

UNIVERZITA KARLOVA
Právnická fakulta

Veronika Hloušková

**Dokazování elektronickými důkazními
prostředky**

Diplomová práce

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

Katedra trestního práva

Datum vypracování práce (uzavření rukopisu): 7. února 2024

Prohlašuji, že jsem předkládanou diplomovou prací na téma „*Dokazování elektronickými důkazními prostředky*“ vypracovala samostatně, že všechny použité zdroje byly řádně uvedeny a že práce nebyla využita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 235 707 znaků včetně mezer.

Veronika Hloušková

V Praze dne 7. února 2024

Poděkování

Ráda bych tímto poděkovala vedoucímu své diplomové práce prof. JUDr. Bc. Tomáši Gřivnovi, Ph.D. za jeho vstřícnost, ochotu a cenné rady, které mi v průběhu vypracování diplomové práce poskytl. Rovněž děkuji své rodině a svým blízkým za jejich neutuchající podporu, trpělivost a především lásku, kterou mi poskytovali v průběhu celého studia, včetně studia v zahraničí.

Obsah

ÚVOD	6
1. DOKAZOVÁNÍ V TRESTNÍM ŘÍZENÍ	8
1.1. VÝZNAM A PODSTATA DOKAZOVÁNÍ	8
1.2. DŮKAZNÍ PRÁVO A ZÁSADY	10
1.3. POJEM PŘEDMĚT DŮKAZU, DŮKAZNÍ PROSTŘEDEK A DŮKAZ	11
1.4. DĚLENÍ DŮKAZŮ	13
1.5. PŘEDMĚT A ROZSAH DOKAZOVÁNÍ	16
1.6. PROCES DOKAZOVÁNÍ	18
2. ELEKTRONICKÉ DŮKAZNÍ PROSTŘEDKY	20
2.1. ROZDĚLENÍ NA KATEGORIE	22
2.2. PROCESNÍ POSTUPY ZAJIŠŤOVÁNÍ ELEKTRONICKÝCH DŮKAZNÍCH PROSTŘEDKŮ	23
2.2.1. <i>Zajištění zařízení a datových nosičů</i>	24
2.2.2. <i>Získání přístupu ke vzdáleným datům</i>	26
2.2.3. <i>Získání dat od ISP</i>	29
2.2.3.1. <i>Charakter poskytovatele</i>	29
2.2.3.2. <i>Charakter zajišťovaných dat</i>	30
2.3. JEDNOTLIVÉ PROCESNÍ INSTITUTY ZAJIŠTĚNÍ	32
2.3.1. <i>Odposlech a záznam telekomunikačního provozu</i>	32
2.3.2. <i>Zjišťování údajů o uskutečněném telekomunikačním provozu</i>	38
2.3.2.1. <i>Data retention</i>	42
2.3.3. <i>Sledování osob a věcí</i>	44
2.3.3.1. <i>Prostorové odposlechy</i>	45
2.3.3.2. <i>Obsah emailových schránek</i>	48
2.3.4. <i>Domovní prohlídka a prohlídka jiných prostor</i>	49
2.3.5. <i>Předložení nebo vydání věci a odnětí věci</i>	52
2.3.6. <i>Uchování dat uložených v počítačovém systému a znemožnění přístupu</i>	54
3. MEZINÁRODNĚPRÁVNÍ ÚPRAVA ELEKTRONICKÝCH DŮKAZNÍCH PROSTŘEDKŮ	57
3.1. RADA EVROPY A BUDAPEŠŤSKÁ ÚMLUVA	58
3.1.1. <i>Oblast působnosti Budapešťské úmluvy</i>	59
3.1.2. <i>Druhý dodatkový protokol</i>	60

3.2.	PRÁVO EVROPSKÉ UNIE.....	62
3.2.1.	<i>Evropský vyšetřovací příkaz</i>	62
3.2.2.	<i>Evropský vydávací příkaz a evropský uchovávací příkaz</i>	64
3.2.2.1.	<i>Kritické zhodnocení nově přijaté legislativy</i>	66
3.2.3.	<i>Společné vyšetřovací týmy</i>	68
3.3.	CLOUD ACT	69
3.3.1.	<i>Efektivnější přístup k elektronickým důkazům?</i>	70
3.3.1.1.	<i>Konflikt s GDPR</i>	71
3.3.2.	<i>Proces vyjednávání s Evropskou unií a odpovídající ochrana údajů</i>	72
4.	CHARAKTERISTIKA DOKAZOVÁNÍ Z JEDNOTLIVÝCH DŮKAZNÍCH PROSTŘEDKŮ	74
4.1.	ZDROJE DŮKAZŮ	74
4.1.1.	<i>Emailové schránky</i>	74
4.1.2.	<i>Sociální sítě</i>	77
4.1.3.	<i>Cloudová úložiště</i>	79
4.1.4.	<i>Mobilní telefony</i>	81
5.	APLIKAČNÍ PRAXE	85
5.1.	NÁRODNÍ CENTRÁLA PROTI ORGANIZOVANÉMU ZLOČINU	85
5.1.1.	<i>Rozhovor s policistou</i>	85
5.2.	ODDĚLENÍ ANALYTIKY A KYBERNETICKÉ KRIMINALITY	87
5.2.1.	<i>Rozhovor s policistou</i>	87
	ZÁVĚR.....	89
	SEZNAM ZKRATEK.....	93
	SEZNAM POUŽITÝCH ZDROJŮ	95
	ABSTRAKT	105
	ABSTRACT	106

Úvod

„Jakmile vidíme, jak věci fungují, jsme schopni činit moudřejší rozhodnutí. To platí dvojnásobně pro regulaci technologií.“¹, tak mluví v jedné ze svých kapitol Joshua A. T. Fairfield, profesor práva ve státě Virginia, autor knihy reagující na technologický pokrok v souvislosti s právem. Přestože se diplomová práce zabývá českou právní úpravou² *elektronických důkazních prostředků*, je příhodné na tomto místě poznamenat, že regulace moderních technologií je výzvou pro právní řády celého světa.

Informační a komunikační technologie již neodmyslitelně patří k našemu životu a s velkou rychlostí propojují svět. Ačkoliv nám v mnohém usnadňují či jinak zlepšují život, existence nových technologií má i svá proti. V kontextu trestního práva jejich nástup umožnil vznik nové trestné činnosti³ a současně jejich prostřednictvím usnadnil páchaní některých trestných činů již existujících⁴. Nové technologie používáme na každém kroku, a s tím souvisí i množství digitálních stop,⁵ které během dne každý z nás vytváříme. Otevírají se nové perspektivy a možnosti toho, co může být prostředkem dokazování, včetně množství a druhu informací, které mohou být takovým prostřednictvím zjištěny. Je tedy nepochybné, že ve společnosti neustávající digitalizace se trestní právo nachází před výzvou.

Přestože se zákonodárci i soudci prostřednictvím svých nástrojů snaží na technologický pokrok reagovat, regulace přichází zpravidla o několik měsíců, spíše let, později, nežli je to se samotným nástupem moderních technologií. To se s odkazem na naplnění požadavku předvídatelnosti práva může zdát žádoucí. Otázkou však zůstává, jaká časová prodleva mezi existencí⁶ nových technologií a jejich vhodnou právní regulací je přijatelná. Za příležitostné považuji zdůraznit, že současná právní úprava trestního práva procesního pochází z 60. let 20. století, kdy zákonodárce s novými technologiemi, které mohou být zdrojem elektronických důkazů, při normotvorbě nepočítal. Přestože původní znění trestního řádu prošlo od té doby

¹ FAIRFIELD, JAT., *Runaway technology; Can law keep up?* Cambridge University Press. 2021. ISBN 978-1-108-44457-6. s. 76

² Poznámka autorky: Práce se zabývá právní úpravou v České republice v kontextu unijního práva a mezinárodní úpravy, jíž je naše legislativa vázána, popř. v souvislosti s mezinárodní úpravou, jejíž přijetí je vyjednáváno.

³ „*Cyber-dependent crimes*“ jsou trestné činy závislé na kyberprostoru (např. DDoS útok, malware).

⁴ „*Cyber-enabled crimes*“ jsou trestné činy kyberneticky umožněné, páchané s využitím informačních a komunikačních technologií, tyto trestné činy však existovaly nezávisle na kyberprostoru (např. podvod).

⁵ Za *digitální stopu* můžeme označit jakoukoliv informaci s vypovídající hodnotou, která je uložena či přenášena v digitální podobě. Jedná se o definici uznávanou širokým okruhem odborníků, navrženou skupinou SWGDE Srov. PORADA, V. *Kriminalistika: technické, forenzní a kybernetické aspekty*. 2. aktualizované a rozšířené vydání. Plzeň: Aleš Čeněk, 2019. ISBN 978-80-7380-741-2. s. 185

⁶ Včetně pochopení, jak nové technologie fungují a jaké množství a druh informací mohou obsahovat, zejména s ohledem na ústavně zaručená práva.

mnoha novelizacemi, stále se nesetkáváme s komplexní právní úpravou, která by se získávání elektronických důkazů věnovala či by je alespoň zakotvovala. Právní nástroje, které doposud reagovaly na situace diametrálně odlišné, však nelze pomocí analogie nekonečně užívat i pro situace zcela nové. A to zejména s přihlédnutím k ochraně ústavně garantovaných práv osob, která jsou při zajišťování elektronických důkazních prostředků mnohdy prolamována.

Cílem této práce je tak *analyzovat současnou právní úpravu dokazování elektronickými důkazními prostředky, zhodnotit ji z hlediska její dostatečnosti, efektivity a současně vhodnosti pro zajištění ochrany základních lidských práv*. Pozornost bude věnována užití procesních institutů trestního řádu k zajištění a uchování elektronických důkazních prostředků z různých hledisek tak, aby bylo dosaženo komplexního pohledu na tuto problematiku a práce identifikovala klíčové otázky s ní spjaté.

Tato diplomová práce je vedena zejména *metodou analýzy*. Zpočátku však bude užitá převážně *metoda deskriptivní*, která si klade za cíl uvést do problematiky dokazování a vymezit teoretické pojmy, jež jsou pro pochopení této práce stěžejní. V rámci jednotlivých kapitol je použita mimo analýzu i *komparativní metoda*. Jako součást dílčích shrnutí kapitol a závěru této práce budou navržena možná východiska právní úpravy *de lege ferenda*, užitá tak bude i *metoda preskriptivní*. Práce současně obsahuje *kvalitativní výzkum* provedený prostřednictvím rozhovorů s policisty, kteří se elektronickými důkazy zabývají v praxi.

1. Dokazování v trestním řízení

1.1. Význam a podstata dokazování

Dokazování tvoří důležitou součást trestního řízení, jsou při něm uplatňovány základní zásady trestního procesu.⁷ Aby mohl být naplněn účel trestního řízení tak, jak předpokládá ustanovení § 1 odst. 1 trestního řádu, musí být zjištěn skutkový základ pro rozhodování a další postup. Vedle rozhodování tak můžeme označit dokazování jako jednu z nejdůležitějších procesních činností orgánů činných v trestním řízení. Za dokazování můžeme označit takový postup orgánů činných v trestním řízení, jehož prostřednictvím jsou zjišťovány trestné činy a osoby, které trestný čin spáchaly či se na jeho spáchání jinak podílely.⁸

„V tradicích všech moderních právních řádů světa představuje dokazování dosud jediný a nenahraditelný postup ke zjištění pravdy v rozsahu požadovaném tím kterým právním řádem“⁹, význam dokazování je tedy nutné chápat jako jedinou možnost, prostřednictvím které orgány činné v trestním řízení mohou poznat skutkový stav věci, o němž nejsou důvodné pochybnosti, a to v nezbytném rozsahu tak, aby mohlo dojít k jeho trestněprávnímu posouzení a rozhodnutí.¹⁰

Jak je naznačeno výše, je nezbytností, aby dokazování bylo provedeno v potřebném rozsahu, kvalitě a zejména za dodržení zákonných požadavků. Orgány činné v trestním řízení opatřují informace o konkrétní minulé události či jiné skutečnosti významné z hlediska trestního práva, ze které pomocí logického postupu upraveného trestními předpisy odvozují úsudek o předmětu dokazování. Jedině takové zjištění může vést ke správnému a spravedlivému rozhodnutí ve věci.¹¹ Je však vhodné upozornit na dva zájmy, k jejichž střetu při dokazování dochází. Prvním z nich je zájem společnosti na trestním stíhání pachatelů trestných činů a druhým integrita individuálních či celospolečenských hodnot přesahující trestní stíhání. Velmi důležitou roli při těchto otázkách, jež se jeví být spornými a jež nejsou upraveny zákonem, hraje judikatura Ústavního soudu a současně i rozhodnutí obecných soudů, které se velmi významně podílí na sjednocování přípustných způsobů a postupů při dokazování.¹²

⁷ JELÍNEK, J. *Trestní právo procesní*. 7. aktualizované a doplněné vydání podle stavu k 1.9. 2023. Praha: Leges, 2023. ISBN 978-80-7502-687-3. s. 408-409

⁸ POLČÁK, R., PŮRY, F., HARAŠTA, J., MYŠKA, M. a STUPKA, V. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015, ISBN 978-80-210-8073-7. s. 253

⁹ KALVODOVÁ, V., ŠÁMAL, P. a HRUŠÁKOVÁ, M. *Dokazování v trestním řízení – právní, kriminologické a kriminalistické aspekty*. Brno: Masarykova univerzita, 2015. ISBN 978-80-210-8072-0. s. 29

¹⁰ POLČÁK, R., PŮRY, F., HARAŠTA, J., MYŠKA, M. a STUPKA, V. *Elektronické důkazy v trestním řízení*. Op. cit., s. 253

¹¹ *Tamtéž*, s. 253

¹² JELÍNEK, J. *Trestní právo procesní*. Op. cit., s. 408-409

Nesmíme však opomenout ani přeshraniční legislativu, která upravuje základní standardy dokazování, jakou je např. Úmluva o ochraně lidských práv a základních svobod pocházející od Rady Evropy. Přijetím výše uvedené úmluvy se Česká republika zavázala k jejímu dodržování a z tohoto důvodu je nezbytné přihlížet nejen k judikatuře vnitrostátní, ale v tomto případě i k judikatuře Evropského soudu pro lidská práva. Důležitou roli sehrává v případě dokazování především článek 6 Úmluvy pro lidská práva a základní svobody, který se týká spravedlivého procesu. Není výjimečné, že dojde ke střetu vnitrostátní právní úpravy a její aplikace s požadavky Úmluvy. V těchto případech pak v souladu s přímou aplikací a postavením Úmluvy nad vnitrostátní právní úpravou musíme užít přímé aplikace ustanovení Úmluvy.¹³

Je důležité zdůraznit, že Úmluva neobsahuje zvláštní ustanovení o dokazování, ta je upravena státy v rámci vnitrostátní úpravy, a to zejména s přihlédnutím k rozdílnostem mezi právní úpravou v jednotlivých evropských zemích. Nicméně v souladu s požadavkem spravedlivého procesu dle článku 6 Úmluvy jsou upraveny jisté mantinely, které dávají základ vnitrostátní úpravě dokazování.

Mezi atributy práva na spravedlivý proces ve smyslu Úmluvy řadíme zejména princip *rovnosti zbraní*, který lze vysvětlit jako možnost každé strany trestního procesu hájit své zájmy a zároveň požadavek, aby ani jedna ze stran neměla podstatnou výhodu vůči odpůrci straně. V kontextu dokazování je smyslem zásady možnost navrhování a předkládání důkazů na svou obhajobu či na podporu svého tvrzení. Druhým atributem, jenž by neměl být opomenut, je *právo na rozhodnutí věci v přiměřené lhůtě*. A konečně třetím atributem, jenž považuji za nezbytný uvést, je *požadavek kontradiktornosti*, který navazuje na princip rovnosti zbraní. Požadavek kontradiktornosti má za cíl zabezpečit, aby bylo dosaženo projednání věci za podmínek, které nestaví protistranu do nevýhodného postavení. Zejména se jedná o možnost každé ze stran seznámit se se všemi tvrzeními, důkazy, podklady, navrhopat je, a dále možnost vyjádřit se a eventuálně popírat argumenty, tvrzení a důkazy navrhované protistranou či obstarané soudem. V trestním řízení se uplatňují především při předkládání a provádění důkazů, zejména pak při výslechu svědků.¹⁴

Pro shrnutí, za dokazování můžeme v trestním právu procesním označit zákonem upravený postup orgánů činných v trestním řízení, který má za úkol umožnit poznání důležitých skutečností pro rozhodnutí ve věci, tedy vyhledat důkazy, provést je a následně procesně zajistit

¹³ JELÍNEK, J. *Trestní právo procesní*. Op. cit., s. 408-409

¹⁴ *Tamtéž*, s. 408-409

a zhodnotit získané poznatky.¹⁵ Je vhodné neopomenout, že dokazování není omezeno pouze na rozhodnutí ve věci, ale i na procesní rozhodnutí.^{16,17}

1.2. Důkazní právo a zásady

Důkazní právo, za které teorie označuje souhrn pravidel a předpisů, jež upravují stádia dokazování jako je vyhledávání, provádění a hodnocení důkazů, vychází ze základních zásad trestního procesu. Stádia dokazování spolu vzájemně souvisejí a prolínají se, zejm. *provádění a hodnocení důkazů*.¹⁸ Mezi zásady uvedené ve větě výše je nezbytné řadit zásadu oficiality (§ 2 odst. 4 trestního řádu), zásadu vyhledávací (§ 2 odst. 5 trestního řádu), zásadu presumpce nevinny (§ 2 odst. 2 trestního řádu), zásadu materiální pravdy (§ 2 odst. 5 trestního řádu), zásadu volného hodnocení důkazů (§ 2 odst. 6 trestního řádu) a zásadu bezprostřednosti a ústnosti (§ 2 odst. 10, odst. 11 trestního řádu).

Postup orgánů činných v trestním řízení vedoucí k opatření a zajištění určité relevantní okolnosti, aby mohlo v rámci trestního řízení dojít k jejímu provedení a hodnocení, označujeme jako *vyhledávání důkazů*. Další fázi, resp. procesní činností, kdy je přípustným, zákonem stanoveným způsobem zjišťován předmět důkazu, nazýváme *provádění důkazů*. Je důležité podotknout, že okolnost, kdy důkaz, nebyl vyžádán či vyhledán orgánem činným v trestním řízení, nemůže být důvodem, aby byl takový důkaz odmítnut.¹⁹

Poslední fází je *hodnocení důkazů*, jedná se o rozumový a myšlenkový postup, kdy dochází k hodnocení pravdivosti, závažnosti a zákonnosti důkazu. S tím souvisí i prověrka důkazů, v rámci, které dochází k prověřování již hodnocených důkazů v souladu se zásadou volného hodnocení důkazů, tj. povinností hodnotit každý důkaz zvlášť, ale i ve vzájemné souvislosti. Konečné hodnocení důkazů však probíhá až v rámci meritorního rozhodnutí spolu s odůvodněním tohoto rozhodnutí, tedy po opatření veškerého důkazního materiálu.^{20,21}

Za účel dokazování v trestním řízení můžeme označit rekonstrukci okolnosti z minulosti tak, aby poznání bylo jejím věrným odrazem, tj. ve shodě se s touto okolností. To jediné

¹⁵ JELÍNEK, J. *Trestní právo procesní*. Op. cit., s. 413

¹⁶ Srov. rozhodování o vazbě

¹⁷ KALVODOVÁ, V., ŠÁMAL, P. a HRUŠÁKOVÁ, M. *Dokazování v trestním řízení – právní, kriminologické a kriminalistické aspekty*. Op. cit., s. 28

¹⁸ FENYK, J., CÍSAŘOVÁ, D., GRÍVNA, T. a kol. *Trestní právo procesní*. 7. vydání. Praha: Wolters Kluwer ČR, 2019, 952 s. ISBN 978-80-7598-306-0., s. 345

¹⁹ § 89 odst. 2 trestního řádu

²⁰ FENYK, J., CÍSAŘOVÁ, D., GRÍVNA, T. a kol. *Trestní právo procesní*. Op. cit., s. 345

²¹ Srov. § 125 odst. 1 a § 134 odst. 2 trestního řádu

umožňuje orgánům činným v trestním řízení poznat pravdu, a jedině ta může být podkladem pro spravedlivé rozhodnutí ve věci.²²

1.3. Pojem předmět důkazu, důkazní prostředek a důkaz

K pochopení dokazování v trestním řízení a současně pro porozumění této práci je vhodné nejprve vymežit následující pojmy, mezi kterými je nutné rozlišovat. Jedná se jmenovitě o *předmět důkazu* (ten je dále možno členit na *předmět dokazování* a *předmět jednotlivého důkazu*), *důkazní prostředek* a *důkaz*.

Jako *předmět důkazu* označujeme skutečnost, která má být orgány činnými v trestním řízení zjištěna, a na které přímo či nepřímo závisí rozhodnutí ve věci samé. Jedná se o skutečnost, kterou je nezbytné v rámci trestního řízení dokázat či vyvrátit. V této souvislosti dále rozlišujeme *předmět dokazování* a *předmět jednotlivého důkazu*. *Předmět dokazování* neboli také rozsah je souborem skutečností, které je nutné v rámci trestního řízení dokázat. Tento rozsah se může v průběhu řízení měnit podle toho, jaký okruh okolností je nutné ve věci dokazovat, je však nutné, aby byl v každé fázi dokazování přesně vymezen. Trestní řád tyto skutečnosti demonstrativně uvádí.²³ Za *předmět jednotlivého důkazu* označujeme dílčí skutkovou okolnost, jenž má být v rámci procesu dokazování zjištěna.²⁴ *Předmětem dokazování* tedy může být například skutečnost, zda došlo k internetovému podvodu či zda byl tento skutek spáchán obviněným. *Předmětem jednotlivého důkazu* mohou být např. záznamy logování k online bankovníctví poškozeného či emailová komunikace mezi pachatelem a poškozeným s falešným odkazem.

Aby mohlo dojít ke zjištění výše uvedené skutečnosti, je zapotřebí využití *důkazního prostředku*. Jedná se o způsob, pomocí kterého orgán činný v trestním řízení poznává skutečnosti, resp. nabývá potřebných poznatků, ať už přímým pozorováním, tj. svými smysly (ohledání osoby či věci, výslech osob) či seznamování se s obsahem zpráv o předmětu důkazu zachycených na věcech (písemně, promítáním, přehráním).²⁵ Jedná se tedy o konkrétní prostředek či způsob, jakým je možné takovou skutečnost prokázat nebo vyvrátit. Trestní řád uvádí, že za důkaz může sloužit „vše, co může přispět k objasnění věci“²⁶. Je však nutné přihlídnout i k ustanovení § 99 a § 100 trestního řádu, které uvádí, že někdy zákon použití

²² FENYK, J., CÍSAŘOVÁ, D., GŘIVNA, T. a kol. *Trestní právo procesní*. Op. cit., s. 347

²³ § 89 odst. 1 trestního řádu

²⁴ FENYK, J., CÍSAŘOVÁ, D., GŘIVNA, T. a kol. *Trestní právo procesní*. Op. cit., s. 346

²⁵ JELÍNEK, J. *Trestní právo procesní*. Op. cit., s. 432-433

²⁶ § 89 odst. 2 trestního řádu

některého důkazního prostředku zcela zakazuje, děje se tomu tak v případech, kdy by provedením došlo ke způsobení vážné škody státu či ohrožení jiných chráněných zájmů.²⁷ Současně je třeba poznamenat, že v souladu s již citovaným dovětkem ustanovení § 89 odst. 2 trestního řádu, má mít provedený důkazní prostředek souvislost se skutečností, která je dokazována.²⁸ Za elektronický důkazní prostředek můžeme označit vše, jenž může být zdrojem²⁹ informace a je uchováváno v elektronické podobě. *Elektronickým důkazním prostředkem* jsou tak zejména data, která v sobě nesou informaci a jsou schopné ji zobrazit.³⁰ Může se jednat například o data nesoucí v sobě informace o zachycené aktivitě, data ve formě textových zpráv, obrazových, zvukových či obrazově-zvukových záznamů, informace o poloze.

K výše uvedenému je dále nezbytné uvést i *nepřípustnost* či *nezpůsobilost* některých důkazů. U *nepřípustnosti* mluvíme o případech, kdy je důkaz získán nezákonným donucením či hrozbou takového donucení, s výjimkou, kdy je takový důkaz použit proti osobě, jež takové donucení či hrozby sama použila.³¹ Za *nezpůsobilý* je v souladu s odbornou literaturou považován také důkaz, který je dle aktuálního stavu lidského poznání nespolehlivý, či u takového důkazu nelze kontrolovat postup tak, aby byla zaručena ochrana základních práv a svobod osob, jež se účastní takového provádění důkazu. Jen výjimečně však zákon požaduje, aby ke zjištění konkrétní skutečnosti bylo použito konkrétního důkazního prostředku.^{32,33}

V neposlední řadě je vhodné definovat *důkaz*, za ten označujeme přímý poznatek, informaci, kterou orgán činný v trestním řízení o předmětu důkazu získal pomocí procesního úkonu, tedy poznatky získané provedením ohledání, obsah výpovědi osob či obsah listin apod. Je důležité zdůraznit, že každý procesní důkaz je pevně spjat s určitou věcí (předměty ohledání, listiny) nebo určitou osobou (výslech, ohledání osoby), které můžeme označit za *nositele* či *prameny důkazu*.³⁴ Za *důkaz* můžeme označit data již interpretovaná (analyzovaná), jež pro zpracovatele mají smysl.³⁵ Jedná se o projev důkazního prostředku v konkrétním případě,

²⁷ § 89 odst. 2 trestního řádu

²⁸ ŠÁMAL, P. a kol. *Trestní řád*. 7. vydání. Praha: C. H. Beck, 2013. ISBN 978-80-7400-465-0., s.1308-1394

²⁹ Ze kterého orgán činný v trestním řízení čerpá.

³⁰ POLČÁK, R., PÚRY, F., HARAŠTA, J., MYŠKA, M. a STUPKA, V. *Elektronické důkazy v trestním řízení*. Op. cit., s. 94-95

³¹ § 89 odst. 3 trestního řádu

³² Srov. Nezbytnost znalce u zjištění příčiny smrti člověka, v případech podezření na způsobení smrti trestným činem.

³³ FENYK, J., CÍSAŘOVÁ, D., GRIVNA, T. a kol. *Trestní právo procesní*. Op. cit., s. 349

³⁴ JELÍNEK, J. *Trestní právo procesní*. Op. cit., s. 412

³⁵ POLČÁK, R., PÚRY, F., HARAŠTA, J., MYŠKA, M. a STUPKA, V. *Elektronické důkazy v trestním řízení*. Op. cit., s. 94-95

ve světle elektronických důkazů můžeme za příklad uvést fotografie pachatele zachycené bezpečnostní kamerou na místě činu.

V průběhu vyšetřování se sledují různé aspekty spojené s konkrétním trestným činem. Předmětem dokazování jsou mnohé skutečnosti týkající se krádeže, zatímco předmětem jednotlivých důkazů mohou být konkrétní detaily, například fotografie pachatele nebo geolokalizační data telefonu. K získání nezbytných informací jsou použity různé důkazní prostředky, včetně ohledání místa činu, výslechu svědků nebo záznamů telekomunikačního provozu. Konkrétní důkaz může například spočívat ve fotografii pachatele zachycené bezpečnostní kamerou. Je však klíčové zajistit, aby všechny důkazy byly shromážděny a použity zákonně, tj. v souladu s platnými právními normami a současně s důrazem na autentičnost a integritu informací.

1.4. Dělení důkazů

Důkazy můžeme dělit podle několika kritérií. Toto dělení si klade za cíl lepší pochopení významu a povahy jednotlivých důkazů, nejen pro teorii, ale zejména pro praxi. Ačkoliv tradice dělení důkazů není v trestněprávní teorii zcela jednotná³⁶, učebnicová literatura se přiklání ke třem kategoriím uvedeným níže.

První kategorií, která zde bude představena, je dělení důkazů na základě vztahu k předmětu řízení na důkazy *usvědčující* a *ospravedlňující*. Jak by se dalo dovodit samotným jazykovým výkladem, usvědčujícími důkazy rozumíme důkazy, jež prokazují skutečnosti svědčící proti obviněnému, zatímco ospravedlňujícími důkazy ty, které svědčí ve prospěch obviněného. Důkaz, který může mít za určitých okolností ospravedlňující povahu, bude za jiných okolností důkazem usvědčujícím. I samotná změna povahy důkazu během trestního řízení je možná, tedy to, že důkaz, který byl prvně předložen jako usvědčující, se během řízení ukáže jako ospravedlňující či obráceně. Z toho plyne, že konečná klasifikace důkazu je možná až dle závěrečného hodnocení všech důkazů.³⁷ Za příklad elektronického důkazu můžeme uvést video (zvukově-obrazový) záznam z bezpečnostních kamer zachycující osobu pachatele na místě činu, který může být jak *usvědčujícím* důkazem, v případě, kdy osobou zachycenou na záznamu bude obviněný A. Naopak se bude jednat o důkaz *ospravedlňující*, bude-li zjištěno, že osoba zachycená při páchaní trestné činnosti je rozdílná od osoby obviněného A, a to právě ve vztahu k trestnímu stíhání proti obviněnému A.

³⁶ FENYK, J., CÍSAŘOVÁ, D., GRIVNA, T. a kol. *Trestní právo procesní*. Op. cit., s. 358

³⁷ JELÍNEK, J. *Trestní právo procesní*. Op. cit., s. 434-435

Jednotlivé hodnocení důkazů během řízení má však neméně význam, neboť brání jednostrannému přístupu orgánů činných v trestním řízení, a z toho důvodu ho užívá i trestní řád. Orgány činné v trestním řízení musí v souladu se zákonem stejně důkladně objasňovat okolnosti, které svědčí proti obviněnému, jako okolnosti svědčící v jeho prospěch.³⁸ Ve světle shora vymezeného je však důležité zdůraznit, že tímto dělením se nevystihuje podstata důkazu, ale pouze se jím zakládá na významu důkazů pro rozhodnutí o dokazované skutečnosti.³⁹

V závislosti na vztahu k dokazované skutečnosti odborná literatura dále dělí důkazy na *přímé* (prosté) a *nepřímé* (složené neboli také indicie). První podkategorií je důkaz *přímý*, za takový označujeme důkaz, jež přímo potvrzuje či vyvrací dokazovanou skutečnost, resp. vinu. Důkaz *nepřímý* je potom ten, který dokazuje skutečnost jinou, která je vedlejší, avšak může z ní být usuzována skutečnost hlavní, takový důkaz je pak označován jako důkaz z indicií. *Nepřímým* důkazem je tedy objasňována skutečnost, jež má být dokázána, a to s pomocí skutečnosti jiné, jež má k této skutečnosti nepřímý vztah. Jak uvádí Jelínek, nepřímé důkazy často bývají jedinými a v praxi jsou proto velmi důležité k objasnění věci.⁴⁰ Okolnost, že se jedná o důkazy *nepřímé* je však nestaví do slabší, méně spolehlivé či nevýznamné pozice oproti důkazům *přímým*, vždy záleží na jednotlivé věci a okolnostech případu, tzn. v konkrétní věci mohou být pro bezpečné objasnění věci *nepřímé* důkazy naopak významnějšími. Co je však potřebné zdůraznit je, že dokazování *nepřímými* důkazy je obtížnější a takové důkazy musí být s okolnostmi případu v příčinné souvislosti, a to přesvědčivě. Jak uvádí odborná literatura,⁴¹ u *přímých* důkazů je tato souvislost jasná. *Nepřímé* důkazy mj. umožňují prověřit důkazy *přímé* a doplnit mezery v řízení.⁴²

„Při používání nepřímých důkazů se v praxi často přehlíží, že souhrn nepřímých důkazů musí podávat ucelený obraz o trestném jednání obviněného tak, aby žádný z jednotlivých důkazů nepřipouštěl jiný ani pravděpodobný výklad, který by odporoval nebo narušoval verzi obvinění.“⁴³ K dokázání hlavní skutečnosti, tedy v případě, kdy nepřímý důkaz není spojen s přímým důkazem, nestačí pouze jediný nepřímý důkaz, ale těchto nepřímých důkazů musí být více, a současně je nezbytné, aby tvořily uzavřený „řetěz“. *„Aby nepřímé důkazy byly způsobilé k prokázání viny obviněného, musí však tvořit logickou a ničím nenarušovanou soustavu vzájemně se doplňujících a podmiňujících důkazů, které ve svém celku spolehlivě prokazují*

³⁸ Srov. § 2 odst. 5 trestního řádu

³⁹ FENYK, J., CÍSAŘOVÁ, D., GRIVNA, T. a kol. *Trestní právo procesní*. Op. cit., s. 358

⁴⁰ JELÍNEK, J. *Trestní právo procesní*. Op. cit., s. 435-436

⁴¹ FENYK, J., CÍSAŘOVÁ, D., GRIVNA, T. a kol. *Trestní právo procesní*. Op. cit., s. 360

⁴² *Tamtéž*, s. 360

⁴³ Rozsudek Nejvyššího soudu Československé socialistické republiky sp. zn. 7 Tz 11/68, ze dne 9. 4. 1968

všechny okolnosti zažalovaného skutku a přesvědčivě svědčí pro vinu obviněného a zároveň vylučují možnost úvahy o jiném závěru.⁴⁴ Polčák u elektronických důkazů, jakými může být např. emailová zpráva či vyhotovené CD, dále rozvíjí diskuzi nad problematikou zkoumání autorství. K jeho určení může být využit mimo jiné i znalec, který ve svém znaleckém posudku provede jazykovou analýzu a interpretaci textu, dále se posuzuje možnost fyzického přístupu k zařízení, ze kterého byl email odeslán, znalost přístupového klíče, elektronický podpis apod.⁴⁵ Jak bylo nastíněno, ačkoliv došlo k odeslání emailu ze schránky osoby A, nelze vyloučit, že nemohlo dojít ke zfalšování či neoprávněnému přístupu do emailové schránky jiného a vytvoření předmětné emailové zprávy osobou rozdílnou od osoby A. Na základě toho, zda se povede pomocí jiných důkazů určit či neurčit autorství, bude na důkaz pohlíženo jako na *přímý* či *nepřímý*.

Třetí kategorizací, která zde je stručně popsána, jsou důkazy *původní* (bezprostřední) a *odvozené* (zprostředkované). Jako *původní* je označován důkaz, jež vychází z přímého zdroje poznání, je jím např. výpověď svědka o skutečnostech, které pozoroval vlastními smysly či originál listiny. Naproti tomu za *odvozený* důkaz označujeme ten, jež je ze zprostředkovaného pramene, může jím být např. výpověď svědka, který skutečnost nepozoroval vlastními smysly, ale pouze reprodukuje to, co ví o skutečnosti z doslechu, či vyšetřovací pokus.⁴⁶

Odborná literatura se shoduje, že orgán činný v trestním řízení by se měl zejména snažit vyhledat důkazy, které budou svou povahou *původní*⁴⁷. V případech, kdy tomu tak není možné (např. jediný svědek skutečnosti zemřel a jiné *původní* důkazy nejsou k dispozici), je nutno rozhodnout na jejich podkladě *odvozených*. Orgány činné v trestním řízení si však musí počínat velmi pozorně při jejich prověřování a hodnocení, neboť je zde větší šance, že mohlo dojít k překroucení dokazované skutečnosti.⁴⁸ „Ze zásady volného hodnocení důkazů plyne mimo jiné to, že zákon nepředepisuje důkazní sílu jednotlivých druhů důkazů ani nevylučuje použití odvozeného důkazu (např. tzv. „svědectví z doslechu“).“⁴⁹ Svůj význam mají *odvozené* důkazy dále i při jejich užití ke zjištění důkazu *původního*.⁵⁰ Mám za to, že za *původní* elektronický důkaz bychom mohli označit zvukový záznam telefonátu pořízený orgány činnými v trestním

⁴⁴ Rozsudek Nejvyššího soudu Československé socialistické republiky sp. zn. 7 Tz 11/68, ze dne 9. 4. 1968

⁴⁵ POLČÁK, R., PÚRY, F., HARAŠTA, J., MYŠKA, M. a STUPKA, V. *Elektronické důkazy v trestním řízení*. Op. cit., s. 133

⁴⁶ FENYK, J., CÍSAŘOVÁ, D., GRIVNA, T. a kol. *Trestní právo procesní*. Op. cit., s. 359

⁴⁷ Srov. § 2 odst. 10 trestního řádu

⁴⁸ JELÍNEK, J. *Trestní právo procesní*. Op. cit., s. 435-436

⁴⁹ Usnesení Ústavního soudu ze dne 13. 3. 2014, sp. zn. III. ÚS 859/13

⁵⁰ JELÍNEK, J. *Trestní právo procesní*. Op. cit., s. 435-436

řízení v rámci použití ustanovení trestního řádu⁵¹ o odposlechu a záznamu telekomunikačního provozu. Naproti tomu za *odvozený* elektronický důkaz by byl považován například snímek obrazovky komunikace probíhající na sociální síti, která byla orgánu činnému v trestním řízení předložena ze strany poškozeného (nikoliv pořízená samotným policejním orgánem).

Původní důkaz bude velmi často i důkazem *přímým*, zatímco *odvozený* důkaz bude důkazem *nepřímým*. I přesto, jak bylo popsáno výše, se jedná o dvě zcela rozdílné kategorie, a proto je jejich směšování nesprávné.

1.5. Předmět a rozsah dokazování

Z dikce zákona plyne, že *předmětem dokazování* jsou okolnosti, které jsou pro trestní řízení důležité, demonstrativní výčet okolností nalezneme v ustanovení § 89 odst. 1 trestního řádu. Závisí na skutečných podmínkách a okolnostech konkrétního případu, tj. za současného vlivu trestního práva hmotného, a také formě a stádiu trestního řízení. Odborná literatura⁵² je systematicky shrnuje pouze do tří následujících skupin dle hledisek, ze kterých na ně nahlížíme.

Prvním je *hledisko hmotného práva*, na základě kterého zkoumáme *okolnosti důležité pro rozhodnutí ve věci samé*, dále na okolnosti pohlížíme z *hlediska procesního práva*, kdy zkoumáme, zda se jedná o *okolnosti důležité pro postup v trestní řízení* a posledním hlediskem je spojení výše uvedených, tzn. *hledisko hmotného i procesního práva*, na jehož základě zkoumáme *okolnosti důležité pro použití odklonů, resp. zvláštních způsobů řízení*.⁵³ Stejně jako je tomu v případě výčtu okolností v zákoně, je třeba zdůraznit, že ani konkrétní okolnosti, jež budou v konkrétním případě předmětem dokazování, nelze vymezit taxativně. Orgán činný v trestním řízení se však nezabývá zjištěními, které nemají pro objasnění konkrétního případu význam, *a contrario* by takové dokazování vedlo k nepřehlednosti a nadměrnému zmohutnění trestního řízení.⁵⁴ „*Rozsah dokazování není bezbřehý. Pokud proto soud prvního stupně provedl dokazování okolností uvedených v § 89 odst. 1 TrŘ v nezbytném rozsahu, je opatřování dalších důkazů nadbytečné a trestní stíhání by pouze nedůvodně protahovalo.*“⁵⁵ Je vhodné shrnout, že tato výběrovost je důležitá k efektivnímu průběhu trestního řízení.

⁵¹ § 88 trestního řádu

⁵² FENYK, J., CÍSAŘOVÁ, D., GRIVNA, T. a kol. *Trestní právo procesní*. Op. cit., s. 350

⁵³ *Tamtéž*, s. 350-351

⁵⁴ Srov. § 55, § 56 nebo § 69 zákona č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů (zákon o soudnictví ve věcech mládeže)

⁵⁵ Usnesení Vrchního soudu v Praze ze dne 14. 9. 2006, sp. zn. 2 To 62/2006

V souvislosti s *hlediskem hmotného práva* zkoumáme okolnosti, které tvoří znaky trestného činu, tj. jednání, následek, příčinnou souvislost mezi nimi, zda je tu zavinění a trestně odpovědný pachatel, a zda trestní odpovědnost není z nějakého důvodu vyloučena. Dále se zabýváme okolnostmi, které nasvědčují či vyvracejí, že obviněný je pachatelem trestného činu, pro nějž se trestní řízení vede. Zkoumají se následně i okolnosti podmiňující důvody vylučující protiprávnost, tedy trestnost, srov. nutná obrana, krajní nouze, svolení poškozeného či promlčení, milost, účinná lítost. V rámci *hmotněprávního hlediska* dále zkoumáme i okolnosti, které vedly k trestné činnosti či umožnily její spáchání, okolnosti rozhodné pro určení výměry trestu, o náhradě škody, nemajetkové újmy či vydání bezdůvodného obohacení.⁵⁶

U *procesněprávního hlediska* uvádí odborná literatura např. okolnosti odůvodňující přerušení řízení či zproštění povinnosti svědčit. Při dokazování těchto okolností postačí důkaz prostředky, jež jsou orgánu činnému v trestním řízení k dispozici, a postačí též nižší hodnověrnost takového důkazu, než je tomu u hmotněprávních okolností.⁵⁷

Ve třetím případě, tj. *spojení procesněprávního a hmotného hlediska*, je podřízeno dokazování takových okolností jejich účelu. Je zde vyžadována skupina důkazů, jež potvrzuje i některé jiné skutečnosti, které však s hmotným právem nemusí bezprostředně souviset, srov. náhrada škody, stanovisko poškozeného.⁵⁸

Vždy je však u shora uvedeného nutné dokazovat okolnosti, které jsou důležitými pro hodnocení věrohodnosti důkazů. Pro srovnání např. zda byla dána schopnost svědka správně vnímat skutečnost, o které podával výpověď, resp. zda nebyla schopnost vnímat skutečnosti snížena či vyloučena.⁵⁹ Jak bylo zmíněno výše, určení předmětu dokazování, tj. rozsahu, je nutné v každé fázi dokazování přesně a jasně vymezit. Toto vymezení však není předmětem jednoho úkonu, ale konečný závěr o tom, co bude předmětem dokazování ve věci, se bude měnit v průběhu dokazování, a to v souvislosti s tím, jaké jsou dosud zjištěné výsledky dokazování.

Co však nebude předmětem dokazování, jsou právní předpisy a mezinárodní smlouvy uveřejněné ve Sbírce zákonů a mezinárodních smluv,⁶⁰ zde se uplatní zásada *iura novit curia* (soud zná právo). *A contrario* je však nutné dokazovat právní normy, které uveřejněny v těchto

⁵⁶ FENYK, J., CÍSAŘOVÁ, D., GRIVNA, T. a kol. *Trestní právo procesní*. Op. cit., s. 351

⁵⁷ *Tamtéž*, s. 353

⁵⁸ *Tamtéž*.

⁵⁹ JELÍNEK, J. *Trestní právo procesní*. Op. cit., s. 430

⁶⁰ Zákon č. 222/2016 Sb., o Sbírce zákonů a mezinárodních smluv a o tvorbě právních předpisů vyhlášených ve Sbírce zákonů a mezinárodních smluv (zákon o Sbírce zákonů a mezinárodních smluv)

sbírkách nejsou. S tím souvisí i další skutečnosti, které dokazovat nelze, vyplývající z ustanovení § 9 odst. 2 trestního řádu. Jedná se o otázky týkající se osobního stavu, jež jsou vyhrazeny výlučně občanskoprávnímu soudnímu řízení.

Pokud však i po vyčerpání všech důkazů, které bylo možné vyhledat a provést, jsou stále pochybnosti důležité pro rozhodnutí ve věci, je nezbytné rozhodnout v souladu se zásadou *in dubio pro reo*, tj. v pochybnostech ve prospěch obžalovaného.

1.6. Proces dokazování

V rámci dokazování jsou uváděny tři stádia průběhu dokazování, jmenovitě se jedná o *vyhledávání důkazů*, *provádění důkazů* a jejich *hodnocení*.

V prvním stádiu *vyhledávání důkazů* orgány činné v trestním řízení vyvíjejí činnost, při které vyhledávají důkazy o skutečnostech relevantních pro trestní řízení. Ve *fázi prověřování* je vyhledávání důkazů omezeno zejména na následující okolnost. Jsou zjišťovány skutečnosti důvodně nasvědčující spáchání trestného činu, resp. skutečnosti nasvědčující, že skutek je trestným činem a že ho spáchala určitá osoba. Po zahájení trestního stíhání, ve *fázi vyšetřování*, dochází ze strany orgánů činných v trestním řízení k vyhledávání důkazů, jež jsou podkladem pro obžalobu.⁶¹

Druhou fází je *provádění důkazů*, tato fáze je zejména soustředěna do řízení před soudem. Zde orgány činné v trestním řízení stanoveným postupem zjišťují předmět důkazu a dochází k jeho hodnocení. Těžištěm dokazování je hlavní líčení, jehož cílem je prokázání, zda je skutek, o němž se trestní řízení vede, trestným činem a zda obžalovaný je pachatelem tohoto skutku. Řízení je vedeno zásadou materiální pravdy a předseda senátu je povinen provést veškeré důkazy tak, aby o zjištěném skutkovém stavu nebyly důvodné pochybnosti.⁶² Jako příklad *elektronických důkazů* můžeme uvést předložení fotografií, přehrání zvukového či obrazového záznamu za použití příslušné techniky či čtení znaleckého posudku o výsledku ohledání a zkoumání předmětného datového nosiče.⁶³ Současně může v souladu s ustanovením § 183 odst. 1 trestního řádu předseda senátu kdykoliv požádat policejní orgán o opatření jednotlivého důkazu.⁶⁴ Dříve, než je uskutečněno hlavní líčení, je *provádění důkazů* možné i v rámci předběžného projednání obžaloby, jež může fakultativně následovat po přípravném

⁶¹ FENYK, J., CÍSAŘOVÁ, D., GRIVNA, T. a kol. *Trestní právo procesní*. Op. cit., s. 480-482

⁶² *Tamtéž*, s. 345-346

⁶³ POLČÁK, R., PÚRY, F., HARAŠTA, J., MYŠKA, M. a STUPKA, V. *Elektronické důkazy v trestním řízení*. Op. cit., s. 65

⁶⁴ FENYK, J., CÍSAŘOVÁ, D., GRIVNA, T. a kol. *Trestní právo procesní*. Op. cit., s. 345-346

řízení poté, co byla podána obžaloba (*a contrario* to nelze u podání návrhu na potrestání). Pokud je rozhodnuto o konání předběžného projednání, je *provádění důkazů* (např. přehrání zvukového záznamu) soustředěno pouze na zjištění, zda byl důkaz zajištěn v souladu s procesními předpisy a nemá vady⁶⁵, které by jeho použití v řízení znemožňovaly.⁶⁶

Poslední fází je *hodnocení důkazů*, v rámci kterého soud s přihlédnutím k zásadě volného hodnocení důkazů hodnotí nejprve každý jednotlivý důkaz samostatně a následně veškeré důkazy ve vzájemné souvislosti. Jedná se o „*závěrečný rozumový a myšlenkový postup, kterým se hodnotí závažnost (upotřebitelnost z hlediska skutkového stavu), zákonnost (přípustnost jeho opatření a provedení), pravdivost důkazu (zda obsahuje pravdivé skutečnosti)*“.⁶⁷

Dle teorie jsou tyto fáze rozděleny v průběhu trestního řízení do jednotlivých stádií, avšak není to podmínkou a jednotlivé fáze mohou probíhat pouze v jednom ze stádií, např. ve stádiu *přípravného řízení*. *Elektronické důkazy*, které byly v souladu se zákonem získány pomocí operativně pátracích prostředků v rámci přípravného řízení, lze použít v průběhu celého řízení, srov. § 158b odst. 3 trestního řádu. Jako příklad si můžeme uvést data získaná z obsahu emailové schránky, která byla orgány činnými v trestním řízení získána v souladu s ustanovením o sledování osob a věcí.

⁶⁵ Blíže k nedodržení procesních předpisů je pojednáno v kapitole 1.3 této práce.

⁶⁶ FENYK, J., CÍSAŘOVÁ, D., GRIVNA, T. a kol. *Trestní právo procesní*. Op. cit., s. 345-346

⁶⁷ *Tamtéž*, s. 346

2. Elektronické důkazní prostředky

Právní úprava dokazování v České republice se formulovala v šedesátých letech 20. století, a přestože prošla značnou novelizací, vznikala v době, kdy zákonodárce netušil, co je „*internet nebo technologie generující elektronické důkazy*“⁶⁸, a tak netvořil a ani nemohl tvořit normy, které by moderním technologiím odpovídaly.

Trestní řízení je upraveno na vnitrostátní úrovni, což vede ke zdatelným rozdílům mezi jednotlivými právními jurisdikcemi. Ačkoliv se při normotvorbě jednotlivé národy inspirují a čerpají z právní úpravy jiných, zejm. okolních států a do národního právního řádu jsou implementovány mezinárodní nástroje, jako jsou *mezinárodní úmluvy* a v případě členských států Evropské Unie také *komunitární právo*, na mezinárodní úrovni k dokazování elektronickými důkazními prostředky žádný právní rámec národům poskytován není. Nezbyvá tedy než uvést, že vývoj informačních a komunikačních technologií tak přináší pro trestní řízení (a pro dokazování) jednoznačně velkou výzvu.

Tím spíše můžeme dovodit, že v současně účinné právní úpravě⁶⁹ není definován ani pojem elektronický důkaz, resp. *elektronický důkazní prostředek*. Casey ve své publikaci uvádí že je můžeme definovat jako „*jakákoliv data ukládána či přenášena pomocí počítače, která podporují či vyvracejí domněnku o tom, jak k trestnému činu došlo, nebo která se týkají rozhodujících prvků trestného činu, jako je úmysl nebo nevinu*“⁷⁰. Mason však upozorňuje na skutečnost, že informační a komunikační technologie se neustále vyvíjí a je tedy obtížné stanovit definici tak, aby byla přílehavá.⁷¹ Za vhodný způsob, jak elektronické důkazní prostředky definovat, je odbornou veřejností⁷² považován popis jejich specifických znaků a vlastností. Hlavním společným znakem elektronických důkazních prostředků je, že informace v nich uchovávané jsou v podobě, jež je pro běžného člověka smysly obtížně vnímatelná, a pro jejich výklad je nutné využití dalšího elektronického zařízení, které tyto informace převede do podoby, která je již člověkem vnímatelná.⁷³ V této souvislosti můžeme uvést, že se jedná

⁶⁸ STUPKA, V., PROVAZNÍK, J., VOSTOUPAL J. *Elektronické důkazy jako výzva pro trestní proces*. 2022, Právník 4/2022, Ročník 161, s. 335

⁶⁹ Uzávěrka této diplomové práce je ke dni 7. 2. 2024

⁷⁰ CASEY, E., BRENNER, S. W., KOOPS, B., ROBINSON, T., SCHATZ, B. et al. *Digital evidence and computer crime: forensic science, computers and the internet*. Third edition. Amsterdam: Elsevier Academic Press, 2011. ISBN 978-0-12-374268-1. s. 7

⁷¹ MASON, S., SENG, D. *Electronic evidence*. Fourth edition. London: Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017. ISBN 1-911507-07-9. s. 18-20

⁷² KALVODOVÁ, V., ŠÁMAL, P. a HRUŠÁKOVÁ, M. *Dokazování v trestním řízení – právní, kriminologické a kriminalistické aspekty*. Op. cit. s. 312

⁷³ *Tamtéž*.

o „*důkazní prostředky, k jejichž převodu do podoby srozumitelné pro člověka je třeba použít elektronické zařízení.*“⁷⁴.

Obdobně nejsou v trestním řádu upraveny instituty a procesní postupy, jež by se vztahovaly výhradně k zajišťování elektronických důkazů. A to i přesto, že zákonodárce s pojmem *elektronický dokument* pracuje, srov. § 59 odst. 1, 2 trestního řádu (podání učiněné elektronicky), § 85b odst. 12 trestního řádu (listiny obsahující skutečnosti, na které se vztahuje povinnost mlčenlivosti advokáta), § 62 odst. 1 věta první trestního řádu (doručování do elektronického systému datových schránek). Trestní řád současně pracuje i s dalšími instituty mající *elektronickou povahu*, jako je např. pořízení obrazového či zvukového záznamu o prováděném úkonu jako zvláštního způsobu protokolace, v rámci odposlechů a záznamů telekomunikačního provozu, u operativně pátracích prostředků a využití zvukových, obrazových a jiných záznamů, nebo využití videokonferenčního zařízení při provádění úkonů v rámci trestního procesu.⁷⁵

Z důvodu existence velkého množství elektronických zařízení je velmi důležité, aby bylo pro získání důkazu zvoleno takové, jež nejlépe umožní získání veškerých (možných) informací v něm obsažených. V případě nezvolení vhodného zařízení nám mohou informace důležité pro dané trestní řízení uniknout, a to může mít bezesporu za následek ovlivnění výsledku dokazování.

Na příkladu paměťové karty použité ke zhotovení digitálních fotografií si můžeme ukázat množství informací, které získáme dle volby elektronického zařízení. Pokud bychom zvolili digitální fotoaparát, ukáže se nám fotografie jako taková, resp. její vizuální zobrazení, v případě modernějších zařízení i jistá metadata, např. čas vyhotovení fotografie nebo nastavení fotoaparátu v době pořízení fotografie. Taková fotografie však pravděpodobně bude obsahovat i další data, která fotoaparát nebude schopen interpretovat a jež mohou být z hlediska dokazování stěžejní. Snadněji představitelným případem bude CD obsahující hudební nahrávky. Za použití zařízení – hudebního CD přehrávače budeme schopni interpretovat pouze samotný audio záznam. Ostatní data nám však zůstanou skryta⁷⁶. Současně mohou na být CD uloženy i jiné datové stopy jako jsou fotografie, elektronické dokumenty či video záznamy, které jsou hudebním CD přehrávačem nečitelná. V neposlední řadě považuji za vhodné uvést

⁷⁴ KOČÍ, M. *Elektronické důkazní prostředky*. Diplomová práce. Brno: Masarykova univerzita, 2012

⁷⁵ POLČÁK, R., PÚRY, F., HARAŠTA, J., MYŠKA, M. a STUPKA, V. *Elektronické důkazy v trestním řízení*. Op. cit., s. 73

⁷⁶ Srov. Např. datum pořízení audio nahrávky, to zda byla audionahrávka dále upravena v jiné aplikaci, kdy došlo k jejímu umístění na CD apod.

jako příklad získávání důkazů z webové stránky, kde bude množství obsažených informací, jež mohou zůstat na základě volby interpretačního zařízení „skryté“, o poznání širší. Pokud bychom například vytiskli printscreen stránky, získáme pouze informace o jejím obsahu, který je vnímatelný pouhými smysly člověka (design stránky, grafika, fotografie a obsažený text). Budeme však ochuzeni o data jako je zdrojový kód stránky (v něm mohou být následně ukryty stěžejní informace, jako např. prostřednictvím jakého softwaru byl vytvořen, nebo kdo je tvůrcem)⁷⁷ a další důležitá metadata.

2.1. Rozdělení na kategorie

První kategorií, kterou je možné uvést, jsou *elektronické dokumenty, metadata a provozní data vytvořená aplikacemi*. Pro bližší charakteristiku je předmětné specifikovat, že informace do *elektronických dokumentů* jsou zaznamenávány člověkem, např. vytvořením digitální fotografie, audio či video záznamu, ale i prosté textové dokumenty apod. Za *metadata* označujeme informace, které obsahují další informace o výše uvedeném, tj. pomocí jakého programu byl dokument/fotografie vytvořena, kdo, kdy a kde jej vytvořil vč. informací přímo nesouvisejících s pořizovatelem jako jsou provozní a pomocná data (např. automaticky pořizované záznamy, logy). Tyto informace jsou přidány samotnou aplikací, ve které dochází k jejich vzniku.⁷⁸ Z logiky věci můžeme dojít k závěru, že data vytvořená automaticky aplikací budou oproti dokumentům vytvořeným uživatelem jako důkaz věrohodnější, jelikož je nelze snadno upravovat. Můžeme shrnout, že první kategorie dat tedy přímo obsahuje určité informace.

Druhou kategorií jsou *aplikace*, tj. data s určitou dynamikou v rámci počítačového systému, jež určují procesy systému, resp. „co“ a „jak“ má dělat.⁷⁹ Jedná se o informace zprostředkovávající tvorbu dat uvedených v první kategorii a interpretaci vytvořených dat do podoby vnímatelné smysly člověka.⁸⁰ Tyto však v současné době nejsou s ohledem na ustanovením § 89 odst. 1 trestního řádu předmětem dokazování, neboť jak plyne ze smyslu tohoto ustanovení, nespádají do vymezení „*nezbytného rozsahu*“, protože není předpokládána jejich následná editace.

⁷⁷ KALVODOVÁ, V., ŠÁMAL, P. a HRUŠÁKOVÁ, M. *Dokazování v trestním řízení – právní, kriminologické a kriminalistické aspekty*. Op. cit., s. 314

⁷⁸ *Tamtéž*, s. 312-313

⁷⁹ POLČÁK, R., PÚRY, F., HARAŠTA, J., MYŠKA, M. a STUPKA, V. *Elektronické důkazy v trestním řízení*. Op. cit., s. 96

⁸⁰ KALVODOVÁ, V., ŠÁMAL, P. a HRUŠÁKOVÁ, M. *Dokazování v trestním řízení – právní, kriminologické a kriminalistické aspekty*. Op. cit., s. 312-313

2.2. Procesní postupy zajišťování elektronických důkazních prostředků

Jak již bylo uvedeno na začátku této kapitoly, v současné právní úpravě, a to i přes množství novelizací, neexistují konkrétní procesní nástroje, které by byly určeny k zajišťování *elektronických důkazních prostředků*. Vycházíme z institutů zákonodárcem původně pro tyto důkazní prostředky nezamýšlených a z obecného ustanovení, dle kterého může v trestním řízení jako důkaz „*sloužit vše, co může přispět k objasnění věci*“⁸¹. V důsledku výše uvedeného však v praxi dochází při jejich zajišťování k vysoké nejednotnosti, vyplývající z nesourodého výběru konkrétního institutu, který je aplikován. Tento výběr navíc dle Kalvodové⁸² v mnoha případech nezávisí pouze na druhu důkazního prostředku, ale také na konkrétním vyšetřovateli a jeho praxi, v neposlední řadě je výběr institutu závislý i na osobě, od které je důkazní prostředek zajišťován.

Lze tedy shrnout, že *elektronické důkazní prostředky* lze opatřit ze strany orgánu činného v trestním řízení instituty či kombinací institutů upravených v trestním řádu, jelikož však zákonodárce při jejich tvorbě přímo nepočítal s jejich využitím pro elektronické důkazy, můžeme v mnoha případech mluvit o jejich nepřiléhavosti. Za vhodné považuji zmínit i fakt, že požadavky na ukotvení konkrétních procesních ustanovení týkajících se vyšetřování a zajišťování elektronických důkazních prostředků ukládá České republice i přijetí *Budapeštské úmluvy*, jež byla ze strany státu ratifikována již v roce 2013, tedy před více než 10 lety.

Polčák⁸³ uvádí hned několik procesních postupů, jichž je v praxi využíváno pro zajištění elektronických důkazních prostředků. Jsou jimi: *vydání a odnětí věci* (§ 78 a § 79 trestního řádu); *domovní prohlídky, prohlídky jiných prostor a pozemků a osobní prohlídky* (§ 82 - 85b trestního řádu); *odposlech a záznam telekomunikačního provozu* (§ 88 trestního řádu, vč. *přeshraničního odposlechu* (§ 64 ZMJS)); *vyžádání údajů o uskutečněném telekomunikačním provozu* (§ 88a trestního řádu), *ohledání* (§ 113 trestního řádu), *znalecký posudek a odborné vyjádření* (§ 105-111 trestního řádu) a operativně pátrací prostředek *sledování osob a věci* (§ 158d odst. 3 trestního řádu)

Považuji za nezbytné poukázat i na skutečnost, že shora uvedené zajišťování elektronických důkazních prostředků pomocí nepřiléhavých institutů je postupem „*v praxi*

⁸¹ § 89 odst. 2 trestního řádu

⁸² KALVODOVÁ, V., ŠÁMAL, P. a HRUŠÁKOVÁ, M. *Dokazování v trestním řízení – právní, kriminologické a kriminalistické aspekty*. Op. cit., s. 315

⁸³ POLČÁK, R. a kol. *Právo informačních technologií*. Praha: Wolters Kluwer ČR, 2018, 656 s., ISBN 978-80-7598-045-8. s. 572

*netestovaným a legislativně a judikatorně nezachyceným*⁸⁴. Z toho důvodu takto získaný důkaz může být v trestním řízení *nepoužitelným* (srov. nepřípustnost, neúčinnost),⁸⁵ resp. existuje zde mnohem vyšší riziko *nepřípustnosti*, než tomu bude u jiných důkazních prostředků, pro něž zákonodárce institut zamýšlel.

2.2.1. Zajištění zařízení a datových nosičů

Zajištění zařízení nebo datového nosiče (obsahujícího určitá data) je jedním ze způsobů, jehož prostřednictvím je možné zajistit důkazy pro trestní řízení.

Jednou z možností je využití ustanovení § 78 a § 79 trestního řádu o *vydání a odnětí věci*. Ten, kdo „*má u sebe věc, která může sloužit pro důkazní účely, je povinen ji na vyzvání předložit soudu, státnímu zástupci nebo policejnímu orgánu*“⁸⁶, jedná se o tzv. ediční povinnost, jejímž prostřednictvím je zajištění procesně snadné. Osoba, na kterou se bude ediční povinnost vztahovat, nemusí být výlučně vlastníkem, ale bude se jednat o kohokoliv, kdo má předmětnou věc u sebe, např. zaměstnavatel, poskytovatel služby či provozovatel serveru housingu. Věc může být i odňata, pokud osoba neuposlechne a předmětnou věc nevydá.⁸⁷

Určitým omezením *vydání a odnětí věci* je však ustanovení § 78 odst. 2 trestního řádu, které stanoví, že tímto způsobem nelze zajistit dokument, který obsahuje skutečnosti, o kterých platí zákaz výslechu (utajované informace dle zákona č. 412/2005 Sb.; data týkající se mlčenlivosti advokáta; osobní údaje apod.).⁸⁸ Okolnost, že datový nosič či zařízení může výše uvedené skutečnosti obsahovat však neznamená, že by nemohlo dojít k jejich zajištění, s ohledem na ustanovení § 2 odst. 5 trestního řádu. Shodně se vyjádřil i Ústavní soud, který konstatoval, že za splnění zákonných podmínek „*[...] lze jako věci důležité pro trestní řízení zajistit i výpočetní techniku a záznamová média, případně jejich kopie, i když existuje možnost, že zajištěné nosiče informací obsahují [...] i informace o skutečnostech, které se netýkají probíhajícího trestního řízení a ke kterým se váže státem uložená nebo uznaná povinnost mlčenlivosti.*“⁸⁹, je však nutné postupovat v souladu se zásadou přiměřenosti a zdrženlivosti.

Dalším způsobem zajištění zařízení či nosiče informací, jak již bylo nastíněno výše, je využití ustanovení § 82 - 85b trestního řádu o *domovní prohlídce* nebo *prohlídce jiných*

⁸⁴ *Tamtéž.*

⁸⁵ Blíže je k nepřípustnosti a neúčinnosti pojednáno v kapitole 1.3. této práce

⁸⁶ § 78 trestního řádu

⁸⁷ POLČÁK, R. a kol. *Právo informačních technologií*. Op. cit., s. 573

⁸⁸ POLČÁK, R., PÚRY, F., HARAŠTA, J., MYŠKA, M. a STUPKA, V. *Elektronické důkazy v trestním řízení*. Op. cit., s. 102

⁸⁹ Usnesení Ústavního soudu ze dne 28. 3. 2002, sp. zn. IV. ÚS 2/02

prostor. Rozhodnutí *sui generis* je oprávněn vydat předseda senátu či soudce na návrh státního zástupce v přípravném řízení. Aby došlo k náležitému zajištění a zaprotokolování, je vhodné, aby prohlídky probíhaly za přítomnosti vyškoleného vyšetřovatele či znalce.⁹⁰

Polčák uvádí, že zajišťování by mělo respektovat vlastnosti konkrétního zařízení, to by mělo být vypnuté a v případě, kdy je zajišťován samotný datový nosič, měl by být od zařízení odpojený. Takové důkazní prostředky se zaprotokolují a zapečetí do antistatického vaku. Je vhodné, aby byla zapečetěna všechna rozhraní zařízení nebo bylo zařízení ihned vloženo do vaku či boxu.⁹¹ Také se provádí kontrolní součet, tzv. *hash kód*, který zajistí neměnnost obsahu nosiče a současně tak důkaz o tom, že při zajišťování nedošlo k pozměnění dat ze strany třetí osoby.⁹² První přístup k datům uchovaným v zařízení by pak měl mít znalec. Složitější to však bude v případě, kdy je zařízení v provozu. Je zde riziko, že odpojením či vypnutím dojde nejen ke ztrátě dat, ale i přístupu k datům, jež jsou dostupná na vzdáleném úložišti, či k zašifrovaným datům. Před tím, než dojde k odpojení takového zařízení je nezbytné, aby došlo k *ohledání věci* dle ustanovení § 113 trestního řádu. Prostřednictvím *ohledání* dojde k ověření, zda existuje nějaká z možných překážek, jež by mohla bránit úspěšné forenzní analýze. K protokolu se pořizuje fotodokumentace či videozáznam a dochází ke stejnému postupu jako u odpojených zařízení. Je důležité, aby nedošlo ke smazání, úpravě či jiné kompromitaci dat a zajišťována byla celá zařízení, nikoliv pouze datová úložiště či bitové kopie, jelikož zpřístupnění může být na sebe vázáno.⁹³

U obou druhů institutů pro zajištění je nutné zohlednit okolnosti konkrétního případu. Orgány činné v trestním řízení musí vždy postupovat v souladu se zásadou *zdrženlivosti a přiměřenosti*. Ta však nesmí být v rozporu s požadavkem na efektivnost a bezpečnost zajištění dat a zařízení. Současně by při zajišťování měly být vždy přítomny osoby, které jsou k tomu speciálně vyškoleny, aby nedošlo ke znehodnocení důkazního materiálu.

Zásada přiměřenosti a zdrženlivosti nebyla respektována například při zajišťování důkazního materiálu v případě trestního řízení vedeného proti společnosti Mironet. Tato společnost byla v roce 2000 největším prodejcem počítačů online a nabízela počítače s operačním systémem na platformě Linux. Z důvodu údajného porušování autorských práv, prodejem kradeného softwaru, podala společnost Microsoft na Mironet u policejního orgánu

⁹⁰ POLČÁK, R., PÚRY, F., HARAŠTA, J., MYŠKA, M. a STUPKA, V. *Elektronické důkazy v trestním řízení*. Op. cit., s. 102

⁹¹ *Tamtéž.*, s. 103

⁹² *Tamtéž.*, s. 111, s.132

⁹³ *Tamtéž.* s. 103

trestní oznámení.⁹⁴ V rámci trestního stíhání bylo společnosti zajištěno veškeré počítačové vybavení, servery, data a účetnictví. Mironet tak díky tomuto velkému zásahu neměla možnost pokračovat ve svém podnikání a takřka zkrachovala. O dva roky později se navíc trestní stíhání ukázalo jako nezákonné a došlo k jeho zastavení. Jediné, co bylo nalezeno, byla demoverze programu Microsoft, a to pouze v jednom prodaném počítači.⁹⁵ Společnost však díky nepřiměřenosti zásahu, resp. nesprávnému postupu ze strany policejního orgánu, přišla o své postavení na trhu a požaduje⁹⁶ tak za ušlý zisk a znehodnocení společnosti od státu náhradu škody v řádu stovek milionů.

2.2.2. Získání přístupu ke vzdáleným datům

Tak jako je tomu u získávání elektronických důkazních prostředků skrze zajištění zařízení a datových nosičů, k získání dat ze vzdálených úložišť nebo služeb, lze využít několik možných institutů obsažených v trestním řádu. V tomto ohledu považuji za vhodné pro upřesnění nejprve rozdělit vzdálená data, resp. v síti získávané informace, na *volně dostupné* a *volně nedostupné*. Vedle toho je v této kapitole popsáno zvláštní postavení zajišťování *elektronické komunikace*, které se liší v závislosti na tom, zda se jedná o *data obsažená ve schránce*, tj. komunikaci v době zajišťování již uskutečněnou, či o *komunikaci probíhající v reálném čase* tzv. „do budoucna“.

U dat, jež jsou *volně dostupná* v síti, v případech, kde nedochází k překonávání žádného bezpečnostního opatření, je možné bez dalšího přistupovat k obsahu dostupnému na internetu a pořizovat z tohoto obsahu důkazní prostředky.⁹⁷ V rámci zajišťování důkazních prostředků je vycházeno z ustanovení § 112 trestního řádu, zejména je důležité, aby z tohoto procesního úkonu byl sepsán protokol. Ve světle vhodnosti volby prostředků, jež je podrobněji rozebrána výše, je důležité vždy vycházet z vlastností elektronických dat a dynamiky internetového prostředí. V tomto smyslu je tedy pro zajištění největšího možného množství důkazního

⁹⁴ POKORNÝ, M. *Mironet, který skoro zničila policejní razie, má nárok na odškodné od státu. Chce 626 milionů.* Aktuálně.cz [online]. 2017 [cit. 13. 12. 2023]. Dostupné z: <https://zpravy.aktualne.cz/domaci/mironet-ma-opet-sanci-na-stamilionove-odskodne-za-zatah-poli>

⁹⁵ ČT24. *Mironet se dál soudí se státem, odškodné za policejní zásah může přesáhnout miliardu* ČT24 [online]. 2017 [cit. 13. 12. 2023]. Dostupné z: <https://ct24.ceskatelevize.cz/clanek/ekonomika/mironet-se-dal-soudi-se-statem-odskodne-za-policejni-zasah-muze-presahnout-miliardu-100371>

⁹⁶ POKORNÝ, M. *Mironet, který skoro zničila policejní razie, má nárok na odškodné od státu. Chce 626 milionů.* Op., cit.

⁹⁷ POLČÁK, R., PÚRY, F., HARAŠTA, J., MYŠKA, M. a STUPKA, V. *Elektronické důkazy v trestním řízení.* Op. cit., s. 103

materiálu vhodné, mimo fotografií či printscreenů obrazovky, zajistit především zdrojový kód webové stránky.⁹⁸ Zajištění vhodné dokumentace je v tomto ohledu klíčové.

K datům v síti *volně nedostupným* lze získat přístup prostřednictvím přístupových údajů poskytnutých dobrovolně během výslechu, podání vysvětlení či jinak. Volně nedostupná data je nutné vykládat v tom smyslu, že se jedná o data zabezpečená, a tedy v souladu s ustanovením § 158d odst. 3 trestního zákoníku o operativním pátracím prostředku *sledování osob a věcí* je považovat za písemnosti a záznamy uchovávané v soukromí.⁹⁹ Do obsahu takových informací je možné ze strany orgánu činných v trestním řízení nahlížet, pokud s tím výslovně nesouhlasí ten, do jehož práv a svobod se zasahuje (tento souhlas lze však dodatečně odvolat), jen po předchozím písemném povolení soudce. Srov. náleží Ústavního soudu ve věci zjišťování ze sociálních sítí: „*Pokud orgány činné v trestním řízení [...] musí v nezbytně nutné míře přistoupit k určitému omezení základních lidských práv a svobod účastníků řízení (např. vazba, domovní prohlídka, odposlech a záznam telekomunikačního provozu), je jejich povinností postupovat striktně v souladu s trestním řádem a v jeho mantinelech, za maximálního šetření těchto práv.*“¹⁰⁰

Jsou-li přístupové údaje získávány v rámci trestního řízení *jiným způsobem*, tj. od osoby rozdílné od té, do jejichž práv má být zasahováno, nebo má dojít k překonání technického bezpečnostního opatření (např. jejich nalezením či získáním údajů uložených na zajištěném zařízení), jedná se o tak zásadní zásah do práv a svobod jedince, pro nějž zákon stanoví vysoké standardy kontroly.¹⁰¹ Jak již bylo uvedeno v odstavci výše, jedná se o nezbytný souhlas soudce ve smyslu ustanovení § 158d odst. 3 trestního zákoníku, který může být vydán na základě písemné žádosti. V případě, kdy věc nenese odkladu, lze k datům přistoupit i bez souhlasu, avšak musí být bezprostředně o takový souhlas požádáno. V případě, že do 48 hodin tento souhlas policejní orgán neobdrží, je jeho povinností takto získaná data zničit.¹⁰²

Aby získaná *volně dostupná* i *volně nedostupná* data mohla být v trestním řízení využita jako důkazní materiál, musí být o jejich zajištění vždy sepsán písemný protokol.¹⁰³

Dalším způsobem, jak získat přístup ke vzdáleným datům, jež jsou zabezpečená, tj. *volně nedostupná*, je pomocí zařízení, jež je způsobilé k přístupu, tzn. jsou v nich uchovány

⁹⁸ *Tamtéž*, s. 103-104

⁹⁹ POLČÁK, R. a kol. *Právo informačních technologií*. Op. cit., s. 575

¹⁰⁰ Nález Ústavního soudu ze dne 30. 10. 2014, sp. zn. III. ÚS 3844/13

¹⁰¹ POLČÁK, R. a kol. *Právo informačních technologií*. Op. cit., s. 576

¹⁰² § 158d odst. 3 trestního řádu

¹⁰³ POLČÁK, R. a kol. *Právo informačních technologií*. Op. cit., s. 575

přístupové údaje ke službě či jsou ke službě připojeny (prostřednictvím nainstalovaného účtu uživatele, cookies prohlížeče apod). Jedná se zejména o mobilní telefony, tablety, chytré hodinky, počítače, notebooky či další zařízení. Vzhledem k okolnosti, že jsou přístupové údaje uchovávány na zajištěném zařízení, tzn. data jsou získávána *jiným způsobem*, postupuje se i v této situaci dle ustanovení § 158d trestního zákoníku.¹⁰⁴ Vzhledem k tomu, jak je vykládán počítačový systém: „*zařízení anebo skupina vzájemně propojených nebo přidružených zařízení, z nichž jedno nebo více provádí na základě programu automatické zpracování dat [...] i data uložená, zpracovaná, opětovně vyhledaná nebo přenesená tímto zařízením anebo skupinou zařízení za účelem jeho nebo jejich provozu, použití, ochrany a údržby.*“¹⁰⁵, tedy jako synonymum pro počítač, mohl by být obsah (služby či cloudové úložiště) vzájemně propojených zařízení chápán jako součást počítačového systému. Přístup k datům na nich uložených, by tak byl umožněn bez dalšího souhlasu, resp. povolení soudce, a to na základě ustanovení § 78-79, § 82 nebo § 113 trestního zákoníku. S tímto širokým výkladem se však neztotožňuje Polčák, když uvádí: „*[...]přístup ke vzdálené službě připojené k zajištěnému zařízení doporučujeme realizovat teprve na základě souhlasu soudce [...], neboť nepochybně jde o samostatný přístup do soukromého virtuálního prostoru.*“¹⁰⁶.

Data, jež jsou předmětem *elektronické komunikace* a jsou uchovávána na vzdáleném zabezpečeném úložišti či službě, tj. e-mail, komunikační/chatovací služby (srov. Facebook, Messenger, Whatsapp, Instagram apod.), mají, jak bylo nastíněno v úvodu této podkapitoly, zvláštní postavení. V souladu s výkladovým stanoviskem NSZ č. 1/2015 rozlišujeme zajištění *komunikace probíhající v reálném čase* od *zajištění dat obsažených ve schránkách*, tj. komunikaci k okamžiku zajištění již uskutečněnou.

Dle výše uvedeného stanoviska je pro případ *probíhající komunikace*, která je obdobně jako telekomunikační provoz uskutečňována v sítích elektronických komunikací a současně obsahuje data, nutné využít ustanovení § 88 odst. 1 trestního řádu, tj. *odposlech a záznam telekomunikačního provozu*. Jednorázové zajištění *dat obsažených ve schránkách*, je dle výkladového stanoviska provedeno pomocí ustanovení § 158d odst. 3 trestního řádu, tj. operativně pátrací prostředek *sledování osob a věcí*. Využití tohoto institutu uvádí zmíněné

¹⁰⁴ POLČÁK, R., PÚRY, F., HARAŠTA, J., MYŠKA, M. a SUPKA, V. *Elektronické důkazy v trestním řízení*. Op. cit., s. 104-105

¹⁰⁵ GŘIVNA, T., DVOŘÁK, M. § 136a [Počítačový systém]. In: ŠÁMAL, P. a kol. *Trestní zákoník*. 3. vydání. Praha: C. H. Beck, 2023, s. 1827.

¹⁰⁶ POLČÁK, R., PÚRY, F., HARAŠTA, J., MYŠKA, M. a STUPKA, V. *Elektronické důkazy v trestním řízení*. Op. cit., s. 105

výkladové stanovisko jako jediné vhodné, a to z toho důvodu, že data, jež jsou jeho prostřednictvím zajišťována, mají povahu *dat uchovávaných v soukromí*.¹⁰⁷

V závěru je s ohledem na to, že většina služeb dnes nabízí obě možné funkce, tedy jak funkci *komunikačního prostředku*, tak i funkci *úložiště*, vhodné shrnout nezbytnost správné volby prostředku pro zajištění dat. Bude tomu tak například u zajištění komunikace na sociální síti Messenger spadající pod platformu Meta. Orgán činný v trestním řízení při prvním přístupu do služby Messenger zajistí data, jež jsou na platformě přítomná již v době zajištění, a to za pomoci operativně pátracího prostředku dle ustanovení § 158d odst. 3 trestního řádu. V případě, že v konkrétní věci existuje zájem i na následném zajišťování dat, resp. komunikace, která bude teprve uskutečněna v budoucnu, je pro toto zajištění nutné využít institutu odposlechu a záznamu telekomunikačního provozu dle ustanovení § 88 trestního řádu.

2.2.3. Získání dat od ISP

Data mohou orgány činné v trestním řízení získat také přímo od poskytovatelů informačních služeb. V první řadě musíme odlišit, jaký je charakter poskytovatele, od kterého jsou data žádána. Zda se jedná o *poskytovatele telekomunikačních služeb* ve smyslu zákona č. 127/2005 Sb., o elektronických komunikacích, nebo zda jde o *poskytovatele služeb informační společnosti* ve smyslu zákona č. 480/2004 Sb., o některých službách informační společnosti. Dalším aspektem je *charakter zajišťovaných dat*. Ten je nutné zohlednit zejména s ohledem na různou míru ochrany a v návaznosti na to i volbu procesních nástrojů, jež budou pro zajištění využity.¹⁰⁸ Využití tohoto postupu bude připadat zejména v úvahu, nebyl-li udělen souhlas oprávněných osob¹⁰⁹ a příslušná data nemohla být získána jiným způsobem¹¹⁰.

2.2.3.1. Charakter poskytovatele

Ve smyslu zákona o elektronických komunikacích je *poskytovatelem telekomunikačních služeb* myšlen podnikatel, tj. právnická nebo fyzická osoba, která poskytuje veřejnosti telekomunikační služby nebo telekomunikační síť. To znamená, že jde o subjekty, které zajišťují infrastrukturu veřejné komunikační sítě či připojení k ní.¹¹¹ V souladu s právní

¹⁰⁷ Výkladové stanovisko NSZ č. 1/2015

¹⁰⁸ POLČÁK, R., PÚRY, F., HARAŠTA, J., MYŠKA, M. a STUPKA, V. *Elektronické důkazy v trestním řízení*. Op. cit., s. 106-107

¹⁰⁹ Například udělením zákonem předvídaného souhlasu s poskytnutím dat ve smyslu ustanovení § 158d odst. 6 trestního řádu.

¹¹⁰ Viz v podkapitolách výše.

¹¹¹ POLČÁK, R., PÚRY, F., HARAŠTA, J., MYŠKA, M. a STUPKA, V. *Elektronické důkazy v trestním řízení*. Op. cit., s. 107

úpravou je poskytovatel telekomunikačních služeb povinen splňovat určité právní a technické požadavky, jakými jsou např. registrace u příslušného regulačního orgánu, dodržování standardů pro kvalitu služeb a ochranu osobních, provozních a lokalizačních údajů a důvěrnost komunikací (srov. § 88 a § 89 zákona o elektronických komunikacích). V tomto smyslu jsou poskytovatelé zejména povinni nepřipustit odposlech, zachycení, ukládání či jiné sledování zpráv a s nimi souvisejících údajů osobami, jež jsou rozdílné od uživatelů, a to bez souhlasu těchto dotčených uživatelů, nestanoví-li zákon¹¹² jinak. V souladu s ustanovením § 88 zákona o elektronických komunikacích tím však není dotčeno technické ukládání údajů nezbytné pro přenos zpráv.¹¹³ Zákon ve svém ustanovení § 1 upravuje i výčet obsahu služeb poskytovaných pomocí sítí elektronických komunikací, na něž se právní úprava nevztahuje, jedná se o: „[...] obsah rozhlasového a televizního vysílání, finančních služeb a některých služeb informační společnosti, není-li dále stanoveno jinak.“¹¹⁴

Naproti tomu *poskytovatelem služeb informační společnosti* je myšlen subjekt, jež prostřednictvím sítě elektronických komunikací poskytuje jakoukoliv (zpravidla úplatnou) službu, a to na individuální žádost uživatele podanou elektronickými prostředky. Jedná se o různé online služby. Příkladem si můžeme uvést služby jako jsou vyhledávače, poskytování e-mailových služeb, sociální platformy, e-commerce, další online informační a zábavní služby vč. diskusních serverů, poskytování cloudových služeb, filehosting, a další.¹¹⁵ Zákon o některých službách informační společnosti reguluje tyto poskytovatele zejména v oblasti odpovědnosti či šíření obchodních sdělení.¹¹⁶

Rozdíl mezi charakterem uvedených poskytovatelů tedy spočívá v tom, že *poskyvatelé telekomunikačních služeb* se primárně zaměřují na infrastrukturu a přenos dat, zatímco *poskyvatelé informační společnosti* se soustředí na obsah a služby poskytované prostřednictvím infrastruktury.

2.2.3.2. Charakter zajišťovaných dat

K vyžádání dat, jejichž obsahem *nejsou* informace, které podléhají povinnosti mlčenlivosti, postačí využití ustanovení § 8 odst. 1 trestního řádu, které stanoví: „*Státní orgány, právnické a fyzické osoby jsou povinny bez zbytečného odkladu [...] vyhovovat dožádáním*

¹¹² Tím je např. ustanovení § 88 trestního řádu

¹¹³ § 88an. zákona o elektronických komunikacích

¹¹⁴ § 1 zákona o elektronických komunikacích

¹¹⁵ POLČÁK, R. a kol. *Právo informačních technologií*. Op. cit., s. 577

¹¹⁶ § 3an. zákona o některých službách informační společnosti

*orgánů činných v trestním řízení při plnění jejich úkolů.*¹¹⁷ Takto mohou být získána např. obsahová data, data zveřejněná uživatelem, logy zaznamenávané poskytovatelem, jež nepodléhají telekomunikačnímu tajemství, informace související s uživatelskými účty či o fungování služby a metadata. V neposlední řadě mohou být tímto způsobem zajištěna i data podobná provozním a lokalizačním údajům, která nejsou dožadována od *poskytovatele telekomunikačních služeb* dle zákona o elektronických komunikacích. Obsahem těchto dat však nesmí být žádné osobní údaje či utajované informace dle zvláštního zákona (v tomto případě musí jejich poskytnutí povinná osoba odmítnout).¹¹⁸

Data mající charakter *záznamů uchovávaných v soukromí* jsou bez dalšího ta, která jsou uživatelem u poskytovatele služby uchovávána pod bezpečnostním opatřením, jakým může být např. uživatelské jméno a heslo. V případě vyžádání dat tohoto charakteru je nutné, aby orgány činné v trestním řízení postupovaly v souladu s ustanovením upravující sledování osob a věcí, srov. § 158d odst. 3 trestního řádu.¹¹⁹

Provozní a lokalizační údaje ve smyslu ustanovení § 90 a § 91 zákona o elektronických komunikacích mají zvláštní postavení, jelikož se jedná o údaje, které jsou poskytovateli zpracovávána pro potřeby přenosu zprávy sítí elektronických komunikací nebo pro její účtování, a údaje, které určují zeměpisnou polohu telekomunikačního zařízení uživatele. Poskytovateli plyne povinnost tyto údaje uchovávat po dobu určenou zákonem. K jejich zajištění je možné využít ustanovení § 88a trestního řádu, avšak to je možné využít jen v případech, týká-li se stíhání úmyslných trestných činů se stanovením horní hranice trestu odnětí svobody nejméně v délce 3 let, nebo u vyjmenovaných trestných činů, vždy za současné podmínky, že sledovaného účelu nelze dosáhnout jinak či by bylo jeho dosažení značně ztíženo. Zákonodárce touto omezující podmínkou (subsidiarity použití) odkazuje na základní zásady trestního procesu, kterými jsou zásada přiměřenosti a zdrženlivosti.¹²⁰

Zvláštní postavení mají i *obsahová data komunikovaná prostřednictvím sítí elektronických komunikací*, na něž se vztahuje telekomunikační tajemství.¹²¹ V souladu s výkladovým stanoviskem NSZ č. 1/2015 je nutno postupovat do budoucna, a tedy zajišťování je možné pouze za podmínek odposlechu a záznamu telekomunikačního provozu dle ustanovení

¹¹⁷ § 8 trestního řádu

¹¹⁸ POLČÁK, R., PŮRY, F., HARAŠTA, J., MYŠKA, M. a STUPKA, V. *Elektronické důkazy v trestním řízení*. Op. cit., s. 107

¹¹⁹ POLČÁK, R. a kol. *Právo informačních technologií*. Op. cit., s. 578

¹²⁰ POLČÁK, R., PŮRY, F., HARAŠTA, J., MYŠKA, M. a STUPKA, V. *Elektronické důkazy v trestním řízení*. Op. cit., s. 108

¹²¹ POLČÁK, R. a kol. *Právo informačních technologií*. Op. cit., s. 578

§ 88 trestního řádu. I v tomto případě je možné využít institutu¹²² pouze za předpokladu, že se jedná o jeden z taxativně vymezených trestných činů (trestní sazbou, jednotlivě vyjmenovaných či stanovených na základě vyhlášené mezinárodní smlouvy), pro který zákon odposlech umožňuje.

2.3. Jednotlivé procesní instituty zajištění

V aktuální právní úpravě nenalezneme procesní instituty vztahující se přímo k zajišťování *elektronických důkazů*¹²³, současně nelze ani jednotlivá ustanovení trestního řádu podřadit pod jednotlivé procesní postupy, které byly charakterizovány v předešlé kapitole. Ačkoliv uvedená ustanovení trestního řádu nebyla zákonodárcem původně určena pro jejich aplikaci při získávání elektronických důkazů¹²⁴, shledávám za více než příhodné charakterizovat použití jednotlivých vybraných institutů speciálně v kontextu zajišťování či jiného nakládání s digitálními stopami, které se opírá zejména o metodické pokyny NSZ¹²⁵ a dosavadní judikaturu. Některé instituty, na rozdíl od jiných, považuji za vhodné charakterizovat více do hloubky, z toho důvodu není všem procesním institutům věnován stejný rozsah.

2.3.1. Odposlech a záznam telekomunikačního provozu

Nařízením¹²⁶ odposlechu a záznamu telekomunikačního provozu dle ustanovení § 88 trestního řádu dochází k prolomení jednoho ze základních lidských práv chráněných článkem 13 Listiny: „*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.*“¹²⁷ Jak je uvedeno i v komentářové literatuře¹²⁸, je nezbytné, aby byl smysl tohoto článku vykládán ve vztahu

¹²² § 88 trestního řádu

¹²³ Viz výše

¹²⁴ Netýká se ustanovení § 7b trestního řádu.

¹²⁵ Výkladové stanovisko NSZ č. 4/2005 a výkladové stanovisko NSZ č. 1/2015

¹²⁶ Odposlech a záznam telekomunikačního provozu je dle ustanovení § 88 odst. 2 trestního řádu oprávněn nařídít předseda senátu a v rámci přípravného řízení na návrh státního zástupce soudce. Dle ustanovení § 88 odst. 5 trestního řádu je možno, aby byl odposlech a záznam telekomunikačního provozu nařízen orgánem činným v trestním řízení bez příkazu, nebo jím byl proveden sám, a to za splnění podmínky, že s tím a) uživatel odposlouchávané stanice souhlasí nebo b) vede-li se trestní stíhání pro některý z trestných činů uvedených v tomto ustanovení, srov. § 168, § 169, § 171, § 200, § 352, § 353, § 354 trestního zákoníku.

¹²⁷ Čl. 13 Listiny

¹²⁸ KOKEŠ, M. Čl. 13 [Ochrana důvěrnosti komunikace]. In: HUSSEINI, F., BARTOŇ, M., KOKEŠ, M., KOPA, M. a kol. *Listina základních práv a svobod*. 1. vydání (1. aktualizace). Praha: C. H. Beck, 2021, marg. č. 1–2

k nástupu dalších komunikačních prostředků, jako jsou např. sociální sítě, mobilní telefony či jiná elektronická komunikace, šířeji a aplikovat ho s v souladu s technologickým vývojem i na tyto nové prostředky, jež bezesporu obsahují *důvěrnou komunikaci*.

Nejedná se však pouze o národní úpravu, na kterou je nutné nahlížet světle nových technologií, ale i na nadnárodní legislativu týkající se ochrany základních lidských práv. V této souvislosti konkrétně na článek 8 Evropské úmluvy. Ten ve své textaci zmiňuje ještě užší pojem, a to *korespondence*. Judikaturou ze strany Evropského soudu pro lidská práva je však dále rozvíjen na ochranu „*důvěrnosti soukromé komunikace, prováděné (fyzickými či právníckými osobami) prostřednictvím široké palety komunikačních prostředků*“¹²⁹. Velmi pestrá judikatura v této souvislosti pojem vykládá v šíři¹³⁰ dopisů, telefonických hovorů, odposlechů prováděných veřejnou mocí včetně údajů o telekomunikačním provozu,¹³¹ emailové komunikace¹³², používání webových stránek, nebo korespondence uložené v počítačích či na sdílených serverech a zařízeních¹³³. Vzhledem k tomu, že se jedná o významný zásah do soukromí osoby, jsou pro jeho umožnění stanoveny trestním řádem velmi přísné požadavky.

Ústavní soud se otázkou přípustnosti zásahu veřejné moci do práva na *důvěrnost komunikace* ve smyslu užití odposlechů zabýval hned několikrát. Opakovaně¹³⁴ se přitom vyslovil, že je nutné, aby pro vydání soudního příkazu byly splněny náležitosti, za kterých je to umožněno: „*jen v řádně zahájeném trestním řízení pro zákonem kvalifikovanou trestnou činnost, a musí být podložen relevantními indiciemi, z nichž lze dovodit důvodné podezření ze spáchání takového trestného činu. Příkaz musí být individualizován ve vztahu ke konkrétní osobě, která je uživatelem telefonní stanice. Konečně musí příkaz alespoň v minimální míře konkrétně uvést, jaké skutečnosti významné pro trestní řízení mají být takto zjištěny, a z čeho je to vyvozováno.*“¹³⁵. Kromě toho, že k užití tohoto institutu se musí přistupovat

¹²⁹ *Tamtéž*, marg. č. 5

¹³⁰ Zejména, nikoliv výlučně. Jedná se o příkladný, pro práci relevantní, výčet.

¹³¹ Srov. ESLP 12433/86, *Lüdi proti Švýcarsku*; ESLP 9248/81, *Klass a další proti Německu*; ESLP 23224/94, *Kopp proti Švýcarsku*; ESLP 5935/02, *Heglas proti ČR*; ESLP 44787/98, *P. G. a J. H. proti Spojenému království*; ESLP 27798/95, *Amman proti Švýcarsku*

¹³² Srov. ESLP 61496/08, *Bărbulescu proti Rumunsku*

¹³³ Srov. ESLP 74336/01, *Wieser a Bicos Beteiligungen GmbH proti Rakousku*; ESLP 50882/99, *Petri Sallinen a další proti Finsku*; ESLP 65755/01, *Iliya Stefanov proti Bulharsku*

¹³⁴ Srov. Nález Ústavního soudu ze dne 23. 5. 2007, sp. zn. II. ÚS 615/06; Nález Ústavního soudu ze dne 29. 2. 2008, sp. zn. I. ÚS 3038/07

¹³⁵ KOKEŠ, M. Čl. 13 [Ochrana důvěrnosti komunikace]. In: HUSSEINI, F., BARTOŇ, M., KOKEŠ, M., KOPA, M. a kol. *Listina základních práv a svobod*. Op. cit. marg. č. 15

až subsidiárně,¹³⁶ tj. nelze-li k vyšetřování trestné činnosti užít méně invazivního způsobu,¹³⁷ jsou k nařízení odposlechu a jeho následné procesní použitelnosti v trestním řízení nutné následující předpoklady:

- a. užití odposlechu pouze pro omezený okruh trestných činů, u jejichž vyšetřování může být jeho užití nařízeno:
 - i. zločiny¹³⁸ s horní hranicí trestní sazby nejméně 8 let stanovenou zákonem u příslušné skutkové podstaty;
 - ii. taxativně vyjmenované trestné činy¹³⁹; nebo
 - iii. jiné úmyslné trestné činy, k jejichž stíhání je Česká republika zavázána na základě vyhlášené mezinárodní smlouvy¹⁴⁰
- b. soulad se zákonnými náležitostmi, resp. podmínkami vydání příkazu k odposlechu,¹⁴¹ vč. maximální doby trvání¹⁴² a průběžného vyhodnocování, zda důvody pro nařízení trvají
- c. připojení protokolu o záznamu.¹⁴³

Nadto je potřebné uvést, že pokud v rámci odposlechu bude zjištěno, že probíhá *komunikace mezi obviněným a jeho obhájcem*, je nutné, aby policejní orgán pro jeho nepřipustnost ihned takový záznam zničil a informace, jež se dozvěděl, nikde nepoužil. O jeho zničení se pořídí protokol. Tato nepřipustnost odposlechu vyplývá přímo z ustanovení § 88 odst. 1 trestního řádu. Ještě dále jde v tomto ohledu Gřivna, dle kterého: „*Ochrana důvěrné komunikace není vázána na okamžik zahájení trestního stíhání. Je širší. Pokrývá nejméně celé trestní řízení a patrně i dobu před jeho zahájením (dovozeno z povinné mlčenlivosti advokáta a zákazu jeho výslechu o skutečnostech, které se dozvěděl v souvislosti s poskytováním právních*

¹³⁶ Nelze-li účelu dosáhnout jiným způsobem, či by jinak jeho dosažení bylo podstatně ztíženo. Srov. § 88 odst. 1 trestního řádu

¹³⁷ Srov. Usnesení Nejvyššího soudu ze dne 15. 11. 2016, sp. zn. 4 Pzo 14/2016

¹³⁸ Srov. § 13 odst. 2 trestního zákoníku

¹³⁹ Jedná se o trestné činy upravené v ustanovení § 226, § 248 odst. 1 e) a odst. 2-4, § 256, § 257, § 258 trestního zákoníku.

¹⁴⁰ Na tomto základě je možné povolit odposlech např. při stíhání drogových trestných činů.

¹⁴¹ Příkaz musí obsahovat účel odposlechu; uživatelskou adresu/zařízení a jeho uživatel, pokud je totožnost uživatele známa; doba, po kterou je odposlech nařízen (ta nesmí být delší než 4 měsíce); a zejména konkrétní skutkové okolnosti, jež odůvodňují použití předmětného institutu (odůvodněna musí být i doba). Srov. ustanovení § 88 odst. 1 až odst. 4 trestního řádu.

¹⁴² Pokud se to dle dosavadního odposlechu jeví za vhodné a pro vyšetřování nezbytné, je možné tuto dobu prodloužit, a to až o 4 měsíce, i opakovaně. O prodloužení rozhoduje soudce vyššího soudu. U přípravného řízení pak na návrh státního zástupce krajský soud. Srov. ustanovení § 88 trestního řádu.

¹⁴³ Pro užití záznamu telekomunikačního provozu jako důkazu v trestním řízení je nezbytné připojit k němu protokol splňující podmínky stanovené ustanovením § 88 odst. 6 trestního řádu. Srov. ŠÁMAL, P., RŮŽIČKA, M. § 88 [Důvody nařízení a postup]. In: ŠÁMAL, P. a kol. *Trestní řád*. Op. cit., s. 1212

služeb).¹⁴⁴ V tomto smyslu se vyjádřili i jiní odborníci¹⁴⁵. Je vytýkáno, že ochrana důvěrné komunikace by měla být v tomto smyslu vykládána extenzivně a nepřipustnost odposlechu by měla zahrnovat i komunikaci mezi obhájcem a podezřelým¹⁴⁶. Dle komentářové literatury a dosavadní rozhodovací praxe Ústavního soudu¹⁴⁷ je však ochrana důvěrné komunikace mezi obhájcem a osobou, již udílí své právní rady, vázána až na okamžik, ke kterému je proti ní zahájeno trestní stíhání.

Ve světle výše uvedeného považují také za důležité poukázat na *nepřipustnost nahodilého použití odposlechu* na získávání informací, resp. aby až nařízeným odposlechem bylo získáno podezření, zda se osoba, jejíž odposlech byl nařízen, dopustila nějaké trestné činnosti. V tomto smyslu se vyjádřil Ústavní soud následovně: „*Z hlediska ústavně chráněných základních práv je nepřipustné, aby zahájení úkonů k objasňování a prověřování skutečností důvodně nasvědčujících tomu, že byl spáchán trestný čin podle § 158 odst. 3 trestního řádu, např. ve formě odposlechů, bylo zneužíváno jako prostředku k teprve dodatečnému opatřování podkladů pro tento postup, tj. samotné důvodnosti podezření.*“¹⁴⁸.

Shora uvedené však nebrání tomu, aby byl odposlech, který byl nařízen v souladu se zákonem použit i v *jiné věci*.¹⁴⁹ Podmínkou takového užití je, aby pro trestný čin, o jehož trestní stíhání se jedná, mohl být v souladu s ustanovením § 88 odst. 1 trestního řádu, odposlech nařízen. Zjednodušeně řečeno, musí se jednat o některý z limitovaného okruhu trestných činů, pro který to zákon umožňuje. V opačném případě je užití odposlechu pro objasnění jiné věci vyloučeno.

Každoročně je ze strany Policejního prezidia České republiky Úřadem služby kriminální policie a vyšetřování zpracovávána analýza¹⁵⁰ týkající se mj. i odposlechů a záznamu telekomunikačního provozu. Pro účely této diplomové práce považují za přínosné uvést, jaký podíl při nařízení odposlechů tvoří jednotlivé druhy trestné činnosti.

¹⁴⁴ GŘIVNA, T. *Právo na zachování důvěrné komunikace mezi advokátem a jeho klientem*. Bulletin Advokacie. 2017, č. 6, s. 61–66

¹⁴⁵ VANTUCH, P. *Nezákonný odposlech advokáta*. Bulletin advokacie. 2008, č. 3, s. 15–24

¹⁴⁶ Osoba podezřelá ze spáchání trestného činu, proti které doposud nebylo zahájeno trestní stíhání ve smyslu ustanovení § 76 trestního řádu.

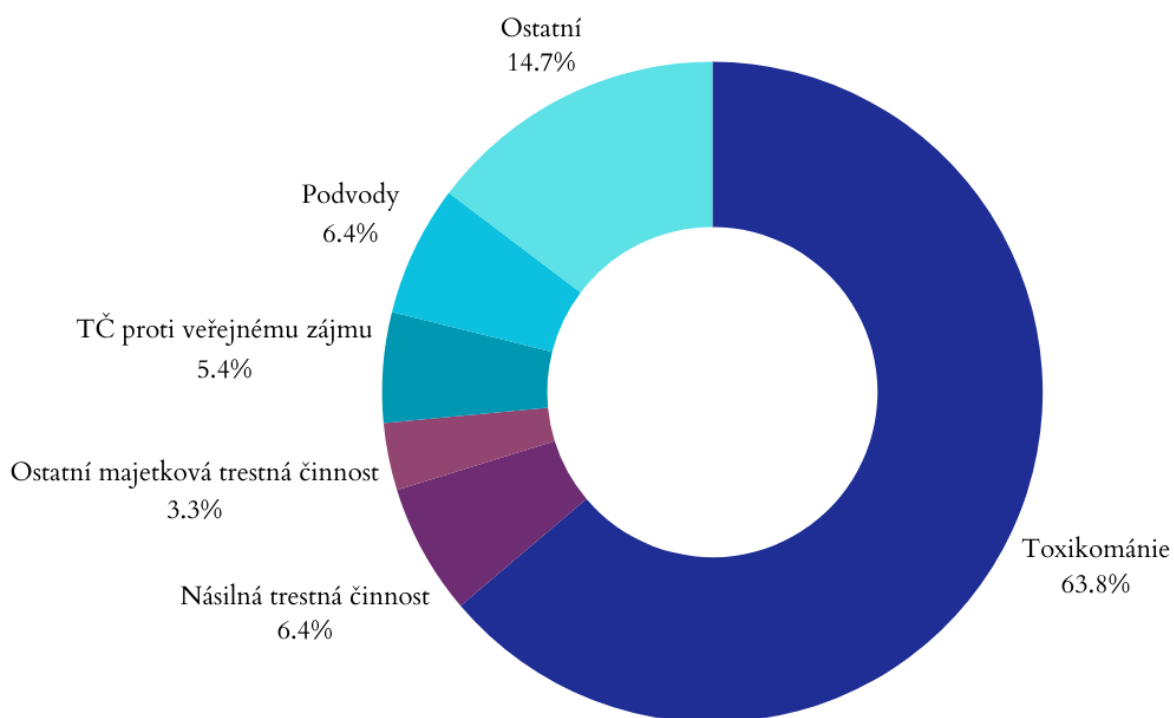
¹⁴⁷ Usnesení Ústavního soudu ze dne 12. 11. 2014, sp. zn. I. ÚS 1638/14

¹⁴⁸ Nález Ústavního soudu ze dne 27. 9. 2007 sp. zn. II.ÚS 789/06

¹⁴⁹ Srov. ustanovení § 88 odst. 6 věta třetí trestního řádu

¹⁵⁰ Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR za rok 2022, [online], [cit. 7. 1. 2024]. Dostupné z: <https://www.mvcr.cz/clanek/odposlechy-zaznamy-telekomunikacniho-provozu-a-sledovani-osob.aspx>

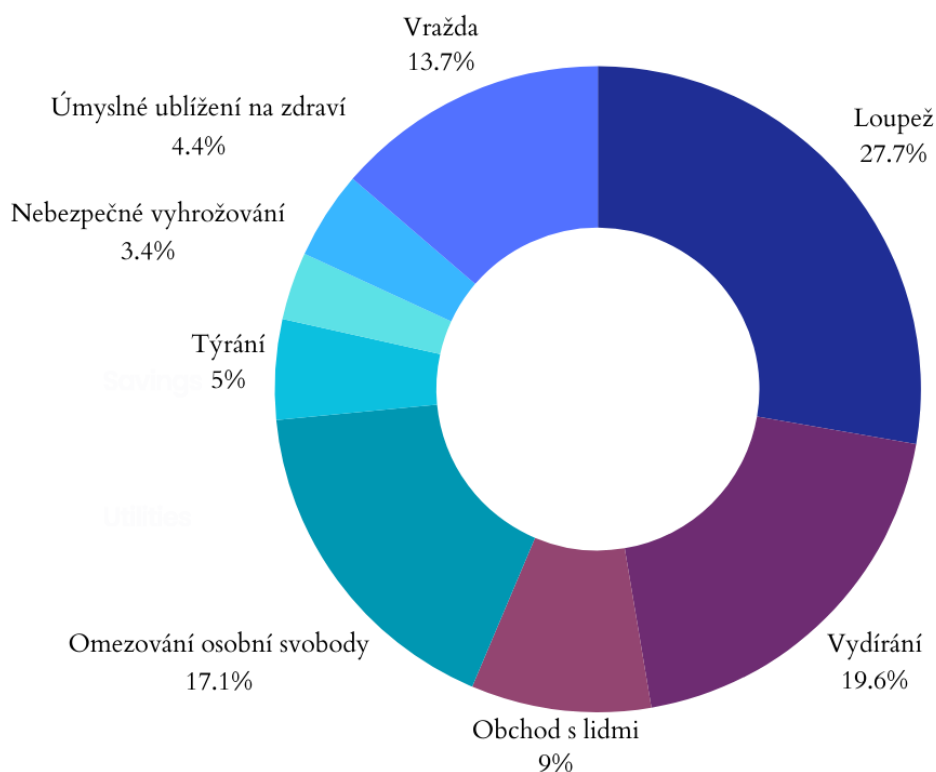
Nejaktuálnější uveřejněná analýza za rok 2022¹⁵¹ uvádí, že nejčastěji (v 63,8 %) byly odposlechy použity v souvislosti s toxikománií (celkem v 2983 případech). Naproti tomu ostatní trestná činnost, v souvislosti, se kterou došlo k nasazení odposlechů, tvoří jen jednotky procent. Nejvyšší podíl představuje násilná trestná činnost a podvody (v obou případech se jedná o 300 případů) a trestná činnost páchaná proti veřejnému zájmu (celkem 251 případů). Zbylá procenta tvoří od nejvyššího podílu: ostatní majetková trestná činnost, trestné činy proti hospodářské kázni, daňová trestná činnost, mravnostní trestná činnost, krádeže, trestné činy proti měně, krádeže vloupáním a porušení nehmotných práv a nekalá soutěž. V rámci násilné trestné činnosti byly odposlechy nasazeny ve 27,7 % případů u loupeží, podíl 19,6 % představovaly trestné činy vydírání a v 17,1 % se odposlechy týkaly omezování osobní svobody.



Graf 1: Podíl jednotlivých druhů trestné činnosti, pro které byl nařízen odposlech a záznam telekomunikačního provozu v roce 2022¹⁵²

¹⁵¹ Zpracování a uveřejnění analýzy bylo k 6. říjnu 2023.

¹⁵² Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR za rok 2022. Op. cit.



Graf 2: Podíl jednotlivých typů násilné trestné činnosti, pro které byl nařízen odposlech a záznam telekomunikačního provozu v roce 2022 z celkem 300 úkonů¹⁵³

Jak již bylo uvedeno v kapitole 2.2.3., ustanovení § 88 trestního řádu je v rámci zajišťování datových stop významné pro zajišťování komunikace *pro futuro*. Při zajištění datového nosiče např. v rámci ustanovení § 82 an. trestního řádu o domovní prohlídce, může policejní orgán postupovat bez toho, aniž by bylo třeba příkazu soudce.¹⁵⁴ Takový postup je však vzhledem k výše diskutované důvěrnosti komunikace, resp. telekomunikačnímu tajemství, vyloučen v okamžiku, kdy na datový nosič začnou přicházet zprávy, se kterými se vlastník datového nosiče v době zajištění neměl možnost seznámit.¹⁵⁵ Pokud tedy policejní orgán bude chtít zajišťovat obsah komunikace probíhající *v reálném čase*, je nutné dodržet podmínky stanovené ustanovením § 88 o odposlechu a záznamu telekomunikačního provozu, které v souladu s ochranou základních práv člověka klade na jeho povolení poměrně přísné podmínky.

¹⁵³ Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR za rok 2022. Op. cit.

¹⁵⁴ Výkladové stanovisko NSZ č. 4/2005

¹⁵⁵ Výkladové stanovisko NSZ č. 1/2015

V závěru je vhodné zmínit, že zákonodárce na příslušný orgán, po pravomocném skončení věci, klade informační povinnost vůči osobě, která byla na základě ustanovení § 88 trestního řádu odposlouchávána. S tím souvisí i právo na možnost obrany v podobě přezkumu zákonnosti vydaného příkazu Nejvyšším soudem. Nutné je však zdůraznit, že ustanovení z této informační povinnosti zakládá výjimky.¹⁵⁶

2.3.2. Zjišťování údajů o uskutečněném telekomunikačním provozu

Na rozdíl od ustanovení § 88 trestního řádu charakterizovaného výše, které pomáhá orgánům činným v trestním řízení k zajištění obsahu komunikace, ustanovení § 88a trestního řádu slouží k zjišťování provozních¹⁵⁷ a lokalizačních¹⁵⁸ údajů souvisejícími s provedeným komunikačním provozem.¹⁵⁹ Těmi se rozumí „zejména údaje vedoucí k dohledání a identifikaci zdroje a adresáta komunikace a dále údaje vedoucí ke zjištění data, času, způsobu a doby trvání komunikace“,¹⁶⁰ lze díky nim tak zjistit např. polohu zařízení v době, kdy byla uskutečněna komunikace.

Podobně jako je tomu v případě ustanovení o odposlechu¹⁶¹, jsou i pro vydání příkazu ve smyslu ustanovení § 88a trestního řádu zákonodárcem kladena poměrně přísná kritéria. Předně je třeba zdůraznit, že je vycházeno zejména z článku 13 Listiny, jež „nezakládá pouze ochranu tajemství vlastního obsahu telefonických zpráv, ale i dalších údajů evidovaných při registraci telekomunikačního provozu ve vztahu ke konkrétním osobám“¹⁶², a na prolomení této ochrany ze strany orgánů činných v trestním řízení je tedy v tomto smyslu nutné splnění konkrétních podmínek. Aby bylo v rámci trestního řízení možné nařídit zjištění údajů o telekomunikačním provozu podléhajících telekomunikačnímu tajemství či údajů pod ochranou osobních a zprostředkovatelských dat¹⁶³ a byla zajištěna jejich následná procesní použitelnost v řízení, je nezbytné naplnit následující předpoklady:

¹⁵⁶ Srov. § 88 odst. 8, odst. 9 trestního řádu. Blíže je informační povinnost a s ní související možnost přezkumu rozvedena v kapitole 2.3.2.

¹⁵⁷ Údaje, které jsou zpracovávány pro potřeby přenosu zprávy sítí elektronických komunikací nebo pro její účtování, srov. § 90 zákona o elektronických komunikacích

¹⁵⁸ Údaje určují zeměpisnou polohu telekomunikačního koncového zařízení uživatele veřejně dostupné služby elektronických komunikací, srov. § 91 zákona o elektronických komunikacích

¹⁵⁹ JELÍNEK, J. *Trestní zákoník a trestní řád s poznámkami a judikaturou: zákon o soudnictví ve věcech mládeže, zákon o trestní odpovědnosti právnických osob a řízení proti nim, advokátní tarif*. 9. aktualizované vydání. Praha: Leges, 2022. ISBN 978-80-7502-637-8., s. 804

¹⁶⁰ § 97 odst. 4 zákona o elektronických komunikacích

¹⁶¹ Ustanovení § 88 trestního řádu je detailněji popsáno v kapitole 2.3.1. této práce.

¹⁶² Nález Ústavního soudu ze dne 27. 8. 2001, sp. zn. IV. ÚS 78/01

¹⁶³ Srov. § 97 zákona o elektronických komunikacích; blíže k tomuto v kapitole 2.3.2.1. níže

- a. užití ustanovení pouze pro omezený okruh trestných činů, u jejichž vyšetřování může být jeho užití nařízeno:
 - i. úmyslné trestné činy s horní hranicí trestní sazby nejméně 3 léta stanovenou zákonem u příslušné skutkové podstaty;
 - ii. taxativně vyjmenované trestné činy¹⁶⁴; nebo
 - iii. jiné úmyslné trestné činy, k jejichž stíhání je Česká republika zavázána na základě vyhlášené mezinárodní smlouvy,
- b. soulad se zákonnými náležitostmi, resp. podmínkami vydání příkazu k zjištění údajů,¹⁶⁵ vč. náležitého písemného odůvodnění (pokud se vydání příkazu opírá o vyhlášenou mezinárodní smlouvu¹⁶⁶, musí být i uveden i konkrétní odkaz na tuto mezinárodní smlouvu), a týká-li se žádost konkrétního uživatele, i jeho totožnost, pokud je známa.

K vydání příkazu je oprávněn v řízení před soudem předseda senátu a v přípravném řízení soudce na návrh státního zástupce. Tohoto příkazu však není třeba, pokud k tomu dá souhlas uživatel telekomunikačního zařízení, jehož se zjišťování ve smyslu ustanovení § 88a trestního řádu týká. Současně je nutné upozornit, že zákon ukládá orgánu činnému v trestním řízení, který věc pravomocně skončil, povinnost, aby uživatele telekomunikačního zařízení¹⁶⁷ informoval o tom, že byl proveden úkon ve smyslu § 88a trestního řádu.¹⁶⁸ Orgán tuto osobu poučí o možnosti podat v šestiměsíční lhůtě návrh na přezkum zákonnosti tohoto příkazu, a to k Nejvyššímu soudu. Zákonodárce však tuto povinnost neukládá vždy, naopak taxativně vymezuje¹⁶⁹, kdy je podávání informace ze strany orgánu činného v trestním řízení omezeno. Co však zákonodárce neupravuje¹⁷⁰ je otázka provozních a lokalizačních údajů

¹⁶⁴ Jedná se o trestné činy upravené v ustanovení § 182, § 209, § 230, § 231, § 353, § 354, §357, § 364, § 365 trestního zákoníku. Dle důvodové zprávy k návrhu novely č. 273/2012 Sb. vyjmenované trestné činy jsou páčány převážně prostřednictvím internetu a mobilních telefonů, bez provozních a lokalizačních údajů by u těchto trestných činů nemohlo dojít k jejich objasnění, či by objasnění bylo podstatně ztíženo. Srov. Důvodová zpráva k zákonu č. 273/2012 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a některé další zákony; ŠÁMAL, P., RŮŽIČKA, M. § 88 [Důvody nařízení a postup]. In: ŠÁMAL, P. a kol. *Trestní řád*. Op. cit., s. 1231

¹⁶⁵ Ustanovení je možno užít pouze subsidiárně v případě, kdy nelze sledovaného účelu dosáhnout jiným způsobem či by jeho dosažení bylo podstatně ztíženo, srov. § 88a odst. 1 trestního řádu

¹⁶⁶ Viz výše v bodu a. iii.

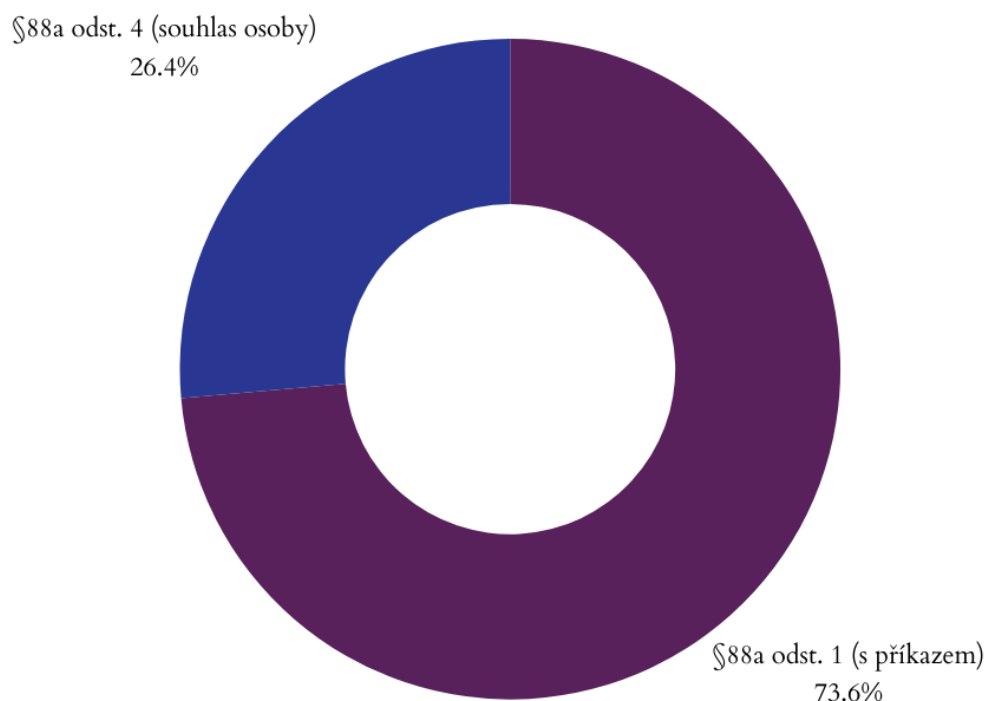
¹⁶⁷ Je-li znám

¹⁶⁸ Tuto informační povinnost má dle podmínek stanovených zákonem orgán činný v trestním řízení i v případě úkonu dle § 88 trestního řádu, srov. § 88 odst. 8, 9 trestního řádu.

¹⁶⁹ Jedná se o řízení, resp. případy nejzávažnější trestné činnosti, kdy by podáním takové informace mohlo dojít k ohrožení zdraví, života, práv a svobod osob či bezpečnosti státu nebo by došlo ke zmaření účelu trestního řízení. Důvody se shodují s důvody nepodání informace dle § 88 odst. 9 trestního řádu. Srov. ŠÁMAL, P., RŮŽIČKA, M. § 88a [Údaje o uskutečněném telekomunikačním provozu]. In: ŠÁMAL, Pavel a kol. *Trestní řád* Op. cit. s. 1234 a § 88 [Důvody nařízení a postup]. In: ŠÁMAL, P. a kol. *Trestní řád*. Op. cit., s. 1215

¹⁷⁰ Srov. ustanovení § 88 odst. 1 trestního řádu zakotvuje nepřipustnost užití ustanovení v případě komunikace mezi obhájcem a obviněným

a jejich zjištění na základě ustanovení § 88a trestního řádu ve vztahu ke *komunikaci mezi obviněným a obhájcem*.



Graf 3: Podíl výpisů o provozních a lokalizačních údajích v závislosti na tom, zda bylo k jejich zjištění postupováno dle §88a odst. 1 trestního řádu, nebo dle § 88a odst. 4 trestního řádu v roce 2022 z celkem 77 382 úkonů¹⁷¹

Analýza¹⁷² týkající se odposlechů a sledování osob, jež byla diskutována v kapitole 2.3.1., v rámci své anonymizované kazuistiky uvádí i případy, kdy bylo ze strany orgánů činných v trestním řízení efektivně využito ustanovení § 88a trestního řádu. Pro tuto práci je relevantní případ týkající zjištění důkazů o komunikaci s konkrétním cloudovým úložištěm, na kterém docházelo k trestné činnosti ve formě sdílení dětské pornografie¹⁷³. Útvar policie díky komplexní analýze zjistil přístupové IP adresy do emailové schránky osoby podezřelé vč. IP adresy, jež sloužila pro přihlašování na předmětné cloudové úložiště s protiprávným obsahem. Na základě příkazu vydaného dle ustanovení § 88a trestního řádu policejní orgán zjistil údaje k předmětným IP adresám, ze kterých bylo možné následně identifikovat

¹⁷¹ Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR za rok 2022, Op. cit.

¹⁷² *Tamtéž*.

¹⁷³ Trestný čin výroba a jiné nakládání s dětskou pornografií dle ustanovení § 192 trestního zákoníku.

podezřelého (jednalo se o okruh uživatelů využívajících dynamickou¹⁷⁴ IP adresu). Následně mohl být podezřelý obviněn.¹⁷⁵

Jak bylo nastíněno v úvodu této podkapitoly, musíme chápat rozdíl mezi institutem upraveným v ustanovení § 88a a ustanovení § 88 trestního řádu. Ten však nespočívá pouze v druhu údajů získaných díky použití těchto ustanovení orgány činnými v trestním řízení či odlišných podmínkách kladených zákonodárcem na jejich nařízení. Rozdíl je nezbytné spatřovat i v ohledu na časové období, na které je možno příkaz vydat. Zatímco ustanovení o odposlechu a záznamu telekomunikačního provozu směřuje *do budoucna*, institut upravený v ustanovení §88a trestního řádu se vztahuje, jak vyplývá i ze samotného textu zákona, na *již uskutečněný telekomunikační provoz*, tj. jedná se o údaje z minulosti^{176,177}. K tomuto se přiklání i komentářová literatura¹⁷⁸, Jelínek tuto skutečnost dále podkládá tím, že zákon nestanoví ani žádnou lhůtu, pro kterou by příkaz bylo možné do budoucna vydat.¹⁷⁹ Je však nutné podotknout, že rozhodovací praxe v tomto směru není jednotná¹⁸⁰.

Nejvyšší soud ve svém usnesení sp. zn. 4 Tdo 1591/2018 uvedl, že v situaci, kdy zjištění těchto údajů může orgánům činným v trestním řízení pomoci s odhalením či usvědčením pachatele a tato trestná činnost je v době vydání příkazu ve stádiu přípravy, lze příkaz o zjištění údajů o telekomunikačním provozu „*v odůvodněných případech vydat i tzv. do budoucna*“.¹⁸¹ Dále argumentoval, že způsob, jakým je zasahováno do základních lidských práv dle ustanovení § 88a trestního řádu, není natolik velký jako je tomu v ustanovení § 88 trestního řádu. Ve svém usnesení uvádí, že jsou zjišťovány „*jen údaje o uskutečněném telekomunikačním provozu, ovšem není zde zjišťován vlastní obsah těchto zpráv*“¹⁸². Toto bylo v roce 2019 podpořeno ze strany Ústavního soudu, když jakožto ochránce ústavnosti ve svém usnesení I. ÚS 2838/19 neshledal žádné porušení ústavně zaručených práv, a to i přes argumentaci

¹⁷⁴ IP adresa, která je přidělena více uživatelům v určitém čase.

¹⁷⁵ Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR za rok 2022, Op. cit.

¹⁷⁶ ŠÁMAL, P., RŮŽIČKA, M. § 88 [Důvody nařízení a postup]. In: ŠÁMAL, P. a kol. *Trestní řád*. Op. cit., s. 1196.

¹⁷⁷ TLAPÁK NAVRÁTILOVÁ, J. a GALOVCOVÁ, I. *Uchovávání dat uložených v počítačovém systému – poskytování součinnosti, nebo nahrazování činnosti orgánů činných v trestním řízení*. Advokátní deník. [online]. 2019 [cit. 8. 1. 2024]. Dostupné z: <https://advokatnidenik.cz/2019/12/11/uchovavani-dat-ulozenych-v-pocitacovem-systemu-poskytovani-soucinnosti-nebo-nahrazovani-cinnosti-organu-cinnych-v-trestnim-rizeni/>

¹⁷⁸ ŠÁMAL, P., RŮŽIČKA, M. § 88 [Důvody nařízení a postup]. In: ŠÁMAL, P. a kol. *Trestní řád*. Op. cit., s. 1196.

¹⁷⁹ JELÍNEK, J. *Trestní zákoník a trestní řád s poznámkami a judikaturou: zákon o soudnictví ve věcech mládeže, zákon o trestní odpovědnosti právnických osob a řízení proti nim, advokátní tarif*. Op. cit., s. 804

¹⁸⁰ K tomu více níže v této podkapitole.

¹⁸¹ Usnesení Nejvyššího soudu ze dne 7. 5. 2019, sp. zn. 4 Tdo 1591/2018

¹⁸² Usnesení Nejvyššího soudu ze dne 7. 5. 2019, sp. zn. 4 Tdo 1591/2018

stěžovatele k nedodržení zákonnosti u vydání příkazu dle ustanovení § 88a trestního řádu, tj. umožnění směřování příkazu vydaného na základě § 88a trestního řádu *do budoucna*.¹⁸³ To, zda se v případě provozních a lokalizačních údajů dá mluvit o mírnějším zásahu do základního lidského práva, jak se vyjádřil Nejvyšší soud¹⁸⁴, není jednoznačné. Ačkoliv Ústavní soud ve výše zmiňovaném usnesení¹⁸⁵ Nejvyšší soud podpořil a neshledal zásah do lidských práv úkonu ve smyslu §88a trestního řádu *do budoucna*, ve svém nálezu Pl. ÚS 45/17 se k míře zásahu do soukromí vyjádřil následovně: „*Údaje o telekomunikačním provozu mohou mít mnohdy větší vypovídací hodnotu než znalost obsahu komunikace, [...]; provozní a lokalizační údaje zasluhují z hlediska ochrany základních práv podobnou míru regulace.*“¹⁸⁶ Dovození tedy, že argumentace Nejvyššího soudu, tj. že se v případě provozních a lokalizačních údajů jedná o mírnější zásah do soukromí, a tedy je možné příkaz ve smyslu § 88a trestního řádu směřovat *do budoucna* (ačkoliv zákonodárce neuvádí žádné časové období, pro které může být příkaz vydán, ani záruky ochrany ve formě průběžného vyhodnocování, zda i nadále trvají důvody),¹⁸⁷ je nesprávná.

2.3.2.1. Data retention

Osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací jsou povinny při této činnosti v souladu s § 97 odst. 3 zákona o elektronických komunikacích tyto údaje po dobu šesti měsíců uchovávat.¹⁸⁸ Tzv. *data retention* představuje „*plošné uchovávání provozních a lokalizačních údajů*“,¹⁸⁹ prostřednictvím kterého se stát při plnění svých úkolů¹⁹⁰ snaží „*neztratit v době informační společnosti krok*“¹⁹¹. Rozsah uchovávaných údajů definuje ustanovení § 2 Vyhlášky o uchovávání, předávání a likvidaci provozních a lokalizačních údajů¹⁹², srov. například se jedná o telefonní čísla volajícího a volaného, unikátní identifikátor mobilního zařízení tzv. IMEI, datum a čas zahájení komunikace, délku hovoru, IP adresa, identifikátor uživatelského účtu, typ připojení, adresa elektronické pošty uživatele.

¹⁸³ Usnesení Ústavního soudu ze dne 8. 10. 2019, sp. zn. I. ÚS 2838/19

¹⁸⁴ Usnesení Nejvyššího soudu ze dne 7. 5. 2019, sp. zn. 4 Tdo 1591/2018

¹⁸⁵ Usnesení Ústavního soudu ze dne 8. 10. 2019, sp. zn. I. ÚS 2838/19

¹⁸⁶ Nález Ústavního soudu ze dne 14. 5. 2019, sp. zn. Pl. ÚS 45/17

¹⁸⁷ Srov. § 88 odst. 2 a odst. 3 trestního řádu

¹⁸⁸ § 97 odst. 3 zákona o elektronických komunikacích

¹⁸⁹ Nález Ústavního soudu ze dne 14. 5. 2019, sp. zn. Pl. ÚS 45/17

¹⁹⁰ Plnění účelu trestního práva, tj. ochrany zájmů společnosti, státu, práv a oprávněných zájmů osob.

¹⁹¹ Nález Ústavního soudu ze dne 14. 5. 2019, sp. zn. Pl. ÚS 45/17

¹⁹² Vyhláška č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů

Uchování údajů slouží zejména k tomu, aby si je orgán činný v trestním řízení mohl za podmínek a pro účely stanovené trestním řádem a trestním zákoníkem vyžádat, tyto údaje pak musí být bezodkladně poskytnuty. Mimo to mohou být provozní a lokalizační údaje v souladu se zákonem o elektronických komunikacích poskytnuty Policii ČR při pátrání po pohřešované osobě, určení identity mrtvol, prověřování osoby, jež je chráněna či předcházení hrozeb souvisejících s terorismem. Obdobně tomu je u poskytnutí údajů Bezpečnostní informační službě, Vojenskému zpravodajství či České národní bance, vždy je však nezbytné, aby byly splněny podmínky zvláštního právního předpisu, který jejich vyžádání subjektu v předmětné věci umožňuje.¹⁹³

Ustanovení týkající se uchování dat byla pro svoji ústavní (ne)konformitu několikrát podrobena přezkumu Ústavním soudem. V nálezu Pl. ÚS 24/10 se soud zabýval zejména otázkou záruky na *informační sebeurčení*, tj. aby jedinec mohl rozhodovat sám o sobě samém ve smyslu objemu a podmínek, za kterých budou zpřístupněna data týkající se jeho soukromí. Zdůraznil totiž, že kombinací a delším pozorováním lze díky těmto údajům získat „*detaillní informace o společenské nebo politické příslušnosti, jakož i o osobních zálibách, sklonech nebo slabostech jednotlivých osob*“¹⁹⁴. Původní znění ustanovení § 97 odst. 3 a 4 zákona o elektronických komunikacích¹⁹⁵ tak bylo pro ústavní nekonformnost nálezem derogováno.¹⁹⁶ V návaznosti na to Ústavní soud zrušil svým nálezem Pl. ÚS 24/11 také ustanovení § 88a trestního řádu, které dle rozhodnutí neprošlo testem proporcionality.¹⁹⁷ Zákonodárce později v této souvislosti přijal novelu¹⁹⁸ týkající se předmětných ustanovení a data retention znovuzavedl.

Ve svém pozdějším nálezu Pl. ÚS 45/17 (Data retention III) se Ústavní soud vyslovil, že pro zajištění „*minimalizace zásahu*“¹⁹⁹ do základních práv garantovaných Listinou základních práv a svobod²⁰⁰ je esenciální, aby byly stanoveny přísné podmínky pro uchování a zpřístupnění dat²⁰¹ a současně pro jejich využití ve smyslu zjišťování údajů o uskutečněném

¹⁹³ § 97 odst. 3 písm. a) zákona o elektronických komunikacích

¹⁹⁴ Nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/10

¹⁹⁵ Původní ustanovení bylo transpozicí Směrnice Evropského parlamentu a Rady č. 2006/24/ES tzv. „*Směrnice o data retention*“, ta byla zrušena Soudním dvorem EU rozhodnutím C-293/12 a C-594/12 *Digital Rights Ireland Ltd* ze dne 8. 4. 2014 pro rozpor s Listinou základních práv EU. Srov. Rozsudek Soudního dvora EU ze dne 8. 4. 2014, sp. zn. C-293/12; C-594/12

¹⁹⁶ Nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/10

¹⁹⁷ Nález Ústavního soudu ze dne 20. 12. 2011, sp. zn. Pl. ÚS 24/11

¹⁹⁸ Novela vychází z nálezů Ústavního soudu Pl. ÚS 24/10 a Pl. ÚS 24/11

¹⁹⁹ Nález Ústavního soudu ze dne 14. 5. 2019, sp. zn. Pl. ÚS 45/17

²⁰⁰ V této věci se týká článku 10 odst. 2 Listiny a článku 10 odst. 3 ve spojení s článkem 13 Listiny

²⁰¹ § 97 odst. 3 a 4 zákona o elektronických komunikacích

telekomunikačním provozu²⁰². Upozornil také na důležitost nastavení efektivních prostředků obrany²⁰³ jakožto záruk před možným zneužitím těchto údajů. Dle Ústavního soudu je však existence transparentního rámce, který bude upravovat podmínky uchování a zpřístupnění dat, nutná. Vyjádřil se tak s odkazem na vývoj společnosti a širokému užívání elektronické komunikace. Vyhováním návrhu na zrušení ustanovení o uchovávání údajů (a jeho následná absence) by dle soudu vedla pouze k jiné (netransparentní) variantě. S odkazem na neexistenci „šetrnějšího“²⁰⁴ způsobu využívání údajů ze strany státu tak svým nálezem ponechal ustanovení o shromažďování a využívání provozních a lokalizačních údajů v platnosti.²⁰⁵ Ústavní soud se ve svém nálezu však nijak nevypořádává s rozhodnutími Soudního dvora EU ve věcech C-203/15 a C-698/15²⁰⁶, které jsou v tomto ohledu stěžejní. Je vhodné také poznamenat, že Soudní dvůr EU v souvislosti s problematikou data retention rozhodoval ještě několikrát²⁰⁷, kde mj. zopakoval, že není dovoleno preventivní nevyběrové a plošné shromažďování.²⁰⁸ Otázkou tedy zůstává, zda se s tímto Ústavní soud vypořádal správně a opravdu není šetrnější alternativa, která by základní práva jedince garantovaná Listinou chránila lépe, resp. širěji.

2.3.3. Sledování osob a věcí

Dalším významným procesněprávním institutem je ustanovení § 158d trestního řádu o sledování osob a věcí. Jedná se o jeden ze tří taxativně vymezených operativně pátracích prostředků, jehož použití trestní řád v řízení o úmyslných trestných činech umožňuje.^{209,210} Jak uvádí komentářová literatura, ustanovení předpokládá tři druhy sledování osob a věcí. Můžeme je dělit na obecné *sledování dle odstavce 1*, *sledování dle odstavce 2* (v rámci kterého jsou pořizovány obrazové a zvukové záznamy či jiné ve smyslu § 158b odst. 3 trestního řádu)

²⁰² § 88a trestního řádu

²⁰³ Srov. § 88a odst. 2 trestního řádu, dále také níže v této podkapitole.

²⁰⁴ Nález Ústavního soudu ze dne 14. 5. 2019, sp. zn. Pl. ÚS 45/17

²⁰⁵ Nález Ústavního soudu ze dne 14. 5. 2019, sp. zn. Pl. ÚS 45/17

²⁰⁶ Srov. Soudní dvůr EU se v rozhodnutích C-203/15 a C-698/15 *Tele2 Sverige AB and Watson* ze dne 21. 12. 2016 vyjádřil, že čl. 15 odst. 1 Směrnice Evropského parlamentu a Rady 2002/58/ES ve spojení s příslušnými články Listiny základních práv EU, musí být interpretován v tom smyslu, že brání, aby právními rámci členských států bylo zavedeno plošné a nerozlišující uchovávání provozních a lokalizačních údajů všech účastníků. Srov. Rozsudek Soudního dvora EU ze dne 21. 12. 2016, sp. zn. C-203/15; C-698/15

²⁰⁷ Srov. C-623/17 *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others*; C-746/18 *H. K v. Prokuratuur*

²⁰⁸ Je to možné pouze v případě, kdy může být závažně ohrožena bezpečnost, jen po jasně vymezený časový úsek a po rozhodnutí orgánu k tomu příslušnému. Srov. C-511/18, C-512/18 a C-520/18 *La Quadrature du Net and Others v. Premier ministre and Others*

²⁰⁹ Srov. §158b odst. 1 trestního řádu

²¹⁰ ŠÁMAL, P. *Operativně pátrací prostředky*. In: HENDRYCH, D. a kol. *Právníký slovník*. 3. vydání. Praha: C. H. Beck, 2009

a sledování dle odstavce 3 (skrže které je zasahováno do ústavně zaručených práv²¹¹). Význam dělení spočívá mj. v tom, zda je k jejich provedení nutné povolení, a popřípadě kdo je oprávněn povolení udělit a jaké k jeho udělení musí být naplněny předpoklady. Tento „stupeň přísnosti“ se v zásadě odvíjí od míry zásahu do základních lidských práv. Ve všech případech se jedná o sledování probíhající utajeně ve vztahu k těm, kteří se sledovanou věcí disponují, nebo jsou osobami sledovanými. Využity mohou být nejrůznější nástroje, a to v závislosti na tom, podle jakého odstavce se sledování provádí.²¹² Z hlediska relevance pro tuto práci považuji za vhodné rozebrat pouze sledování podle odstavce 2 a 3. V této souvislosti si dovoluji rozdělit podkapitoly dle „místa“ užití ustanovení o sledování osob a věcí.

2.3.3.1. *Prostorové odposlechy*

Ačkoliv zákonodárce v trestním řádu nikde tzv. prostorové odposlechy přímo neupravuje, odborná právní literatura s tímto pojmem běžně pracuje.²¹³ Můžeme je chápat jako utajené sledování zvuku nebo obrazu, a to v jakémkoliv prostoru, kde je to možné za pomoci technického vybavení provést. Jelínek za prostorové odposlechy označuje: „*utajené získávání informací pomocí speciálních, pro tyto účely sestavených technických prostředků a zařízení zaznamenávajících obraz, zvuk, přesný pohyb i činnost sledovaných osob v reálném čase a prostoru*“²¹⁴. Pro srovnání je možné si představit jakýkoliv veřejnosti přístupný prostor, např. ulice, hromadné dopravní prostředky, restaurační zařízení, kavárny, knihovny apod. Nesmíme však opomenout možnost užití ustanovení o sledování i na soukromé prostory jako je byt či dům.²¹⁵ V tomto případě se však bude aplikovat, na rozdíl od veřejně přístupných prostorů, přísnější režim spadající pod odstavec 3, tj. k umožnění sledování je zapotřebí povolení soudce, neboť dochází k zásahu do základního práva na nedotknutelnost obydlí.²¹⁶

Jak již bylo naznačeno v předchozím odstavci, v rámci užití ustanovení o sledování osob a věcí dochází k významnému zásahu do oblasti ústavně zaručených práv a svobod. Zejména

²¹¹ Srov. listovní tajemství, tajemství jiných písemností a záznamů uchovávaných v soukromí či nedotknutelnost obydlí.

²¹² ŠÁMAL, P., RŮŽIČKA, M. § 158d [Sledování osob a věcí]. In: ŠÁMAL, P. a kol. *Trestní řád*. Op. cit., s. 2004

²¹³ Srov. JELÍNEK, J. *K chybějící právní úpravě tzv. prostorového odposlechu v trestním řádu*. Bulletin advokacie, 2018, č. 7-8, s. 13-19; GRÍVNA, T. *Zákonnost důkazů získaných sledováním osob a věcí*. In: JELÍNEK, J. *Dokazování v trestním řízení v kontextu práva na spravedlivý proces*. Praha: Leges, 2018. ISBN 978-80-7502-287-5. s. 314-326; JELÍNEK, M. *Ústavní meze prostorových odposlechů ke sledování osob a věcí podle § 158d trestního řádu*. Bulletin advokacie, 2010, č. 5, s. 31-33

²¹⁴ JELÍNEK, J., *K chybějící právní úpravě tzv. prostorového odposlechu v trestním řádu*, Op. cit., s. 13-19

²¹⁵ *Tamtéž*.

²¹⁶ Nedotknutelnost obydlí chráněnou článkem 12 Listiny je nutno ji rozšířit i na prostory užívanými k pracovní nebo podnikatelské činnosti či uspokojování zájmových aktivit a vlastních potřeb, srov. Nález Ústavního soudu ze dne 8. 6. 2010, sp. zn. Pl. ÚS 3/09

se jedná o článek 7 Listiny, který chrání nedotknutelnost osoby a jejího soukromí. Požadavek na přiměřenost a užití operativně pátracího prostředku jen za okolností, kdy je to pro trestní řízení nezbytné, nalezneme také v článku 8 odst. 2 Evropské úmluvy. Evropský soud pro lidská práva dále ve své judikatuře tento článek chránící právo jedince na respektování jeho soukromého a rodinného života rozvádí a rozšiřuje ho i na místa veřejnosti přístupná, pokud je sledování prováděno „*způsobem nebo v míře, kterou nelze běžně předvídat*“.²¹⁷ Lze tedy uzavřít, že zájem veřejnosti na stíhání trestné činnosti je v tomto ohledu ve střetu s právem na soukromí jednotlivce. O to více je nepochopitelné, že tzv. povolovací režim v případě § 158d odst. 2 a odst. 3 trestního řádu podléhá zásadně nižší míře ochrany základních práv, když neposkytuje stejné záruky jako v případě ustanovení o odposlechu. Umožnění postupu o *prostorovém odposlechu* klade oproti postupu dle ustanovení § 88 a § 88a trestního řádu mnohem mírnější, resp. nižší požadavky, a to navzdory ekvivalentnímu zásahu těchto procesních postupů do soukromí jednotlivce. Konečně si tedy shrneme předpoklady, které je nezbytné naplnit pro zákonost povolení k sledování osob a věcí:

- a. užití ustanovení pro úmyslné trestné činy;²¹⁸
- b. podmíněno
 - i. písemným povolením státního zástupce pro sledování zvukových, obrazových či jiných záznamů;
 - ii. předchozím povolením soudce pro sledování zasahující do nedotknutelnosti obydlí, listovního tajemství, zjišťování obsahu jiných písemností či záznamů uchovávaných v soukromí;
 - iii. bez povolení, jedná-li se o neodkladnou věc a nejedná-li se o sledování dle odst. 3, za těchto okolností je policejní orgán povinen požádat o povolení dodatečně, neobdrží-li ho do 48 hodin, je jeho povinností, aby sledování ukončil, zničil záznam s ním spojený a informace, jež se v souvislosti s tím dozvěděl, nepoužil;
 - iv. bez povolení, je-li dán výslovný souhlas osoby, do jejíž práv a svobod je sledováním zasahováno (lze pro odst. 2 i odst. 3), sledování je však podmíněno trvajícím souhlasem, v opačném případě je sledování ihned zastaveno,

²¹⁷ ESLP 35623/05 *Uzun proti Německu*, bod 48

²¹⁸ Srov. Oproti úpravě § 88 a 88a trestního řádu se jedná o mnohem širší škálu trestných činů, pro které může být postup povolen.

- c. splnění náležitostí žádosti o povolení, zejména její písemná forma a odůvodnění vč. stanovení doby pro kterou má být povolení uděleno,²¹⁹
- d. přiložení protokolu s nutnými náležitostmi.

Z výše uvedeného je možné identifikovat chybějící instituty, které jsou odborníky²²⁰ včetně Stálé komise pro kontrolu odposlechu²²¹, zákonodárci vytýkány právě v souvislosti s garancí ochrany základních lidských práv. Problémem současné právní úpravy je především *neexistence informační povinnosti* orgánu činného v trestním řízení (po pravomocném skončení věci) vůči sledované osobě ve spojení s *nemožností přezkumu zákonnosti povolení* u Nejvyššího soudu, srov. úprava ustanovení § 88 a § 88a trestního řádu. Dále je možné zákonodárci vytýkat ukotvení velmi *širokého okruhu trestných činů*²²², na něž je možné prostorové odposlechy povolit. Zejména by se však úprava *de lege ferenda* měla zaměřit na srovnání podmínek, které zákon stanoví pro umožnění prostorového odposlechu, a to právě s podmínkami stanovenými pro § 88 a § 88a trestního řádu, tj. nařízení soudem. Gřivna²²³ dále připomíná *absenci vyhodnocení průběhu sledování při žádosti o prodloužení sledování a doby, jež by stanovovala, kdy má dojít ke zničení obsahu z emailových schránek či získaných záznamů*. Na tyto rozdíly v nastavení podmínek pro nařízení prostorových odposlechu a odposlechu dle § 88 a § 88a trestního řádu upozorňuje v souvislosti s pochybami o ústavní konformitě.

Dále považuji za vhodné poukázat na možnost užití záznamu pořízeného při sledování a s ním připojeného protokolu jako důkazu v *jiné věci*, je-li naplněna podmínka vedení trestního řízení o úmyslném trestném činu nebo dá-li osoba, o jejíž práva a svobody se v rámci sledování jedná, k jeho užití souhlas. Dané ustanovení trestního řádu se však vztahuje jen na sledování *dle odstavce 2*, tj. kde postačí povolení státního zástupce.²²⁴ Nejvyšší soud se však ve svém usnesení 8 Tdo 647/2020 a později 7 Tdo 865/2020 vyjádřil, že je možné použít prostorové odposlechy v *jiné věci* i *dle odstavce 3*. Zdůraznil však, že je nutné vyvažovat mezi závažností trestného činu, pro který má být záznam použit (jako pro „věc jinou“), a závažností zásahu

²¹⁹ Nejvyšší možná doba pro povolení o sledování je 6 měsíců, je však možné žádat o její prodloužení vždy o nejvýše dalších 6 měsíců, srov. § 158d odst. 4 trestního řádu.

²²⁰ Srov. GŘIVNA, T. *Zákonnost důkazů získaných sledováním osob a věcí*. In: JELÍNEK, J. *Dokazování v trestním řízení v kontextu práva na spravedlivý proces*. Op. cit., s. 314; JELÍNEK, J., *K chybějící právní úpravě tzv. prostorového odposlechu v trestním řádu*, Op. cit., s. 13-19

²²¹ Stálá komise pro kontrolu použití odposlechu a záznamu telekomunikačního provozu, použití sledování osob a věcí a rušení provozu elektronických komunikací. *Usnesení č. 25 (23. února 2017)* Psp.cz. [online] [cit. 10. 1. 2024]. Dostupné z: <https://www.psp.cz/sqw/text/text2.sqw?idd=102715>

²²² Všechny úmyslné trestné činy

²²³ GŘIVNA, T. *Zákonnost důkazů získaných sledováním osob a věcí*. In: JELÍNEK, J. *Dokazování v trestním řízení v kontextu práva na spravedlivý proces*. Op. cit., s. 325-6

²²⁴ § 158d odst. 10 trestního řádu

do soukromí jedince a práva na nedotknutelnost osoby. Dle soudu tedy nelze souhlasit s užitím záznamu pro nepoměrně méně závažný trestný čin. Aby mohl být záznam užit v jiné trestní věci, je nutný soulad s principem proporcionality.²²⁵

V závěru je nutné shrnout, že obdobně jako je tomu u stanovení § 88 trestního řádu, je i ustanovením o sledování chráněna *komunikace mezi obhájcem a obviněným*.²²⁶ V případě, kdy policejní orgán zjistí, že sledováním bylo zasaženo do této chráněné komunikace, nesmí okolnosti, jež se dozvěděl, použít a zjištěný obsah²²⁷ musí zničit. Zákonodárce však i zde váže dobu ochrany na vydání usnesení o zahájení trestního stíhání ve smyslu ustanovení § 160 odst. 1 trestního řádu.

2.3.3.2. *Obsah emailových schránek*

V souvislosti s ustanovením o sledování osob a věcí je nutné si zdůraznit využití tohoto ustanovení v případě získávání obsahu z emailových schránek, konkrétně s pomocí ustanovení § 158d odst. 3 trestního řádu. Jak bude dále rozvedeno v kapitole 3.1.1., pro získávání informací z emailových schránek je nutné z hlediska použitelnosti ustanovení rozlišovat časové hledisko, tj. zda se jedná o získávání informací *aktuálního obsahu schránky* či *do budoucna*, a dále okolnost, zda má orgán činný v trestním řízení *datový nosič k dispozici* nebo *nikoliv*.

Jak uvádí Polčák, nesmíme zapomínat na snadnou, ať již úmyslnou či neúmyslnou pozměnitelnost emailové zprávy včetně metadat s ní souvisejících. V tomto ohledu tedy nelze brát autenticitu emailové komunikace za samozřejmou a problematická je i s ní související věrohodnost důkazu.²²⁸ Elektronická komunikace, resp. emailová komunikace je však používaná denně, a to nejen pro soukromé účely, ale dnes je skrze ni uskutečňována zejména komunikace v pracovním či akademickém prostředí. Pro orgány činné v trestním řízení je tak získávání informací z tohoto zdroje důležité. Ustanovení o sledování osob a věcí se užije, je-li zajišťován obsah emailových schránek *komunikace již proběhlé* a *datový nosič nemá* orgán činný v trestním řízení *ve své dispozici*.

K využití ustanovení § 158d odst. 3 trestního řádu se ve svém usnesení vyjádřil již v roce 2013 Ústavní soud: „*předmětem sledování budou právě data na těchto zařízeních uložená, jejichž otisk lze pořídit za využití utajené operativně pátrací techniky. Pořízení otisku*

²²⁵ Usnesení Nejvyššího soudu ze dne 25. 8. 2020, sp. zn. 8 Tdo 647/2020; Usnesení Nejvyššího soudu ze dne 1. 9. 2020, sp. zn. 7 Tdo 865/2020

²²⁶ Srov. § 158d odst. 1 věta 2 trestního řádu

²²⁷ Obrazový, zvukový či obdobný záznam.

²²⁸ POLČÁK, R., PÚRY, F., HARAŠTA, J., MYŠKA, M. a STUPKA, V. *Elektronické důkazy v trestním řízení*. Op. cit., s. 117

*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.*²²⁹, což později sjednotila i metodika, resp. výkladové stanovisko NSZ č. 1/2015, které se k výše uvedenému usnesení odkazuje. A contrario z toho vyplývá, že není možné využít tohoto institutu pro zajišťování emailové komunikace, která probíhá či bude probíhat *v budoucnu*. Dle NSZ je tak možné ustanovení § 158d odst. 3 trestního řádu „*považovat za zákonnou licenci prolamující ústavně zaručené právo na ochranu soukromí v e-mailové schránce se nacházejících záznamů*“.²³⁰ Informace, které se za pomoci ustanovení o sledování dají z emailové schránky takto zajistit, tvoří celý obsah emailové schránky, tj. složka *doručených, odeslaných, rozepsaných* či *smazaných* zpráv.²³¹

Pro zajišťování elektronické komunikace probíhající *v reálném čase*, resp. *do budoucnosti*, je dle stanoviska nutné užití ustanovení o odposlechu § 88 trestního řádu. Stanovisko dále poukazuje na nesjednocenost praxe a užití různých institutů trestního řádu včetně např. ustanovení § 8 odst. 1 trestního řádu (jehož užití je však dle Nejvyššího státního zastupitelství z důvodu ochrany základních lidských práv v tomto případě nesprávné).²³²

2.3.4. Domovní prohlídka a prohlídka jiných prostor

Dalšími procesními instituty, kterými orgán činný v trestním řízení při zajišťování elektronických důkazů disponuje, je domovní prohlídka a prohlídka jiných prostor a pozemků zakotvená v ustanoveních § 82-85c trestního řádu. Protože se jedná o ustanovení, která umožňují zásah do ústavně garantovaných práv a svobod, je nutné naplnění určitých předpokladů, aby jejich nařízení bylo přípustné, srov. článek 8 Evropské úmluvy a článek 12 odst. 2 Listiny. Jejich využití nastává v případech, kdy má orgán činný v trestním řízení důvodné podezření, že se v obydlí²³³ či jiných prostorách, které nejsou přístupné veřejnosti,²³⁴ nachází věc či osoba, která je důležitá pro trestní řízení. Na základě těchto ustanovení lze takovou osobu nebo věc zajistit (či zajistit věc u osoby²³⁵).

²²⁹ Usnesení Ústavního soudu ze dne 3. 10. 2013, sp. zn. III. ÚS 3812/12

²³⁰ *Tamtéž*.

²³¹ KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z.s.p.o, 2016. ISBN 978-80-88168-15-7. s. 448

²³² Výkladové stanovisko NSZ č. 1/2015

²³³ Pojem obydlí se dle komentářové literatury dá vzhledem k chráněnému zájmu chápat nejen jako byt, dům či chata, ale také jako hotelový pokoj, ubytovna, výchovný ústav, vysokoškolská kolej apod. Srov. ŠÁMAL, P., RŮŽIČKA, M. § 82 [*Důvody domovní prohlídky a osobní prohlídky a prohlídky jiných prostor a pozemků*]. In: ŠÁMAL, P. a kol. *Trestní řád*. Op. cit., s. 1112

²³⁴ Např. kancelář, živnostenská provozovna, samostatné garáže, lodě, automobily. Srov. *Tamtéž*, s. 1114.

²³⁵ V případě osobní prohlídky.

Na základě ustanovení § 83 trestního řádu je k nařízení domovní prohlídky a současně prohlídky jiných prostor a pozemků oprávněn předseda senátu a v přípravném řízení soudce na návrh státního zástupce.²³⁶ Je nezbytné, aby byl příkaz písemný a s řádným odůvodněním.²³⁷ Při prohlídce se příkaz doručí osobě, u níž se prohlídka koná, nejpozději však do 24 hodin po odpadnutí překážky, brání-li okolnosti bezprostřednímu doručení. Prohlídku jiných prostor a pozemků je na základě ustanovení § 83a odst. 2 trestního řádu možné policejním orgánem provést i bez příkazu, pokud věc nenese odkladu a nelze příkaz získat předem. Jakmile je to možné, tj. bezodkladně, je však policejní orgán nucen si takový příkaz vyžádat. Pokud příkaz není dodatečně vydán, nelze důkaz získaný na základě tohoto úkonu dále v trestním řízení použít. Obdobně tomu bude u provedení prohlídky jiných prostor a pozemků na základě písemného souhlasu uživatele daných prostor, srov. § 83a odst. 3 trestního řádu. V této souvislosti je policejní orgán povinen ihned vyrozumět osobu jinak oprávněnou k vydání příkazu²³⁸.

Předcházet domovní prohlídce a prohlídce jiných prostor by měl výslech uživatele dotčeného prostoru, a to z důvodu dosažení dobrovolného vydání věci ve smyslu ustanovení § 78 trestního řádu, jež odůvodňuje nařízení prohlídky.²³⁹ Pokud však věc nenese odkladu (popřípadě výslech nelze provést bezprostředně), zákonodárce v poslední větě ustanovení § 84 trestního řádu od předchozího výsledku upouští. Orgán vykonávající prohlídku musí umožnit osobám, jež jsou uživateli daných prostor, popř. zletilému členu domácnosti či zaměstnanci, aby se úkonu účastnil a o tomto právu příslušnou osobu poučit. Současně je orgán v souladu s § 85 odst. 2 trestního řádu vždy povinen zajistit přítomnost nezúčastněné osoby, jejíž podpis následně připojí k protokolu o provedené prohlídce, srov. § 85 odst. 3 trestního řádu. Osoba, u níž je prohlídka vykonávána, je povinna úkon strpět a současně je policejnímu orgánu umožněno případný odpor či překážku překonat, srov. § 85 a § 85a trestního řádu.

Zaměříme-li se na elektronické důkazy, je třeba především uvést, na jaké věci se orgán činným v trestním řízení při zajišťování v rámci domovní prohlídky či prohlídky jiných prostor zaměřuje. Zajišťování se bude týkat především počítačových systémů a obdobných předmětů,

²³⁶ V případě, že se jedná o neodkladný úkon, zákon umožňuje, aby příkaz byl nařízen předsedou senátu či soudcem, které jsou příslušní v obvodu, kde se prohlídka koná. Srov. § 83 odst. 1 trestního řádu a § 18 trestního řádu.

²³⁷ Odůvodnění musí být vždy na základě konkrétních skutkových okolností, popřípadě „čím – a v čem – pokládá zákonem stanovené podmínky za naplněné“, nelze se odkázat pouze na ustanovení zákona. Srov. Nález Ústavního soudu ze dne 28. 4. 2009, sp. zn. I. ÚS 536/06

²³⁸ Srov. předsedu senátu a v přípravném řízení státního zástupce

²³⁹ KOLOUCH, J. *CyberCrime*. Op. cit., s. 429

tj. stolní počítače, notebooky, mobilní telefony, servery, datová úložiště, tablety, herní konzole (Playstation, Xbox), tiskárny, paměťová média (pevné disky, SSD karty a jiné paměťové karty, flash disky, CD, DVD apod). Dále se policejní orgán bude zabývat tím, jak jsou připojeny počítačové systémy k síti Internet (způsob, zjištění konkrétních ISP či připojení k NAS²⁴⁰) a jakým způsobem jsou připojeny počítačové systémy do lokální sítě (např. propojení jednotlivých počítačů mezi sebou, jejich umístění v síti, zjištění oprávnění osob k přístupu do určitých částí sítě).^{241,242} Vždy je vhodné, aby zajišťování výše uvedených počítačových systémů a nosičů probíhalo s odborností, jako např. kriminalistickým technikem či policistou k tomu vyškoleným.²⁴³

Kolouch²⁴⁴ dále uvádí, že v příkazu k domovní prohlídce či prohlídce jiných prostor je vždy důležité uvést, k jakým věcem se příkaz vztahuje v celé možné šíři, a došlo tak k zajištění veškerých věcí, které s trestnou činností mohou mít souvislost. Pokud by příkaz byl specifikován pouze na jednu věc, nebylo by policejnímu orgánu umožněno zajistit ostatní věci důležité pro dané trestní řízení, aniž by nebyl vydán další příkaz.

V této souvislosti zákonodárce pamatuje i na případy, kdy je prováděla prohlídka v prostorech, v nichž je *vykonávána advokacie*. Orgán provádějící úkon si dle § 85b trestního řádu musí v případě, je-li možné, že se v prostorách nacházejí listiny obsahující skutečnosti, na které se vztahuje *mlčenlivost advokáta*²⁴⁵, vyžádat součinnost České advokátní komory a seznámit se s jejich obsahem pouze za přítomnosti jejich zástupce, který musí s tímto úkonem souhlasit. Pokud by byl souhlas odepřen, není možné se s listinami seznamovat. Tento souhlas však lze nahradit, a to na návrh, soudcem soudu, jež je nejbližší nadřízený soudu, který domovní prohlídku nařídil. Návrh však musí v souladu s ustanovením § 85 odst. 4 trestního řádu specifikovat konkrétní listiny, pro něž se souhlas zástupce České advokátní komory nahrazuje a současně i konkretizovat, proč a na základě jakých skutečností má být souhlas nahrazen. Návrh musí být podán nejpozději do 15 dní ode dne udělení nesouhlasu zástupce České advokátní komory. Za stěžejní považuji uvést rozhodnutí Nejvyššího soudu Tpjn 306/2014, které svým stanoviskem rozšiřuje po minulých rozhodnutích²⁴⁶ pojem *prostorů k výkonu advokacie* i na: „*jakýkoli prostor, který souvisí s výkonem advokacie a v němž se proto vyskytují*

²⁴⁰ Z anglického *Network Attached Storage* – datové úložiště na síti

²⁴¹ KOLOUCH, J. *CyberCrime*. Op. cit., s. 429-430

²⁴² POLČÁK, R., PŮRY, F., HARAŠTA, J., MYŠKA, M. a STUPKA, V. *Elektronické důkazy v trestním řízení*. Op. cit., s. 76

²⁴³ KOLOUCH, J. *CyberCrime*. Op. cit., s. 430

²⁴⁴ *Tamtéž*.

²⁴⁵ Blíže v ustanovení § 21 zákona č. 85/1996 Sb., o advokacii

²⁴⁶ Srov. Usnesení Městského soudu v Praze ze dne 9. 7. 2014, sp. zn. Nt 615/2014

*informace o klientech, ať již v písemné, elektronické či jiné podobě*²⁴⁷ a v souvislosti elektronickou podobou tyto „prostory“ dále specifikuje na *„různá elektronická úložiště dat, a to ať už jde o webové stránky advokáta, vlastní datová úložiště advokáta nenacházející se v 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)*²⁴⁸. To považuji za stěžejní, jelikož v současné době jsou tyto úložiště běžnou praxí.

Souhlas zástupce České advokátní komory je dle usnesení Ústavního soudu III. ÚS 3988/13 zakotven k tomu účelu, aby nebylo zasaženo do práva na obhajobu, rovnosti zbraní, a především tak nebyl oslaben či prolomen požadavek mlčenlivosti advokáta.²⁴⁹ Ve svém nálezu II. ÚS 2894/08-2 se Ústavní soud již dříve k mlčenlivosti advokáta vyjádřil jako k povinnosti, jež je uložena *„advokátovi v zájmu jeho klientů a pro jejich ochranu*²⁵⁰. Je tedy vhodné, aby mlčenlivost advokáta stanovená mu ustanovením § 21 zákona č. 85/1996 Sb., o advokacii, byla respektována a zachována v celé šíři, tedy pamatovala na nové technologické možnosti, které jsou při výkonu advokacie využívány. V souvislosti s tím komentářová literatura specifikuje pojem listiny jako *„jakákoli písemnost bez ohledu na to, na jakém materiálu je zachycena*²⁵¹ a pojem jiného nosiče informací jako *„materiál, do kterého nebo na který lze zaznamenávat data a z kterého lze data opět získat*²⁵² a to včetně uvedení příkladů, kterým je, dle judikatury a odborné veřejnosti, mj. i mobilní telefon²⁵³, tablet, elektronické čtečky knih, diktafony a jiné digitální záznamníky zvuku či obrazu nebo např. GPS navigace.²⁵⁴ Představit si tak lze *veškeré nosiče informací, které mohou obsahovat informace, jež je advokát povinen zachovávat v tajnosti a chránit tím vzájemnou důvěrnost mezi ním a klientem.*

2.3.5. Předložení nebo vydání věci a odnětí věci

Jedním z velmi často užitých institutů pro zajištění elektronických důkazních prostředků je bezpochyby ustanovení § 78 a § 79 trestního řádu o předložení nebo vydání věci či odnětí věci. Zákonodárce tímto stanovil povinnost každého k předložení věci důležité pro trestní

²⁴⁷ Stanovisko Nejvyššího soudu ze dne 25. 6. 2015, sp. zn. Tpjn 306/2014

²⁴⁸ Stanovisko Nejvyššího soudu ze dne 25. 6. 2015, sp. zn. Tpjn 306/2014

²⁴⁹ Usnesení Ústavního soudu ze dne 24. 3. 2014, sp. zn. III. ÚS 3988/13

²⁵⁰ Nález Ústavního soudu ze dne 28. 8. 2009, sp. zn. II. ÚS 2894/08-2

²⁵¹ ŠÁMAL, P., RŮŽIČKA, M. § 85b [Součinnost České advokátní komory]. In: ŠÁMAL, P. a kol. *Trestní řád*. Op. cit., s. 1162.

²⁵² *Tamtéž*.

²⁵³ Srov. Nález Ústavního soudu ze dne 25. 11. 2010, sp. zn. II. ÚS 889/10

²⁵⁴ SMEJKAL, V. *Ochrana dat advokátů v elektronických úložištích*. Bulletin advokacie, 2015, č. 3, s. 15-22

řízení²⁵⁵, popřípadě ediční povinnost (vydání) takovéto věci, a to na výzvu²⁵⁶ předsedy senátu a v rámci přípravného řízení státního zástupce či policejního orgánu. Zároveň musí být osoba poučena o tom, jaký následek nastane, když nedojde k uposlechnutí této výzvy. Tím je možnost odnětí na základě ustanovení § 79 trestního řádu, případně uložení pořádkové pokuty dle ustanovení § 66 trestního řádu.²⁵⁷ Je však vhodné zdůraznit odstavce 2 tohoto ustanovení, kterým zákonodárce vyjímá z uvedené povinnosti listiny a jiné hmotné nosiče, jejichž obsah souvisí s okolnostmi, na které se vztahuje zákaz výslechu, a to za okolností, že nedojde ke zproštění mlčenlivosti²⁵⁸ či zproštění povinnosti, aby věc zůstala utajena.

Ustanovení neopomíjí ani zásadu *nemo tenetur se ipsum accusare*, neboli *zákazu sebeobviňování*, která vychází především z článku 36 odst. 1 Listiny, na základě kterého nelze donucovat obviněného k vydání důkazu, jež by svědčil v jeho neprospěch.²⁵⁹ Pořádkovou pokutou dle ustanovení § 66 trestního řádu k vydání věci tedy nelze obviněného v souladu s tímto zákazem nutit.²⁶⁰ Je však možné využít právě ustanovení § 79 trestního řádu o odnětí věci. Tento úkon je osoba již povinna strpět, což zásadě *zákazu sebeobviňování*, jak dovodil Ústavní soud ve svém nálezu III. ÚS 644/05, již vzhledem k „neaktivitě“ obviněného neodporuje.²⁶¹ Příkaz na základě ustanovení § 79 trestního řádu je vydáván předsedou senátu a u přípravného řízení státním zástupcem či policejním orgánem.

O vydání či odnětí věci se v souladu s ustanovením § 55 odst. 1 trestního řádu vyhotoví protokol, kde bude zajištěná věc důkladně popsána tak, aby nedošlo k záměně s jinou věcí a později mohla být případně na základě popisu věc vrácena.²⁶² Popis zpravidla obsahuje název výrobku včetně jeho číselného označení, název výrobce, barvu či možné vady věci. Zejména budou zajišťovány mobilní telefony, počítače, datová úložiště, externí a interní paměťová média, ale např. i herní konzole či tiskárny a 3D tiskárny.²⁶³

²⁵⁵ Srov. § 112 odst. 1 a odst. 2 trestního řádu

²⁵⁶ Výzva má formu opatření. Srov. KOLOUCH, J. *CyberCrime*. Op. cit., s. 420

²⁵⁷ Srov. § 78 odst. 1 trestního řádu.

²⁵⁸ V případě mlčenlivosti advokáta, může být zproštění uděleno jen ze strany jeho klienta a po smrti (případně zániku právnické osoby) jeho právní nástupce. Srov. § 21 zákona č. 85/1996 Sb., o advokacii; ŠÁMAL, P., RŮŽIČKA, M. § 78 [Povinnost k vydání věci]. In: ŠÁMAL, P. a kol. *Trestní řád*. Op. cit., s. 1018

²⁵⁹ HERCZEG, J. *Zásada „nemo tenetur“ a práva obviněného v trestním řízení*. Bulletin advokacie, 2010, č. 1-2, s. 38-47

²⁶⁰ POLČÁK, R., PÚRY, F., HARAŠTA, J., MYŠKA, M. a STUPKA, V. *Elektronické důkazy v trestním řízení*. Op. cit., s. 74

²⁶¹ Nález Ústavního soudu ze dne 23. 3. 2006, sp. zn. III. ÚS 644/05

²⁶² POLČÁK, R., PÚRY, F., HARAŠTA, J., MYŠKA, M. a STUPKA, V. *Elektronické důkazy v trestním řízení*. Op. cit., s. 74-75

²⁶³ KOLOUCH, J. *CyberCrime*. Op. cit., s. 427

2.3.6. Uchování dat uložených v počítačovém systému a znemožnění přístupu

Relevantním institutem pro tuto práci je i ustanovení § 7b trestního řádu upravující nakládání s daty, která jsou uložena v počítačovém systému nebo na nosiči informací včetně vzdálených úložišť (např. Microsoft OneDrive, Google Drive, iCloud). V této souvislosti se nejedná o zajišťovací institut, ale o nástroj, jehož prostřednictvím má orgán činný v trestním řízení možnost za pomoci osoby ve specifickém postavení²⁶⁴ zachovat určitá data k pozdějšímu zajištění, a to na základě některého ze zákonných ustanovení popsanych výše v této práci. Do trestního řádu bylo toto ustanovení vloženo novelou s účinností ke dni 1. 2. 2019.

Je vhodné poznamenat, že orgán činný v trestním řízení užíval tohoto nástroje již dříve, a to za užití obecného ustanovení o dožádání dle § 8 odst. 1 trestního řádu.²⁶⁵ K tomu se zákonodárce ostatně také kriticky vyjadřuje v důvodové zprávě novely. Potřebu přijetí ustanovení odůvodňuje nejen zajištěním implementace článku 16 a 29 Budapešťské úmluvy a nedostatečnou úpravou rychlého uchování dat, ale i odkazem na současnou situaci, přičemž uvádí, že: „v praxi je pro tento účel využíváno obecného ustanovení § 8 tr. ř. o součinnosti [...] nebo obecných policejních postupů“²⁶⁶. Zakotvení považuje za žádoucí i s ohledem k dalším úpravám postupů „při spolupráci s jinými státy za tímto účelem“²⁶⁷. Tato novela je však ze strany odborné veřejnosti²⁶⁸ kritizována zejména pro oprávnění²⁶⁹, jež jsou tímto ustanovením umožněna.

Institut zakotvený v ustanovení § 7b trestního řádu představuje tzv. *zmrazení dat* neboli *data freeze* či *data preservation* a umožňuje, jak již bylo nastíněno výše, aby jakákoliv osoba, která drží či má pod kontrolou konkrétní data, po určitou dobu²⁷⁰ na základě příkazu orgánu

²⁶⁴ Tou je osoba držící či mající pod kontrolou relevantní data. Označována je jako držitel dat z anglického „*data-holder*“, bude jím např. poskytovatel služeb. Srov. Vláda: 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, č. 287/2018 Dz

²⁶⁵ POLČÁK, R., PÚRY, F., HARAŠTA, J., MYŠKA, M. a STUPKA, V. *Elektronické důkazy v trestním řízení*. Op. cit., s. 108

²⁶⁶ Vláda: 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, č. 287/2018 Dz

²⁶⁷ *Tamtéž*.

²⁶⁸ Např. TOMAN, P. *Podstrčený paragraf § 7b trestního řádu. Kde se vzal a o čem je*. Advokatnidenik.cz [online]. Česká advokátní komora. Publikováno 22. 7. 2019 [cit. 20. 1. 2024]. Dostupné z: <https://advokatnidenik.cz/2019/07/22/podstrceny-paragraf-7b-trestniho-radu-kde-se-vzal-a-o-cem-je/>; SOKOL, T. *Povinnost dle § 7b trestního řádu z pohledu advokáta*. Advokatnidenik.cz [online]. Česká advokátní komora. Publikováno 2. 8. 2019 [cit. 20. 1. 2024]. Dostupné z: <https://advokatnidenik.cz/2019/08/02/povinnost-dle-7b-tr-radu-z-pohledu-advokata/>; TLAPÁK NAVRÁTILOVÁ, J., GALOVCOVÁ, I. *Uchovávání dat uložených v počítačovém systému – poskytování součinnosti, nebo nahrazování činnosti orgánů činných v trestním řízení?*. Bulletin advokacie, 2019, č. 11, s. 36-39

²⁶⁹ Blíže bude předmět kritiky rozebrán níže v této práci.

²⁷⁰ Nejvýše však v délce 90 dní, srov. § 7b odst. 4 trestního řádu

činného v trestním řízení tato data uchovala, a to v nezměněné podobě. Popřípadě k nim znemožnila přístup jiným osobám a současně uchovala v tajnosti i informaci, že jí uchování dat bylo nařízeno. Takový příkaz je dle § 7b odst. 3 trestního řádu oprávněn vydat předseda senátu a v rámci přípravného řízení státní zástupce či policejní orgán, ten však potřebuje předchozí souhlas²⁷¹ státního zástupce. Příkaz, který je bezprostředně doručen osobě, vůči které povinnost směřuje, musí být náležitě odůvodněn včetně konkrétního označení dat, na které se uchování či znemožnění přístupu vztahuje a doby, pro kterou má být takto učiněno. Současně je třeba uvést, že ustanovení se týká jen dat již existujících, nelze tedy takto postupovat směrem k datům, která jsou *aktuálně přenášena* či budou *v budoucnu*.²⁷² Nižší procesní standardy, tj. možnost nařízení příkazu v přípravném řízení pouze ze strany policejního orgánu se souhlasem státního zástupce (či bez souhlasu, pokud se jedná o případ, kdy věc nenese odkladu), odůvodňuje Stupka a kol.²⁷³ pouhým zajišťováním integrity (nezměnitelnosti) dat, nikoliv jejich vydáním orgánu činném v trestním řízení.

V řadě odborné veřejnosti však ustanovení vyvolává obavy, a to právě s poukazem na *neúměrný zásah do základních práv a svobod osob*, když není nastavena dostatečná záruka v podobě naplnění nutných podmínek pro užití institutu jako je tomu např. u ustanovení § 88 či §88a trestního řádu. Těmi je mj. stanovena závažnost trestného činu, na který se dá nástroje užít, a to včetně úpravy případů, kdy se bude jednat o důvěrnost komunikace mezi obhájcem a klientem.²⁷⁴ Zákonodárce tímto staví držitele dat do pozice, kde musí *aktivně konat* namísto orgánů činných v trestním řízení, a to v podobě nakládání s daty, jelikož subjekt sám zasahuje do práv jiných osob a „*realizuje tak úkon trestního řízení, který může být v budoucnu využit při prokazování trestné činnosti konkrétních osob*“²⁷⁵. Vzhledem k tomu, že nejde pouze o uchování komunikace, ale i o možnost znemožnění přístupu, tj. faktického vypnutí určité aplikace, webové stránky (např. e-shopu) či emailové schránky, může být takovým zásahem způsobena vysoká škoda. Jako příklad uvádí Toman²⁷⁶ znemožnění přístupu do emailové schránky ve chvíli uzavírání obchodní transakce nebo v rámci soudního řízení blízké koncentrační či odvolací lhůty. Jiným vytykaným bodem jsou například i náklady

²⁷¹ Předchozí souhlas není vyžadován, pokud ho ze strany policejního orgánu nelze získat a současně tato věc nenese odkladu.

²⁷² Vláda: 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, č. 287/2018 Dz

²⁷³ STUPKA, V., PROVAZNÍK, J., VOSTOUPAL, J. *Elektronické důkazy jako výzva pro trestní proces*. Op. cit., s. 332-349

²⁷⁴ TOMAN, P. *Podstrčený paragraf § 7b trestního řádu. Kde se vzal a o čem je*. Op. cit.

²⁷⁵ NAVRÁTILOVÁ, J., GALOVCOVÁ, I. *Uchovávání dat uložených v počítačovém systému – poskytování součinnosti, nebo nahrazování činnosti orgánů činných v trestním řízení?*. Op. cit., s. 36-39

²⁷⁶ TOMAN, P. *Podstrčený paragraf § 7b trestního řádu. Kde se vzal a o čem je*. Op. cit.

na uchovávání dat, které vzhledem k možnosti uchovávání dat až po dobu 90 dní, nemusí být zanedbatelné.²⁷⁷

Dle autorek příspěvku týkajícího se zavedení ustanovení § 7b do trestního řádu je problémem aplikační praxe také následné získávání těchto zmrazených dat. Za využití institutu § 158d odst. 3 trestního řádu dochází k jejich vyžádání Útvarem zvláštních činností služby kriminální policie a vyšetřování, a s tím k obcházení zákonného postupu, jelikož je získáván obsah komunikace „za období předcházející době, po kterou je povoleno sledování, a to i bez toho, že by byl vydán příkaz k odposlechu“²⁷⁸. Odposlech však stanoví časové podmínky na omezenou šíři trestných činů, pro něž je možné ho uplatnit.²⁷⁹ Jak podotýká Zaoralová,²⁸⁰ ustanovení o odposlechu je k ustanovení o sledování osob a věcí speciální, a tedy použitelnost dat získaných za pomoci § 158d odst. 3 trestního řádu může mít vliv na použitelnost důkazu.

V závěru považuji za vhodné poukázat na odlišnost oproti institutu rozebranému v kapitole 2.3.2.1., *data retention*, které plošně uchovává data, jež jsou vytvářena *v přítomnosti*.²⁸¹ Uchování dat ve smyslu *data preservation* se vztahuje na konkrétně určená (již existující) data, po určenou dobu, přičemž cílem tohoto uchování je ochrana před změnou, zničením či ztracením dat a jejich následná možnost užití pro určité trestní řízení. Důvodová zpráva k novele dále uvádí, že uchování dat může být důležité zejména v boji proti kyberkriminalitě páchané s využitím internetu. Ačkoliv mají orgány činné v trestním řízení možnost zajistit data na místě, vzhledem k jejich lehké změnitelnosti, smazání či jiné manipulaci, může dojít k jejich zničení, a tedy ztrátě důkazního prostředku. Možnost zajištění dat přímo od správce dat v tomto ohledu tedy dle důvodové zprávy může hrát klíčovou roli.²⁸²

²⁷⁷ *Tamtéž.*

²⁷⁸ NAVRÁTILOVÁ, J., GALOVCOVÁ, I. *Uchovávání dat uložených v počítačovém systému – poskytování součinnosti, nebo nahrazování činnosti orgánů činných v trestním řízení?*. Op. cit., s. 36-39

²⁷⁹ *Tamtéž.*

²⁸⁰ ZAORALOVÁ, P. *Procesní použitelnost důkazů v trestním řízení a její meze*. Praha: Leges, 2018. ISBN 978-80-7502-310-0. s. 252

²⁸¹ § 97 odst. 3 zákona o elektronických komunikacích

²⁸² Vláda: 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, č. 287/2018 Dz

3. Mezinárodněprávní úprava elektronických důkazních prostředků

Tak jako je tomu na národní úrovni, i na mezinárodním poli je vzhledem k *povaze informačních a komunikačních technologií* více než žádoucí, aby existovala efektivní právní úprava, která nastaví právní rámec pro instituty spolupráce jednotlivých států při získávání *elektronických důkazních prostředků*. Souvisí to s povahou online prostředí, které nemá žádné státní hranice, propojením světa prostřednictvím sítě Internet a rychlostí, kterou se mohou data důležitá pro trestní řízení pohybovat včetně narůstajícího využívání cloudových úložišť.²⁸³ Oběťmi trestných činů mohou být velmi často osoby na území jiného státu, než kde se nachází data s trestním řízením související, podléhající na tomto základě jurisdikci jiného státu. Přihlédneme-li navíc k *nestálosti* elektronických důkazů, je více než žádoucí nastavení účinné vzájemné součinnosti mezi jednotlivými státy a jejich aktéry. Těmi budou nejen orgány činné v trestním řízení, ale také osoby soukromého práva, jako jsou např. poskytovatelé sociálních sítí či e-shopů nabízejících své služby v celosvětovém měřítku.

V případě úpravy týkající se *elektronických důkazních prostředků* na mezinárodní úrovni mluvíme zejména o Budapešťské úmluvě včetně Dodatkových protokolů,²⁸⁴ jež zavazuje mimo signatářské státy Rady Evropy i mnoho jiných států, které nejsou členy²⁸⁵ této mezinárodní organizace. Přestože Úmluva o kyberkriminalitě pochází již z roku 2001, Česká republika ji ratifikovala až v roce 2013²⁸⁶. Budapešťská úmluva je důležitým právním rámcem v oblasti elektronických důkazů, obsahuje výčet kybernetických trestných činů a současně procesní část zahrnující instituty, jimiž státy mohou tuto trestnou činnost stíhat. Druhou klíčovou mezinárodní organizací, jež zavádí pro své členské státy mezinárodněprávní nástroje v této věci, je Evropská unie. V oblasti unijního práva a kyberkriminality však nemůžeme mluvit o ucelené právní úpravě, ale spíše o jednotlivých nástrojích. Nejvýznamnějším institutem je bezesporu *evropský vyšetřovací příkaz* upravující zajišťování dat na území Evropské unie. Tento nástroj byl implementován do národního právního rámce zákonem o mezinárodní justiční spolupráci ve věcech trestních, a to na základě Směrnice o evropském vyšetřovacím příkazu²⁸⁷. Se zeměmi, které nejsou součástí Evropské unie

²⁸³ Cloudová úložiště často mění místo, kde se nacházejí, a to na základě vyvažování zátěže (z anglického „load balancing“). Tato změna umístění je automatizovaná a probíhá zcela bez rozhodnutí osob. Srov. SMEJKAL, V. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. ISBN 978-80-7380-849-5., s. 855

²⁸⁴ Oba dodatkové protokoly jsou rozebrány níže v kapitole 3.1 této práce.

²⁸⁵ Např. Spojené státy, Japonsko, Kanada, Austrálie či Kolumbie

²⁸⁶ Podepsala ji již v roce 2005.

²⁸⁷ Směrnice Evropského parlamentu a Rady 2014/41/EU ze dne 3. dubna 2014 o evropském vyšetřovacím příkazu v trestních věcech

je pro vykonání vyšetřovacích úkonů za hranicemi České republiky užíváno mechanismu mezinárodní právní pomoci, tento proces ve srovnání s využitím evropského vyšetřovacího příkazu však trvá mnohem déle.²⁸⁸ Za vhodné považuji zmínit i Smlouvu o vzájemné právní pomoci v trestních věcech²⁸⁹ uzavřenou mezi Českou republikou a Spojenými státy, která upravuje vzájemnou spolupráci při zajišťování důkazů a pro Českou republiku se stala závaznou v roce 2000. Po vstupu do Evropské unie a následném uzavření Dohody o vzájemné právní pomoci mezi Evropskou unií a Spojenými státy²⁹⁰ (s platností ke dni 1. února 2010), byla téhož roku mezi Českou republikou a Spojenými státy přijata Dodatková úmluva o vzájemné právní pomoci v trestních věcech²⁹¹.

V následujících podkapitolách budou charakterizovány jednotlivé mezinárodní instrumenty Rady Evropy a Evropské unie společně s výzvou, které čelí zcela nová právní úprava, jež byla poměrně nedávno přijata v souvislosti s Budapešťskou úmluvou²⁹² a také přijetím Nařízení o evropských vydávacích a uchovávacích příkazech²⁹³ jako dlouho připravovaný legislativní akt unijního práva. Krátce bude v souvislosti s elektronickými důkazy a unijním právem rozebrán i zákon Spojených států pro celosvětový přístup k datům, tzv. CLOUD Act. Výše nastíněnou úpravu o mezinárodní spolupráci v trestních věcech se Spojenými státy již blíže nerozebírám.

3.1. Rada Evropy a Budapešťská úmluva

Odborná literatura²⁹⁴ zabývající se problematikou kyberkriminality se shoduje na tom, že Budapešťská úmluva je na mezinárodní úrovni stěžejním, nejvýznamnějším a nejkompexnějším dokumentem v této oblasti. Budapešťská úmluva zavazuje signatářské

²⁸⁸ Zákon o mezinárodní justiční spolupráci ve věcech trestních

²⁸⁹ Sdělení č. 40/2000 Sb. m. s., Ministerstva zahraničních věcí o sjednání Smlouvy mezi Českou republikou a Spojenými státy americkými o vzájemné právní pomoci v trestních věcech

²⁹⁰ Sdělení č. 5/2010 Sb. m. s., Ministerstva zahraničních věcí o sjednání Dohody o vzájemné právní pomoci mezi Evropskou unií a Spojenými státy americkými

²⁹¹ Sdělení č. 7/2010 Sb. m. s., Ministerstva zahraničních věcí o sjednání Dodatkové úmluvy o vzájemné právní pomoci v trestních věcech mezi Českou republikou a Spojenými státy americkými

²⁹² Jedná se o druhý dodatkový protokol k Budapešťské úmluvě o posílené spolupráci a zpřístupnění elektronických důkazů, který přijala Rada Evropy a Evropská Unie zmocnila členské státy k jejímu přijetí, viz kapitola 3.1. této práce

²⁹³ Nařízení Evropského parlamentu a Rady (EU) 2023/1543 ze dne 12. července 2023 o evropském vydávacím příkazu a evropském uchovávacím příkazu pro elektronické důkazy v trestním řízení a pro výkon trestu odnětí svobody po skončení trestního řízení.

²⁹⁴ Např. SMEJKAL, V. *Kybernetická kriminalita*. Op. cit. s. 855-857; KOLOUCH, J. *CyberCrime*. Op. cit., s. 331-337; POLČÁK, R. a kol. *Právo informačních technologií*. Op. cit., s. 548-552; GRIVNA, T. a POLČÁK, R. *Kyberkriminalita a právo*. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4., s.193-220

státy²⁹⁵ k implementaci instrumentů²⁹⁶, jež budou účinně umožňovat postih trestných činů páchaných v *kyberprostoru*. Klade si za cíl sjednocení postupu ve stíhání definovaných trestných činů bez ohledu na to, kde ke spáchání trestného činu došlo. Polčák²⁹⁷ uvádí, že v rámci postupných Dodatkových protokolů má být tato jurisdikce dále rozšiřována, a to s ohledem na aktuální vývoj a dynamiku prostředí informačních a komunikačních technologií.

3.1.1. Oblast působnosti Budapešťské úmluvy

Budapešťská úmluva se skládá celkem ze 48 článků a je dělena do 4 kapitol, kterým předchází preambule. V kapitole I jsou vymezeny pojmy, které tato úmluva dále užívá, nalezneme zde definici *počítačového systému, počítačových dat, poskytovatele služby a provozních dat*. Kapitola II se dělí celkem na tři části, přičemž 1. část upravuje trestní právo hmotné, 2. část trestní právo procesní a 3. část se věnuje soudní pravomoci, to vše ve smyslu zaměření této úmluvy. Hmotněprávní úprava v 1. části mimo jiné²⁹⁸ definuje 4 kategorie skutkových podstat trestných činů, jejichž jednotné pojmenování si klade za cíl jejich účinné stíhání na území signatářských států. Jedná se jmenovitě o tyto kategorie skutkových podstat: *trestné činy proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů; trestné činy související s počítačem; trestné činy související s obsahem*²⁹⁹; *trestné činy týkající se porušení autorského práva a práv souvisejících s právem autorským*. Procesněprávní úprava je z hlediska této práce nejvýznamnější, jelikož upravuje procesní nástroje zajišťování a dalšího nakládání s elektronickými důkazy. Kapitola III upravuje mezinárodní spolupráci a dále se dělí na dvě části upravující obecné zásady a zvláštní ustanovení. Kapitola IV obsahuje závěrečné ustanovení zakotvující např. územní působnost, účinky samotné úmluvy, výhrady, urovnání sporů, porady či výpovědi. Budapešťská úmluva, konkrétně její hmotněprávní část zakotvující *trestné činy související s obsahem*, je na základě *Dodatkového protokolu*³⁰⁰ rozšířena

²⁹⁵ Aktuální seznam signatářských států Budapešťské úmluvy je dohledatelný na:

<https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatyid=185>

²⁹⁶ Na základě článku 14-21 Budapešťské úmluvy se signatářské státy zavázaly včlenit obsah a smysl této úmluvy, aby bylo na mezinárodní úrovni umožněno vyšetřování a objasňování tohoto typu trestných činů. Srov. KOLOUCH, J. *CyberCrime*. Op. cit., s. 332

²⁹⁷ POLČÁK, R. *Právo na internetu: spam a odpovědnost ISP*. Brno: Computer Press, 2007. ISBN 978-80-251-1777-4., s. 16

²⁹⁸ Obsažena je dále úprava pokusu, účastenství, odpovědnosti právnických osob, trestů a opatření.

²⁹⁹ Trestné činy související s dětskou pornografií

³⁰⁰ Sdělení č. 9/2015 Sb. m. s., Ministerstva zahraničních věcí o sjednání Dodatkového protokolu k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů

o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů.

Zaměříme-li se na *elektronické důkazní prostředky*, Budapešťská úmluva v tomto směru nastavuje konkrétní nástroje pro spolupráci mezi jednotlivými národy. Tyto mechanismy vychází především z multilaterálních a bilaterálních smluv o mezinárodní justiční spolupráci v trestních věcech a také z národních úprav. Negativním, avšak velmi častým jevem je zdlouhavý postup, který přeshraniční spolupráci v trestních věcech doprovází. Budapešťská úmluva se tedy snaží především o účinné nastavení a realizaci těchto nástrojů. Zakládá státům povinnost zakotvit do svého právního rámce pravidla, resp. procesní prostředky pro možnost spolupráce určitých orgánů v souvislosti s problematikou elektronických důkazů.³⁰¹ Jedná se především o *příkaz k předložení dat*³⁰², *urychlené uchování dat*³⁰³, *uchování a zpřístupnění provozních dat, prohlídku a zajištění*³⁰⁴, *shromažďování dat v reálném čase* či *odposlech obsahových dat*. Na základě článku 14 Budapešťské úmluvy se implementované nástroje užijí pro zajištění všech *důkazů v elektronické formě*.³⁰⁵ Vhodné je také zdůraznit úpravu pravidel pro určení jurisdikce, ta spočívá v užití principu personality či teritoriality, jež má být v souvislosti s územím a občany signatářských států aplikována pro trestné činy definované v Budapešťské úmluvě. Jak bylo naznačeno v úvodu této kapitoly, jedná se o případy přístupu k elektronickým důkazům nacházejícím se v jurisdikci odlišného státu, než je ten, který trestnou činnost vyšetřuje.³⁰⁶

3.1.2. Druhý dodatkový protokol

Poměrně nedávno, v květnu roku 2022, byl schválen a zpřístupněn k podpisu *Druhý dodatkový protokol* k Budapešťské úmluvě o kyberkriminalitě o posílené spolupráci a zpřístupnění elektronických důkazů³⁰⁷ (dále i jen „druhý dodatkový protokol“), který

³⁰¹ STUPKA, V., PROVAZNÍK, J., VOSTOUPAL, J. *Elektronické důkazy jako výzva pro trestní proces*. Op. cit., s. 336

³⁰² Na jeho základě je umožněno orgánům činným v trestním řízení vyžadovat data od držitelů. Srov. POLČÁK, R. a kol. *Právo informačních technologií*. Op. cit., s. 550

³⁰³ Tzv. *freezing order*, jehož prostřednictvím poskytovatelé služeb uchovají integritu konkrétních dat pro následné vyžádání ze strany orgánu činných v trestním řízení. V národní úpravě je tato povinnost provedena ustanovením § 7b trestního řádu.

³⁰⁴ V případech, kdy je více účinné, aby byla data analyzována přímo poskytovateli. Srov. POLČÁK, R. a kol. *Právo informačních technologií*. Op. cit., s. 550

³⁰⁵ Čl. 14 odst. 2 písm. c) Budapešťské úmluvy

³⁰⁶ STUPKA, V., PROVAZNÍK, J., VOSTOUPAL, J. *Elektronické důkazy jako výzva pro trestní proces*. Op. cit. s. 336-337

³⁰⁷ Druhý dodatkový protokol k Budapešťské úmluvě o posílené spolupráci a zpřístupnění elektronických důkazů, k nahlédnutí zde: <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treaty-num=224> ; v českém jazyce zde: <https://data.consilium.europa.eu/doc/document/ST-14898-2021-INIT/cs/pdf>

vypracovala pracovní skupina sestavená Výborem signatářských států Budapešťské úmluvy.³⁰⁸ Cílem druhého dodatkového protokolu je zejména efektivnější nastavení spolupráce mezi státy, přímé spolupráce s poskytovateli služeb v jiných státech, které jsou smluvními stranami,³⁰⁹ a současně s tím i posílení záruk a ochrana osobních údajů.³¹⁰ Pro urychlení získávání informací o účastnících a provozních údajích se ve směru k dožadovaným státům a poskytovatelům služeb zavádí lhůty.³¹¹ Pro zrychlené zpřístupnění počítačových dat v případech mimořádných událostí se zavádí signatářským státům povinnost do právního řádu zakotvit a funkčně zabezpečit vznik „kontaktních míst“ fungujících 24 hodin denně 7 dní v týdnu, kam se mohou obracet „kontaktní místa“ jiného smluvního státu pro okamžitou pomoc.³¹² Dalšími body tohoto dodatkového protokolu jsou možnost využití videokonferenčního zařízení pro výpověď svědka či znalce³¹³ či vznik společných vyšetřovacích týmů³¹⁴ pro usnadnění a zefektivnění trestního řízení.

Vzhledem k tomu, že Evropská unie nemůže být sama smluvní stranou, přijala Evropská rada³¹⁵ dne 12. února 2023 rozhodnutí³¹⁶, kterým zmocnila členské státy k podpisu druhého dodatkového protokolu. Ve kterém mj. uvedla, že vhodnost přijetí tohoto dodatkového protokolu spočívá v jeho celosvětové aplikaci a vysoké úrovni ochrany osob ve smyslu ochrany osobních údajů.³¹⁷ V současnosti podepsalo tento druhý dodatkový protokol již 43 států³¹⁸ včetně Belgie, Nizozemska, Německa, Francie, Kanady, Japonska či Spojených států. Česká republika ke dni odevzdání této diplomové práce k druhému dodatkovému protokolu prozatím nepřistoupila. V oblasti mezinárodní spolupráce je dodatkový protokol zabývající se přeshraničním přístupem k elektronickým důkazům bezpochyby velkým přínosem. Dosavadní postupy v rámci mezinárodní justiční spolupráce jsou velmi zdlouhavé, a tudíž

³⁰⁸ Cybercrime Convention Committee (T-CY)

³⁰⁹ Velmi často jsou získávány údaje k uživatelským účtům, tzn. např. k IP adresám, emailovým schránkám, doménám. Srov. STUPKA, V., PROVAZNÍK, J., VOSTOUPAL, J. *Elektronické důkazy jako výzva pro trestní proces*. Op. cit. s. 337

³¹⁰ MINÁRIK, T. *Council of Europe Ponders a New Treaty on Cloud Evidence*. CCDCOE, www.ccdcoe.org [online]. 2017 [cit. 23. 1. 2024]. Dostupné z: <https://ccdcoe.org/incyber-articles/council-of-europe-ponders-a-new-treaty-on-cloud-evidence/>

³¹¹ Srov. čl. 8 odst. 6 písm. a) druhého dodatkového protokolu

³¹² Srov. čl. 9 druhého dodatkového protokolu

³¹³ Srov. čl. 11 druhého dodatkového protokolu

³¹⁴ Srov. čl. 12 druhého dodatkového protokolu

³¹⁵ Evropská rada jakožto instituce Evropské unie určuje její priority a politické směřování.

³¹⁶ Rozhodnutí Rady (EU) 2023/436 ze dne 14. února 2023, kterým se členské státy zmocňují, aby v zájmu Evropské unie ratifikovaly Druhý dodatkový protokol k Úmluvě o počítačové kriminalitě o posílené spolupráci a zpřístupňování elektronických důkazů, 32023D0436

³¹⁷ RADA EU, *Přístup k elektronickým důkazům: Rada zmocnila členské státy k podpisu mezinárodní dohody*. Tisková zpráva, www.consilium.europa.eu. [online]. 2022 [cit. 23. 1. 2024] Dostupné z: <https://www.consilium.europa.eu/cs/press/press-releases/2022/04/05/access-to-e-evidence-council-authorises-member-states-to-sign-international-agreement/>

³¹⁸ Seznam signatářských států je k náhledu zde: <https://www.coe.int/en/web/cybercrime/second-additional-protocol>

nedostatečně efektivní, zejména přihlédneme-li k vývoji moderních technologií. Časová náročnost procesu získávání elektronických důkazů může ohrozit celé trestní řízení, jelikož není ojedinělé, že dojde k znehodnocení takového důkazu, a tedy k jeho nepoužitelnosti. Lze shrnout, že stávající úprava vzájemné pomoci států v trestních věcech nestíhá dostatečně reagovat na výzvy, které nové technologie přináší. Vznik a přijetí druhého dodatkového protokolu je tak dle mého názoru vhodným krokem kupředu, který může mít zásadní vliv na efektivitu stíhání trestných činů vyžadujícího přeshraniční spolupráci.

3.2. Právo Evropské unie

Unijní úprava v souvislosti se sjednocením a zefektivněním zajišťování a jiným nakládáním s elektronickými důkazy v rámci trestního řízení přijala postupně několik právních instrumentů. Vzhledem k charakteru kyberprostoru je nezbytné, aby byl nastaven mechanismus, jež reaguje na narůstající digitalizaci doby. Postupně budou představeny nástroje, které Evropská unie zavádí, a jež mají souvislost s meritem této práce. Bude tedy rozebrán *evropský vyšetřovací příkaz*, *evropský vydávací příkaz*³¹⁹ a *evropský uchovávací příkaz*, mimo to bude představen institut *společného vyšetřovacího týmu*.

3.2.1. Evropský vyšetřovací příkaz

Evropský vyšetřovací příkaz byl zaveden na základě Směrnice o evropském vyšetřovacím příkazu³²⁰ z roku 2014 a ze strany České republiky byl implementován do zákona o mezinárodní justiční spolupráci ve věcech trestních novelou zákon č. 178/2018 Sb. Jedná se o nástroj, který je vydán k provedení určitých vyšetřovacích úkonů včetně získání důkazů v jiném členském státě, než je členský stát, jehož jurisdikci podléhá justiční orgán, který příkaz vydal (a trestní řízení vede). Tedy v případě, kdy je v rámci trestního řízení žádoucí či nezbytné získat důkazy nesoucí v sobě přeshraniční prvek³²¹, je tímto nástrojem umožněno získat důkazy z jiného členského státu zjednodušeně, a to za pomoci k tomu určeného standardizovaného formuláře.³²²

³¹⁹ Poznámka autorky: V návrhu nařízení a odborné literatuře (z doby před přijetím nařízení) se mluví o *evropském předávacím příkazu*, v oficiálním překladu do českého jazyka na stránkách <https://eur-lex.europa.eu> je již v textu nařízení uváděn *evropský vydávací příkaz*. Jedná se však o ten samý institut (anglický pojem „*European Production Order*“ je beze změny) a pro účely této práce pracuji jen s tímto pojmem. Blíže k tomuto v závěru podkapitoly 3.2.

³²⁰ Směrnice Evropského parlamentu a Rady 2014/41/EU ze dne 3. dubna 2014 o evropském vyšetřovacím příkazu v trestních věcech¹

³²¹ Např. informace o uživateli emailové schránky, obsah zpráv z Messengeru

³²² STAŇKOVÁ, P. *Vyšetřování kybernetické kriminality a její budoucí předpokládaný vývoj*. Revue pro právo a technologie, 2023, č. 28, s. 31-60

Příkaz je možné užít pro velkou škálu vyšetřovacích úkonů, nelze však jeho pomocí realizovat *společný vyšetřovací tým*³²³. Současně se musí jednat o případy, kdy je pro vyšetřovací úkon dána nezbytnost, přiměřenost a obdobná použitelnost ve vnitrostátních případech.³²⁴ Jak uvádí Polčák,³²⁵ evropský vyšetřovací příkaz může eliminovat určité formality zdržující tyto vyšetřovací úkony, a to s ohledem na princip vzájemného uznávání mezi členskými státy. Další okolností, která má možnost urychlit procesní úkon, je povinnost vykonávajícího státu přistupovat k příkazu nediskriminačně, tj. stejně jako k vlastnímu rozhodnutí, a nemožnost odložit či odmítnout výkon příkazu až na konkrétně vymezené případy. K efektivitě přispívají i současně jasně nastavené lhůty³²⁶, které musí být pro uznání a výkon příkazu naplněny.

Z hlediska odlišnosti jurisdikcí jednotlivých členských států v oblasti trestního práva a úpravy zajišťování důkazů, není však fungování tohoto institutu bezproblémové. Dožádaný členský stát se musí (neodporuje-li to základním zásadám) „řídít formálními náležitostmi a postupy výslovně uvedenými dožadujícím členským státem“³²⁷ vycházejícími z Úmluvy o vzájemné pomoci v trestních věcech mezi členskými státy Evropské unie.³²⁸ Přestože se tato zásada promítá i do nástrojů³²⁹ jako je právě evropský vyšetřovací příkaz, a v tomto ohledu si tedy dožadující stát může stanovit podmínky provedení úkonu, neexistují zde žádná transparentní pravidla ani zavedený „minimální standard“. To vede mezi jednotlivými státy k rozdílům ve vyhodnocení, a s tím vyvstává i otázka (ne)přípustnosti takto získaných důkazů. Ta byla členskými státy v mnoha případech napadena. Důvodem, kdy bylo rozhodnuto

³²³ STUPKA, V., PROVAZNÍK, J., VOSTOUPAL, J. *Elektronické důkazy jako výzva pro trestní proces*. Op. cit. s. 339

³²⁴ EUROPEAN E-JUSTICE: Evropský vyšetřovací příkaz, vzájemná právní pomoc a společné vyšetřovací týmy, e-justice.europa.eu [online]. 2019 [cit. 24. 1. 2024], Dostupné z: https://e-justice.europa.eu/content_european_investigation_order_mutual_legal_assistance_and_joint_investigation_teams-92-cs.do

³²⁵ POLČÁK, R. a kol. *Právo informačních technologií*. Op. cit., s. 552

³²⁶ Po posouzení naplnění podmínek pro výkon příkazu činí justiční orgán v souladu se lhůtou v tomto příkazu uvedenou, jinak bezodkladně a nejpozději do 30 dnů od obdržení příkazu. Pokud justiční orgán nemůže tyto lhůty naplnit, musí bezodkladně informovat žádající členský stát, a to včetně odůvodnění a uvedení předpokládané doby. Pro provedení vyžadovaného úkonu je stanovena lhůta 90 dnů. Srov. zákon o mezinárodní justiční spolupráci ve věcech trestních

³²⁷ Sdělení č. 55/2006 Sb. m. s. Ministerstva zahraničních věcí o přístupu České republiky k Úmluvě o vzájemné pomoci v trestních věcech mezi členskými státy Evropské unie, vypracované Radou na základě článku 34 Smlouvy o Evropské unii čl. 4 odst. 1

³²⁸ *Tamtéž*.

³²⁹ STUPKA, V. *Vzájemná přípustnost elektronických důkazů v EU*. Přednáška. Brno: MUNI LAW, 14. 9. 2023, MUNI LAW, Masarykova univerzita Právnická fakulta. [online]. 2023 [cit. 24. 1. 2024]. Dostupné z: <https://cpit.law.muni.cz/dokumenty/60446>

o nepřipustnosti je např. nedostatečná informace pro posouzení proporcionality (Německo) či neexistence ekvivalentního procesního nástroje (Nizozemsko; Německo).³³⁰

3.2.2. Evropský vydávací příkaz a evropský uchovávací příkaz

Evropský vydávací příkaz a evropský uchovávací příkaz jsou nově přijatými instituty na základě Nařízení Evropského parlamentu a Rady (EU) 2023/1543 ze dne 12. července 2023³³¹ (dále i jen „Nařízení o evropském vydávacím příkazu a evropském uchovávacím příkazu“). Tyto mechanismy mají zrychlit a usnadnit získávání elektronických důkazů a zabránit jejich smazání. Jejich cílem není nahradit *evropský vyšetřovací příkaz*, ale poskytnout policejním a justičním orgánům další nástroj, který umožní přístup k důkazům v elektronické podobě v rámci celé Evropské unie, a to *přímo od poskytovatelů služeb*. Hlavním přínosem by měla být lepší funkce spolupráce mezi orgány členských států a poskytovateli služeb usídlenými mimo území Evropské unie. Poskytovatelé služeb na internetu velmi často ukládají údaje související s uživateli služby na serverech, jež se nachází v řadě států (v rámci Evropské unie i mimo ni), což orgánům činným v trestním řízení podstatně ztěžuje jejich získávání.³³² Důvodová zpráva k návrhu nařízení³³³ se odkazuje na nestálou povahu elektronických důkazů a snaží se tímto nařízením, s ohledem na zachování vysokých standardů ochrany základních lidských práv, nastavit účinné mechanismy. Nařízení má být použitelné od 18. srpna 2026, tj. 36 měsíců po jeho vstupu v platnost (do stejného data musí být implementována doprovázející Směrnice (EU) 2023/1544³³⁴).

Na základě obou nových příkazů mohou příslušné vydávající orgány přímo žádat poskytovatele služeb, na které se bude vztahovat nařízení³³⁵, tj. poskytovatele nabízející své služby v Evropské unii včetně těch, kteří zde nejsou usazeni.³³⁶ V souladu

³³⁰ STUPKA, Václav. *Vzájemná přípustnost elektronických důkazů v EU*. Op. cit.

³³¹ Nařízení Evropského parlamentu a Rady (EU) 2023/1543 ze dne 12. července 2023 o evropském vydávacím příkazu a evropském uchovávacím příkazu pro elektronické důkazy v trestním řízení a pro výkon trestu odnětí svobody po skončení trestního řízení.

³³² RADA EU, *Rada přijala právní předpisy EU o lepším přístupu k elektronickým důkazům*. Tisková zpráva, www.consilium.europa.eu/. [online]. 2023 [24. 1. 2024]. Dostupné z: <https://www.consilium.europa.eu/cs/press/press-releases/2023/06/27/council-adopts-eu-laws-on-better-access-to-electronic-evidence/>

³³³ Důvodová zpráva k návrhu nařízení Evropského parlamentu a Rady o evropských vydávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech, COM (2018) 225 final; 2018/0108 (COD). Štrasburk, [online]. 2018 [cit. 24. 1. 2024]. Dostupné z: https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0017.02/DOC_1&format=PDF

³³⁴ Směrnice Evropského parlamentu a Rady (EU) 2023/1544 ze dne 12. července 2023, kterou se stanoví harmonizovaná pravidla pro určování určených provozoven a jmenování zástupců za účelem shromažďování elektronických důkazů v trestním řízení.

³³⁵ SMEJKAL, V. *Kybernetická kriminalita. 3. rozšířené a aktualizované vydání*. Op. cit. s. 856-857

³³⁶ Čl. 2 Nařízení o evropském vydávacím příkazu a evropském uchovávacím příkazu

s článkem 3 odst. 3 nařízení jsou jimi poskytovatelé služeb nabízející: *služby elektronické komunikace, služby informační společnosti* (umožňující vzájemnou komunikaci mezi uživateli; umožňující uchování či jiné zpracování údajů jménem uživatele a toto uchovávání údajů je hlavní složkou poskytované služby) a *služby názvů internetových domén a číslování adres internetového protokolu*.³³⁷ Nevztahuje se však na poskytovatele finančních služeb a poskytovatele, kteří poskytují služby výhradně ve svém členském státu.³³⁸ Nařízení nezapomíná ani na definici samotných elektronických důkazů, jimiž rozumí: „*údaje o účastníkovi, údaje o provozu nebo údaje o obsahu uložené poskytovatelem služeb nebo jeho jménem v elektronické podobě v době doručení certifikátu*.“³³⁹

Příkazy k vydání či uchování elektronických důkazů musí být předány adresátovi, tj. přímo určené provozovně nebo konkrétně určenému zástupci (ten bude muset být fyzicky přítomen v Evropské unii)^{340,341}, a to na základě certifikátu, resp. certifikátu evropského vydávacího příkazu (EPOC) a certifikátu evropského uchovávacího příkazu (EPOC-PR).³⁴² Odpovědnost za nevyhovění příkazu nese současně provozovna (nebo právní zástupce) a samotný poskytovatel služeb. Nařízení dále zakládá členským státům povinnost zavést peněžité sankce pro případy nesplnění této povinnosti a současně přijmout opatření zajišťující uplatňování nařízení.³⁴³

Evropský vydávací příkaz

Evropský vydávací příkaz nastavuje povinnost poskytovatele předat vyžádané údaje do 10 dnů, není-li určena dřívější doba, v naléhavých případech je tato doba zkrácena dokonce na 8 hodin.³⁴⁴ Aby mohl být vydávací příkaz příslušným orgánem vydán, je nutné naplnění určitých podmínek. Příkaz musí být pro účely řízení nezbytný a přiměřený, zohledňovat práva osoby, již se vyžadované údaje týkají. Současně musí být možné vydat takový příkaz za stejných podmínek ve státu vydávacího orgánu. Dále jsou stanoveny konkrétní požadavky týkající se závažnosti trestných činů, popř. výkonu trestu odnětí svobody či ochranného opatření, pro které je možné příkaz vydat. Tyto požadavky jsou odlišeny dle toho, zda se příkaz

³³⁷ Čl. 3 odst. 3 *Tamtéž*.

³³⁸ Summaries of EU Legislation, *Elektronické důkazy v trestním řízení*. 17. 11. 2023. In: EUR-Lex [online]. 2023 [cit. 24. 1. 2024]. Dostupné z: <https://eur-lex.europa.eu/CS/legal-content/summary/electronic-evidence-in-criminal-proceedings.html?fromSummary=23>

³³⁹ Čl. 3 odst. 8 Nařízení o evropském vydávacím příkazu a evropském uchovávacím příkazu

³⁴⁰ Čl. 7 ve spojení s čl. 3 odst. 5, odst. 6, odst. 7 *Tamtéž*.

³⁴¹ Pro harmonizaci pravidel jmenování právních zástupců bude sloužit Směrnice (EU) 2023/1544

³⁴² Čl. 9 a čl. 7 Nařízení o evropském vydávacím příkazu a evropském uchovávacím příkazu

³⁴³ Preambule bod (69) a čl. 15 *Tamtéž*.

³⁴⁴ Čl. 10 odst. 1, odst. 3 *Tamtéž*.

týká vydání údajů o účastníkovi (včetně údajů výhradně k identifikaci účastníka)³⁴⁵, nebo zda jsou požadovány údaje o provozu či obsahové údaje³⁴⁶. Důležité je také zmínit, že nařízení ve svém článku 12 stanoví i důvody, pro které je možné, aby vydání žádaných údajů bylo odmítnuto. Současně pak stanoví vydávajícímu orgánu, aby informoval osobu, jejíž údaje byly vyžadovány, a to bezprostředně po tomto úkonu. Je však možné tuto informační povinnost odložit, a to v případech, kdy by informace ohrozila další vyšetřování trestné činnosti.³⁴⁷ Osoba, o jejíž údaje se jednalo, má pak možnost napadnout zákonnost, popřípadě přiměřenost a nezbytnost vydaného příkazu u justičního orgánu vydávajícího státu.³⁴⁸

Evropský uchovávací příkaz

Při žádosti o uchování (nesmazání) údajů na základě evropského uchovávacího příkazu, je stanovena doba této povinnosti po 60 dnů. Je-li to nezbytné (pro pozdější získání údajů na základě žádosti o vydání) a požádá-li vydávající orgán o prodloužení této doby, uchová adresát údaje po dalších 30 dnů. Pokud bude ze strany vydávajícího orgánu potvrzeno, že byla podána žádost o vydání, uchování bude trvat tak dlouho, dokud to k jejich vydání bude nezbytné. Pokud vydávající orgán již nepovažuje za nutné, aby byly údaje uchovávány, bezprostředně o této skutečnosti adresáta informuje.³⁴⁹ Obdobně jako je tomu u druhého příkazu, i zde musí být naplněny podmínky pro umožnění jeho vydání. Tyto podmínky jsou však ve srovnání s evropským vydávacím příkazem nastaveny mírněji. Příkaz musí naplňovat nezbytnost a přiměřenost pro zabránění odstranění, smazání či změně údajů, aby mohl být později uplatněn jiný (další) postup³⁵⁰, a to se zohledněním práv osoby, o jejíž údaje jde. Umožněno je ho vydat pro stíhání všech trestných činů a specifikovány jsou podmínky u jeho vydání pro případ výkonu trestu odnětí svobody či ochranného opatření.³⁵¹

3.2.2.1. Kritické zhodnocení nově přijaté legislativy

V důvodové zprávě k návrhu nařízení uváděno, že zachovává práva osob, kterých se nařízení bude dotýkat. Mám za to, že záruky nejsou nastaveny dostatečně,

³⁴⁵ Čl. 5 odst. 3 *Tamtéž.*; Příkaz je možné vydat u všech trestných činů. Dále jsou konkretizovány podmínky pro případ výkonu trestu odnětí svobody a ochranných opatření.

³⁴⁶ Čl. 5 odst. 4 *Tamtéž.*; Příkaz je možné vydat pro trestné činy páchané pomocí informačního systému vymezené na základě konkrétních směrnic, trestné činy související s bojem proti terorismu (směrnice EU 2017/541), v ostatních případech pro trestné činy (ve vydávajícím státě) postihnutelných trestem odnětí svobody s horní hranicí nejméně 3 roky. Dále jsou konkretizovány podmínky pro případ výkonu trestu odnětí svobody a ochranných opatření.

³⁴⁷ Čl. 13 *Tamtéž.*

³⁴⁸ Čl. 18 *Tamtéž.*

³⁴⁹ Čl. 11 odst. 1 *Tamtéž.*

³⁵⁰ Evropský vydávací příkaz, evropský vyšetřovací příkaz či vzájemná právní pomoc

³⁵¹ Čl. 3 odst. 6 Nařízení o evropském vydávacím příkazu a evropském uchovávacím příkazu

a to i s ohledem na okolnost, že se tyto přeshraniční žádosti týkají více než 50 % trestních stíhání³⁵², jak uvádí sama Rada EU. Již v průběhu legislativního procesu se k nedostatečným zárukám kriticky vyjadřoval Evropský inspektor ochrany osobních údajů.³⁵³ Zajištění elektronických důkazů, např. textových zpráv, emailů či údajů o provozu, je přitom klíčové při vyšetřování až 85 % trestné činnosti³⁵⁴ v rámci Evropské Unie. Právě s přihlédnutím k této skutečnosti by měl být unijní zákonodárce opatrný a dbát na ochranu základních práv jedince. Výše uvedené právní nástroje jsou poskytovány ze strany soudních orgánů vydávajícího státu. Ochrana údajů, které jsou o osobách shromažďovány, se v nařízení však omezuje především na případy *evropských vydávacích příkazů*. Naopak elektronické důkazy shromážděné na základě *evropského uchovávacího příkazu* zůstávají mimo oblast působnosti opravných prostředků s odůvodněním, že samy o sobě nevedou ke zpřístupnění údajů příslušnému orgánu (popřípadě po jejich zajištění na základě evropského vydávacího příkazu, je tento přezkum umožněn skrze ustanovení k tomuto příkazu). Domnívám se však, že tento argument není dostatečný a unijní zákonodárce měl i v případě uchování údajů přijmout vyšší záruky procesní obrany.

Jak správně podotýká Topalnakos³⁵⁵, nemělo by se přehlížet, že poskytovatel služeb může mít podle svých vnitrostátních právních předpisů povinnost smazat nebo omezit zpracování údajů, o jejichž uchování bylo požádáno na základě *evropského uchovávacího příkazu*. Uchovávání takových údajů by tak vedlo k porušení práv osob ve smyslu článku 6 a 7 Listiny EU, tj. práva respektování soukromého a rodinného života a práva na ochranu osobních údajů.³⁵⁶ Navíc je třeba neopomenout, že nařízením je umožněno prodloužení uchování údajů fakticky na *dobu neurčitou*, když nestanoví žádnou nejzazší dobu, po kterou by od uchování muselo být vždy upuštěno.³⁵⁷ I tyto okolnosti tak shledávám za problematické.

Problematický mi přijde i oficiální překlad nařízení, který mluví o *evropském vydávacím příkazu*. Zatímco doposud se v překladu návrhu a současně pak i ve všech odborných

³⁵² RADA EU, *Rada přijala právní předpisy EU o lepším přístupu k elektronickým důkazům*. Op. cit.

³⁵³ EDPS, *EDPS Opinion on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters*. Opinion 7/2019., 6. listopadu 2019. [online]. 2019 [cit. 24. 1. 2024]. Dostupné z: https://edps.europa.eu/sites/default/files/publication/19-11-06_opinion_on_e_evidence_proposals_en.pdf

³⁵⁴ Summaries of EU Legislation, *Elektronické důkazy v trestním řízení*. Op. cit.

³⁵⁵ TOPALNAKOS, P, *Critical Issues in the New EU Regulation on Electronic Evidence in Criminal Proceedings*. Eucrim 2023/2 [online]. 2023 [24. 1. 2024] s. 200-203, Dostupné z: https://eucrim.eu/media/issue/pdf/eucrim_issue_2023-02.pdf#page=94

³⁵⁶ Listina EU

³⁵⁷ Srov. čl. 11 odst. 2 Nařízení o evropském vydávacím příkazu a evropském uchovávacím příkazu

publikacích³⁵⁸ a člancích³⁵⁹, které vedly diskuzi nad přijetím tohoto nařízení, uváděl *evropský předávací příkaz*³⁶⁰, po přijetí nařízení došlo ke změně. V anglické verzi návrhu nařízení i nařízením samotném se přitom název nijak nemění a zůstává zachován jako *European Production Order*. Bude tedy vhodné, aby český zákonodárce v rámci adaptace nařízení do vnitrostátního práva přistupoval k tomuto pojmenování s ohledem na smysl a účel tohoto příkazu. Pojmy „vydání“ a „předání“ jsou ve světle mezinárodní justiční spolupráce ve věcech trestních chápány rozdílně.

V závěru je nutné shrnout, že ačkoliv je vhodné, aby došlo k větší efektivitě spolupráce orgánů činných v trestním řízení mezi členskými státy s možností přímého kontaktování poskytovatelů služeb, nemělo by tím být neproporcionálně zasahováno do základních práv a svobod jednotlivců. Současně by jim měly být poskytnuty dostatečné záruky k možnosti obrany před možným nezákonným či nepřiměřeným zásahem.

3.2.3. Společné vyšetřovací týmy

V případech časově náročných a složitých přeshraničních trestných činů je klíčová rychlost a účinnost takového vyšetřování. Společný vyšetřovací tým je tak na poli Evropské unie dalším nástrojem přeshraniční spolupráce v trestních věcech. Pravidla stanovující podmínky pro jejich zřízení a fungování jsou upraveny Rámcovým rozhodnutím Rady (2002/465/SVV).³⁶¹ Tyto vyšetřovací týmy jsou zřizovány na základě písemné dohody na dobu 12 až 24 měsíců. Tvoří jej orgány činné v trestním řízení, jako jsou soudci a státní zástupci, z několika členských států. Cílem je přímá spolupráce a komunikace mezi orgány, tj. vyměňování důkazů a informací či sdílení zkušeností a technického vybavení v reálném čase a provádění společných vyšetřovacích operací. Eurojust uvádí, že se jedná o nejefektivnější metodu, jak se vypořádat se zvýšenou sofistikovaností organizované trestné činnosti.³⁶² Společný vyšetřovací tým byl zřízen například v souvislosti s válkou na Ukrajině pro vyšetřování válečných zločinů, a s tím spojeným shromažďováním (elektronických)

³⁵⁸ Srov. SMEJKAL, V. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Op. cit. s. 856-857

³⁵⁹ Srov. STUPKA, V., PROVAZNÍK, J., VOSTOUPAL, J. *Elektronické důkazy jako výzva pro trestní proces*. Op. cit. s. 338-340; STAŇKOVÁ, P. *Vyšetřování kybernetické kriminality a její budoucí předpokládaný vývoj*. Op. cit., s. 31-60

³⁶⁰ Srov. anglická verze *návrhu nařízení* k nahlédnutí zde: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN> ; anglická verze *nařízení* k nahlédnutí zde: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1543&qid=1706106309143>

³⁶¹ Rámcové rozhodnutí Rady ze dne 13. června 2002 o společných vyšetřovacích týmech (2002/465/SVV)

³⁶² European Union Agency For Criminal Justice Cooperation. *Joint investigation teams*. In: eurojust.europa.eu. [online]. [cit. 24. 1. 2024]. Dostupné z: <https://www.eurojust.europa.eu/judicial-cooperation/eurojust-role-facilitating-judicial-cooperation-instruments/joint-investigation-teams>

důkazů a předávání odpovědných osob. Mezi prvními státy tohoto vyšetřovacího týmu byly Ukrajina, Litva a Polsko.³⁶³ Současně je vhodné zmínit, že výhodou vzniku společných vyšetřovacích týmů je i finanční podpora poskytovaná Eurojustem, popř. jinými agenturami Evropské unie, snižující dopad nákladů vzniklých v důsledku nadnárodního rozměru vyšetřování.³⁶⁴ Tento institut považuji v době propojeného světa za velmi užitečný nástroj, jak efektivně potírat přeshraniční trestnou činnost a mimo jiné získat přístup k elektronickým důkazům.

3.3. CLOUD Act

Kongres Spojených států přijal v březnu roku 2018 zákon, který v souvislosti s vyšetřováním trestné činnosti³⁶⁵ umožňuje vnitrostátním orgánům urychleně získat údaje přímo od amerických poskytovatelů služeb, bez ohledu na to, kde jsou tato data uložena, tzv. CLOUD Act (The Clarifying Lawful Overseas Use of Data Act).³⁶⁶ Tento zákon má dvě části, v *první části* je stanovena poskytovatelům povinnost uchovávat a předkládat údaje nehledě na to, kde se nacházejí, a *druhá část* dává Spojeným státům oprávnění uzavírat tzv. *executive agreements* neboli výkonné dohody s dalšími státy.³⁶⁷ Uzavřením dohody je zahraničním státům umožněn³⁶⁸ přístup k elektronickým důkazům od poskytovatelů služeb sídlících ve Spojených státech, nacházejícím se (fyzicky na serverech) kdekoli na světě. CLOUD Act tímto rozšiřuje geografickou působnost již dříve přijatého zákona Stored Communications Act.³⁶⁹ Poskytovatelé jsou na základě této dohody zavázáni k povinnosti plnit příkazy směřující ke zpřístupnění údajů, a to za současné ochrany soukromí a práv osob.³⁷⁰

³⁶³ European Union Agency For Criminal Justice Cooperation. *Joint investigation team into alleged crimes committed in Ukraine*. In: eurojust.europa.eu. [online]. [cit. 24. 1. 2024]. Dostupné z: <https://www.eurojust.europa.eu/joint-investigation-team-alleged-crimes-committed-ukraine>

³⁶⁴ European Union Agency For Criminal Justice Cooperation. *Joint investigation teams*. Opt. cit.

³⁶⁵ Zejména v souvislosti s vyšetřováním závažné trestné činnosti jako je terorismus, násilná trestná činnost, sexuální zneužívání dětí včetně trestné činnosti související s kyberkriminalitou

³⁶⁶ V této souvislosti je vhodné zmínit případ *United States v. Microsoft Corp. (Microsoft Ireland)*. Jednalo se o zajištění údajů z uživatelských účtů osob podezřelých z trestné činnosti. Tyto účty provozovala společnost Microsoft a údaje byly uloženy na serverech, které se fyzicky nacházely na území Irska. S tímto argumentem je odmítla společnost vydat. V průběhu byl však přijat zákon CLOUD Act, který vnitrostátním orgánům umožnil údaje získat bez ohledu na jurisdikci jejich fyzického umístění. Srov. Rozhodnutí Nejvyššího soudu Spojených států ve věci *United States v. Microsoft Corp. (Microsoft Ireland)*, z 17. 4. 2018. No. 17-2

³⁶⁷ Office of International Affairs. *CLOUD Act Resources*. In: www.justice.gov. [online]. [cit. 25. 1. 2024]. Dostupné z: <https://www.justice.gov/criminal/cloud-act-resources>

³⁶⁸ Na základě vzájemnosti

³⁶⁹ SMEJKAL, V. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Op. cit. s. 855

³⁷⁰ European Union Agency For Criminal Justice Cooperation. *The CLOUD Act*. In: eurojust.europa.eu. [online]. [cit. 25. 1. 2024]. Dostupné z: <https://www.eurojust.europa.eu/publication/cloud-act>

Uvedená výkonná dohoda byla podepsána s Austrálií³⁷¹ a Spojeným královstvím,³⁷² vyjednávání kromě Evropské unie započalo s Kanadou. V následujících odstavcích bude charakterizován vztah mezi zákonem CLOUD Act a Evropskou Unií. Bude podrobně rozebráno, jakým způsobem tento zákon upravuje předávání elektronických údajů. Zároveň budou zdůrazněny klíčové body, které vedou k tomu, že přijetí CLOUD Act vyvolává poměrně velké kontroverze a diskuse.

3.3.1. Efektivnější přístup k elektronickým důkazům?

Americká vláda odůvodnila přijetí tohoto aktu dramaticky vysokým nárůstem žádostí zahraničních států o vzájemnou právní pomoc, týkající se právě žádostí o elektronické důkazy. Dle jejich tvrzení však často jediná souvislost se Spojenými státy spočívala v tom, že údaje jsou v držení mezinárodních (globálních) poskytovatelů služeb tam sídlících, avšak osoby, o jejichž údaje se jedná, jsou z jiných zemí.³⁷³ Evropská unie se se Spojenými státy shoduje, že stávající mechanismus, tedy předávání elektronických důkazů v trestních věcech na základě smlouvy o vzájemné právní pomoci z roku 2010 (včetně prováděcích smluv jednotlivých členských států), není vzhledem k objemu dat a s tím souvisejícího množství žádostí, udržitelný.

Z toho důvodu Evropská komise zmocnila v roce 2019 Radu (EU) k zahájení jednání za účelem sjednání dohody mezi Evropskou unií a Spojenými státy o přeshraničním přístupu k elektronickým důkazům pro justiční spolupráci v trestních věcech.³⁷⁴ Vzhledem ke své radikálnosti však CLOUD Act vzbudil v rámci zemí Evropské unie řadu kritiky především v oblasti ochrany základních práv osob, zejména ochrany osobních údajů. Obdobné argumenty měla v této souvislosti společnost Microsoft již v rámci sporu *United States v. Microsoft Corp.*, který probíhal právě v době přijetí CLOUD Actu.³⁷⁵ Tyto obavy se však zdají být oprávněné, a to vzhledem k postupům a dosavadní (ne)přiměřenosti Spojených států ve směru ke zpracování osobních údajů a jiných právních norem týkajících se práva na soukromí.³⁷⁶

³⁷¹ Srov. Dohoda mezi Austrálií a Spojenými státy k nahlédnutí zde: <https://www.homeaffairs.gov.au/nat-security/files/cloud-act-agreement-signed.pdf>

³⁷² Srov. Dohoda mezi Spojeným královstvím a Spojenými státy k nahlédnutí zde: <https://www.justice.gov/d9/pages/attachments/2019/10/07/us-ukcloudagt10.3.2019-withsidenotes.pdf>

³⁷³ Office of International Affairs. *CLOUD Act Resources*. Op. cit.

³⁷⁴ Doporučení pro Rozhodnutí Rady o zmocnění k zahájení jednání za účelem dosažení dohody mezi Evropskou unií a Spojenými státy americkými o přeshraničním přístupu k elektronickým důkazům pro justiční spolupráci v trestních věcech. In: EUR-Lex [online]. [25. 1. 2024]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=COM:2019:0070:FIN>

³⁷⁵ Rozhodnutí Nejvyššího soudu Spojených států ve věci *United States v. Microsoft Corp. (Microsoft Ireland)*, 17. 4. 2018. No. 17-2

³⁷⁶ Blíže budou tyto postupy Spojených států rozvedeny níže v kapitole 3.3.2.

3.3.1.1. Konflikt s GDPR

Evropský sbor pro ochranu osobních údajů se k důsledkům přijetí zákona vyjádřil v tom smyslu, že je nejprve třeba komplexní dohody, která bude mezi zeměmi Evropské unie a Spojenými státy nastavovat, v souvislosti s přeshraničním přístupem, pevné hmotněprávní i procesněprávní záruky ochrany základních práv osob. Ty by měly být nastaveny zejména s důrazem na ochranu osobních údajů, která je v rámci Evropské unie zakotvena Obecným nařízením o ochraně osobních údajů neboli GDPR. Tím dojde i k nastavení právní jistoty pro poskytovatele služeb,³⁷⁷ která je důležitá zejména z toho důvodu, aby se v případě přijetí výkonné dohody poskytovatelé nebáli postupovat ve smyslu jejího zavedení. Obavy poskytovatelů by mohly pramenit právě z porušení ustanovení GDPR, za které hrozí vysoké pokuty.³⁷⁸

Jedním z velmi diskutovaných problémů přijetí je neexistence žádného právního základu (např. mezinárodní dohody (úmluva o mezinárodní právní pomoci))³⁷⁹ pro postup, jež předpokládá CLOUD Act. V souladu s článkem 48 GDPR nejsou z toho důvodu na základě žádosti, jakou předpokládá CLOUD Act, poskytovatelé služeb (na které se vztahuje unijní právo) oprávněni přímo zpřístupnit a předat osobní údaje do třetí země³⁸⁰. Výjimku by mohly tvořit pouze případy, kdy je vyhovění žádosti nezbytné pro životně důležité zájmy subjektu údajů nebo jiné fyzické osoby^{381,382}. K tomu se vyjádřil i Evropský inspektor ochrany osobních údajů, který k uzavření dohody uvedl následující: „*poskytovatelé služeb, kteří jsou správci osobních údajů, jejichž zpracování podléhá GDPR nebo jiným právním předpisům EU či členských států, budou čelit [vzájemnému] střetu právních předpisů*“.³⁸³

³⁷⁷ EDPB, *Evropský sbor pro ochranu osobních údajů – dvanácté plenární zasedání*, www.edpb.europa.eu. [online]. [cit. 25. 1. 2024], Dostupné z: https://edpb.europa.eu/news/news/2019/european-data-protection-board-twelfth-plenary-session_cs

³⁷⁸ Centre for Europea Policy Studies (CEPS), *Cross-border data access in criminal proceedings and the future of digital justice*. In: <https://www.ceps.eu> [online]. [cit. 25. 1. 2024]. Dostupné z: <https://cdn.ceps.eu/wp-content/uploads/2020/10/TFR-Cross-Border-Data-Access.pdf>

³⁷⁹ Srov. zákonnost zpracování (důvody zpracování) vycházející z čl. 6 GDPR

³⁸⁰ Spojeným státům

³⁸¹ EDPS, ANNEX. *Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence*. In: www.edpb.europa.eu. [online]. [cit. 25. 1. 2024]. Dostupné z: https://edpb.europa.eu/sites/default/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdfs s. 4

³⁸² Čl. 6 odst. 1 písm. d) GDPR

³⁸³ EDPS, ANNEX. *Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence* Op. cit.

3.3.2. Proces vyjednávání s Evropskou unií a odpovídající ochrana údajů

První jednání mezi Evropskou unií a Spojenými státy proběhlo v roce 2019, po dvou letech byla jednání zcela pozastavena z důvodu přípravy unijních předpisů týkajících se elektronických důkazů³⁸⁴. Mimo jiné tento pokrok ve vyjednávání zkomplikovala rozhodnutí Soudního dvora EU související s nedůvěrou v přiměřenost Spojených států ve vztahu k získávání dat a ochrany osobních údajů *Schrems I* a *Schrems II*. Ta navazovala na odhalení masového sledování ze strany americké Národní bezpečnostní agentury (NSA) bývalým zaměstnancem Edwardem Snowdenem. Dohled se uskutečňoval nad různými formami elektronické komunikace (včetně emailové komunikace i internetového vyhledávání), a to nejen v rámci Spojených států, ale po celém světě, tj. včetně Evropy.³⁸⁵ Soudní dvůr EU ve svém rozhodnutí C-362/14 konstatoval možnost států (i přes existenci rozhodnutí ve smyslu článku 45 GDPR³⁸⁶) posoudit, zda předání osobních údajů do třetí země splňuje požadavky stanovené unijním právem.³⁸⁷ Vzhledem k obavě z možného porušování práv zaručených občanům článkem 7 a 8 Listiny EU rozhodl o neplatnosti tehdejšího rozhodnutí o odpovídající úrovni ochrany předávaných osobních údajů, tzv. *Safe Harbour*.³⁸⁸ Později byl tento režim nahrazen rozhodnutím *Privacy Shield*, který měl za cíl nastavovat vyšší záruky ochrany. V roce 2020 však Soudní dvůr EU v případě C-311/18 prohlásil za neplatné i rozhodnutí *Privacy Shield* a současně nastínil kritéria³⁸⁹, která je nutné pro soulad s unijním právem naplnit.³⁹⁰

Obavy vznesené v posledním rozhodnutí C-311/18 má řešit nově přijatý výkonný dekret č. 14086 „*Posílení záruk pro činnosti USA v oblasti signálového zpravodajství*“ (EO 14086) z října 2022, ten má zaručit soudní přezkum ochrany údajů. V reakci na to vydala Evropská unie rozhodnutí o odpovídající ochraně pro bezpečný a spolehlivý tok údajů mezi Evropskou unií a Spojenými státy.³⁹¹ Tímto rozhodnutím staví Evropská komise poskytovanou úroveň ochrany osobních údajů zpracovávaných z Evropské unie americkými společnostmi naroveň

³⁸⁴ Nařízení o evropském vydávacím příkazu a evropském uchovávacím příkazu

³⁸⁵ SUMNER, S. *You: For Sale: Protecting Your Personal Data and Privacy Online*, 2015. ISBN 978-0-12-803405-7. s. 17-48

³⁸⁶ Rozhodnutí Komise o tom, že třetí země zabezpečuje odpovídající úroveň ochrany osobních údajů, srov. v tomto případě se jednalo o Rozhodnutí Evropské Komise 2000/520

³⁸⁷ Rozhodnutí *Schrems I* se týká podání několika stížností evropským orgánům pro ochranu údajů z důvodu nakládání s údaji uživatelů ze strany společnosti Facebook.

³⁸⁸ Rozsudek Soudního dvora EU ze dne 6. 10. 2015, sp. zn. C-362/14

³⁸⁹ Nezbytnost, přiměřenost a nastavení soudní ochrany

³⁹⁰ Rozsudek Soudního dvora EU ze dne 16. 7. 2020, sp. zn. C-311/18

³⁹¹ European Commission. *Adequacy decision for the EU-US Data Privacy Framework*. In: [commission.europa.eu/](https://commission.europa.eu/online) [online]. [cit. 25. 1. 2024] Dostupné z: https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf

s Evropskou unií, pokud se řídí podle nového *Rámce EU–USA pro ochranu údajů*,³⁹² ve smyslu článku 45 odst. 3 GDPR. Pro možnost připojit se k tomuto rámci, jsou americkým společnostem stanoveny přísné podmínky,³⁹³ kterými se musí řídit. V opačném případě je předávání umožněno jen v režimu záruk. V souvislosti s trestním řízením se Evropská komise u přijetí tohoto rozhodnutí vyjádřila následovně: „*Právní rámec USA navíc stanoví řadu záruk ohledně přístupu orgánů veřejné moci USA, zejména pro účely prosazování trestního práva a národní bezpečnosti, k údajům předávaným na základě rámce. Přístup k údajům je omezen na to, co je pro účely ochrany národní bezpečnosti nezbytné a přiměřené.*“³⁹⁴

Po několika letech je tedy dohoda umožňující urychlené zajištění elektronických důkazů opět předmětem diskuze. Po přijetí nařízení, jež upravuje vydávání a uchovávání elektronických důkazů³⁹⁵, byla jednání mezi Spojenými státy a Evropskou unií znovu obnovena. Možným přístupem při vyjednávání by mohlo být omezení druhů elektronických důkazů, které lze takto jednostranně vyžádat. Propp³⁹⁶ uvádí jako příklad vyloučení postupu dle zákona CLOUD Act pro určitý typ citlivých údajů, např. údajů týkajících se vlády (státu). Otázkou však zůstává, zda je možné vyjednat takovou dohodu, aby bylo zajištěno udržení vysoké míry ochrany osobních údajů tak, jak předpokládá GDPR, a současně bylo zamezeno potenciálním porušením unijních zásad týkajících se práva na soukromí. Jsem však přesvědčena, že je nutné dát za pravdu stanovisku americké vlády o neudržitelnosti současných mechanismů, zejména v době stále narůstající digitalizace. Kontroverze kolem zákona CLOUD Act značí potřebu pečlivého vyvážení mezi účinným zajišťováním elektronických důkazů a respektováním základních práv na soukromí jedinců. Bude tedy třeba přijmout dohodu, která bude oběma subjektům poskytovat v rámci trestního řízení efektivní přístup k datům a současně nastavovat přísné podmínky užití, a to včetně záruk soudního přezkumu zákonnosti. Americký CLOUD Act tak bezpochyby představuje výzvu pro budoucí směřování právní regulace v oblasti kybernetické bezpečnosti a ochrany údajů.

³⁹² *Tamtéž.*

³⁹³ Např. vymazání osobních údajů, když již nebudou potřeba k účelu, pro který byly shromážděny

³⁹⁴ Evropská Komise. *Ochrana údajů: Evropská komise přijala nové rozhodnutí o odpovídající ochraně pro bezpečný a spolehlivý tok údajů mezi EU a USA*. In: ec.europa.eu. [online]. [cit. 25. 1. 2024]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/cs/ip_23_3721

³⁹⁵ Nařízení o evropském vydávacím příkazu a evropském uchovávacím příkazu

³⁹⁶ PROPP, K. *Navigating Toward an EU-U.S. Agreement on Electronic Evidence*. In: Lawfare. 1. prosince 2023 [online]. [cit. 24. 1. 2024]. Dostupné z: <https://www.lawfaremedia.org/article/navigating-toward-an-eu-u.s.-agreement-on-electronic-evidence>

4. Charakteristika dokazování z jednotlivých důkazních prostředků

Žijeme v moderní době, která se stává stále více digitalizovanou, a mnohé naše činnosti se přenáší do online prostředí. Běžně používáme mobilní telefony, chytré hodinky, stolní počítače, notebooky či tablety, zálohujeme a ukládáme si data na cloudová úložiště, pohybujeme se v internetovém prostředí a s ostatními komunikujeme prostřednictvím sociálních sítí, nejrůznějších komunikačních platform (včetně např. Discordu) či emailů, a to jak v rámci volnočasových aktivit, tak výkonu pracovních povinností. Mnoho transakcí probíhá elektronicky a v rámci předcházení trestné činnosti jsou některé prostory monitorované. Nejedna generace užívá k zábavě herní konzole jako je např. PlayStation či Xbox, v autě jsme zvyklí synchronizovat mobilní telefon k tzv. infotainmentu, který nám umožní nahrát kontakty a volat přátelům, rodině či kolegům, zobrazí nám navigaci, nebo nás připojí k našemu hudebnímu playlistu. S tím neodmyslitelně souvisí i množství datových stop, které denně během našich životů vznikne.

Není proto s údivem, že i orgány činné v trestním řízení se čím dál častěji obracejí na elektronické zdroje důkazů, které jim pomáhají při dokazování v rámci trestního řízení. Jak bylo představeno v předešlých kapitolách, tyto nové perspektivy se stávají nedílnou součástí kriminalistického vyšetřování a trestněprávního procesu. Nejenže však rozšiřují možnosti pro dokazování, ale přinášejí také nové právní, technické a etické výzvy. V následující kapitole tak budou představeny vybrané elektronické důkazní prostředky. Charakterizováno bude, jakým způsobem je možné získat data prostřednictvím *emailu*, *ze sociálních sítí* a *v cloudovém úložišti*. Na závěr bude popsána problematika získávání dat z *chytrých mobilních telefonů*, zejména z pohledu otázky zásahu do ústavně zaručeného práva na soukromí.

4.1. Zdroje důkazů

4.1.1. Emailové schránky

Email je stále jedním z velmi často užívaných prostředků elektronické komunikace, především v prostředí uskutečňování formální komunikace. Orgány činné v trestním řízení mohou v emailové schránce získat zprávy *doručené*, *odeslané*, *koncepty*, či zprávy umístěné *v koši*, které však ještě nejsou smazány (dále zprávy, které jsou vyhodnoceny jako *spam* či *hromadné*). V souvislosti s výběrem vhodného právního institutu zajištění není rozhodující, zda si uživatel emailové schránky zprávu přečetl, ale zda tuto možnost objektivně měl. Pokud to nebylo uživateli umožněno, je důležité zhodnotit, zda tomu tak bylo v důsledku

vlivu orgánů činných v trestním řízení, či jiných překážek nezávislých na jeho vůli.³⁹⁷ Zajištění obsahu emailové komunikace bude charakterizováno v rámci dvou situací, těmi jsou *zajištění datového nosiče informací a přístup k datům jiným způsobem*.

Zajištění datového nosiče informací

K *zajištění datového nosiče informací* orgánem činným v trestním řízení může dojít (pokud není vydán z vlastní iniciativy osoby³⁹⁸) např. způsobem dle ustanovení § 78 či § 79 trestního řádu o vydání či odnětí věci, ustanovení § 83, § 83a či § 83b trestního řádu o domovní prohlídce, prohlídce jiných prostor a pozemků či osobní prohlídce, alternativně na základě ustanovení § 113 trestního řádu prostřednictvím ohledání. Nejvyšší soud rozdělil ve svém usnesení 7 Tz 9/2000 ochranu tajemství zpráv dopravovaných v telekomunikačním provozu na období, kdy je zpráva přepravována, a období po doručení. S odkazem na ustanovení § 78 odst. 2 trestního řádu konstatoval, že u zpráv teprve přepravovaných „nelze [...] vystačit s aplikací institutů vydání a odnětí věci“³⁹⁹. Pokud se tedy policejnímu orgánu podaří zajistit nosič informací, bude přístup k obsahu zpráv záviset na okolnosti, zda se jedná o

- a. *zprávy přijaté na nosiči do chvíle jeho zajištění* příslušným orgánem – v tomto případě je umožněno orgánům činným v trestním řízení přistupovat k datům (obsahu zpráv) bez dalšího;⁴⁰⁰
- b. *zprávy přijaté na nosiči po jeho zajištění* příslušným orgánem – k přístupu je nezbytné žádat o povolení soudce na základě ustanovení § 88 trestního řádu o odposlechu (adresát se s obsahem nemohl seznámit, je zde stále trvajících zvláštní povinnost mlčenlivosti⁴⁰¹).

Přístup k datům jiným způsobem

Při přístupu k obsahu emailové schránky *jiným způsobem* musí orgány činné v trestním řízení využít jiného procesního institutu. Ústavní soud se ve svém usnesení III. ÚS 3812/12 vyjádřil následovně: „Z hlediska ústavněprávní kontroly je podstatné, že soud ve svém povolení dostatečně jasně specifikoval okruh počítačů, které mají být sledovány. V rámci sledování elektronických zařízení z povahy věci plyne, že předmětem sledování budou právě data

³⁹⁷ POLČÁK, R., PÚRY, F., HARAŠTA, J., MYŠKA, M. a STUPKA, V. *Elektronické důkazy v trestním řízení*. Op. cit., s. 126

³⁹⁸ Např. oznamovatelem

³⁹⁹ Usnesení Nejvyššího soudu ze dne 15. 12. 2000, sp. zn. 7 Tz 9/2000

⁴⁰⁰ Zákonná ustanovení, kterými byl nosič zajištěn jsou dostatečným zákonným podkladem, který předpokládá Listina na prolomení ochrany tajemství zpráv uchovávaných v soukromí. Srov. Usnesení Nejvyššího soudu ze dne 15. 12. 2000, sp. zn. 7 Tz 9/2000

⁴⁰¹ Viz § 89 zákona o elektronických komunikacích

na těchto zařízeních uložená, jejichž otisk lze pořídit za využití utajené operativně pátrací techniky.⁴⁰², odmítl však takový postup u dat, která jsou předmětem telekomunikačního provozu (zde je nutné postupovat dle ustanovení § 88a trestního řádu). Příslušný orgán tedy může pro obsah

- a. zpráv již doručených využít postupu dle ustanovení § 158d odst. 1 a odst. 3 trestního řádu o sledování;⁴⁰³
- b. zpráv přijatých do budoucna (probíhající komunikace) užít postupu dle ustanovení § 88 trestního řádu o odposlechu;
- c. zpráv v procesu doručování užít ustanovení § 88 trestního řádu o odposlechu. Nejvyšší soud tuto velmi krátkou⁴⁰⁴ časovou linii vymezil v případě elektronické komunikace jako dobu, která „začíná jejím odesláním z počítače odesílatele a končí okamžikem doručení zprávy do počítače (e-mailové schránky) příjemce.“⁴⁰⁵. Tato situace však může nastat a je nutné, aby bylo postupováno v souladu s tajemstvím dopravovaných zpráv, pro které zákonodárce stanoví nutnost užití ustanovení o odposlechu.

Gřivna a Richter ve své publikaci však upozorňují na zásadní rozdílnost úrovně ochrany při zajišťování dat, kterou tato praxe vyvolává. Příkladem je uvedena emailová zpráva, jež může být na základě aplikace (např. Outlook) stažena v paměti mobilního telefonu, a bude tak zajišťována bez dalšího, resp. na základě ustanovení, kterým bude zajištěn mobilní telefon (např. § 78, § 79 či §113 trestního řádu). Pokud však stejná (již doručená) emailová zpráva nebude v mobilním telefonu stažena⁴⁰⁶, nastává druhá situace, kdy bude zapotřebí využít institutu § 158d odst. 3 trestního řádu, tj. bude vyžadován příkaz soudce. Třetí popisovanou situací je doručení emailové zprávy na mobilní telefon až po zajištění zařízení např. v důsledku nepřipojení k internetu. V této situaci je nutné postupovat dle ustanovení § 88 trestního řádu, přestože není zcela jednoznačné, zda se dá hovořit o komunikaci probíhající do budoucna. Okolnost, že by nastavení fungování mobilního telefonu rozhodovalo (mnohdy bez přičinění

⁴⁰² Usnesení Ústavního soudu ze dne 3. 10. 2013, sp. zn. III. ÚS 3812/12

⁴⁰³ Polčák však upozorňuje na nedostatek této konstrukce, jelikož to může vést k tomu, že policejní orgány budou sváděny k opakovanému či kontinuálnímu vstupu do schránky na základě příkazu vydaného dle ustanovení § 158d trestního řádu, což fakticky můžeme přirovnat k odposlechu, který však v daném případě nebyl schválen. Srov. POLČÁK, R., PŮRY, F., HARAŠTA, J., MYŠKA, M. a STUPKA, V. *Elektronické důkazy v trestním řízení*. Op. cit., s. 128-129

⁴⁰⁴ V řádu vteřin

⁴⁰⁵ Usnesení Nejvyššího soudu ze dne 21. 5. 2009, sp. zn. 11 Tdo 349/2009

⁴⁰⁶ Jako příklad je uváděna optimalizace zařízení

uživatelé) o úrovni ochrany, považují autoři za absurdní.⁴⁰⁷ K tomuto názoru je třeba se přiklonit, jelikož je nedůvodné, aby o rozdílné míře ochrany před zásahem ústavně zaručených práv rozhodovalo technické nastavení či vůbec okolnost, kde se nacházejí⁴⁰⁸ zajišťovaná data.

V rámci provádění důkazu před soudem je prokazována pravost⁴⁰⁹ a autorství emailové zprávy, k tomu může napomoci např. svědecká výpověď, znalecký posudek, posouzení možnosti fyzického přístupu k zařízení či podstatné rysy zprávy ve vztahu k okolnostem případu.⁴¹⁰ Vhodné je také upozornit na informace, které nejsou v samotném „těle“ emailové zprávy, ale pro dokazování jsou velmi podstatné. Tyto informace jsou obsaženy v tzv. *hlavičce emailu* (zdrojový kód). Orgánům činným v trestním řízení pomáhají určit např. cestu přes servery, skutečnou adresu odesílatele a adresáta, čas odeslání a přijetí emailu či informace k operačnímu systému, ze kterého byla zpráva odeslána.⁴¹¹ Tato hlavička se čte odspodu a pomáhá příslušným orgánům k určení poskytovatele připojení či poskytovatele emailové služby.

4.1.2. Sociální sítě

Sociální sítě jsou dnes již využívány napříč všemi generacemi, jejich prostřednictvím komunikujeme s rodinou, přáteli, vyhledáváme volné pracovní pozice, seznamujeme se, sdílíme (své) fotografie, videa, názory a mnoho dalšího. V závislosti na typu platformy či výběru způsobu tak činíme soukromě či veřejně.⁴¹² Je třeba rozumět, že jde o „*službu, typicky poskytovanou ISP, v kyberprostoru na základě odsouhlasených smluvních podmínek*“.⁴¹³ Nutností (založenou smluvními podmínkami dané sociální sítě) je vytvoření uživatelského profilu,⁴¹⁴ prostřednictvím kterého komunikace a sdílení dat na platformě probíhá.

⁴⁰⁷ GŘIVNA, T., RICHTER, M. *Zajištění elektronického důkazu a související koncepční otázky*. In: GŘIVNA, T., RICHTER, M. a ŠIMÁNOVA, H. *Vliv nových technologií na trestní právo*. Praha: Auditorium, 2022. ISBN 978-80-87284-95-7. s. 20-23

⁴⁰⁸ Blíže tomu bude věnována pozornost v závěru této práce.

⁴⁰⁹ Emailovou zprávu lze zfalšovat mnoha způsoby, např. složitěji (užití VPN, TOR) či jednoduše (upravením textu či hlavičky).

⁴¹⁰ POLČÁK, R., PÚRY, F., HARAŠTA, J., MYŠKA, M. a STUPKA, V. *Elektronické důkazy v trestním řízení*. Op. cit., s. 132-134

⁴¹¹ KOLOUCH, J. *CyberCrime*. Op. cit., s. 138-139

⁴¹² K tomuto více níže v této podkapitole.

⁴¹³ KOLOUCH, J. *CyberCrime*. Op. cit., s. 152

⁴¹⁴ Ty však mohou být zcela fiktivní, nemusí se jednat o existující fyzickou či právnickou osobu. Srov. ČERNÁ, M., ČERNÝ, M. *Úvod do problematiky sociálních sítí*. In: Metodický portál RVP.CZ [online]. [cit. 26. 1. 2024]. Dostupné z: <http://clanky.rvp.cz/clanek/o/g/15075/UVOD-DO-PROBLEMATIKY-SOCIALNICH-SITI.html/>

Ačkoliv osoby musí při zakládání uživatelských účtů se smluvními podmínkami souhlasit, fakticky však k jejich čtení ze strany běžných uživatelů nedochází. A to přestože právě na jejich základě „je pak o uživateli zjišťována celá řada informací (velmi často značně soukromých), které mohou být v souladu s těmito podmínkami předávány dalším osobám, ale zejména archivovány téměř neomezenou dobu.“⁴¹⁵ Profil uživatele je provázaný s provozními údaji (IP adresa, druh webového prohlížeče, záznamy týkající se místa a času přihlášení) a metadaty souborů, které jsou z větší části pro samotného uživatele nedostupné.⁴¹⁶ Je tedy vhodné zvolit adekvátní zabezpečení (např. dvoufázové zabezpečení pomocí telefonního čísla) a současně zvážit, jaké informace sdílíme a zejména jak širokému okruhu adresátů je sdělujeme (zda zcela veřejně, nebo v uzavřené skupině či nastavením soukromého profilu). V tomto směru se již v roce 2013 vyjádřil Ústavní soud ve svém nálezu III. ÚS 3844/13 týkající se sociální sítě Facebook: „Povaha sociální sítě Facebook není jednoznačně soukromá či veřejná, neboť záleží na každém uživateli, jakou míru ochrany soukromí na svém profilu zvolí.“⁴¹⁷ Pokud se orgán činný v trestním řízení rozhodne zajišťovat data mající soukromou povahu, je třeba v souladu s ochranou ústavně zaručených práv a svobod osob postupovat dle institutů v trestním řádu k tomu určených, nikoliv použitím pouhého institutu ohledání či dožádání.

Ústavní soud se k problematice veřejné a soukromé povahy sociálních sítí vyjádřil znovu ve svém nálezu III. ÚS 3564/18 týkajícím se získávání printscreenů od informátora⁴¹⁸ na sociálních sítích, které však nejsou volně přístupné⁴¹⁹. Konstatoval, že: „Sám původce informace sdělované po sociálních sítích si může předem učinit obrázek, jakému okruhu subjektů informaci poskytuje či jaký okruh subjektů se může s informací seznámit a případně tuto informaci poskytnout někomu dalšímu, včetně policie.“⁴²⁰, a tedy v této situaci není pro zákonné zajištění důkazů za podmínek stanovených zákonem o Policii ČR nutný příkaz či souhlas soudu.

V závěru je třeba připomenout, že situace získávání dat je značně odlišná v případě, kdy se bude jednat o zahraniční poskytovatele. Pro zajištění dat je třeba využít mezinárodní

⁴¹⁵ KOLOUCH, J. *CyberCrime*. Op. cit., s. 152

⁴¹⁶ POLČÁK, R., PŮRY, F., HARAŠTA, J., MYŠKA, M. a STUPKA, V. *Elektronické důkazy v trestním řízení*. Op. cit., s. 141-143

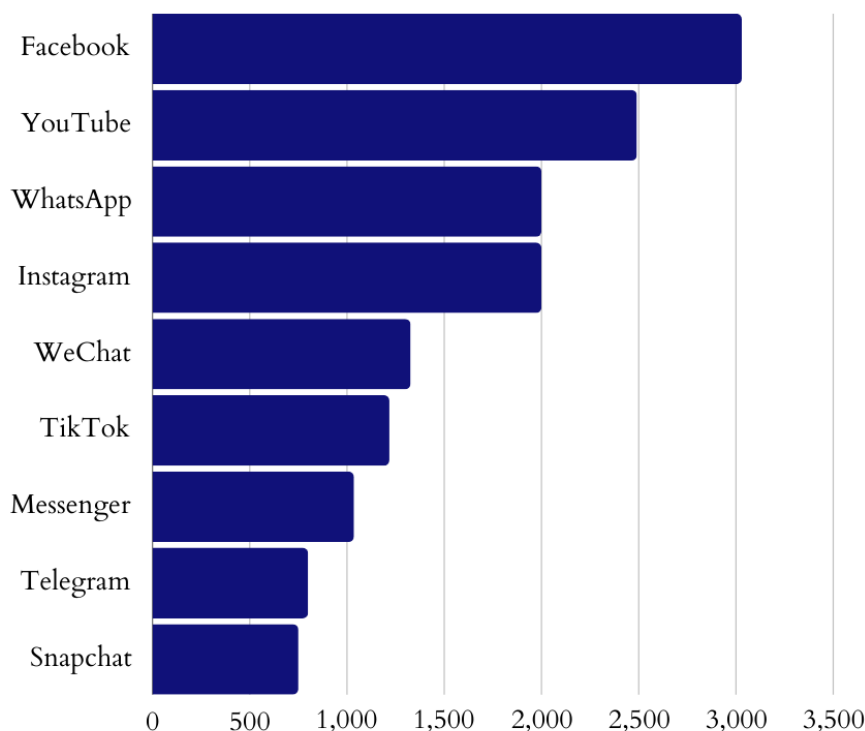
⁴¹⁷ Nález Ústavního soudu ze dne 30. 10. 2014, sp. zn. III. ÚS 3844/13

⁴¹⁸ § 72 - § 74 zákona č. 273/2008 Sb., o Policii České republiky

⁴¹⁹ Např. uzavřená skupina na Facebooku

⁴²⁰ Nález Ústavního soudu ze dne 28. 5. 2019, sp. zn. III. ÚS 3564/18

právní pomoci či některého z institutů umožňujícího přístup k důkazům v elektronické podobě přímo od poskytovatelů služeb v rámci Evropské unie.⁴²¹



Graf 4: Celosvětový počet aktivních uživatelů na sociálních sítích v (říjnu) roku 2023, čísla jsou v milionech⁴²²

4.1.3. Cloudová úložiště

Mnoho z nás využívá služeb *cloud computingu*,⁴²³ zálohujeme si tak data, optimalizujeme fyzické úložiště mobilního telefonu či notebooku, rozšiřujeme tímto způsobem počet zařízení, resp. místa⁴²⁴, ze kterých je možné se k datům dostat. Polčák uvádí, že „myšlenka [je] založena na globálním charakteru počítačové sítě Internet, prostřednictvím kterého jsou propojovány jednotlivé servery a datová úložiště do logického celku.“⁴²⁵

⁴²¹ Blíže k této problematice a nově zavedeným unijním institutům v kapitole 3 této práce.

⁴²² Datareportal, *Global Social Media Statistics, 2023* In: datareportal.com. [online]. 2023 [cit. 26.1.2024] Dostupné z: <https://datareportal.com/social-media-users>

⁴²³ *Cloud computing* můžeme definovat jako „model umožňující všudypřítomný, snadný, na vyžádání dostupný síťový přístup ke sdílenému fondu konfigurovatelných výpočetních zdrojů (např. sítí, serverů, úložišť, aplikací a služeb), které lze rychle poskytnout a uvolnit s minimálním úsilím o správu nebo interakci s poskytovatelem služeb.“ Srov. MELL, P., GRANCE, T. *The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology*. 2011 [online]. [cit. 28. 1. 2024]. Dostupné z: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

⁴²⁴ Dosažitelná jsou díky *cloud computingu* odkudkoliv, a to za pomoci webového prohlížeče či klienta aplikace. Srov. SMEJKAL, V. *Kybernetická kriminalita*. Op. cit., s. 71-76

⁴²⁵ POLČÁK, R., PÚRY, F., HARAŠTA, J., MYŠKA, M. a STUPKA, V. *Elektronické důkazy v trestním řízení*. Op. cit., s. 92

Tato vzdálená úložiště obsahují mnohá data, která mohou být v rámci vyšetřování trestné činnosti předmětem zájmu orgánů činných v trestním řízení. Krátce bude představeno, na základě jakých právních institutů se k datům uloženým na cloudových úložištích mohou příslušné orgány dostat.

Pokud budou data z cloudového úložiště *současně stažena a uložena v datovém nosiči*⁴²⁶ pomocí synchronizace a orgán činný v trestním řízení se k tomuto nosiči dostane za využití některého z institutů, jakým je např. vydání či odnětí věci nebo domovní prohlídka (ustanovení § 78, § 79 či § 82 an. trestního řádu), a dojde při zajišťování důkazů k vytvoření otisku pevného disku, není k přístupu k elektronickým důkazům již dalších právních úkonů třeba.

Diskutovanou otázkou je, na základě jakého institutu je možné zajistit data z *webového rozhraní cloudových úložišť*, jež budou nalezena v rámci domovní prohlídky. Na jedné straně se objevuje názor, že cloudové úložiště je samo o sobě počítačovým systémem, a tedy není možné pojem počítačový systém dle Budapešťské úmluvy⁴²⁷ vykládat v tom smyslu, že za skupinu propojených zařízení lze považovat i cloudové úložiště. Pokud by tak byl „v rámci domovní prohlídky [zajištěn] počítač pachatele, na kterém jsou ve webovém prohlížeči uloženy přístupové údaje do cloudového úložiště, mohl by policista zajistit data uložená v tomto úložišti již na základě povolení k domovní prohlídce.“⁴²⁸, tento extenzivní výklad je tak dle názoru autorů třeba pokládat za nesprávný. Hlaváčová a Chorvát navíc odkazují na zahraniční úpravu v Dánsku, Austrálii či Kanadě,⁴²⁹ kde je příkaz soudce ke vstupu do cloudového úložiště nutností.⁴³⁰ Tomuto však oponuje jiný autor s argumentem, že „základním rysem diskutovaného cloudového úložiště je právě naopak jeho připojenost do prostoru prohlídky [a ...] není vůbec podstatné, zda cloudové úložiště budeme chápat jako do určité míry samostatný počítačový systém či nikoliv“⁴³¹. Za důležitou náležitost (zákonného zajištění) naopak považuje konkrétní uvedení vzdálených úložišť mezi předměty, na které

⁴²⁶ Např. počítači

⁴²⁷ Dle čl. 1 písm. a. Budapešťské úmluvy se počítačovým systémem rozumí „jakékoli zařízení nebo skupinu propojených nebo přidružených zařízení, z nichž jedno nebo více provádí automatické zpracování dat podle programu“.

⁴²⁸ HLAVÁČOVÁ, K., CHORVÁT, O. *Přístup orgánů činných v trestním řízení k datům uloženým v cloudu*. Revue pro právo a technologie, 2016, č. 14, s. 3-24

⁴²⁹ MAXWEL, W., WOLF, Ch., *A Global Reality: Governmental Access to Data in the Cloud*. 2012 [online]. [cit. 26. 1. 2024]. Dostupné z: https://www.hoganlovells.com/-/media/hogan-lovells/pdf/publication/revise-government-access-to-cloud-data-paper-18-july-12_pdf.pdf

⁴³⁰ HLAVÁČOVÁ, K., CHORVÁT, O. *Přístup orgánů činných v trestním řízení k datům uloženým v cloudu*. Op. cit., s. 3-24

⁴³¹ DOSTÁL, O. *Zajišťování důkazů u počítačové kriminality – dožádání, vydání věci a prohlídky (1. díl)*. Trestněprávní revue, 2019, č. 3, s. 66-71

se bude příkaz k domovní prohlídce vztahovat. Dalšího institutu k zajištění dat z cloudového úložiště však dle autora není potřeba.⁴³²

S tímto oponentním názorem však nelze souhlasit, a to vzhledem k tomu, že je daným způsobem prolamováno právo na soukromí a na informační sebeurčení za použití institutu (např. § 78 či § 79 trestního řádu), kterým zákonodárce zásah ústavně garantovaného práva nepředpokládá a nezaručuje tak adekvátní záruky v podobě souhlasu soudce či státního zástupce. Dle mého je tedy vhodné užít postup dle ustanovení § 158d odst. 3 trestního řádu a zajistit tímto způsobem určitou garanci ochrany zajišťovaných dat. K tomuto názoru se přikláním i vzhledem k již zmiňované judikatuře Ústavního soudu III. ÚS 3812/12, který pro porizení otisku elektronických dat předpokládá postup dle ustanovení o sledování. Smejkal⁴³³ tento postup zajištění dat na cloudových úložištích (dle § 158d odst. 3 trestního řádu) vidí jako „*jediný možný*“.

Dalším možným postupem orgánů činných v trestním řízení bude *součinnost s poskytovatelem cloudových úložišť*. Pokud tedy datové nosiče nelze zajistit (a současně nebudou vydány poskytovatelem), i zde bude užito ustanovení § 158d odst. 3 trestního řádu. Opět se však potýkáme s okolností, kdy většina poskytovatelů (cloudových) služeb jsou osoby sídlící v zahraničí s daty uloženými na úložištích mimo území České republiky. V tomto smyslu je pak nutné zajišťovat data cestou mezinárodní justiční spolupráce, která s sebou přináší značná úskalí, zejména týkající se časového hlediska.

4.1.4. Mobilní telefony

Pomocí mobilního telefonu komunikujeme denně, už mnoho let se nejedná pouze o prostředek uskutečňování telekomunikačního provozu, tj. volání a zasílání sms zpráv, ale využíváme ho i k dalším formám elektronické komunikace (např. skrze sociální sítě jako je Facebook, Messenger, Instagram, WhatsApp, LinkedIn, BeReal, TikTok či Telegram). Současně naše mobilní telefony obsahují mnoho dat jako jsou fotografie, videa a jiné soubory, povinnosti uložené do poznámek či kalendáře, přístupy do mobilních bankovníctví či emailových schránek, elektronickou klíčenku (jejímž obsahem jsou přístupové údaje) nebo aplikace obsahující údaje o našem zdraví a mnoho dalšího. Chytré mobilní telefony současně aktivně využívají polohových služeb na základě GPS modulu, který nejen že obsahuje údaje o poloze, resp. pohybu mobilního telefonu, ale ve spojení např. s navigací (mapami)

⁴³² *Tamtéž.*

⁴³³ SMEJKAL, V. *Kybernetická kriminalita. 3. rozšířené a aktualizované vydání*, Op. cit. 847

či aplikacemi umožňujícími najít spoje hromadné dopravy také data o vyhledávaných cestách.⁴³⁴ S tím souvisí i zaznamenaná historie vyhledávání na internetu. Současně mohou být mobilní telefony spárované s jinými zařízeními⁴³⁵, která jsou schopná zaznamenávat další vlastnosti jako je měření tepu⁴³⁶ či uběhnuté (ujeté) kilometry.

Je třeba také připomenout, že některá z těchto dat jsou uložena přímo v paměti mobilního telefonu, zatímco jiná mohou být (např. z důvodu optimalizace paměti) z telefonu přístupná pouze prostřednictvím webového rozhraní⁴³⁷, přičemž tyto dva způsoby se vzájemně nevyklučují. I přes uložení dat na cloudových úložištích jsou na mobilním telefonu velmi snadno a často přímo (skrze aplikaci) přístupná. Shrňme-li výše uvedené, je zřejmé, že pro orgány činné v trestním řízení může být mobilní telefon bohatým zdrojem důkazů. Naproti tomu je však nutné zohlednit, že jsou „*shromažďována data a informace, která o soukromí, událostech a činnostech v soukromém životě jednotlivců vypovídají neporovnatelně více [...], než by oni sami vědomě ze svého soukromí zpřístupnili*“⁴³⁸ a zajišťování elektronických důkazů z mobilních telefonů tak velmi znatelně zasahuje do ústavně garantovaného práva na informační sebeurčení⁴³⁹. Aby k tomuto prolomení mohlo dojít, vždy musí být splněny zákonodárcem stanovené podmínky. V následujících odstavcích bude rozvedeno, na základě jakých právních institutů se k datům uloženým na mobilních telefonech mohou příslušné orgány dostat, a zda současné postupy reflektují výše uvedenou míru zásahu do základních práv a svobod jedinců.

Vzhledem k tomu, že na mobilním telefonu se nachází mj. elektronické důkazy, jejichž zajišťování ze strany orgánů činných v trestním řízení bylo podrobně popsáno výše v této práci, případně přímo v této kapitole (telefonní hovory a údaje s nimi související⁴⁴⁰, emailové

⁴³⁴ POLČÁK, R., PÚRY, F., HARAŠTA, J., MYŠKA, M. a STUPKA, V. *Elektronické důkazy v trestním řízení*. Op. cit., s. 199

⁴³⁵ Např. chytré hodinky, infotainment v automobilu, asistenti „chytré domácnosti“, ale můžeme mluvit i o zařízeních jako jsou běžecské pásy.

⁴³⁶ Srov. ČTK, *Zsuzsová měla vyšší tep, Kočner pročítal média. Objevily se nové důkazy ke Kuciakovi*. In: Aktuálně.cz [online]. [cit. 27. 1. 2024]. Dostupné z: <https://zpravy.aktualne.cz/zahranici/zsuzsova-mela-vyssi-tep-kocner-procital-media-objevily-se-no/r~760f8d0c729011ebb0fa0cc47ab5f122/>

⁴³⁷ Uložena však budou na cloudovém úložišti. K tomu více v kapitole 4.1.3. této práce.

⁴³⁸ KOKEŠ, M. Čl. 10 [*Právo na soukromý a rodinný život; právo na informační sebeurčení*]. In: HUSSEINI, F., BARTOŇ, M., KOKEŠ, M., KOPA, M. a kol. *Listina základních práv a svobod*. Op. cit., marg. č. 10

⁴³⁹ Čl. 10 odst. 3 Listiny ve spojení s čl. 13 Listiny

⁴⁴⁰ Viz kapitola 2.3.1 a 2.3.2. této práce

zprávy⁴⁴¹, sociální sítě⁴⁴² včetně elektronické komunikace⁴⁴³ a cloudové úložiště⁴⁴⁴), pozornost bude soustředěna k diskutovanému tématu, kterým je přístup k elektronickým důkazům ze zajištěného mobilního telefonu, resp. nosiče informací.

Zajistit zařízení mohou orgány činné v trestním řízení za užití institutu vydání či odnětí věci upraveného v ustanovení § 78 či § 79 trestního řádu, popřípadě v rámci prováděné domovní prohlídky, prohlídky jiných prostor či osobní prohlídky, jež jsou upraveny v ustanovení § 83 an. trestního řádu.⁴⁴⁵ Zařízení je možné ohledat na základě ustanovení § 113 trestního řádu, pod tím si lze představit sejmutí daktyloskopických stop či zjištění známek poškození, tj. ohledání zvenčí.⁴⁴⁶ Co se týče dat, která zajištěný mobilní telefon obsahuje, současná praxe k nim přistupuje bez dalších procesních postupů⁴⁴⁷ (vztahuje na ně postup, jímž bylo zajištěno zařízení samotné). Tato dosavadní praxe vychází zejména z výkladového stanoviska NSZ č. 4/2005, které takový způsob v případě zajišťování dat, na která se již nevztahuje zvláštní povinnost mlčenlivosti,⁴⁴⁸ dovoluje. Navazující výkladové stanovisko NSZ č. 1/2015 nechává právní závěry původního stanoviska ve směru k zajišťování dat z mobilního telefonu za použitelné.

Co je však nutné zohlednit je doba, ve které bylo (zejména) první stanovisko vydáno a prudký rozvoj digitálního světa, který svět za 19 let zaznamenal. K tomu Marešová uvádí, že „[m]nožství informací v tehdejších telefonech bylo nesrovnatelně nižší a jeho předmětem byly zejména informace o hovorech a SMS (MMS) zprávy.“⁴⁴⁹, s postupem vyjádřeným v obou uvedených stanoviscích NSZ, se však neztotožňuje. Právě s ohledem na zastaralost těchto stanovisek (zejména prvního, dle kterého se praxe fakticky řídí) je dle mého nemožné i nadále shledávat tuto právní metodiku za aplikovatelnou.

⁴⁴¹ Viz kapitola 4.1.1. této práce

⁴⁴² Viz kapitola 4.1.2. této práce

⁴⁴³ Obdobně jako v případě zajišťování emailových zpráv (prostředek elektronické komunikace). Viz výkladové stanovisko NSZ č. 4/2005 ve spojení výkladovým stanoviskem NSZ č. 1/2015.

⁴⁴⁴ Viz kapitola 4.1.3 této práce

⁴⁴⁵ POLČÁK, R., PÚRY, F., HARAŠTA, J., MYŠKA, M. a STUPKA, V. *Elektronické důkazy v trestním řízení*. Op. cit., s. 201-202

⁴⁴⁶ MAREŠOVÁ, E. *Problematika získávání informací z mobilních telefonů v rámci trestního řízení*. Trestněprávní revue, 2021, č. 3, s. 146-155

⁴⁴⁷ DOSTÁL, O. *Zajišťování důkazů u počítačové kriminality – úložiště, e-maily, telefony, sociální sítě a logy* (4. díl). Trestněprávní revue, 2019, č. 6, s. 123-127

⁴⁴⁸ Vyplývající ze zákona o elektronických komunikacích; na zajištění komunikace do budoucna je nutné užití postupu dle ustanovení § 88 trestního řádu.

⁴⁴⁹ MAREŠOVÁ, E. *Problematika získávání informací z mobilních telefonů v rámci trestního řízení*. Op. cit. s. 146-155

Obsah nosiče informací je ve stanovisku nepřímě přirovnáván k obsahu listin uchovávaných v soukromí, přihlédneme-li však k „výčtu soukromých informací, které zpravidla [mobilní telefon] obsahuje, je zásah způsobený přístupem k celému jeho obsahu nesrovnatelný s přístupem k obsahu například dopisu či smlouvy.“⁴⁵⁰ S ohledem na množství nejrůznějších dat, která může mobilní telefon obsahovat, jak bylo naznačeno v úvodu této podkapitoly, se jedná se o velmi významný zásah do práva na *informační sebeurčení*. Ačkoliv toto právo může být prolomeno, mělo by se tak dít na základě principu proporcionality.

Vzhledem k výše uvedenému, je tedy naprosto nezbytné, aby orgány činné v trestním řízení při zajišťování obsahu dbaly na zásadu přiměřenosti a zdrženlivosti. To však v případě současně aplikované metodiky není naplňováno.

De lege ferenda by tak bylo vhodné, aby zákonodárce zakotvil přílehlavý právní rámec či NSZ při tvorbě metodiky zvažilo sjednocení spočívající např. v užití nabízejícího se ustanovení § 158d odst. 3 trestního řádu, které nastavuje přísnější podmínky a jeho aplikace podléhá souhlasu soudce. K názoru, že pro přístup do obsahu chytrého mobilního telefonu je nutný souhlas soudce, dospěl již v roce 2014 ve svých rozhodnutích *United States v. Wurie*⁴⁵¹ a *Riley vs. California*⁴⁵² i Nejvyšší soud Spojených států. Předseda Nejvyššího soudu John Roberts se ve svém stanovisku k rozhodnutí vyjádřil v tom smyslu, že „*mobilní telefony se jak kvantitativně, tak kvalitativně liší od jiných předmětů, které může mít zatčený u sebe*“,⁴⁵³ což vyvolává mnohem větší obavy o soukromí než prohlídka jiných předmětů.⁴⁵⁴

Nezbývá než připomenout, že pokud orgán činný v trestním řízení nemá mobilní telefon ve své dispozici a zajišťuje informace *jiným způsobem*, přichází v úvahu užití zákonných postupů, kde jsou podmínky⁴⁵⁵ nepoměrně přísnější. Vezmeme-li v úvahu, že informace, které jsou příslušné orgány z mobilního telefonu schopny získat, jsou mnohdy způsobilé určit i psychologický profil uživatele takového zařízení⁴⁵⁶, je současná právní úprava a její aplikační praxe zcela neproporcionální.

⁴⁵⁰ *Tamtéž*.

⁴⁵¹ Rozhodnutí Nejvyššího soudu Spojených států ve věci *United States v. Wurie* z 25. 6. 2014, 728 F.3d 1

⁴⁵² Rozhodnutí Nejvyššího soudu Spojených států ve věci *Riley v. California* z 25. 6. 2014, 573 U.S. 373

⁴⁵³ *Tamtéž*.

⁴⁵⁴ REIBER, L. *Mobile forensic investigations: a guide to evidence collection, analysis, and presentation*. Second edition. New York: McGraw-Hill Education, 2019. ISBN 978-1-260-13509-1. s. 86-87

⁴⁵⁵ Srov. podmínky určující pro jaké trestné činy je možné ustanovení užít; omezení v podobě souhlasu soudce či státního zástupce; přezkum

⁴⁵⁶ POLČÁK, R., PŮRY, F., HARAŠTA, J., MYŠKA, M. a STUPKA, V. *Elektronické důkazy v trestním řízení*. Op. cit., s. 197

5. Aplikační praxe

V rámci vypracování své diplomové práce jsem se rozhodla kontaktovat policisty, uskutečnit s nimi *rozhovory*, a získat tak poznatky z praxe. Pro účely této práce však uvádím pouze jméno policisty působícího u *Služby kriminální policie a vyšetřování Oddělení analytiky a kybernetické kriminality, Obvodního ředitelství, Prahy-IV*, druhého policistu, který mi poskytl rozhovor a jež působí v rámci *Národní centrály proti organizovanému zločinu služby kriminální policie a vyšetřování*, zachovávám v anonymitě.

5.1. Národní centrála proti organizovanému zločinu

První rozhovor jsem vedla s policistou, který působí jako analytik na *Národní centrále proti organizovanému zločinu služby kriminální policie a vyšetřování*. Jedná se o útvar s celostátní působností, který se zabývá odhalováním organizovaného zločinu, závažné hospodářské kriminality, finanční kriminality a korupce.

5.1.1. Rozhovor s policistou

Policista v úvodu našeho rozhovoru uvádí, že *elektronickým důkazním prostředkem* může to být prakticky vše, veškeré elektronické nosiče, které mohou obsahovat relevantní informace, tj. digitální data. Velkým problémem policejního orgánu však je zahlcenost balastními daty, jež pro trestní řízení nejsou relevantní. Přesto je orgán činný v trestním řízení musí zkoumat a dostat se k těm důležitým. Forenzní analýza dat je tímto značně ztížena. S rostoucím časem stále kontinuálně stoupá i množství dat, což je opravdu velký problém. Příkladem je mj. účetnictví, které dříve probíhalo papírově, ale dnes je téměř vše prováděno pomocí programů na počítači.

Zmíněná zahlcenost daty klade vysoké nároky nejen na výpočetní výkon a kapacitu úložiště, ale ze strany policejního orgánu je nutné používat i sofistikovanější nástroje. Existují nejrůznější forenzní software programy, které data získaná z nosiče roztrídí podle typu souboru. Umělá inteligence policejním orgánům pomáhá např. k třídění informací skrze IČO, textu nacházejícího se na fotografiích a printscreech obrazovky. Dále je používána např. na audio nahrávky, pokud je sinusoida neměnná (nikdo nemluví), dá se tato část automaticky vymazat. V případě, kdy je v pozadí rádio nebo televize, není však tento postup možný a podstatně to práci ztěžuje. Dalším příkladem může být i videozáznam z kamery, kdy je např. u videonahrávky náměstí umožněno (pomocí umělé inteligence) vybrat pouze určitou část, kde víme, že mělo dojít k relevantní události. Ona nám sama zaznamená, když tuto „čáru“ někdo překročí a vybere z videa pouze relevantní části. Lze shrnout, že velmi často je technicky

i legálně zajištění a vyhodnocení dat možné, ale jejich množství analýzu velmi zpomaluje či téměř znemožňuje. Je však třeba připomenout, že orgány činné v trestním řízení jsou z principu jeden až dva roky pozadu, a to ve smyslu technologického vybavení. Roste i složitost šifrování a míra zabezpečení zařízení.

V rámci zajištění dat se vždy udělá originál a nejlépe ještě na místě i ověřená kopie. Nikdy se však nepracuje s originálem, vždy se používá pouze kopie. Policista v této souvislosti používá spojení, že existují pouze „*data zálohovaná*“ a „*data ztracená*“, upozorňuje tím tak na důležitost pořízení kopie. Záloha se provádí vždy po zajištění dat na nějaký z nosičů informací (např. SSD, flashdisk, nepřepisovatelné CD), dříve se zálohovalo na jeden hard disk. Je však nebezpečí, že hard disk se znehodnotí, a tím dojde i ke ztrátě dat. Po zajištění dat se vytvoří kontrolní součet, tzv. *hash kód* (data jsou pořád stejná, záruka nezměnitelnosti), jakmile by v obsahu byl navíc, byť i jediný bit, *hash kód* se změní. Naproti tomu v případě, když dojde k přejmenování či přesunutí na jiné úložiště, ale obsah zůstane stejný, *hash kód* se nezmění. Jde tedy o neměnnost obsahu, která je při zajišťování digitálních stop velmi důležitá pro zabezpečení zákonnosti takového zajištění. Provedení kontrolního součtu na místě však není nutnou podmínkou, např. pokud je nosičů velké množství, nebo to situace na místě ohledání/domovní prohlídky či prohlídky jiných prostor, z časových důvodů neumožňuje. Nosič informací se však vždy vloží do speciálního obalu určeného na důkazy, např. do *orgatechu*, a *hash kód* se udělá potom (je zde nezbytná přítomnost osoby dosvědčující, že tomu tak bylo). V takovém případě je to ale považováno za důkaz věcný.

Přezkoumatelnost u soudu zajistí v případě fyzických důkazů pečeť, nebo vložení do speciálního obalu. Pokud se jedná o elektronický důkaz, musí se zajistit jeho neměnnost, ta se provádí způsobem, který by se dal nazvat až primitivním. Je jím např. fotografie (vždy se scrolluje a znovu vyfotí), printscreen či záznam obrazovky počítače. Jde o zajištění důkazu o tom, že v dané chvíli byly v počítači konkrétní složky, otevřené záložky, chaty (a co v nich bylo). U technika je vždy přítomna i nezúčastněná osoba,⁴⁵⁷ která následně podepisuje protokol o tom, že byla při daném úkonu a technik nic nepozměnil. Výstupem může být např. protokol o domovní prohlídce či prohlídce jiných prostor, do kterého se musí zanést, zda technik na místě udělal kontrolní součet. Nezúčastněná osoba podepisuje, že toho byla svědkem.

Pokud v praxi přijede technik na místo,⁴⁵⁸ zajistí např. kameru na domě, flashdisk, vytvoří *hash kód* a nechá podepsat protokol nezúčastněnou osobou či uživatelem nosiče

⁴⁵⁷ Tou může být i sám uživatel, jemuž se nosič zajišťuje, kdokoli v kanceláři, rodinní příslušníci, starosta apod.

⁴⁵⁸ V rámci domovní prohlídky, prohlídky jiných prostor, nebo ohledání.

informací. Jak již bylo zmíněno, pokud je na to čas již na místě, udělá se bezprostředně i záloha. Do protokolu se pak přímo uvádí, že originál je např. na CD, a zároveň kopie na SSD. Pokud se jedná o velké množství dat, napíše se, že byla vytvořena bitová kopie pevného disku zařízení s popisem tohoto zařízení.

V závěru rozhovoru policista dodává, že čím níže postavený útvar Policie ČR, tím méně je odborníků na zajišťování elektronických důkazních prostředků. S tím souvisí, že bohužel není kladen takový důraz na to, zda je zajišťován věcný či elektronický důkaz, resp. s elektronickým důkazem je zacházeno jako s důkazem věcným.

5.2. Oddělení analytiky a kybernetické kriminality

Druhý rozhovor mi poskytl policista por. Mgr. Karel Svoboda působící jako komisař v rámci *Služby kriminální policie a vyšetřování, Oddělení analytiky a kybernetické kriminality, Obvodního ředitelství, Prahy-IV*. Tento úvar má územně vymezenou působnost na území městských částí Prahy 4, Prahy 10, Prahy 11, Prahy 12, Prahy 15 a Prahy 22.

5.2.1. Rozhovor s policistou

Tento rozhovor probíhal jako druhý, z tohoto důvodu jsem své otázky související s elektronickými důkazy zaměřovala již jen na vybrané informace, které jsem chtěla upřesnit. Policista ihned ze začátku podotýká, že samotný přístup k zajištění elektronických dat jako věcí je nepřiléhavý, jelikož zatímco zajištěná věc se vrací,⁴⁵⁹ zajištěná data nikoliv.

Při zajišťování elektronických dat z emailu policejní orgán žádá soud, který vydá povolení/nařídí provedení, následně je žádán *Útvar zvláštních činností služby kriminální policie a vyšetřování*, který potřebná data získává od poskytovatelů služeb. V souvislosti s přístupem k obsahu zpráv v emailové schránce pokládá policista za (v praxi) nepochopitelné, že pro přístup k datům budoucím i minulým je třeba užít obě ustanovení, tj. užitím ustanovení § 88 trestního řádu o odposlechu je možné se dostat jen k datům budoucím, nikoliv však k obsahu schránky k datu zajištění (a je tedy nutné žádat současně o povolení sledování podle ustanovení § 158d odst. 3 trestního řádu). Navíc přísnost ustanovení o odposlechu je vzhledem k tomu, jak to funguje v praxi, nepřiléhavá. Nejde totiž o odposlech v reálném čase, poskytovatelé pouze občas během dne pošlou žádaná data. Dle policisty by bylo lepší užití ustanovení o sledování, protože fakticky dochází ke sledování. Pokud by odposlech fungoval tak, jak má, vše by bylo zaznamenané. V praxi se ale například nelze dostat ani k vymazaným

⁴⁵⁹ Ne však výlučně, srov. propadnutí věci § 70 trestního zákoníku, zabránění věci § 101 trestního zákoníku

zprávám. Příkladem uvádí způsob komunikace pachatelů ve složce *rozepsaných* zpráv a jejich průběžné mazání. Nejen, že se policejní orgán v tomto případě musel trefit přímo do konkrétních časů, ale i tak zde byla v danou chvíli jen jedna zpráva. Zmiňuje, že *de lege ferenda* by mělo existovat ustanovení umožňující získání obsahu celé emailové schránky, které by např. vyžadovalo souhlas státního zástupce. Opakuje, že zásah v podobě získávání obsahu emailové schránky v reálném čase se nedá srovnat se zásahem do základních práv v podobě telefonního odposlechu, a poukazuje tak na přísnost tohoto ustanovení ve vztahu k jeho užití na obsah emailových schránek.

Obecně je však mnohem větší problém s přeshraničními poskytovateli. Na základě ustanovení § 88a trestního řádu lze získat pouze provozní a lokalizační údaje. Pro získání obsahu emailové schránky je však třeba užít mechanismu mezinárodní právní pomoci, ta už poté záleží na poskytovateli služeb. V tomto ohledu však zajišťování naráží zejména na časový problém, jelikož trvá velmi dlouho. Např. Gmail si navíc ještě vyhrazuje právo údaje vůbec nevydat. Ve svých licenčních podmínkách má dokonce ustanovení, že co je obsahem emailových schránek, je oprávněn sám použít. Sami poskytovatelé tak (na základě licenčních podmínek) přichází s podněty na Policii ČR.

V neposlední řadě se policista vyjadřuje k technickému zabezpečení nezměnitelnosti dat při jejich analýze. Nosič informací připojí ke speciálnímu zařízení, které zajistí integritu a neměnnost. Toto technické zařízení umožní data číst a nezapisovat (na disku se pouze zaznamená, že se roztočilo), ale kontrolní součet, resp. *hash kód* se nezmění. Existují dva typy *hash kódů*, MD5 – jeho vytvoření trvá krátce, ale je kratší a SHA256 – ten je průkaznější. V praxi se vytváří oba.

Policista na závěr zdůrazňuje, že vždy záleží, na „co vše“ je povolení k domovní prohlídce. Musí tam být specifikováno kvůli čemu a za jakým účelem je vydáno, to jediné je pak možné v rámci tohoto úkonu zajistit.

Závěr

Informační a komunikační technologie jsou bezpochyby aktuálním tématem a přináší do právní praxe nejen *nové možnosti*, ale zejména jsou *velkou výzvou* pro trestní proces. S ohledem na neustálý nárůst jejich užití a přenos mnohých aktivit do online prostředí jsou orgány činné v trestním řízení v rámci dokazování čím dál více vedeny k využití *elektronických důkazních prostředků*. Ty jsou zdrojem mnohých informací o našem životě. V současné době příslušné orgány využívají procesních institutů, které jsou ve vztahu k nim aplikovány analogicky,⁴⁶⁰ ne vždy je ale v praxi zcela sjednoceno jejich užití, a ne vždy jsou tyto procesní instituty pro dané zdroje důkazů přiléhavé. Se stále se měnící dobou navíc i adekvátnost užití určitých institutů, o které se dalo mluvit před pár lety, nemusí být vzhledem k nárůstu množství informací nacházejících se na zařízení či službě,⁴⁶¹ aktuální.

Cílem této práce bylo *analyzovat současnou právní úpravu a zhodnotit, zda je vzhledem k neustálému vývoji moderních technologií dostačující a efektivní. Současně s tím byla hodnocena i vhodnost užití těchto institutů ve vztahu k zárukám ochrany základních lidských práv*. Mám za to, že tento cíl byl splněn, neboť analýza procesních institutů trestního řádu byla provedena z několika hledisek, a tudíž komplexně. Mimo průběžné hodnocení v textu práce je v následujících odstavcích provedeno shrnující zhodnocení odpovídající na vymezenou výzkumnou otázku. Jelikož je obsah práce velmi široký, shrnutí se týká pouze nejdůležitějších bodů rozebírané problematiky.

Aplikace *současných institutů trestního řádu* orgány činnými v trestním řízení pro zajištění elektronických důkazů je poměrně komplikovaná.

Pokud se jedná o zajištění obsahu *elektronické komunikace*, např. emailových schránek, a není-li obsažen přeshraniční prvek, považuji užití ustanovení o sledování osob a věcí (§ 158d odst. 3 trestního řádu) pro zprávy již *doručené* a ustanovení o odposlechu (§ 88 trestního řádu) pro zprávy *do budoucna* za *dostačující přesto nepřiléhavé*. Ustanovení upravující odposlech je, s ohledem na to, pro jaké trestné činy ho lze nařídit, přísné. Naproti tomu ustanovení o sledování osob a věcí je, ve vztahu k ustanovení o odposlechu, až nepoměrně široké. Současně je nutné připomenout okolnost, že přístup k obsahu elektronické komunikace *do budoucna* fakticky neprobíhá v daném momentu⁴⁶², ale jedná se o výpisy zasílané zpětně (s určitou pravidelností) policejnímu orgánu, tj. není tomu jako u odposlechu *per se*. Z tohoto důvodu bych *de lege*

⁴⁶⁰ Ne výlučně, srov. § 7b trestního řádu

⁴⁶¹ Např. mobilní telefony, které nyní oproti minulosti obsahují zásadně rozdílné (větší) množství informací

⁴⁶² V současné praxi, aktuální ke dni uzavření rukopisu této práce.

ferenda navrhla určité *přiblížení*⁴⁶³ *výctu trestných činů*, pro které je možné procesní instituty v případě elektronické komunikace užít, a to tak, aby užití bylo pro policejní orgán efektivní, přesto však bylo dostatečně omezující, a tudíž chránilo základní práva jednotlivce.

Ačkoliv oba procesní instituty (§ 88 trestního řádu a § 158d odst. 3 trestního řádu) obsahují záruky v podobě nutnosti nařízení soudcem, jako velmi problematickou shledávám *chybějící informační povinnost* orgánu činného v trestním řízení a s ní spojenou *možnost přezkumu zákonnosti povolení* ze strany Nejvyššího soudu v případě postupu dle ustanovení o sledování osob a věcí. Tuto neproporcionalitu prostředků ochrany vnímám směrem k zajišťování obsahu elektronické komunikace za nesprávnou. Považuji tak za vhodné, aby zákonodárce *de lege ferenda* tyto záruky ochrany zásahu do práv osob, jež jsou garantována Listinou, sjednotil, resp. *rozšířil* i pro ustanovení o sledování osob a věcí.

Za zcela nerefluktující, zejména s nárůstem množství informací uchovávaných na elektronických zařízeních, však shledávám postup při zajištění obsahu (zpráv)⁴⁶⁴ v případě, kdy má orgán činný v trestním řízení ve své dispozici nosič informací. V tomto ohledu umožňuje výkladové stanovisko NSZ č. 4/2005 ve spojení se stanoviskem NSZ č. 1/2015 přístup k obsahu nosiče informací bez dalších procesních institutů, než kterých bylo zapotřebí pro získání daného zařízení. To považuji za nepřijatelné, zejména např. u chytrých mobilních telefonů či notebooků, jelikož na tomto základě tak může dojít k prolomení práva na informační sebeurčení bez dalších procesních záruk. Přestože proti může stát argument, že nutnost povolování (a s tím spojená délka řízení) může být v rozporu se zájmem společnosti na stíhání trestné činnosti, je s ohledem na digitalizaci společnosti nutné stát za vyšší ochranou práva jednotlivce na soukromí. Možným návrhem *de lege ferenda* by zde mohlo být *rozlišení nosičů informací*, pro které je *nutností užití dalšího procesního ustanovení obsahujícího procesní záruky* ve formě povolení soudce, popř. následného přezkumu zákonnosti. V této souvislosti by bylo za takový nosič informací bezesporu vhodné určit chytrý mobilní telefon.

V případech, kde je *obsažen přeshraniční prvek*, je pro získávání elektronických důkazů nezbytné využít mezinárodních institutů spolupráce. To je v dnešní době globalizace společnosti poměrně častým jevem, jelikož poskytovatelé služeb jsou často zahraničními

⁴⁶³ Záměrně není užito slovo sjednocení, jelikož je bezesporu, že získávání obsahu *do budoucna* je větším zásahem do práv osob. Ve směru k možnosti užití ustanovení o sledování osob a věcí (na již *doručenou komunikaci*) je však naopak okruh trestných činů, pro které je možné ho nařídit, až příliš široký.

⁴⁶⁴ Týká se obsahu zpráv *přijatých na nosiči informací do doby jeho zajištění*. Pro obsah zpráv *do budoucna* je v praxi užíváno i v případě zajištěného nosiče ustanovení § 88 trestního řádu.

osobami a elektronické důkazy tak podléhají jurisdikci jiného státu.⁴⁶⁵ Vzhledem k nestálosti těchto důkazů je nezbytné zakotvení mechanismů, které nad rámec smluv o mezinárodní právní pomoci mezi jednotlivými státy umožní jejich *získání urychleně*, případně bude jejich prostřednictvím možné získávané údaje *po určitou dobu uchovat*. V tomto směru za poslední rok značně pokročila jak sama Evropská unie přijetím nařízení o evropském vydávacím příkazu a evropském uchovávacím příkazu, tak ve spolupráci se Spojenými státy znovuoobnověním vyjednávání týkajícího se možného uzavření výkonné dohody na základě zákona CLOUD Act. Velmi aktuálním je také druhý dodatkový protokol k Budapešťské úmluvě, který byl přijat Radou Evropy a otevřen státům k podpisu.

Zaměříme-li se na unijní legislativu, ta zakotvuje umožnění *přímé spolupráce orgánů činných v trestním řízení a poskytovatelů služeb* při přeshraničním získávání elektronických důkazů. Na základě evropského vydávacího příkazu tak bude umožněno získat důkazy od poskytovatele v jiném členském státě do 10 dní (v naléhavých případech do 8 hodin). To lze i přes diskutovaná negativa, která s sebou nařízení přináší a jež nelze opomínat⁴⁶⁶, hodnotit pozitivně, jelikož na základě již dříve zakotveného unijního mechanismu v podobě evropského vyšetřovacího příkazu tento proces trval až 120 dní (za užití vzájemné právní pomoci až 10 měsíců). Současně s ním byl zaveden i evropský uchovávací příkaz, kterým lze poskytovatele služeb žádat o uchování příslušných údajů v souvislosti s dalším postupem. Tyto nástroje tak mají za cíl pomoci současné situaci přeshraniční spolupráce, která je v dnešním světě již neefektivní. Použitelnost těchto právních mechanismů na úrovni členských států je stanovena na 17. srpna 2026.

Všechny tyto nové přeshraniční přístupy k elektronickým důkazním prostředkům (či diskuze nad nimi) lze hodnotit, vzhledem k technologickému pokroku a množství důkazů v elektronické podobě, jako krok správným směrem. Kritiku ze strany států a odborníků směřující zejména k obavám z (ne)náležitě ochrany základních lidských práv, jež je s touto problematikou neoddělitelně spojena, je však třeba považovat za odůvodněnou. Správné vyvážení právní úpravy, *umožňující efektivní přístup k elektronickým důkazům a současně poskytující ochranu základním právům osob*, je z mého pohledu klíčové.

Nezbývá než uzavřít, že pokrok není možné zastavit, a stejně tak nesmíme zastavit odezvu práva na něj a vývoj nových technologií ignorovat. Přílehlavý právní rámec je tak nezbytným předpokladem pro to, aby byl technologický potenciál využit účinně a souběžně

⁴⁶⁵ Mimo to se mohou fyzická úložiště dat těchto poskytovatelů nacházet ve třetí zemi.

⁴⁶⁶ Viz kapitola 3.2.2.1. této práce

nedocházelo k nepřiměřenému zásahu do ústavně garantovaných práv. Ačkoliv je, jak bylo shrnuto výše, současná právní úprava dostačující k tomu, aby měly (za pomoci analogie) orgány činné v trestním řízení přístup k elektronickým důkazům, domnívám se, že vzhledem k neustávajícímu nárůstu nových výzev v oblasti technologií, není tento stav udržitelný. Nejen, že současná praxe vychází z metodiky Nejvyššího státního zastupitelství, která již nereflektuje současný stav poznání o informačních a komunikačních technologiích, ale i aplikace na jejím základě je mnohdy nejednotná. Uvážíme-li, že trestní právo vychází ze zásad, jakými je například *subsidiarita trestní represe* či *in dubio pro reo*, jejichž smyslem je z velmi obecného hlediska obezřetnost a opatrnost, je nepřipustné, aby nebyla stanovena právní úprava reflektující existenci informačních a komunikačních technologií, která jednotlivcům poskytne právní jistotu.

Z mého pohledu by tak mělo *de lege ferenda* dojít ke komplexní legislativní změně týkající se *procesní úpravy elektronických důkazních prostředků, včetně samotného zakotvení definice tohoto pojmu*. Mám za to, že pouze touto cestou bude v době *digitální revoluce* zaručena předvídatelnost práva a naplněny požadavky ochrany kladené lidskoprávními katalogy. A jedině tak bude možné s dobou, která přináší neustále nové technologické výzvy, *udržet krok*.

Seznam zkratek

Budapešťská úmluva	Sdělení č. 104/2013 Sb. m. s., Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě
ESLP	Evropský soud pro lidská práva
Evropská úmluva	Sdělení č. 209/1992 Sb., o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících
GDPR	Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
Listina	Usnesení č. 2/1993 Sb., předsednictva České národní rady o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky, ve znění pozdějších ústavních zákonů
Listina EU	Listina základních práv Evropské unie
Soudní dvůr EU	Soudní dvůr Evropské unie
Spojené království	Spojené království Velké Británie a Severního Irska
Spojené státy	Spojené státy americké
trestní řád	Zákon č. 141/1961 Sb., o trestním řízení soudním
trestní zákoník	Zákon č. 40/2009 Sb., trestní zákoník
Ústava	Ústavní zákon č. 1/1993 Sb., Ústava České republiky.
výkladové stanovisko NSZ č. 4/2005	BENEŠOVÁ, M. Stanovisko ke sjednocení výkladu zákonů a jiných právních předpisů k postupu v případech, kdy je třeba pro účely trestního řízení zjistit obsah údajů uložených v nalezeném, vydaném či odňatém mobilním telefonu, včetně údajů uložených na SIM kartě. Sbíрка výkladových stanovisek nejvyššího státního zastupitelství, 2005, č. 4

výkladové stanovisko NSZ č. 1/2015	ZEMAN, P. Stanovisko ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek. Sbírnka výkladových stanovisek nejvyššího státního zastupitelství, 2015, č. 1
zákon o elektronických komunikacích	Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů
zákon o mezinárodní justiční spolupráci ve věcech trestních	Zákon č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních
zákon o některých službách informační společnosti	Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů

Seznam použitých zdrojů

1. Seznam použité literatury

Monografie a komentáře

CASEY, E., BRENNER, S. W., KOOPS, B., ROBINSON, T., SCHATZ, B. et al. *Digital evidence and computer crime: forensic science, computers and the internet*. Third edition. Amsterdam: Elsevier Academic Press, 2011. ISBN 978-0-12-374268-1.

FENYK, J., CÍSAŘOVÁ, D., GRĚVNA, T. a kol. *Trestní právo procesní*. 7. vydání. Praha: Wolters Kluwer ČR, 2019, 952 s. ISBN 978-80-7598-306-0.

GRĚVNA, T. a POLČÁK, R. *Kyberkriminalita a právo*. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4.

GRĚVNA, T., RICHTER, M. a ŠIMÁNOVÁ, H. *Vliv nových technologií na trestní právo*. Praha: Auditorium, 2022. ISBN 978-80-87284-95-7.

HENDRYCH, D. a kol. *Právní slovník*. 3. vydání. Praha: C. H. Beck, 2009.

HUSSEINI, F., BARTOŇ, M., KOKEŠ, M., KOPA, M. a kol. *Listina základních práv a svobod*. 1. vydání (1. aktualizace). Praha: C. H. Beck, 2021

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

JELÍNEK, J. *Trestní právo procesní*. 7. aktualizované a doplněné vydání podle stavu k 1.9. 2023. Praha: Leges, 2023. ISBN 978-80-7502-687-3.

JELÍNEK, J. *Trestní zákoník a trestní řád s poznámkami a judikaturou: zákon o soudnictví ve věcech mládeže, zákon o trestní odpovědnosti právnických osob a řízení proti nim, advokátní tarif*. 9. aktualizované vydání. Praha: Leges, 2022. ISBN 978-80-7502-637-8.

KALVODOVÁ, V., ŠÁMAL, P. a HRUŠÁKOVÁ, M. *Dokazování v trestním řízení – právní, kriminologické a kriminalistické aspekty*. Brno: Masarykova univerzita, 2015. ISBN 978-80-210-8072-0.

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

MASON, S., SENG, D.. *Electronic evidence*. Fourth edition. London: Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017. ISBN 1-911507-07-9.

POLČÁK, R., PÚRY, F., HARAŠTA, J., MYŠKA, M. a STUPKA, V. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015, ISBN 978-80-210-8073-7.

POLČÁK, R. a kol. *Právo informačních technologií*. Praha: Wolters Kluwer ČR, 2018, 656 s., ISBN 978-80-7598-045-8.

POLČÁK, R. *Právo na internetu: spam a odpovědnost ISP*. Brno: Computer Press, 2007. ISBN 978-80-251-1777-4., s. 16

PORADA, V. *Kriminalistika: technické, forenzní a kybernetické aspekty*. 2. aktualizované a rozšířené vydání. Plzeň: Aleš Čeněk, 2019. ISBN 978-80-7380-741-2.

REIBER, L. *Mobile forensic investigations: a guide to evidence collection, analysis, and presentation. Second edition*. New York: McGraw-Hill Education, 2019. ISBN 978-1-260-13509-1.

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

SUMNER, S. *You: For Sale: Protecting Your Personal Data and Privacy Online*, 2015. ISBN 978-0-12-803405-7.

ŠÁMAL, P. a kol. *Trestní řád*. 7. vydání. Praha: C. H. Beck, 2013. ISBN 978-80-7400-465-0.

ŠÁMAL, P. a kol. *Trestní zákoník*. 3. vydání. Praha: C. H. Beck, 2023

ZAORALOVÁ, P. *Procesní použitelnost důkazů v trestním řízení a její meze*. Praha: Leges, 2018. ISBN 978-80-7502-310-0.

Odborné články

DOSTÁL, O. *Zajišťování důkazů u počítačové kriminality – dožádání, vydání věci a prohlídka (1. díl)*. Trestněprávní revue, 2019, č. 3, s. 66-71

DOSTÁL, O. *Zajišťování důkazů u počítačové kriminality – úložiště, e-maily, telefony, sociální sítě a logy (4. díl)*. Trestněprávní revue, 2019, č. 6, s. 123-127

GRÍVNA, T. *Právo na zachování důvěrné komunikace mezi advokátem a jeho klientem*. Bulletin Advokacie. 2017, č. 6, s. 61–66

HERCZEG, J. *Zásada „nemo tenetur“ a práva obviněného v trestním řízení*. Bulletin advokacie, 2010, č. 1-2, s. 38-47

HLAVÁČOVÁ, K., CHORVÁT, O. *Přístup orgánů činných v trestním řízení k datům uloženým v cloudu*. Revue pro právo a technologie, 2016, č. 14, s. 3-24

JELÍNEK, J. *K chybějící právní úpravě tzv. prostorového odposlechu v trestním řádu*. Bulletin advokacie, 2018, č. 7-8, s. 13-19

JELÍNEK, M. *Ústavní meze prostorových odposlechů ke sledování osob a věci podle § 158d trestního řádu*. Bulletin advokacie, 2010, č. 5, s. 31-33

MAREŠOVÁ, E. *Problematika získávání informací z mobilních telefonů v rámci trestního řízení*. Trestněprávní revue, 2021, č. 3, s. 146-155

SMEJKAL, V. *Ochrana dat advokátů v elektronických úložištích*. Bulletin advokacie, 2015, č. 3, s. 15-22

STAŇKOVÁ, P. *Vyšetřování kybernetické kriminality a její budoucí předpokládaný vývoj*. Revue pro právo a technologie, 2023, č. 28, s. 31-60

STUPKA, V., PROVAZNÍK, J., VOSTOUPAL J. *Elektronické důkazy jako výzva pro trestní proces*. 2022, Právník 4/2022, Ročník 161, s. 335

TLAPÁK NAVRÁTILOVÁ, J., GALOVCOVÁ, I. *Uchovávání dat uložených v počítačovém systému – poskytování součinnosti, nebo nahrazování činnosti orgánů činných v trestním řízení?*. Bulletin advokacie, 2019, č. 11, s. 36-39

VANTUCH, P. *Nezákonný odposlech advokáta*. Bulletin advokacie. 2008, č. 3, s. 15–24

2. Seznam použitých internetových zdrojů

Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR za rok 2022, [online], [cit. dne 7. 1. 2024], dostupné z: <https://www.mvcr.cz/clanek/odposlechy-zaznamy-telekomunikacniho-provozu-a-sledovani-osob.aspx>

CEPS: Centre for Europea Policy Studies. *Cross-border data access in criminal proceedings and the future of digital justice*. In: <https://www.ceps.eu> [online]. [25. 1. 2024]. Dostupné z: <https://cdn.ceps.eu/wp-content/uploads/2020/10/TFR-Cross-Border-Data-Access.pdf>

ČERNÁ, M., ČERNÝ, M. *Úvod do problematiky sociálních sítí*. In: Metodický portál RVP.CZ [online]. [cit. 26. 1. 2024]. Dostupný z: <http://clanky.rvp.cz/clanek/o/g/15075/UVOD-DO-PROBLEMATIKY-SOCIALNICH-SITI.html/>

ČTK, *Zsuzsová měla vyšší tep, Kočner pročítal média. Objevily se nové důkazy ke Kuciakovi*. In: Aktuálně.cz [online]. [cit. 27. 1. 2024]. Dostupné z: <https://zpravy.aktualne.cz/zahranici/zsuzsova-mela-vyssi-tep-kocner-procital-media-objevily-se-no/r~760f8d0c729011ebb0fa0cc47ab5f122/>

ČT24. *Mironet se dál soudí se státem, odškodné za policejní zásah může přesáhnout miliardu ČT24* [online]. 2017 [cit. 2023-12-13]. Dostupné z: <https://ct24.ceskatelevize.cz/clanek/ekonomika/mironet-se-dal-soudi-se-statem-odškodne-za-policejni-zasah-muze-presahnout-miliardu-100371>

Datareportal, *Global Social Media Statistics*, 2023 In: datareportal.com. [online]. 2023 [cit. 26.1.2024] Dostupný z: <https://datareportal.com/social-media-users>

EDPB, *Evropský sbor pro ochranu osobních údajů – dvanácté plenární zasedání*, [www.edpb.europa.eu](https://edpb.europa.eu). [online]. 2019 [cit. 25. 1. 2024], Dostupné z: https://edpb.europa.eu/news/news/2019/european-data-protection-board-twelfth-plenary-session_cs

EDPS, *ANNEX. Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence*. In: www.edpb.europa.eu. [online]. [cit. 25. 1. 2024]. Dostupný z: https://edpb.europa.eu/sites/default/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf

EDPS, *EDPS Opinion on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters*. Opinion 7/2019., 6. listopadu 2019.

[online]. 2019 [cit. 24. 1. 2024]. Dostupné z: https://edps.europa.eu/sites/default/files/publication/19-11-06_opinion_on_e_evidence_proposals_en.pdf

EUROPEAN E-JUSTICE: *Evropský vyšetřovací příkaz, vzájemná právní pomoc a společné vyšetřovací týmy*, e-justice.europa.eu [online]. 2019 [cit. 24. 1. 2024], Dostupné z: https://e-justice.europa.eu/content_european_investigation_order_mutual_legal_assistance_and_joint_investigation_teams-92-cs.do

European Union Agency For Criminal Justice Cooperation. *Joint investigation team into alleged crimes committed in Ukraine*. In: eurojust.europa.eu. [online]. [cit. 24. 1. 2024]. Dostupné z: <https://www.eurojust.europa.eu/joint-investigation-team-alleged-crimes-committed-ukraine>

European Union Agency For Criminal Justice Cooperation. *Joint investigation teams*. In: eurojust.europa.eu. [online]. [cit. 24. 1. 2024]. Dostupné z: <https://www.eurojust.europa.eu/judicial-cooperation/eurojust-role-facilitating-judicial-cooperation-instruments/joint-investigation-teams>

European Union Agency For Criminal Justice Cooperation. *The COUD Act*. In: eurojust.europa.eu. [online]. [cit. 25. 1. 2024]. Dostupné z: <https://www.eurojust.europa.eu/publication/cloud-act>

Evropská Komise. Ochrana údajů: *Evropská komise přijala nové rozhodnutí o odpovídající ochraně pro bezpečný a spolehlivý tok údajů mezi EU a USA*. In: ec.europa.eu. [online]. [cit. 25. 1. 2024]. Dostupný z: https://ec.europa.eu/commission/presscorner/detail/cs/ip_23_3721

MAXWEL, W., WOLF, Ch., *A Global Reality: Governmental Access to Data in the Cloud*. 2012 [online]. [cit. 26. 1. 2024]. Dostupný z: https://www.hoganlovells.com/-/media/hogan-lovells/pdf/publication/revised-government-access-to-cloud-data-paper-18-july-12_pdf.pdf

MELL, P., GRANCE, T. *The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology*. [online]. 2011 [cit. 28. 1. 2024]. Dostupný z: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

MINÁRIK, T. *Council of Europe Ponders a New Treaty on Cloud Evidence*. CCDCOE, www.ccdcoe.org [online]. 2017 [cit. 23. 1. 2024]. Dostupné z: <https://ccdcoe.org/incyder-articles/council-of-europe-ponders-a-new-treaty-on-cloud-evidence/>

Office of International Affairs. *CLOUD Act Resources*. In: www.justice.gov. [online]. [cit. 25. 1. 2024]. Dostupný z: <https://www.justice.gov/criminal/cloud-act-resources>

POKORNÝ, M. *Mironet, který skoro zničila policejní razie, má nárok na odškodné od státu. Chce 626 milionů*. Aktuálně.cz [online]. 2017 [cit. 2023-12-13]. Dostupné z: <https://zpravy.aktualne.cz/domaci/mironet-ma-opet-sanci-na-stamilionove-odskodne-za-zatah-poli>

PROPP, K. *Navigating Toward an EU-U.S. Agreement on Electronic Evidence*. In: Lawfare. 1. prosince 2023 [online]. 2023 [cit. 24. 1. 2024]. Dostupné z: <https://www.lawfaremedia.org/article/navigating-toward-an-eu-u.s.-agreement-on-electronic-evidence>

RADA EU, *Přístup k elektronickým důkazům: Rada zmocnila členské státy k podpisu mezinárodní dohody*. Tisková zpráva, www.consilium.europa.eu. [online]. 2022 [cit. 23. 1. 2024] Dostupné z: <https://www.consilium.europa.eu/cs/press/press-releases/2022/04/05/access-to-e-evidence-council-authorises-member-states-to-sign-international-agreement/>

RADA EU, *Rada přijala právní předpisy EU o lepším přístupu k elektronickým důkazům*. Tisková zpráva, www.consilium.europa.eu/. [online]. 2023 [cit. 24. 1. 2024] Dostupné z: <https://www.consilium.europa.eu/cs/press/press-releases/2023/06/27/council-adopts-eu-laws-on-better-access-to-electronic-evidence/>

SOKOL, T. *Povinnost dle § 7b trestního řádu z pohledu advokáta*. Advokatnidenik.cz [online]. Česká advokátní komora. Publikováno 2. 8. 2019 [cit. 20. 1. 2024]. Dostupné z: <https://advokatnidenik.cz/2019/08/02/povinnost-dle-%E2%99%A7-7b-tr-radu-z-pohledu-advokata/>

Stálá komise pro kontrolu použití odposlechu a záznamu telekomunikačního provozu, použití sledování osob a věcí a rušení provozu elektronických komunikací. Usnesení č. 25 (23. února 2017) Psp.cz. [online] [cit. 10. 1. 2024]. Dostupné z: <https://www.psp.cz/sqw/text/text2.sqw?idd=102715>

STUPKA, V. *Vzájemná přípustnost elektronických důkazů v EU*. Přednáška. Brno: MUNI LAW, 14. 9. 2023, MUNI LAW, Masarykova univerzita Právnická fakulta. [online]. 2023 [cit. 24. 1. 2024]. Dostupné z: <https://cpit.law.muni.cz/dokumenty/60446>

Summaries of EU Legislation, *Elektronické důkazy v trestním řízení*. 17. 11. 2023. In: EUR-Lex [online]. 2023 [cit. 24. 1. 2024]. Dostupné z: <https://eur-lex.europa.eu/CS/legal-content/summary/electronic-evidence-in-criminal-proceedings.html?fromSummary=23>

TLAPÁK NAVRÁTILOVÁ, J. a GALOVCOVÁ, I. *Uchovávání dat uložených v počítačovém systému – poskytování součinnosti, nebo nahrazování činnosti orgánů činných v trestním řízení*. Advokátní deník. [online] [cit. 5. 1. 2024]. Dostupné z: <https://advokatnidenik.cz/2019/12/11/uchovavani-dat-ulozenych-v-pocitacovem-systemu-poskytovani-soucinnosti-nebo-nahrazovani-cinnosti-organu-cinnych-v-trestnim-rizeni/>

TOMAN, P. *Podstrčený paragraf § 7b trestního řádu*. Kde se vzal a o čem je. Advokatnidenik.cz [online]. Česká advokátní komora. Publikováno 22. 7. 2019 [cit. 20. 1. 2024]. Dostupné z: <https://advokatnidenik.cz/2019/07/22/podstrceny-paragraf-7b-trestniho-radu-kde-se-vzal-a-o-cem-je/>

TOPALNAKOS, P, *Critical Issues in the New EU Regulation on Electronic Evidence in Criminal Proceedings*. Eucrim 2023/2 [online]. 2023 [24. 1. 2024] s. 200-203, Dostupné z: https://eucrim.eu/media/issue/pdf/eucrim_issue_2023-02.pdf#page=94

3. Seznam použitých právních předpisů

Listina základních práv Evropské unie, dokument 2012/C326/02

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

Nařízení Evropského parlamentu a Rady (EU) 2023/1543 ze dne 12. července 2023 o evropském vydávacím příkazu a evropském uchovávacím příkazu pro elektronické důkazy v trestním řízení a pro výkon trestu odnětí svobody po skončení trestního řízení

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

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

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

Sdělení č. 5/2010 Sb. m. s., Ministerstva zahraničních věcí o sjednání Dohody o vzájemné právní pomoci mezi Evropskou unií a Spojenými státy americkými

Sdělení č. 55/2006 Sb. m. s. Ministerstva zahraničních věcí o přístupu České republiky k Úmluvě o vzájemné pomoci v trestních věcech mezi členskými státy Evropské unie, vypracované Radou na základě článku 34 Smlouvy o Evropské unii čl. 4 odst. 1

Sdělení č. 7/2010 Sb. m. s., Ministerstva zahraničních věcí o sjednání Dodatkové úmluvy o vzájemné právní pomoci v trestních věcech mezi Českou republikou a Spojenými státy americkými

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

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

Směrnice Evropského parlamentu a Rady (EU) 2023/1544 ze dne 12. července 2023, kterou se stanoví harmonizovaná pravidla pro určování určených provozoven a jmenování zástupců za účelem shromažďování elektronických důkazů v trestním řízení.

Usnesení č. 2/1993 Sb., předsednictva České národní rady o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky, ve znění pozdějších ústavních zákonů

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

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

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

Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů

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

Zákon č. 222/2016 Sb., o Sbírce zákonů a mezinárodních smluv a o tvorbě právních předpisů vyhlášených ve Sbírce zákonů a mezinárodních smluv (zákon o Sbírce zákonů a mezinárodních smluv), ve znění pozdějších předpisů

Zákon č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů

Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů

Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů, ve znění pozdějších předpisů

Zákon č. 85/1996 Sb., o advokacii, ve znění pozdějších předpisů

4. Seznam použité judikatury

Judikatura českých soudů

Nález Ústavního soudu ze dne 27. 8. 2001, sp. zn. IV. ÚS 78/01

Nález Ústavního soudu ze dne 23. 3. 2006, sp. zn. III. ÚS 644/05

Nález Ústavního soudu ze dne 23. 5. 2007, sp. zn. II. ÚS 615/06

Nález Ústavního soudu ze dne 27. 9. 2007 sp. zn. II.ÚS 789/06

Nález Ústavního soudu ze dne 29. 2. 2008, sp. zn. I. ÚS 3038/07

Nález Ústavního soudu ze dne 28. 4. 2009, sp. zn. I. ÚS 536/06

Nález Ústavního soudu ze dne 28. 8. 2009, sp. zn. II. ÚS 2894/08-2

Nález Ústavního soudu ze dne 8. 6. 2010, sp. zn. Pl. ÚS 3/09

Nález Ústavního soudu ze dne 25. 11. 2010, sp. zn. II. ÚS 889/10

Nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/10

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

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

Nález Ústavního soudu ze dne 14. 5. 2019, sp. zn. Pl. ÚS 45/17

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

Stanovisko Nejvyššího soudu ze dne 25. 6. 2015, sp. zn. Tpjn 306/2014

Usnesení Nejvyššího soudu ze dne 21. 5. 2009, sp. zn. 11 Tdo 349/2009

Usnesení Nejvyššího soudu ze dne 15. 11. 2016, sp. zn. 4 Pzo 14/2016

Usnesení Nejvyššího soudu ze dne 7. 5. 2019, sp. zn. 4 Tdo 1591/2018
Usnesení Nejvyššího soudu ze dne 25. 8. 2020, sp. zn. 8 Tdo 647/2020
Usnesení Nejvyššího soudu ze dne 1. 9. 2020, sp. zn. 7 Tdo 865/2020
Usnesení Městského soudu v Praze ze dne 9. 7. 2014, sp. zn. Nt 615/2014
Usnesení Ústavního soudu ze dne 28. 3. 2002, sp. zn. IV. ÚS 2/02
Usnesení Ústavního soudu ze dne 3. 10. 2013, sp. zn. III. ÚS 3812/12
Usnesení Ústavního soudu ze dne 13. 3. 2014, sp. zn. III. ÚS 859/13
Usnesení Ústavního soudu ze dne 24. 3. 2014, sp. zn. III. ÚS 3988/13
Usnesení Ústavního soudu ze dne 12. 11. 2014, sp. zn. I. ÚS 1638/14
Usnesení Ústavního soudu ze dne 8. 10. 2019, sp. zn. I. ÚS 2838/19
Usnesení Vrchního soudu v Praze ze dne 14. 9. 2006, sp. zn. 2 To 62/2006

Judikatura ESLP

ESLP 9248/81, Klass a další proti Německu
ESLP 12433/86, Lüdi proti Švýcarsku
ESLP 23224/94, Kopp proti Švýcarsku
ESLP 27798/95, Amman proti Švýcarsku
ESLP 44787/98, P. G. a J. H. proti Spojenému království
ESLP 50882/99, Petri Sallinen a další proti Finsku
ESLP 65755/01, Iliya Stefanov proti Bulharsku
ESLP 74336/01, Wieser a Bicos Beteiligungen GmbH proti Rakousku
ESLP 5935/02, Heglas proti ČR
ESLP 35623/05 Uzun proti Německu
ESLP 61496/08, Bărbulescu proti Rumunsku

Rozsudky Soudního dvora Evropské unie

Rozsudek Soudního dvora EU ze dne 8. 4. 2014, sp. zn. C-293/12; C-594/12
Rozsudek Soudního dvora EU ze dne 6. 10. 2015, sp. zn. C-362/14
Rozsudek Soudního dvora EU ze dne 21. 12. 2016, sp. zn. C-203/15; C-698/15
Rozsudek Soudního dvora EU ze dne 6. 10. 2020, sp. zn. C-511/18
Rozsudek Soudního dvora EU ze dne 6. 10. 2020, sp. zn. C-623/17
Rozsudek Soudního dvora EU ze dne 2. 3. 2021, sp. zn. C-746/18
Rozsudek Soudního dvora EU ze dne 16. 7. 2020, sp. zn. C-311/18

Ostatní judikatura

Rozhodnutí Nejvyššího soudu Spojených států ve věci *United States v. Wurie* z 25. 6. 2014, 728 F.3d 1

Rozhodnutí Nejvyššího soudu Spojených států ve věci *Riley v. California* z 25. 6. 2014, 573 U.S. 373

Rozhodnutí Nejvyššího soudu Spojených států ve věci *United States v. Microsoft Corp. (Microsoft Ireland)*. z 17. 4. 2018, No. 17-2

Rozsudek Nejvyššího soudu Československé socialistické republiky sp. zn. 7 Tz 11/68, ze dne 9. 4. 1968

5. Seznam ostatních zdrojů

BENEŠOVÁ, M. Stanovisko ke sjednocení výkladu zákonů a jiných právních předpisů k postupu v případech, kdy je třeba pro účely trestního řízení zjistit obsah údajů uložených v nalezeném, vydaném či odňatém mobilním telefonu, včetně údajů uložených na SIM kartě. Sbírká výkladových stanovisek nejvyššího státního zastupitelství, 2005, č. 4

Doporučení pro Rozhodnutí Rady o zmocnění k zahájení jednání za účelem dosažení dohody mezi Evropskou unií a Spojenými státy americkými o přeshraničním přístupu k elektronickým důkazům pro justiční spolupráci v trestních věcech In: EUR-Lex [online]. [25. 1. 2024]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=COM:2019:0070:FIN>

Důvodová zpráva k návrhu nařízení Evropského parlamentu a Rady o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech, COM (2018) 225 final; 2018/0108 (COD). Štrasburk, 17. 4. 2018. [online]. 2018 [cit. 24. 1. 2024]. Dostupný z: https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0017.02/DOC_1&format=PDF

Důvodová zpráva k zákonu č. 273/2012 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a některé další zákony

European Commission. *Adequacy decision for the EU-US Data Privacy Framework*. In: commission.europa.eu/ [online]. [cit. 25. 1. 2024] Dostupný z: https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf

FAIRFIELD, JAT., *Runaway technology; Can law keep up?* Cambridge University Press. 2021. ISBN 978-1-108-44457-6.

KOČÍ, M. *Elektronické důkazní prostředky*. Diplomová práce. Brno: Masarykova univerzita, 2012

Rámcové rozhodnutí Rady ze dne 13. června 2002 o společných vyšetřovacích týmech (2002/465/SVV)

Rozhodnutí Rady (EU) 2023/436 ze dne 14. února 2023, kterým se členské státy zmocňují, aby v zájmu Evropské unie ratifikovaly Druhý dodatkový protokol k Úmluvě o počítačové kriminalitě o posílené spolupráci a zpřístupňování elektronických důkazů, 32023D0436

Vláda: 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, č. 287/2018 Dz.

ZEMAN, P. Stanovisko ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek. Sbíрка výkladových stanovisek nejvyššího státního zastupitelství, 2015, č. 1

Dokazování elektronickými důkazními prostředky

Abstrakt

Předmětem této diplomové práce je analýza procesních nástrojů, které jsou orgánům činným v trestním řízení svěřeny na základě zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád), a jež jsou současnou praxí užívány v souvislosti s dokazováním elektronickými důkazními prostředky. Hlavním cílem této práce je zhodnocení, zda je současná právní úprava dostačující k účinnému zajištění elektronických důkazů a zároveň chrání ústavně garantovaná práva osob, aniž by docházelo k nepřiměřenému zásahu do těchto práv. Vhodně nastavená procesněprávní úprava je s ohledem na rozvoj informačních a komunikačních technologií žádoucí a činí tak řešenou problematiku velmi aktuální.

První kapitola se za užití převážně deskriptivní metody zabývá dokazováním v trestním řízení obecně, což je pro pochopení celé práce zásadní. Neopomíná současně odkazovat na elektronické důkazní prostředky, a to zejména na příkladech. Druhá kapitola je klíčovou částí celé práce, analyzuje právní úpravu elektronických důkazních prostředků z několika pohledů. Nejprve je pro přehlednost dělí na kategorie, dále se zabývá procesními postupy, jimiž může dojít k jejich zajištění, a to na základě toho, zda orgán činný v trestním řízení má ve své dispozici datový nosič či nikoliv. Konečně pak do hloubky analyzuje procesní instituty trestního řádu užívané k zajištění, popř. uchování elektronických důkazů. Zejména se kriticky zaměřuje na nastavení podmínek, za kterých je možné dané procesní nástroje užít. V rámci třetí kapitoly je poskytnut pohled na tuto problematiku na úrovni unijního a mezinárodního práva. Pozornost je věnována zejména nově přijaté úpravě v rámci Rady Evropy a Evropské unie. Současně je diskutován americký zákon CLOUD Act, nad jehož výkonnou mezinárodní dohodou vyjednávají Spojené státy společně s Evropskou unií. Čtvrtá část práce rozebírá zajišťování elektronických důkazů z emailových schránek, sociálních sítí, cloudových úložišť a mobilních telefonů, aplikuje tak obecné závěry z předchozích částí na konkrétní situace. Poslední kapitola obohacuje práci o poznatky z aplikační praxe prostřednictvím rozhovorů s příslušníky policejních orgánů. Práce vyzdvihuje aktuální výzvy pro trestní proces, které s sebou nové technologie přináší, a současně nabízí možné návrhy de lege ferenda.

Klíčová slova: elektronické důkazy, nové technologie a právo, dokazování v trestním řízení, přeshraniční přístup k elektronickým důkazům, digitalizace

Substantiation of Electronic Evidence

Abstract

The subject of this master thesis is the analysis of the procedural instruments that are entrusted to the law enforcement authorities on the basis of Act No. 141/1961 Coll., on Criminal Procedure (Criminal Procedure Code) and which are used in current practice in connection with substantiation of electronic evidence. The main aim of this master thesis is to evaluate whether the current legislation is sufficient to effectively secure electronic evidence and at the same time protects constitutionally guaranteed fundamental rights of persons without unreasonable interference with these rights. Appropriately set procedural regulation is desirable with regard to the development of information and communication technologies, and therefore this issue is very relevant.

The first chapter deals with evidence in criminal proceedings in general, using a mainly descriptive method, which is essential for understanding the whole master thesis. At the same time, it does not neglect to refer to electronic evidence, especially through examples. The second chapter is the key part of the whole master thesis, analysing the legal regulation of electronic evidence from several perspectives. First, it divides them into categories for clarity, and then discusses the procedural methods by which they can be seized, based on whether or not the law enforcement authority has a data carrier in its possession. Finally, it analyses in depth the procedural instruments of the Code of Criminal Procedure used to seize or preserve electronic evidence. In particular, it critically focuses on the setting of conditions under which the given procedural instruments can be used. In the third chapter, a perspective on this issue at the level of EU and international law is provided. Attention is paid in particular to the newly adopted regulation within the Council of Europe and the European Union. At the same time, the American CLOUD Act, whose implementing international agreement is being negotiated by the United States with the European Union, is discussed. The fourth part of the master thesis discusses the seizure of electronic evidence from email, social networks, cloud storage and mobile phones, applying the general conclusions of the previous parts to specific situations. The last chapter enriches the master thesis with insights from practice through interviews with police officers. The thesis highlights the current challenges for the criminal procedure brought by new technologies, while offering possible *de lege ferenda* proposals.

Keywords: electronic evidence, new technologies and law, substantiation in criminal proceedings, cross-border access to electronic evidence, digitalisation