupovat podle §158d, odst. 3 TrŘ. Podmínky, které stanoví §158d, odst. 3 TrŘ jsou při tom přísnější, zejména je vyžadován souhlas soudce. Pro zjištění obsahu komunikace, která byla na zařízení doručená až po jeho zajištění (ať už přímo do zařízení nebo jen do platformy ke které má zařízení přístup), budou orgány činné v trestním řízení muset postupovat podle §88 TrŘ.[152]

Lze tak dojít k závěru, že v situaci, kdy jsou elektronická data zajišťována jako součást osobního zařízení, není jejich povaha, ani potenciální citlivost obsažených informací, právně respektována, ani brána na zřetel. Pokud se ale elektronická data zajišťují bez svého nosiče, popř. pouze prostřednictvím svého elektronického zařízení, vyvěrá jejich specifická povaha na povrch a je jim poskytována vyšší ochrana. Vyvstává tak otázka, zda je zde legitimní důvod pro to, aby byla datům poskytována nižší ochrana čistě v závislosti na tom, zda jsou umístěna na zajišťovaném elektronickém zařízení či nikoliv. Gřivna a Richter k tomuto uvádí, že „*Degradace procesní ochrany dat uchovávaných v soukromí jen z důvodů, že došlo k zajištění jejich nosiče, pak nemá oporu ve znění trestního řádu (srov dikci § 158d, odst. 3) a vede k nedůvodným kvalitativním rozdílům v ochraně základních práv a obcházení ochrany poskytované §158d, odst. 3 tr. řádu.*“[153]

4.2 Prostorový odposlech

Pojem prostorového odposlechu trestní zákoník nedefinuje. Lze jej však chápat jako sledování vizuálu, zvuků i pohybů osoby v reálném čase a to kdekoli, kde je to technicky možné (tj. doma, na pracovišti, v dopravním prostředku, na veřejnosti…), a to za využití zvláštního elektronického zařízení, které je k takovému sledování určeno. S ohledem na to, že odposlech a záznam telekomunikačního provozu je trestním řádem výslovně upraven,[154] je třeba vycházet z toho, že odposlech a záznam telekomunikačního provozu pod pojem prostorového odposlechu nespadá. Je tak nutné odlišovat dva typy odposlechů – prostorový

[152] GŘIVNA, Tomáš a Martin RICHTER. *Zajištění elektronického důkazu a související koncepční otázky*.; *Výkladové stanovisko Nejvyššího státního zastupitelství č.1/2015 ze dne 26. 1. 2015, sp. zn. 1 SL 760/2014*.
[153] GŘIVNA, Tomáš a Martin RICHTER. *Zajištění elektronického důkazu a související koncepční otázky*, s. 25.
[154] §88 a §88a TrŘ.

odposlech a odposlech komunikačního provozu. (k záznamu a odposlechu telekomunikačního provozu viz též kapitolu 3.4.3).[155]

Vzhledem k tomu, že prostorový odposlech není v zákoně výslovně definován, nejsou ani výslovně upraveny podmínky, za jakých má být používán. V praxi je pro jeho nařízení využíván institut sledování osob a věcí, upravený v §158d, odst. 2 a 3 TrŘ. Není-li prostorovým odposlechem zasahováno do ústavně zaručených práv, upravených v odst. 3, postupuje se podle odst. 2 a k jeho uskutečnění postačí povolení státního zástupce. Je-li do práv upravených v odst. 3 zasahováno, postupuje se podle tohoto odstavce a k uskutečnění prostorového odposlechu je zapotřebí povolení soudce. Jelínek je toho názoru, že by úprava měla být sjednocena a povolení soudce by mělo být vyžadováno vždy.[156] Osobně se však spíše ztotožňuji s názorem Ščerbové, která tvrdí, že odlišný povolovací režim má své odůvodnění a nedochází-li k zásahu do vyjmenovaných práv, tedy zejména je-li odposlouchávající zařízení umístěno na veřejně přístupném místě (například ve veřejné hromadné dopravě), kde může každý rozumně předpokládat, že se nepohybuje v soukromí a že může být někým zaznamenán (např. bezpečnostní kamerou), lze mírnější povolovací režim z hlediska ochrany lidských práv a svobod, zejména pak práva na soukromí, považovat za dostatečný.[157]

4.2.1 Prostorový odposlech a odposlech telekomunikačního provozu

Argument pro mírnější povolovací režim, uvedený výše, tedy, že pokud se osoba nachází na veřejném místě, může rozumně předpokládat, že může být někým zaznamenávána, lze využít i v kontextu odposlechu telekomunikačního v provozu. Každý, kdo používá komunikační prostředky, si je zpravidla vědom toho, že za sebou zanechává nějakou digitální stopu (např. lokalizační údaje nebo text SMS zprávy uložený v mobilním telefonu toho, s kým komunikuje) a může rozumně předpokládat, že je jistá šance, že se k takovým datům může dostat někdo jiný než ten, komu jsou určena a může tomu své chování přizpůsobit. V případě odposlechu telekomunikačního provozu ovšem platí, že zásah do soukromí je nevyhnutelný, a přísnější povolovací režim, tedy zejména to, že zákon vyžaduje povolení soudce, je na místě.

[155] JELÍNEK, Jiří. K chybějící právní úpravě tzv. prostorového odposlechu v trestním řádu. *Bulletin advokacie*. 2018.
[156] JELÍNEK, Jiří. K otázkám prostorového odposlechu v trestním řízení a jeho chybějící právní úpravě v českém trestním řádu. In: *Ochrana základních práv a svobod v trestním řízení*. Praha: Leges, 2020, s. 42.
[157] ŠČERBOVÁ, Veronika. *Zamyšlení nad skutečně aktuálními problémy právní úpravy tzv. prostorových odposlechů*, s. 22.

V případě prostorového odposlechu může však být zaznamenáván kdokoliv, kdo se vyskytne v místě, kde je odposlouchávací zařízení, nikoliv pouze ten, kdo se vědomě účastní telekomunikačního provozu. Při prostorovém odposlechu, který je nařízen podle §158d, odst. 3, tak bezesporu dochází k minimálně stejnému zásahu do práv jako při nařízení odposlechu telekomunikačního provozu.[158] Na rozdíl od úpravy odposlechu telekomunikačního provozu však není použití prostorového odposlechu omezeno jen na vyjmenované společensky závažnější trestné činy (postačí podezření, že byl spáchán úmyslný trestný čin) a není explicitně zakotvena povinnost orgánů činných v trestním řízení následně informovat dotčené osoby o tom, že byl prostorový odposlech proveden.[159] Vyvstává tak otázka, jestli je zde mírnější režim z hlediska standardu ochrany práv odůvodněný a zda by nemělo být dosaženo alespoň stejné procesní ochrany.

Odlišný přístup k těmto dvěma druhům odposlechů, lze vidět i použitelnosti záznamů pro účely trestního řízení v jiné věci. Příkladem lze uvést fiktivní situaci, kdy došlo k umístění odposlouchávacího zařízení v domově podezřelého z účasti na organizované zločinecké skupině[160], která se soustavně dopouští trestného činu obchodování s lidmi[161]. Podezření se později neprokáže, nicméně v době, kdy bylo v domově podezřelého umístěno odposlouchávací zařízení, jej navštívil kamarád lékař, kterého podezřelý poprosil, aby mu vystavil potvrzení o dočasné pracovní neschopnosti, protože ho to tam, kde momentálně pracuje nebaví, a chce mít dostatek času na to, aby si mohl najít nové zaměstnání a ve stávajícím zaměstnání nemá nárok na čerpání dovolené. Kamarád lékař mu takové potvrzení vystaví a podezřelý mu zato věnuje láhev vína. Oba se tak tímto jednáním dopustili přečinu padělání a vystavení nepravdivé lékařské zprávy, posudku a nálezu podle §350 TZ. Láhev vína lze považovat za úplatek[162] a v úvahu tak připadá i spáchání přečinu podplacení podle §332, odst. 1 TZ a přijetí úplatku podle §331, odst.1 TZ. Pokud by taková skutečnost byla zjištěna při použití odposlechu telekomunikačního zařízení, nebylo by možné tento záznam jako důkaz v řízení vedeném pro zjištěné trestné činy použít, a to s ohledem na §88, odst. 6 TrŘ, který stanoví, že v jiné trestní věci je možné odposlech telekomunikačního provozu

[158] JELÍNEK, Jiří. *K otázkám prostorového odposlechu v trestním řízení a jeho chybějící právní úpravě v českém trestním řádu*, s. 36.
[159] Ščerbová poukazuje na to, že je těžké vymezit osoby, kterých by se informační povinnost měla týkat – v odposlouchávaném místě můžou být zaznamenávány nejrůznější osoby, kdy jejich záznam nemusí představovat závažný zásah do jejich soukromí. Vyhledávání všech těchto osob by mohlo být pro orgány činné v trestním řízení velmi časově náročné, a i z hlediska ochrany práv a svobod takových osob nadbytečné, protože záznam nemusí nutně zasahovat do práv a svobod podle §158d, odst. 3 TrŘ. ŠČERBOVÁ, Veronika. *Zamyšlení nad skutečně aktuálními problémy právní úpravy tzv. prostorových odposlechů*, s. 24.
[160] Podle §361 TZ.
[161] Podle §168 TZ.
[162] Podle §334, odst. 1 TZ.

použít jako důkaz jen pokud by v takové jiné trestní věci bylo rovněž možné nařídit odposlech telekomunikačního provozu, kdy nařízení telekomunikačního provozu je možné jen je-li vedeno trestní řízení pro některý ze „závažnějších“ trestných činů, uvedených v§88, odst. 1 TrŘ. Pro použitelnost záznamu získaného za užití §158d, odst. 3 TrŘ jako důkazu pro účely trestního řízení v jiné věci, postačí, je-li tento jiný trestný čin též úmyslný. Domnívám se, že není žádný legitimní důvod k tomu, aby se přistupovalo odlišně, čistě na základě toho, který ze dvou druhů odposlechů byl využit.[163]

Ačkoliv výše uvedený výčet problematických aspektů prostorového odposlechu jistě není kompletní, myslím si že lze na jeho základě dojít k závěru, že úprava prostorového odposlechu může představovat stejný, nebo dokonce závažnější zásah do lidských práv, než představuje odposlech telekomunikačního provozu a je tak na místě vést diskuzi o tom, zda jsou zde důvody pro to, proč by měl být prostorový odposlech v některých případech probíhat za mírnějších podmínek než za jakých probíhá odposlech telekomunikačního provozu.

4.3 Meze získávání přístupových údajů

Přístup k některým elektronickým datům může být zabezpečen, například heslem či biometrickým údajem (např. otiskem prstu či funkcí rozpoznání obličeje). Je-li pro účely dokazování třeba dostat se k datům, která má ten, proti komu se řízení vede, zabezpečen heslem nebo jinak a neumožní-li taková osoba orgánům činným v trestní řízení dobrovolně přístup, budou orgány činné v trestním řízení zpravidla postupovat podle ustanovení upravujícího sledování osob a věcí, a to v rámci „třetího“ nejpřísnějšího režimu, upraveného v §158d, odst. 3 TrŘ, tedy stejným způsobem, jakým jsou zajišťovaná data, aniž by se současně zajišťoval jejich nosič, ale též stejným postupem, kterým je nařizován prostorový odposlech.[164]

Zajímavé mi přijdou úvahy některých autorů[165], kteří od sebe odlišují situace, kdy jsou elektronická data zabezpečena heslem a kdy jsou zabezpečena biometrickým údajem. Platí totiž, že nutit osobu, proti níž se řízení vede, ke sdělení usvědčující informace, je v trestním řízení nepřípustné. Na druhou stranu sejmout otisky či odebrat krev je možné

[163] ŠČERBOVÁ, Veronika. *Zamyšlení nad skutečně aktuálními problémy právní úpravy tzv. prostorových odposlechů*, s. 25–26.
[164] STUPKA, Václav. *Kyberkriminalita*, s. 575–577.
[165] Zásada zákazu nucení k sebeobviňování ve světle nových technologií a související procesněprávní aspekty. In: BOHUSLAV, Lukáš. *Ochrana základních práv a svobod v trestním řízení*. Praha: Leges, 2020.; GOLDMAN, Kara. Biometric Passwords and the Privilege against Self-Incrimination. *Cardozo Arts & Entertainment Law Journal*. 2015, roč. 33, č. 1.

i přes odpor takové osoby. Analogicky tak lze dojít k závěru, že zatímco nutit ke sdělení hesla možné není, odemknutí elektronického zařízení za pomocí násilného přiložení prstu toho, proti němuž se řízení vede, možné je. Takový výklad bez pochyby nedůvodně rozlišuje mezi dvěma v zásadě totožnými situacemi a není v praxi používán. Nicméně platí, že výslovné ustanovení o prolamování hesel trestní řád neobsahuje. S ohledem na to, co bylo řečeno o datech, která se nachází přímo v osobním zařízení a s ohledem na to co bylo řečeno o dvou režimech odposlechů, není neobvyklé, aby docházelo na základě dodržování formálních pravidel k nedůvodným odlišným postupům a nejde tak vyloučit, že výklad popsaný v tomto odstavci bude orgán činný v trestním řízení v konkrétním případě považovat za vhodný. Je tak na místě zvážit, zda by trestní zákoník neměl obsahovat výslovné ustanovení, které by problematiku prolamování hesel, upravovalo.

4.4 Dožádání

K tomu, aby orgány činné v trestním řízení mohly zajistit věc důležitou pro trestní řízení, zejména pramen důkazů, je někdy potřebná součinnost třetích osob. Obecnou povinnost bezplatně poskytovat součinnost orgánům činným v trestním řízení při plnění jejich úkolů zakotvuje §8, odst. 1 TrŘ. Povinnost této součinnosti mají státní orgány, ale i fyzické a právnické osoby a součinnost má být poskytnuta bez zbytečného odkladu. V odst. 7 je dále upraveno, že každý je povinen zachovávat mlčenlivost o skutečnostech, o kterých se dozvěděl v souvislosti s poskytnutím takové součinností. Pokud není součinnost poskytnuta nebo není poskytnuta vhodně, je možné uložit pořádkovou pokutu podle §66 TrŘ. Vzhledem k tomu, že ustanovení §8 TrŘ zakotvuje obecnou povinnost, platí, že obsahuje-li trestní řád speciální úpravu, obecná úprava se nepoužije. Příkladem lze uvést §88a TrŘ, který upravuje podmínky získávání metadat souvisejících s telekomunikačním provozem, ale i tzv. urychlené zajištění dat, které je upravené v §7b TrŘ.

4.5 Urychlené zajištění dat třetí osobou podle §7b TrŘ

§7b TrŘ je systematicky upraveno na začátku trestního řádu, nicméně materiálně jej lze řadit mezi předběžná opatření.[166] Postup podle §7b TrŘ totiž slouží k tomu, aby byla elektronická data dočasně „zamrazena“ (někdy je využíváno termínu *data freeze*) nebo znepřístupněna, a to za účelem předejití jejich ztrátě, zničení nebo pozměnění. U takových dat se předpokládá, že budou nebo mohou být následně zajištěna orgánem činným v trestním

[166] *Aplikační stanovisko Odboru bezpečnostní politiky ministerstva vnitra ze dne 21. 8. 2019. č. j. MV-115844-2/OBP-2019*. 2019, s. 1.

řízení. Podstatou §7b, odst. 1 TrŘ je tedy to, že umožňuje orgánům činným v trestním řízení nařídit:

1) jakékoliv osobě, aby
2) data důležitá pro trestní řízení, zejména pak data důležitá pro dokazování (tedy jakákoliv elektronická data, která je třeba v příkazu dostatečně specifikovat)[167],
3) která jsou uložena v počítačovém systému nebo na nosiči informací, jež osoba drží nebo má pod svou kontrolou,
4) uchovala v nezměněné podobě, případně i utajila informaci, že k takovému uchovávání dochází či
5) zamezila přístupu k nim (typicky aby zablokovala webovou stránku), a to
6) až po dobu 90 dnů (pro účely mezinárodní justiční spolupráce až po dobu 180 dnů)[168]

Příkaz soudce k takovému procesnímu úkonu není zapotřebí – nesnese-li věc odkladu může příkaz vydat i policejní orgán.

4.5.1 Kritika §7b TrŘ

Ač §7b TrŘ bezpochyby dává orgánům činným v trestním řízení velmi užitečný nástroj k „zamrazení" dat, je třeba konstatovat, že zařazení tohoto nástroje do trestního řádu, resp. způsobu, jakým byl do trestního řádu zařazen, mnoho autorů kritizuje. Toto ustanovení bylo do trestního řádu přidáno[169] především proto, aby byly naplněny závazky plynoucí z Budapešťské úmluvy. Jeho zařazení však proběhlo bez širších koncepčních změn a jedná se tak o jediné ustanovení trestního řádu, které s pojmem dat pracuje. Toman o něm dokonce hovoří jako o podstrčeném paragrafu, který proklouzl při novele zákona s minimální pozorností a bez odborné diskuze, protože většina pozornosti byla věnována zavedení nové skutkové podstaty maření trestného činu.[170] Zásadní argumenty autorů, proč je tato implementace považována za nevhodnou, se pokusím shrnout níže.

§7b TrŘ přesahuje rámec toho, k čemu se Česká republika zavázala v Budapešťské úmluvě. Budapešťská úmluva totiž tento institut požaduje pouze ve vztahu k odhalování počítačové kriminality (kyberkriminality), nikoliv obecně, k jiným trestným činům.[171]

---

[167] *Důvodová zpráva k zákonu č. 287/2018 Sb. kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a některé další zákony*.
[168] Ibid.
[169] Do trestního řádu bylo zařazeno novelou č. 287/2018 Sb., účinnou od 1.2.2019.
[170] TOMAN, Petr. Podstrčený paragraf 7b trestního řádu – kde se vzal a o čem je. *Advokátní deník*. 2019.
[171] TLAPÁK NAVRÁTILOVÁ, Jana a Ingrid GALOVCOVÁ. *Uchovávání dat uložených v počítačovém systému - poskytování součinnosti, nebo nahrazování činnosti orgánů činných v trestním řízení?* s. 36–39.

§7b TrŘ zakotvuje aktivní déletrvající povinnost třetích osob účasti na úkonech trestního řízení – nikoliv jednorázovou činnost, kterou zakotvuje například §8 nebo §88a TrŘ. Není rozhodné, jakým způsobem získala tato osoba k datům přístup. Ustanovení dále neřeší otázku nákladů, které tato osoba s uchováváním dat má, ani to, jakým způsobem má uchovávání dat probíhat. Ač je v důvodové zprávě[172] uvedeno, že má takové uchování provádět důvěryhodná osoba, požadavky na kvalifikaci takové osoby kladeny nejsou – uchovávání tak může být přeneseno i na úplného „technického amatéra“, který může uchováváním elektronická data znehodnotit. Teoreticky by tak mohlo dojít například k tomu, že je-li třeba uchovat data, která se nachází na Facebookovém osobním profilu viditelném pouze přátelům osoby, jejíž data mají být zajištěna, je možné povinnost k uchování dat uložit komukoliv, kdo k nim má přístup, tedy na základě titulu toho, že je „Facebookovým přítelem“ dané přítelem osoby.[173]

§7b TrŘ neupravuje poměr k jiným zajišťovacím institutům. Teoreticky tak lze jejím prostřednictvím obcházet další zajišťovací instituty, především odposlech podle §88 TrŘ, jehož použití je možné jen za splnění přísnějších podmínek.[174] Na takové tvrzení reaguje Stanovisko Odboru bezpečnostní politiky ministerstva vnitra České republiky[175], které uzavírá, že příkaz podle §7b TrŘ se vztahuje pouze na data, která již existují, nikoliv *pro futuro,* tedy na data, která teprve vzniknou.

§7b TrŘ upravuje pouze uchovávání dat, nevěnuje se tomu, jakým způsobem má dojít k jejich následnému vydání orgánu činnému v trestním řízení nebo co se s nimi stane, v případě, že vydána nejsou. Rozhodne-li orgán činný v trestní řízení, že budou „zmrazená data“ potřebná pro účely trestního řízení, je tak v praxi činěno především za použití §158d, odst. 3 TrŘ, tedy za použití úpravy pro sledování osob a věcí. Vhodnost postupu podle tohoto ustanovení je však diskutabilní - §158d TrŘ míří na získání dat, která mají sledováním teprve vzniknout – tedy *pro futuro*, což je, jak uvádím v předchozím odstavci, vyloučeno a jsou jím namísto toho zajišťována data, která už vznikla. Podobný argument lze použít v souvislosti se zajišťováním soukromých dat, uložených na vzdáleném úložišti, kde je k jejich zajišťování používáno stejného postupu (srov. kapitola 4.1.2).[176]

---

[172] *Důvodová zpráva k zákonu č. 287/2018 Sb. kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a některé další zákony*.
[173] TLAPÁK NAVRÁTILOVÁ, Jana a Ingrid GALOVCOVÁ. *Uchovávání dat uložených v počítačovém systému – poskytování součinnosti, nebo nahrazování činnosti orgánů činných v trestním řízení?* s. 36–39.
[174] TOMAN, Petr. *Podstrčený paragraf 7b trestního řádu – kde se vzal a o čem je*.
[175] *Aplikační stanovisko Odboru bezpečnostní politiky ministerstva vnitra ze dne 21. 8. 2019. č. j. MV-115844-2/OBP-2019*.
[176] TLAPÁK NAVRÁTILOVÁ, Jana. Poskytování součinnosti uchováváním dat v kontextu respektování základních práv a svobod jednotlivce. In: *Vliv nových technologií na trestní právo*. Praha: Auditorium, 2022, s. 32.; SOKOL, Tomáš. Povinnost dle §7b trestního řádu z pohledu advokáta. *Advokátní deník*. 2019.

Otázky vyvolává též oprávnění podle §7b TrŘ, které zmocňuje orgány činné v trestním řízení k tomu, aby nařídili zamezení přístupu k datům. Takové zamezení přístupu může například znamenat zablokování webové stránky, e-mailové schránky nebo nejrůznějších vzdálených úložišť. Takové zablokování může však mít pro osobou, jejíž data jsou blokována, nedozírné následky. Pokud by např. 90 dní nefungoval e-shop malého živnostníka, vedlo by to v kontextu konkurenčního prostředí velkého množství internetových obchodů téměř jistě k ukončení jeho činnosti.[177]

Mou osobní a konečnou poznámkou k §7b TrŘ budiž to, že z terminologického hlediska a s ohledem na to, co uvádím v kapitole 2.1, nepovažuji použití pojmů počítačový systém a nosič informací za vhodné, protože i zde, stejně jako v §183, odst. 1 TZ, není pojem počítačového systému použit v souladu s výkladovým ustanovením §136a TZ.

4.6 Shrnutí

Používání zajišťovacích institutů, popsaných v kapitole 3, naráží v souvislosti se zajišťováním elektronických dat na jisté aplikační problémy. V zásadě bezproblémové je zajišťování dat, spadajících pod pojem telekomunikačního provozu, postupem podle §88 TrŘ. Takové ustanovení se použije vždy, mají-li zajišťovaná data charakter telekomunikačního provozu a jsou-li zajišťována *pro futuro*. Co se týče jiných dat, je momentální praxe taková, že to, jakým způsobem budou elektronická data zajišťována, se především odvíjí od toho, jestli se spolu s nimi zajišťuje elektronické zařízení, na němž jsou přímo uložena nebo nikoliv. Orgány činné v trestním řízení mohou zajistit elektronické zařízení jako kteroukoliv jinou věc a k datům, která jsou v něm přímo uložena k momentu jeho zajištění, přistupovat bez dalšího. Pokud se zajišťují data, která nejsou přímo uložena v elektronickém zařízení, jako v nosiči dat, a pokud se nejedná o data, která jsou volně přístupná nebo data vyžadující postup podle §88 nebo §88a TrŘ, je v praxi postupováno podle §158d TrŘ. Otázkou je, zda je zde důvod pro to, aby k v zásadě stejným datům byla poskytována diametrálně odlišná ochrana a zda by neměla být míra ochrany dat sjednocena.

Existují dva druhy odposlechů – odposlech telekomunikačního zařízení, který je v zákoně upraven v §88 TrŘ a prostorový odposlech, jehož výslovnou právní úpravu trestní zákoník neposkytuje a v praxi je tak při jeho nařízení postupováno podle §158d, odst. 2 nebo odst. 3 TrŘ. Při obou odposleších dochází minimálně ke stejně závažným zásahům do práva na soukromí, nicméně míra procesní ochrany, která je každému z nich poskytována, je odlišná. Myslím si, že takové rozdíly jsou v některých případech nedůvodné a měly by

[177] TOMAN, Petr. *Podstrčený paragraf 7b trestního řádu – kde se vzal a o čem je*.

především být sjednoceny podmínky kladené na jejich nařízení, zejména by měly být oba odposlechy použitelné pouze při vyšetřování společensky závažnějších trestných činů.

Při vyšetřování trestných činů potřebují někdy orgány činné v trestním řízení součinnost od třetích osob. Obecným ustanovením zakotvující povinnost součinnosti třetím osobám je §8 TrŘ. Jediné ustanovení trestního řádu, které výslovně pracuje s elektronickými daty, je §7b TrŘ, které upravuje podmínky „zmrazení" dat, popř. zamezení přístupu k datům, jež je možné uložit komukoliv. Toto ustanovení bylo do trestního zákoníku vloženo proto, aby Česká republika splnila závazky plynoucí z Budapešťské úmluvy a zdá se tak, že koncepčně do pojetí trestního řádu nesedí. Příkladem lze uvést to, že je otázkou, zda je zde legitimní důvod pro to, aby třetí osobě byla uložena součinnost trvající až po dobu 90 dnů bez nároku na jakoukoliv finanční kompenzaci, dále jak posoudit kompetence takové osoby k této déletrvající součinnosti a jak postupovat v souvislosti se zajištěním již „zamrazených dat". V praxi se pro zajištění používá postup podle §158d, odst. 3 TrŘ. Ač se z možností, které trestní řád pro zajištění věcí nabízí, zdá být tento postup jako nejvhodnější, je třeba uvažovat nad tím, zda by neměl být tento postup trestním zákoníkem výslovně upraven přímo v §7b TrŘ.

Závěr

Elektronický důkaz je pojem, který trestní řád nevymezuje. Lze jej ovšem chápat jako informaci důležitou pro trestní řízení, mající původ v elektronickém zařízení a vycházející z elektronických dat, která umožňuje přímý poznatek o tom, co je předmětem dokazování. V souvislosti s elektronickými důkazy se zdá být vhodným odlišovat mezi tím, co jsou elektronická zařízení (popř. nosiče dat) a elektronická data a nesjednocovat všechny tyto pojmy pod pojem počítačového systému způsobem, kterým tak činí trestní zákoník v definici počítačového systému v §136a.

Elektronická data či elektronická zařízení tak mohou být pramenem, ze kterého orgány činné v trestním řízení, čerpají důkazy. Taková data či zařízení musí být nejprve vyhledána, poté zajištěna, provedena a nakonec zhodnocena. Celý postup musí probíhat zákonným způsobem, jinak nebude možné elektronické důkazy použít jako podklad pro rozhodnutí. Postupy, které mají být dodržovány v souvislosti se získáváním elektronických důkazů, však často z trestního řádu výslovně nevyplývají (s existencí elektronických důkazů v zásadě počítá pouze §7b, §88, §88a a §158d TrŘ) a vznikají tak některé aplikační otázky, především jaký postup zvolit tak, aby byly získané elektronické důkazy v trestním řízení použitelné a aby při postupu nedošlo k disproporcionálnímu zásahu do lidských práv a svobod. Největší nejasnosti, týkající se elektronických důkazů, se objevují v souvislosti s jejich vyhledáváním a zajišťováním.

Trestní řád upravuje standardizované postupy, jež slouží k vyhledávání a zajišťování důkazních pramenů. U každého z těchto postupů zákonodárce předpokládá potenciální míru zásahů do základních práv a svobod a stanovuje procesní záruky jejich ochrany. Zajišťovací instituty, které předpokládají nejvyšší míru zásahu do základních práv mají nejpřísnější podmínky a zásadně je nelze provést bez předchozího souhlasu soudce.

Konkrétní postupy (a jejich povolovací režimy), kterými jsou zajišťovány prameny elektronických důkazů, jsou často založené na formálním hledisku toho, jakým způsobem zajišťování probíhá. Specifická charakteristika elektronických důkazů často způsobuje, že následováním formálně stanovených postupů dochází k tomu, že v případech, majících podobné výsledky, jsou uplatňovány odlišné zajišťovací instituty, různé povolovací režimy a je poskytována nestejná ochrana práv a svobod. Pro podporu tohoto tvrzení lze uvést v praxi uplatňovaný odlišný režim zajišťování elektronických dat, ke kterému dochází čistě na základě toho, zda se fyzicky vyskytují v elektronickém zařízení nebo nikoliv a odlišné podmínky, za kterých lze nařídit odposlech telekomunikačního provozu a prostorový odposlech.

Dále se zdá, že v situaci, kdy orgánům činným v trestním řízením chybí výslovná úprava, je hojně využíváno operativně pátracího prostředku sledování osob a věcí podle §158d, odst. 3 TrŘ, kterého se využívá jak v souvislosti se zajišťováním elektronických dat nezajišťovaných současně s elektronickým zařízením, tak v souvislosti s prolamováním hesel, používáním prostorového odposlechu, ale i při zajišťování dat „zamrazených" podle §7b TrŘ.

Hypotéza, ze které vycházím v úvodu této práce, totiž že trestní řád nedostatečně reflektuje specifika související s používáním nových technologií při dokazování, se tak zdá být potvrzenou. Ač si netroufám činit konkrétní návrhy *de lege ferenda*, myslím si, že povaha elektronických dat a to, jaké jejich zajišťování může představovat zásahy do soukromí, by mělo být zákonodárcem reflektováno, měly by jim být poskytnuty dostatečné procesní záruky a především by měla být sjednocena úprava postupů majících stejný faktický dopad.

Seznam zkratek

Budapešťská úmluva	Sdělení č. 104/2013 Sb. m. s. Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě
Listina	Usnesení předsednictva České národní rady č. 2/1993 Sb. o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součástí ústavního pořádku České republiky
NS	Nejvyšší soud České republiky
občanský zákoník/OZ	Zákon č. 89/2012 Sb., občanský zákoník
trestní řád/TrŘ	Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád)
trestní zákoník/TZ	Zákon č. 40/2009 Sb., trestní zákoník
ÚS	Ústavní soud České republiky
ústava	Ústavní pořádek ve smyslu čl. 112, odst. 1 ústavního zákona č. 1/1993 Sb., Ústava České republiky
zákon o mezinárodní justiční spolupráci	Zákon č.104/2013 Sb., o mezinárodní justiční spolupráci
ZEK	Zákon č. 127/2005 Sb. Zákon o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)

Seznam použitých zdrojů

1. Seznam použité literatury

ADAMOVÁ, Karolina a Ladislav SOUKUP. *Prameny k dějinám práva v českých zemích*. 2. vyd. Plzeň: Aleš Čeněk s.r.o., 2010. ISBN 978-80-7380-271-4.

BOHUSLAV, Lukáš. Zásada zákazu nucení k sebeobviňování ve světle nových technologií a související procesněprávní aspekty. In: JELÍNEK, J. a kol. *Ochrana základních práv a svobod v trestním řízení*. Praha: Leges, 2020. s. 396-402. ISBN 978-80-7502-444-2.

CÍSAŘOVÁ, Dagmar a Tomáš GŘIVNA. Hlava IV Základní zásady trestního řízení. In: FENYK, J., CÍSAŘOVÁ, D., GŘIVNA, T. a kol. *Trestní právo procení*. 7. vyd. Praha: Wolters Kluwer ČR, 2019. s. 92-119. ISBN: 978-80-7598-307-7.

FENYK, Jaroslav a Jan PROVAZNÍK. Hlava XIII Obecné výklady o důkazech. In: FENYK, J., CÍSAŘOVÁ, D., GŘIVNA, T. a kol. *Trestní právo procení*. 7. vydání. vyd. Praha: Wolters Kluwer ČR, 2019. s. 343-375. ISBN: 978-80-7598-307-7.

GOLDMAN, Kara. Biometric Passwords and the Privilege against Self-Incrimination. *Cardozo Arts & Entertainment Law Journal*. 2015, roč. 33, č. 1, s. 211–236.

GOODISON, Sean E., Robert C. DAVIS a Brian A. JACKSON. *Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence*. RAND Corporation. ISBN 978-0-8330-9141-3.

GŘIVNA, Tomáš a Marek DVOŘÁK. §136a Počítačový systém. In: ŠÁMAL, P. a kol. *Trestní zákoník. Komentář.* 3. vydání. vyd. Praha: C. H. Beck, 2023. s. 1827-1831 ISBN: 978-80-7400-893-1.

GŘIVNA, Tomáš a Marek DVOŘÁK. §230 Neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací. In: ŠÁMAL, P. a kol. *Trestní zákoník. Komentář.* 3. vydání. vyd. Praha: C. H. Beck, 2023. s. 2949-2970. ISBN: 978-80-7400-893-1.

GŘIVNA, Tomáš a Václav MANDÁK. Hlava XII Zajištění osob, věcí a jiných majetkových hodnot důležitých pro trestní řízení. In: FENYK, J., CÍSAŘOVÁ, D., GŘIVNA, T. a kol. *Trestní právo procení*. 7. vydání. vyd. Praha: Wolters Kluwer ČR, 2019. s. 343-375. ISBN: 978-80-7598-307-7.

GŘIVNA, Tomáš a Martin RICHTER. Zajištění elektronického důkazu a související koncepční otázky. In: GŘIVNA, T., RICHTER, M., ŠIMÁNOVÁ, H. a kol. *Vliv nových technologií na trestní právo*. Praha: Auditorium, 2022. s. 13-27. ISBN 978-80-87284-95-7.

CHOCHOLATÝ, Jan. Využití mobilního telefonu v trestním řízení. *Časopis pro právní vědu a praxi*. 2005, roč. 13, č. 1. s. 71-74. ISSN 1805-2789.

JELÍNEK, Jiří. I. Pojem trestního práva, jeho funkce, zásady trestního práva. In: JELÍNEK, J. a kol. *Trestní právo hmotné. Obecná část. Zvláštní část.* 8. vyd. vyd. Praha: Leges, 2022. s. 23-50. ISBN 978-80-7502-576-0.

JELÍNEK, Jiří. I. Úvodní výklady. In: JELÍNEK, J. a kol. *Trestní právo procesní*. 6. aktualizované vydání. vyd. Praha: Leges, 2021. Edice Student. s. 17-32. ISBN 978-80-7502-550-0.

JELÍNEK, Jiří. K otázkám prostorového odposlechu v trestním řízení a jeho chybějící právní úpravě v českém trestním řádu. In: JELÍNEK, J. a kol. *Ochrana základních práv a svobod v trestním řízení*. Praha: Leges, 2020. s. 35-45. ISBN 978-80-7502-444-2.

JELÍNEK, Jiří. XV. Obecné výklady o důkazech. In: JELÍNEK, J. a kol. *Trestní právo procesní*. 6. vyd. Praha: Leges, 2021. Edice Student. s. 397-427. ISBN 978-80-7502-550-0.

JELÍNEK, Jiří. XX. Přípravné řízení. In: JELÍNEK, J. a kol. *Trestní právo procesní*. 6. vyd. Praha: Leges, 2021. Edice Student. s. 528-548. ISBN 978-80-7502-550-0.

JIRÁSEK, Jiří a Jiří MULÁK. II. Ochrana ústavně zaručených práv a svobod v trestním řízení. In: JELÍNEK, J. a kol. *Trestní právo procesní*. 6. vyd. Praha: Leges, 2021. Edice Student. s. 34-55. ISBN 978-80-7502-550-0.

KLÍMA, Karel. Trestněprocesní rizika možného zákonného vstupu do ústavněprávních lidských hodnot. In: JELÍNEK, J. a kol. *Ochrana základních práv a svobod v trestním řízení*. Praha: Leges, 2020. s. 15-25. ISBN 978-80-7502-444-2.

KOLOUCH, Jan. *CyberCrime*. 1. vyd. CZ.NIC, 2016. ISBN 978-80-88168-18-8.

MCMILLAN, Jack E. R., William B. GLISSON a Michael BROMBY. *Investigating the Increase in Mobile Phone Evidence in Criminal Activities*. Wailea, HI, USA: IEEE, 2013. s. 4900-4909. ISBN 978-0-7695-4892-0.

PEJČOCHOVÁ, Alena a Tomáš ELBERT. VIII. Dokazování daty z mobilních komunikačních zařízení. In: POLČÁK, R., PÚRY, F., HARAŠTA, J. a kol. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015. Spisy Právnické Fakulty Masarykovy Univerzity svazek č. 542. Řada teoretická. s. 197-219. ISBN 978-80-210-8073-7.

POLČÁK, Radim. I. Důkaz a Informace. In: POLČÁK, R., PÚRY, F., HARAŠTA, J. a kol. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, 2015. Spisy Právnické Fakulty Masarykovy Univerzity svazek č. 542. Řada teoretická. s. 15-44. ISBN 978-80-210-8073-7.

PÚRY, František. §89 Obecná ustanovení. In: ŠÁMAL, P. a kol. *Trestní řád: komentář*. 7. vyd. Praha: C. H. Beck, 2013. s. 1308-1394. ISBN 978-80-7400-465-0.

PÚRY, František. II. Dokazování v trestním řízení. In: POLČÁK, R., PÚRY, F., HARAŠTA, J. a kol. *Elektronické důkazy v trestním řízení*. Brno: Masarykova

univerzita, 2015. Spisy Právnické Fakulty Masarykovy Univerzity svazek č. 542. Řada teoretická. s. 45-81. ISBN 978-80-210-8073-7.

SKALICKÁ, Veronika. Není odposlech jako odposlech. *Trestněprávní revue*. roč. 2022, č. 1. s. 20. ISSN 1213-5313.

SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o, 2022. ISBN 978-80-7380-849-5.

STUPKA, Václav. III. Data jako důkaz v trestním řízení. In: POLČÁK, R., PÚRY, F., HARAŠTA, J. a kol. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015. Spisy Právnické Fakulty Masarykovy Univerzity svazek č. 542. Řada teoretická. s. 83-114. ISBN 978-80-210-8073-7.

STUPKA, Václav. Kyberkriminalita. In: POLČÁK, R. a kol. *Právo informačních technologií*. 1. vyd. Praha: Wolters Kluwer ČR, 2018. s. 541-584. ISBN 978-80-7598-045-8.

STUPKA, Václav. VII. Dokazování odposlechem. In: POLČÁK, R., PÚRY, F., HARAŠTA, J. a kol. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015. Spisy Právnické Fakulty Masarykovy Univerzity svazek č. 542. Řada teoretická. s. 181-194. ISBN 978-80-210-8073-7.

ŠÁMAL, Pavel a Miroslav RŮŽIČKA. §87c. In: ŠÁMAL, P. a kol. *Trestní řád: komentář*. 7. vyd. Praha: C. H. Beck, 2013. s. 1191. ISBN 978-80-7400-465-0.

ŠÁMAL, Pavel a Miroslav RŮŽIČKA. §158d. In: ŠÁMAL, P. a kol. *Trestní řád: komentář*. 7. vyd. Praha: C. H. Beck, 2013. s. 2001-2012. ISBN 978-80-7400-465-0.

ŠÁMALOVÁ, Milada. §133 Obydlí. In: ŠÁMAL, P. a kol. *Trestní zákoník. Komentář.* 3. vyd. Praha: C. H. Beck, 2023. s. 1797-1804. ISBN: 978-80-7400-893-1.

ŠČERBOVÁ, Veronika. Zamyšlení nad skutečně aktuálními problémy právní úpravy tzv. prostorových odposlechů. Státní zastupitelství. roč. 2019, č. 4. s. 19-26. ISSN: 1803-7631.

TIBITANZLOVÁ, Alena a Petra ZAORALOVÁ. K použitelnosti soukromých záznamů jako důkazu v trestním řízení. *Bulletin advokacie*. roč. 2023, č. 9. s. 14. ISSN 1805-8280.

TLAPÁK NAVRÁTILOVÁ, Jana. Poskytování součinnosti uchováváním dat v kontextu respektování základních práv a svobod jednotlivce. In: JELÍNEK, J. a kol. *Vliv nových technologií na trestní právo*. Praha: Auditorium, 2022. s. 26-34. ISBN 978-80-87284-95-7.

TLAPÁK NAVRÁTILOVÁ, Jana a Ingrid GALOVCOVÁ. Uchovávání dat uložených v počítačovém systému – poskytování součinnosti, nebo nahrazování činnosti orgánů činných v trestním řízení? *Bulletin advokacie*. roč. 2019, č. 11. s. 36. ISSN 1805-8280.

VLČEK, Eduard. *Dějiny trestního práva v českých zemích a v Československu*. Brno: Masarykova univerzita Brno – Právnická fakulta, 2007. ISBN 978-80-210-4056-4.

2. Seznam použitých internetových zdrojů

Evropská komise. Evropský vyšetřovací příkaz, vzájemná právní pomoc a společné vyšetřovací týmy. E-justice.europa.eu. Online. 25.11.2019. Dostupné z: https://e-justice.europa.eu/92/CS/european_investigation_order_mutual_legal_assistance_and_joint_investigation_teams [cit. 2024-05-15].

Elektronické důkazy v trestním řízení – vydávací a uchovávací příkaz. eur-lex.europa.eu. Online. 30.5.2023. Dostupné z: https://eur-lex.europa.eu/CS/legal-content/summary/electronic-evidence-in-criminal-proceedings-production-and-preservation-orders.html [cit. 2024-05-15].

GUO, Elieen. A Roomba recorded a woman on the toilet. How did screenshots end up on Facebook? Technologyreview.com. Online. 19.12.2022. Dostupné z: https://www.technologyreview.com/2022/12/19/1065306/roomba-irobot-robot-vacuums-artificial-intelligence-training-data-privacy/ [cit. 2023-12-01].

Lepší přístup k elektronickým důkazům pro boj proti trestné činnosti. Consilium.europa.eu. Online. 2023. Dostupné z https://www.consilium.europa.eu/cs/policies/e-evidence/ [cit. 2024-01-04].

RYAN-MOSLEY, Tate. How to hack a smart fridge? Technologyreview.com. Online. 8.5.2023. Dostupné z: https://www.technologyreview.com/2023/05/08/1072708/hack-smart-fridge-digital-forensics/ [cit. 2023-12-01].

JELÍNEK, Jiří. K chybějící právní úpravě tzv. prostorového odposlechu v trestním řádu. *Bulletin advokacie*. Online. 22.09.2018. č. 7-8. ISSN 1805-8280. Dostupné z: http://www.bulletin-advokacie.cz/k-chybejici-pravni-uprave-tzv.-prostoroveho-odposlechu-v-trestnim-radu [cit. 2024-04-04].

Rekodifikace procesních předpisů. Justice.cz. Online. Dostupné z: https://justice.cz/web/msp/rekodifikace [cit. 2024-03-25].

SOKOL, Tomáš. Povinnost dle §7b trestního řádu z pohledu advokáta. *Advokátní deník*. Online. 18.10.2019. č. 9. ISSN 2571-3558. Dostupné z: https://advokatnidenik.cz/2019/10/18/povinnost-dle-%C2%A7-7b-trestniho-radu-z-pohledu-advokata/ [cit. 2024-04-10].

TOMAN, Petr. Podstrčený paragraf 7b trestního řádu – kde se vzal a o čem je. *Advokátní deník*. Online. 22.7.2019. ISSN 2571-3558. Dostupné z: https://advokatnidenik.cz/2019/07/22/podstrceny-paragraf-7b-trestniho-radu-kde-se-vzal-a-o-cem-je/ [cit. 2024-04-09].

VANTUCH, Pavel. Kdy může obhajoba důkazy vyhledat, kdy předložit a kdy jen navrhnout jeho provedení. *Bulletin advokacie*. Online. 02.10.2013. ISSN 1805-8280. Dostupné z: http://www.bulletin-advokacie.cz/kdy-muze-obhajoba-dukaz-vyhledat-kdy-predlozit-a-kdy-jen-navrhnout-jeho-provedeni [cit. 2024-03-28].

3. Seznam použitých právních předpisů

Zákon č. 41/1961 Sb., o trestním řízení soudním

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

Usnesení předsednictva České národní rady č. 2/1993 Sb., Listina základních práv a svobod

Zákon č. 106/1999 Sb., o svobodném přístupu k informacím

Zákon č. 121/2000 Sb., autorský zákoník

Zákon č. 218/2003 Sb., o soudnictví ve věcech mládeže

Zákon č. 480/2004 Sb., o některých službách informační společnosti

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

Zákon č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti

Zákon č. 273/2008 Sb, o Policii České republiky.

Zákon č. 40/2009 Sb., trestní zákoník

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

Sdělení č. 40/2000 Sb. m. s. Ministerstva zahraničních věcí o sjednání Smlouvy mezi Českou republikou a Spojenými státy americkými o vzájemné právní pomoci v trestních věcech

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

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

Zákon č. 287/2018 Sb. kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a některé další zákony

Zákon č. 130/2022 Sb., kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, zákon č. 45/2013 Sb., o obětech trestných činů a o změně některých zákonů (zákon o obětech trestných činů), ve znění pozdějších předpisů, a některé další zákony

Nařízení (EU) 2023/1543 o evropském vydávacím příkazu a evropském uchovávacím příkazu pro elektronické důkazy v trestním řízení a pro výkon trestu odnětí svobody po skončení trestního řízení

4. Seznam použité judikatury

Riley v. California, decided on 29. 4. 2014, 573 U.S. 373.

Nález ÚS ze dne 12. 10. 1994, sp. zn. Pl. ÚS 4/94.

Nález ÚS ze dne 1. 3. 2000, sp. zn. II. ÚS 517/99.

Nález ÚS ze dne 28. 3. 2002, sp. zn. IV. ÚS 2/02.

Usnesení NS ze dne 15. 3. 2005 sp. zn. 5 Tdo 291/2005

Usnesení NS ze dne 3. 5. 2007, sp. zn. 5 Tdo 459/2007.

Usnesení ÚS ze dne 8. 2. 2010, sp. zn IV. ÚS 2425/09.

Usnesení ÚS ze dne 20. 10. 2011, sp. zn. II. ÚS 143/06.

Usnesení ÚS ze dne 3. 10. 2013, sp. zn. ÚS 3812/12.

Nález ÚS ze dne 30. 10. 2014, sp. zn. III. ÚS 3844/13.

Usnesení NS ze dne 12. 11. 2014, sp. zn. 5 Tdo 1136/2014.

Nález ÚS ze dne 14. 5. 2019, sp. zn. PL. ÚS 45/17.

Nález ÚS ze dne 28. 5. 2019, sp. zn. III. ÚS 3564/18.

Usnesení NS ze dne 13. 12. 2023, sp. zn. 5 Pzo 10/2023.

Usnesení ÚS ze dne 21. 2. 2024, sp. zn. IV. ÚS 2750/23.

5. Seznam ostatních zdrojů

Aplikační stanovisko Odboru bezpečnostní politiky ministerstva vnitra ze dne 21. 8. 2019. č. j. MV-115844-2/OBP-2019. 2019.

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

CELBOVÁ, Ludmila. Metadata. In: *KTD: Česká terminologická databáze knihovnictví a informační vědy (TDKIV)*. 2003. Praha: Národní knihovna ČR.

DSarman@msp.justice.cz. 2024-04-05. Ministerstvo Spravedlnosti ČR – k dotazu na rekodifikaci trestního řádu. E-mail [osobní komunikace].

JAKUB, Klein. *Dokazování elektronickými důkazními prostředky. Procesní aspekty v trestním řízení*. 2019, Diplomová práce, Univerzita Karlova, Právnická fakulta.

Společné sdělení Evropskému parlamentu, Radě, Evropskému hospodářskému výboru a sociálnímu výboru a Výboru regionů; Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor. 2013. CELEX 52013JC0001.

Výkladové stanovisko Nejvyššího státního zastupitelství č.1/2015 ze dne 26. 1. 2015, sp. zn. 1 SL 760/2014. 2015.

Seznam příloh

Příloha č. (Tabulka č.2)

Přehled nejdůležitějších „zákonných pojistek ochrany práv a svobod“ u vybraných institutů

Procesní úkon	Policejní orgán	Státní zástupce	Soud[178]	Další zákonné „pojistky“ ochrany práv a svobod
Výzva k předložení nebo vydání věci (§78 TrŘ)	Může vyzvat v přípravném řízení.	Může vyzvat v přípravném řízení.	Může nařídit.	1) Právo žádat o vrácení věci. 2) Povinnost vydat písemné potvrzení o převzetí věci nebo opis protokolu. 3) Povinnost se nevztahuje na věc, jejíž obsah se týká okolnosti, o které platí zákaz výslechu. 4) Povinnost upozornit na možné následky nevyhovění.
Odnětí věci (§79 TrŘ)	Může přikázat s předchozím souhlasem státního zástupce; bez předchozího souhlasu jen nesnese-li věc odkladu. Pokud neodnímá věc orgán, který příkaz vydal, vykoná policejní orgán.	Může přikázat v přípravném řízení	Může přikázat.	1) Právo žádat o vrácení věci. 2) Povinnost vydat písemné potvrzení o odnětí věci nebo opis protokolu. 3) Přibrání nezúčastněné osoby (podle možností).
Osobní prohlídka (§83b TrŘ)	Může vykonat, pokud nelze příkaz nebo dosáhnout předem a věc nesnese odkladu nebo jde-li o osobu přistiženou při činu nebo o osobu, na kterou byl vydán příkaz k zatčení. Pokud nevykonává orgán, který příkaz vydal, vykoná policejní orgán	Může přikázat v přípravném řízení.	Může přikázat.	1) Vykonává vždy osoba stejného pohlaví.

[178] V přípravném řízení soudce, v řízení před soudem zpravidla předseda senátu.

Procesní úkon	Policejní orgán	Státní zástupce	Soud[178]	Další zákonné „pojistky“ ochrany práv a svobod
Domovní prohlídka (§82 a §83 TrŘ)	Vykoná prohlídku na příkaz soudce.	V přípravném řízení může dát soudci návrh k nařízení.	Může nařídit.	1) Nutnost přibrat nezúčastněnou osobu. 2) Subsidiární vůči mírnějším úkonům. 3) Ten, u koho se má prohlídka konat, je zpravidla předem vyslechnut. 4) Osoba, u které se prohlídka koná, může být prohlídce přítomna. 5) Příkaz musí být písemný a odůvodněný, doručí se osobě, u níž se prohlídka koná při prohlídce, nebo nejpozději 24 hodin po tom, co je možné doručit. 6) Je-li v prostoru vykonávána advokacie, je třeba přibrat Českou advokátní komoru.
Prohlídka jiných prostor a pozemku (§82 a §83a TrŘ)	Může provést, pokud uživatel prostor nebo pozemků písemně souhlasí nebo pokud příkazu nelze předem dosáhnout a věc nesnese odkladu. Je povinen si bezodkladně dodatečně vyžádat souhlas bez kterého nelze výsledek úkonu použít jako důkaz.	V přípravném řízení může dát soudci návrh k nařízení.	Může přikázat	1) Nutnost přibrat nezúčastněnou osobu. 2) Ten, u koho se má prohlídka konat, je zpravidla předem vyslechnut. 3) Osoba, u které se prohlídka koná, může být prohlídce přítomna. 4) Příkaz musí být písemný a odůvodněný, doručí se osobě, u níž se prohlídka koná. 5) Je-li v prostoru vykonávána advokacie, je třeba přibrat Českou advokátní komoru.

Procesní úkon	Policejní orgán	Státní zástupce	Soud[178]	Další zákonné „pojistky“ ochrany práv a svobod
Zadržení zásilky (§86 TrŘ)	Nemůže přikázat, ale na jeho příkaz může být zásilka pozdržena (neobdrží-li dopravce příkaz státního zástupce nebo soudu do tří dnů, nesmí zásilku dále zadržovat).	Může přikázat v přípravném řízení.	Může přikázat.	
Otevření zásilky (§87 TrŘ)	Může otevřít se souhlasem soudce v přípravném řízení.	Může otevřít se souhlasem soudce v přípravném řízení.	Může otevřít.	
Součinnost podle §7b	Může přikázat s předchozím souhlasem státního zástupce; bez předchozího souhlasu jen nesnese-li věc odkladu.	Může přikázat v přípravném řízení.	Může přikázat.	

Procesní úkon	Policejní orgán	Státní zástupce	Soud[178]	Další zákonné „pojistky“ ochrany práv a svobod
Odposlech a záznam telekomunikačního provozu (§88 TrŘ)	Bez příkazu soudce jen se souhlasem účastníka, a to jen pro trestné činy uvedené v §88, odst.5 TrŘ. Provádí Policie ČR, v součinnosti se subjekty provozujícími veřejné komunikační sítě nebo veřejné dostupné služby elektronických komunikací podle ZEK.	V přípravném řízení může dát soudci návrh k nařízení.	Může přikázat	1) Nutnost přebrat nezúčastněnou osobu. 2) Subsidiární vůči mírnějším úkonům. 3) Příkaz musí být písemný a odůvodněný. 4) Doba provádění nesmí být delší než 4 měsíce (nadřízený orgán může prodlužovat) 5) Nebyly-li zjištěny skutečnosti významné pro trestní řízení, je záznamy nutné zničit. 6) Zaznamenávání komunikace mezi obhájcem a obviněným je nepřípustné. 7) Po pravomocném skončení věci je třeba informovat uživatele o možnosti podat Nejvyššímu soudu návrh na přezkoumání zákonnosti příkazu. 8) Možné nařídit, jen (1) jedná-li se o zločin, na který zákon stanoví trest odnětí svobody s horní hranicí nejméně osm let, (2) jedná-li se o některý z taxativně vyjmenovaných trestných činů uvedených v §88 TrŘ, (3) stanoví-li tak mezinárodní smlouva

Procesní úkon		Policejní orgán	Státní zástupce	Soud[178]	Další zákonné „pojistky“ ochrany práv a svobod
Zjišťování údajů o uskutečněném telekomunikačním provozu (§88a TrŘ)		Bez příkazu soudce jen se souhlasem uživatele, ke kterému se mají údaje vztahovat.	V přípravném řízení může dát soudci návrh k nařízení. Bez příkazu soudce jen se souhlasem uživatele, ke kterému se mají údaje vztahovat.	Může přikázat.	1) Příkaz musí být písemný a odůvodněný. 2) Po pravomocném skončení věci je třeba informovat uživatele o možnosti podat Nejvyššímu soudu návrh na přezkoumání zákonnosti příkazu. 3) Možné nařídit jen jen (1) jedná-li se o zločin, na který zákon stanoví trest odnětí svobody s horní hranicí nejméně tři roky, (2) jedná-li se o některý z taxativně vyjmenovaných trestných činů uvedených v §88a TrŘ, (3) stanoví-li tak mezinárodní smlouva.
Sledování osob a věcí (§158d TrŘ)	odst. 1	Může vykonat samostatně.	Může písemně povolit.	Může povolit.	1) Nelze sledovat komunikaci s obhájcem
	odst. 2	Nemůže vykonat bez povolení, leda by šlo o neodkladný úkon (v takovém případě musí do 48 hodin získat povolení, jinak sledování ukončit a výsledky sledování nepoužít) nebo by s tím výslovně souhlasil ten, do jehož práv má být zasahováno.	Může písemně povolit.	Může povolit.	1) Nelze sledovat komunikaci s obhájcem 2) Lze povolit jen na základě odůvodněné písemné žádosti. 3) Sledování nesmí být povoleno na dobu delší než 6 měsíců. 4) V jiné trestní věci lze získaný důkaz použít jen jedná-li se též o trestní řízení vedené o úmyslném trestném činu.
	odst. 3	Nemůže vykonat bez povolení, leda by s tím výslovně souhlasil ten, do jehož práv má být zasahováno.	Nemůže povolit.	Může povolit.	1) Nelze sledovat komunikaci s obhájcem 2) Lze povolit jen na základě odůvodněné písemné žádosti. 3) Sledování nesmí být povoleno na dobu delší než 6 měsíců. 4) V jiné trestní věci lze získaný důkaz použít jen jedná-li se též o trestní řízení vedené o úmyslném trestném činu.

Elektronický důkaz v trestním řízení

Abstrakt

V momentální době ovlivňují nové technologie snad všechny aspekty našeho každodenního života. Není tak překvapivé, že jejich působení lze pozorovat i v kontextu trestního práva. V souvislosti s novými technologiemi jednak vznikají nové druhy trestné činnosti (popř. je tradiční trestná činnost páchána novým způsobem) a jednak se rozšiřují možnosti, kterými mohou být trestné činy nebo jiné trestněprávně relevantní skutečnosti, odhalovány a dokazovány. Zatímco však rozvoj nových technologií probíhá bezprecedentní rychlostí, legislativa do jisté míry zaostává. Ač trestní zákoník s novými technologiemi alespoň částečně počítá, trestní řád ještě neprošel dlouhodobě diskutovanou rekodifikací a nové technologie jsou v něm upraveny jen velmi kuse. Cílem diplomové práce je tak jednak prokázání hypotézy, že trestní řád nedostatečně reflektuje výzvy, které nové technologie přináší a jednak charakteristika elektronického důkazu, popis toho, jakým způsobem je s ním v rámci dokazování zacházeno a dále též právní analýza vybraných problematických aspektů související především se zajišťováním elektronických dat. Pozornost je krom pojmu elektronického důkazu věnována též dalším souvisejícím pojmům, například: elektronické zařízení, nosič dat a elektronická data. Práce též poskytuje některé obecné výklady, související s dokazováním, zejména je v ní charakterizován proces dokazování a jsou v ní popsány operativně pátrací prostředky a zajišťovací instituty. Zvláštní pozornost je pak věnována analýze ustanovení, jež jsou v souvislosti se zajišťováním elektronických důkazů často používány, ač je jejich vhodnost či správnost do jisté míry diskutabilní. Především se jedná o problematiku zajišťování dat, ať už za současného zajišťování jejich hmotného nosiče nebo bez něj, prolamování hesel, používání prostorového odposlechu a jeho odlišení od poslechu telekomunikačního provozu a v neposlední řadě se práce zaměřuje na tzv. urychlené zajištění dat třetí osobou podle §7b trestního řádu.

Klíčová slova: elektronický důkaz, dokazování, nové technologie v trestním řízení, zajišťování elektronických dat

Electronic evidence in criminal proceedings

Abstract

New technologies are currently influencing almost every aspect of our daily lives. It is therefore not surprising that such influence can also be observed in the context of criminal law. New types of crime are being committed and "traditional crimes" are sometimes being committed in a new way. However, new technologies are also expanding ways by which criminally relevant information can be detected. While the development of new technologies is proceeding at an unprecedented speed, it might be argued that legislation is lagging behind. Although the Criminal Code does take new technologies into account (at least to some extent), the Criminal Procedure Code has not yet undergone the long-discussed recodification and the regulation of new technologies in criminal proceedings is quite loose. The aim of the master thesis is thus to characterize electronic evidence, to describe how it is being handled in the context of criminal proceedings, and to provide a legal analysis of selected problematic aspects related primarily to the impoundage of electronic data. Attention is also paid to concepts related to electronic evidence, such as the perception of electronic device, data carrier and electronic data and their definition in comparison to the term of computer system. The thesis provides some general explanations related to substantiation, especially the characteristics of the process of substantiation and it describes operative search means and seizure of items. Particular attention is then paid to the analysis of provisions that are often used in connection with the impoundage of electronic evidence, although their appropriateness or correctness is to some extent debatable. The thesis describes the issue of securing data, whether with or without securing its data carrier, password cracking, wiretapping (and its distinction from interception of telecommunication) and it also briefly deals with the so-called expedited seizure of data by a third party under §7b of the Criminal Procedure Code.

Key words: electronic evidence, substantiation, new technologies in criminal proceedings, impoundage of electronic data