UNIVERZITA KARLOVA

Právnická fakulta

Jakub Klein

Dokazování elektronickými důkaznímі prostředky

Procesní aspekty v trestním řízení

Diplomová práce

Vedoucí diplomové práce: doc. JUDr. Bc. Tomáš Gřivna, Ph.D.

Katedra trestního práva

Datum vypracování práce (uzavření rukopisu): 8. března 2019

Prohlašuji, že jsem předkládanou diplomovou práci vypracoval 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 188 039 znaků včetně mezer.

Jakub Klein

V Praze dne 10. března 2019

Poděkování za odbornou pomoc, podnětné komentáře, konzultace a vedení práce patří v prvé řadě doc. JUDr. Bc. Tomáši Gřivnovi, Ph.D. Bez něj by tato práce nevznikla.

Velké díky dále patří Miloslavu Keltnerovi, Ivu Kozáčkovi, Barboře Majerové a rodičům za každou připomínku a četné diskuse nad tématem a formou této práce.

Obsah

1 Úvod

Ruku v ruce s rozvojem technologie se velká část komunikace lidí přesunula do virtuálního prostoru, a to zejména do komunikačních kanálů služeb typu e-mailů, SMS, informačních cloudových úložišť, digitálních záznamů kamerových systémů, elektronických platebních systémů, kryptoměn, informačních kanálů soustředících velké množství informací na internetu či na obdobné informační sítě. Společně s těmito médii se i trestní právo muselo vyrovnat se skutečností, že některé formy kriminality budou částečně nebo zcela probíhat ve virtuálním světě. Ve virtuálním světě se tady často budou vyskytovat i důkazy relevantní pro trestní řízení. Pro zajištění těchto důkazů je potřeba specifických mechanismů trestního práva procesního, a to zejména mechanizmů, při nichž jsou zajištěny podmínky pro spravedlivý proces tak, aby mohl orgán činný v trestním řízení vydat kvalifikované rozhodnutí.

Trestní řád se k existenci elektronických důkazů přímo nevyjadřuje, dle § 89 zákona č. 141/1961 Sb., o trestním řízení soudním, ve znění pozdějších předpisů[1] (dále jako „trestní řádu" či zkráceně „tr. ř.") za důkaz může sloužit vše, co může přispět k objasnění věci, zejména výpovědi obviněného a svědků, znalecké posudky, věci a listiny důležité pro trestní řízení a ohledání. Tento demonstrativní výčet důkazů, které může pro potřeby trestního řízení navrhovat jak orgán činný v trestním řízení, tak i obviněný či další oprávněné osoby v rámci trestního řízení, dává možnost opatřovat důkazy i ve formě elektronické. Zásadním dělícím prvkem, který elektronické formy důkazů odlišuje od prostředku „*klasického důkazu*", je jeho neurčitá povaha, respektive povaha informace s potenciální důkazní hodnotou. Elektronická informace není typickým listinným důkazem, přestože ze své podstaty může takovou podobu mít (např. vytištěný strojový kód). Není však ani typickým věcným důkazem, protože samo zachycení informace, byť na trvalý neměnitelný nosič (např. papír), je jednak nepraktické, ale hlavně pro, případné předvádění důkazu před soudem nevypovídající, navíc sama povaha elektronické informace předpokládá její nestabilitu v čase. Elektronický důkaz tak ve své informační podstatě představuje specifický druh nehmotného věcného důkazu, se kterým si ne vždy procesní strany dokáží jednoduše poradit. Pro praktické hodnocení elektronických důkazů je nutné poukázat na to, že trestní řád nijak nevylučuje

[1] Tato práce zahrnuje změny trestního řádu, trestního zákoníku a některých dalších předpisů provedenou novelou, zákonem č. 287/2018 Sb., kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a některé další zákony vstoupivší v účinnost 1. února 2019.

přípustnost některých důkazních prostředků především vyjma omezení daných § 89 tr. ř. a důkazů opatřených či provedených v rozporu se zákonem.

Soudy v České republice nejsou dle zásady volného hodnocení důkazů zpravidla vázány ničím jiným, než zákonností a vlastním přesvědčením.[2] To samé platí pro důkazy, které mají svůj původ v elektronické informaci. Obecně platí, že „*při aplikaci práva je nutné zajistit materiální pravdu do míry, o níž můžeme na základě konkrétních okolností prohlásit, že nám ohledně minulého děje vytváří praktickou jistotu*."[3] U elektronických důkazů je situace s nakládáním s důkazy složitější hlavně z důvodu chybějící specifické procesní normy, která by nakládání s nimi upravovala. Judikatorně ani legislativně není zcela jasné, jakým způsobem má být s elektronickými důkazy nakládáno. Tyto vady trestního práva procesního mohou mít za následek prohlášení některých důkazů, leč získaných v dobré víře, za relativně či absolutně neúčinné. A naopak mohou být důkazy, které nebyly získány a zajištěny po právu, nevědomky akceptovány jako zákonně zajištěné a provedené. Takový stav je nežádoucí a v konečném důsledku může být takový důkaz soudem vyhodnocen jako důkaz, který má podstatnou vadu,[4] což může mít za následek nesprávné rozhodnutí orgánu činného v trestním řízení.

Cílem této práce je analyzovat českou právní úpravu a použitelnost institutů souvisejících s dokazováním v trestním řízení ve spojení s elektronickými důkazy. Práce se nejprve zabývá relativně abstraktním pojmem informace a jeho relevancí pro hodnocení důkazů v trestním řízení. Pokračuje přehledem mezinárodních závazků České republiky v oblasti kyberkriminality s důrazem na Budapešťskou úmluvu a Evropskou úmluvou o lidských právech. V dalších kapitolách analyzuje obecné zásady dokazování s přihlédnutím k problematice elektronických důkazů. Kapitola 5 se zabývá instituty zajišťování a provádění důkazů, přičemž každý z analyzovaných institutů zkoumán z hlediska jeho aplikovatelnosti pro elektronické důkazy. Poslední kapitola hodnotí praktické postupy při dokazování vybranými elektronickými nosiči důkazů a hodnotí metodické pokyny Nejvyššího státního zastupitelství, které jsou závazné pro

[2] ŠÁMAL, Pavel, MUSIL, Jan, KUCHTA, Josef, FRYŠTÁK, Marek a KALVODOVÁ, Věra. *Trestní právo procesní. 4. přeprac. vyd.* Praha: C.H. Beck, 2013, s. 385.

[3] STUPKA, Václav. *Data jako důkaz v trestním řízení.* In: POLČÁK, Radim, František PÚRY, Jakub HARAŠTA, Matěj MYŠKA a Václav STUPKA. *Elektronické důkazy v trestním řízení.* Brno: Masarykova univerzita, 2015, s. 100.

[4] Tamtéž.

státní zástupce. Účelem této práce je tak popsat dokazování elektronickými důkazními prostředky v kontextu současné právní úpravy a poskytnout reflexi k problematickým ustanovením a postupům při nedostatečně konkrétní úpravě řádného procesního zajištění a provedení elektronických důkazů v trestním řízení.

2 Povaha informace

Dokazování v trestním řízení je posloupností kroků, které mají vyústit v kvalifikované rozhodnutí o dalším postupu orgánů činných v trestním řízení. Bez řádného dokazování není možné jakkoliv kvalifikovaně rozhodnout. Pokud se však chceme zabývat dokazováním jako elementární součástí trestního řízení a hledáním materiální pravdy v trestním řízení, je potřeba nejprve definovat, co to je informace, jakou má formu a jakým způsobem je nutné nahlížet na informaci ve vztahu k elektronickým důkazům. Pro pochopení specifik elektronických důkazů je tak klíčové si informaci a její faktickou a právní povahu správně definovat. Z této definice je následně možné vyvodit důsledky, které vyplývají ze zjištěných poznatků.

2.1 Teoretické základy povahy informace

Přestože výraz informace je obecně užívaný a každý je schopen pojem informace do jisté míry pochopit a alespoň na příkladech vysvětlit, co se pod ním skrývá, pro právo však může být relativně složité jej definovat. Euroatlantická kultura založená primárně na vědeckém zkoumání problémů a na jejich následné aplikaci do života se musí srovnat se skutečností, že informace je nejasný a často i nestálý pojem a závěry vyplývající z interpretace dat mohou být v každou chvíli vyloženy jiným způsobem[5]. Tato nestálost interpretace informace je dána jak problematikou subjektivních názorů osoby, která informace interpretuje,[6] tak i skutečností, že relevance některých informací a objektivní poznatky společnosti se s časem mění. I z toho důvodu je důležité na informaci hledět jako na entitu, která nemá stejné vlastnosti v každém okamžiku a v každém jediném místě.

Informaci, z latinského *in-formatio*, tedy ztvárnění či vytváření, lze definovat mnoha způsoby, pro účely této práce je však příhodná následující definice, která vychází z informatiky, konkrétně pak

[5] II. Senát Ústavního soudu v nálezu sp. zn. II. ÚS 2587/18 ze dne 25. února 2019 potvrdil nutnost kontroly aplikace nejaktuálnějších vědeckých postupů v trestním řízení ve vztahu k potenciální obnově řízení: „*Nový vědecký poznatek, který se vztahuje k zásadnímu důkaznímu prostředku použitému v trestním řízení, je přitom novou skutečností ve smyslu § 278 odst. 1 trestního řádu. V rámci obnovovacího řízení tak může metodika sloužit jako důkazní prostředek při dokazování procesní podmínky řízení, tj. dokazování, zda jsou splněny podmínky pro konání obnoveného řízení.*“

[6] POLČÁK, Radim. *Důkaz a informace*. In: POLČÁK, Radim, František PÚRY, Jakub HARAŠTA, Matěj MYŠKA a Václav STUPKA. *Elektronické důkazy v trestním řízení.* Brno: Masarykova univerzita, 2015, s. 26.

z díla Norberta Wienera, který tvrdil, že „*informace je opakem entropie.*“[7] Pro účely elektronických důkazů je tento poznatek klíčový, neboť právě vyrušení náhodných a rušivých elementů je klíčovým postupem pro správnou a pravdivou interpretaci důkazu. Jestliže tedy má sdělení entropickou formu, ze které nelze jednoznačně odfiltrovat informaci, nemá takové sdělení jakoukoliv vypovídací hodnotu. Na druhou stranu kvalitní informace, tedy informace, ze které lze dovodit jednoznačné závěry, může být pro osobu, která ji interpretuje, způsobilá stát se důkazem.

2.2 Vypovídací hodnota informace

Jedním z atributů informace je její vypovídací hodnota. Z čistě praktického hlediska je informace, která neposkytne žádný relevantní podnět, zbytečná. Pro účely trestního řízení je navíc klíčové zajistit, aby informace, kterou orgán činný v trestním řízení interpretuje, byla v relativně blízké souvislosti se skutkem, nebo s okolnostmi, které jsou rozhodující pro posouzení viny, trestu a splnění požadavků pro trestní odpovědnost.[8] Pokud tedy informace není pouze „bílým šumem“, je pro účely trestního řízení vždy nutné posoudit její relevanci.

Orgán činný v trestním řízení je povinen zhodnotit všechny relevantní důkazy, a to jak důkazy ve prospěch obžalovaného, tak důkazy, které hrají v jeho neprospěch. [9] Samotná vypovídají hodnota důkazu je už vždy odvislá od podmínky zjištění materiální pravdy v rámci trestního řízení a zásady volného hodnocení důkazů orgánem činným v trestním řízení.[10] Aby orgán dokázal vyhodnotit informaci, musí si bezpodmínečně odpovědět na otázku, zda se skutečně jedná o informaci, která má souvislost s trestním řízením, respektive zda se jedná o informaci, která je způsobilá vnést do případu nové podněty.

---

[7] WIENER, Norbert. *Cybernetics Or On the Control and Communication in the Animal and the Machine.* Cambridge: MIT Press, 1961, str. 11. Entropii se rozumí neuspořádanost, nahodilost výskytu, viz např. definice entropie v online encyklopedii Wikipedia: *Entropia*. Dostupné z URL: https://cs.wikipedia.org/wiki/Entropie, datum přístupu: 21. ledna 2019.

[8] Srov. § 89 tr. ř

[9] Srov. § 2 odst. 5 tr. ř

[10] MULÁK, Jiří. *Základní zásady trestního řízení a právo na spravedlivý proces.* Praha: 2018, disertační práce: Univerzita Karlova, Právnická fakulta. In: JELÍNEK, Jiří a kol. *Dokazování v trestním řízení v kontextu práva na spravedlivý proces*. Praha: Leges, 2018, s. 145.

Jak píše Polčák: „[…] *skutkový stav je přímým důsledkem dosažení praktické jistoty. Jedná se o komplexní skutkovou informaci, na jejímž základě je v řízení přímo konstruován právní imperativ.*“[11] Jednotlivé informace tedy pomocí procesu dokazování vytváří přibližný otisk skutku, který se v minulosti stal. Je pak úkolem orgánů činných v trestním řízení tomuto otisku dát co nejkonkrétnější kontury, právě taková interpretace jednotlivých dílčích informací je klíčová pro řádné zjištění skutkového stavu.

Polčák dále formálně rozlišuje tři právní skutečnosti, podle kterých je relativní pravda, tj. právě otisk skutečnosti, konstruována. Jedná se o *předpokládané skutečnosti*, *známé skutečnosti* a *prokazatelné skutečnosti*. Předpokládané skutečnosti jsou okolnosti, které se zpravidla dokazovat nemusí. Jedná se o skutečnosti, které obvykle vyplývají z platného práva. V rámci předpokládaných skutečností rozlišujeme domněnky a fikce. Domněnka typicky vychází z určité zákonem předpokládané skutečnosti, která se ve světě realizuje (např. domněnka otcovství). Můžeme rozlišovat domněnky vyvratitelné a nevyvratitelné, ty se však objevují a v rámci aplikace práva uplatňují spíše výjimečně.[12] Fikce jsou na druhou stranu specifické svojí relativní odpoutaností od skutečnosti. Fikce totiž mohou (a často i bývají) na rozdíl od ostatních informací zcela v rozporu se skutkovým stavem. Zákonodárce stanovuje zákonem určenou fikci zejména v případech, kdy je nutné autoritativně stanovit skutkový stav bez ohledu na ostatní skutečnosti. V trestním právu se s fikcemi setkáváme zejména v souvislosti s výkonem trestu (např. § 106 tr. zák. stanovuje, že v případě zahlazení odsouzení se na pachatele hledí, jako by nebyl odsouzen) nebo při doručování (např. § 64 odst. 5 tr. ř.: „*Nevyzvedne-li si adresát písemnost do deseti dnů od uložení, považuje se poslední den této lhůty za den doručení.*“). Fikce, přestože mohou být v rozporu s objektivní realitou, zpravidla nedávají možnost důkazu opakem,[13] neboť ze své podstaty připouštějí, že ke skutečnosti, kterou postulují, nemusí dojít. Takovým příkladem je i zmiňované ustanovení § 106 tr. zák., neboť je v rozporu s objektivní realitou. Pachatel byl odsouzen (soud disponuje pravomocným rozsudkem o vině a trestu), přesto se na něj po vykonání trestu hledí, jako by nikdy odsouzen nebyl.

[11] POLČÁK, Radim. *Důkaz a informace.* In: POLČÁK, Radim, František PÚRY, Jakub HARAŠTA, Matěj MYŠKA a Václav STUPKA. *Elektronické důkazy v trestním řízení.* Brno: Masarykova univerzita, 2015, s. 41.
[12] GERLOCH, Aleš. *Teorie práva. 7. vydání.* Plzeň: Aleš Čeněk, 2017, s. 207.
[13] Tamtéž.

Známé skutečnosti nejsou zpravidla předmětem dokazování, neboť by se jednalo o nadbytečnou činnost orgánů činných v trestním řízení. Polčák dělí[14] skutečnosti známé na notoriety, typicky skutečnosti obecně známé veřejnosti, oficiality, skutečnosti, které je orgán činný v trestním řízení povinen znát dle zásady *iura novit curia*, a skutečnosti, které orgán činný v trestním řízení zná z rozhodovací praxe své nebo jiných orgánů, typicky jsou to například dřívější odsouzení obviněného. Skutečnosti známé, jejichž existence není podrobena myšlenkovému postupu hodnocení důkazů, orgán zpravidla pouze konstatuje a v rámci dokazování či odůvodnění na ně odkáže.

Klíčovým projevem skutkového stavu pak jsou *prokazatelné skutečnosti*, tedy informace, jejichž pravdivost, vypovídací hodnotu a relevanci je nutné podrobit hodnotícímu soudu, tedy dokazování. Jestliže trestní právo pracuje s nevyvratitelnými domněnkami a fikcemi, nejsou takové skutečnosti relevantní pro samotné dokazování o vině a trestu, ale zpravidla se jedná o skutečnosti, které leží mimo trestní právo (např. domněnka otcovství dle občanského zákoníku), či se týkají konkrétních skutečností, které mohou být výhodné pro obviněného.[15] Trestní právo nemůže otázky důležité pro rozhodnutí, tedy i průběh samotného dokazování, formalizovat a zjednodušit pomocí nevyvratitelných domněnek a fikcí, protože by se z rozhodování stal pouhý formální generátor rozhodnutí a soud by zcela popřel zásadu zjištění materiální pravdy.

2.3 Informace a odvozená informace

S nástupem internetu a efektivnějších a rychlejších metod datové analýzy se značně rozšířila možnost orgánů činných v trestním řízení využívat pro vyšetřování trestné činnosti odvozené informace, také nazývané jako *metadata*. Metadata se dají definovat jako vlastnosti elektronického

[14] POLČÁK, Radim. *Důkaz a informace.* In: POLČÁK, Radim, PÚRY, František, HARAŠTA, Jakub a kol. *Elektronické důkazy v trestním řízení. 1. vydání.* Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 43

[15] Jestliže trestní právo procesní pracuje s fikcemi mimo trestní řád, často se jedná o fikce statusové, o takových skutkových věcech nemůže rozhodovat soud v trestním řízení (srov. § 9 tr. ř. o posuzování předběžných otázek). Další problematikou týkající se dokazování, které může být v rozporu s materiální pravdou je problematika tzv. odklonů (srov. §175a) a zjednodušeného řízení (srov. § 314d odst. 2 tr. ř.), kdy součástí rozhodnutí, respektive skutkového stavu se může stát okolnost, která nemá oporu v realitě, vice viz PROVAZNÍK Jan. *Trestněprocesní ingerence do podmínek trestní odpovědnosti.* Brno: Právní rozhledy 2015, 8, s. 283.

dokumentu či souboru (např. e-mailu, internetové stránky, PDF souboru…), případně soubor takových dat, které přímo neobsahují informace týkající se obsahu takového dokumentu, ale popisují charakteristiky, kterými se dokument navenek projevuje.[16] Legální definic metadat nabízí § 3 odst. 10 zákona o svobodném přístupu k informacím[17], jsou to „*data popisující souvislosti, obsah a strukturu zaznamenaných informací a jejich správu v průběhu času.*“ Přestože je aplikovatelnost této definice omezena pouze pro účely zákona o svobodném přístupu k informacím, lze jí dle mého názoru rozšířit i na další právní předpisy, například na trestní právo. Vztah dat dokumentu a jeho metadat lze popsat jako vztah mezi obsahem popsaného papíru, typovými znaky papíru, na kterém je zpráva napsaná, tedy například jeho gramáž, použitý font, barva, či chemické složení inkoustu.[18] Výhodou analýzy metadat je, že uživatel často nemá ponětí, že se tyto údaje při elektronickém styku generují. Metadata jsou relativně širokým pojmem a mohou zahrnovat jak informace o jednotlivém dokumentu, tak i informace generované například při provozu telekomunikačních sítí.

Z právního hlediska existují metadata do jisté míry v šedé zóně, neboť není vždy jednoznačné, jaká data orgán činný v trestním řízení tímto může získat a zejména jakým způsobem. Kvalitní analýza metadat totiž může o původním uživateli odhalit více, než by se na první pohled mohlo zdát. Typickým příkladem budiž lokalizační data v aplikaci, která periodicky snímá GPS souřadnice uživatele mobilního telefonu. Jestliže není takový mobilní telefon zaheslovaný a byl-li odebrán (viz kapitola 5.2) obviněnému postupem dle trestního řádu, tedy se souhlasem státního zástupce, je sporné, zda může policejní orgán využít tato metadata bez souhlasu soudu, neboť se jednoznačně jedná o zásah do soukromí obviněného a takový zásah do ústavně garantovaných práv je možný pouze se souhlasem soudu. Podobných problémů s daty, která se analyzují, aniž by k tomu příslušný orgán měl řádné oprávnění, může být mnoho. Například soubor uložený na veřejně přístupném úložišti, který by byl sám o sobě zašifrovaný, bez speciálního postupu zajistit.[19]

[16] SCHAFER Burkhard, MASON, Stephen. *The characteristics of electronic evidence.* In: MASON, Stephen, SENG, Daniel. *Electronic Evidence, Fourth edition*. London: University of London, Institute of Advanced Legal Studies for the SAS, 2017, s. 27.

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

[18] SCHAFER Burkhard, MASON, Stephen. *The characteristics of electronic evidence.* In: MASON, Stephen, SENG, Daniel. *Electronic Evidence, Fourth edition*. London: University of London, Institute of Advanced Legal Studies for the SAS, 2017, s. 27.

[19] Takovým zajišťovacím institutem může být např. postup dle § 158d tr. ř., viz kapitola 5.2.

Uživatelský obsah zpravidla nelze považovat za veřejně dostupný, jeho metadata (tedy například čas posledního uložení, nebo formát dokumentu) však už informací soukromou být nemusí.[20]

Specifickou formou elektronických dat jsou data a postupy, které uživatelům umožňují pohybovat se v prostředí relativně anonymně, případně elektronické dokumenty zabezpečit šifrováním,[21] které znemožní či znesnadní třetí osobě přístup ke čtení obsahu dokumentu. Zvláštním fenoménem jsou tzv. kryptoměny, zejména Bitcoin. Prostředky sloužící k anonymizaci, např. VPN sítě (*Virtual Private Network*) a internetové protokoly (například TOR[22]), které provozovateli služby elektronické komunikace a zprostředkovaně i orgánům činným v trestním řízení znemožní sledování uživatelovy aktivity na internetu a omezí možnost jejich možnost zjistit, na jaké internetové stránky uživatel přistupuje a s jakými vzdálenými servery komunikuje. Používání anonymizačních nástrojů není zakázané, přestože některé státy[23] využívání například VPN sítí striktně omezují. Pro některé osoby, které pracují s citlivými osobními údaji, dokonce může být užití zabezpečovacích technologií klíčové (například advokáti, bezpečnostní složky). Pro orgány činné v trestním řízení však může používání těchto nástrojů představovat značnou komplikaci, zejména pak při vyšetřování sofistikované trestné činnosti. Navíc zde objektivní zájem společnosti na objasnění trestné činnosti naráží na princip ochrany soukromí jednotlivce definovaný v Listině

[20] Metadata mohou různou měrou vypovídat o soukromí člověka. Zatímco metadata, která jsou striktně technického charakteru (např. různé statistiky návštěvnosti internetových stránek a vytíženosti), jsou zpravidla charakteru nepodléhajícího jakékoliv speciální ochraně, data, ze kterých lze dovodit skutečnosti, které mají soukromý charakter, je třeba považovat za soukromá. Mezi data, která podléhají ochraně, patří rovněž data jinak utajovaná, srov. POLČÁK, Radim, PÚRY, František, HARAŠTA, Jakub a kol. *Elektronické důkazy v trestním řízení. 1. vydání.* Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 107. Soukromí dat, respektive ochranu osobních údajů je nutné interpretovat i v souvislosti s právní úpravou zpracování osobních údajů, zejména pak s nařízením Evropského parlamentu a Rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (známé jako „GDPR“) a směrnicí Směrnicí Evropského parlamentu a Rady (EU) 2016/680, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů a o volném pohybu těchto údajů.

[21] „*Šifrováním nástroj či postup, pro převedení obsahu komunikace do takové podoby, aby pouze zamýšlený adresát jej mohl převést zpět a rozumět mu*“ PERKINS, Aaron. *Encryption Use: Law and Anarchy on the Digital Frontier.* Houston: Houston Law Review, 2005, 41(5). s. 1627 [autorův překlad].

[22] Zkratka je akronymem anglického T*he Onion Network*, jedná se o technologii, která je založená na distribuovaném zabezpečení a přesměrovávání připojení přes velké množství serverů, což případné sledování připojení činí obtížné. MORRILL, R. Daniel. *An Investigation of the Digital Millennium Copyright Act (DMCA) and the Applicability to the Darknet: An Ex Post Facto Quantitative Non-Experimental Study.* San Diego: Northcentral University, 2016, s. 4.

[23] Čínská lidová republika následovaná Ruskou federací a dalšími zeměmi omezily možnosti využití VPN kombinací technických a represivních opatření. ARTHUR, Charles. China Cracks Down on VPN Use. Guardian News [online]. London: The Guardian, 2011, 12. května 2011 [cit. 2019].

základních práv a svobod[24] (dále je „Listina“) v čl. 7 odst. 1. S rozšířením šifrování mezi běžné lidi však lze předpokládat, že nastane tlak, aby obvinění mohli být donuceni ke sdělení bezpečnostního hesla, případně aby společnosti, které šifrování či anonymizaci zajišťují, byly povinny zajistit bezpečnostním složkám tzv. *backdoor*[25], tedy skrytý přístup k uživatelským datům.

2.4 Důkaz a informace

Jak již bylo zmíněno výše, elektronická data lze chápat jako dosud neinterpretovanou množinu informací. Jejich vypovídací hodnota vychází z interpretace pomocí sdělovacího prostředku, např. počítačového programu nebo jiného zobrazovacího prostředku. Tím pádem není možné posoudit důkaz bezprostředně.[26] To samozřejmě přináší nejeden problém do rozhodovacího procesu subjektů trestního řízení, neboť tyto osoby zpravidla nejsou dostatečně expertně nadáni, aby posoudili, zda technologické hledisko pramenu důkazu a užitý důkazní prostředek splňují kritéria, která na ně trestní řád klade. Typickým příkladem elektronického důkazu, který má ve vnějším světě diametrálně odlišnou podobu od světa elektronického, je internetová stránka. Zdrojový kód, nejčastěji ve formě Hypertext Markup jazyka (zkráceně známější pod zkratkou „*html*“), se významně liší od zobrazované formy a pro laika může být téměř nečitelný. Zobrazovací metoda (např. pomocí internetového prohlížeče) může volbou rozlišných nestandardizovaných řešení dramaticky změnit i zobrazovací rozsah informací.[27] Řešením může samozřejmě být posuzování jednotlivých zobrazovacích prostředků a funkce každého programu či zdrojového kódu znalcem, ovšem tato metoda se přinejmenším ve větším měřítku jeví jako nehospodárná

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

[25] Tajný program pod označením PRISM americké bezpečnostní agentury NSA zveřejnil Edward Snowden, NSA se souhlasem amerického soudu prováděla sběr informací, zejména metadat, některé americké společnosti (např. Microsoft, Google či Apple) umožnily NSA instalaci *backdoor*, která obcházela uživatelské šifrování, srov. GREENWALD, Glenn, Ewen MACASKILL, Laura POITRAS, Spencer ACKERMAN a Sominic RUSHE. Microsoft handed the NSA access to encrypted messages. The Guardian [online]. Londýn: The Guardian, 2013, 12. června 2013 [cit. 2019].

[26] STANFIELD, Allison, MASON, Stephen. *Authenticating electronic evidence.* In: MASON, Stephen, SENG, Daniel. *Electronic Evidence, Fourth edition*. London: University of London, Institute of Advanced Legal Studies for the SAS, 2017, s. 196.

[27] Různé prohlížeče mohou stránky zobrazit jiným způsobem, nejčastěji se jedná o posuny různých grafických objektů, ale změny mohou být signifikantnější, viz např. SLEGG, JENNIFER. *Google: Issues When Serving Different HTML & Content to Different Browsers.* TheSEMPost [online]. 2015, 11. září 2015 [cit. 2019]..

a nepřiměřeně zdlouhavá. Doktrína, zejména anglosaská[28], ale i kontinentální[29], však na software zpravidla pohlíží jako na spolehlivý zdroj informace. Přestože trestní řád elektronická data jako speciální důkazní prostředek nezná, obecná rozhodovací praxe se využívání tzv. spolehlivých důkazních prostředků zpravidla nebrání[30] a logicky jejich použití ve spojení se zásadou volného hodnocení důkazů.

[28] SCHAFER Burkhard, MASON, Stephen. *The characteristics of electronic evidence.* In: MASON, Stephen, SENG, Daniel. *Electronic Evidence, Fourth edition*. London: University of London, Institute of Advanced Legal Studies for the SAS, 2017, s. 22.

[29] Například § 562 odst. 2 obč. z. předpokládá, že elektronickou evidenci je třeba zpravidla pokládat za spolehlivou, tedy způsobilé být řádným důkazem, jsou-li prováděny systematicky, posloupně a jsou-li chráněny proti změnám.

[30] POLČÁK, Radim. *Důkaz a informace.* In: POLČÁK, Radim, PÚRY, František, HARAŠTA, Jakub a kol. *Elektronické důkazy v trestním řízení. 1. vydání.* Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 43

3 Mezinárodní úprava

S rostoucí důležitostí informačních technologií si mezinárodní komunita dala za cíl kodifikovat základní principy boje s kriminalitou, která se čím dál více posouvala do virtuálního a do té doby právně hůře uchopitelného prostoru. I z toho důvodu s rozvojem internetu a internetové kriminality pokládala za klíčové stanovit hmotněprávní a procesněprávní základy odpovědnosti na internetu. Jak bylo popsáno v první kapitole, kyberprostor nezná konvenční státní hranice a stíhání jednotlivých trestných činů a zajišťování důkazů může být nemožné. I proto vznikla v souvislosti se snahou účinně bojovat proti kyberkriminalitě Budapešťská úmluva. Nejprve je však nutné se zabývat jiným dokumentem Rady Evropy, Evropskou úmluvou o lidských právech (dále „EÚLP"), který Tvoří základ systému ochrany lidských práv v Evropě a je důležitý pro aplikaci a výklad zásadních ustanovení Listiny a trestního řádu orgány činnými v trestním řízení, obecnými soudy i Ústavním soudem.

3.1 Evropská úmluva o lidských právech

Základním lidskoprávním dokumentem, který má v České republice přímou aplikovatelnost[31] je evropská Úmluva o ochraně lidských práv a základních svobod. Ve vztahu k procesním aspektům elektronických důkazů, respektive k dokazování v trestním řízení obecně, je třeba hledat odpověď na přípustnost důkazů v článku 6 EÚLP, který obecně upravuje právo na spravedlivý proces. Pro důkazy jako pramen poznání skutku jsou klíčová následující ustanovení:

> *(1) Každý má právo na to, aby jeho záležitost byla spravedlivě, veřejně a v přiměřené lhůtě projednána nezávislým a nestranným soudem zřízeným zákonem, který rozhodne o jeho občanských právech nebo závazcích nebo o oprávněnosti jakéhokoli trestního obvinění proti němu.* […]
>
> *(2) Každý, kdo je obviněn z trestného činu, se považuje za nevinného, dokud jeho vina nebyla prokázána zákonným způsobem.*
>
> *(3) Každý, kdo je obviněn z trestného činu, má tato minimální práva:* […]

[31] Jednak prostřednictvím stížnosti u ESLP, jednak je žádoucí, aby výklad práva byl v souladu s mezinárodními závazky České republiky, zejména pak mezinárodními smlouvami týkajícími se lidských práv. Srov. nález Ústavního soudu č. 403/2002 Sb. dne 25. června 2002.

d) vyslýchat nebo dát vyslýchat svědky proti sobě a dosáhnout předvolání a výslech svědků ve svůj prospěch za stejných podmínek, jako svědků proti sobě […]

Evropský soud pro lidská práva (dále jen „ESLP“) chápe právo na spravedlivý proces ve vztahu k trestnímu právu jako „*základní ochranný štít pro ty, vůči kterým jsou nástroje trestního práva namířeny, tedy osobám obviněným ze spáchání trestné činnosti*.“[32] Přestože EÚLP ustanovení zabývající se dokazováním a přípustností důkazů přímo neobsahuje, právě právo na spravedlivý proces zaručuje, že bude dodržen zákonný postup při dokazování. Princip zákonnosti je upraven v čl. 6 odst. 2 EÚLP. Jak podotýká Vostrá, EÚLP nestanovuje důvody přípustnosti a hodnocení důkazů, předmětem ochrany je spravedlivý proces jako celek.[33]

Dalším důležitým ustanovením EÚLP je čl. 8, který chrání právo na respektování soukromého a rodinného života:

(1) Každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence.

(2) Státní orgán nemůže do výkonu tohoto práva zasahovat kromě případů, kdy je to v souladu se zákonem a nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných.

Důkazy, které orgány činné v trestním řízení zajišťují, jsou často zásahem do soukromé sféry osoby. Ustanovení tohoto článku jsou považována za tzv. relativní práva[34], neboť obvykle přichází do rozporu s jinými právy uvedenými v EÚLP. I z toho vyplývá, že při aplikaci čl. 8 je vždy třeba postupovat obezřetně a aplikovat test proporcionality zejména při řešení otázky zásahu veřejné moci do soukromí v souvislosti s trestním řízením (nejčastěji soukromí obviněných). I proto je třeba dbát, aby zásah do soukromí obviněných byl proveden jen v nezbytně nutné míře, vyvážené

[32] KMEC, Jiří. *Kapitola XVI. Právo na spravedlivý proces (čl. 6 EÚLP).* In: KOSŘAŘ, Jiří, KRATOCHVÍL, Jan a BOBEK, Michal. *Evropská úmluva o lidských právech: komentář.* Praha: C.H. Beck, 2012, s. 565.

[33] VOSTRÁ, Zuzana. *Vybrané doktríny ESLP a jejich vliv na proces dokazování*. In: JELÍNEK, Jiří a kol. *Dokazování v trestním řízení v kontextu práva na spravedlivý proces*. Praha: Leges, 2018, s. 44.

[34] VOSTRÁ, Zuzana. *Vybrané doktríny ESLP a jejich vliv na proces dokazování*. In: JELÍNEK, Jiří a kol. *Dokazování v trestním řízení v kontextu práva na spravedlivý proces*. Praha: Leges, 2018, s. 53.

intenzitou veřejného zájmu na vyšetření trestného činu. V trestním řádu je tak obecným promítnutím čl. 8 EÚLP zásada zdrženlivosti orgánů činných v trestním řízení, která se manifestuje jednak v jednotlivých ustanoveních trestního řádu (srov. např. § 102 odst. 1 tr. ř.: „*Je-li jako svědek vyslýchána osoba mladší než osmnáct let* […] *je třeba výslech provádět zvlášť šetrně a po obsahové stránce tak, aby výslech v dalším řízení zpravidla už nebylo třeba opakovat.")* a obecně v § 52 tr. ř. při provádění jednotlivých procesních úkonů: „*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.*" K aplikaci čl. 8 EÚLP ve vztahu k nepřiměřeným zásahům do soukromí při zajišťování důkazů se vyjádřil ESLP např. v případu Miailhe proti Francii[35], který zdůraznil, že: „[ESLP] *uznává, že státy mohou pokládat za nezbytné použít určitých opatření, jako jsou domovní prohlídky a zabavení věci, aby mohly zajistit důkazy a* […] *stíhat jejich pachatele. Je ale také třeba, aby jejich legislativa a praxe v dané oblasti nabízely adekvátní a dostatečné záruky proti zneužití* […] *Při absenci soudního příkazu byly omezení* […] *stanovené zákonem příliš volné na to, aby zasahování do práv stěžovatelů byla striktně přiměřená sledovanému legitimnímu cíli.*"[36] Právo na soukromí tak není absolutní, stát však musí nastavit přiměřené kontrolní mechanismy (např. přezkum jiným orgánem) a proporcionální omezení, aby byla lidská práva adekvátně šetřena. Právo na soukromý život se může při zajišťování elektronických důkazů objevit v souvislosti s právem na spravedlivý proces. Jako neoprávněný a excesivní zásah státu do soukromého života ESLP vyhodnotil domovní prohlídku bez předchozího příkazu soudu, protože nebyly splněny podmínky neodkladnosti úkonu, který zasahoval do lidských práv stěžovatele. Jestliže se nejedná o zásah, u něhož nelze vyčkat na souhlas soudu, je zajištění počítače bez soudního povolení, kterého dle španělské právní úpravy nebylo třeba, v rozporu se zásadou proporcionality legitimních cílů ochrany společnosti v demokratickém zřízení.[37]

[35] Rozhodnutí Evropského soudu pro lidská práva, Miailhe proti Francii (č. 2), stížnost č. 18978/91, ze dne 26 září 1996.

[36] KRATOCHVÍL Vladimír. *Dopad rozhodnutí evropského soudu pro lidská práva na trestní právo ČR.* Praha: Masarykova univerzita, Právnická fakulta, 2011, s. 44 [materiál k přednáškám].

[37] Rozhodnutí Evropského soudu pro lidská práva, Trabajo Rueda proti Španělsku, stížnost č. 32600/12, ze dne 30. května 2017.

Podobně bylo rozhodnuto o porušení práva na soukromý život ve věci ruského novináře, kterému byla celním orgánem zabavena paměťová karta s fotografiemi k reportáži z Abcházie. Dle ESLP zásah do práv, tedy prohlídka a zabavení paměťové karty, který byl umožněn podzákonným dekretem prezidenta pro boj s extremismem, konstituuje zásah do soukromého života. Mimo konstatování o porušení práva na soukromí soud deklaroval, že dekret nezaručoval dostatečné záruky ochrany a přezkumu.[38] V jiné věci ESLP shledal jako neproporcionální zásah do soukromí spočívající v tajném nahrávání podezřelého orgánem britské policie za účelem jeho pozdější rekognice.[39]

Štrasburský soud do jisté míry vytváří obecný rámec pro uplatňování postupů orgánů veřejné moci. Podle čl. 46 EÚLP jsou rozsudky konstitutivní. Porušení práv stěžovatele však zakládá právo na pokračování řízení ve stádiu, které předcházelo vydání zrušeného rozhodnutí (srov. § 314h tr. ř.).[40] Především však ESLP pomocí rozhodnutí organicky dotváří limity pro uplatňování práv vyplývající z EÚLP, které orgány činné v trestním řízení i normotvůrci musí reflektovat. Pojetí spravedlivého procesu a práva na soukromí je v judikatuře ESLP extenzivní a soud jej zpravidla vykládá v širokých souvislostech umožňujících šetření práv obviněných. I proto by orgány činné v trestním řízení při aplikaci české právní úpravy měly mít na paměti, že každý neproporcionální a nedovolený zásah do práva na spravedlivý proces a práva na soukromý život může mít za následek procesní neúčinnost takového úkonu.

3.2 Budapešťská úmluva

Nejdůležitějším mezinárodním dokumentem ve vztahu ke kyberkriminalitě je bezesporu Budapešťská úmluva.[41] Její význam je zásadní nejen z důvodu autority Rady Evropy jako důležité

[38] Rozhodnutí Evropského soudu pro lidská práva, Ivashchenko proti Rusku, stížnost č. 61064/10 ze dne 13. února 2018.

[39] Rozhodnutí Evropského soudu pro lidská práva, Perry proti Spojenému království Velké Británie a Severního Irska, stížnost č. 63737/00, ze dne 17. června 2003.

[40] Zprostředkovaně skrze zrušení rozhodnutí Ústavního soudu dle zákona o Ústavním soudu.

[41] Úmluva o počítačové kriminalitě byla Českou republikou ratifikována v roce 2011, vyhlášena je pod č. 104/2011 Sb. m. s. Překlad názvu Budapešťské úmluvy v češtině (v angličtině je nazvána "*Convention on Cybercrime"*) vychází dle mého názoru z nedostatku citu a znalostí zákonodárce, neboť počítačová kriminalita je jen částí fenoménu kybernetické kriminality; k Budapešťské úmluvě byla následně přijat ještě dodatkový protokol týkající se problematiky *hate crime* páchané v kyberprostoru, ten však z procesního hlediska oproti Budapešťské úmluvě nepřináší změny.

mezinárodní instituce, ale i skutečností, že se jedná o první ucelený mezinárodní dokument, který si dává za cíl komplexně harmonizovat hmotněprávní a procesněprávní instituty v oblasti trestní politiky jednotlivých států. Budapešťská úmluva ideově navazuje na EÚLP, koncepce Budapešťské úmluvy je však vytvořená tak, aby k ní mohly přistoupit i státy, které nejsou jejími signatáři.[42]

Už při vyjednávání o podobě Budapešťské úmluvy členské státy doufaly, že bude mít dosah i do států, které nejsou členy Rady Evropy, což se nakonec do jisté míry vyplnilo, neboť na počátku roku 2019 ratifikovalo Budapešťskou úmluvu 62 států včetně 19 nečlenských států[43] (jsou jimi například Spojené státy americké, Kanada, Japonsko, Izrael, ale i některé africké státy). Relativně vysoký počet států, které se zavázaly dodržovat závazky vyplývající z Budapešťské úmluvy, je dán mj. záměrem přijmout kompromisní verzi dokumentu.[44]

Přestože se Budapešťská úmluva primárně zabývá hmotným právem, zejména pak definuje jednotlivé skutkové podstaty v souvislosti s kyberzločincem, tak jsou pro účely této práce důležitější principy zakotvené v části druhé Úmluvy. Tato část totiž zakotvuje některé základní instituty řádného zajišťování důkazů a následnou další práci s elektronickými důkazy. Ukládá signatářům, aby do svého právního řádu zapracovali legislativní změny pro realizaci úkonů, které vyžaduje Úmluva.

Mezi tyto úkony patří:

(1) *Urychlené uchovávání uložených počítačových dat a urychlené částečné zpřístupnění provozních dat za účelem zajištění důkazních prostředků v počítačových sítích, respektive lokalizačních údajů typicky spojovaných s daty mobilních operátorů* [čl. 16 a 17 Budapešťské úmluvy]*;*
(2) *příkaz k předložení dat, který upravuje pravomoc orgánů činných v trestním řízení vyžadovat od osob, které disponují daty, které jsou důležité pro trestní řízení, jejich předložení například na datovém nosiči* [čl. 18 Budapešťské úmluvy]*;*

[42] GŘIVNA, Tomáš, POLČÁK, Radim a kol. *Kyberkriminalita a právo.* Praha: Auditorium, 2008, s. 104.
[43] Aktuální stav je dostupný u centrálního depozitáře Rady Evropy.
[44] CLOUGH, Jonathan. *A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation.* Monash University Law Review. Clayton, 2014, 40(3), s. 710.

(3) prohlídka a zajištění uložených počítačových dat je úkonem umožňujícím příslušnému orgánu zajistit data, která jsou důležitá pro řádné provedení úkonů v trestním řízení, a umožňující osobě, která má odborné znalosti, jejich prozkoumání [čl. 19 Budapešťské úmluvy]*;*

(4) shromažďování provozních dat v reálném čase například pomocí sledování počítačové sítě [čl. 20 Budapešťské úmluvy]*; a*

(5) odposlech obsahových dat. [čl. 21 Budapešťské úmluvy]

Všechny výše popsané instrumenty spadají rovněž pod režim ustanovení článků 14 a 15 Budapešťské úmluvy.[45] Tato ustanovení ukládají povinnost je užívat pouze v mezích vnitrostátních předpisů (tedy v mezích stanovených zákony a ústavním pořádkem) a v mezích mezinárodních smluv chránících lidská práva a svobody. Budapešťská úmluva tak přímo odkazuje na základní lidskoprávní dokumenty – EÚLP a Mezinárodní pakt OSN o občanských a politických právech z roku 1966.

Česká republika podepsala Budapešťskou úmluvu v roce 2005, ale ratifikovala ji až v roce 2013. Při pohledu na český právní řád se nabízí otázka, zda Česká republika promítla požadavky vyplývající z Budapešťské úmluvy dostatečně. Co se týče procesněprávních závazků vyplývajících z Úmluvy, nezdá se, že by je zákonodárce v plném rozsahu do české legislativy převedl. Zákonodárce sice v souvislosti s ratifikací Budapešťské úmluvy deklaroval, že právní řád je v souladu s mezinárodněprávními požadavky,[46] ale některé instrumenty jsou z pohledu procesních postupů problematické. Jak podotýká Stupka: „*Aby však mohly české orgány činné v trestním řízení tyto v Úmluvě poměrně detailně popsané procesní úkony realizovat, jsou v současné situaci nuceny v podstatě ‚ohýbat' aktuální instituty trestního práva procesního. Například zajištění dat uchovávaných u ISP se na úrovni jednotlivých policejních obvodů realizuje prostřednictví různých procesních nástrojů, ke sjednocení realizace zajištění e-mailových dat muselo být vypracováno stanovisko Nejvyššího státního zastupitelství a v neposlední řad nástroj, kterým by mohly orgány*

[45] Články 14 a 15 definují rozsah procesních ustanovení, podmínky a záruky včetně postupů a případných výhrad z Budapešťské úmluvy.

[46] Viz např. ratifikační dokumenty úmluvy, 104. Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě, č. 104/2013 Sb. m. s.

činné v trestním řízení přikázat ISP uchovávání uživatelských dat, prakticky neexistuje.“[47] Taková situace je samozřejmě nepříznivá, a to nejen z hlediska mezinárodních závazků České republiky, ale především z hlediska osob, které právo každodenně aplikují. Současný stav tak přináší do procesního zajišťování důkazů element nejistoty.

Z pohledu procesních postupů je třeba zmínit, že Budapešťská úmluva upravuje v čl. 23 a násl. Úmluvy i otázky mezinárodní spolupráce mezi orgány činnými v trestním řízení. Z důvodu komplexnosti mezinárodní a vnitrostátní úpravy není v možnostech této práce se zevrubně touto problematikou zaobírat. Budapešťská úmluva funguje jako doplněk bilaterálních či multilaterálních smluv mezi signatáři. V článku 27 je definován mechanismus nastavující vztah dvou signatářů, kteří mezi sebou nemají uzavřenou smlouvu o mezinárodní justiční spolupráci v trestních věcech.

Z obecného hlediska je samozřejmě příznivé, že Česká republika ratifikovala mezinárodní dokument, který je klíčový pro boj s kyberkriminalitou. Je však zarážející, že zákonodárce nedokázal všechny mezinárodní závazky řádně promítnout do platného práva a praxe tak musí hledat v současném nevyhovujícím stavu kreativní řešení pomocí výkladu. To samozřejmě přináší problémy při aplikaci práva i v rozhodovací praxi, neboť ne vždy musí být jasné, zda orgány činné v trestním řízení postupovaly v souladu se zákonem. Nelze samozřejmě říci, že legislativa České republiky je v zásadním rozporu s Budapešťskou úmluvou (český právní řád například od 1. února 2019 umožňuje tzv. *data freeze*, aplikaci ustanovení článků 16 a 29 Budapešťské úmluvy, viz kapitola 5.2.9). Výklad jednotlivých procesních institutů a s nimi související problematika jsou shrnuty v kapitole 5.2, pojednávající o platném právu.

[47] STUPKA, Václav. *Kyberkriminalita*. In: POLČÁK, Radim. *Právo informačních technologií*, Praha: Wolters Kluwer, 2018, s. 556.

4 Zásady dokazování

Účelem trestního řízení je odhalit a spravedlivě potrestat pachatele skutku, který naplnil znaky trestného činu podle trestního práva hmotného.[48] Účelem procesního práva trestního, zejména pak trestního řádu, je stanovení postupu při realizaci hmotného práva, a to jak během přípravného řízení, tak zejména v řízeních před soudem. K tomu, aby orgány činné v trestním řízení dospěly ke spravedlivému rozhodnutí, musí objektivním způsobem poznat okolnosti skutku, pro který se vede trestní řízení. Takovým institutem poznání je právě dokazování. Orgány činné v trestním řízení Zpravidla nejsou být bezprostředním zdrojem poznání vnější reality (srov. § 30 odst. 1 tr. ř.) a dokazování jim umožňuje na základě podnětů rozhodnout o skutku.

V rámci trestního řádu je dokazování upraveno v hlavě páté, ustanovení § 89 a násl. demonstrativně vypočítávají, jaké okolnosti jsou předmětem dokazování: existence skutku, zda skutek spáchal obviněný, závažnost, osobní poměry pachatele, jaké následky skutek zanechal, zejména ve vztahu k poškozeným, či motiv obviněného. Orgány činné v trestním řízení mohou zjišťovat (a zpravidla tak i činí) další dílčí okolnosti, které souvisejí se skutkem, zejména pak, zda jsou splněny všechny předpoklady trestní odpovědnosti obviněného. Dokazování však nesmí být bezbřehé a okruh otázek, které je potřeba odpovědět v rámci trestního řízení, musí být vždy jasně ohraničený. Na jednu stranu musí umožnit organum činným v trestním řízení spolehlivě zjistit všechny relevantní informace pro vydání rozhodnutí. Na stranu druhou soud musí vždy s přihlédnutím k § 2 tr. ř. zohledňovat požadavek rychlého projednání a rozhodnutí věci v trestním řízení, zásadu hospodárnosti a zásadu šetření práv osob při provádění úkonů, ať už to jsou to výslechy svědků či jiné zásahy do soukromí a integrity osob.

Nelze však zaměňovat postup orgánů činných v trestním řízení před zahájením trestního stíhání dle § 160 odst. 1 tr. ř. a po něm. Ve fázi před zahájením trestního stíhání, zejména v souvislosti s prověřováním, nelze mluvit o dokazování *per se*, neboť součástí institucionalizovaného procesu

[48] JELÍNEK, Jiří. *Trestní právo procesní. 2. vyd. podle novelizované právní úpravy účinné od 1.9. 2011.* Praha: Leges, 2011, s. 21.

dokazování je mj. právo obviněného, případně dalších osob, účastnit se různých úkonů a kontrolovat orgány činné v trestním řízení tak, aby jeho práva byla řádně šetřena.[49]

Podle § 89 odst. 2 tr. ř. může za důkaz sloužit vše, co může přispět k objasnění věci, zejména výpovědi obviněného a svědků, znalecké posudky, věci a listiny důležité pro trestní řízení a ohledání. Zákonodárce tímto značně širokým pojetím důkazu jako poznávacího prostředku v trestním řízení vyjadřuje benevolenci při jeho použití k objasnění skutku, případně dalších okolností (např. osobním poměrům obviněného). Trestní řád tak správně předjímá, že dokazování různými důkazními prostředky může být závislé na stavu vědeckého poznání a stavu technologií.[50]

4.1 Základní zákonné zásady při dokazování

Vzhledem k tomu, že dokazování, respektive následné zjištění skutkových okolností, je klíčovou součástí trestního řízení, je nutné připomenout, že tento specifický instrument je určující pro zjištění skutkového stavu. Jak píše Šámal[51]: „*Účelem dokazování v českém trestním řízení je zjistit skutkový stav věcí, o němž nejsou důvodné pochybnosti, a to v rozsahu, který je nezbytný pro rozhodnutí orgánů činných v trestním řízení* […] *jen takové zjištění* [skutkového stavu] *provedené v dostatečné kvalitě, v potřebném rozsahu a za dodržení všech zákonných požadavků, může vést ke správnému, byť zprostředkovanému poznání skutečnosti* […] *a přesvědčivému rozhodnutí ve věci.*“ Stejně jako v trestním řízení obecně, tak i během dokazování, musí orgány činné v trestním řízení postupovat procesně správně a respektovat základní zásady, kterými se dokazování řídí. Hasch identifikuje[52], že v rámci dokazovaní je nutné primárně respektovat následující zásady: zjištění

[49] Některé úkony mohou orgány činné v trestním řízení provést i před zahájením trestního stíhání, typicky se jedná o neodkladné a neopakovatelné úkony dle § 158 odst. 3, odst. 9 tr. ř., případně úkony související se zkráceným řízením apod. Tyto úkony jsou však zpravidla opatřeny vlastní procesní úpravou, která má zajistit, že práva osob budou šetřena (např. neodkladný a neopakovatelný úkon výslechu svědka, který je procesně použitelný pouze za podmínek stanovených v § 158a tr. ř.).

[50] Srov. nález Ústavního soudu sp. zn. II. ÚS 4266/16 ze dne 27. března 2017, zabývající se problematikou pachových stop a přezkoumatelností vědecké metody za nimi stojící, domnívám se, že toto pravidlo lze užít i pro zkoumání elektronických stop, kdy znalecké zkoumání dat musí být provedeno s ohledem na nejnovější poznatky a užitím nejpřesvědčivější metodologie zkoumání.

[51] ŠÁMAL, Pavel, MUSIL, Jan, KUCHTA, Josef, FRYŠTÁK, Marek a KALVODOVÁ, Věra. *Trestní právo procesní. 4. přeprac. vyd.* V Praze: C.H. Beck, 2013, s. 348.

[52] HASCH, Karel: *Obecné výklady o důkazech.* In: JELÍNEK, Jiří a kol. *Trestní právo procesní. 2. aktualizované vydaní*. Praha: Leges: 2011, s. 354 an.

materiální pravdy, zásadu vyhledávací, zásadu presumpce neviny, zásadu bezprostřednosti a ústnosti a zásadu volného hodnocení důkazů. Jednotlivé zásady dokazování v trestním řízení (společně pak s ostatními zásadami, kterými se řídí trestní právo) nelze vykládat samostatně, ale vždy v kontextu dalších zásad. Některé zásady totiž v konkrétních situacích mohou být ve vzájemném rozporu.

Zásadou zjištění materiální pravdy se rozumí povinnost orgánů činných v trestním řízení zjistit skutkový stav předmětu trestního řízení tak, jak se skutečně udál. Obecně je zásada materiální pravdy upravena v § 2 odst. 5 tr. ř. Komentářová literatura[53] připomíná, že například výpověď obviněného obsahující doznání je pouze jedním z důkazů. Orgány činné v trestním řízení jsou vždy povinny hodnotit důkazy jednotlivě i v souhrnu s dalšími důkazy. Materiální pravdy ve své krystalické podstatě nelze spolehlivě nikdy v trestním řízení dosáhnout, i proto není záhodno tento právní pojem zaměňovat s pojmem filosofickým či pojmem faktického pojetí pravdy.[54] Právo si totiž vždy musí vystačit s jistou dávkou nejistoty, která zpravidla ve sporných situacích nastává.

Zásada vyhledávací vychází stejně jako zásada zjištění materiální pravdy z § 2 odst. 5 tr. ř. Nejšířeji uplatnitelná je v přípravném řízení, kdy jsou orgány činné v trestním řízení povinny vyhledávat důkazy svědčící jak ve prospěch, tak i v neprospěch osoby, proti níž se trestní řízení vede. Orgány činné v trestním řízení (ostatně i další subjekty trestního řízení, nejčastěji obvinění) jsou povinny vyhledávat důkazy, které jsou relevantní a v souladu s procesními postupy, navrhovat je k provedení, či přímo provádět. [55] S ohledem na roli jednotlivých subjektů trestního řízení je důležité si vždy odpovědět na otázku, kdo má procesní odpovědnosti při zjišťování skutkového stavu. Zde se zásada vyhledávací striktně kryje se zásadou presumpce neviny. Je totiž vždy povinností orgánů činných v trestním řízení, aby prokázaly skutkový stav tak, aby o něm nebyly důvodné pochybnosti.

[53] DRAŠÍK, Antonín, FENYK, Jaroslav a kol. *Trestní řád. Komentář I. a II. díl.* Praha: Wolters Kluwer ČR, 2017, s. 14.

[54] JELÍNEK, Jiří a kol. *Trestní právo procesní. 2. aktualizované vydaní*. Praha: Leges: 2011, s. 151.

[55] Povinnost vyhledávat důkazy dalšími subjekty trestního řízení je relativní. Přestože primární odpovědnost zajistit důkazy a prokázat vinu nade vší pochybnosti leží na státním zástupci, i obviněný by měl projevit iniciativu a může se vyjadřovat k jednotlivým důkazům (srov. např. § 33 odst. 1 tr. ř.) a zprostředkovaně i jeho obhájce (srov. 41 odst. 1 tr. ř.), přesto stále platí, že obviněný má právo nevypovídat.

Právě presumpce neviny, jako jedna z nejdůležitějších zásad trestního práva, všem ukládá hledět na osobu, proti níž se vede trestní řízení, jako na nevinnou, dokud pravomocným odsuzujícím rozsudkem není shledána vinnou. V případě dokazování se zásada presumpce neviny projevuje, jak poukazuje Jelínek, tím, že „*vina musí být obviněnému prokázána zákonnými prostředky, obviněný není povinen dokazovat svoji nevinu.*“[56] Jelínek dále zmiňuje, že pouze na základě samotné taktiky obhajoby nemůže orgán činný v trestním řízení dovozovat, že osoba, proti níž se vede trestní řízení, skutek spáchala, což ostatně i vyplývá z judikatury Nevyššího soudu.[57] Procesním důsledkem uplatnění zásady presumpce neviny při dokazování skutkových okolností je pravidlo *in dubio pro reo*.

Zásada bezprostřednosti je typickou zásadou uplatnitelnou zejména při vyhledávání důkazů a dokazování samotném. Jestliže má orgán činný v trestním řízení spravedlivě rozhodnout, tedy zejména s ohledem na hodnověrnost a přesvědčivost jednotlivých důkazů, je žádoucí, aby se dostal co nejblíže původci takového důkazu. Šámal k tomu uvádí[58], že soud má povinnost čerpat důkazy z pramene nebližšího dokazované skutečnosti. Toto platí nejen pro svědecké výpovědi, ale i pro listinné důkazy a další důkazní prostředky, neboť je samozřejmé, že každým stupněm vzdálenosti od zdroje se spolehlivost důkazu zmenšuje. Podobně to platí i pro zásadu ústnosti, která se však plně projevuje až v řízení před soudem.[59]

Zásada volného hodnocení důkazů je ze všech zásad nejabstraktnějším požadavkem. Vychází ze samotného filosofického principu soudce jako nezávislého arbitra. Volné hodnocení důkazů je myšlenkový proces orgánů činných v trestním řízení (v přípravném řízení typicky policejního orgánu a státního zástupce, v řízení před soudem soudce), ve kterém je potřeba každý důkaz jednotlivě a ve vzájemné souvislosti posoudit z hlediska pravdivosti, hodnověrnosti a výpovědní

[56] JELÍNEK, Jiří. *Základní zásady trestního řízení.* In: JELÍNEK, Jiří a kol. *Trestní právo procesní. 2. aktualizované vydaní*. Praha: Leges: 2011, s. 136.

[57] Srov. rozhodnutí Nejvyššího soudu vydané pod 33/1968 II. Sb. rozh. tr. In: JELÍNEK, Jiří a kol. *Trestní právo procesní. 2. aktualizované vydaní*. Praha: Leges: 2011, s. 136.

[58] ŠÁMAL, Pavel, MUSIL, Jan, KUCHTA, Josef, FRYŠTÁK, Marek a KALVODOVÁ, Věra. *Trestní právo procesní. 4. přeprac. vyd.* V Praze: C.H. Beck, 2013, s. 353.

[59] Imperativ ústnosti je trestním řádem v určitých případech nabourán, typicky je ústnost omezena s ohledem např. na § 211 a § 212 tr. ř. Za určitých podmínek lze místo výslechu přistoupit k přečtení protokolu o výpovědi svědka či obviněného. Dále se zásada ústnosti neprojevuje v případě vydání trestního příkazu, kdy hlavní líčení není nařízeno vůbec, dalším příkladem oslabení principu ústnosti je při zjednodušeném řízení možnost upustit od dokazování skutečností, které státní zástupce a obviněný pokládají za nesporné (srov. § 314d tr. ř.).

hodnoty ve vztahu ke skutku. Zákonodárce pro účely trestního řízení nepředkládá návod, podle kterého by měly být jednotlivé důkazy hodnoceny, judikatura však dovodila jisté mantinely, kterými se soudy musí řídit při aplikaci volného hodnocení důkazů, viz níže. Zásada volného hodnocení důkazů je palčivou otázkou nejen v české praxi, ale léta se jí zabývá odborná veřejnost ve všech vyspělých právních kulturách, tedy tam kde se aplikuje zásada volného hodnocení důkazů. Např. v anglosaské literatuře se v souvislosti s volným hodnocením důkazů objevuje termín „*black box*“, neboli černá skřínka.[60] Obviněný nikdy „nevidí do hlavy“ osoby, která rozhoduje a nikdy nelze jednoznačně posoudit, jakým způsobem soudce rozhodující o jeho vině vzal v potaz jednotlivé důkazy. Jediným vodítkem pro posouzení myšlenkového procesu soudu je odůvodněné rozhodnutí, kterým soud, případně jiný orgán, kvalifikovaně zhodnotí zjištěné skutkové okolnosti, na jejichž základě vydal rozhodnutí.

4.2 Dokazování a ústavní limity

Český právní řád je založený na demokratických principech. Nejzásadnějším dokumentem chránícím ústavně zaručená práva jednotlivců je Listina základních práv a svobod, vyhlášená jako usnesení předsednictva České národní rady č. 2/1992 Sb., a ústavní zákon č. 1/1993 Sb., Ústava České republiky (dále jen „Ústava“ a „Listina"). Ústava ve vztahu k trestnímu řízení vytváří rámec fungování jednotlivých institucí, definuje obecnou působnost soustavy soudů, Nejvyššího soudu, Ústavního soudu, státního zastupitelství, případně dalších součástí exekutivy. Stát vystupuje při aplikaci trestního práva ve vztahu vrchnostenském, Listina tak ve vztahu k základním právům občanů a dalších osob obsahuje garance ochrany před libovůlí státu jako entity, která drží monopol na násilí[61].

Účelem této časti práce je ukázat, jak některá Listinou ústavně garantovaná práva vstupují do problematiky dokazování a následně tato práva konfrontovat s aplikační praxí. Pro účely

[60] Samotný pojem je de facto připodobnění hlavy soudce (či poroty) při hodnocení důkazů k černé skříncе, tedy k přístroji, u něhož nevíme, jakým způsobem funguje. Stejně jako v českém trestním procesu i v americké trestněprávní kultuře je rozhodování soudců (či porotců) neveřejné a složitě přezkoumatelné (srov. např. § 58 tr. ř.), např. Simon ve svém článku zajímavě shrnuje, jak některé aspekty kognitivních omylů mohou generovat nesprávná a nespravedlivá rozhodnutí. SIMON, Dan. *A Third View of the Black Box: Cognitive Coherence in Legal Decision Making.* Chicago: University of Chicago Law Review, 2004, 71(2), s. 511.

[61] WEBER, Max. *Metodologie, sociologie a politika. 1. vyd.* Praha: Oikoymenh, 1998, str. 247.

procesního užití důkazů (např. elektronických důkazů) je v trestním řízení klíčová analýza následujících práv garantovaných Listinou: právo na spravedlivý proces, právo na osobní integritu a soukromí, právo na nedotknutelnost obydlí a jiných prostor a právo na zajištění listovního a telekomunikačního tajemství.

Z pohledu ochrany základních práv lze rozlišit, že tzv. první generace lidských práv vymezuje přednostně negativní závazek státu, který se musí zdržet zasahování do života jednotlivce. Negativní závazek státu je navíc posílen zásadou aktivních zásahů vrchnostenské moci, která musí vytvářet podmínky pro uplatňování takových práv,[62] příkladem pozitivního závazku státu s ohledem na práva první generace budiž vytvoření soustavy soudní moci, která bude spravedlivě rozhodovat o právech osob.

4.2.1 Právo na spravedlivý proces

Právo na spravedlivý proces koncepčně vychází, jak již bylo zmíněno výše, z čl. 6 EÚLP. Ústavodárce toto právo v případě trestního řízení zakotvil primárně ve dvou vzájemně souvisejících ustanoveních.

Čl. 8 odst. 2, věta první Listiny vysloveně stanovuje:

> *„Nikdo nesmí být stíhán nebo zbaven svobody jinak než z důvodů a způsobem, který stanoví zákon.“*

Čl. 2 odst. 2, který definuje zásadu enumerativnosti veřejnoprávních pretenzí:

> *„Státní moc lze uplatňovat jen v případech a v mezích stanovených zákonem, a to způsobem, který zákon stanoví.“*

Přestože by se mohlo zdát, že čl. 8 odst. 2 Listiny míří primárně na ukládání trestněprávních sankcí, je třeba jej vykládat šířeji. Šámal k tomu podotýká[63], že *fair* výsledek trestního řízení lze dosáhnout

[62] WINTR, Jan. *Principy českého ústavního práva. 4. vydání.* Plzeň: Aleš Čeněk, 2018, s. 140.
[63] ŠÁMAL, Pavel: *Limity trestního práva procesního.* In: ŠÁMAL, Pavel, MUSIL, Jan, KUCHTA, Josef, FRYŠTÁK, Marek a KALVODOVÁ, Věra. *Trestní právo procesní. 4. přeprac. vyd.* V Praze: C.H. Beck, 2013, s. 67.

pouze za předpokladu řádného, zákonného procesu, mj. i dodržováním zákonem dovolených procesních postupů orgánů činných v trestním řízení. Šámal dále odkazuje na judikaturu Ústavního soudu, kde spravedlivým procesem není pouze potrestání skutečného pachatele, ale i postup, kterým k takovému rozhodnutí orgány činné v trestním řízení dospěly.[64] Tedy zejména otázka zákonnosti jednotlivých úkonů a minimalizace zásahů dle čl. 4 Listiny. Aby trestní řízení mohlo být považováno za spravedlivé, je třeba jej vést v souladu se zákonem a zároveň při šetření základních práv. Pavlíček v této věci připomíná, že i stíhání, které není podmíněno zákonnými důvody, je *contra constitutionem*,[65] což dle mého názoru platí i pro důkazy, které nejsou získány procesně správně. Pokud by trestní stíhání, případně i samotné odsouzení bylo vystavěno na základě důkazů, které nebyly opatřeny zákonem předpokládaným způsobem, trpělo by zásadními vadami.[66] Právo na spravedlivý proces samozřejmě zahrnuje širokou škálu institutů, např. právo na zákonného soudce, právo na tlumočníka, právo na obhájce, nebo zákaz sebeobviňování, ale úvaha o dalších institutech je nad rámec této práce.

4.2.2 Zásahy do nedotknutelnosti obydlí a jiných prostor

Zaručení nedotknutelnosti obydlí vychází z práva na respektování osobní autonomie člověka, který se nejsvobodněji realizuje právě tam, kde se cítí nejbezpečněji, tedy ve svém domově. Článek 12 Listiny definuje právo na nedotknutelnost následovně:

(1) Obydlí je nedotknutelné. Není dovoleno do něj vstoupit bez souhlasu toho, kdo v něm bydlí.

(2) Domovní prohlídka je přípustná jen pro účely trestního řízení, a to na písemný odůvodněný příkaz soudce. Způsob provedení domovní prohlídky stanoví zákon.

(3) Jiné zásahy do nedotknutelnosti obydlí mohou být zákonem dovoleny, jen je-li to v demokratické společnosti nezbytné pro ochranu života nebo zdraví osob, pro ochranu

[64] Nález Ústavního soudu č. 214/1994 Sb. In: ŠÁMAL, Pavel, MUSIL, Jan, KUCHTA, Josef, FRYŠTÁK, Marek a KALVODOVÁ, Věra. *Trestní právo procesní. 4. přeprac. vyd.* V Praze: C.H. Beck, 2013, s. 67.

[65] PAVLÍČEK, Václav: *Práva, svobody a povinnosti.* In: PAVLÍČEK, Václav a kol. *Ústavní právo a státověda II. díl. 2. vydání.* Praha: Leges, 2015, s. 538.

[66] K problematice teorie otrávených plodů trestního řízení existuje bohatá judikatura zejména ve Spojených státech amerických, její uplatnění v české aplikační praxi je sporné, více viz článek Jiřího Herczega (HERCZEG, Jiří. *Plody z otráveného stromu a ústavněprávní limity získávání informací v trestním řízení*. Praha: Trestněprávní revue. 2009, č. 3, s. 65-70).

práv a svobod druhých anebo pro odvrácení závažného ohrožení veřejné bezpečnosti a pořádku. Pokud je obydlí užíváno také pro podnikání nebo provozování jiné hospodářské činnosti, mohou být takové zásahy zákonem dovoleny, též je-li to nezbytné pro plnění úkolů veřejné správy.

Ústavní soud chápe obydlí nebývale široce. V plenárním nálezu[67] z roku 2010 rozhodl, že tehdy platné ustanovení trestního řádu, které umožnilo vstup na pozemek jen s příkazem státního zástupce, je protiústavní: „[…] *autonomní naplňování soukromého života a pracovní či zájmové aktivity spolu úzce souvisejí, nelze činit ostré prostorové oddělení soukromí v místech užívaných k bydlení od soukromí vytvářeného v místech a prostředí sloužících k pracovní či podnikatelské činnosti anebo k uspokojování vlastních potřeb či zájmových aktivit, byť činnosti odehrávající se v prostorách veřejnosti přístupných, resp. neuzavřených, např. podnikatelská činnost, budou moci podléhat jistým omezením, která mohou představovat určitý zásah do práva na soukromý život.*" Šíře soukromí, kterou v nálezu vymezil Ústavní soud, do jisté míry překračuje už tak široké doktrinální vymezení téhož práva ze strany ESLP.[68]

Městský soud v Praze na druhou stranu v nedávném rozhodnutí pojem soukromí překvapivě zúžil, když dal za pravdu orgánům činným v trestním řízení a nahradil souhlas České advokátní komory s prohlídkou prostor, v nichž je vykonávána advokacie. Tím pádem se policie mohla seznámit s obsahem elektronických listin advokátní kanceláře (a zřejmě i listin klientů) na serverech, které nebyly v budově advokátní kanceláře, ale byly využívány jako jedno ze vzdálených úložišť.[69] Ústavní soud později sice stížnost odmítl[70] jako zjevně neopodstatněnou, ale v odůvodnění se přiklonil k názoru, že § 85b tr. ř. je problematický. Ve věci vymezení prostor sloužících k výkonu advokacie rovněž odkázal na stanovisko trestního kolegia Nejvyššího soudu[71] k výkonu prohlídky u advokáta: „*Postup podle § 85b tr. ř.* […] [lze uplatnit i na] *různá elektronická úložiště dat, a to ať už jde o webové stránky advokáta, vlastní datová úložiště advokáta nenacházející se v*

[67] Nález Ústavního soudu sp. zn. Pl. ÚS 3/09 ze dne 8. června 2010.
[68] WINTR, Jan. *Principy českého ústavního práva. 4. vydání.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018, s. 159.
[69] Shrnutí rozhodnutí Městského soudu je obsaženo v usnesení Ústavního soudu sp. zn. I. ÚS 2878/14-2, ze dne 26. října 2015. Podstatným závěrem Městského soudu je, že povolení zajištění důkazu bylo vydáno bez procedury předvídané v § 85b tr. ř. Významnou okolností v tomto případě bylo, že jednou z osob, které byly vyšetřované orgány činnými v trestním řízení byl advokát v té kanceláři působící.
[70] Usnesení Ústavního soudu sp. zn. I. ÚS 2878/14-2, ze dne 26. října 2015.
[71] Stanovisko Nejvyššího soudu sp. zn. Tpjn 306/2014 ze dne 25. června 2015.

místech běžného výkonu advokátní praxe nebo úložiště provozovaná od advokáta odlišnou osobou, umožňující dálkový přístup pomocí internetové sítě (např. různé typy tzv. hostingů, cloudů, serverů).“ Připustil tedy i možnost zvýšené ochrany dat, která jsou uložena v kanceláři pouze virtuálně. Tyto závěry však dle mého názoru lze zobecnit nejen pro prohlídky v kancelářích advokátů, ale obecně na prostory, které osoba považuje za svou osobní doménu.

Pro účely dokazování, respektive pro účely zajištění důkazů, je tak vždy nutné řádně posoudit, zda případný zásah do soukromé sféry osoby není zásahem do domovní svobody. Pokud orgán činný v trestním řízení zasahuje do dat, například i pomocí vzdáleného přístupu, měl by si odpovědět na otázku, zda svým zásahem nezasahuje do soukromé sféry (např. obydlí či kanceláře) osoby a zda pro takový zásah má příslušné povolení.

4.2.3 Listovní a telekomunikační tajemství, soukromí

S ochranou soukromí souvislí i právo upravené v čl. 13 Listiny, právo na ochranu listovního tajemství:

> *Nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením.*

Ústavní soud i judikatura ESLP dovozují, že listovní tajemství je speciální realizací práva na soukromí dle čl. 7, přičemž meze této ochrany jsou dány zákonem.[72] „[…] *k omezení osobní integrity a soukromí (tj. k prolomení ochrany) může ze strany veřejné moci dojít jen zcela výjimečně a jen je-li to nezbytné a účelu sledovaného veřejným zájmem nelze dosáhnout jinak.*“ Tyto zásahy zákonodárce začlenil zejména do ustanovení § 86 až 87c a § 88 a 88a tr. ř. Platí, že předmětem ochrany je zpravidla obsah zpráv, nikoliv tzv. vedlejší data, u nichž platí odlišný právní režim: „[ochrana] *se vždy vztahuje na obsah zásilek a písemností. Pokud však jde o jiné ‚vedlejší‘ písemnosti a záznamy vzniklé v souvislosti s provozem poštovních a telekomunikačních služeb,*

[72] Nález Ústavního soudu sp. zn. I. ÚS 3038/07 ze dne 29. února 2008.

na jejichž vzniku se podílí také provozovatel poštovních a telekomunikačních služeb, eventuálně též státní orgány, není tato ochrana bezvýjimečná. Tato ochrana se vztahuje toliko na ty ‚vedlejší' údaje, z nichž by bylo možno, byť i zprostředkovaně, zjišťovat informace týkající se osobní sféry lidí, zejména osobních dat, intimního, společenského a hospodářského života lidí a institucí."[73]

Ochrana se nevztahuje pouze na dopravované zprávy, ale i na záznamy uchovávané v soukromí. Opakem soukromého záznamu je záznam přístupný dopředu neznámu okruhu osob. Projeví-li osoba, která disponuje záznamem, vůli jej zveřejnit nebo je z jejího jednání zřejmé, že je s takovým výsledkem srozuměna, nepodléhá tento záznam ochraně listovního tajemství. V každém případě je žádoucí, aby orgány činné v trestním řízení nahlížely na záznamy uchovávané v soukromí spíše jako na záznamy hodné zvýšené ochrany.

4.3 Vady v dokazování

Účelem dokazování je co nejpřesnější zprostředkované poznání skutku orgánem, který je v trestním řízení způsobilý vydat autoritativní rozhodnutí. Orgány činné v trestním řízení vykonávají své pravomoci ve vrchnostenském postavení, tedy jsou vázány přísnými pravidly, která upravují jejich činnost při získávání a provádění důkazů. Jestliže subjekty trestního řízení nevyhoví požadavkům, které na ně klade právní úprava, může důkaz, který byl získán či proveden v rozporu se zásadou legality, tedy *contra legem*, trpět vadou. Podle možnosti nápravy takové vady rozlišujeme mezi relativní a absolutní neúčinností důkazu.

Absolutní neúčinnost důkazu vyjadřuje přítomnost nejzávažnější chyby při procesu dokazování. Jak píše Šámal: „*Absolutní neúčinnost důkazu je důsledkem existence podstatné (závažné) vady, která je neodstranitelná.*"[74] Trestní řád za absolutně neúčinný důkaz považuje důkaz, který byl získán pod hrozbou donucení. Ustanovení § 89 odst. 3 tr. ř. v této souvislosti stanovuje, že „*důkaz získaný nezákonným donucením nebo hrozbou takového donucení nesmí být použit v* [trestním] *řízení.*" Nezákonným donucením se rozumí „*fyzické* […] *psychické působení na vůli osoby, od níž*

[73] Usnesení Ústavního soudu sp. zn. IV. ÚS 554/03 ze dne 29. dubna 2004.
[74] ŠÁMAL, Pavel. *Dokazování v trestním řízení.* In: ŠÁMAL, Pavel, MUSIL, Jan, KUCHTA, Josef, FRYŠTÁK, Marek a KALVODOVÁ, Věra. *Trestní právo procesní. 4. přeprac. vyd.* Praha: C.H. Beck, 2013, s. 370.

byl takový důkaz získán [a to i] *v případě, pokud by k realizaci hrozby mělo dojít ve vzdálenější budoucnosti.*“[75] Klíčovým slovem je však pojem nezákonný, jedná-li se o donucení, které zákon umožňuje, např. hrozba pořádkovou pokutou při nesplnění ediční povinnosti[76] (srov. § 78 odst. 1 tr. ř.), bude hrozba zákonná, tedy i důkaz bude získán řádně. Absolutně neúčinný důkaz je takový, u něhož vadu nelze odstranit. V praxi nastávají dva typy vad důkazů: buď se jedná o důkaz, který nikdy nebyl způsobilý stát se důkazem, například vyšetření na fyziodetekčním přístroji[77], nebo nastala taková vada při zajišťování důkazu, kterou už nelze zpětně zhojit, např. provedení odposlechu a záznamu telekomunikačního provozu policejním orgánem bez souhlasu soudce, když je takový souhlas nutný (srov. § 88 odst. 5 tr. ř.).

Vady relativně neúčinných důkazů lze zpravidla zhojit, nelze však k takovému důkazu přihlížet, dokud není vada odstraněna.[78] Zhojit takovou vadu lze nejčastěji opakováním procesního úkonu, pokud nemá vliv na pravdivost či vypovídající hodnotu důkazu. Relativní a absolutní neúčinnost důkazu nelze zaměňovat s mírou intenzity vady samotné. Jestliže důkaz trpí nepodstatnou vadou, je stále procesně použitelný. Důkaz, který trpí vadou podstatnou, je buď absolutně, nebo relativně neúčinným důkazem.

Vzhledem ke skutečnosti, že elektronické důkazy jsou důkazy, které typicky nemají stanoveny vlastní detailní procesní postupy, mohou se orgány činné v trestním řízení při jejich zajišťování jednoduše dostat do situace, kdy opatřený důkaz není procesně použitelný, neboť byl opatřen způsobem, který je v rozporu se zákonem a znovu takový důkaz obvykle z technických důvodů opatřit nelze. Příkladem budiž zajištění důkazu (elektronických dokumentů) policejním orgánem prostřednictvím přístupu do zaheslovaného cloudového úložiště přes odebraný mobilní telefon. Zatímco obsah telefonu zajištěného prostřednictvím ustanovení § 79 tr. ř. může orgán činný v trestním řízení ohledat, na obsah úložiště, které je k takovému telefonu připojeno, je nutné si obstarat samostatné povolení (srov. kapitolu 6.1), které vyžaduje souhlas soudce. Jestliže

[75] ŠÁMAL, Pavel, GŘIVNA, Tomáš, HERCZEG, Jiří, KRATOCHVÍL, Vladimír, PÚRY, František, RIZMAN, Stanislav, ŠÁMALOVÁ, Milada, VÁLKOVÁ, Helena, VANDUCHOVÁ, Marie. *Trestní zákoník (EVK). 2.vydání.* Praha: Nakladatelství C. H. Beck, 2012, s. 1349.

[76] DRAŠTÍK, Antonín. *Zajištění osob, věcí a jiných majetkových hodnot důležitých pro trestní řízení.* In: JELÍNEK, Jiří a kol. *Trestní právo procesní. 2. aktualizované vydaní*. Praha: Leges: 2011, s. 348.

[77] Srov. Povaha vyšetření na „detektoru lži“, usnesení Nejvyššího soudu sp. zn. 6 To 12/92 ze dne 25. března 1992, vydané ve Sbírce rozhodnutí Nejvyššího soudu pod č. R 8/1993.

[78] JELÍNEK, Jiří. *Zánik trestní odpovědnosti.* In: JELÍNEK, Jiří a kol. *Trestní právo hmotné. 5. aktualizované vydání. Obecná část. Zvláštní část.* Praha: Leges, 2016, s. 361.

je mezitím obsah serveru smazán, nelze úkon zajištění dat v cloudu opakovat a důkaz, který byl zajištěn jiným než povoleným způsobem, je nepoužitelný.

4.4 Analogie v trestním právu procesním

Jedním z principů trestního práva je legální licence státu vynucovat potrestání nejzávažnějších prohřešků osob i proti jejich vůli. Společně s možností ukládat sankce za trestné činy definované v trestním právu hmotném je však stát vázaný zásadou enumerativnosti veřejnoprávních pretenzí a zásadou *nulum crimen, nulla poena sine lege* vyjádřenou v článku 2 odst. 4 Listiny: „*Jen zákon stanoví, které jednání je trestným činem a jaký trest, jakož i jaké jiné újmy na právech nebo majetku, lze za jeho spáchání uložit.*“ Analogií rozumíme postup osoby, která právo aplikuje na situace, které nejsou pozitivně vymezeny za účelem vyplnění mezer v zákonné úpravě. Hmotné právo v souladu se zásadou *nulum crime sine lege, nula poena sine lege scripta* zakazuje analogii, která je v neprospěch pachatele.[79] Na druhou stranu trestní právo procesní v zásadě užití analogie připouští.

Připuštění analogie v trestním právu procesním vychází ze skutečnosti, že zákonodárce i při vší pečlivosti nemůže předpokládat všechny okolnosti, které v souvislosti s trestním řízením mohou nastat. Z připuštění analogie jako formy výkladu procesního práva literatura vyčleňuje dva typy ustanovení, u nichž není analogie přípustná[80]: Zakázána je analogie v případě zásahu do základních práv a svobod[81] a stanovuje-li trestní řád taxativní výčet možností postupu.[82]

Vzhledem k omezené úpravě institutů spojených s elektronickými důkazy často soudu nezbude než uchýlit se při aplikaci procesních norem k analogickému výkladu. S ohledem na výše uvedené je však vždy nutné odpovědět na otázku, zda je možné analogii použít. Dokazování (např. zajišťovací instituty) do práv osob zasahuje často v souvislosti se zájmem společnosti na odhalování trestné činnosti a potrestání pachatele. Přípustná je tak analogie, která některým ustanovením trestního

[79] JELÍNEK, Jiří. *Prameny trestního práva hmotného a výklad trestních zákonů.* In: JELÍNEK, Jiří a kol. *Trestní právo hmotné. 5. aktualizované vydání. Obecná část. Zvláštní část.* Praha: Leges, 2016, s. 64.
[80] KUCHTA, Josef: *Trestněprocesní normy.* In: ŠÁMAL, Pavel, MUSIL, Jan, KUCHTA, Josef a kol. *Trestní právo procesní. 4. přepracované vydání*. Praha: C. H. Beck, 2013, s. 52.
[81] Jedná se např. o podmínky pro povedení domovní prohlídky.
[82] Jedná se např. o dovolací důvody.

řádu dává nový význam. Kupříkladu věcným důkazem rozumíme i data, která s pojetím věci v klasickém slova smyslu mají relativně málo společného (svojí unikátní formou jsou kombinací hmotného a nehmotného důkazu, neboť mají jak nehmotný základ – informaci, tak se zpravidla nacházejí na hmotném nosiči informací, srov. kapitola 0). Nepřístupná je analogie, která zasáhne do ústavně garantovaných práv osoby. Nelze např. analogicky rozšiřovat důvody pro povolení sledování věci dle § 158d tr. ř. tak, aby orgány činné v trestním řízení mohly zajistit takový důkaz, pro jehož zajištění by jinak museli použít jiný důkazní prostředek, nebo jehož užití není dle trestního řádu přípustné.

5 Instituty zajišťování a provádění důkazů

Abychom správně pochopili speciální formy dokazování, v našem případě formy dokazování elektronickými důkazními prostředky, je potřeba nejprve přiblížit důkazy a dokazovací formy obecně.

Jak píše Jelínek: „*Dokazování tvoří podstatnou a nezastupitelnou součást trestního řízení* […] *Je zvláštní formou poznání výseče objektivní reality.*“[83] Orgán činný v trestním řízení se v rámci zjišťování materiální pravdy procesem dokazování, získáváním a interpretací okolností, které jsou důležité pro jeho rozhodnutí, snaží obsáhnout co nejpřesnější vyjádření skutku. Předmětem trestního řízení je pouze skutek, tedy vyhledávat a zajišťovat důkazy, které se netýkají předmětu řízení, není přípustné. Pro dokazování trestní řád upravuje specifické formální procedury, instituty, které umožňují zajistit důkazy pro další řízení (tzv. důkazní prostředky), a instituty, pomocí níž se orgány činné v trestním řízení seznamují s důkazy a procesně je provádějí.

5.1 Důkazy a procesní předpoklady jejich provádění

Jak bylo probráno výše, za důkaz může sloužit vše, co může přispět k objasnění předmětu trestního řízení. Trestní řád tak procesním stranám dává možnost nabídnout soudu (v přípravném řízení pak orgánu činnému v trestním řízení) cokoliv, co může objasnit skutek. Demonstrativní výčet jednotlivých důkazních prostředků dle § 89 odst. 2 tr. ř. je třeba zohlednit jako seznam nejčastějších důkazních prostředků. Předmětem dokazování jsou zejména okolnosti důležité pro věc samotnou, tedy okolnosti, zda došlo k naplnění skutkové podstaty trestného činu, okolnosti svědčící o tom, zda skutek spáchal obviněný a okolnosti důležité pro případné uložení sankce, a to ať už trestu, ochranného opatření, náhrady škody, nemajetkové újmy či bezdůvodného obohacení.[84]

Z pohledu nauky o důkazech je nutné rozlišovat terminologicky mezi třemi pojmy: *důkaz*, *důkazní prostředek* a *pramen důkazu*. Důkazem se rozumí výsledek intelektuální činnosti procesních stran

[83] JELÍNEK, Jiří. *Obecné výklady o důkazech.* In: JELÍNEK, Jiří a kol. *Trestní právo procesní. 2. aktualizované vydaní*. Praha: Leges: 2011, s. 349.

[84] PÚRY, František. *Dokazování v trestním řízení.* In: POLČÁK, Radim, PÚRY, František, HARAŠTA, Jakub a kol. *Elektronické důkazy v trestním řízení. 1. vydání.* Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 53.

při dokazování, tedy typicky se jedná o závěry znalce, výsledek ohledání místa činu, obsah dokumentu nalezeného na počítači nebo například výpis hovorů obviněného. Důkazním prostředkem se rozumí procesní činnost stran, která směřuje k poznání skutkových či jiných okolností důležitých pro rozhodnutí ve věci, typicky se bude jednat o výslech svědka dle § 101 tr. ř., nebo ohledání dle § 113 tr. ř. Pramenem důkazu jsou pak osoby či věci (movité či nemovité, hmotné či nehmotné), které jsou způsobilé k tomu se stát důkazem s pomocí důkazních prostředků. Z pohledu elektronických důkazů se jedná např. o telefon obsahující SMS, e-mailovou schránku, paměť počítače apod. Trestní řád mezi těmito pojmy důsledně nerozlišuje[85] (např. § 112 tr. ř. je dle nauky spíše důkazním prostředkem než důkazem) a používá v zásadě pouze dva pojmy: *důkaz a důkazní materiál*, přičemž důkazním materiálem má zákonodárce na mysli soubor všech důkazů (srov. ustanovení § 76 a § 77 tr. ř. týkající se zadržené osoby). Toto rozlišení však zpravidla vyplývá z kontextu ustanovení.

To, že věc či osoba je způsobilá být pramenem důkazu a skutečně může nějaký důkaz poskytnout, ještě neznamená, že takový důkaz je procesně použitelný. Kromě otázky nepřípustnosti důkazu (srov. kapitolu 4.3) je nutné se vyrovnat s otázkou, zda bylo užito důkazního prostředku (rozuměj zajišťovacího institutu), který je přípustný pro jeho získání. Cílem této kapitoly je shrnout jaké důkazní prostředky mohou orgány činné v trestním řízení využít. Na okraj lze podotknout, že některé důkazní prostředky jsou ve spojení s elektronickými důkazy méně relevantní (např. výslech svědka), a proto se jimi tato práce nebude zevrubně zabývat.

5.1.1 Procesní iniciativa stran

Trestní řád vychází ze zásady procesní rovnosti stran, ta se v případě procesu dokazování před soudem zrcadlí v trestním řádu v § 2 odst. 5, podle kterého „*v řízení před soudem státní zástupce a obviněný mohou na podporu svých stanovisek navrhovat a provádět důkazy*.“ Tato zásada je dále rozvedena v § 89 odst. 2 tr. ř. Jediným důvodem odmítnutí důkazu tedy nesmí být skutečnost, že nebyl předložen orgánem činným v trestním řízení. Judikatura v této věci přijala jednoznačný

[85] ŠÁMAL, Pavel. *Dokazování v trestním řízení.* In: ŠÁMAL, Pavel, MUSIL, Jan, KUCHTA, Josef a kol. *Trestní právo procesní. 4. přepracované vydání*. Praha: C. H. Beck, 2013, s. 348.

výklad. Například I. senát Ústavního soudu se ve svém rozhodnutí[86] vyjádřil k důkazní iniciativě stran (v tomto případu důkaz svědeckou výpovědí navržený obviněným) tak, že odmítnutí provedení důkazu musí být řádně odůvodněno: „[…] *zamítnutí důkazních návrhů účastníků řízení bez věcně adekvátního odůvodnění, zatěžuje takový postup soudu nepřezkoumatelností, neboť vykazuje libovůli, a tak porušuje i čl. 2 odst. 2 Listiny.*“ Není-li tedy případné odmítnutí důkazu soudem věrohodně vysvětleno, jedná se o zásah do práva na spravedlivý proces.

Trestní řád nenabízí jednoznačnou odpověď na otázku, jakým způsobem má obviněný zajišťovat důkazy. Zatímco orgány činné v trestním řízení jsou vázány relativně restriktivními procesními podmínkami, jejichž porušení může mít za následek neúčinnost důkazu (viz kapitola 4.3), osoba obviněná má v této věci relativně volnější prostor pro manévrování. Tento prostor vyplývá z několika okolností. Jednak z požadavku kladeného na orgány činné v trestním řízení unést důkazní břemeno, které je v trestním řízení nastaveno vysoko, vina se zpravidla musí prokázat tak, aby byl zjištěn skutkový stav věci, o němž nejsou důvodné pochybnosti.[87] Další okolností, která posiluje postavení obviněného, je ustanovení věty druhé § 89 odst. 2. tr. ř.: „*Každá ze stran může důkaz vyhledat, předložit nebo jeho provedení navrhnout.*“ Obviněnému, častěji pak jeho advokátovi, trestní řád dává možnost důkazy vyhledat bez součinnosti orgánu činného v trestním řízení[88], tedy oprávnění žádat například po třetích osobách součinnost. Zásadní je však oprávnění obviněného navrhnout provedení důkazu. Jak píše Vantuch[89], je třeba rozdělit navržení provedení důkazu na dvě kategorie. První z nich je navržení provedení důkazu, který obviněný (příp. advokát) vyhledal a prověřil. Takovými důkazy jsou listiny, obsah počítače, znalecké posudky vypracované znalcem obhajoby, se kterými se obviněný seznámil. Druhou kategorií jsou potenciální důkazy, u nich obhajoba předpokládá, že budou svědčit ve prospěch obviněného, ale s jejich obsahem se z objektivních důvodů seznámit nemůže. U elektronických důkazů by se dalo uvažovat

[86] Nález Ústavního soudu sp. zn. I.ÚS 2610/11 ze dne 13. října 2011.
[87] Srov. § 2 odst. 5 tr. ř.
[88] Ve Spojených státech funguje dokazování jiným způsobem než v kontinentálním prostředí, v civilním řízení může účastník požádat soud o vydání příkazu k poskytnutí informací od protistrany, v rámci zvláštního předsoudního procesu nazývaného *discovery*. To samozřejmě platí i pro elektronické informace, tzv. *e-discovery* (srov. MASON, Stephen, SHELDON, Andrew, DRIES, Hein. *Proof: the technical collection and examination of electronic evidence.* In: MASON, Stephen, SENG, Daniel. *Electronic Evidence, Fourth edition*. London: University of London, Institute of Advanced Legal Studies for the SAS, 2017, s. 291).
[89] VANTUCH, Pavel. *Kdy může obhajoba důkaz vyhledat, kdy předložit a kdy jen navrhnout jeho provedení?* Praha: Bulletin advokacie, 2013, s. 13.

např. o geolokačních údajích z mobilního telefonu nebo zajištění obsahu paměti PC osoby, u níž se má za to, že má ve svém držení věci důležité pro trestní řízení.

Pokud tedy obviněný chce předkládat důkazy svědčící v jeho prospěch, je vázán toliko obecnými požadavky na opatření takových důkazů, zpravidla se tak bude jednat o zákaz opatření důkazu nezákonným donucením či hrozbou dle § 89 odst. 3 tr. ř. nebo zákaz důkazu, jehož získáním by došlo k zásadnímu porušení práv a svobod třetích osob (např. pokud by obviněný nebo další osoba získali důkaz protiprávním jednáním, např. neoprávněným vstupem do počítače). Jestliže však obviněný má za to, že důkaz existuje a není možné se k němu dostat legální cestou, měl by požádat o opatření důkazu orgán činný v trestním řízení.

To, že je strana oprávněna navrhovat provedení důkazů ještě neznamená, že orgány činné v trestním řízení, případně předseda senátu řízení před soudem, jsou povinny jí vyhovět. Ústavní soud rozeznává tři základní důvody, pro které soud může provedení či opatření důkazu odmítnout.[90] Těmito důvody jsou jednak nízká relevance směrem k předmětu trestního řízení, jednak nízká potenciální vypovídací hodnota a konečně nadbytečnost, tedy skutečnost, že takový důkaz nepřinese do procesu dokazování žádné nové informace.

5.1.2 Postup při dokazování

Dokazování zásadně probíhá ve všech stádiích trestního řízení, přičemž v každé ze zásadních fází řízení, tj. během fáze prověřování, vyšetřování, řízení před nalézacím soudem, řízení o opravných prostředcích a ve vykonávacím řízení má dokazování různý význam a různé funkce.[91]

Ve fázi prověřování, tj. před zahájením trestního stíhání, leží těžiště dokazování v poznávací funkci. Orgány činné v trestním řízení jsou povinny na základě důkazů shromážděných během prověřování (zpravidla pak užitím různých operativně pátracích prostředků) a dalších informací

[90] Nález Ústavního soudu sp. zn. I. ÚS 733/01 ze dne 24. února 2004, citováno podle Polčák, 2015, s. 72.

[91] JELÍNEK, Jiří. *Jednotlivé důkazní prostředky.* In: JELÍNEK, Jiří a kol. *Trestní právo procesní. 2. aktualizované vydaní*. Praha: Leges: 2011, s. 392. Během všech etap trestního řízení lze proces dokazování rozdělit na čtyři fáze: vyhledání, provedení a procesní zajištění, prověrka a hodnocení důkazu (srov. POLČÁK, Radim, PÚRY, František, HARAŠTA, Jakub a kol. *Elektronické důkazy v trestním řízení. 1. vydání.* Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 66).

vyhodnotit, zda je důvodné uvažovat o zahájení trestního stíhání. Jak dále podotýká Šámal[92], tyto úkony zpravidla činí policejní orgán po sepsání záznamu o zahájení úkonů trestního řízení dle § 158 odst. 3 tr. ř. Mezi tyto úkony můžeme zařadit vyžádání vysvětlení od různých osob, jakož i zajištění odborných vyjádření, ohledání věci a místa činu, případně i samotné zajištění věci pro důkazní účely. Úřední záznam dle § 158 odst. 6 tr. ř. obvykle nelze použít jako důkaz v řízení před soudem, je toliko podkladem pro další rozhodnutí státního zástupce, policejní orgán, případně později pro obviněného. Aby bylo možné důkaz procesně použít, je žádoucí, aby byl dodatečně řádně procesně proveden (např. výslechem). Druhým procesním nástrojem je protokol, který sepíše policejní orgán dle § 158 odst. 3 ve spojení s § 55 tr. ř. Protokol může být procesně použitelný i v dalších fázích trestního řízení, srov. § 211 a 212 tr. ř.

Operativně pátrací prostředky byly začleněny do trestního řádu zákonem č. 265/2001 Sb. Pro účely této práce je nejdůležitějším nástrojem institut sledování osob a věci dle § 158d tr. ř. (dále jen „sledování“). Vzhledem k omezené úpravě elektronických důkazních prostředků je klíčové zmínit ustanovení § 158d odst. 3 tr. ř. Tento operativně pátrací prostředek lze užít ve třech různých stupních přísnosti: prosté sledování, sledování se záznamem a sledování zasahující do práv osoby. Prosté sledování podle odst. 1 je běžným úkonem, o kterém rozhoduje pouze policejní orgán, má-li být použitelné jako důkaz v dalším řízení je klíčové, aby se o tomto úkonu sepsal protokol. Jak podotýká Draštík[93], takové sledování lze pouze zřídka užít jako důkaz v dalším řízení (teoreticky lze použít jako důkazní prostředek svědeckou výpověď osoby, která byla účastna sledování). Sledování dle odst. 2 je sledování, při kterém je pořizován záznam, tedy dle dikce zákona zvukový, obrazový či jinak zachycený. Policejní orgán tak může provést takový úkon sledování pouze na základě písemného povolení státního zástupce, případně bez povolení, nesnese-li odkladu, je možné jej provést, přičemž státní zástupce může tento úkon povolit do 48 hodin. Neučiní-li tak, je policejní orgán povinen výsledky sledování zničit (srov. § 158d odst. 5 tr. ř.).

Sledování zasahující do práv osob lze dle § 158d odst. 3 tr. ř. provádět pouze s předchozím souhlasem soudu na základě odůvodněné žádosti. Zasahováním do práv osob se v tomto případě

[92] ŠÁMAL, Pavel. *Dokazování v trestním řízení.* In: ŠÁMAL, Pavel, MUSIL, Jan, KUCHTA, Josef a kol. *Trestní právo procesní. 4. přepracované vydání*. Praha: C. H. Beck, 2013, s. 362.
[93] DRAŠÍK, Antonín, FENYK, Jaroslav a kol. *Trestní řád. Komentář I. a II. díl.* Praha: Wolters Kluwer ČR, 2017, s. 1195.

rozumí činnost, při níž policejní orgány zasahují do základních práv osoby, která je předmětem sledování. Takovými zásahy je dle Šámala zásah do nedotknutelnosti obydlí dle čl. 12 odst. 1 Listiny, zásah do listovního tajemství a tajemství jiných písemností a záznamů dle čl. 13 Listiny a zajišťování písemností a záznamů uchovávaných v soukromí dle čl. 7 odst. 1 a čl. 10 odst. 2, ať už se jedná o data ve fyzické, elektronické či zvukové podobě.[94] Operativně pátrací prostředky jsou toliko doplňkem speciálních institutů trestního řádu[95] upravených v § 78 a násl. tr. ř. Touto procesní cestou tak lze tak zajistit důkazy pouze tehdy, není-li namístě užít jiný, konkrétnější, důkazní prostředek.

Od zahájení trestního stíhání dle § 160 odst. 1 tr. ř. probíhá fáze vyšetřování. Procesní úkony prováděné orgány činnými v trestním řízení se liší podle charakteru samotného vyšetřování. Jestliže probíhá zkrácené vyšetřování, dokazování se provádí dle § 158 an. tr. ř.[96] Jediným obligatorním úkonem je výslech podezřelého. Na druhou stranu při rozšířením vyšetřování, tedy v případech, kdy je prvním stupněm příslušným pro řízení krajský soud, postupuje orgán činný v trestním řízení v souladu s § 168 an. tr. ř., není tak vázán omezeními vyplývajícími z § 164 odst. 1 tr. ř. a může provádět i úkon, který není neodkladným a neopakovatelným úkonem, např. výslech svědka. Standardní vyšetřování je možné provádět v souladu s § 164 tr. ř. Důkazy, které orgán činný v trestném řízení opatřil před zahájením trestního stíhání, se nemusí opakovat, jsou-li provedeny způsobem odpovídajícím ustanovením trestního řádu. Během vyšetřování má obviněný, respektive jeho obhájce, právo účastnit se vyšetřovacích úkonů.

Těžištěm dokazování je hlavní líčení.[97] Oproti přípravnému řízení, při němž státní zástupce funguje jako garant zákonnosti a autoritativně rozhoduje o podání obžaloby (tzv. *dominus litis)*, je v řízení před soudem v roli strany. Zastupuje veřejný zájem a stává se procesní stranou. Během hlavního líčení může předseda senátu po policejním orgánu či státním zástupci požadovat, aby zajistili další důkazy důležité pro rozhodnutí (srov. § 180 odst. 2, § 183 odst. 1). Obecně lze podotknout,

[94] ŠÁMAL, Pavel, RŮŽIČKA, Miroslav. *§ 158d [Sledování osob a věcí]*. In: ŠÁMAL, Pavel a GŘIVNA, Tomáš. *Trestní řád: komentář. 7., dopl. a přeprac. vyd.* Praha: C.H. Beck, 2013, s. 2006.
[95] Tamtéž.
[96] ŠÁMAL, Pavel. *Dokazování v trestním řízení.* In: ŠÁMAL, Pavel, MUSIL, Jan, KUCHTA, Josef a kol. *Trestní právo procesní. 4. přepracované vydání*. Praha: C. H. Beck, 2013, s. 363.
[97] Tamtéž.

že z pohledu soudní praxe není opatřování důkazů během fáze hlavního líčení časté.[98] Soudce má totiž možnost (nejčastěji během předběžného projednání obžaloby dle § 188 odst. písm. e), případně dle § 221 odst. 1) vrátit věc státnímu zástupci k došetření. U ostatních řízení (tj. u odvolacího řízení, řízení o mimořádných opravných prostředcích a ve vykonávacích řízeních) se dokazování provádí velmi omezeně.[99]

5.2 Instituty zajišťování důkazů dle trestního řádu

V předchozí kapitole bylo předestřeno, jakým způsobem a v jakých fázích trestního řízení strany jednotlivé důkazy mohou provádět. Neméně důležité však je, jakým způsobem mohou být důkazy získány, respektive jak zajistit důkazy tak, aby byly procesně použitelné a proveditelné v rámci dalších fází trestního řízení. Jedním z důvodů, proč trestní řád pozitivně upravuje zákonnost získávání různých druhů důkazů, je zejména zachování rovnosti zbraní stran trestního řízení a legality postupu orgánů činných v trestním řízení. Jelikož elektronické důkazy jsou především věcného charakteru, bude tato kapitola pojednávat o pramenech důkazů, které nemají osobní povahu.[100] Mezi ně patří součinnost osob, vydání a odnětí věci, osobní prohlídka, domovní prohlídka a prohlídka jiných prostor a pozemků, zadržení a otevření zásilky, odposlech a záznam telekomunikačního provozu, zjišťování údajů o uskutečněném telekomunikačním provozu a operativně pátrací prostředky. V souvislosti s novelou provedenou zákonem č. 287/2018 Sb., kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a některé další zákony, vstoupilo v účinnost i ustanovení § 7b tr. ř., které má povahu zajišťovacího institutu vzhledem k elektronickým důkazům.

[98] Srov. POKORNÝ, Marek: *Rázná soudkyně Miklová otřásla zvyklostmi české justice. Její případy citují i v zahraničí.* Praha: Hospodářské noviny, Právní rádce, 21. prosince 2018 [cit. 2019].

[99] Srov. např. § 263 odst. 6, § 265r odst. 7, § 282 odst. 1 tr. ř.

[100] Pro účely této práce vzhledem k povaze jednotlivých zajišťovacích úkonů nebude věnován prostor specifickým institutům trestního řádu, typicky vazbě a dalším úkonům k zajištění osoby, proti níž se řízení vede. Stejně tak jsou pro předmět dokazování elektronickými důkazními prostředky málo podstatné instituty zajištění peněžních prostředků, nemovitostí a obecně předběžná opatřená dle § 88b až § 88o tr. ř. Důkazem, který nemá osobní povahu se myslí důkaz, který má způsobilost obsahovat elektronickou informaci.

5.2.1 Součinnost osob

Běžným institutem zajištění věcí pro trestní řízení je tzv. dožádání[101], neboli součinnost státních orgánů a právnických a fyzických osob v souvislosti s trestním řízením. Ustanovení § 8 tr. ř. stanovuje, že tyto „*osoby jsou povinny bez zbytečného odkladu, a nestanoví-li zvláštní předpis jinak, i bez úplaty vyhovovat dožádáním orgánů činných v trestním řízení při plnění jejich úkolů.*" Dožádání je úkon, pomocí kterého je orgán činný v trestním řízení oprávněn požadovat součinnost „*k zajištění povahy, rozsahu nebo umístění věcí důležitých*" pro účely zjištění okolností skutku. Zákonodárce ustanovením § 8 předpokládá určitou míru nucené spolupráce osob, které nemusejí být subjekty trestního řízení, a to bezúplatně.[102] Jestliže povinná osoba nechce spolupracovat, je možné jí po splnění zákonných požadavků uložit pořádkovou pokutu (srov. § 66 tr. ř.). Užití institutu součinnosti s osobami je omezeno několika faktory: zásadou zákazu sebeobviňování, zásadou subsidiarity a zásadou zákonného postupu dle jiného právního předpisu. Z časového hlediska mohou orgány činné v trestním řízení úkon dožádání provést v průběhu celého trestního řízení.

Při dožádání se vždy použije zásada *nemo tenetur se ipsum accusare*, která umožňuje někdy součinnost odepřít. Na druhou stranu nikdo nesmí být nucen odevzdat věci či záznamy a činit prohlášení, která jsou způsobilá mu zapříčinit trestní stíhání. Při posuzování oprávněnosti odepřít součinnost tak existuje tenká hranice mezi osobou, která nechce spolupracovat svévolně, a osobou, která ví, že poskytnutí součinnosti by mohlo mít za následek její trestní stíhání. Orgány činné v trestním řízení by tak měly vždy zvažovat, zda a za jakých podmínek ji mohou k součinnosti přimět. Druhým omezením dožádání je subsidiarita tohoto nástroje. Protože je dožádání nejobecnějším instrumentem zajištění důkazů či informací dle trestního řádu, je vždy třeba na něj nahlížet jako na nástroj, který je možné použít, jen neexistuje-li nástroj speciální. Konečně, možnost získávat takovýmto způsobem informace od různých subjektů je omezena speciálním

[101] Dožádáním trestní řád označuje rovněž postup podle § 53 tr. ř., v přídě takového dožádání však vzniká povinnost dožadovaného orgánu (např. soudu) provést určitý procesní úkon trestního řízení za dožadující orgán. Dožádáním se v tomto případě rovněž nemyslí postup provádění úkonů v souvislosti s mezinárodní justiční spolupráci.

[102] Speciální zákony mohou určit, že dožádaným osobám se poskytne určitá náhrada za prostředky či čas vynaložený v souvislosti s poskytováním součinnosti orgánům činným v trestním řízení, např. § 15 odst. 14 zákona č. 48/1997 Sb., o veřejném zdravotním pojištění, stanovuje úhradu nákladů zdravotních služeb provedením na pokyn orgánu činného v trestním řízení (srov. ŠÁMAL, Pavel a kol. Trestní řád II. 7. vydání. I. díl. Praha: C. H. Beck, 2013, s. 126).

postupem dle jiných zákonů, respektive zákonnou povinností uchovávat informace v tajnosti. Netýká se to pouze informací vedených v utajovaném režimu, ale i informací, u nichž zákon předpokládá povinnost mlčenlivosti (případně tzv. uznané mlčenlivosti).[103]

Ustanovení o součinnosti státních orgánů a právnických a fyzických osob dále v § 8 odst. 5 tr. ř. zakotvuje mechanismus, podle kterého lze povinnost důvěrnosti či mlčenlivosti prolomit se souhlasem soudu: „*Nestanoví-li zvláštní zákon podmínky, za nichž lze pro účely trestního řízení sdělovat informace, které jsou podle takového zákona utajovány, nebo na něž se vztahuje povinnost mlčenlivosti, lze tyto informace pro trestní řízení vyžadovat po předchozím souhlasu soudce.*" Není-li tedy ve zvláštním předpisu upraven postup pro prolomení mlčenlivosti, může soud vyslovit souhlas s prolomením důvěrnosti.[104]

Povinnost součinnosti státních orgánů a fyzických či právnických osob při zajišťování elektronických důkazů je rozsáhlá. Speciálním ustanovením, které upravuje povinnost mlčenlivosti s ohledem na různá technická a provozní data, je § 89 odst. 1 zákona o elektronických komunikacích: „*Podnikatelé zajišťující veřejné komunikační sítě nebo poskytující veřejně dostupné služby elektronických komunikací jsou povinni zajistit technicky a organizačně důvěrnost zpráv a s nimi spojených provozních a lokalizačních údajů* […] *to nebrání technickému ukládání údajů, které je nezbytné pro přenos zpráv, aniž by byla dotčena zásada důvěrnosti.*" Zatímco provozní a lokalizační údaje jsou vždy považovány za důvěrné,[105] technické údaje do této kategorie nepatří. Podzákonný právní předpis, vyhláška o uchovávání, předávání a likvidaci provozních a lokalizačních údajů[106], v § 2 přesněji definuje jednotlivé provozní a lokalizační údaje, např. délka komunikace u veřejné telefonní sítě, adresu MAC zařízení uživatele služby u poskytovatele internetového připojení nebo identifikátor uživatelského účtu u služby přístupu ke schránce elektronické pošty. Údaje, které nejsou provozními, lokalizačními či uživatelskými údaji a vznikly v souvislosti s elektronickou komunikací bývají zpravidla technickými údaji *a contrario*. Zatímco

[103] ŠÁMAL, Pavel. *§ 1 až 12*. In: ŠÁMAL, Pavel a GŘIVNA, Tomáš. *Trestní řád: komentář. 7., dopl. a přeprac. vyd.* Praha: C.H. Beck, 2013, s. 126.

[104] DRAŠÍK, Antonín, FENYK, Jaroslav a kol. *Trestní řád. Komentář I. a II. díl.* Praha: Wolters Kluwer ČR, 2017, s. 64.

[105] Srov. § 90 a 91 zákona o elektronických komunikacích.

[106] Vyhláška č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů, vyhláška pak navazuje na směrnici Evropského parlamentu a Rady 2006/24/ES o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí.

pro technické informace lze užít institutu vyžadování součinnosti dle § 8 tr. ř., u ostatních dat toho od osob, které podléhají regulaci zákona o elektronických komunikacích, vyžadovat nelze.

5.2.2 Vydání a odnětí věci

Jedním z nejčastějším a nejtypičtějších úkonů zajištění věci je vydání a odnětí věci, které je upraveno v § 78 a 79 tr. ř. Oprávnění se opírá o zásadu spolupráce veřejnosti (tj. fyzických a právnických osob) s orgány činnými v trestním řízení při trestním řízení upravenou např. v § 8 odst. 1 tr. ř., přičemž trestní řád u osob, které jsou povinny podle jiného právního předpisu, jiného ustanovení trestního řádu nebo státem uznané povinnosti mlčenlivosti, zásadu spolupráce do jisté míry omezuje.[107]

Povinnost předložit či vydat věc důležitou pro trestní řízení (tzv. ediční povinnost) souvisí s nutností přimět osoby k dobrovolné součinnosti. Tuto výzvu (formou se jedná o opatření, rozhodnutí *sui generis*) může komukoliv adresovat předseda senátu, v přípravném řízení pak státní zástupce či policejní orgán. Ediční povinnost se týká každého s výjimkou osob, které jsou vyňaty z působnosti trestního řádu,[108] osob s povinností mlčenlivosti, osob, které požívají státem uznané povinnosti mlčenlivosti a samozřejmě v souladu s § 78 odst. 3 osob, kterým se předložením či vydáním zasáhne do práva na sebeobviňování případně obviňování osoby blízké (srov. § 99 a § 100 tr. ř.), tato osoba nemůže být nucena „*dobrovolně*“ vydat věc, která by zapříčinila trestní stíhání sebe nebo osoby blízké, ustanovení o pořádkové pokutě se pro ní tedy nepoužijí.

Odnětí věci dle § 79 tr. ř. představuje institut přímo navazující na ediční povinnost: „*Nebyla-li věc, která může sloužit pro důkazní účely, na vyzvání předložena nebo vydána tím, kdo ji má u sebe, může mu být na příkaz předsedy senátu a v přípravném řízení na příkaz státního zástupce nebo policejního orgánu odňata* […]“ Příkaz k tomuto úkonu může vydat předseda senátu, v případě

[107] Omezení těchto práv vyplývá jednak z mezinárodních závazků České republiky, jednak státem uznanou povinnost mlčenlivosti (typicky se týká zpovědního tajemství) a jednak z právních předpisů (např. zákona č. 85/1996 Sb., o advokacii, 154/1994 Sb., o bezpečnostní informační službě, zákona č. 6/2002 Sb., o soudech a soudcích, zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti a mnoha dalších), typicky existují zákonem předpokládané předpoklady a možnosti sdělení informací a poskytnutí věcí pro trestní řízení.

[108] DRAŠTÍK, Antonín. *Zajištění osob, věcí a jiných majetkových hodnot důležitých pro trestní řízení.* In: JELÍNEK, Jiří a kol. *Trestní právo procesní. 2. aktualizované vydaní*. Praha: Leges: 2011, s. 348.

přípravného řízení pak státní zástupce. Nesnese-li tento úkon odkladu, může policejní orgán věc odejmout i bez předchozího souhlasu státního zástupce.

Pro účely zajišťování elektronických důkazů se v případě obou institutů bude nejčastěji jednat o různé nosiče informací, mobilní telefony, počítače, serverová úložiště či SIM karty. Na hmotné věci se však tato úprava nutně vztahovat nemusí, teoreticky lze požadovat vydání či předložení věci i s ohledem na věci nehmotné, tedy například elektronickou korespondenci nebo software kód uložený na serveru. Pro přípustnost použití odnětí věci musí orgán, který vydává takový příkaz, odpovědět na otázku, zda nezasahuje do ústavně zaručených práv třetích osob, a zda by nebylo ústavně konformnější rozhodnout o domovní prohlídce, případně prohlídce jiných prostor (viz dále).

5.2.3 Domovní prohlídka a prohlídka jiných prostor a pozemků

Domovní prohlídka je úzce spjata s ústavně zakotveným právem na ochranu soukromí a soukromí domova, právo na obojí je upraveno přímo v Listině v čl. 7 odst. 1, respektive v čl. 12 odst. 1 a odst. 2. Jak bylo pojednáno v kapitole 4.2.2, nedotknutelnost obydlí je nutno chápat extenzivně, nejedná se pouze o místo trvalého pobytu ve smyslu zákona o evidenci obyvatel a rodných číslech, jedná se o místo, ve kterém osoba, která přebývá v dané lokalitě realizuje své právo na soukromí. Zákonodárce v souladu s čl. 12 odst. 2 stanovuje přísné podmínky zásahu do tohoto práva, až na výjimky nelze zasáhnout do nedotknutelnosti domova bez souhlasu soudu.

Úprava domovní prohlídky a prohlídky prostor nesloužících k bydlení a pozemků je pozitivně upravena v trestním řádu v § 82 a násl. Základní podmínkou pro umožnění provedení domovní prohlídky je skutečnost, že orgán činný v trestním řízení má za to, že existuje důvodné podezření, že v obydlí osoby se nachází věc (případně osoba), která je důležitá pro trestní řízení. Domovní prohlídku povoluje předseda senátu, v přípravném řízení soudce na návrh státního zástupce (srov. § 83 odst. 1 tr. ř.). Bez souhlasu soudu lze do obydlí vstoupit pouze v případech stanovených § 83c tr. ř., toto ustanovení zároveň předjímá, že policejní orgán nemůže provádět při vstupu do obydlí jakékoliv jiné úkony směřující k zajištění důkazů. Tímto se zabezpečuje, aby nebyla obcházena ustanovení zajišťující domovní prohlídku. Judikatura a nauka však dovodily, že

zajištění důkazů, které kauzálně souvisí se vstupem do obydlí, je možné.[109] Prohlídku jiných neveřejně přístupných (srov. § 82 odst. 2 tr. ř.[110]) prostor a pozemků lze provést pouze ze stejných důvodů a za stejných podmínek jako domovní prohlídku.[111]

Pro elektronické důkazy je klíčové určit, kde se nalézají. Lze rozlišovat v zásadě dvě situace: data se buď nalézají na paměťovém médiu (CD, DVD, hard disk, paměť RAM apod.), nebo se nalézají na cloudovém či obdobném úložišti. Otázka umístění dat je odvislá od toho, zda uživatel může či nemůže přistupovat k datům bezprostředně, nejčastěji pomocí vzdáleného přístupu k jinému počítači pomocí údajů už uložených přístupových uživatelských jmen a hesel. Pokud by se data nacházela na místě, pro které by soud nevydal povolení k domovní prohlídce, nebylo by možné taková data procesně zajistit jako důkaz pro další fáze trestního řízení. Někteří autoři[112] však nabízejí i alternativní odpověď na otázku, zda lze taková data přímo použít: Gřivna ve výkladu[113] k § 230 tr. z. uvádí, že počítačovým systémem se rozumí „*jakékoli zařízení nebo skupina vzájemně propojených nebo souvisejících zařízení, z nichž jedno nebo více provádí na základě programu automatické zpracování dat."* Takové vymezení počítačového systému, respektive věci, na kterou se vztahuje domovní prohlídka by zahrnovala i všechna místa, na která se lze vzdáleně připojit. Domnívám se však, že toto extenzivní pojetí počítačového systému, respektive zahrnutí dat, která nelze zajistit tzv. *offline* je v rozporu s logikou trestního řádu a ústavně zaručených práv osob. Pro zajištění důkazů, které se nacházejí mimo místo, na kterém se provádí domovní prohlídka, jsou zpravidla použitelné jiné procesní instrumenty (např. zajištění pomocí operativně pátracích

[109] ŠÁMAL, Pavel, RŮŽIČKA, Miroslav. *§ 83 [Vstup do obydlí, jiných prostor a na pozemek]*. In: ŠÁMAL, Pavel a GŘIVNA, Tomáš. *Trestní řád: komentář. 7., dopl. a přeprac. vyd.* Praha: C.H. Beck, 2013, s. 1143.

[110] Prohlídku veřejně přístupných prostor lze zpravidla provést způsobem, na který se nevztahují omezení ustanovení § 82 a násl.

[111] K otázce rozdílu mezi domovní prohlídkou a prohlídkou jiných prostor a pozemků se vyjádřil Ústavní soud ve svém plenárním stanovisku vydaném pod sp. zn. Pl. ÚS-st. 31/10, které navazovalo na nález Ústavního soudu vydaný pod sp. zn. II. ÚS 860/10 ze dne 2. září 2010. Na základě tehdy platné právní úpravy byl státním zástupcem vydán příkaz k prohlídce jiných prostor, který byl následně Ústavním soudem zrušen jako protiústavní. Ústavní soud ve svém stanovisku vyjádřil přesvědčení že zásah do soukromí u jiných prostor a pozemků nabývá podobné intenzity jako zásah do domovní svobody, tudíž by mechanismus kontroly prohlídky měl podléhat pod moc soudní, neboť zasahuje do ústavně zaručených práv osob.

[112] Srov. např. ŠÁMAL, Pavel a kol. *Trestní řád I. 7.* vydání. Praha: C. H. Beck, 2013 In: POLČÁK, Radim, PÚRY, František, HARAŠTA, Jakub a kol. *Elektronické důkazy v trestním řízení. 1. vydání.* Brno: Masarykova univerzita, Právnická fakulta*,* 2015, s. 105.

[113] GŘIVNA, Tomáš. *§ 230 [Neoprávněný přístup k počítačovému systému a nosiči informací]*. In: ŠÁMAL, Pavel, GŘIVNA, Tomáš, HERCZEG, Jiří, KRATOCHVÍL, Vladimír, PÚRY, František, RIZMAN, Stanislav, ŠÁMALOVÁ, Milada, VÁLKOVÁ, Helena, VANDUCHOVÁ, Marie. *Trestní zákoník (EVK). 2.vydání.* Praha: Nakladatelství C. H. Beck, 2012, s. 2300.

prostředků dle § 158d tr. ř. nebo přímé vyžádání věci důležité pro trestní řízení od osoby, která jí disponuje). Navíc dle zásady přiměřenosti a minimalizace zásahů dle § 2 odst. 1 ve spojení s § 52 tr. ř. jsou orgány činné v trestním řízení povinny postupovat šetrně. Přístupem do počítačového systému by navíc postupovaly *contra lege* a v krajním případě by mohly naplnit znaky skutkové podstaty neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 odst. 1 písm. a) tr. z. O provedené domovní prohlídce se sepisuje protokol, který je součástí spisu a slouží jako dokument, který věrohodně zachycuje průběh tohoto úkonu.

5.2.4 Osobní prohlídka

Osobní prohlídkou se rozumí úkon nejčastěji policejního orgánu, který se řídí ustanovením § 82 odst. 3 tr. ř., a to pouze existuje-li důvodné podezření, že osoba u sebe má věc důležitou pro trestní řízení. Rovněž lze dovodit zákonnost osobní prohlídky u osoby zadržené či zatčené, nebo osoby, která se bere do vazby, existuje-li podezření, že osoba u sebe má věc, která by mohla ohrozit život její, nebo život jiné osoby (typicky se tedy jedná o zajištění zbraně).[114] Z hlediska elektronických důkazů se dále tato podkapitola bude věnovat toliko postupu dle § 82 odst. 3 tr. ř.

Podmínky pro provedení osobní prohlídky obsahuje § 83b tr. ř. Nařídit ji může pouze předseda senátu, nebo státní zástupce v přípravném řízení, případně s jeho souhlasem policejní orgán. Policejní orgán je oprávněn ji provést bez příkazu soudu nebo souhlasu státního zástupce jen v souvislosti neodkladností tohoto úkonu nebo jedná-li se o osobu, na kterou byl vydán příkaz k zatčení (srov. § 83b odst. 4 tr. ř.). Typicky je osobní prohlídka do jisté míry operativním opatřením, kterým policejní orgán získává důkaz přímo od pachatele. Jedná se o typický zásah veřejné moci do ústavně chráněného soukromí osoby[115] a osoba takový zásah musí strpět (srov. § 85a tr. ř.). Zákonodárce tento rozpor mezi zásahem do práv jednotlivce a veřejným zájmem (akceschopností orgánů činných v trestním řízení) vyřešil výše zmíněnou delegací rozhodování na soud, státního zástupce, případně operativně na policejní orgán. Z hlediska ústavněprávního by

[114] Jak připomíná Šámal (srov. ŠÁMAL, Pavel, MUSIL, Jan, KUCHTA, Josef a kol. *Trestní právo procesní. 4. přepracované vydání*. Praha: C. H. Beck, 2013, s. 304), v případě zbraně se nemusí jednat o *důvodné podezření*, postačí tzv. prosté podezření vycházející z běžných okolností.

[115] KREJČÍ, Zdeněk. *Prohlídka dle trestního řádu ve světle rozhodování Ústavního soudu.* Kriminalistika. 2009, 42(4), s. 320.

prohlídka jako zásah do práva na soukromí jednotlivce měla podléhat souhlasu soudu, avšak nejde o zásah tolik invazivní, aby vyžadoval soudní ochranu ex ante. Prakticky však tomu tak není a s ohledem na proporcionalitu zásahu, takové řešení zřejmě ani není žádoucí.

Zákon, aniž by to bylo vysloveně zmíněno, předjímá, že věci zajištěné tímto způsobem, budou mít spíše povahu hmotných věcí. Lze předpokládat, že osoba, jejíž věc byla takto zajištěna, může u sebe mít nosič elektronických informací, může se jednat např. o mobilní telefon, či paměťové médium. V souvislosti s osobní prohlídkou a zákonností získání případných důkazů pro další řízení je žádoucí zmínit, že Nejvyšší soud dovodil, že důkaz, který byl získán v rozporu s ustanoveními upravujícími osobní prohlídku, je důkazem absolutně neúčinným.[116] Vzhledem k ústavně daným předpokladům ochrany osobnosti je nutné, aby orgány činné v trestním řízení vždy při využití institutu osobní prohlídky postupovaly restriktivně a je-li to možné, po předchozím výslechu osoby, která má být osobní prohlídce podrobena. Věc, která je osobní prohlídkou zajištěna, by měla být následně ohledána (viz níže) a o prohlídce a ohledání by měl být sepsán protokol.

5.2.5 Zadržení, otevření a sledování zásilky

Institut zadržení, otevření a sledování zásilky je relativně specifickým institutem obstarávání důkazů v rámci trestního řízení. Poštovní tajemství, respektive důvěrnost doručovaných zásilek, je chráněna v Listině v čl. 13, který důvěrnost komunikace mezi osobami pokládá za právo, které je možné omezit pouze zákonem. Zadržení, otevření a sledování zásilky jsou instituty, z nichž každý má svá specifika a umožňuje objasňovat skutek pomocí zjištěných informací. Pozitivně jsou tyto důkazní prostředky upraveny v § 86 až 87a tr. ř. Všechny instituty jsou aplikovatelné pouze na tzv. *přepravované* zásilky, tedy jakmile zásilka přejde do sféry dispozice adresáta, není možné tyto nástroje využít.[117]

[116] Usnesení Nejvyššího soudu sp. zn. 7 Tdo 783/2010 ze dne 4. srpna 2010. In: ŠÁMAL, Pavel. ŠÁMAL, Pavel, MUSIL, Jan, KUCHTA, Josef a kol. *Trestní právo procesní. 4. přepracované vydání*. Praha: C. H. Beck, 2013, s. 1140.

[117] ŠÁMAL, Pavel. *Zajišťovací úkony a předběžná opatření.* In: ŠÁMAL, Pavel. ŠÁMAL, Pavel, MUSIL, Jan, KUCHTA, Josef a kol. *Trestní právo procesní. 4. přepracované vydání*. Praha: C. H. Beck, 2013, s. 319.

Pro zadržení zásilky platí: „*Je-li k objasnění skutečností důležitých pro trestní řízení v konkrétní věci nutno zjistit obsah nedoručených poštovních zásilek, jiných zásilek nebo telegramů, nařídí předseda senátu a v přípravném řízení státní zástupce, aby je pošta nebo osoba provádějící jejich přepravu vydaly jemu a v přípravném řízení buď státnímu zástupci nebo policejnímu orgánu.*“ Zásilka přitom dle § 86 odst. 2 tr. ř. může být zadržena i bez příkazu předsedy senátu, nebo státního zástupce, maximálně však na 3 dny. Navíc, jak podotýká Jelínek, zadržení zásilky se nutně nemusí týkat jen zásilky odesílané obviněným nebo jemu adresované zásilky, ale týká se obsahu této zásilky, tedy typicky může zasahovat i do práv třetích osob.[118] Otevření zásilky, která je zadržena v souladu s § 86 tr. ř., může provést policejní orgán či státní zástupce pouze se souhlasem předsedy senátu, případně se souhlasem soudce v přípravném řízení. Tímto je ošetřena ústavnost zásahu do listovního tajemství dle Listiny.

Účelem institutu záměny zásilky je zamezení distribuce závadného obsahu zásilky. Primárně ustanovení § 87a tr. ř. míří na psychotropní látky a kontraband, ovšem vztahuje se i na „*věci určené ke spáchání trestného činu, anebo věci z trestného činu pocházející*.“ Záměna zásilky stejně jako otevření zásilky podléhá souhlasu soudu. Blízkým institutem je i tzv. *sledovaná zásilka*, která má blízko k operativně pátracím prostředkům (srov. § 158d tr. ř.). Využití tohoto institutu je možné pouze v přípravném řízení, a to zejména ve spojení s případným dočasným odložením trestního stíhání.[119]

Využití výše uvedených institutů při zajišťování elektronických důkazů je možné, leč z praktického hlediska málo použitelné.[120] Mohlo by se jevit jako užitečné použít jej pro zajištění zpráv přepravovaných např. e-mailem. E-mailovou zprávu lze považovat za přepravovanou jinou zásilku[121] ve smyslu ustanovení § 87 odst. 1 tr. ř., ovšem v případě e-mailu dochází k doručení téměř okamžitě. Vzhledem ke skutečnosti, že se musí jednat o zásilky *přepravované,* použije se

---

[118] JELÍNEK, Jiří. *Obecné výklady o důkazech.* In: JELÍNEK, Jiří a kol. *Trestní právo procesní. 2. aktualizované vydaní*. Praha: Leges: 2011, s. 357.

[119] JELÍNEK, Jiří. *Obecné výklady o důkazech.* In: JELÍNEK, Jiří a kol. *Trestní právo procesní. 2. aktualizované vydaní*. Praha: Leges: 2011, s. 359.

[120] KOLOUCH, Jan, *Cybercrime*. Praha: CZ.NIC, 2016, s. 422.

[121] ŠÁMAL, Pavel, GŘIVNA, Tomáš, HERCZEG, Jiří, KRATOCHVÍL, Vladimír, PÚRY, František, RIZMAN, Stanislav, ŠÁMALOVÁ, Milada, VÁLKOVÁ, Helena, VANDUCHOVÁ, Marie. *Trestní zákoník (EVK). 2.vydání.* Praha: Nakladatelství C. H. Beck, 2012, s. 1170. Ustanovení o zadržení zásilky se vztahuje na širokou škálu služeb od klasické pošty, přes fax až po telegramy, poskytovatelé různých služeb e-mailové komunikace, např. Gmail, Seznam.cz apod. podléhají úpravě zákona č. 480/2004 Sb., o některých službách informační společnosti.

institut vydání věci (přímo od poskytovatele, adresáta, odesílatele), zprávy se zajistí pomocí domovní prohlídky, prohlídky jiných prostor, sledování věci, nebo dle odposlechu a záznamu telekomunikačního provozu, případně dalších institutů. Nepraktičnost tohoto institutu zajištění důkazu je mj. i v tom, že pro každou jednotlivou zprávu by měl orgán činný v trestním řízení vydat separátní rozhodnutí.

5.2.6 Odposlech a záznam telekomunikačního provozu

Jedním z klíčových nástrojů pro potírání kriminality, zejména pak kriminality organizované, je institut odposlechu. Odposlechem se rozumí „[…] *záměrné a utajené a soustavné vnímání obsahu komunikace zprostředkované telekomunikačními sítěmi nebo prostřednictvím k tomu určených zařízení. Záznamem je souběžné zachycení obsahu na nosičích* […] *umožňujících jejich uchování a reprodukci.*"[122] Výjimečnost tohoto institutu, na rozdíl od většiny dalších důkazních prostředků, je v tom, že se jedná o zajištění důkazů *pro futuro*, tedy nikoliv zjištění toho, co se už stalo, ale toho, co se stane v buducnosti. Orgány činné v trestním řízení tak předpokládají, že osoba odposlouchávaná či osoba, která bude figurovat na záznamu, prozradí skutečnosti důležité pro trestní řízení během doby odposlouchávání či zaznamenávání. Odposlech a záznam jsou významným zásahem do soukromí člověka, trestní řád pro něj tedy stanovuje relativně přísné požadavky pro povolení.

Úprava institutu odposlechu a záznamu provozu je v trestním řádu upravena v § 88. Omezujícím prvkem pro posouzení zákonnosti nařízení odposlechu je horní hranice trestní sazby u zločinů (srov. § 13 odst. 2 tr. z.), která musí činit nejméně 8 let. Nad rámec toho je možné nařídit odposlech a záznam telekomunikačního provozu pro vyjmenované trestné činy[123] nebo trestné činy, jejichž stíhání je požadováno mezinárodními závazky České republiky[124], přičemž vždy se musí jednat o

[122] ŠÁMAL, Pavel. *Zajišťovací úkony a předběžná opatření.* In: ŠÁMAL, Pavel, MUSIL, Jan, KUCHTA, Josef a kol. *Trestní právo procesní. 4. přepracované vydání*. Praha: C. H. Beck, 2013, s. 325.

[123] Podle § 88 odst. 1 tr. ř. se jedná typicky o trestné činy, u nichž se předpokládá propojení veřejného zájmu v odhalení trestné činnosti, veřejných zdrojů a tzv. „*trestných činů bez oběti*", tedy trestných činů, kdy poškozený nebývá konkrétní právnická a fyzická osoba, ale typicky organizační složka státu, či hospodářství a důvěra v něj jako celek, přičemž jsou to zároveň trestné činy, kde zpravidla existuje důkazní nouze. Typickým trestným činem dle předchozí věty jsou pletichy při zadávání veřejné zakázky a při veřejné dražbě, či zjednání výhody při zadání veřejné zakázky, při veřejné soutěži a veřejné dražbě.

[124] Z pohledu elektronických důkazů se bezesporu bude jednat mj. o trestné činy definované v Budapešťské úmluvě.

úmyslné trestné činy. Vzhledem k tomu, že odposlech a záznam jsou výrazným zásahem do soukromí osoby, trestní řád vyžaduje, aby se těchto prostředků užívalo subsidiárně, podmínkou pro povolení takového záznamu tak je, že lze důvodně přepokládat, že orgán činný v trestním řízení nemůže důvodně přepokládat, že lze objasnění skutku dosáhnout způsobem, který je méně invazivní.

Specifičnost tohoto institutu je dána i skutečností, že odposlech je vždy nařizován na omezené časové období (srov. § 88 odst. 2 tr. ř.), navíc je policejní orgán povinen průběžně vyhodnocovat, zda nadále trvají důvody dalšího odposlechu či záznamu. O povolení odposlechu a záznamu rozhoduje na návrh státního zástupce soudce v přípravném řízení, nebo předseda senátu v hlavním líčení, o povolování pokračování záznamu a odposlechu pak rozhoduje krajský soud. Ve vyjmenovaných věcech může odposlech a záznam nařídit policejní orgán sám, ovšem pouze se souhlasem[125] uživatele odposlouchané stanice. Procesně požadovanou formou výsledku odposlechu a záznamu je protokol, který obsahuje údaj o místě, času, způsobu a obsahu provedeného záznamu společně se zvukovým, obrazovým či obdobným záznamem.

V souvislosti s elektronickými důkazy lze zmínit, že odposlech a záznam představují velmi užitečný nástroj pro objasňování skutku, zejména v případech, trestných činů „bez oběti", například různých hospodářských trestných činů. Pojem *telekomunikační provoz* ingeruje do trestního práva procesního ze zákona č. 127/2005 Sb., o elektronických komunikacích, podle jehož § 136 odst. 20 písm. a): „*Obsahuje-li zvláštní právní předpis ustanovení o telekomunikačním provozu, rozumí se tím přenášená zpráva podle tohoto zákona.*" Kolouch[126] k tomu poznamenává, že výše uvedený zákon předpokládá, že se jedná o jakoukoliv „*informaci, která se vyměňuje nebo přenáší mezi konečným počtem účastníků nebo uživatelů prostřednictvím veřejně dostupné sítě služby elektronických komunikací.*" Definice dle tohoto zákona je ale do značné míry limitující,

[125] Je-li vedeno trestní řízení pro trestný čin obchodování s lidmi (§ 168 tr. z.), svěření dítěte do moci jiného (§ 169 tr. z.), omezování osobní svobody (§ 171 tr. z.), vydírání (§ 175 tr. z.), únosu dítěte a osoby stižené duševní poruchou (§ 200 tr. z.), násilí proti skupině obyvatelů a proti jednotlivci (§ 352 tr. z.), nebezpečného vyhrožování (§ 353 tr. z.) nebo nebezpečného pronásledování (§ 354 tr. z.), postačí souhlas uživatele odposlouchávané stanice, srov. § 88 odst. 5 tr. ř.

[126] KOLOUCH, Jan, *Cybercrime*. Praha: CZ.NIC, 2016, s. 430.

neboť by se tak o telekomunikační provoz jednalo pouze ve vztahu k ISP[127]. Účelem ustanovení § 88 tr. ř. je však v mezích zákona postihnout komunikaci všemi prostředky, i proto Kolouch tvrdí, že komunikací se musí rozumět vše, co je pokládáno za výměnu informací dle Budapešťské úmluvy. K tomuto názoru se ostatně přiklonil[128] i Ústavní soud: "*S ohledem na to, že jsou stanovena pravidla pro odposlech a záznam telekomunikačního provozu ze strany těchto orgánů, která umožňují kromě dalších údajů pořídit především obsah telefonické zprávy* (pozn: např. SMS zprávy)*, je možné postupovat podle těchto pravidel i při pořizování či získávání těchto ‚dalších' údajů, tj. při evidování telekomunikačního provozu. Orgány činné v trestním řízení* […] *jsou tedy v případě pořizování či získávání evidence telekomunikačního provozu povinny postupovat přiměřeně podle § 88 trestního řádu."* Ústavní soud tak na základě analogie aproboval užití institutu záznamu a odposlechu pro širokou škálu různých technologických forem komunikace. Soud v něm mj. poukázal na skutečnost, že právě odposlech a záznam jsou relativně přísné instituty co do podmínek povolení i následné kontroly zákonnosti a proporcionality.

Právě podle ustanovení § 88 tr. ř. probíhá často monitorování elektronické komunikace, ať už je to telefonem, mobilním telefonem, ale i pomocí e-mailů, VoIP[129] sítí, či různých textových či audiovizuálních přenosech. Pomocí záznamu a odposlechu lze rovněž monitorovat aktivitu na sítích, kdy provozovatel je povinen strpět určité zásahy a při odposlechu poskytnout patřičnou součinnost (srov. např. § 96 zákona o elektronických komunikacích). Provozovatelé, kteří podléhají zákonu o elektronických komunikacích, jsou navíc povinni poskytnout Policii České republiky záznamy, jež jsou ve srozumitelné podobě, tedy např. nešifrované.

Vzhledem k tomu, že odposlech a záznam telekomunikačního provozu podléhají ze všech forem zajišťování důkazů nejširšímu kontrolnímu mechanismu, zcela jistě se bude jednat o ustanovení speciální vůči operativně pátracím prostředkům dle § 158d.[130] Pokud je tedy nařízeno sledování

[127] ISP je anglická zkratka *Internet service provider*, neboli poskytovatele internetového připojení, srov. § 2 písm. d) zákon č. 480/2004 Sb., o některých službách informační společnosti: „poskytovatelem služby každá fyzická nebo právnická osoba, která poskytuje některou ze služeb informační společnosti".

[128] Nález Ústavního soudu České republiky č. II. ÚS 502/2000, ze dne 22. listopadu 2000.

[129] VoIP (anglicky „*Voice over IP"*) je forma komunikace používající internetový protokol, jedná se o standardní prostředek hlasových služeb, který nemusí být přímo závislý na mobilních či terestriálních poskytovatelích telekomunikačních služeb. Typicky se využívá ve firemních sítích (tzv. IP telefonie). Pozitivně je upraven v zákoně o elektronických komunikacích.

[130] KOLOUCH, Jan, *Cybercrime*. Praha: CZ.NIC, 2016, s. 442.

osob a věcí, přestože se jedná o telekomunikační provoz, bude se jednat o důkaz, který trpí vadou (viz. kapitola 4.3).

5.2.7 Vyžádání údajů o uskutečněném telekomunikačním provozu

Podobně jako záznam a odposlech telekomunikačního provozu, i vyžádání údajů o uskutečněném telekomunikačním provozu upravené v § 88a tr. ř. je zásahem do práva na soukromí osoby. I na tento institut se vztahují relativně striktní omezení pro povolení získání záznamu. Trestní řád jej umožňuje vyžadovat pouze pro úmyslné trestné činy, u kterých trestní zákoník stanovuje trest odnětí svobody nejméně tři roky, a dále pro vyjmenované úmyslné trestné činy (např. nebezpečné vyhrožování, neoprávněný přístup k počítačovému systému a nosiči informací nebo trestný čin podvodu) a pro úmyslné trestné činy, k jejichž stíhání se Česká republika zavázala mezinárodní smlouvou.[131]

Využití záznamu lze považovat za méně závažný zásah do soukromí jedince, proto jsou oproti odposlechům a záznamům provozu podmínky nastaveny mírněji: soudce může k vydání takových informací vydat příkaz na návrh státního zástupce v přípravném řízení, v řízení před soudem vydává takový příkaz předseda senátu. Podobně jako v případě odposlechu a záznamu provozu podléhá záznam podmínce subsidiarity zásahu do práv osoby, jejíž údaje jsou zpracovávány. Podle § 97 odst. 3 písm. b) zákona o elektronických komunikacích je adresátem tohoto příkazu právnická či fyzická osoba, která takové zařízení provozuje.[132] Trestní řád zároveň upravuje možnost zpřístupnit údaje bez ohledu na výše uvedená omezení, pokud souhlas s jejich poskytnutím udělí uživatel telekomunikačního zařízení, případně pokud je třeba těchto údajů využít pro operativní bezodkladné úkony pátraní po některých osobách.[133] Trestní řád nespecifikuje, kým se rozumí *uživatel telekomunikačního zařízení*, podle logiky chráněného práva na soukromí se musí jednat o uživatele, jehož záznamy mají být zjištěny, tedy nejčastěji koncový uživatel tohoto zařízení.

---

[131] Viz výše výklad k odposlechu a záznamu telekomunikačního provozu v kapitole 5.2.6.

[132] KUCHTA, Josef. *Zajišťovací úkony a předběžná opatření.* In: ŠÁMAL, Pavel, MUSIL, Jan, KUCHTA, Josef a kol. *Trestní právo procesní. 4. přepracované vydání*. Praha: C. H. Beck, 2013, s. 331.

[133] Podle § 96 odst. 3 písm. b) zákona o elektronických komunikacích. může údaje využít i policie, jestliže tak činí *„pro účely zahájeného pátrání po konkrétní hledané nebo pohřešované osobě, zjištění totožnosti osoby neznámé totožnosti nebo totožnosti nalezené mrtvoly, předcházení nebo odhalování konkrétních hrozeb v oblasti terorismu nebo prověřování chráněné osoby a při splnění podmínek stanovených zvláštním právním předpisem“*.

V souvislosti se zajištěním takových dat je ovšem důležité se vypořádat s otázkou, zda lze příkaz získat i pro data, která vzniknou v budoucnosti, nebo pouze pro data, která vznikla do okamžiku vydání rozhodnutí. Ustanovení § 88a tr. ř. nedává na tuto otázku jednoznačnou odpověď. Například Kolouch ve své monografii argumentuje, že je třeba vycházet z jazykového a historického výkladu tohoto ustanovení, neboť předchozí úprava uváděla jako předmět zajištění „*[data] o uskutečněném telekomunikačním provozu* […]," zatímco současná úprava upravuje předmět zajištění jinak: „*Je-li třeba zjistit údaje o telekomunikačním provozu* […]."[134] S touto interpretací však nelze souhlasit. Jedná se o jistou formu analogie v trestním právu, která *a priori* není v trestním právu procesním nedovolená, ovšem v tomto případě se jedná o jednoznačný zásah do ústavně daných práv osoby, uživatele, případě dalších osob, jejichž údaje jsou získávány. Analogie je v tomto případě nepřípustná, neboť analogií nelze zasahovat do ústavních práv jedince[135], jak již bylo uvedeno výše v kapitole 4.4, a rozšiřovat časový úsek, pro který jsou lokalizační a provozní údaje zaznamenávány a následně *pro futuro* i zajišťovány. Jestliže není v ustanovení § 88a stanovena doba, musí se vycházet ze zásady minimalizace zásahů do práv osob a ze zásady enumerativnosti veřejnoprávních pretenzí. Pokud by orgány činné v trestním řízení potřebovaly zajistit provoz (tedy *de facto* monitorovat aktivitu v telekomunikačním zařízení, např. v počítačové síti) i v budoucnu, je potřeba pro takové monitorování zajistit příkaz dle § 88 tr. ř., který stanovuje jednoznačné lhůty pro užití, a navíc lépe chrání ústavní práva uživatelů. Podobný názor s ohledem na oprávněnost nařízení záznamu do budoucna zastává část odborné veřejnosti.[136]

Institut vyžádání údajů o telekomunikačním provozu je silným instrumentem orgánů činných v trestním řízení. V dnešní době je běžné, že každý zanechává své lokalizační údaje na každém kroku, ať již ve formě komunikace s věží mobilního operátora, či během prohlížení internetových stránek. Oprávnění vyžadovat takové informace, i vzhledem k tomu, že jsou to často informace soukromé, patří mezi zásadní zásahy do práv člověka.

[134] KOLOUCH, Jan, *Cybercrime*. Praha: CZ.NIC, 2016, s. 443.
[135] JELÍNEK, Jiří. *Trestněprávní normy, jejich výklad a působnost.* In: JELÍNEK, Jiří a kol. *Trestní právo procesní. 2. aktualizované vydaní*. Praha: Leges: 2011, s. 72.
[136] JELÍNEK, Jiří. *K chybějící právní úpravě tzv. prostorového odposlechu v trestním řádu.* Bulletin advokacie, 2018, č. 7-8, 2018, s. 15.

5.2.8 Operativně pátrací prostředky

Nad rámec toho, co bylo rozebíráno v kapitole 5.1.2, je pro přípustnost operativně pátracích prostředků, zejména pak sledování věcí, nutno zmínit, že je vždy potřeba na ně pohlížet jako na důkazní prostředek, který by měl být využíván subsidiárně k ostatním, pozitivně upraveným, důkazním prostředkům. Například sledováním věci dle § 158d tr. ř. by bylo sice možné zajistit důkazy o provozních a telekomunikačních datech, ale vzhledem ke specialitě ustanovení § 88a vůči § 158d tr. ř. by takové povolení bylo v rozporu se zákonem. Na problematické aspekty využití tohoto důkazního prostředku mj. upozorňuje[137] i Jelínek. Pokud však žádný jiný institut nelze použít při zajištění důkazů, nezbude orgánu činnému v trestním řízení nic jiného, než zajistit jej podle § 158d tr. ř. Tento důkazní prostředek se v souvislosti s elektronickými důkazními prostředky užívá při zajišťování obsahu serverů či internetových stránek, pokud se nejedná o provozní nebo lokalizační data, více níže v kapitole 6.1.

5.2.9 Data freeze

Zcela novým důkazním prostředkem je institut uložení povinnosti osobě při zajištění dat, někdy také nazývaný *data freeze*. Data freeze, upravený v § 7b tr. ř., byl do trestního řádu přidán v novelou zákonem č. 287/2018 Sb., kterým se mění zákon č. 40/2009 Sb., trestní zákoník:

> *(1) Je-li zapotřebí zabránit ztrátě, zničení nebo pozměnění dat důležitých pro trestní řízení, která jsou uložena v počítačovém systému nebo na nosiči informací, lze nařídit osobě, která uvedená data drží nebo je má pod svojí kontrolou, aby taková data uchovala v nezměněné podobě po dobu stanovenou v příkazu a učinila potřebná opatření, aby nedošlo ke zpřístupnění informace o tom, že bylo nařízeno uchování dat.*
>
> *(2) Je-li to zapotřebí k zabránění pokračování v trestné činnosti nebo jejímu opakování, lze nařídit osobě, která drží nebo má pod svojí kontrolou data, která jsou uložena v počítačovém systému nebo na nosiči informací, aby znemožnila přístup jiných osob k takovým datům.* […]

[137] JELÍNEK, Jiří, *K chybějící právní úpravě tzv. prostorového odposlechu v trestním řádu*. Praha: Bulletin advokacie, 7-8, 2018, s. 17.

Zařazení předmětného ustanovení do trestního řádu je výsledkem opožděné implementace mezinárodních závazků České republiky vyplývajících z Budapešťské úmluvy, konkrétně článků 16 a 29.[138] Data freeze nelze jednoznačně nazvat důkazním prostředkem, neboť pomocí něj nelze zajistit důkaz, jedná se totiž spíše o operativní postup orgánu činného v trestním řízení směřující k zachování potenciálního důkazu. Osoba, která je adresátem příkazu, je povinna data vymezená v rozhodnutí zajistit před změnou po dobu stanovenou v příkazu, nejdéle však 90 dní, příkaz může rovněž obsahovat povinnost znepřístupnit tato data uživateli. V přípravném řízení vydává příkaz státní zástupce, v řízení před soudem předseda senátu a v případech, kdy nelze předchozí souhlas včas zajistit, může data freeze nařídit i sám policejní orgán. Na rozdíl od úpravy institutu uchovávání telekomunikačních dat například pro potřeby vyžádání záznamů dle § 88a tr. ř.[139] se jedná o veškerá data vymezená v příkazu. Důvodová zpráva dále uvádí, že v souladu s Budapešťskou úmluvou se jedná o veškerá myslitelná data, tedy i například signály či data uložená v krátkodobých pamětích (např. RAM, data uložená v technických úložištích komponentů apod.).

Jak bylo zmíněno, nejedná se o klasický důkazní prostředek, ale spíše o opatření, kterým si orgány činné v trestním řízení vyžádají zajištění ohrožených dat. Má-li tato data v držení osoba, která není osobou důvěryhodnou (tedy osobou, která by mohla mít zájem na tom taková data zničit či změnit), může orgán činný v trestním řízení nařídit zajištění těchto dat do doby, než bude možné je procesně správně zajistit (např. přizváním znalce).

Důležitost tohoto procesního institutu je možné spatřovat i v rámci mezinárodní justiční spolupráce.[140] Vzájemné uznávání těchto institutů ve více zemích může mít pozitivní vliv na odhalování trestné činnosti v souvislosti s globalizací kybernetické kriminality.

Vzhledem k tomu, že toto ustanovení vstoupilo v účinnost 1. února 2019, je otázkou, zda bude použitelné. Pokud orgány činné v trestním řízení chtějí procesně data zajistit, mohou pro to využít

[138] 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.

[139] Povinnost tzv. *data-retention period* tedy povinnosti uchovávat provozní data provozovatelů telekomunikačních sítí vychází z povinnosti stanovené zákonem č. 27/2005 Sb., o elektronických komunikacích v § 97, odst. 3, data retention směřuje vůči údajům všech uživatelů, na rozdíl od data freeze, kde povinnost směřuje ke konkrétním datům označeným v příkazu.

[140] Srov. § 65a zákona č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních, který byl novelizován společně s § 7b tr. ř.

přímo instituty k tomu určené (např. dle § 88a tr. ř., vydání věci dle § 78 tr. ř., sledování věci dle § 158d tr. ř. apod.). Pokud by postupovaly dle § 7b tr. ř., mohlo by se z jejich pohledu jednat o zdvojení činnosti. Na druhou stranu data freeze přináší možnost rychle a operativně zajistit data před změnou či zničením zejména v přípravném řízení i bez předchozího souhlasu soudu.

5.3 Dokazování

Dokazováním se rozumí „*trestním řádem vymezený postup orgánů činných v trestním řízení za zákonem vymezené součinností stran, jehož smyslem je poznání skutkových okolností důležitých pro další postup orgánů činných v trestním řízení a v konečné fázi i pro rozhodnutí.*“[141] Tato podkapitola se na rozdíl od předchozí kapitoly specificky zabývá postupem, kterým se prokazují skutečnosti důležité pro trestní řízení, nikoliv postupem orgánů pro procesně použitelné zajištění takových důkazů.

Jak píše Jelínek[142] a jak bylo zmíněno výše, trestní řád poskytuje v § 89 odst. 2 pouze demonstrativní výčet použitelných důkazů. Mezi výslovně upravené důkazy patří výslech obviněného a svědka, zvláštní způsoby dokazování (konfrontace, rekognice, vyšetřovací pokus, rekonstrukce a prověrka na místě), znalecké zkoumání, ohledání. Cílem této kapitoly je popsat mechanismy, které jsou při zajišťování elektronických důkazů dobře použitelné. Zde je třeba podotknout, že ne všechny instituty jsou způsobilé k tomu umožnit přímé zajištění elektronických důkazů. Například výpověď obviněného či svědka je typickým, navíc v případě obviněného též obligatorním,[143] důkazem v trestním řízení. Pro účely elektronických důkazů jsou však některé důkazní prameny z logiky věci nezpůsobilé k tomu, aby obsahovaly elektronické důkazy. Další text tedy omezí výklad pouze na ty důkazní prostředky, které jsou v tomto smyslu nejpoužitelnější, tedy na ohledání a znalecké, případně odborné vyjádření. Oba instituty jsou vzájemně provázány, neboť ohledání často provádí znalec.

[141] ŠÁMAL, Pavel. *Dokazování v trestním řízení.* In: ŠÁMAL, Pavel, MUSIL, Jan, KUCHTA, Josef a kol. *Trestní právo procesní. 4. přepracované vydání*. Praha: C. H. Beck, 2013, s. 346.
[142] JELÍNEK, Jiří. *Jednotlivé důkazní prostředky.* In: JELÍNEK, Jiří a kol. *Trestní právo procesní. 2. aktualizované vydaní*. Praha: Leges: 2011, s. 383.
[143] Srov. např. § 92 odst. 2, § 207 odst. 1 tr. ř.

5.3.1 Ohledání

Ohledání je běžným úkonem orgánů činných v trestním řízení při dokazování. Trestní řád upravuje institut ohledání v § 113:

(1) Ohledání se koná, mají-li být přímým pozorováním objasněny skutečnosti důležité pro trestní řízení. K ohledání se zpravidla přibere znalec.

(2) Protokol o ohledání musí poskytovat úplný a věrný obraz předmětu ohledání; mají se proto k němu přiložit fotografie, náčrty a jiné pomůcky.

Předmětem ohledání může být osoba či věc (ve smyslu § 489 zákona č. 89/2012 Sb., občanský zákoník, tedy „*vše, co je rozdílné od osoby a slouží potřebě lidí*“ včetně věcí nehmotných, například dat uložených na nosiči informací[144]). Přestože trestní řád v § 113 odst. 1 větě druhé stanovuje, že by se k ohledání zpravidla měl přibrat znalec, praxe orgánů činných v trestním řízení tomu neodpovídá, neboť ohledání je rutinním úkonem a přibrání znalce by bylo nejen zbytečné (např. přečtení listinného důkazu), ale i nákladné[145]. Výsledkem ohledání je formální protokol o ohledání, ve kterém osoba, která ohledání provedla, vylíčí všechny podstatné okolnosti a případně i přiloží další informace (např. videozáznam z ohledání). Samotný úkon ohledání, který činí orgán činný v trestním řízení, probíhá zpravidla za účasti techniků, zaměstnanců Policie ČR (srov. § 112 odst. 1 z. pol. ČR).

Ohledání věci je procesním úkonem, kterým se přímým pozorováním pramenu důkazu osoba k tomu oprávněná seznamuje s obsahem či vlastnostmi dané věci. Při objasňování kriminality, která zahrnuje elektronické důkazy, se lze často s důkazním materiálem jednoduše a efektivně seznámit pomocí ohledání. Jak podotýká Polčák: „[ohledání se provádí] *pomocí vstupních a výstupních komponent zařízení. V případě počítače například pomocí klávesnice, myši, monitoru, případně tiskárny. Stejně tak lze ohledat dostupná data online, například prostřednictvím počítače vyšetřovatele.*“[146] V případě prostého ohledání však důkaz může trpět dvěma závažnými vadami,

[144] Trestní zákoník v § 134 také upřesňuje, co je věcí:„*Věcí se rozumí i ovladatelná přírodní síla. Ustanovení o věcech se vztahují i na živá zvířata a zpracované oddělené části lidského těla, nevyplývá-li z jednotlivých ustanovení trestního zákona něco jiného.*“ Tato definice je však pro účely elektronických důkazů nedostačující.

[145] ŠÁMAL, Pavel. *Dokazování v trestním řízení.* In: ŠÁMAL, Pavel, MUSIL, Jan, KUCHTA, Josef a kol. *Trestní právo procesní. 4. přepracované vydání*. Praha: C. H. Beck, 2013, s. 404.

[146] STUPKA, Václav. *Kyberkriminalita*. In: POLČÁK, Radim a kol. *Právo informačních technologií.* Praha: Wolters Kluwer, 2018, s. 586.

jednak nižší vypovídající hodnotou a jednak může být důkaz neodbornou manipulací znehodnocen. Policista či zaměstnanec Policie ČR by měl v každém případě hodnověrně zaznamenat průběh takového ohledání, tj. jakým způsobem se dostal k datům, jaký program použil apod., nejlépe přímo do protokolu o ohledání, případně metodiku o přístupu a ohledání dat přidá jako přílohu protokolu. Právě řádná dokumentace procesu o přístupu k datům je klíčová, bez jednoznačného a dokumentovaného postupu (zpravidla prováděného policejním orgánem) nelze vždy hodnověrně replikovat výsledky. Nebezpečí znehodnocení důkazu nesprávným nakládáním je akutní, a to zejména pro data, která jsou nestabilní (např. operační paměť). Obě nebezpečí mohou být minimalizována zapojením odborného pracovníka specificky vyškoleného na zajišťování elektronických stop, ovšem nejbezpečnějším přístupem s ohledem na volatilitu elektronických důkazů je využití znalce.

5.3.2 Využití posudku znalce a odborné vyjádření

Znalcem se rozumí osoba, která má speciální odborné znalosti ve své znalecké oblasti. Zákon č. 36/1967 Sb., o znalcích a tlumočnících, v § 4 odst. 1 písm. e) stanovuje, že jmenovat znalcem lze osobu, která „*má potřebné znalosti a zkušenosti z oboru* […]*, v němž má jako znalec* […] *působit, především toho, kdo absolvoval speciální výuku pro znaleckou* […] *činnost, jde-li o jmenování pro obor* […]*, v němž je taková výuka zavedena.*“ Osobu znalce zpravidla jmenuje předseda krajského soudu (srov. § 3 odst. 1 zákona o znalcích a tlumočnících). Jmenovaný znalec je následně zapsán společně se svou expertizou do seznamu znalců a tlumočníků, který vedou krajské soudy. Úkolem znalce v trestním řízení je nestranně posoudit skutkové okolnosti, které jsou důležité pro vydání rozhodnutí. Specifickou roli pak hrají znalecké ústavy, jejich služeb je využíváno buď jako prostředku pro přezkoumání znaleckého posudku, případně pro zvlášť náročné znalecké posuzování.[147] Jestliže orgán činný v trestním řízení v přípravném řízení, případně předseda senátu v řízení před soudem, vyhodnotí, že je potřeba přizvat znalce, učiní tak opatřením. Důkaz znaleckým posudkem se provede buď výslechem znalce do protokolu nebo se znalec odvolá

[147] Srov. § 110 odst. 1 tr. ř., Nejvyšší soud ČR v rozhodnutí sp. zn. 5 Tdo 113/2013-79 ze dne 26. června 2013 mj. kritizoval nadužívání posudků ústavů, posudek ústavu by tak skutečně měl být užit pouze v nejsložitějších věcech a přibrání znaleckého ústavu či obdobné instituce musí být řádně zdůvodněno.

na písemné vyhotovení posudku a formálně jej tak potvrdí. Alternativně se posudek či protokol o výslechu znalce přečte, jsou-li dány podmínky dle ustanovení § 211 odst. 5 tr. ř.[148]

Odborné vyjádření představuje další formu důkazu, respektive zkoumání odborných skutkových okolností. Odborné vyjádření se zpravidla opatřuje v jednodušších případech nebo v oblastech, ve kterých není zapsán žádný znalec. Fryšták k tomu poznamenává: „*Odborné vyjádření nemá nikde stanovené přesné formální náležitosti jako je jeho obsah, forma atd., nemusí (ale může) být vypracováno znalcem nebo znaleckým pracovištěm, ani není výsledkem znalecké činnosti. Jde o ‚odborné vyjádření' osoby znalé, tzn. odborníka k určité dílčí otázce.*"[149] Z formálního hlediska je rozdíl mezí znaleckým posudkem a odborným vyjádřením pouze forma výstupu. Odborné vyjádření je listinný důkaz ve smyslu § 112 tr. ř., na druhou stranu znalecký posudek, respektive výslech znalce, je důkazem *sui generesis*. Jak vyplývá ze zásady volného hodnocení důkazů, oba důkazy mají formálně stejnou důkazní sílu, ale v praxi je důkazní síla znaleckého posudku významná a pro objasnění skutkových okolností často představuje klíčový důkaz.

Nelze jednoznačně říci, že by se odborná vyjádření pro analýzu elektronických důkazů nevyužívala, ale typicky se pro řádné ohledání a interpretaci dat užije znalecký posudek.[150] Pro oblast elektronických dat je nejčastěji využívaným znaleckým oborem kybernetika, podobor výpočetní technika, případně kybernetická odvětví různá.[151] Znalec se v souvislosti se zajišťováním a zkoumáním elektronických důkazů objevuje v průběhu vyšetřování skutku ve dvou základních rolích: v roli osoby, která se účastní ohledání místa činu a zajištění případných nosičů důkazního materiálu, a v roli osoby, která expertně zkoumá nosiče a extrapoluje z dat skutečnosti relevantní pro trestní řízení (samotné znalecké zkoumání na základě zadaných otázek pro znalecký posudek).

---

[148] PÚRY, František. *Dokazování v trestním řízení.* In: POLČÁK, Radim. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 80.

[149] FRYŠTÁK, Marek. *Dny práva – 2010 – Days of Law, 1. vyd.: Odborné vyjádření versus znalecký posudek*. Brno: Masarykova Univerzita, 2010, s. 2.

[150] STUPKA, Václav. *Kyberkriminalita*. In: POLČÁK, Radim a kol. *Právo informačních technologií.* Praha: Wolters Kluwer, 2018, s. 583.

[151] SMEJKAL, Vladimír. *Kybernetická kriminalita. 2. rozšířené a aktualizované vydání*. Plzeň: Aleš Čeněk, 2018, s. 732.

Důvodem přítomnosti znalce při zajišťovacích úkonech je skutečnost, že často disponuje odbornými znalostmi, které převyšují znalosti či schopnosti policejních techniků. V této roli často figuruje jako konzultant, který dbá na to, aby data byla řádně technicky zajištěna, např. formou vytvoření identické bitové kopie.[152] Jak pokračuje Kolouch, je žádoucí, aby datové nosiče nebyly jakýmkoliv způsobem změněny či poškozeny, takové kopie lze následně podrobit zkoumání, aniž by došlo ke znehodnocení zdrojového datového nosiče. Některé systémy mohou odpojením od zdroje smazat část své paměti, případně restartováním může dojít k procesu zašifrování informace.[153] Znalecký posudek, jenž je výsledkem znaleckého zkoumání, odpovídá na otázky, které znalec obdržel v zadání posudku.

[152] KOLOUCH, Jan, *Cybercrime*. Praha: CZ.NIC, 2016, s. 452.
[153] VYSKOČIL, Ladislav: *Zajišťování digitálních stop.* [online] Policie ČR: SKPV KŘP JmK Brno, s. 15. Prezentace.

6 Aplikace v trestněprávní praxi

Počítačové a výpočetní systémy a s nimi související elektronická data, která lze používat pro účely trestního řízení, jsou na území České republiky, respektive Československa, už více než půl století. Trestní řád na tento specifický druh důkazů zatím nedokázal komplexně reagovat. Dokud byla výpočetní technika pouze v rukou několika státních, zejména pak výzkumných institucí, nebylo nutné se datům podrobně věnovat. S rozvojem internetu, osobních počítačů, mobilních telefonů a spotřební elektroniky, které generují značné množství dat, jež mohou být použita mj. v trestním řízení, je záhodno se zamyslet nad tím, jak orgány činné v trestním řízení postupují, jakým způsobem se zjišťují skutečnosti z datových nosičů a jak se nauka a praxe prolínají.

6.1 Vybrané zdroje důkazů

Existuje nepřeberné množství různých elektronických důkazů a nosičů stop, které mohou mít hodnotu pro trestní řízení. Ať už se jedná o zvukové nahrávky, záznamy z kamerových systémů, počítačový kód nebo lokalizační data GPS. Následující kapitola se bude zabývat několika z v praxi nejobvyklejších pramenů důkazů, které orgány činné v trestním řízení využívají za účelem zjištění skutkového stavu. E-mail byl vybrán jako pramen důkazů, který má vnější charakteristiky listiny a používá se často v soukromé i veřejné korespondenci. Obsah internetových stránek byl vybrán pro ukázání rozdílu mezi soukromým a veřejným pramenem důkazu. A konečně data získaná z korespondence pomocí tzv. *instantních messengerů* jsou důležitá pro jejich specifika při zajišťování od poskytovatelů, kteří zpravidla nespadají pod českou jurisdikci.

6.1.1 E-mail

Jednou z nejčastějších dorozumívacích metod (nejen) v kybernetickém prostoru je v současnosti bezesporu e-mail a jeho přílohy. Z legálního hlediska[154] jde dle § 2 písm. b) zákona o některých službách informační společnosti o „*textová, hlasová, zvuková nebo obrazová zpráva poslaná*

[154] Zákon o některých službách informační společnosti sice uvádí, že definice e-mailu se užije pouze pro účely tohoto zákona, ovšem mám za to, že pro interpretační účely je v pořádku přiměřeně použít tuto definici i pro jiné oblasti práva.

prostřednictvím veřejné sítě elektronických komunikací, která může být uložena v síti nebo v koncovém zařízení uživatele, dokud ji uživatel nevyzvedne.“ Tato komunikace je zpravidla soukromého charakteru[155], tedy mezi předem určeným odesílatelem a příjemcem zprávy, a požívá podobné ochrany jako poštovní zásilka.[156] Technologie e-mailu funguje na principu výměny informací mezi uživatelským rozhraním, které pomocí STMP protokolu Mail Transfer Agent (MTA) serveru předá informaci o destinaci odeslané zprávy. MTA následně rozhodne o směřování zprávy na základě dotazu na DNS (*Domain Name Server*), který jej nasměřuje na konkrétní server adresáta, adresát si následně zprávu může vyzvednout ve svém MTA.[157]

Obsah e-mailu je považován podobně jako obsah dopisu za důvěrnou informaci, která podléhá ochraně garantované Listinou (viz výše). Proto každé jeho zobrazení musí být řádně aprobováno příslušným institutem zajištění důkazu. Pokud není e-mail vydán dobrovolně (srov. § 78 tr. ř.), je vždy potřeba souhlasu soudu, pokud e-mail nelze zajistit jako fyzickou zprávu na zařízení, které má osoba u sebe. Zajištění e-mailu jako datové zprávy může proběhnout v několika fázích ukládání či přenosu,[158] přičemž v každé fázi jde o jiné technologické řešení intercepce:

(i) během vytváření (pasní);

(ii) po uložení konceptu e-mailu;

(iii) v průběhu odeslání na MTA odesílatele;

(iv) během přenosu mezi MTA odesílatele a MTA příjemce;

(v) v průběhu stahování z MTA příjemce, případně během zobrazování e-mailu na cílovém serveru MTA (např. rozhraní Gmail.com);

(vi) po stažení zprávy do zařízení příjemce; a

(vii) po smazání zprávy.

---

[155] Faktem je, že více než 50 % emailové komunikace je tzv, nevyžádanou komunikací (*spam*), takové sdělení ale zpravidla nemá parametry, které by ji považovaly za komunikaci soukromou, viz např. *Spam: share of global email traffic 2014-2018: Global spam volume as percentage of total e-mail traffic from January 2014 to September 2018, by month.* Statista: The Statistics Portal [online]. New York: Statista, 2019, 2019 [cit. 2019].

[156] KLEMENT, Petr. *Dokazování e-mailem.* In: POLČÁK, Radim. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 117.

[157] WEIR, George R. S., MASON, Stephen. *The sources of electronic evidence.* In: MASON, Stephen, SENG, Daniel. *Electronic Evidence, Fourth edition*. London: University of London, Institute of Advanced Legal Studies for the SAS, 2017, s. 14.

[158] KOUHOUT, Jiří a BEHR, Tomáš. *Elektronická pošta a její záznam pro trestní řízení.* Trestněprávní revue. 2011, 10(4),, s. 101.

Pro přehlednost se tato práce bude zabývat pouze případem, kdy pro administraci bude využíván pouze e-mailový klient (např. MS Outlook).[159] Body (i), (ii), (vi) a (vii) probíhají zpravidla na lokálních zařízeních odesílatele, respektive příjemce zprávy. Jestliže není dosaženo dobrovolného vydání věci, musí se orgán činný v trestním řízení vypořádat s otázkou, kdy je e-mailová zpráva doručena adresátovi a nevztahuje se na ní Listinou uznaná ochrana přepravovaných zpráv. Nejvyšší soud rozhodl, že zajištění důkazu doručené zprávy je možné v souladu s § 77, resp. § 78 tr. ř., neboť tato ustanovení dostatečně chrání práva osoby, od které tato data byla získána „[…] *je nezbytné rozdělit ochranu listovního tajemství, resp. ochranu tajemství zpráv dopravovaných v telekomunikačním provozu, na etapu přepravy a období, kdy již zpráva byla doručena* […] *Pokud jde o etapu přepravy,* […] *nelze k prolomení ochrany tajemství těchto zpráv v době, kdy jsou přepravovány k jejich adresátovi vystačit s aplikací institutů vydání a odnětí věci. Pro zjištění obsahu těchto zpráv je nezbytné použít postup předpokládaný § 86, § 87 a § 88 tr. ř* [pozn. podle současné úpravy by do výčtu spadal i postup dle § 88a tr. ř.]. *Avšak v případě, že zpráva již příjemci byla předána – je v jeho dispozici, zvýšená ochrana, kterou požívala v průběhu přepravy končí. Je pouze na příjemci zprávy, jak s ní naloží,* […] *nic nebrání aplikaci postupu podle ustanovení § 78 a § 79 tr. ř., které jsou dostatečným zákonným podkladem předpokládaným čl. 13 Listiny pro prolomení ochrany tajemství takových zpráv, pokud jsou uchovávané v soukromí.*"[160] Nelze-li datový nosič zajistit odnětím věci, je potřeba přistoupit k jinému způsobu zajištění. Typicky se nabízí domovní prohlídka, prohlídka jiných prostor a pozemků apod.

Jestliže se zpráva nenachází v dispozici odesílatele či adresáta, tedy je-li na zařízeních poskytovatele služby, tzv. na cestě, je situace o něco složitější. E-mail totiž bude v režimu přepravované zprávy a bude podléhat přísnějšímu režimu zajištění. Jak bylo uvedeno v kapitole 5.2, přístup k takovým datům by měl být zásadně omezen a zajištění důkazu by mělo probíhat formou získání povolení nasazení operativně pátracího prostředku dle § 158d odst. 3 se souhlasem soudu. Jak dovozuje Stupka: „*chtějí-li* [orgány činné v trestním řízení] *přistupovat k* […] *datům po*

[159] Pokud by uživatel pro psaní užíval webových stránek, tzv. internetového klienta, byla by data zpravidla uložena na serveru poskytovatele této služby. Některé služby umožňují agregaci více e-mailových adres do jedné společné schránky, logika zajištění je však podobná jako v případě jedné adresy, pouze je potřeba dávat pozor, zda se zpráva nachází na serveru poskytovatele služby, nebo na lokálním zařízení uživatele.

[160] Usnesení Nejvyššího soudu ČR sp. zn. 7 Tz 9/2000 ze dne 15. prosince 2000.

překonání bezpečnostního opatření, jde o poměrně zásadní zásah do práv a svobod.“[161] Je-li tak e-mail uchováván na serveru poskytovatele služby, je vždy žádoucí, aby bylo vyžádáno nasazení těchto prostředků.

Poslední možností, leč z praktického hlediska spíše okrajovou, je zajištění e-mailu v průběhu doručování, tedy po odeslání a před doručením adresátovi, dle rozdělení výše se jedná o body (iii), (iv) a (v). Mechanismy zajištění pomocí institutu zadržení, otevření a sledování zásilky jsou z technicko-právních důvodů v podstatě vyloučeny (srov. kapitolu 5.2.5). Orgány činné v trestním řízené se tak většinou musí uchýlit k jiným institutům. Technické provedení intercepce e-mailu není složité,[162] fakticky je však potřeba postupovat podle § 88 tr. ř., neboť na takové zprávy se vztahuje ochrana přepravovaných zpráv. Zákonodárce pro přepravované zprávy stanovil přísnější režim jak pro povolování, tak pro následnou kontrolu.

Ověření věrohodnosti odesílatele (rozuměj e-mailového účtu) a příjemce zprávy probíhá forenzní analýzou, která prozkoumá zejména celou hlavičku e-mailu, ve které je uložena například IP adresa odesílatele a příjemce, jedinečné ID zprávy, program, který odesílatel používá, datum a čas odeslání a další informace, které mohou být pro orgány činné v trestním řízení relevantní pro posouzení nejen věrohodnosti e-mailu, ale mohou mít vliv i na zjištění jiných skutkových okolností řešené věci.[163] Skutečnost, že e-mail byl odeslán ze zjištěné IP adresy ještě sama o sobě nemusí znamenat, že byl odeslán osobou, která má k e-mailové schránce přístup. Jak zdůraznil Nejvyšší správní soud, e-mail, respektive IP adresa, ze které byl e-mail odeslán, je zpravidla nepřímým důkazem, který pouze představuje významné vodítko při posuzování skutečnosti, zda je možné uznat pachatele přestupku zodpovědným za jeho odeslání.[164]

Při zajišťování e-mailů a dokazování skutečností z nich vyplývajících musí orgány činné v trestním řízení postupovat obezřetně a vždy zvažovat, zda pro daný úkon je potřeba souhlasu soudu a jaký institut využít, jinak hrozí, že se důkaz může stát procesně nepoužitelným. V pochybách je žádoucí

[161] STUPKA, Václav. *Kyberkriminalita*. In: POLČÁK, Radim a kol. *Právo informačních technologií.* Praha: Wolters Kluwer, 2018, s. 576.
[162] Srov. KOHOUT, Jiří, BEHR, Tomáš: *Elektronická pošta a její záznam pro trestní řízení*. Praha: Trestněprávní revue 4/2011, s. 101.
[163] KLEMENT, Petr. *Dokazování e-mailem.* In: POLČÁK, Radim. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 130.
[164] Rozsudek Nejvyššího správního soudu ČR sp. zn. 1 As 90/2008 vydaný dne 17. července 2008.

vždy upřednostnit důkazní prostředek, který nabízí osobě, jejíž práva jsou zajišťovacím úkonem omezena, vždy nejvyšší míru ochrany práv.

6.1.2 Internetová stránka a sociální síť

Internet se stal součástí každodenního života, odehrává se na něm soukromá činnost, obchodní prezentace i prodej. Není proto překvapením, že internetové stránky jsou nositelem důkazů. Internet je dynamické médium, v každý okamžik se mění. Internetové stránky vznikají a zanikají, stejně tak jako jejich obsah. Obsah internetu lze rozdělit na tři kategorie[165] podle toho, jakým způsobem může uživatel přistupovat k informacím: *surface web* (tedy viditelný, uživatelský, tzv. indexovaný internet), *deep web* (obsah internetu, který není veřejně přístupný nebo není indexovaný vyhledávači, spadá sem i obsah, který je technicky či jiným způsobem zabezpečený), poslední skupinou je *dark web* (internet, na který se lze dostat pouze použitím speciálních programů).[166] Důvodem, proč je žádoucí rozlišovat jednotlivé typy přístupnosti internetu, je vyřešení otázky veřejnosti přístupu na stránku. Zatímco klasický surface web je zpravidla veřejně přístupný všem uživatelům, pro prohlížení deep webu a částečně i dark webu je často potřeba získání specifického přístupu.

I proto s ohledem na procesní pravidla zajišťování důkazů je pro orgány činné v trestním řízení klíčové odpovědět na zásadní otázku, zda webová stránka je, či není veřejnou. Jestliže stránka je veřejnou, probíhá zajištění důkazu jednoduše ohledáním a sepsáním protokolu o ohledání. Typickým formátem stránky, která je *de facto* grafickým vyjádřením kódu, je formát html za pomoci protokolu http či https. Není proto skoro nikdy žádoucí, aby zajištění stránky probíhalo pouze pomocí funkce printscreen (tedy sejmutí obrázku obrazovky), neboť takovým postupem se ztrácí velké množství dalších informací, např. metadat (viz. kapitola 2.3).

Pro data, která nejsou veřejně přístupná, platí odlišný režim. K rozlišení veřejné a soukromé informace, se vyjádřil ve věci informací na sociální síti Facebook Ústavní soud: „*Povaha sociální sítě Facebook není jednoznačně soukromá či veřejná, neboť záleží na každém uživateli, jakou míru*

[165] KOLOUCH, Jan, *Cybercrime*. Praha: CZ.NIC, 2016, s. 48.
[166] Mezi specializované programy lze zařadit například anonymizační prohlížeč Tor.

ochrany soukromí na svém profilu zvolí. Rozhodnou-li se orgány činné v trestním řízení zjišťovat z facebookového profilu informace soukromé povahy, musí dodržovat rámec stanovený zákonem a respektovat obecné principy, na nichž je založena jejich činnost, zejména šetřit ústavně zaručená práva a svobody dotčených osob."[167] Sociální sítě umožňují užitím speciálního kódu, *tzv. metatagu,* pro vyhledávače označit stránku za soukromou, tedy nevyhledatelnou skrze indexované vyhledávače. Matějka k tomu podotýká, že „[…] *společenské normy v on-line prostředí* […] *nepřímo dotvářejí určité preference člověka ve vztahu k jeho požadavkům zachovávat soukromí.* […] *Obsah* [označený jako soukromý, který by] *neměl být dále šířen* […] *umožňuje kvalitativně vyšší předpoklad* [jeho] *garance.*"[168] Technické prostředky pro označení příspěvku na sociální síti za soukromý tak sice existují, z rozhodovací praxe však zatím nevyplývá, že by orgány činné v trestním řízení takové technické aspekty určení soukromí jakýmkoliv způsobem reflektovaly. Pojmy veřejný a soukromý prostor jsou neurčitými právními pojmy, pokud je však stránka veřejně dostupná pro širokou veřejnost (např. formou prosté registrace), tj. bez nutnosti získávat specifický omezený přístup, má se za to, že je veřejnou. Na druhou stranu neveřejná stránka zpravidla obsahuje informace, které osoba, která je na internet přidala, považuje za záležitost soukromou. Pro soukromou prezentaci je žádoucí využít institut zajištění důkazu, který dostatečně zaručuje ústavně chráněná práva, tudíž pouhé ohledání není na místě, i kdyby orgány činné v trestním řízení získaly přístup k takové stránce.

Je-li potřeba získat obsah ze zdrojů, které nejsou veřejné, jsou možnosti orgánů činných v trestním řízení do jisté míry omezeny. Jestliže se nejdříve zaměříme na běžné internetové stránky spadající pod české domény *.cz*, je národním správcem domén CZ.NIC, sdružení právnících osob, které na základě smlouvy s organizací ICANN spravuje internetová doménová jména a zjišťuje identity registrovaných vlastníků domén. Spolupráce s českou entitou bývá bezproblémová, nejčastěji probíhá prostřednictví dožádání[169] na konkrétní provozní data dle § 7 tr. ř. (tzv. součinnost právnických osob). Právnické osoby, které jsou osoby povinné dle zákona o elektronických komunikacích, mají navíc dle vyhlášky Ministerstva vnitra o uchovávání, předávání a likvidaci

[167] Nález Ústavního soudu sp. zn. III. ÚS 3844/13 ze dne 30. října 2014.
[168] MATĚJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí. 1. vydání.* Praha: CZ.NIC, 2013, s. 118.
[169] KOLOUCH, Jan, *Cybercrime*. Praha: CZ.NIC, 2016, s. 48.

provozních a lokalizačních údajů povinnost uchovávat specifická data.[170] Pokud se jedná o údaje, které mají povahu dat soukromých, je potřeba postupovat v souladu s § 88 tr. ř.

Jestliže je server v zahraničí, respektive jedná-li se o provozovatele, který nemá v České republice právní působnost, je zpravidla nutné využít institutů mezinárodní justiční spolupráce. Toto je ožehavé zejména co se týče sociálních sítí. Všechny velké sociální sítě sídlí v zahraničí, v Evropě mají často pouze obchodní zastoupení, pokud tedy neexistuje neformální dohoda o předávání dat orgánům činným v trestním řízení, může takové zajištění dat trvat delší dobu. Některé sociální sítě si vypracovaly metodiky posuzování žádostí, které do jisté míry operují mimo režim mezinárodní spolupráce v trestních věcech.[171]

Dokazování pomocí webové stránky z právního hlediska nevybočuje z ostatních institutů zajišťování důkazů. Protože je však internet globalizované prostředí, může pro orgány činné v trestním řízení zajišťování důkazů znamenat velmi úpornou práci, neboť ne vždy je možné jednoduše zajistit důkaz pro další řízení. Jestliže se orgány činné v trestním řízení neseznámí se všemi relevantními důkazy, může být rozhodnuto nespravedlivě, neboť nemusejí být zjištěny všechny důležité okolnosti skutku.

6.1.3 Komunikační platformy

Data vzniklá v souvislosti s komunikačními platformami, které se nenacházejí v české jurisdikci, jsou bezesporu jedním z nejnáročnějších důkazů na zajištění. Komunikační platformou zde rozumíme specializované nástroje či aplikace na mobilních telefonech, kterými jejich uživatelé mezi sebou v rámci sítě komunikují, nejčastěji využitím internetového či obdobného protokolu.[172] Typickými představiteli takových služeb jsou Skype, WhatsApp či Viber. Každý provozovatel aplikace užívá jiné technologické řešení. Standardně však technologie funguje na principu částečné serverové centralizace a peer-to-peer komunikace mezi klienty-uživateli. Nejběžnějším komunikačním protokolem je *Extensible Messaging and Presence Protocol*, který funguje a hraje

[170] BUDKA, Ivan. *Využití právních nástrojů pro potírání organizovaného zločinu.* Praha: Institut pro kriminologii a sociální prevenci, 2017, s. 21.
[171] Viz kapitola 6.2.3.
[172] Wikipedia. *Instant messaging.* Dostupnost z URL: https://en.wikipedia.org/wiki/Instant_messaging #Clients, datum přístupu: 22. února 2019.

roli centralizovaného serveru, jenž zpracovává primární požadavky uživatele (např. odeslání dotazu, zda osoba, které uživatel chce napsat zprávu, je online), server následně vyrozumí žadatele a adresáta o požadavku komunikace, načež samotná komunikace probíhá formou peer-to-peer, tedy přímým propojením dvou uživatelů.[173] Některé aplikace, například WhatsApp společnosti Facebook či iCloud od společnosti Apple, využívají či umožňují využívat centralizovaný server určený pro archivaci komunikace.[174]

V dalším výkladu se tato kapitola bude věnovat datům, která nebyla uložena jako archiv komunikací na serveru poskytovatele služby.[175] Pokud totiž neexistuje databáze, kde by byly uloženy zprávy či další dokumenty, je veškerý obsah ukládán tzv. *lokálně*, tedy na komunikačním zařízení uživatele (například na mobilním telefonu). Aby orgány činné v trestním řízení dosáhly na tato data, musejí se fyzicky či vzdáleně dostat ke konkrétnímu zařízení.

Zařízení je obvykle zajišťováno vydáním, odejmutím, osobní prohlídkou (má-li jej osoba u sebe), případně lze za zákonných podmínek přistoupit k domovní prohlídce, prohlídce jiných prostor a pozemků (za předpokladů uvedených v kapitole 5.2.3.). Jestliže je mobilní telefon nalezen (např. na místě činu), může jej orgán činný v trestním řízení zajistit např. ohledáním. Jak poukazují[176] Pejčochová a Elbert, „[…] *není vyloučeno, že policejní orgány namísto mobilního telefonu získají pouze data v něm uložená, a to bez vědomí uživatele."* Možnost využít § 158d odst. 3 tr. ř. k získání otisku elektronických dat potvrdil[177] také Ústavní soud: „*V rámci sledování elektronických zařízení z povahy věci plyne, že předmětem sledování budou právě data na* […] *zařízeních uložená, jejichž otisk lze pořídit za využití utajené operativně pátrací techniky. Pořízení otisku elektronických dat lze povolit postupem dle § 158d odst. 3 tr. řádu, pokud jde o data na sledovaných počítačích již uložená, nikoli o data telekomunikačního provozu.*" Jednou z možností je i užití taktických počítačových technik a nástrojů pro sledování, např. instalace software pro vzdálený přístupu do

[173] Wikipedia. *XMPP*. URL:https://en.wikipedia.org/wiki/XMPP, datum přístupu: 22. února 2019.
[174] NEWMAN, Lily Hay. Encrypted Messaging Isn't Magic. Wired [online]. New York: Wired Magazine, 2018, 14. června 2018 [cit. 2019].
[175] Postup získání přístupu k archivovanému obsahu zpráv, tedy k datům na serveru poskytovatele je obdobný jako v případě přístupu na neveřejné úložiště, orgán činný v trestním řízení by si měl opatřit souhlas soudu dle § 158d odst. 3 tr. ř., viz kapitola 5.2.8.
[176] PEJČOCHOVÁ, Alena, ELBERT, Tomáš. *Dokazování daty mobilních komunikačních zařízení.* In: POLČÁK, Radim. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 202.
[177] Srov. usnesení Ústavního soudu sp. zn. III. ÚS 3812/12 ze dne 3. října 2013.

telefonu pomocí *malware*. Problematické však může být samotné přečtení zajištěných zpráv. Některé programy umožňují uživatelské end-to-end šifrování[178] pro zajištění důvěry komunikace. Pro překonání šifrování je potřeba užít speciální postupy, typicky za pomoci znalce.

Nad rámec obsahu zpráv uživatel zpravidla při jejich zasílání zanechává různá metadata a další provozní či technická data, která mohou mít důkazní hodnotu. Komunikační platformy, které užívají centralizovanou či částečně centralizovanou infrastrukturu, uchovávají některá provozní data, např. IP adresy, data přístupu, dotazy na online status adresáta zprávy apod. Orgán činný v trestním řízení, jestliže by vyžadoval od takové platformy předmětná data, by musel postupovat v souladu s ustanovením § 88a tr. ř., tedy vyžádat součinnost provozovatele. Tento postup v praxi často naráží na globalizovanou formu internetu. Komunikační platformy obvykle nemají sídlo v Evropské unii, a už vůbec ne v České republice. Vyžádání takových dat tak může být složité a zdlouhavé.

6.2 Metodiky Nejvyššího státního zastupitelství

Ústavní ani Nevyšší soud České republiky se ve své rozhodovací praxi prozatím nedostaly ke komplexnímu hodnocení přípustnosti jednotlivých elektronických důkazních prostředků. Přestože existuje relativně bohatá judikatura národních soudů i Evropského soudu pro lidská práva k dílčím otázkám nasazení odposlechu,[179] zásahu do důvěry listovního tajemství či neplatnosti důkazů, soudy se procesními otázkami zajišťování důkazů zabývaly spíše okrajově. I proto se v souvislosti s nejednotnými postupy jednotlivých státních zástupců rozhodlo Nejvyšší státní zastupitelství vytvořit metodický pokyn pro státní zástupce, kterým by v rámci své působnosti jako hierarchicky nejvyšší orgán dozoru nad státním zastupitelstvím standardizovalo postupy při zajišťování elektronických důkazů. Právo vydávat takové stanovisko vychází z § 12 odst. 2 zákona č. 283/1993 Sb., o státním zastupitelství. Jedním z úkolů Nejvyššího státního zastupitelství je mj. „*sjednocení*

[178] End-to-end šifrování je založeno nejčastěji založeno na principu veřejného klíče, data jsou zašifrována v okamžiku, kdy je uživatel odešle adresátovi a je to pouze adresát, kdo pomocí veřejného klíče může obsah přečíst. K pojmu end-to-end šifrování viz např. TechTarget: end-to-end encryption (E2EE), dostupné z URL: https://searchsecurity.techtarget.com/definition/end-to-end-encryption-E2EE, datum přístupu: 22. února 2019.

[179] Srov. např. rozsudek Evropského soudu pro lidská práva ve věci stížnosti č. 5029/71 Klass a ostatní proti Německu ze dne 6. září 1978.

a usměrnění postupu státních zástupců při výkonu působnosti státního zastupitelství,“ přičemž tyto „*pokyny jsou závazné pro státní zástupce.*“ Důvodem, proč je žádoucí se metodikami Nejvyššího státního zastupitelství zabývat, je jejich vnitřní závaznost směrem ke státním zástupcům. Problematické aspekty metodik by mohly mít krajně nepříznivý vliv na případná budoucí trestní řízení, jestliže by Nejvyšší soud, Ústavní soud, či ESLP shledal některé postupy za vadné.

Stanoviska, která jsou určující pro elektronické důkazy, jsou tři. Jednak se jedná o stanovisko k obsahu údajů uložených na mobilním telefonu a SIM kartě vydané pod pořadovým číslem 4/2005 ve Sbírce výkladových stanovisek Nejvyššího státního zastupitelství, ze dne 6. června 2005 (dále „Stanovisko k mobilním telefonům“), dále jde o stanovisko k problematice zajišťování obsahu mobilních telefonů a jiných právních datových nosičů, včetně obsahu e-mailových schránek vydané pod pořadovým číslem 1/2015 ve Sbírce výkladových stanovisek Nejvyššího státního zastupitelství, ze dne 26. ledna 2015 (dále „Stanovisko k datovým nosičům“) a posledně stanovisko k problematice pořizování a nakládání s odposlechem a záznamem telekomunikačního provozu vydané pod pořadovým číslem 1/2018 ve Sbírce výkladových stanovisek Nejvyššího státního zastupitelství, ze dne 11. listopadu 2018 (dále „Stanovisko k telekomunikačnímu provozu“).

6.2.1 Obsah stanovisek

Stanovisko k mobilním telefonům bylo vydáno v souvislosti s rozšiřujícím se počtem uživatelů mobilních telefonů, tedy i množstvím pachatelů trestné činnosti, kteří používají mobilní telefony mj. jako nástroj usnadňující komunikaci. Mobilní telefony v té době neměly standardně internetové mobilní připojení,[180] i proto se orgány činné v trestním řízení při posuzování důkazních prostředků využitelných pro zajištění důkazu zaměřily primárně na oblast SMS, hovory v historii telefonu, data na SIM kartě a problematiku opatření dat, které se na telefon dostaly poté, co je měly k dispozici už orgány činné v trestním řízení. Podle Nejvyššího státního zastupitelství je postup dle § 78, § 79 tr. ř. ústavně konformním ve vztahu k odebrání věci a k datům, které se na této věci už

[180] Prvním tzv. „*chytrým*“ mobilním telefonem, který se dokázal masivně rozšířit na trhu byl až iPhone společnosti Apple, telefony v době vydání stanoviska měly nejčastěji pouze telefonní funkce, SMS, MMS funkce, některé dokázaly fotit fotografie v nižší kvalitě, případně ukládat a přehrávat hudební soubory, internet byl z větší části provozován pod platformou WAP, ale vybrané telefony uměly i standardní internetové připojení.

nacházejí. Alternativním důkazním prostředkem pro zajištění věcí a dat s nimi souvisejících jsou rovněž postupy dle § 82 tr. ř., tedy domovní prohlídka, případně prohlídka jiných prostor a pozemků.

Volně navazující Stanovisko k datovým nosičům reflektuje problematiku rozšíření elektronické komunikace a většího množství ukládaných dat a forem komunikace. Reflexe starší metodiky ostatně naráží i na problematiku vymezení informačních služeb v zákoně o některých službách informační společnosti. Oproti starší metodikou doporučenému postupu zajištění probíhající komunikace dle § 88a tr. ř. se Nejvyšší státní zastupitelství ve Stanovisku k datovým nosičům vymezilo vůči užívání tohoto institutu, a to s ohledem na vymezení *telekomunikačního provozu* v zákoně o elektronických komunikacích. Nejdůležitější sdělení však bezesporu vymezilo vztah užití institutu § 88 tr. ř. a operativně pátracích prostředků dle § 158d odst. 3 tr. ř. Nejvyšší státní zastupitelství správně identifikovalo, že ustanovení § 88a tr. ř. se vztahuje pouze na tzv. vedlejší, provozní data[181], nikoliv na data, která tvoří obsah sdělení, např. e-mailu. Stanovisko dále rozvíjelo další alternativu, se kterou se orgány činné v trestním řízení setkávají, a to skutečnost, že datové nosiče mohou data i po zajištění přijímat, např. formou automatického stahování e-mailů do schránky uživatele: „[…] *zjištění dodatečně došlých zpráv* […] *při absenci souhlasu uživatele podle § 88 odst. 5, resp. § 88a odst. 4 trestního řádu, možné jen na základě případného souhlasu soudce podle § 8 odst. 5 trestního řádu.*“[182] Užití obecného souhlasu soudu dle § 8 odst. 5 tr. ř. je důsledkem nejednoznačné zákonné úpravy, data automaticky stahovaná z takových úložišť (např. e-mailových serverů) totiž zpravidla podléhají důvěrnosti dle zákona o některých službách informační společnosti (viz výše), a zároveň jsou to bezesporu údaje, které podléhají ochraně základních práv a svobod. Stanovisko k datovým nosičům tak přineslo určitou jednotnost pro formu zajišťování důkazů, ale mnoho otázek zůstalo neřešených.

[181] U e-mailové, ale i další komunikace se zpravidla bude považovat za provozní informace data, která vznikají mimo vůli uživatele, jsou zpravidla výsledkem činnosti poskytovatele služby a ze své podstaty jsou technického rázu, např. IP přístupové adresy, nebo čas přístupu do schránky. Provozovatelé služeb informační společnosti však nemají na rozdíl od telefonních operátorů zákonnou povinnost tato data shromažďovat, tudíž ani nemohou dostát povinnosti taková data poskytnout, více srov. KOLOUCH, Jan, *Cybercrime*. Praha: CZ.NIC, 2016, s. 432; § 90 odst. 1 a § 91 odst. 1 zákona o elektronických komunikacích a Stanovisko Nejvyššího státního zastupitelství poř. č. 4/2015 ze dne 26. ledna 2015, s. 9.

[182] Stanovisko Nejvyššího státního zastupitelství poř. č. 4/2015 ze dne 26. ledna 2015, s. 8.

6.2.2 Neřešené otázky metodiky

Jak bylo zmíněno výše, metodické pokyny Nejvyššího státního zastupitelství se snaží sporným přístupem vyplnit mezeru v legislativě a v soudní praxi. Trestní řád nenabízí ucelený procesní návod pro užití důkazních prostředků elektronických dat. Přestože se Ústavní a Nejvyšší soud k některým dílčím otázkám, zejména pak otázkám odposlechu, vyjadřovaly opakovaně, není povaha dat jednoznačně vyřešena. Metodika jistě pomáhá státním zástupcům konajícím dozor nad trestním řízením sjednotit rozhodovací praxi v relativně složitých procesech zajišťování důkazů. Nelze však říci, že by tyto pokyny byly vyčerpávající.

Hlavním problémem současné praxe jsou data, která lze nazvat *hybridní*. Jejich povaha není ani čistě technická, ani čistě uživatelská, navíc svojí povahou jsou to často data, která je nutné považovat za citlivá a dozajista chráněná Listinou jako soukromá. Typickým příkladem jsou lokalizační data GPS, která ukládá mobilní telefon v souvislosti s provozem jednotlivých aplikací a služeb. Tato data, částečně uložená na účtu poskytovatele služby, částečně v paměti telefonu či jiného přenosného média, se pokládají za data, která lze zajistit pouhým odnětím věci, tedy úkonem, pro který stačí příkaz státního zástupce. Díky zevrubné analýze lokalizačních dat lze velmi efektivně rekonstruovat do nejmenších detailů pohyb osoby na přesnost několika málo metrů, případně i zjistit okolnosti skutku pomocí amatérských zařízení, která monitorují zdravotní stav.[183]

Taková data mají do jisté míry povahu podobnou datům, které schraňuje mobilní operátor při používání GSM telefonu v síti. Tyto údaje jsou často závislé na geograficko-morfologických podmínkách krajiny či města. Data z věží tak trpí vysokým rozptylem a relativní nepřesností.[184] Je otázkou, zda v případě GPS dat, která zajistí orgán činný v trestním řízení, případně znalec forenzní analýzou obsahu mobilního telefonu, lze postupovat v souladu s § 79 tr. ř. Zákonodárce totiž zcela výslovně data podobného rázu zařadil pod přísný režim § 88a tr. ř., kdy sběr lokalizačních údajů uživatelských stanic musí být povolen soudem a takové povolení je možné pouze pro trestné činy

[183] Využití dat z tzv. smart zařízení může být problematické, ale i velmi efektivní při vyšetřování, viz např. RATANAPHANYARAT, Carissa. Smart Devices, Criminal Investigations and Your Privacy: What You Need to Know. Next Advisor: In-depth, Independent Research [online]. Burlingame, CA: Next Advisor, 2018, 3. května 2018 [cit. 2019].

[184] Srov. např. TRAN, Minh. *Accurate Location Detection: White Paper: System and method that allows for cost effective location detection accuracy that exceeds current FCC standards.* Federal Communication Commission [online]. Springfield, VA: Vláda Spojených států amerických, 2014, 2014 [cit. 2019], s. 5.

definované v prvním odstavci tohoto ustanovení. Jak bylo vysvětleno v kapitole 4.4, analogie v trestním právu procesním je přípustná pouze za předpokladu, že není zasahováno do ústavních práv osob, kterých se takový zásah týká. Tento „*test ústavnosti*“ však postup naznačený v metodice Nejvyššího státního zastupitelství postrádá.

Dále je otázkou, do jaké míry lze při zajišťování důkazů postupovat dle § 8 odst. 5 tr. ř. Jak bylo nastíněno v kapitole 5.2.1, souhlas soudu lze vyžadovat v souvislosti se zákonem uznanou či zákonem ukotvenou povinností tajnosti či důvěrnosti obsahu. E-mailová komunikace bezesporu spadá[185] pod důvěrnou komunikaci. Dle mého názoru je takový postup *contra legem*, neboť existuje mechanismus, jakým zajistit obsah např. e-mailové zprávy (např. § 158d odst. 3, § 88 tr. ř. apod.), ty ale zpravidla vyžadují přísnější mechanismus povolení než postup podle § 8 odst. 5 tr. ř. Nasazení operativně pátracích prostředků podléhá podmínce konkretizace trestní činnosti, zatímco ustanovení § 8 odst. 5 se toliko omezuje na plnění úkolů policie. Ustanovení § 88 zase předpokládá jejich nasazení pouze pro taxativně vyjmenované případy (srov. 5.2.6). Možnost prolomení mlčenlivosti ve spojení s e-mailovou komunikací tak je dle § 8 odst. 5 velmi omezena. Proto by mělo být povolování prolomení důvěrnosti zpráv na počítačových sítích posuzováno přísněji než prismatem § 8 odst. 5. Toto ustanovení je totiž *lex generalis* vůči ostatním ustanovením upravujícím zajišťování důkazních prostředků.

6.2.3 Další vývoj

Při stávajícím technologickém pokroku lze očekávat, že se v blízké budoucnosti objeví technologie, které posunou komunikační mechanismy ještě dále. Ať už se bude jednat o nové typy bezpečnostních aplikací a šifrování, které nebude možné v rozumném časovém intervalu rozšifrovat, decentralizované komunikační platformy nebo i další řešení, která mají vztah k informacím v elektronické podobě. Všechna tato data budou dříve či později předmětem zájmu orgánů činných v trestním řízení. V nejbližší budoucnosti je však záhodno se zabývat

[185] Srov. vyhláška Ministerstva průmyslu a obchodu č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů, a zákon o elektronických komunikacích. Názvosloví volně navazuje na směrnici Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí.

bezprostřednějšími výzvami, a to internacionalizací působení pachatelů trestné činnosti a souladem dokazování elektronickými důkazními prostředky s principy trestního práva procesního, ústavními základy spravedlivého procesu a mezinárodními závazky České republiky.

Jak bylo nastíněno výše, internet je médium, které je svobodné a až na výjimky[186] globalizované. Výměna informací probíhá vmžiku a obsah se neustále mění. Jurisdikce a vymahatelnost práva jednotlivými státy, zejména pak státy menšími či středními, je značně omezená i s ohledem na skutečnost, že v současné době jedním z nejprogresivnějších regionů v inovacích informačních technologií jsou bezesporu Spojené státy americké. Možnosti zajištění důkazů a případného pachatele, který může pobývat kdekoliv, jsou tudíž problematické. I proto je ve veřejném zájmu, aby Česká republika co nejúžeji spolupracovala s justičními a policejními orgány dalších zemí, a aby s ohledem na volatilitu elektronické informace v digitální podobě byla taková spolupráce rychlá a efektivní.

Na úrovni Evropské unie dochází k posílení spolupráce v trestních věcech. Po přijetí Lisabonské smlouvy mohou členské státy v souladu s čl. 82 odst. 1 Smlouvy o fungování Evropské unie harmonizovat určité aspekty trestního práva procesního. V souvislosti s rozšiřováním evropského rozměru trestního práva procesního došlo mj. k přijetí úpravy o zřízení Úřadu evropského veřejného žalobce,[187] funguje tzv. evropský zajišťovací příkaz týkající se mj. zajištění důkazů dostupných v jiných jurisdikcích Evropské unie potřebných pro trestní řízení,[188] navazující tzv. evropský důkazní příkaz[189] a mnoho dalších procesněprávních instrumentů. V oblasti zajišťování elektronických důkazů orgány Evropské unie aktuálně projednávají návrh nařízení Evropského parlamentu a Rady o evropských předávacích a uchovávacích příkazech pro elektronické důkazy

[186] Srov. HORWITZ, Josh. After China's crackdown, now Russia is banning VPNs too. Quartz [online]. New York: Quartz, 2017, 31. července 2017 [cit. 2019].

[187] Nařízení Rady (EU) 2017/1939 o zřízení Úřadu evropského veřejného žalobce vstoupilo v platnost dne 20. listopadu 2017.

[188] Rámcové rozhodnutí Rady 2003/577/SVV ze dne 22. července 2003, o výkonu příkazů k zajištění majetku nebo důkazních prostředků v Evropské unii. In: JELÍNEK, Jiří a kol. *Trestní právo procesní. 2. aktualizované vydaní*. Praha: Leges: 2011, s. 97.

[189] Rámcové rozhodnutí Rady 2003/577/SVV ze dne 18. prosince 2008, o evropském důkazním příkazu k zajištění předmětů, listin a údajů pro účely řízení v trestních věcech. In: JELÍNEK, Jiří a kol. *Trestní právo procesní. 2. aktualizované vydaní*. Praha: Leges: 2011, s. 98.

v trestních věcech.[190] Implementace tohoto nařízení by mohla mít významný vliv na přeshraniční zajišťování elektronických důkazů. Jak uvádí důvodová zpráva k návrhu nařízení, „*příkaz lze vydat za účelem uchování nebo předání údajů, které jsou uloženy u poskytovatele služeb v jiné jurisdikci a které jsou potřebné jako důkazy* […] *příkazy mohou být doručeny poskytovatelům služeb elektronické komunikace, sociálním sítím, online tržištím, jiným poskytovatelům hostingových služeb a poskytovatelům internetové infrastruktury, jako jsou registry IP adres a názvů domén, nebo jejich právním zástupcům, existují-li.*“ [191] Jako jednu z výhod nařízení lze spatřovat rychlost zajištění důkazů, které se nacházejí v jiných evropských jurisdikcích. Dle čl. 9 je stát, který je žádán o zajištění důkazu, povinen konat (rozuměj učinit kroky k zajištění důkazu) ve lhůtě 10 dní, respektive ve lhůtě 6 hodin, jedná-li se o naléhavý případ.[192] Poskytovatelům služeb a subjektům, které nemají v Evropské unii pobočku či provozovnu, navíc vzniká povinnost ustanovit právního zástupce pro vyřizování příkazů. Z pohledu zjišťování skutkového stavu orgány činnými v trestním řízení lze předpokládat, že se jedná o efektivní návrh. Své výhrady však shrnula například Rada evropských advokátních komor, která návrh nařízení ve svém stanovisku nepodpořila zejména s ohledem na porušení zásady proporcionality, rovnosti zbraní a nedostatečné možnosti přezkumu.[193]

Další možnou cestou pro zajištění elektronických důkazů je dobrovolnost jejich vydávání přímo poskytovateli služeb. Technologičtí giganti jako Google či Facebook mají propracovanou metodiku spolupráce s orgány činnými v trestním řízení. Například Google nad rámec mezinárodní justiční spolupráce poskytuje na základě příslušných zajišťovacích institutů za určitých podmínek data dobrovolně, tedy přímo: „*Na bázi dobrovolnosti, můžeme poskytnout data orgánům mimo Spojené státy* […] *a to za předpokladu, že taková žádost je v souladu s mezinárodním právem, právem Spojených států, podmínkami společnosti Google a zákonnými podmínkami státu, který*

[190] Návrh nařízení Evropského parlamentu a Rady o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech 2018/0108/COD, stav legislativního procesu je dostupný na URL: https://eur-lex.europa.eu/procedure/CS/2018_108.

[191] Důvodová zpráva k návrhu nařízení Evropského parlamentu a Rady o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech 2018/0108/COD.

[192] Naléhavé případy zahrnují bezprostřední ohrožení života nebo tělesné integrity osoby a bezprostřední ohrožení kritické infrastruktury.

[193] RADA EVROPSKÝCH ADVOKÁTNÍCH KOMOR. *Stanovisko CCBE k návrhu nařízení o evropských předávacích a uchovávacích*. Brusel: 13. schůze jednání představenstva, 7-8. listopadu 2018.

žádá [o vydání dat]."[194] Podobné politiky má i sociální síť Facebook, Linkedin a další zejména americké společnosti.

Neméně důležitým faktorem pro další osud dokazování elektronickými důkazními prostředky je v současné době Ústavním soudem projednávaná stížnost[195] skupiny poslanců navrhující zrušení části ustanovení zákona o elektronických komunikacích, zákona o Policii ČR, trestního řádu a vyhlášky o uchovávání, předávání a likvidaci provozních a lokalizačních údajů. Návrh na zrušení předpisů, které regulují zajišťování lokalizačních dat od provozovatelů, reaguje na rozpor platné právní úpravy s ústavně garantovaným právem na soukromí, listovní tajemství a tajemství jinak dopravovaných zpráv, stejně tak problematickou kompatibilitu s čl. 8 EÚLP. Návrh na zrušení předmětných ustanovení pokládá současnou úpravu sběru provozních dat za neproporcionální a příliš invazivní. Pokud by Ústavní soud rozhodl o zrušení, byť jen části právní úpravy, mohlo by to mít značný vliv na způsob, jakým se data zajišťují. Ostatně, nebylo by to poprvé, kdy Ústavní soud zasáhl do úpravy odposlechů.[196] Navíc, jak bylo diskutováno v kapitole 5.2, odpověď na otázku, jaký institut při zajištění elektronických důkazů užít, není vždy jasná. Bez ohledu na to, jak Ústavní soud rozhodne, bylo by příhodné, aby se zákonodárce a odborná veřejnost zabývali elektronickými důkazy v souvislosti s prací na novém trestním řádu či v rámci novelizace stávajícího trestního řádu.

[194] Legal process for user data requests FAQs. Google [online]. Mountain View, CA: Google [cit. 2019]. [Přeloženo autorem]. Dostupné z: https://support.google.com/transparencyreport/answer/7381738/

[195] VOBOŘIL, Jan. *Návrh na zrušení § 97 odst. 3 a 4 zákona č. 127/2005 Sb., § 68 odst. 2 a § 71 písm. a) zákona č. 273/2008 Sb., § 88a zákona č. 141/1961 Sb., trestního řádu a návrh na zrušení vyhlášky č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů*. Ústavního soudu je návrh veden pod sp. zn. Pl. ÚS 45/17. Dostupnost z: https://www.usoud.cz/fileadmin/user_upload/Tiskova_mluvci/Navrhy/Pl._US_45_17_navrh.pdf

[196] Srov. nález Ústavního soudu sp. zn. Pl. ÚS 24/10 ze dne 22. března 2011.

7 Závěr

Elektronické informace jsou v dnešním světě elektronické komunikace, kontraktace a digitalizace stále důležitější. To platí i pro trestní právo hmotné a procesní. Zatímco hmotné právo dokázalo reagovat na existenci elektronických informací flexibilněji, ať už definicí nových skutkových podstat trestných činů nebo aplikací starších institutů na novou formu páchání trestné činnosti, procesní právo trestní je v přizpůsobení se novým formám kriminality a novým možnostem v dokazování o poznání konzervativnější.

Na mezinárodní úrovni byla přijata Budapešťská úmluva, dokument Rady Evropy, která kromě zakotvení nových trestných činů upravila i rámec pro jejich vymáhání. Česká republika ratifikovala tento dokument až o mnoho let později, přičemž aplikovatelnost některých jejích mechanismů nechala na praxi. Z hlediska mezinárodních závazků, zejména pak Evropské úmluvy o lidských právech, se na elektronické důkazy musí hledět jako na další druh důkazů, se kterými je třeba nakládat v souladu s demokratickými principy. Elektronické informace a užití nových technologií totiž svou abstraktní podstatou svádí k tomu, aby jejich potenciál byl využíván v celé jejich šíři. To však může narazit na základní práva a svobody, zejména na právo na soukromý život a obecně pak na právo na spravedlivý proces. Doktrína ochrany lidských práv v souvislosti se zajišťováním a prováděním elektronických důkazů se ostatně prolíná i do rozhodovací praxe Ústavního soudu a vrcholných instancí soudní soustavy.

Jednotlivé instituty zajištění a dokazování jsou ale vždy nejprve aplikovány na nejnižších úrovních, od policejních orgánů, obhájců, obviněných, poškozených, státních zástupců a soudů prvního stupně. Právě tyto subjekty trestního řízení musí při dokazování vždy zvažovat, který abstraktní institut je použitelný na jimi řešený konkrétní případ. Vzhledem k omezené judikatuře Nejvyššího a Ústavního soudu jim často nezbude než pečlivě zkoumat, na jakých principech (právních a technologických) jsou různé důkazní prameny a důkazy samotné založeny. Nejvyšší státní zastupitelství sice vydalo několik metodických pokynů pro zajišťování a provádění důkazů a s nimi spojených úkonů, avšak tyto pokyny jsou závazné jen pro státní zástupce a samy o sobě nedokázaly pojmout všechny nuance vyplývající z povahy některých technických řešení.

I proto se stává, že některé, zejména zajišťovací instituty, se ne vždy užívají správně. Rozdíl mezi domovní prohlídkou a nasazením operativně pátracích prostředků k získání dat na serveru obviněného je malý, ale může znamenat rozdíl mezi přípustností důkazu v dalším řízení a jeho další procesní neúčinností.

Samostatnou kapitolou je problematika internacionalizace a globalizace informační společnosti, na kterou zejména orgány činné v trestním řízení naráží často. Důkazy mívají v držení zahraniční osoby a dosah české jurisdikce je omezený, nemožný či časově náročný. I proto je důležité, že Evropská unie udělala první kroky směřující k vytvoření mechanismů, díky kterým orgány činné v trestním řízení i v menších státech budou mít větší šanci zajistit důkazy ze zahraničí. Tím pádem budou způsobilejší k tomu kvalifikovaně rozhodnout a zjistit materiální pravdu v trestním řízení.

Ve výhledu na budoucí vývoj lze sledovat dva trendy. Jednak snahu inkorporovat do pozitivního práva podrobnější úpravu získávání důkazů a jednak snahu krystalizovat postupy orgánů činných v trestním řízení tak, aby byla zachována zásada zákonnosti a spravedlivého procesu. Jen tak bude zachován nejdůležitější cíl trestněprávní politiky, tedy rozhodnout spravedlivě o vině a trestu.

Zkratky

Budapešťská úmluva	Mezinárodní smlouva č 104/2011 Sb. m. s., Úmluva o počítačové kriminalitě
ESLP	Evropský soud pro lidská práva
Listina	Usnesení předsednictva České národní rady č. 2/1992 Sb., Listina základních práv a svobod
tr. ř.	Zákon č. 141/1961 Sb., o trestním řízení soudním
tr. zák.	Zákon č. 40/2009 Sb., trestní zákoník
Ústava	Ústavní zákon č. 1/1993 Sb., Ústava České republiky
z. pol. ČR	Zákon č. 273/2008 Sb., o Policii České republiky
obč. z.	Zákon č. 89/2012 Sb., občanský zákoník
ISP	Internet Service Provider, poskytovatel internetového připojení
IP adresa	Adresa internetového protokolu

Použitá literatura

BUDKA, Ivan. *Využití právních nástrojů pro potírání organizovaného zločinu.* Praha: Institut pro kriminologii a sociální prevenci, 2017. ISBN: 978-80-7338-169-1.

ČESKÁ REPUBLIKA. *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.* Praha: Ministerstvo spravedlnosti České republiky, 2018.

CHMELÍK, Jan. *Kamerové systémy a důkazní hodnota informací, které jsou jejich prostřednictvím opatřeny.* Trestní právo. Praha: Walter Kluwer ČR, 2018, 22(1), s. 20-28. ISSN: 1211-2860.

CLOUGH, Jonathan. *A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation.* Monash University Law Review. Clayton, 2014, 40(3), 698-736. ISSN: 0311-3140.

DRAŠÍK, Antonín, FENYK, Jaroslav a kol. *Trestní řád. Komentář I. a II. díl.* Praha: Wolters Kluwer ČR, 2017. ISBN: 978-80-7552-600-7.

FRYŠTÁK, Marek. *Dny práva – 2010 – Days of Law. 1. vydání: Odborné vyjádření versus znalecký posudek.* Brno: Masarykova univerzita, 2010. ISBN: 978-80-210-7687-7

FRYŠTÁK, Marek. *Dokazování v přípravném řízení. 2. vydání.* Brno: Masarykova univerzita, Právnická fakulta, 2015. ISBN: 978-80-210-7687-7.

GERLOCH, Aleš. *Teorie práva. 7. vydání.* Plzeň: Aleš Čeněk, 2017. 335 s. ISBN: 978-80-7380-652-1.

GŘIVNA, Tomáš, POLČÁK, Radim a kol. *Kyberkriminalita a právo.* Praha: Auditorium, 2008. 220 s. ISBN 978-80-903786-7-4.

HANUŠ, Libor. *Ústavněprávní vady důkazního procesu z pohledu judikatury Ústavního soudu.* Brno: Právní rozhledy. 2006, 18, s. 647-653. ISSN 1210-6410.

HERCZEG, Jiří. *Plody z otráveného stromu a ústavněprávní limity získávání informací v trestním řízení.* Trestněprávní revue, 2009, č. 3, s. 65. ISSN 1213-5313.

JELÍNEK, Jiří a kol. *Dokazování v trestním řízení v kontextu práva na spravedlivý proces.* Praha: Leges, 2018. 536 s. ISBN: 978-80-7502-287-5.

JELÍNEK, Jiří a kol. *Trestní právo hmotné. 5. aktualizované vydání. Obecná část. Zvláštní část.* Praha: Leges, 2016. 976 s. ISBN: 978-80-7502-120-5.

JELÍNEK, Jiří. *Trestní právo procesní. 2. vyd. podle novelizované právní úpravy účinné od 1.9. 2011.* Praha: Leges, 2011. Student. ISBN 978-80-87212-92-9.

JELÍNEK, Jiří. *K chybějící právní úpravě tzv. prostorového odposlechu v trestním řádu.* Bulletin advokacie, 2018, č. 7-8, s. 13. ISNN: 1210-6348.

JELÍNEK, Jiří, GŘIVNA, Tomáš, TLAPÁK NAVRÁTILOVÁ, Jana, HERCZEG, Jiří, DANKOVÁ, Katarína a PELC Vladimír. *Trestní právo Evropské unie.* Praha: Leges, 2014. Teoretik. ISBN 978-80-7502-041-3.

KOUHOUT, Jiří a BEHR, Tomáš. *Elektronická pošta a její záznam pro trestní řízení.* Trestněprávní revue. 2011, 10(4), 101-106. ISSN 1213-5313.

KOLOUCH, Jan. *Cybercrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf

KOSŘAŘ, Jiří, KRATOCHVÍL, Jan a BOBEK, Michal. *Evropská úmluva o lidských právech: komentář.* Praha: C.H. Beck, 2012. Velké komentáře. 1660 s. ISBN 978-80-7400-365-3.

KRATOCHVÍL Vladimír. *Dopad rozhodnutí evropského soudu pro lidská práva na trestní právo ČR.* Praha: Masarykova univerzita, Právnická fakulta, 2011, s. 44 [materiál k přednáškám].

KREJČÍ, Zdeněk. *Prohlídka dle trestního řádu ve světle rozhodování Ústavního soudu.* Kriminalistika. 2009, 42(4), s. 278-294. ISSN 1210-9150.

KUCHTA, Josef. *Aktuální problémy počítačové kriminality včetně její prevence.* Časopis pro právní vědu a praxi. 2016, s. 5-19. ISSN 1210-9126.

MASON, Stephen a SENG, Daniel. *Electronic Evidence, Fourth edition.* London: University of London, Institute of Advanced Legal Studies for the SAS, 2017. ISBN: 978-1911507055.

MATEJKA, Ján, KRAUSOVÁ, Alžběta a GÜTTLER Vojen. *Biometrické údaje a jejich právní režim.* Revue pro právo a technologie. 2018, č. 17. s. 91. ISSN 1804-5383.

MATĚJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí. 1. vydání.* Praha: CZ.NIC, 2013. ISBN: 978-80-904248-7-6. Dostupné také z: https://knihy.nic.cz/files/nic/edice/jan_matejka_ijop.pdf.

MORRILL R. Daniel. *An Investigation of the Digital Millennium Copyright Act (DMCA) and the Applicability to the Darknet: An Ex Post Facto Quantitative Non-Experimental Study.* San Diego: Northcentral University, 2016.

MULÁK, Jiří. *Základní zásady trestního řízení a právo na spravedlivý proces.* Praha: 2018, disertační práce: Univerzita Karlova, Právnická fakulta.

NEJEDLÝ, Josef. *Zákonnost důkazů v trestním řízení ve světle Evropské úmluvy o ochraně lidských práv a základních svobod.* Praha: 2012, disertační práce: Univerzita Karlova, Právnická fakulta.

PAVLÍČEK, Václav, GRONSKÝ, Ján, HŘEBEJK, Jiří a kol. *Ústavní právo a státověda. II. díl, Ústavní právo České republiky. 2. aktualizované vydání.* Praha: Leges, 2015. Student. ISBN 978-80-7502-084-0.

PERKINS, Aaron. *Encryption Use: Law and Anarchy on the Digital Frontier.* Houston: Houston Law Review, 2005, 41(5). s. 1627. Dostupné také z: https://heinonline.org/HOL/P?h=hein.journals/hulr41&i=1637.

POKORNÝ, Aleš. *Aktuální problémy dokazování se zaměřením na znaleckou činnost.* Praha: 2010, rigorózní práce: Univerzita Karlova, Právnická fakulta.

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

POLČÁK, Radim, František PÚRY, Jakub HARAŠTA, Matěj MYŠKA a Václav STUPKA. *Elektronické důkazy v trestním řízení.* Brno: Masarykova univerzita, 2015. Spisy Právnické fakulty Masarykovy univerzity. ISBN 978-80-210-8073-7. Dostupné také z: http://science.law.muni.cz/knihy/monografie/Polcak_Elektronicke_dukazy.pdf.

PROVAZNÍK Jan. *Trestněprocesní ingerence do podmínek trestní odpovědnosti.* Brno: Právní rozhledy 2015, 8, s. 283. ISSN 1210-6410.

RADA EVROPSKÝCH ADVOKÁTNÍCH KOMOR. *Stanovisko CCBE k návrhu nařízení o evropských předávacích a uchovávacích příkazech.* 13. schůze jednání představenstva. Brusel: 2018. URL: Dostupné také z: https://www.cak.cz/assets/priloha_7_2018_11.pdf.

ŠABATKOVÁ, Tereza. *Důsledky porušení předpisů o dokazování pro účinnost důkazů.* Praha: 2018, diplomová práce: Univerzita Karlova, Právnická fakulta. Dostupné také z: https://is.cuni.cz/webapps/zzp/download/120305714.

ŠÁMAL, Pavel, GŘIVNA, Tomáš, HERCZEG, Jiří, KRATOCHVÍL, Vladimír, PÚRY, František, RIZMAN, Stanislav, ŠÁMALOVÁ, Milada, VÁLKOVÁ, Helena, VANDUCHOVÁ, Marie. *Trestní zákoník (EVK). 2.vydání.* Praha: Nakladatelství C. H. Beck, 2012, s. 2300. ISBN 978-80-7400-428-5.

ŠÁMAL, Pavel a GŘIVNA, Tomáš. *Trestní řád: komentář. 7., dopl. a přeprac. vyd.* Praha: C.H. Beck, 2013. Velké komentáře. ISBN 978-80-7400-465-0.

ŠÁMAL, Pavel, MUSIL, Jan, KUCHTA, Josef, FRYŠTÁK, Marek a KALVODOVÁ, Věra. *Trestní právo procesní. 4. přeprac. vyd.* V Praze: C.H. Beck, 2013. Academia iuris. ISBN 978-80-7400-496-4.

SIMON, Dan. *A Third View of the Black Box: Cognitive Coherence in Legal Decision Making.* Chicago: University of Chicago Law Review, 2004, 71(2), s. 511. ISSN: 0041-9494. Dostupné také z: https://chicagounbound.uchicago.edu/uclrev/vol71/iss2/3.

SMEJKAL, Vladimír. *Kybernetická kriminalita. 2. rozšířené a aktualizované vydání.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-720-7.

TONRY, Michael. *The Oxford Handbook of Crime and Criminal Justice.* Oxford: Oxford University Press, 2012. ISBN: 978-01-9933-828-3.

VANTUCH, Pavel. *Kdy může obhajoba důkaz vyhledat, kdy předložit a kdy jen navrhnout jeho provedení?* Praha: Bulletin advokacie, 2013, s. 13. ISNN: 1210-6348. Dostupné také z: http://www.bulletin-advokacie.cz/kdy-muze-obhajoba-dukaz-vyhledat-kdy-predlozit-a-kdy-jen-navrhnout-jeho-provedeni?browser=mobi.

WEBER, Max. *Metodologie, sociologie a politika. 1. vyd.* Praha: Oikoymenh, 1998, 354 s. ISBN 80-860-0548-8.

WIENER, Norbert. *Cybernetics Or On the Control and Communication in the Animal and the Machine.* Cambridge: MIT Press, 1961. 196 s. ISBN: 978-11-6319-179-8.

WINTR, Jan. *Principy českého ústavního práva. 4. vydání.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. 286 s. ISBN 978-80-7380-730-6.

ZAORALOVÁ, Petra. *Použitelnost soukromých zvukových a obrazových záznamů jako důkazu v trestním řízení.* Praha: Bulletin advokacie, 2017, 11, s. 28. ISNN: 1210-6348.

Použité právní předpisy

Usnesení předsednictva České národní rady č. 2/1992 Sb., Listina základních práv a svobod

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

Mezinárodní smlouva č 104/2011 Sb. m. s., Úmluva o počítačové kriminalitě

Sdělení federálního ministerstva zahraničních věcí č. 209/1992 Sb., o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících

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

Zákon č. 36/1967 Sb., o znalcích a tlumočnících

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

Zákon č. 89/2012 Sb., občanský zákoník

Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád)

Zákon č. 40/2009 Sb., trestní zákoník

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

Zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech

Zákon č. 36/1967 Sb., o znalcích a tlumočnících

Zákon č. 283/1993 Sb., o státním zastupitelství

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

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

Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí

Nařízením Evropského parlamentu a Rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů

Směrnicí Evropského parlamentu a Rady (EU) 2016/680, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů a o volném pohybu těchto údajů.

Návrh nařízení Evropského parlamentu a Rady o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech 2018/0108/COD

Rámcové rozhodnutí Rady 2003/577/SVV ze dne 18. prosince 2008, o evropském důkazním příkazu k zajištění předmětů, listin a údajů pro účely řízení v trestních věcech

Vyhláška č. 462/2013 Sb., o stanovení výše a způsobu úhrady efektivně vynaložených nákladů na odposlech a záznam zpráv, na uchovávání a poskytování provozních a lokalizačních údajů a na poskytování informací z databáze účastníků veřejně dostupné telefonní služby

Vyhláška č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů

Stanovisko k obsahu údajů uložených na mobilním telefonu a SIM kartě vydané pod pořadovým číslem 4/2005 ve Sbírce výkladových stanovisek Nejvyššího státního zastupitelství, ze dne 6. června 2005

Stanovisko k problematice zajišťování obsahu mobilních telefonů a jiných právních datových nosičů, včetně obsahu e-mailových schránek vydané pod pořadovým číslem 1/2015 ve Sbírce výkladových stanovisek Nejvyššího státního zastupitelství, ze dne 26. ledna 2015

Stanovisko k problematice pořizování a nakládání s odposlechem a záznamem telekomunikačního provozu vydané pod pořadovým číslem 1/2018 ve Sbírce výkladových stanovisek Nejvyššího státního zastupitelství, ze dne 11. listopadu 2018

Seznam judikatury

Nález Ústavního soudu č. 214/1994 Sb. ze dne 12. října 1994.

Nález Ústavního soudu č. II. ÚS 502/2000, ze dne 22. listopadu 2000.

Nález Ústavního soudu č. 403/2002 Sb. dne 25. června 2002.

Nález Ústavního soudu I. ÚS 733/01 ze dne 24. února 2004.

Usnesení Ústavního soudu sp. zn. IV. ÚS 554/03 ze dne 29. dubna 2004.

Nález Ústavního soudu sp. zn. I. ÚS 3038/07 ze dne 29. února 2008.

Nález Ústavního soudu sp. zn. Pl. ÚS 3/09 ze dne 8. června 2010.

Nález Ústavního soudu sp. zn. II. ÚS 860/10 ze dne 2. září 2010.

Nález Ústavního soudu sp. zn. Pl. ÚS 24/10 ze dne 22. března 2011.

Nález Ústavního soudu sp. zn. I. ÚS 2610/11 ze dne 13. října 2011.

Nález Ústavního soudu sp. zn. Pl. ÚS 24/11 ze dne 20. 12. 2011.

Nález Ústavního soudu č. 214/1994 Sb. ze dne 12. prosince 2012.

Usnesení Ústavního soudu sp. zn. III. ÚS 3812/12 ze dne 3. října 2013.

Nález Ústavního soudu sp. zn. III. ÚS 3844/13 ze dne 30. října 2014.

Usnesení Ústavního soudu sp. zn. I. ÚS 2878/14-2, ze dne 26. října 2015.

Nález Ústavního soudu sp. zn. II. ÚS 4266/16 ze dne 27. března 2017.

Nález Ústavního soudu sp. zn. II. ÚS 2587/18 ze dne 25. února 2019

Stanovisko pléna Ústavního soudu sp. zn. Pl. ÚS-st. 31/10 ze dne 14. prosince 2010.

Návrh na zrušení předpisů u Ústavního soudu veden pod sp. zn. Pl. ÚS 45/17.

Rozsudek Nejvyššího soudu vydané pod č. 33/1968 II. Sb. rozh. tr.

Usnesení Nejvyššího soudu sp. zn. 6 To 12/92 ze dne 25.března 1992.

Usnesení Nejvyššího soudu ČR sp. zn. 7 Tz 9/2000 ze dne 15. prosince 2000.

Usnesení Nejvyššího soudu ČR 7 Tdo 783/2010 ze dne 4. srpna 2010.

Usnesení Nejvyššího soudu sp. zn. 5 Tdo 113/2013-79 ze dne 26. června 2013.

Stanovisko Nejvyššího soudu sp. zn. Tpjn 306/2014 ze dne 25. června 2015.

Rozsudek Nejvyššího správního soudu ČR sp. zn. 1 As 90/2008 vydaný dne 17. července 2008

Rozhodnutí Evropského soudu pro lidská práva, Klass a ostatní proti Německu, stížnosti č. 5029/71 ze dne 6. září 1978.

Rozhodnutí Evropského soudu pro lidská práva, Miailhe proti Francii (č. 2), stížnost č. 18978/91 ze dne 26 září 1996.

Rozhodnutí Evropského soudu pro lidská práva, Trabajo Rueda proti Španělsku, stížnost č. 32600/12 ze dne 30. května 2017.

Rozhodnutí Evropského soudu pro lidská práva, Ivashchenko proti Rusku, stížnost č. 61064/10 ze dne 13. února 2018.

Rozhodnutí Evropského soudu pro lidská práva, Perry proti Spojenému království Velké Británie a Severního Irska, stížnost č. 63737/00, ze dne 17. června 2003.

Užité online zdroje

ARTHUR, Charles. China Cracks Down on VPN Use. Guardian News [online]. London: The Guardian, 2011, 12. května 2011 [cit. 2019]. Dostupné z: https://www.theguardian.com/technology/2011/may/13/china-cracks-down-on-vpn-use

GREENWALD, Glenn, Ewen MACASKILL, Laura POITRAS, Spencer ACKERMAN a Sominic RUSHE. Microsoft handed the NSA access to encrypted messages. The Guardian [online]. Londýn: The Guardian, 2013, 12. června 2013 [cit. 2019]. Dostupné z: https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

HORWITZ, Josh. After China's crackdown, now Russia is banning VPNs too. Quartz [online]. New York: Quartz, 2017, 31. července 2017 [cit. 2019]. Dostupné z: https://qz.com/1041927/after-chinas-crackdown-now-russia-is-banning-vpns-too/

Instant messaging: Clients. Wikipedia [online]. Wikipedia, 2019 [cit. 2019]. Dostupné z: https://en.wikipedia.org/wiki/ Instant_messaging#Clients

Legal process for user data requests FAQs. Google [online]. Mountain View, CA: Google [cit. 2019]. Dostupné z: https://support.google.com/transparencyreport/answer/7381738/

NEWMAN, Lily Hay. Encrypted Messaging Isn't Magic. Wired [online]. New York: Wired Magazine, 2018, 14. června 2018 [cit. 2019]. Dostupné z: https://www.wired.com/story/encrypted-messaging-isnt-magic/

POKORNÝ, Marek: *Rázná soudkyně Miklová otřásla zvyklostmi české justice. Její případy citují i v zahraničí.* Praha: Hospodářské noviny, Právní rádce, 21. prosince 2018 [cit. 2019]. Dostupné z: https://pravniradce.ihned.cz/c1-66400810-pripad-razne-soudkyne-miklove-jez-otrasla-zvyklostmi-ceske-justice-jeji-pripady-cituji-i-v-zahranici.

RATANAPHANYARAT, Carissa. Smart Devices, Criminal Investigations and Your Privacy: What You Need to Know. Next Advisor: In-depth, Independent Research [online]. Burlingame, CA: Next Advisor, 2018, 3. května 2018 [cit. 2019]. Dostupné z: https://www.nextadvisor.com/blog/smart-devices-criminal-investigations-and-your-privacy/

ROUSE, Margaret. *End-to-end encryption (E2EE).* SearchSecurity: TechTarget [online]. New York: SearchSecurity, 2015, červenec 2015 [cit. 2019]. Dostupné z: https://searchsecurity.techtarget.com/definition/end-to-end-encryption-E2EE

SLEGG, JENNIFER. *Google: Issues When Serving Different HTML & Content to Different Browsers.* TheSEMPost [online]. 2015, 11. září 2015 [cit. 2019]. Dostupné z: http://www.thesempost.com/google-issues-when-serving-different-html-content-to-different-browsers/

Spam: share of global email traffic 2014-2018: Global spam volume as percentage of total e-mail traffic from January 2014 to September 2018, by month. Statista: The Statistics Portal [online]. New York: Statista, 2019, 2019 [cit. 2019]. Dostupné z: https://www.statista.com/statistics/420391/spam-email-traffic-share/

TRAN, Minh. *Accurate Location Detection: White Paper: System and method that allows for cost effective location detection accuracy that exceeds current FCC standards.* Federal Communication Commission [online]. Springfield, VA: Vláda Spojených států amerických, 2014, 2014 [cit. 2019]. Dostupné z:

https://transition.fcc.gov/pshs/911/Apps%20Wrkshp%202015/911_Help_SMS_WhitePaper0515.pdf

VYSKOČIL, Ladislav: *Zajišťování digitálních stop.* [online] Policie ČR: SKPV KŘP JmK Brno, s. 15. Prezentace. Dostupné z: http://extranet.kr-vysocina.cz/download/odbor_informatiky/ecrime/E-learning/Zajistovani%20digitalnich%20stop.ppt

XMPP. Wikipedia [online]. Wikipedia, 2019 [cit. 2019]. Dostupné z: https://en.wikipedia.org/wiki/XMPP

Dokazování elektronickými důkazními prostředky

Abstrakt

Tato práce se zabývá procesními otázkami zajištění a provádění elektronických důkazů v trestním řízení. Elektronické důkazy jako produkt užívání moderních zařízení jsou v dnešní době běžnou součástí života. I proto je žádoucí, aby trestněprávní úprava a praxe orgánů činných v trestním řízení řádně nastavila mechanismy určené k zajišťování a provádění takových důkazů. V kontextu práva na spravedlivý proces, práva na soukromí, práva na ochranu listovního a obecné zásady minimalizace zásahů do života jednotlivce tato práce hledá odpověď na otázku, jakým způsobem lze v souladu s trestním řádem, ústavním pořádkem a mezinárodními závazky České republiky řádně zajistit a provést elektronické důkazy, tak aby bylo dosaženo účelu trestního řízení, a zároveň aby byly přiměřeně šetřena práva jednotlivců. Výklad se jednak soustřeďuje na zajišťování věcí užitím tradičních institutů, například domovní prohlídky, odebráním věci, operativně-pátracími prostředky, ale i relativně moderními prostředky, například odposlechem a záznamem telekomunikačního provozu. Obecné závěry z dokazování následně práce aplikuje v souvislosti se zajišťováním důkazů u běžně užívaných technologií: e-maily, dokumenty umístěnými na internetových stránkách či na sociálních sítích či zprávami zasílanými prostřednictvím mobilních aplikací. Zjištění jsou na závěr konfrontovány s aktuální rozhodovací praxí orgánů činných v trestním řízení, zejména pak se stanovisky Nejvyššího státního zástupce, které se týkající nosičů elektronických dat.

Klíčová slova: dokazování, elektronické důkazy, trestní právo procesní

Substantiation of Electronic Evidence

Abstract

This thesis addresses the procedural questions of securing and presenting electronic evidence in criminal proceedings. The use of modern devices and the subsequent creation of electronic evidence is very common, making it necessary for legislation as well as investigative, prosecuting and adjudicating bodies to set out an adequate framework for securing and producing such evidence. The thesis seeks to determine the limits of this framework with regard to the rights to a fair trial, privacy and secrecy of correspondence, as well as the principle of public authority interference minimization, keeping in mind that electronic evidence must be secured and produced in accordance with the Criminal Procedure Code, the Constitution and enforceable international treaties, respecting the rights of individuals but also allowing criminal proceedings to reach their ultimate goal. The thesis first concentrates on traditional instruments of securing evidence, e.g. search warrants, seizure of an item, operative-search means or various types of wiretapping. These general findings are then applied to commonly used information technologies, such as emails, documents stored on websites or social media platforms, as well as communication conducted via mobile applications. In its conclusion, the thesis confronts these findings with the current methods used by law enforcement, persecutors and criminal courts when dealing with electronic evidence during criminal proceedings, paying special attention to the Supreme Prosecutor's position on electronic data storage devices.

Key words: substantiation, electronic evidence, criminal procedure