MASARYKOVA UNIVERZITA
PRÁVNICKÁ FAKULTA
Ústav práva a technologií

ELEKTRONICKÉ DŮKAZY V TRESTNÍM ŘÍZENÍ

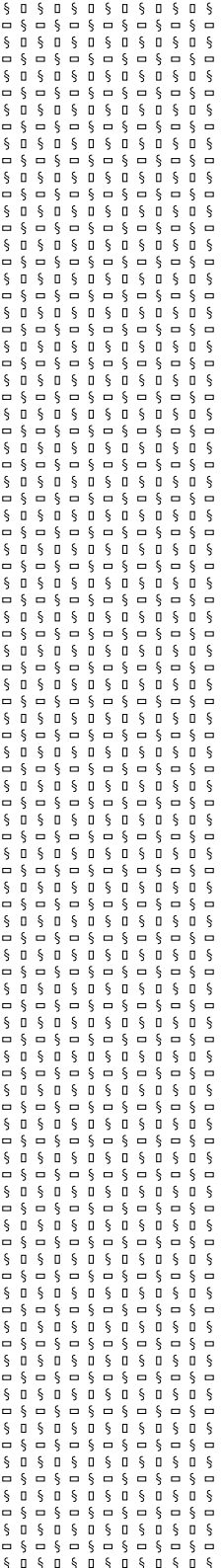
Radim Polčák, František Púry, Jakub Harašta a kolektiv

ACTA UNIVERSITATIS BRUNENSIS

IURIDICA
Editio Scientia vol. 542

SPISY PRÁVNICKÉ FAKULTY
MASARYKOVY UNIVERZITY

řada teoretická, Edice Scientia
svazek č. 542



ELEKTRONICKÉ DŮKAZY V TRESTNÍM ŘÍZENÍ

Radim Polčák, František Púry,
Jakub Harašta a kolektiv

Masarykova univerzita
Brno 2015

Vzor citace:
POLČÁK, Radim ; PÚRY, František ; HARAŠTA, Jakub a kolektiv. Elektronické důkazy v trestním řízení. 1. vyd. Brno : Masarykova univerzita, Právnická fakulta, 2015. 253 s. Spisy Právnické fakulty Masarykovy univerzity, řada teoretická, Edice Scientia č. 542. ISBN 978-80-210-8073-7.

Katalogizace v knize – Národní knihovna ČR

Polčák, Radim

Elektronické důkazy v trestním řízení / Radim Polčák, František Púry, Jakub Harašta a kolektiv. – 1. vydání. Brno: Masarykova univerzita, 2015. - 253 stran. Spisy Právnické fakulty Masarykovy univerzity, řada teoretická, Edice Scientia ; svazek č. 542. ISBN 978-80- 210-8073-7.

004* 343.13* 347.99:004.738* 351.817* 347.94*
- informační technologie
- trestní řízení
- elektronické soudnictví
- elektronická komunikace
- dokazování (právo)
- kolektivní monografie

004 – Počítačová věda. Výpočetní technika. Informační technologie [23]

Tato publikace vznikla na Masarykově univerzitě v rámci řešení projektu „Elektronické důkazy“, číslo projektu MUNI/A/1296/2014 podpořeného z prostředků účelové podpory na specifický vysokoškolský výzkum, kterou poskytlo MŠMT v roce 2015.

Právní stav byl zohledněn ke dni 31. 12. 2015.

Dostupnost elektronických zdrojů byla ověřována k 31. 12. 2015.

Recenzent: doc. JUDr. Ladislav Pokorný, Ph.D.

ISBN 978-80-210-8073-7

Obsah

Předmluva

Elektronické důkazy v procesním právu, a tím více v trestním řízení, v rámci něhož nezřídka dochází k významným zásahům do základních lidských práv a svobod, se staly v posledních desetiletích oblastí, které je třeba věnovat nepochybně zvýšenou pozornost. V době, kdy nezanedbatelná část lidských aktivit probíhá skrze elektronické prostředky, a rostoucí využívání informačních a komunikačních technologií vede k bezprecedentním možnostem ohledně sběru a zpracování dat týkajících se každého jednotlivého člověka, je nutné dbát na to, aby se změny společenské reality projevily rovněž v oblasti právní a právo tak mohlo nadále plnit svůj účel. Nelze přehlédnout, že v současné době je produkováno ohromné množství dat v elektronické podobě (v digitální formě či přesněji v binárním zobrazení), ze kterých je možno získat velké množství informací, z nichž lze usuzovat na relevantní skutkový stav při dokazování v trestním řízení. Přitom autoři důvodně připomínají, že pokaždé, pokud má právo nějaký důvod pracovat s informací, nepostihuje její ideální existenci, ale stanoví samo její vnější jevovou formu a jí pak přiřazuje příslušné právní následky (jde o zajímavý efekt, který je mnohem starší než informačně-vědní disciplíny a který je možno označit jako nutnou formalizaci informace.). Typickým příkladem mohou být instituty jako informace veřejného sektoru, obchodní tajemství, osobní údaj, utajovaná informace nebo třeba autorské dílo.

Pro právo, které ze své podstaty nejlépe reguluje jevy, které zná, je typické, že někdy nebývá schopné reagovat dostatečně pružně na změny společenské reality. Tento problém dopadá v neposlední řadě i na úpravu dokazování elektronickými důkazními prostředky v trestním řízení. Právní praxi však lze přičíst k dobru, že i zde si obvykle dokáže poradit. Ale jak konkrétně? A jak nevynalézat znovu kolo? Proto jsem velmi přivítal vydání této knihy, v níž autoři předkládají fundovaný, ale také čtivý výklad problematiky elektronických důkazních prostředků v trestním řízení, a tím i dostatečně konkrétní odpovědi na uvedené otázky.

Publikace je podle mého názoru na dnešním knižním trhu výjimečná v několika ohledech. V prvé řadě jde o knihu, která se věnuje „vodám“ zatím

nepříliš probádaným. Z tohoto důvodu bylo jistě šťastné, že vedení autorského kolektivu se ujal doc. JUDr. Radim Polčák, Ph.D., jeden z předních českých odborníků v oblasti dnes tolik aktuálního průniku práva a informačních technologií, jehož neutuchající zájem o danou problematiku spojený s originální a bohatou publikační praxí byly pro mne zárukou výběru kvalitního autorského kolektivu i výsledného textu. S potěšením mohu konstatovat, že mé naděje v žádném směru nezklamal.

K silným stránkám publikace patří především to, že se specificky zabývá oblastí, která je důležitá pro velmi široký okruh právníků a obsahuje pojednání od obecné teorie informace a důkazu přes teorii elektronického důkazu a dokazování v trestním procesu až po konkrétní praktické výstupy týkající se každodenní práce s nejčastěji užívanými elektronickými důkazními prostředky v trestním řízení. V souladu s tím, lze výklad v knize rozdělit na část obecnou (kapitoly I a II) a zvláštní (kapitoly III až IX), přičemž obecná část zahrnuje zejména teorii důkazu a informace, vymezení základních pojmů dokazování a analýzu procesu dokazování v trestním řízení. Kapitola I se zabývá mimo jiné i takovými důležitými otázkami, jako je kategorie pravdy, a s ní souvisejícími pojmy absolutní a relativní pravdy, materiální a formální pravdy, volného hodnocení důkazů, opomenutými důkazy, nástroji praktické jistoty či důkazní spolehlivostí atd. Jejich zpracování považuji za velmi přínosné a lze říci i do značné míry za novátorské pro nauku i praxi. V této souvislosti považuji za důležité připomenout tezi Karla Engliše z jeho díla Malá logika (*„Dokazujeme-li tedy, co je pravda, dokazujeme pravdivost svého soudu o skutečnosti. To musí býti předem jasno, že předmětem důkazu není nikdy skutečnost, nýbrž náš soud o skutečnosti, náš poznatek o skutečnosti, co o skutečnosti vypovídáme.“*), která je citována jen v poznámce pod čarou č. 50, se správným závěrem, že „důkaz neslouží ke zjištění materiální pravdy, ale k prokázání pravdivosti skutkového tvrzení (výroku)“, jenž je podle mého názoru velmi důležitý a zasloužil by si bližší rozvedení přímo v textu knihy. Ze všech těchto důvodů doporučuji každému čtenáři věnovat úvodním kapitolám zvýšenou pozornost, neboť osvětlují základní přístupy k dokazování v trestním řízení a tím i k používání elektronických důkazních prostředků, jejichž výklad je obsažen v následujících kapitolách.

Zvláštní část knihy nastíněné oblasti dále rozvádí pro případy jednotlivých druhů elektronických důkazních prostředků a uvedené propojuje s praktickou stránkou věci. Po originálně pojaté a inspirativní obecné části, ve které se autoři neváhali pustit ani do některých kontroverznějších témat a oblastí, čímž nutí čtenáře k dalšímu zamyšlení nad směřováním našeho trestního procesu, publikace předkládá na základě aktuálních poznatků tuzemské právní vědy a praxe kompaktní a čtivý výklad všeho podstatného, co je v současné době v dané oblasti známo. Přitom zohledňuje relevantní judikaturu zdejších soudů a zapracovává rovněž zajímavá rozhodnutí zahraniční. V tomto směru lze upozornit zejména na uváděnou judikaturu Evropského soudu pro lidská práva, neboť nejčastější problém užívání elektronických důkazních prostředků představuje ochrana soukromí.

Výklad je členěn tak, aby čtenáře bezpečně provedl nejprve podstatou každého z jednotlivých druhů elektronických důkazních prostředků, a to postupně od obecného vymezení dat až po data z dohledových systémů kybernetické bezpečnosti, a to včetně jejich základní technické povahy, a dále s ohledem na posloupnost práce i teoretickými a praktickými problémy vztahujícími se k těmto jednotlivým důkazním prostředkům. Přehledná je i struktura jednotlivých podkapitol, kde autoři v zásadě postupují chronologicky od zajištění důkazu přes jeho analýzu, provedení a následné zohlednění soudem ve skutkovém stavu.

Autoři se mimo tradičních elektronických důkazních prostředků, jako je odposlech, provozní a lokalizační údaje či e-mail, zaměřili rovněž na nový fenomén – data z dohledových pracovišť kybernetické bezpečnosti (zpráva o údajích zajištěných v rámci řešení incidentu). To bylo umožněno i tím, že Česká republika je v oblasti kybernetické bezpečnosti v Evropě do značné míry lídrem a udává směr v rámci členských států Evropské unie.

Kniha klade zvláštní důraz na aktuálnost a komplexnost předkládaných informací, což se projevuje v zohlednění aktuální právní úpravy i judikatury, a to jak české, tak i zajímavých příkladů relevantní zahraniční rozhodovací praxe. Autoři tak knihu pojali jako nanejvýš aktuálního a praktického průvodce vším podstatným, co může každého právníka i zvídavého laika v oblasti elektronických důkazních prostředků zajímat, přičemž autoři kladli zvláštní důraz na problematiku práce s elektronickými důkazními prostředky, aby byl

čtenář seznámen se všemi obvyklými úskalími a mohl se s nimi rozumným způsobem vypořádat. Publikace proto v návaznosti na poznatky právní vědy a praxe rozvíjí vlastní originální pohled a upozorňuje na zajímavé problémy v praxi, čímž kniha získává skutečně praktický přesah. Výsledkem je teorií podpořený zajímavý a prakticky orientovaný text, který čtenáře snadno uvede do nesmírně dynamické problematiky.

Konečně chci ocenit zejména to, že předkládané dílo může být užitečné pro široké spektrum právnické veřejnosti při hledání a nacházení cesty k tomu, aby právo i v době bouřlivého rozvoje informačních technologií mohlo stále plnit svůj účel. Výklad umožňuje čtenáři proniknout do soudobého stavu užívání elektronických důkazních prostředků v trestním řízení a současně i poznáním slabých míst vytváří základ pro další zlepšování aplikace práva v této oblasti, neboť tím, že upozorňuje na problémy v současné právní úpravě i praxi, umožňuje nasměrovat cestu k dalšímu žádoucímu vývoji právní úpravy trestního řízení v novém již připravovaném trestním řádu. Předkládaná problematika může být v neposlední řadě velmi zajímavá též pro zainteresovanou laickou veřejnost při rozšiřování povědomí o tom, že právo platí mimo jiné i na počítačových sítích a v cloudech.

Z těchto důvodů věřím, že tato kniha bude nejen vítaným průvodcem pro široký okruh právnické i zvídavé laické veřejnosti, které přináší jak zevrubný úvod, tak i fundovaný výklad nesmírně zajímavé a stále více se rozvíjející problematiky, ale bude rovněž impulzem k dalšímu diskurzu v oblasti práce s elektronickými důkazními prostředky.

Závěrem již jen přeji příjemné a obohacující čtení!

prof. JUDr. Pavel Šámal, Ph.D.

Autoři

Kapitola I — doc. JUDr. Radim Polčák, Ph.D.
vedoucí, Ústav práva a technologií Právnické fakulty MU

Kapitola II — JUDr. František Púry, Ph.D.
soudce a předseda trestního kolegia, Nejvyšší soud

Kapitola III — Mgr. Václav Stupka
asistent, Ústav práva a technologií Právnické fakulty MU a České centrum excelence pro kybernetickou kriminalitu

Kapitola IV — Mgr. Petr Klement
státní zástupce, Nejvyšší státní zastupitelství

Kapitola V — Mgr. Tomáš Abelovský
externí student doktorského studia, Ústav práva a technologií PrF MU, a právník v mezinárodní společnosti

Kapitola VI — JUDr. Matěj Myška, Ph.D.
odborný asistent, Ústav práva a technologií Právnické fakulty MU
a JUDr. Jakub Harašta
asistent, Ústav práva a technologií Právnické fakulty MU

Kapitola VII — Mgr. Václav Stupka
asistent, Ústav práva a technologií Právnické fakulty MU a České centrum excelence pro kybernetickou kriminalitu

Kapitola VIII — Alena Pejčochová, M.A.
doktorandka, Policejní akademie ČR
a Mgr. Tomáš Elbert
advokát

Kapitola IX — JUDr. Jakub Harašta
asistent, Ústav práva a technologií Právnické fakulty MU

I DŮKAZ A INFORMACE

I.1 Informace v právu

Právo lze vnímat jako systém pravidel, jako soubor oprávnění nebo třeba, jak se píše na jednom českém právnickém blogu, jako „intelektuální výzvu, kontext, zábavu, umění, poslání, život". Od poloviny minulého století lze právo nahlížet též jako informační systém, tj. jako soubor informací, jejichž primárním účelem je organizovat společnost[1]. Právní pravidla lze tímto pohledem vnímat jako obecné informace o povinnostech, jejichž objektivně vyjádřenou formou je v kontinentální Evropě především zákon. Individualizované právní normy, tj. adresné imperativy tvořící typicky obsah individuálních právních aktů, lze považovat za informace adresované a bezprostředně závazné. Veškeré procesy v právu, ať už jde o tvorbu právních předpisů, rozhodování sporů nebo o výuku na právnických fakultách, je pak možno vnímat jako procesy tvorby, zpracování nebo komunikace informací a pracovat s nimi za užití metod kybernetiky, resp. obecné informační teorie[2].

Právo však prakticky nikdy nepracuje s informací jako takovou, tj. s informací v jejím ideálním stavu. Tam, kde se právní pravidla pokoušejí přímo postihnout informaci, to obvykle ve výsledku nedopadá dobře[3]. Důvod této skutečnosti je možno hledat v samotné podstatě informace, kterou důkladně popsaly obě shora zmíněné disciplíny v druhé polovině dvacátého století.

1 Obor, který se tomuto pohledu na právo věnuje, označujeme jako právní informatiku, jurimetriku nebo informační teorii práva – jeho dosavadní vývoj mapuje sborník Paliwala, A. (ed.) *History of Legal Informatics*. Zaragoza: Prensas de Universitarias de Zaragoza, 2010.

2 V Československu se takový pohled na právo a právní vědu poprvé objevuje v díle Viktora Knappa. První komplexní česky psaná publikace věnovaná problematice užití metod teoretické kybernetiky v právu přitom obdivuhodně vyšla relativně záhy po vzniku samotné kybernetiky – viz Knapp, V. *O možnosti použití kybernetických metod v právu.* Praha: Nakladatelství Československé akademie věd, 1963. S informačním pojetím důkazu a procesu dokazování se pak můžeme setkat u profesora brněnských práv Josefa Macura – srov. např. Macur, J. *Kompenzace informačního deficitu procesní strany v civilním soudním sporu*. Brno: Masarykova univerzita, 2000 nebo Macur, J. *Důkazní břemeno v civilním soudním řízení*. Brno: Masarykova univerzita, 1995 nebo Macur, J. *Zásada projednací v civilním soudním řízení*. Brno: Masarykova univerzita, 1997.

3 Příkladem takových přešlapů jsou regulatorní pokusy například v oborech duševního vlastnictví nebo ochrany osobních údajů, které s odstupem času hodnotíme přinejlepším jako nepříliš úspěšné – podrobněji viz Polčák, R. Getting European data protection off the ground. *International Data Privacy Law*, 2014, roč. 4, č. 4., str. 282 a násl.

Pro kybernetiku, hledající podstatu fungování života a snažící se ji napodobit, je informace praktickým protikladem entropie[4]. Míra informovanosti určitého systému tedy přímo odpovídá míře jeho vnitřní organizovanosti – tam, kde naopak informace chybí, je výsledkem chaos.

Z právě uvedeného plyne, že za informaci v pravém smyslu toho slova můžeme považovat pouze skutečnost, jejímž projevem je zvýšení organizace určitého systému. Výskyt informace se jiným způsobem než snížením entropie neprojevuje. Současně platí, že entropii nelze v sociálním systému snížit jinak než prostřednictvím informace a že pro člověka je prakticky nemožné poznat výskyt informace jinak než prostřednictvím jejího efektu. Z toho pak lze dovodit, že člověk není vybaven schopností empiricky určit existenci informace jinak než porovnáním míry entropie příslušného systému přinejmenším ve dvou různých okamžicích[5].

Výraz „informace" samozřejmě používáme v řadě populárních významů a za informaci označujeme i data, jejichž výskyt v určitém systému nikdy snížení entropie nepřinese, resp. jejichž přítomnost příslušný systém dokonce chaotizuje. Výrazy jako „informační systém" nebo „informační centrum" pak vlastně neoznačují skutečnost, ale vyjadřují spíše účel, k němuž směřují nejrůznější projevy nejpřirozenějšího z lidských snažení (tj. snahy o popření entropie).

Právo si samozřejmě nemůže dovolit luxus užití výrazu „informace" v jeho ideálním významu, a tak za informaci označuje i data, o jejichž organizačním efektu ani nemáme důvod uvažovat. Přirozeně se přitom v právu objevil zajímavý efekt, který je mnohem starší než informačně-vědní disciplíny a který bychom mohli označit jako nutnou formalizaci informace. Pokaždé, pokud má právo nějaký důvod pracovat s informací, nepostihuje totiž její

4 Zakladatel kybernetiky Norbert Wiener staví své zkoumání fenoménu života na třech základních paradigmatech – 1) informace je protikladem entropie, 2) živé organismy jsou implicitně vybaveny větším než kritickým množstvím informace a 3) organismy, resp. jejich společenství, reagují na změnu podmínek produkcí informace – viz Wiener, N. *Cybernetics: On the Control and Communication in the Animal and the Machine*. Cambridge: MIT Press, 1961, str. 11.

5 Dimenzi času implicitně akcentuje vedle samotné kybernetiky též matematická informační teorie, za jejíhož zakladatele je považován Claude Shannon. Tento obor se věnuje především otázce komunikace, resp. formy, jíž lze prostřednictvím datového transferu docílit efektivního přenosu významu mezi různými systémy. K podstatě informační teorie viz úvodní dvě kapitoly textu, který je považován za základní kámen informační teorie – Shannon, C. E. A Mathematical Theory of Communication. *The Bell Systems Technical Journal*, 1948, roč. 27, č. 3, str. 379 a násl.

ideální existenci, ale stanoví samo její vnější jevovou formu a jí pak přiřazuje příslušné právní následky. Typickým příkladem mohou být instituty jako informace veřejného sektoru, obchodní tajemství, osobní údaj nebo třeba autorské dílo.

Jedním z přirozených důvodů této formalizace informace je, vedle pragmatického významu pro jednoduchost při používání právního pojmového aparátu, zřejmě i skutečnost, že s informací v její ideální formě nelze ze shora popsaného důvodu pracovat jako se statickou kategorií. Právo však nutně potřebuje stabilizovat své objekty, resp. sekundární objekty, v čase, aby bylo možno je z hlediska právních povinností kvalifikovat, manipulovat s nimi nebo je třeba vzájemně porovnávat. Formalizaci informace do podoby informačních institutů tedy můžeme vnímat i jako nutný předpoklad toho, aby k nim šlo stanovovat právní povinnosti.

Druhým důvodem toho, že právo nepracuje s informací, ale s různými způsoby její formalizace (typicky s daty), je skutečnost, že informace, resp. její míra, je podmíněna její dostupností cílovému systému. Informační efekt tedy nezáleží jen na kvalitě dat, ale též na způsobu, kterým jsou komunikována – vedle prosté jejich dostupnosti to přitom může být otázka původce, použitého komunikačního média, momentálního stavu různých typických znaků cílového systému ovlivňujících jeho recepční schopnosti apod.

I.2 Informace o člověku a informační technologie

Euroatlantická právní kultura, jejíž základ leží v křesťanské tradici, je filozoficky orientována na člověka[6]. Pozdější sekulární argumentaci všeobecné centrality člověka přinesl evropské právní kultuře Kant a evidentně ji tím odlišil od ostatních právně-kulturních prostředí zbytku světa[7]. Informace vypovídající o životě člověka tedy musí mít v našich právně-kulturních podmínkách v porovnání s informací o jiných skutečnostech zvláštní normativní, resp. restriktivní režim[8].

6 Srov. Glenn, P. *Legal Traditions of the World*. New York: Oxford University Press, 2004, s. 143 a násl.

7 Viz např. Wood, A. *Kantian Ethics*. Cambridge: Cambridge University Press, 2008, s. 85.

8 V roce 1954, tj. dávno před příchodem osobních komunikačních zařízení, se tímto problémem zabývá Richard Donelly v sepsané přednášce Donelly, C. R. The Law of Evidence: Privacy and Disclosure. *Louisiana Law Review*, 1954, roč. 14, č. 2, s. 361 a násl.

Důraz na ochranu informace o člověku tedy nemůžeme připisovat překotnému technologickému vývoji posledních let nebo nějaké momentální módě. Důvodem toho, že její ochraně dáváme v poslední době větší důraz, je především dostupnost technologií umožňujících její získávání a zpracovávání[9].

Nejde přitom jen o informační a komunikační technologie, jejichž penetrace soukromým životem člověka dosahuje dříve netušených rozměrů. Tlak na ochranu lidského soukromí způsobují též technologie umožňující extrahovat informaci o člověku i z dat, která dříve nebylo možno vůbec získat nebo zpracovat. Díky technologiím schopným zaznamenat pachové stopy nebo analyzovat nepatrné vzorky DNA lze informaci o člověku extrahovat i ze zdrojů, jejichž využití k tomuto účelu by dříve nebylo myslitelné. O životě člověka tak dnes může mnohomluvně vypovídat i čalounění nábytku, sklenice od piva nebo třeba záložka z knihy.

Informační a komunikační technologie jsou specifické tím, že jejich primárním účelem je zpracování a komunikace dat. Skutečnost, že původcem a uživatelem těchto nástrojů je člověk, pak logicky vede k tomu, že data, jež jsou jejich prostřednictvím získávána, shromažďována, zpracovávána a komunikována, se člověka buďto přímo týkají, nebo mu mají být k nějakému užitku.

Pokud jde o zdroje informací o člověku, poslouží běžně používané informační a komunikační technologie zdaleka nejen prostřednictvím dat, které o sobě člověk vědomě dává k dispozici. Daleko za hranice běžné lidské představivosti totiž jdou možnosti využití dat, která jsou prostřednictvím těchto technologií zpracovávána zcela nebo zčásti bez vědomí člověka, o jehož životě vypovídají. Nemusí se přitom nutně jednat přímo o data typu provozních a lokalizačních údajů nebo o různé údaje, které víceméně bez vědomí uživatele zpracovávají a ukládají nebo někam odesílají vysoce přesné senzory různých komunikačních zařízení – vypovídací hodnotu mohou totiž mít i na první pohled banální informace, jakými jsou metadata obrazových či textových souborů, servisní záznamy uložené v paměti osobních automobilů nebo třeba papíry z laserových tiskáren a kopírek (ať už je na nich vytištěno cokoli)[10].

9 Daniel Solove v této souvislosti používá výrazu „radikální transparentnost" – viz Solove, D. *The Digital Person.* New York: New York University Press, 2004, s. 73.

10 Podrobně se novým formám datových stop člověka věnuje Richard Hunter v knize Hunter, R. *World Without Secrets.* New York: John Wiley and Sons, 2002.

Skrytý charakter a ohromná vypovídací hodnota různých zásobáren dat, která mohou být použita k doposud netušenému rozkrytí nejmenších detailů lidského života, logicky působí tlak na adaptaci mechanismů ochrany informačního soukromí člověka a na tvorbu kvalitativně zcela nových ochranných mechanismů. Nezastupitelná je zatím v tomto směru role státu, a to přinejmenším do doby, než bude člověk schopen uvědomit si rozsah a závažnost změn, které přináší bezprecedentní penetrace lidského života uměle vytvořenými informačními nástroji[11].

Nelze očekávat, že běžný uživatel do detailu pochopí fungování vysoce komplexních technologií a k tomu bude ještě schopen odhalit nejrůznější způsoby, jimiž tyto technologie mohou zasáhnout do jeho práva na soukromý život. Dokonce lze z dosavadních zkušeností konstatovat, že po normálním člověku nemůžeme rozumně chtít ani to, aby tam, kde jej provozovatel příslušné technologie o možném zásahu do soukromí informuje, takovou informaci skutečně prostudoval a zařídil se podle ní. Schizofrenní je pak v této situaci role státu, který má na jedné straně chránit člověka před negativními důsledky přirozeného, avšak poněkud překotného technického vývoje, majícího za následek bezprecedentní expozici soukromí a na straně druhé má implicitní povinnost využít nově dostupných dat k tomu, aby plnil své základní funkce (tj. chránil člověka a společnost před chaosem).

V tomto směru, tj. v otázce proporcionality mezi různými aspekty ochrany práv člověka ve vztahu k informačnímu soukromí, můžeme pozorovat značné rozdíly mezi pojetím evropským a severoamerickým. Přestože v obou právních systémech konstatujeme shora uvedenou centralitu člověka, významně se liší v tom, do jaké míry dávají státu možnost nových technologií aktivně či pasivně využívat. Zatímco v USA je běžné, aby měl stát prostřednictvím různých svých agentur v rámci své jurisdikce prakticky neomezený přístup ke všem novým druhům informačních zásobáren, není v Evropě výjimkou, musí-li se orgány veřejné moci potýkat dokonce s překážkami závažnějšími, než je tomu v soukromém sektoru[12].

11 Podrobněji viz Polčák, R. *Internet a proměny práva.* Praha: Auditorium, 2012, s. 330 a násl.

12 Srov. např. Schwartz, P. M. The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures. *Harvard Law Review*, 2013, roč. 126, č. 7, s. 1966 a násl.

Problém existence zařízení a služeb shromažďujících dříve nevídané množství dat o soukromém životě člověka projevuje se nyní v praktickém právu především zvýšenou institucionální pozorností vůči ochraně soukromí a osobních údajů. Některé typy dat jsou na základě praktické potřeby a dosavadních zkušeností s jejich využitím v procesech autoritativní aplikace práva podrobeny zvláštnímu právnímu režimu zpracování a dalšího užití – vznikají tak specifické důkazní instituty, jejichž příkladem může být odposlech nebo zpracování provozních a lokalizačních údajů[13]. V některých jurisdikcích došlo na základě potřeby systematicky řešit proporcionalitu dotčených práv i k vytvoření obecných zákonných institutů, jakými jsou např. procedury k zajištění dat v přípravném řízení nebo instituty využitelné k extrakci dat ze zvlášť chráněných zdrojů (typicky např. z šifrovaných úložišť).

Lze předpokládat, že zvýšená expozice soukromí v souvislosti s trendem privacy-by-design[14] může v dohledné době vedle zákonného ošetření procedur zpracování a využití těchto dat vést též k typické zákonné úpravě dostupnosti a používání konkrétních technologií. Očekávat tak lze především zákonné nebo judikatorní technické standardy či dokonce limity pro nasazení a využití určitých typů technických zařízení nebo služeb informační společnosti. S trochou nadsázky lze tedy konstatovat, že se vývoj právních limitů v oblasti datových nástrojů ubírá podobným směrem jako například v oboru zbraní a střeliva nebo dopravních prostředků, kde předmětem právní regulace nejsou jen důsledky aplikace příslušné technologie, ale právo zde reguluje už jejich samotnou dostupnost a nasazení[15].

I.3 Informace, pravda a čas

Jednou z informačních kategorií, která je v právu formalizována tradičně a s mnohasetletou zkušeností, je kategorie pravdy. Ta sama o sobě představuje specifický parametr označující dle tradiční doktríny soulad výroku

13 Fenoménu data retention, tj. uchovávání provozních a lokalizačních údajů se podrobně věnuje Matěj Myška v knize Myška, M. *Právní aspekty uchovávání provozních a lokalizačních údajů*. Brno: Masarykova univerzita, 2013.

14 Tento pojem označuje obligatorní řešení ochrany osobních údajů na úrovni technických parametrů příslušného systému, který tyto údaje zpracovává – Rubinstein, I. Regulating Privacy by Design. *Berkeley Technology Law Journal*, 2012, roč. 26, č. 3, s. 1409 a násl.

15 Srov. např. analýzy a doporučení, které byly výsledkem celoevropského projektu SMART zaměřeného na inteligentní sledovací systémy – publ. online na adrese smartsurveillance.eu.

s objektivní skutečností a informace jako takové se vlastně ani netýká. Nabízela by se sice možnost, že v případě výroků jejich pravdivost přímo implikuje jejich organizační potenciál, tj. že pravdivý výrok můžeme automaticky a vždy označit za informaci. Ve skutečnosti však mohou pravdivé výroky působit (i v dlouhodobém horizontu) též chaoticky – to v návaznosti na řadu shora zmíněných faktorů týkajících se kvality cílového systému. Dobře načasovaná lež komunikovaná správně zvolenému cílovému systému může mít daleko lepší partikulární i obecný organizační efekt než pravdivé sdělení komunikované ve špatný čas špatnému okruhu adresátů. Pravda je tedy ve vztahu k informaci relativně nezávislou kategorií[16].

Ani pravda ale nepředstavuje konečnou právní kvalifikaci výroku, protože je prakticky nemožné ji kompletně uchopit. Nejde jen o to, že člověk není vybaven schopností objektivně pravdu poznat, ale dokonce lze formulovat a argumentovat odlišné názory i na to, co vlastně pravda ideálně znamená (resp. co má znamenat). Ivan Wernish tento problém ilustruje ve své Cestě do Aščhabadu následovně: „Yün-men řekl mnichům: ‚Opravdová pravda vypadá jako bidlo nad záchodem. Opravdová lež vypadá jako bidlo nad záchodem. Ano, pravda je stejně nedůležitá jako lež. Více záleží na tom, co je mezi nimi. Nevěříte? Tak mi sem někdo přineste záchodové bidlo.' A když mu ten klacek podali, pravil: ‚Řekněme, že jeden z konců, dejme tomu tento, je opravdová pravda, v tom případě ovšem druhý, opačný konec je opravdová lež. A nyní pohleďte, co je mezi konci. Vidíte? Mezi konci je to, oč nutno se opřít, pakliže nechceme spadnout do hoven.'"

V procesním právu je otázka pravdy či pravdivosti vždy pojmově oddělitelná od kategorie platnosti. Zatímco platnost je otázkou objektivní (absolutní) existence právního pravidla a uplatní se při hodnocení existence či kvality potenciálního normativního tlaku, týká se pravdivost naplnění jeho

16 K tomu podrobněji viz Polčák, 2012, op. cit., s. 26 a násl.

subsumpčních podmínek, tj. otázky aktuální existence právního imperativu za daných skutkových okolností[17]. Lévyho slovníkem je tedy pravda důvodem k aktualizaci virtuálního právního pravidla[18].

Jedinou výjimkou, kdy byly v procesním právu obě kategorie spojeny v jeden kompaktní celek, byl superkognitivistický[19] institut ordálu. V tomto případě byla otázka skutkového a právního posouzení příslušného případu spojena vjedno a zjišťování skutkového stavu se tedy mohlo časově i procesně prolnout s verdiktem[20], rozhodnutím o konkrétních právních následcích, a dokonce i s faktickým výkonem právního imperativu. Zaráz byl tedy člověk, to ovšem jen díky presumované účasti Boží vůle, žalován, souzen, odsouzen i potrestán. Jediným důvodem, proč tento vysoce efektivní mechanismus nelze použít v dnešním procesu, je nedostatek presumpce zájmu vyšší moci na každém jednotlivém procesu – zjednodušeně řečeno se nám totiž nepodařilo osvědčit, že je v našich procesech autoritativní aplikace práva Boží vůle k dispozici vždy, když se nám zamane.

Ordál lze použít předně k demonstraci toho, že je v našich dnešních poměrech nutno oddělovat od sebe otázku obecné a konkrétní platnosti právního pravidla, resp. že skutek je nutno v procesu autoritativní aplikace práva oddělovat od práva. Ukazuje ale též i na problém časové adresy skutkové informace, kterou v procesu autoritativní aplikace práva používáme, a na otázku její rozdílnosti od časování zájmového děje. Je-li tedy v procesu užito skutkových informací, je k nim nutno přistupovat vždy s předsudkem jejich zastaralosti.

Harvardský profesor důkazního práva Charles Nesson se s problémem časového odstupu mezi skutkem a procesem autoritativní aplikace práva

17 Problém dichotomie platnosti a pravdivosti výmluvně líčí Ota Weinberger v druhé kapitole své kritiky von Wrighta – viz Weinberger, O. *Alternative Action Theory*. Dordrecht: Springer Science+Business Media, 1998, s. 37 a násl.

18 Právní pravidlo totiž kvůli své obecnosti existuje potenciálně a de facto bez ohledu na čas – až nástup konkrétní právní skutečnosti vede k tomu, že právní pravidlo generuje v určitém čase konkrétní a reálně existující imperativ. K pojmu virtuality a virtualizace viz publikaci Lévy, P. *Becoming Virtual – Reality in the Digital Age*. New York: Plenum Trade, 2002.

19 K pojmové specifikaci kognitivismu viz Holländer, P. *Filosofie práva*. Plzeň: Aleš Čeněk, 2006, s. 94.

20 Tento výraz pochází z latinského vere dicere, tj. říkat pravdu. Jedná se tedy o formalizaci skutkového stavu, resp. v trestním právu procesním o autoritativní konstatování viny.

vyrovnal po svém – prostě si vytvořil imaginární postavu cestovatele časem, kterého nazval Eon. Nessonovy přednášky a konferenční vystoupení byly vždy prodchnuty různou mírou esoteriky, takže posluchačům obvykle trvalo, než přišli na to, že Eon není jen nějakým nahodilým důsledkem konopné terapie (jejímž propagátorem Nesson rovněž je), ale že jde o dokonalý důkazní prostředek. Mít možnost vrátit se v čase a zúčastnit se děje, který nás v procesu autoritativní aplikace práva zajímá, je totiž ideální možností dozvědět se, co a jak se vlastně přihodilo.

Mohlo by se zdát, že roli Nessonova Eon může v našich podmínkách sehrát dokonalý archiv. Pořizování záznamů o všem možném, co se ve světě děje, a jejich následná archivace, totiž umožňují obrátit se v případě potřeby k těmto datům a znovu vyvolat již vyskytnuvší se skutečnost. Ani to by však nebyl dokonalý důkaz, neboť by šlo „pouze" o dokonalý obecný obraz skutečnosti, který by však bylo dále v procesu autoritativní aplikace práva nutno interpretovat. Vyřešil by se tím tedy sice problém samotné dostupnosti základních empirických vodítek ke zkoumání skutkového stavu, stále by ale částečně přetrval problém časového odstupu, neboť pravda, jak nás zajímá v procesu autoritativní aplikace práva, je sice objektivní, to však spíše v kantovském smyslu, tj. jako soubor maximálně pravdivých odpovědí na otázky, které se nám na základě našich dosavadních znalostí aktuálně zdají k věci případné[21].

Tento problém můžeme vidět na příkladu procesů, v nichž jsou před soudy otevírány historické křivdy. I v případě, kdy je věc velmi dobře dokumentována a není tedy problém dostat se k dobovým datům, nemusí vycházet najevo kýžená pravda (tj. původní pravda, na jejímž základě má být

21 Tento postup popisuje Kant v druhé (kanonické) kapitole čtvrté části své Kritiky čistého rozumu – viz Kant, I. *Critique of Pure Reason*. Přel. Meiklejohn, J. M. D. Project Gutenberg, 2003.

s odstupem času rozhodnuto). Stavění, Čermákovými slovy[22], řádu minulosti před soud řádu přítomnosti tedy není jen otázkou odlišného názoru právního či morálního, ale i faktického hodnocení situací, které mohou být dokumentovány s libovolnou precizností, přesto však nikdy ani sebelepší jejich důkaz nemůže dokonale vylíčit minulou skutečnost.

Nessonův Eon namísto toho provádí interpretaci skutečnosti v momentě, kdy se zájmový děj odehrává, a zpět do budoucnosti už nese přímo odpověď na otázky, které se nám, Kantovými slovy, zdají být pro naši věc případné. Tím pádem můžeme mít k dispozici procesně téměř ideální skutkový stav bez ohledu na to, kdy se skutečnost, která nás v řízení zajímá, původně odehrála.

Nessonův Eon tím pádem vlastně spíš vypadá jako bezprostřední projev Boží vůle, tj. jako ordál. Co nám Eon z minulosti přináší, však není pravda (resp. Pravda), ale pouze její poznání či interpretace. Nelze tím pádem na informacích Eon založit prostou sylogistickou aplikaci (zde vlastně spíše implikaci) práva, neboť dokonalý důkaz v tomto případě neznamená objektivní poznání, jehož pravdivostní hodnota by byla stoprocentní, ale „pouze" poznání založené na maximálním přímém kontaktu s kompletní realitou včetně její časové adresy.

22 Psal-li by rozhodnutí v ostře sledovaném případě ústavní revize tzv. Benešových dekretů člověk, který neměl bezprostřední zkušenost s hrůzami druhé světové války, možná by bylo logicky vnitřně konzistentnější či aktuálně politicky korektnější – jen těžko by ale disponovalo takovou mírou přesvědčivosti. Dokonce i přes pádnost Čermákových formulací si dnes jen těžko dokážeme představit situaci, kterou odůvodnění cit. rozhodnutí líčí následovně: *„V odpovědi na další navrhovatelovo tvrzení, že totiž dekret prezidenta republiky č. 108/1945 Sb., stejně jako další dekrety vydané dr. Edvardem Benešem, odporovaly právním zásadám civilizovaných společností Evropy, a že proto je třeba je považovati za akty nikoli práva, ale násilí, jinými slovy, že postrádají povahu práva vůbec, třeba, a to i ve všeobecném smyslu, zdůraznit základní moment vztahující se k jakémukoliv hodnocení minulosti; to, co přichází z minulosti, musí sice i tváří v tvář přítomnosti v principu hodnotově obstát, toto hodnocení minulého nemůže však být soudem přítomnosti nad minulostí. Jinými slovy, řád minulosti nemůže být postaven před soud řádu přítomnosti, jenž je již poučen dalšími zkušenostmi, z těchto zkušeností čerpá a na mnohé jevy pohlíží a hodnotí je s časovým odstupem. Z tohoto zorného úhlu a v kontextu všech souvislostí a událostí v době nacistické okupace a v období na ni úzce navazujícím třeba hodnotit i sám dekret prezidenta republiky ze dne 25. 10. 1945 č. 108/1945 Sb., jehož vydání nebylo ničím jiným než opatřením, v této historické situaci a na bázi tehdy platného právního řádu, reagujícím na předchozí likvidaci státní svrchovanosti, samostatnosti, celistvosti a demokraticko-republikánské státní formy Československé republiky, likvidaci principů demokratického, právního státu, zahrnutých v Ústavní listině Československé republiky z roku 1920, a to nacistickým režimem, jenž se svou ideologií světovlády panské rasy a na tuto ideologii navazujícím terorem pustošícím miliony lidských životů, představuje jeden z nejničivějších totalitních systémů v dějinách lidstva."* Viz nález Ústavního soudu sp. zn. Pl. ÚS 14/94, N 14/3 SbNU 73 (55/1995 Sb.).

Z právě uvedeného plyne, že i pokud by přirozená lidská touha uniknout času[23] vedla k tvorbě nějakého mechanismu podobného Eon, ve výsledku by to stejně nevedlo k dokonalému naplnění požadavku na reflexi materiální pravdy v procesu autoritativní aplikace práva. Dokonalý důkaz by tedy neznamenal dokonalou pravdivost skutkového stavu. I proto, hovoříme-li v právu o pravdě, vždy jde o licenční ústupek, a možná je tím pádem lépe používat jiných výrazů jako například Weinbergerovy praktické jistoty[24] ve smyslu jistoty soudce ohledně toho, že data, která ke skutkové otázce získal, jsou dostatečná k tomu, aby si udělal prakticky použitelný vlastní obrázek o skutkovém stavu[25].

I.4 Absolutní a relativní pravda

Shrneme-li shora uvedené poznatky, nevyznívá výsledek pro otázku naplňování principu zjišťování materiální pravdy příliš dobře. Nemůžeme se totiž spoléhat v soudních řízeních na dokonalou identitu platnosti a pravdivosti, která by jako jediná bezezbytku vedla k materiální pravdě. Ani v případě dokonalého důkazu nemůžeme dosáhnout úplné pravdivosti. Co je snad ještě horší, dokonalý důkaz, vyjma Nessonovy bujné představivosti, neexistuje.

Hovořit za této situace o naplňování principu materiální pravdy jeví se tím pádem podobně, jako když v Císařově pekaři popisují členové alchymistické laboratoře, jak postupují ve snaze o výrobu zlata. Těžko totiž ukázat nějaké použitelné příklady toho, že to skutečně jde – na druhé straně si ale nelze

23 Tuto touhu označuje za vysoce problematickou Hobbes ve svém Leviathanu. Snahu zastavit čas nebo se vrátit v čase zpátky přitom považuje za typický příklad lidských slabostí, před nimiž má člověka chránit Suverén (ten totiž takovou slabostí z Boží vůle netrpí) – viz Hobbes, T. *Leviathan, Or, the Matter, Forme, & Power of a Common-Wealth, Ecclesiastical and Civill*. Project Gutenberg, 2009.

24 Tento teoretický pojem, který se objevil v textu Weinberger, O. Logické a metodologické základy důkazu v oboru práva. *Stát a právo,* 1967, č. 13, převzal a jeho důležitost pro polistopadovou českou trestněprávní praxi zdůraznil Pavel Šámal v práci Šámal, P. *Základní zásady trestního řízení v demokratickém systému.* Praha: SEVT, 1992, s. 185 a násl. Užití tohoto pojmu v ústavní praxi rozebírá Pavol Holländer na str. 200 v knize Holländer, 2006, op. cit. Pojem praktické jistoty se objevuje i v rozhodovací praxi našich vrcholných instancí - srov. např. nález sp. zn. I. ÚS 733/01, N 26/32 SbNU 239, nález sp. zn. I. ÚS 2726/14, usnesení Nejvyššího soudu sp. zn. 8 Tdo 1189/2014 nebo sp. zn. 3 Tdo 567/2013.

25 Procesním důsledkem dosažení praktické jistoty na straně soudu je mimo jiné též možnost uzavřít dokazování a nepřipouštět již další navržené důkazy – k tomu srov. např. nález Ústavního soudu sp. zn. IV. ÚS 570/03, N 91/33 SbNU 377.

otevřeně přiznat, že to nejde, protože pak by zřejmě odpadl důvod si k této snaze kohokoli vydržovat. Praktická či možná spíš přesněji pragmatická jistota pak je v tomto směru přesně tím vedlejším produktem, který ve svých křivulích vytváří alchymista nezapomenutelně ztvárněný Lubomírem Lipským. Není to sice zlato (pravda) v pravém smyslu toho slova, ale je to vysoce užitečný, technicky nepříliš náročný a v konečném důsledku i mnohem lépe použitelný produkt.

Vedle právě zmíněné praktické jistoty, jejíž vztah k pravdě jsme právě připodobnili ke vztahu zlata a slivovice, je klíčem k řešení tohoto problému i filozofická kategorie formální pravdy. Zatímco praktická jistota je otázkou interpretace nedokonalých důkazů a nahrazení jejich informačních deficitů úvahou soudce[26], představuje formální pravda formalizovaný výsledek procesu zjišťování skutkového stavu, tj. způsob, kterým soud o skutkovém stavu informuje v odůvodnění svého rozhodnutí. Soudce tedy bere důkazy, kriticky je hodnotí a dospívá k praktické jistotě ohledně skutku – tato ideální informační kategorie (tj. praktická jistota) pak je vypovězena do výsledného formálního vyjádření (formální pravdy). To, co minulou materiální pravdu (skutek) na konci procesu autoritativní aplikace práva objektivně poznatelným způsobem reflektuje, je tedy pravdou formální[27].

Zatímco je právě zmíněná distinkce mezi formální a materiální pravdou typická pro právní filozofii resp. právní teorii, užívá se pojmů materiální a formální pravdy v procesních odvětvích českého práva v poněkud jiném významu. Filozofické pojetí dichotomie materiální a formální pravdy

26 Přestože jde o vybočení z racionalistické tradice, na níž je naše důkazní právo v současnosti postaveno, je nutno zde přiznat, že tato úvaha nemusí být vždy jen racionální. Především americká teorie důkazního práva tak například otevřeně hovoří o divadelním charakteru dokazování, přičemž soud se může při hodnocení kontradiktorních důkazů dostat de facto do role uměleckého recenzenta – srov. Ariens, M. S. The Law of Evidence and the Idea of Progress. *Loyola of Los Angeles Law Review*, 1992, roč. 25, č. 3, s. 869.

27 V různých právních kulturách se můžeme setkat s různou mírou formalizace procesu tvorby formální pravdy. Zatímco v kontinentální právní kultuře je především díky dominantní úloze soudce otázka dokazování upravena volně (k tomu viz dále v otázce volného hodnocení důkazů), je angloamerický systém typický poměrně detailní a rigorózní úpravou důkazních pravidel (rules of evidence). Pozoruhodně aktuální diskusi výhod a nevýhod angloamerické zákonné teorie důkazní nabízí esejistický text harvardského profesora Ezry Ripley Thayera, který před sto lety vyšel v Michigan Law Review – viz Thayer, E. R. Observations on the Law of Evidence. *Michigan Law Review*. 1915, roč. 13, č. 5, s. 355 a násl.

je totiž založeno na předpokladu, že obě tyto kategorie mají statický charakter. Materiální pravda je tedy skutečným, dokonale nezjistitelným, stavem, zatímco formální pravda představuje jeho formalizovanou, nejčastěji sepsanou, objektivně vnímatelnou reprezentaci[28]. V tomto smyslu je tedy například skutková část odůvodnění rozsudku vždy formální pravdou – jde totiž o objektivně vnímatelnou formalizaci materiální pravdy, kterou na základě dosažení praktické jistoty autoritativně provedl soud.

Procesní disciplíny naproti tomu chápou oba pojmy dynamicky a s praktickým důrazem nikoli na jejich prostou existenci ale na způsob, kterým k nim v procesu autoritativní aplikace práva přistupujeme[29]. V případě materiální pravdy tedy jde o skutečný stav, který s větším či menším úspěchem zjišťujeme prostřednictvím poznávání objektivní skutečnosti. Formální pravda je naproti tomu kategorií, k níž dospíváme prostřednictvím formalizovaných informačních zdrojů bez toho, aby nás objektivní skutečnost měla nutně zajímat (typicky např. v některých případech na základě shodného prohlášení stran).

Je-li tedy proces autoritativní aplikace práva veden principem zjištění materiální pravdy, je předmětem veškeré snahy soudu nebo jiného orgánu veřejné moci objasnění objektivní skutečnosti (či shora uvedeným příměrem výroba zlata). Nejde ani tak o to, že kýžený výsledek je ideální a prakticky nedosažitelný, ale že máme v řízení povinnost vyvinout maximální snahu o přiblížení se k němu. U řízení vedených principem zjištění formální pravdy se orgán autoritativní aplikace práva nemusí pouštět do rozkrývání skutečnosti, ale může si při formulaci skutkových závěrů vystačit s formalizovanými skutečnostmi, které s materiální pravdou nemusí vůbec souviset.

Z hlediska metody lze od sebe formální a materiální pravdu v procesualistickém významu nejlépe odlišit prostřednictvím Oakshottovy gnoseologické dichotomie mezi praktickým a teoretickým poznáním[30]. K přiblížení

28 Srov. např. Holländer, P. *Filosofie práva*. Plzeň: Aleš Čeněk, 2006, s. 194.

29 Šámal rekapituluje historický vývoj obou pojmů a v této souvislosti argumentuje praktickou užitečností termínu materiální pravdy výlučně k procedurálnímu odlišení od pravdy formální. Všímá si přitom i nepříliš smysluplného rozlišování mezi materiální a objektivní pravdou v komunistické trestní doktríně a s odkazem k Weinbergerovi se kloní k názoru, že pravda jako taková žádné přívlastky nepotřebuje – viz Šámal, P. *Základy trestního řízení v demokratickém systému*, 2. vyd. Praha: Codex Bohemia, 1999, s. 291.

30 Viz Oakshott, M. *On Human Conduct*. Oxford: Oxford University Press, 1975, s. 13.

se materiální pravdě potřebujeme dle Oakshotta nutně užít metod teoretického poznání – ani dokonalé informační nástroje (Nessonův Eon) ve spojení s logikou Sherlocka Holmese a intuicí slečny Marplové však nám její úplné poznání nikdy nepřinesou. Naproti tomu formální pravda je dokonale poznatelná, a to pouze za užití praktických (empirických) metod. Příkladem tohoto rozdílu může být třeba rodný list – žádný test, svědecká výpověď ani intuitivní schopnost nacházet stále nové empirické metody určení otcovství nám nikdy nepřinesou v této otázce dokonalou (Boží) jistotu. Naproti tomu formální pravda vyjádřená textem rodného listu je dokonale poznatelná, neboť otec je v něm přesně identifikován.

Pragmatické řešení pojmového problému formální a materiální pravdy nabízí Šámal prostřednictvím pojmů pravdy absolutní a relativní[31]. Absolutní pravdou je v tomto případě skutečný stav, relativní pravdou pak je prostě to, co je uvedeno ve skutkové části odůvodnění rozsudku. Šámal v tomto případě vychází z procesualistické distinkce mezi formální a materiální pravdou, přičemž formální a materiální pravdu chápe jako možnosti resp. metody, jimiž lze absolutní pravdu transformovat do pravdy relativní a zároveň měřit úspěšnost této transformace. Zatímco v případě materiální pravdy se snažíme o pokud možno co nejvyšší míru korespondence mezi absolutní a relativní pravdou, je formální pravda charakteristická tím, že nás poměr mezi objektivní skutečností a její relativní reprezentací nemusí zajímat.

Šámal užívá pojmu relativní pravdy a její kontrapozice k absolutní pravdě především ke zdůraznění shora diskutované skutečnosti, že totiž lidské poznání skutečného stavu nemůže být nikdy dokonalé. Praktickou jistotu soudce lze tedy vždy relativizovat s poukazem na nedokonalost lidských kognitivních schopností.

Pojem relativity jeví se však v této souvislosti vhodně zvoleným i z jiného důvodu – rozhodnutí soudu je totiž vybaveno atributem relativní závaznosti, tj. závaznosti v relaci určených subjektů (typicky státu a stran). Závazným je v relaci ke stranám samozřejmě pouze normativní obsah příslušného rozhodnutí. Ten však je vždy důsledkem subsumpce, jejíž premisou je nutně skutkový stav. I ta část, v níž soud referuje o obsahu své praktické jistoty,

31 Viz Šámal, 1999, op. cit., s. 287.

je tedy integrální součástí subsumpční struktury celého rozhodnutí[32]. Strany jsou v důsledku rozhodnutí sice vázány pouze uloženými normativními povinnostmi,[33] skutková část odůvodnění však je kvůli své logické vazbě k výroku nadána vůči nim přinejmenším atributem relativní známosti. Tento aspekt relativity lze mimo jiné doložit i prostřednictvím fungování institutu nepřezkoumatelnosti – rozsudek, který ke stranám autoritativně nekomunikuje relativní pravdu, je totiž z podstaty nepřezkoumatelný.

Z právě uvedeného plyne ještě jeden aspekt relativity toho, co je uvedeno ve skutkové části odůvodnění rozsudku. Skutková informace (relativní pravda) má z hlediska platného práva smysl pouze v relaci k výroku. Relativní pravda se tedy musí k výroku vztahovat a jen tehdy má soud právo a povinnost o ní v rozsudku referovat. Zatímco se tedy můžeme setkat s tím, že soudy k odůvodněním svých rozsudků připojují obecné právní úvahy ve formě obiter dicta, zřejmě nenacházíme důvod k tomu, aby soud ve skutkové části odůvodnění referoval o skutečnostech, které s rozhodnutým případem nijak nesouvisejí.

Pojmová a metodologická distinkce mezi absolutní a relativní pravdou může nám posloužit též k argumentaci stylu, jímž v kontinentální Evropě píšeme skutkové části odůvodnění individuálních právních aktů. Zatímco v angloamerickém prostředí se můžeme setkat i s kontemplativním vyjádřením skutkové informace, v Evropě je spíše pravidlem, že soud či jiný orgán veřejné moci kategoricky konstatuje pravdu. Je přitom jasné, že člověk, který rozhodnutí psal, nikdy neměl (nemohl mít) stoprocentní jistotu ohledně skutečného stavu – kategorické vyjádření však v tomto smyslu jen

32 Tato skutečnost se v řadě případů projevuje především u kasačních soudů složitostí v oddělení otázek právních a skutkových. Přestože tedy u kasačních soudů ze zásady neprobíhá dokazování, musí se tyto instance často zabývat otázkami, u nichž hranici mezi právní a skutkovou úvahou nelze jednoznačně určit.

33 Strany nezavazuje relativní pravda obsažená v rozhodnutí – to se mimo jiné projevuje tím, že jsou naše věznice plné lidí tvrdících, že nikdy nic špatného neprovedli (přestože je pachatel nucen přijmout trest, nemá povinnost ztotožnit se s relativní pravdou ohledně své viny resp. nemá povinnost tuto pravdu nezpochybňovat).

vhodně podtrhuje fakt, že to, na základě čeho orgán veřejné moci rozhoduje, je „jen" jeho vlastní pragmatické pochopení skutečnosti (tj. že si zde shora uvedeným příměrem nikdo nehraje na výrobu zlata ze švestek).[34]

Skutečnou alchymii procesu autoritativní aplikace práva každopádně nepředstavuje způsob, kterým dotčené fenomény označujeme nebo jímž ke kýženému produktu (relativní pravdě) dospíváme, ale spíše míra pragmatičnosti, s níž racionálně (a případně též intuitivně) hodnotíme kvalitu výsledku a poměřujeme ji náročností použitých nástrojů[35]. Na jedné straně jsme totiž nuceni akceptovat nedosažitelnost absolutní pravdy, na straně druhé však může být snadné podlehnout pokušení a spokojit se s jednoduchým (efektivním) řešením procesní formalizace skutku. Shora uvedeným příměrem je tedy sice jasné, že se nám v procesu autoritativní aplikace práva nikdy nepodaří vyrobit zlato – existuje však reálné riziko, že namísto kvalitní slivovice začneme být spokojeni i s méně kvalitními produkty a nakonec skončíme u jednoduše dosažitelné a ekonomicky výhodné Okeny. V praktických podmínkách našeho soudnictví se tedy máme z hlediska kvality aproximace materiální pravdy důvod obávat především takových hledisek, jako jsou

34 Tomu odpovídá i samotná nátura důkazního práva – jeho hlavním předmětem je totiž otázka, co a jak může ve výsledku vytvořit skutkovou informaci, resp. naopak otázka, co a jak se na tvorbě skutkové informace podílet nemůže. Otázka inkluze, resp. exkluze skutkových dat přitom nemá s materiální pravdou nic společného, neboť má čistě právní (normativní) povahu. Touto úvahou se již na počátku minulého století zabývá jeden z průkopníků medicínského práva Sir Joseph Walton v textu Walton, J. Notes on the Law of Evidence. *Medico-Legal Journal*, 1904, roč. 2, č. 1, s. 675.

35 Zjednodušeně lze hovořit o tom, co nám v souvislostech daných typem procesu, typem prokazované skutečnosti a dalšími okolnostmi stačí k tomu, abychom konstatovali praktickou jistotu. Ústavní soud tuto jinak než pragmaticky neřešitelnou situaci osvětluje v nálezu sp. zn. I. ÚS 173/13 následovně: *„Obdobně trestní nauka vychází z premisy, že absolutní pravdu v řízení zjistit prakticky nelze a určitá nejistota bude vždy přítomna (…). Proto je v oblasti trestního práva konkretizováno, že se nezjišťuje skutečný stav věci, ale skutkový stav musí být zjištěn tak, aby o něm nebyly „důvodné pochybnosti" (…) Přitom je nutno vzít v potaz, že takto formulovaný důkazní standard se aplikuje dokonce i při existenci ústavní zásady in dubio pro reo (…) Je tedy nutno reflektovat, že žádné skutkové okolnosti, které již odezněly, nelze následně, ex post, prokázat s absolutní jistotou. Vždy půjde o otázku určité míry pravděpodobnosti (…). Absolutní jistota je tedy důkazní standard, který není možno v soudním řízení aplikovat, neboť by při tom důkazní břemeno prakticky nebylo možno unést."*

výkonnostní normy pro soudce, principy procesní ekonomie nebo náklady na použití kvalitních forenzních nástrojů či postupů minimálně invazivních vůči dotčeným subjektům[36].

I.5 Volné hodnocení důkazů

Z právě uvedeného může vyplývat poněkud pesimistický závěr v tom směru, že zjišťování skutkového stavu je v praxi jen nutnou parodií na ideály dokonalého procesu autoritativní aplikace práva a že jediné, co celý tento procesní cirkus drží pohromadě, je blažené nevědomí těch, kterých se fakticky týká (tj. účastníků řízení). Tento dojem může v našem (českém) právním prostředí umocňovat mimo jiné i jev, který by šlo označit za perverzní kreativitu při práci se skutkovým stavem[37].

Nabízí se samozřejmě v této souvislosti řečnická otázka nejen v tom smyslu, jak je možné, že naše Advokátní komora trpí ve svém stavu živly zakládající si svůj obchodní model na fingování skutkových informací, ale především, jak je možné, že tento typ kreativity přecházejí bez zvláštního povšimnutí i samotné soudy, nota bene za situace, kdy dělání si bláznů ze soudu evidentně naplňuje skutkovou podstatu kárného provinění i pořádkového deliktu.

Podobně se lze ptát, odkud se z vnitřní formální struktury aplikačního procesu, postaveného na principu zjištění materiální pravdy, vytratila sama aproximativní kategorie pravdivosti, resp. kde se například bere u nás z generace na generaci předávaná pověra o tom, že v trestním řízení je obviněný či obžalovaný podobně, jako má právo nevypovídat vůbec, oprávněn i bez jakéhokoli negativního následku libovolně lhát.

---

36 Míře pragmatizace, resp. ekonomické efektivizace procesu zjišťování skutkového stavu se podrobně věnuje Ron Shapira v článku Shapira, R. Econonic Analysis of the Law of Evidence: A Caveat, Cardozo Law Review, číslo 19, str. 1607 a násl. Hospodárnost, která se později stává předmětem učení law and economics, byla i jedním z ústředních témat Englišova odborného zájmu – pozoruhodně se mu věnuje dokonce i v kompendiu právní logiky. Viz Engliš, K. *Malá logika.* Praha: Melantrich, 1947, s. 419 a násl.

37 Česká praxe nabízí v tomto směru nepřeberné množství dramat od klasicky umělecky ztvárněných radiogramů s fotbalovými kapříky přes scénky o namol opilých spolujezdcích nevysvětlitelně se objevujících na sedadle řidiče až po postmoderní variace na téma „sedmička v krabici."

Oba partikulární problémy, které lze s trochou nadsázky označit za dělání si trhacího kalendáře z principu zjištění materiální pravdy, mají samozřejmě vcelku jednoduchá řešení spočívající v operačním režimu standardních procesních institutů. Vedle obligátních pořádkových či disciplinárních nástrojů jde především o široké meze volného hodnocení důkazů. Jediným limitem skutečně omezujícím kontinentálního soudce v jeho skutkové úvaze je totiž kromě empirie už pouze logika.

Právě uvedené může se projevit příkladně na způsobu, jímž soud skládá jednotlivé faktografické informace do komplexního obrazu minulé skutečnosti relevantní pro příslušný proces autoritativní aplikace práva (tj. do skutkového stavu). U nás až příliš často praktikovanou možností je izolované konsekutivní hodnocení skutkových tvrzení a příslušných důkazů, přičemž neprokázaná tvrzení nebo lži prostě jen nejsou ve výsledném skutkovém stavu zahrnuty, a dokonce ani často nejsou vzájemně odlišeny. Soud tedy postupně přijímá (nebo se táže na) jednotlivá tvrzení a pokud se na základě provedeného dokazování ukáží být neprokázanými nebo lživými, postupuje v obou případech bez předsudků k dalším tvrzením a důkazům.

Druhou možností, která se jeví ve vztahu ke shora zmíněné perverzní skutkové kreativitě (prolhanosti) jako adekvátnější, je souvislé hodnocení dílčích skutkových informací s postupnou tvorbou předporozumění na straně soudu. Soud má v tomto směru plné právo hodnotit lež procesní strany nikoli jen ve vztahu k příslušné skutkové informaci (resp. k příslušnému skutkovému tvrzení), ale může využít této zkušenosti též k pravdivostnímu hodnocení dalších tvrzení.

Nejde přitom o nějaké a priori hodnocení důkazu před jeho provedením, neboť důkaz je pouze součástí komplexní procedury zjištění skutkového stavu. Jestliže tedy strana v řízení lže, má soudce plné právo přistupovat k ověřování dalších tvrzení v témže řízení s pravděpodobnostním předpokladem, že mohou být rovněž lživá (úmyslně nepravdivá). Tento předpoklad pak může soudce v situacích, kdy nelze spolehlivě ověřit korespondenci takových tvrzení s materiální pravdou, transformovat do právní jistoty, aniž by se jednalo o překročení mezí volného hodnocení důkazů nebo porušení principu in dubio pro reo.

Ze shora uvedeného plyne, že nelze chápat jako vybočení ze zákonných mezí volného hodnocení důkazů, pokud soud konstatuje pravdivostní hodnotu konkrétního objektivně neprokazatelného aspektu skutkového stavu na základě procesní zkušenosti získané v průběhu řízení ohledně pravdomluvnosti stran. Přesvědčivosti takto formulované skutkové části odůvodnění rozsudku by určitě též pomohlo, pokud by naše soudy začaly explicitně rozlišovat mezi neprokázaným tvrzením, tj. výrokem, u nějž se nepodařilo prokázat korespondenci s materiální pravdou, a lží. Skutková část odůvodnění postaveného na komplexní práci s kategorií pravdivosti (namísto shora zmíněného konsekutivního hodnocení) by totiž určitě vypadala mnohem výmluvněji, pokud by soud například uvedl, že „obžalovaný lhal, když při výslechu tvrdil, že vozidlo řídila osoba blízká, která po zastavení z vozu utekla, zatímco on si před příchodem policejní hlídky přesedl na místo řidiče a zapnul bezpečnostní pásy, přičemž měl v té době v krvi 2,1 promile alkoholu“, namísto toho, aby soud pouze suše konstatoval, že „nebylo prokázáno tvrzení obžalovaného, že…“.

K teorii volného hodnocení důkazů ještě zbývá dodat drobnou komparatistickou poznámku o jejím opaku, tj. zákonné důkazní teorii, postaru též označované jako zákonná teorie průvodní. S rigorózní zákonnou úpravou dokazování se lze setkat především v zemích angloamerické právní kultury, přičemž nejvýraznější kontury má zřejmě v severoamerickém právu. Pravidla dokazování, angl. rules of evidence, zde fungují jako podrobný normativní standard, upravující způsob získání a zpracování důkazních prostředků, mandatorní postupy pro aplikaci skutkové argumentace a částečně i hodnocení důkazní spolehlivosti[38]. Zatímco se tedy kontinentální teorie zákonného průvodu projevuje jako opak volného hodnocení důkazů, jsou rules of evidence blíže opaku zásady, dle níž lze jako důkaz použít cokoli, co není zákonem zapovězeno[39].

38 Zde je třeba připomenout, že samotná váha důkazu není předmětem rules of evidence – různé procesní souvislosti však zprostředkovaně vedou k tomu, že porota nebo soudce mají v porovnání s evropským soudem v otázce důkazní spolehlivosti nepoměrně menší míru diskrece – srov. Anderson, T., Schum, D., Twinning, W. *Analysis of Evidence.* Cambridge: Cambridge University Press, 2005, s. 227.

39 Podrobněji viz Šámal, 1999, op.cit., s. 293.

Na první pohled se může jevit jako paradoxní situace, kdy kontinentální soudce je v porovnání se svým severoamerickým kolegou co do otázky dokazování mnohem méně svázán pozitivními procesními pravidly. Ve skutečnosti však relativně vyšší míra složitosti angloamerického procesu a možnost rozhodujícího zapojení laického prvku (poroty) do hodnocení skutkového stavu vytvářejí logický tlak na vyšší míru formalizace procesních pravidel, včetně otázek dokazování.

Jen těžko lze pak vzhledem k zásadním rozdílům v základních parametrech procesů autoritativní aplikace práva porovnávat výhody a nevýhody evropského a angloamerického přístupu. Ve velmi obecné rovině lze snad za výhodu volného hodnocení důkazů a principu, že za důkaz může sloužit cokoli, označit především vyšší míru autonomie a též lepší flexibilitu (ta může být důležitá např. při použití nových forenzních technik nebo nových typů důkazních prostředků). Výhodou zákonné teorie důkazní či rules of evidence je naopak vyšší míra a priori jistoty stran ohledně důkazní situace a menší prostor k výše zmíněné perverzní skutkově-argumentační tvořivosti[40].

V obou uvedených právních kulturách lze samozřejmě ze základních důkazních principů nalézt výjimky. I v Evropě tak jsme například zvyklí používat důkazy mající typickou zákonnou úpravu (typické důkazy) a stejně tak lze, byť velmi výjimečně, provést i důkaz mimo rozsah standardních rules of evidence. Hlavní rozdíl mezi volným hodnocením důkazů a zákonnou teorií důkazní pak v tomto směru spočívá v tom, že zatímco angloamerický systém dává atypickým důkazům a priori nižší míru důkazní spolehlivosti, evropský proces mezi důkazní spolehlivostí typických a atypických důkazů nerozlišuje.

Z konkrétních rozdílů mezi oběma právními kulturami je možno poukázat především na odlišné vnímání institutu nepřípustnosti důkazu. Zejména v postkomunistické Evropě je nepřípustnost prakticky ztotožněna s nezákonností získání důkazního prostředku a v důsledku vede až k formalistickému lpění na legendě o otráveném stromě, resp. na předpokladu, že důkazní ovoce ze stromu stiženého libovolnou (klidně i jen kosmetickou) vadou

40 Zajímavé a doposud unikátní srovnání důkazního práva a konkrétních zákonných důkazních institutů amerického a kontinentálního systému provedl v polovině minulého století na vzorku práva rakouského a práva státu New York Arthur Lenhoff – viz Lenhoff, A. The Law of Evidence – A Comparative Study Based Essentially on Austrian and New York Law. *The American Journal of Comparative Law*, 1954, roč. 3, č. 3, s. 313.

je pro proces autoritativní aplikace práva smrtelně jedovaté[41]. V zemích angloamerické právní kultury jde naopak o rozsáhlou doktrínu kombinující ve složité struktuře prvky formální a obsahové[42].

I.6 Opomenutý důkaz

Shora jsme označili komplexní práci s kategorií pravdivosti za konformní s volným hodnocením důkazů, přičemž meze tohoto principu jsme mlhavě načrtli prostřednictvím empirické a logické metody. Díky dosavadní praxi našich nejvyšších soudů a Ústavního soudu můžeme konkrétně pojmenovat, a dokonce i kategorizovat typické případy, které kvůli vybočení z limitů volného hodnocení důkazů považujeme za porušení práva na spravedlivý proces. Společně je označujeme jako situace opomenutého důkazu a dělíme je následovně:

- Důkaz nebyl proveden, přestože mohl mít význam v hodnocení skutkového stavu[43]
- Důkaz nebyl proveden, přestože nutnost jeho provedení vyplývá ze zákona nebo z řízení[44]
- Důkaz byl proveden, ale nebyl zohledněn ve skutkovém stavu[45]
- Důkaz byl proveden, ale byl do skutkového stavu zohledněn nelogickým způsobem[46]

41 Srov. např. Fryšták, M. *Dokazování v přípravném řízení*. Brno: Masarykova univerzita, 2014, s. 191. Tento jednoduchý formalistický přístup je logicky motivován neblahou zkušeností s praktickou aplikací Višinského teorie procesu autoritativní aplikace práva komunistickými prokurátory (viz Višinskij, J. A. *Theorie soudních důkazů v sovětském právu*. Praha: Mír, 1950). Za situace standardního fungování institucí demokratického právního státu však formalistická legenda o otráveném stromě v procesním právu nemá místo. To ostatně dokládá i aktuální rozhodovací praxe Evropského soudu pro lidská práva – srov. např. rozhodnutí ESLP ve věci Gäfgen v. Německo, stížnost č. 22978/05 – nebo Ústavního soudu – srov. např. nález sp. zn. Pl. ÚS 47/13.

42 Srov. např. Krongold, H. L. A Comparative Perspective on the Exclusion of Relevant Evidence: Common Law and Civil Law Jurisdictions. *Dalhousie Journal of Legal Studies*, 2003, roč. 12, s. 97 a násl.

43 V dispozičním procesu k podmínce materiálního vlivu důkazu na skutkový stav přistupuje ještě podmínka jeho navržení, zatímco v inkvizičním procesu jde o objektivní dostupnost důkazního prostředku – srov. např. nálezy Ústavního soudu sp. zn. IV. ÚS 335/05, N 116/41 SbNU 453 nebo I. ÚS 4793/12.

44 Viz např. usnesení Nejvyššího soudu sp. zn. 8 Tdo 1189/2014.

45 Viz např. nález Ústavního soudu sp. zn. IV. ÚS 767/05, N 81/41 SbNU 67.

46 Viz např. nález Ústavního soudu sp. zn. I. ÚS 733/01, N 26/32 SbNU 239.

V prvním případě jde o situace, kdy strana navrhne důkaz, který je způsobilý zvýšit kvalitu skutkového stavu (tj. procesního obrazu materiální pravdy) a soud takový důkaz neprovede. Není v tomto směru vzhledem k principu zjištění materiální pravdy primárně podstatné, zda soud neprovedení navrženého důkazu odůvodní – problém absence odůvodnění neprovedeného důkazu totiž má charakter technický a týká se spíše přesvědčivosti výsledného rozhodnutí resp. práva stran přezkoumatelně se dozvědět, proč bylo rozhodnuto určitým způsobem. Mnohem důležitější je zde úvaha v tom směru, zda mohl neprovedený důkaz objektivně přispět k praktické jistotě. Není pak vybočením z mezí volného hodnocení důkazů, pokud není proveden důkaz, který sice per se vypovídací hodnotu má nebo mít může, ale v dané procesní situaci již bylo praktické jistoty dosaženo (tj. soud již má o skutkovém stavu dostatečně jasno).

Druhý případ se předně týká situací, kdy má soud vzhledem k inkvizičnímu charakteru řízení[47] povinnost aktivně zjistit skutkový stav. Za opomenutý důkaz můžeme v této souvislosti označit stav, kdy soud konstatuje praktickou jistotu, aniž by jí skutečně dosáhl. Druhou možností je zde specifická situace v dispozičním procesu, kdy objektivní nemožnost dosažení praktické jistoty pouze na základě důkazů, s nimiž v řízení disponují strany, zaváže soud k inkvizičnímu postupu a tato povinnost důkaz si aktivně opatřit není ze strany soudu následně naplněna.

Zatímco předchozí dvě alternativy opomenutého důkazu se týkají opomenutí ohledně jeho provedení, ve třetím případě jde o absenci adekvátního informačního projevu provedeného důkazu ve výsledném skutkovém stavu. Od tohoto typu opomenutého důkazu je přitom nutno odlišit situace, kdy soud důkaz provede, ale rozhodne se s ním ve skutkovém stavu nepracovat z důvodu jeho informačního deficitu[48] – tím může být slabá důkazní

47 Josef Macur si v této souvislosti všímá skutečnosti, inkviziční charakter dokazování netýká se čím dál častěji pouze implicitně vyšetřovacích procesů, ale setkáváme se s ním též kvůli technologicky determinovanému utajení skutkových dat i třeba v řízeních o věcech obchodních nebo finančních. S pozoruhodnou intuicí pak Macur konstatuje, že potřeba vyšetřovacího důkazu často roste s technologickou a finančních vyspělostí stran – srov. Macur, 2000, op. cit., s. 25.

48 Pojmu informačního deficitu je zde užito ve vztahu k důkazu resp. k důsledku užití důkazního prostředku. Jiným typem informačního deficitu, tj. deficitem vzniklým v důsledku menší míry informovanosti jedné ze stran, se zabývá Macur (2000, op. cit., s. 110 a násl.).

spolehlivost (nevěrohodnost) nebo třeba nezákonnost získání důkazního prostředku. Je-li informační absence provedeného důkazu ve skutkovém stavu takto odůvodněna, nemůže samozřejmě jít o opomenutý důkaz, resp. o překročení mezí volného hodnocení důkazů ze strany soudu.

Poslední shora uvedenou možnost představují případy, kdy je navržený nebo iniciativně opatřený důkaz sice proveden, jeho informační projev ve skutkovém stavu však odporuje koherenční teorii pravdivosti (tj. důkaz je faktograficky zpracován, ale nelogicky zapojen do celkového procesního obrazu materiální pravdy).

I.7 Nástroje praktické jistoty

V procesech autoritativní aplikace práva si ze shora uvedených důvodů nemůžeme dovolit požadavek na objektivní pravdu. Namísto toho se snažíme zjistit materiální pravdu do míry, o níž můžeme na základě konkrétních okolností prohlásit, že nám ohledně minulého děje vytváří praktickou jistotu[49]. Základní argumentační nástroje praktické jistoty jsou skutkové argumenty pravdivosti, z nichž nejčastěji užíváme:

- Argument korespondencí
- Argument koherencí

Argument korespondencí odpovídá tradiční korespondenční teorii pravdivosti a je postaven na předpokladu, že pravdivým je tvrzení (výrok) korespondující s materiální pravdou. Praktickou jistotu ohledně pravdivosti na základě uplatnění tohoto argumentu získáváme na základě skutkové informace (důkazu), který skutkové tvrzení přímo spojí s prokazovanou skutečností[50].

---

49 Takové prohlášení obvykle není jen otázkou prostého poznání skutečnosti, ale též kvality skutkového argumentu. Pavol Holländer k tomu píše: *„Dokazování má tudíž vícero stránek. Má svoji stránku noetickou a stránku argumentační (a s ní úzce spjaté stránky eristickou a rétorickou)"* – viz Holländer, 2006, op. cit., s. 195.

50 Hodí se zde připomenout, že důkaz neslouží ke zjištění materiální pravdy, ale k prokázání pravdivosti skutkového tvrzení (výroku). To zdůrazňuje i Karel Engliš, když píše: *„Dokazujeme-li tedy, co je pravda, dokazujeme pravdivost svého soudu o skutečnosti. To musí býti předem jasno, že předmětem důkazu není nikdy skutečnost, nýbrž náš soud o skutečnosti, náš poznatek o skutečnosti, co o skutečnosti vypovídáme"* – viz Engliš, 1947, op. cit., s. 277.

Korespondenční argument lze použít v případě, máme-li k dispozici to, co důkazní teorie označuje za přímý důkaz. Jeho obsahová kvalita, resp. materiální použitelnost pro praktickou jistotu je dána především jeho spolehlivostí (procesní věrohodností) a dále pak přímým vztahem ke skutečnosti, kterou prokazuje. Formální kvalita důkazu pak je stejně jako u jiných typů důkazu dána jeho zákonností.

Korespondenční argument používáme zásadně k přímé verifikaci skutkového tvrzení – je-li důkaz spolehlivý, skutkové tvrzení je jím potvrzeno (verifikováno). Výjimkou z této zásady jsou případy, kdy je sice vzhledem ke kvalitě skutkového tvrzení důvod uplatnit korespondenční argument, avšak objektivně neexistuje možnost jeho verifikace.

Typickým příkladem situace, kdy je skutkové tvrzení způsobilé k aplikaci korespondenčního argumentu, ale nelze je verifikovat, jsou skutková tvrzení ohledně skutečností, které nenastaly, ale jejich eventuální opak může generovat přímý důkaz (např. tvrzení ohledně skutečnosti, že nebyl splněn peněžitý závazek). V takovém případě je na místě ověřit korespondenci prostřednictvím falzifikace, tj. nemožnosti prokázání opaku. U nesplněného závazku tedy lze vyjít z důkazu výslechem stran a přitom předpokládat, že pokud byl ve skutečnosti závazek splněn, bude k tomu zřejmě existovat přímý důkaz (např. může být prokázáno předání peněz v hotovosti, zaplacení bankovním převodem apod.) Praktická jistota ohledně korespondence takového tvrzení pak již není otázkou důkazní spolehlivosti verifikačního důkazu (ten v tomto případě logicky není možné obstarat), ale naopak existencí, resp. důkazní spolehlivostí důkazu prokazujícího opak (tj. v tomto případě splnění závazku).

Koherenční argument lze použít u skutkových tvrzení, která nelze vzhledem k okolnostem verifikovat ani falzifikovat. Typicky se koherenční argumentace uplatní v případech, kdy je skutkové tvrzení prokazováno za užití nepřímých důkazů. Důkazní kvalita, resp. způsobilost důkazu zapůsobit

ve smyslu praktické jistoty je v tomto případě dána vedle jeho spolehlivosti (věrohodnosti) ještě kumulativně obsahovou blízkostí k prokazované skutečnosti a dále pak mírou jeho koherence s ostatními důkazy[51].

U nepřímých důkazů je tedy třeba vždy vedle toho, do jaké míry jsou samy o sobě spolehlivé, ještě hodnotit, jak se k prokazované skutečnosti fakticky vztahují a zda nejsou v rozporu s ostatními skutkovými informacemi. Typickým příkladem koherenční argumentace skutkového stavu je otázka spojení virtuální identity s konkrétním člověkem. Nemáme v tomto směru nikdy k dispozici důkaz, kterým by bylo možno verifikovat nebo falsifikovat tvrzení ohledně skutečnosti, že konkrétní člověk např. napsal a odeslal určitý e-mail. Praktickou jistotu však může v tomto směru vytvořit kombinace nepřímých důkazů prokazujících např. skutečnost, že dotyčný byl k systému přihlášen pod identitou, kterou kromě něj nikdo další nepoužívá, že se v době odeslání mailu fyzicky nacházel v témže prostoru jako počítač, z něhož byl e-mail odeslán, nebo že styl, kterým byl e-mail napsán, odpovídá jeho obvyklým způsobům.

Na témže argumentačním základě, tj. na vzájemné koherenci různých skutkových informací, lze naopak postavit i spolehlivé vyvrácení skutkového tvrzení – to za předpokladu, že si jednotlivé skutkové informace vzájemně neodpovídají[52]. Typickým příkladem z trestního práva je alibi – je-li alibi spolehlivě (věrohodně) prokázáno, narušuje koherenci ostatních důkazů do té míry, že nelze logicky prokázat skutkové tvrzení ohledně viny obžalovaného.

I.8 Důkazní spolehlivost

Pojem důkazní spolehlivosti jsme shora použili už několikrát. Jedná se o kategorii, kterou označujeme míru věrohodnosti (důvěryhodnosti) důkazu, tj. o centrální kategorii vyjadřující informační hodnotu důkazu pro příslušné

51 Přes evidentně racionální podstatu nelze koherenci spolehlivě kvantifikovat. Výjimkou mohou být pouze typické (tj. srovnatelné a opakovaně se vyskytující) případy, kdy kvantifikaci jednotlivých parametrů koherence ospravedlňuje relevantní empirická zkušenost – k tomu viz Nissan, E. Can You Measure Circumstantial Evidence? The Background of Probative Formalisms for Law. *Information and Communications Technology Law*, 2001, roč. 10, č. 2, s. 231 a násl.

52 K tomu srov. např. nález Ústavního soudu sp. zn. I. ÚS 733/01, N 26/32 SbNU 239.

řízení. V případě aplikace korespondenčního argumentu je důkazní spolehlivost klíčovou kategorií implikující ověření nebo vyvrácení skutkového tvrzení. U koherenční argumentace skutkového stavu ještě informační hodnota důkazu závisí na míře jeho souvislosti se skutkovým tvrzením. Příkladně tak lze mít spolehlivý důkaz ohledně toho, co měl obžalovaný v den tvrzeného spáchání skutku na sobě – míra toho, jakou informační hodnotu bude mít takový důkaz pro praktickou jistotu ohledně tvrzeného spáchání skutku obžalovaným, však bude záviset na otázce, jak tato informace se skutkovým tvrzením logicky či empiricky souvisí. Otázka důkazní spolehlivosti má v naší procesní praxi zásadně tři možnosti řešení:

a) Empiricko-logickou
b) Konsensuální
c) Zákonnou

Empiricko-logické stanovení důkazní spolehlivosti je v praxi nejčastější, racionalistickou tradicí obecně preferované[53] a v největší míře se v něm projevuje princip volného hodnocení důkazů. Orgán autoritativně aplikující právo má v tomto směru na základě vlastního praktického poznání možnost volné úvahy co do věrohodnosti důkazu potud, nevybočuje-li taková úvaha mimo hranice empirického poznání nebo vnitřní logiky příslušného důkazu.

Od vnitřní logiky samotného důkazu však je v této souvislosti nutno oddělit logický vztah důkazu ke skutkovému tvrzení, resp. jeho vztah k ostatním důkazům (to je otázkou shora zmíněné korespondence nebo koherence). Jestliže lze např. křížovým výslechem dospět ke zpochybnění věrohodnosti svědecké výpovědi, jde o aplikaci empiricko-logické teorie spolehlivosti důkazu. Způsob, kterým se označení takového důkazu jako nespolehlivého projeví ve skutkovém stavu, pak je již otázkou koherenční argumentace praktické jistoty.

Konsensuální způsob hodnocení důkazní spolehlivosti je na místě aplikovat za situace, kdy je pravdivost skutkového tvrzení otázkou kvalifikované

53 Dominance racionality a logiky se v důkazním právu objevuje od 18. století a tato racionalistická tradice se v evropské i angloamerické právní kultuře udržuje doposud. Podrobněji viz Anderson, 2005, op. cit., s. 78 a násl.

shody. Konsensuální důkazy mohou mít charakter výpovědí stran, svědeckých výpovědí, ale též empirických studií zaměřených na chování nebo názory cílové skupiny.

Při důkazu konsensem je třeba obecně předpokládat mnohem menší míru přiblížení k materiální pravdě v porovnání s empiricko-logickým hodnocením důkazní spolehlivosti. Vedle zpravidla problematického vymezení cílové skupiny (samozřejmě s výjimkou případu, kdy ji např. tvoří strany civilního řízení) jde především o otázku zjištění skutečného lidského názoru či postoje – skutková informace, jejíž věrohodnost musí příslušný orgán veřejné moci konsensuálně posoudit, tedy může být značně zavádějící, tendenční a může se i rychle měnit v čase.

Zákonná důkazní spolehlivost staví na zákonných presumpcích. Jejími nástroji jsou zpravidla domněnky a fikce (viz dále), přičemž spolehlivost důkazu není v tomto případě otázkou jeho volného hodnocení, ale je předmětem zákonné konstrukce. To však neznamená, že by bylo možno se zákonnou důkazní spolehlivostí pracovat per se – prokazovaná skutečnost je totiž sice konstruována jako důkazně spolehlivá platným právem, vždy je však potřeba prokázat předpoklad (hypotézu) příslušné právní normy. Jestliže tedy zákon příkladně považuje za důkazně spolehlivý datový záznam pocházející ze systému určité kvality, je nutno předně empiricky hodnotit kvalitu příslušného systému a teprve v důsledku toho pak je možno s touto domněnkou, resp. presumpcí důkazní spolehlivosti pracovat.

I.9 Skutkový stav a právní skutečnosti

Skutkový stav je přímým důsledkem dosažení praktické jistoty. Jedná se o komplexní skutkovou informaci, na jejímž základě je v řízení přímo konstatován právní imperativ. V ideálním případě skutkový stav sestává výlučně z jednotlivých právních skutečností, tj. partikulárních skutkových informací odpovídajících skutkovým podstatám (hypotézám) dotčených právních norem. Jak bylo uvedeno shora, odpovídá nátuře naší právní kultury, pokud je skutkový stav vyjádřen v odůvodnění příslušného rozhodnutí

kategoricky a nekompromisně – vedle toho, že orgán autoritativně aplikující právo dosáhl ohledně skutku praktické jistoty, rovněž takové vyjádření podtrhuje nevyhnutný fakt, že výsledkem každého řízení je vždy relativní pravda.

Z hlediska jejich formalizovaného projevu ve skutkovém stavu můžeme rozlišovat mezi právními skutečnostmi:

- Prokazatelnými
- Předpokládanými
- Známými

Prokazatelné právní skutečnosti, kterých je v praktickém právu valná většina, je ve skutkovém stavu nutno konstatovat korespondenčně nebo koherenčně na základě provedených důkazů. Tomu logicky odpovídá závěr, že tyto skutečnosti je nutno v řízení prokazovat, a to formou důkazů přímých nebo nepřímých.

Předpokládané skutečnosti se naproti tomu projevují ve skutkovém stavu na základě prokázání jejich předpokladu odkazem na příslušnou právní normu. Podle jejich vztahu k materiální pravdě mezi nimi ještě dále rozlišujeme domněnky a fikce.

V případě domněnek je prokazovaný předpoklad indicií a je docela dobře možné, že právní normou konstruovaná právní skutečnost reálně nastala. Ze skutkové části odůvodnění však musí být každopádně patrné, že orgán autoritativně aplikující právo dospěl dokazováním pouze k předpokladu a že skutečnost, která je součástí skutkového stavu, má charakter zákonné domněnky.

U fikcí je naopak běžné, že prokazovaný předpoklad nemá s příslušnou právní skutečností žádnou logickou souvislost nebo je s ní dokonce v logické kontradikci[54]. Podobně jako u domněnky je nutno i fikci ve skutkové části odůvodnění příslušného rozhodnutí náležitě indikovat, tj. konstatovat, na základě jakého argumentu a jak spolehlivým důkazem byl předpoklad prokázán a jakou skutkovou kvalitu dává fikci příslušná právní norma.

54 Účelem fikce v důkazním právu se podrobně zabývá Maksymilian Del Mar v úvodním textu Del Mar, M., Twining, W. (eds.) Legal Fictions in Theory and Practice. Heidelberg: Springer International Publishing, 2015, s. XVI.

Je-li v řízení prokazována některá z předpokládaných skutečností, je nutno věnovat pozornost ještě okolnostem vylučujícím platnost hypotézy právní normy, která domněnku nebo fikci zakládá. V případě nevyvratitelných domněnek právo takovou skutečnost nepředpokládá, zatímco u domněnek vyvratitelných je i při prokázání předpokladu možno korespondenčně nebo koherenčně argumentovat logicky opačnou právní skutečnost.

V případě fikcí není důvod se korespondencí nebo koherencí opačného skutkového tvrzení zabývat – samo užití fikce je totiž dostatečným důkazem toho, že skutečnost tvořící součást skutkového stavu reálně nenastala. Vyloučit užití dispozice, která fikci zakládá, tedy na rozdíl od domněnek nelze prokázáním logického opaku. Namísto toho se zde můžeme setkat s negatorními rozhodovacími metanormami, které na základě hypotézy související s fingovanou právní skutečností způsobí neúčinnost zákonné fikce.

Poslední typ právních skutečností označujeme jako známé. Dle jejich povahy je ještě dále dělíme na notoriety, oficiality a skutečnosti známé z rozhodovací činnosti. V případě zapojení notoriet, tj. právních skutečností všeobecně známých, není nutno zabývat se jejich skutkovou argumentací. Analogicky s tím je možno s tímto typem skutečností pracovat v samotném řízení bez toho, aby bylo třeba navrhovat nebo provádět k nim důkazy.

Podobně jako v případě notoriet neprokazují se ani oficiality, tj. skutečnosti známé z úřední povinnosti. Přímé zahrnutí těchto skutečností do skutkového stavu v tomto případě neumožňuje jejich všeobecná známost ale zákonná povinnost příslušného orgánu znát jejich obsah. Analogicky s notorietami přitom není nutno ve skutkové části odůvodnění tento typ právních skutečností jakkoli hodnotit nebo uvádět, co konkrétně bylo zdrojem jejich poznání.

Skutečnosti známé z rozhodovací činnosti rovněž není nutno prokazovat, neboť je o nich orgán autoritativně aplikující právo obeznámen díky vlastní činnosti. Na rozdíl od notoriet a oficialit však je v tomto případě nutno kvůli přezkoumatelnosti skutkové části odůvodnění uvést přinejmenším informaci o tom, že kvalita, resp. způsob projevení těchto skutečností ve skutkovém stavu jsou dány aktuálními znalostmi příslušného orgánu veřejné moci.

Charakteru tohoto typu právních skutečností odpovídá i forma jejich praktického užití v rámci řízení. Skutečnosti, o nichž strany předpokládají, že jsou příslušnému orgánu veřejné moci známé z rozhodovací činnosti, tak mohou být součástí skutkových tvrzení bez toho, aby k nim bylo nutno od počátku navrhovat důkazy – pokud není kvalita těchto skutečností orgánu autoritativně aplikujícímu právo známa, je jeho právem a povinností důkaz si dodatečně vyžádat nebo si jej aktivně opatřit.

I.10 Shrnutí kapitoly

V této kapitole byla vyložena informační teorie důkazu, tj. pojetí důkazu jako skutkové informace organizující proces autoritativní aplikace práva. Tento způsob chápání důkazu jako právního fenoménu umožňuje systematickou a metodologicky konzistentní práci s důkazem ve vazbě na další fundamenty procesu autoritativní aplikace práva, z nichž jsme za nejdůležitější označili kategorie formální a materiální, resp. absolutní a relativní pravdy, volného hodnocení důkazů, praktické jistoty a důkazní spolehlivosti.

Zvláštní pozornost byla vedle povahy důkazu a základních principů týkajících se jeho zpracování věnována též proměnám důkazních nástrojů v důsledku technického vývoje. Rozvoj osobního využití informačních a komunikačních technologií vede k bezprecedentním možnostem ohledně sběru a zpracování dat týkajících se člověka. I nepatrně vyhlížející věc každodenní potřeby (typicky např. mobilní telefon nebo různé wearables) může v sobě koncentrovat data, jejichž analýzou lze nezřídka získat dokonalý přehled o pracovním i osobním životě člověka – ve vztahu k procesům autoritativní aplikace práva pak je nutno především řešit možnosti, jimiž lze tak hodnotné zdroje důkazů náležitě zužitkovat, to však za současného šetření práv člověka na ochranu soukromí.

Závěr této kapitoly byl věnován základní propedeutice dokazování – věnovali jsme se v tomto směru především typologii skutkové argumentace, základní metodologii stanovení důkazní spolehlivosti a taxonomii právních skutečností vzhledem ke komplexnímu skutkovému stavu. Dokazování v trestním řízení

II DOKAZOVÁNÍ V TRESTNÍM ŘÍZENÍ

II.1 Podstata a význam dokazování v trestním řízení

Dokazování v trestním řízení je vedle rozhodování nejdůležitější procesní činností orgánů činných v trestním řízení, protože umožňuje zjistit skutkový základ pro jejich rozhodování a pro další postup tak, aby mohl být splněn účel trestního řízení vymezený v ustanovení § 1 odst. 1 TŘ. Jím je takový postup orgánů činných v trestním řízení, který zaručí, aby trestné činy byly náležitě zjištěny a jejich pachatelé byli podle zákona spravedlivě potrestáni. Řízení přitom musí působit k upevňování zákonnosti, k předcházení a zamezování trestné činnosti, k výchově občanů v duchu důsledného zachovávání zákonů a pravidel občanského soužití i čestného plnění povinností ke státu a společnosti.

Význam dokazování spočívá především v tom, že jde o jedinou cestu, kterou si orgány činné v trestním řízení mohou a musí obstarat skutkový podklad pro své rozhodnutí, popřípadě pro jiný postup. Předmětem posuzování v trestním řízení jsou totiž takové události vnějšího světa představující skutek či jinou právně významnou skutečnost, které se staly v minulosti a které orgány činné v trestním řízení, jež o nich mají rozhodovat, osobně samy nepozorovaly ani se jich nezúčastnily (a pozorovat je nebo účastnit se jich ani nemohly, protože pak by byly z důvodu podjatosti vyloučeny z možnosti jejich nezávislého a nestranného posouzení). Vzhledem k tomu se orgány činné v trestním řízení mohou seznámit s posuzovanými skutečnostmi jen nepřímo tím, že si *jejich průběh rekonstruují pomocí zprostředkujících skutečností, jimiž jsou právě důkazy*. Na úplnosti, přesnosti a věrnosti takové rekonstrukce pak závisí výsledek trestního řízení a dosažení jeho účelu. Význam dokazování spočívá i v tom, že umožňuje aktivní účast stran v trestním řízení a uplatnění jejich práv.

Účelem dokazování je zjistit skutkový stav věci, o němž nejsou důvodné pochybnosti, a to v rozsahu, který je nezbytný pro každé rozhodnutí orgánů činných v trestním řízení (viz § 2 odst. 5 TŘ). Jen takové zjištění, k němuž dospěly orgány činné v trestním řízení po dokazování provedeném v dostatečné kvalitě, v potřebném rozsahu a za dodržení všech zákonných

požadavků může vést ke správnému, spravedlivému a přesvědčivému rozhodnutí ve věci. Dokazováním si proto opatřují orgány činné v trestním řízení *hodnověrné informace o určité minulé události* či o jiné skutečnosti významné pro trestní řízení, z nichž pomocí logického postupu odvozují úsudek o předmětu dokazování. Činí tak z důvodu, aby bylo jejich rozhodování dostatečně podložené, odůvodněné a přezkoumatelné.

Dokazováním v procesním trestním právu se tedy rozumí zákonem upravený postup orgánů činných v trestním řízení, jehož cílem je umožnit těmto orgánům poznání skutečností důležitých pro jejich rozhodnutí, tedy vyhledat důkazy o nich, tyto důkazy provést, získané poznatky procesně zajistit, zhodnotit a vyvodit z nich potřebné skutkové a právní závěry.

Důkazním právem v objektivním smyslu je pak souhrn právních norem trestního práva procesního, které upravují postup při dokazování. S ním úzce souvisí *teorie důkazů,* která jako součást nauky trestního práva procesního zkoumá platné důkazní právo, hodnotí jeho výklad a aplikaci v praxi a na podkladě toho činí návrhy na zdokonalení právní úpravy dokazování i aplikační praxe.

Dokazování jako procesní činnost velmi úzce souvisí s *kriminalistikou,* jejíž výsledky se přímo projevují při vyhledávání, zajišťování a využití různých důkazních prostředků. Kriminalistika totiž jako forenzní disciplína vypracovává postupy k odhalování, předcházení a vyšetřování trestné činnosti, aplikuje poznatky přírodních, technických a dalších věd za účelem jejich využití v boji se zločinem.

II.2 Právní úprava dokazování a jeho ústavní limity

II.2.1 Základní právní úprava dokazování v trestním řízení

Základní právní úprava trestního řízení včetně procesu dokazování je obsažena v zákoně č. 141/1961 Sb., *trestním řádu*, ve znění pozdějších předpisů. Trestní řád v hlavě páté pod názvem „Dokazování" (§ 89 až § 118 TŘ) upravuje některé *společné otázky* týkající se této důležité procesní činnosti orgánů činných v trestním řízení. Nejde ovšem o úpravu vyčerpávající, protože další pravidla pro dokazování jsou stanovena zaprvé obecně v ustanoveních § 2 odst. 2, 4, 5, 6, 11 a 12 TŘ, kde je obsažena zásada presumpce neviny, zásada oficiality, zásada vyhledávací a zjištění skutkového stavu bez důvodných

pochybností, zásada volného hodnocení důkazů, zásada ústnosti a zásada bezprostřednosti, a zadruhé v dalších ustanoveních specificky pro jednotlivá stadia trestního řízení. Tak např. v ustanovení § 158 odst. 3 TŘ jsou pravidla pro provádění takových úkonů policejního orgánu před zahájením trestního stíhání, z nichž některé směřují k opatření důkazu použitelného i po zahájení trestního stíhání nebo též v řízení před soudem [viz zejména § 158 odst. 3 písm. b) až f) TŘ]. V ustanoveních § 158 odst. 3 písm. i), odst. 9, § 158a, § 160 odst. 4 a § 179b odst. 1 TŘ je upraveno provádění neodkladných a neopakovatelných úkonů před zahájením trestního stíhání, jejichž výsledek je rovněž použitelný v řízení před soudem. V ustanovení § 73 g odst. 3 TŘ jsou pak obsažena pravidla pro dokazování ve vazebním zasedání, v § 164 TŘ pro dokazování v přípravném řízení, v § 179b TŘ při zkráceném přípravném řízení, v § 180 odst. 2, 3 TŘ pro důkazní aktivity státního zástupce a obviněného v řízení před soudem, v § 183a odst. 1 až 3 TŘ pro dokazování mimo hlavní líčení a veřejné zasedání, v § 203 odst. 1, § 207 až § 216 a § 218 TŘ pro hlavní líčení, v § 219 odst. 2, 3 TŘ pro postup v souvislosti s odročením hlavního líčení, v § 235 odst. 2 TŘ pro veřejné zasedání obecně, v § 243 TŘ pro neveřejné zasedání, v § 263 odst. 6, 7 TŘ pro veřejné zasedání konané v řízení o odvolání, v § 265o odst. 2 a § 265r odst. 7 TŘ pro potřebné šetření a rozsah dokazování v řízení o dovolání, v § 276 TŘ pro potřebné šetření v řízení o stížnosti pro porušení zákona, v § 282 odst. 1 a 2 TŘ pro potřebné šetření a zajištění důkazního materiálu v řízení o povolení obnovy, v § 314b odst. 2 a § 314d odst. 2 TŘ pro zjednodušené řízení před samosoudcem, v § 314q odst. 5 TŘ pro rozhodnutí o schválení dohody o vině a trestu atd.

Problematiky dokazování se týkají i *další ustanovení* trestního řádu upravující určité procesní úkony, které mají bezprostřední souvislost s dokazováním, resp. jejichž výsledek může mít důkazní význam. Jde např. o ustanovení § 78 a § 79 TŘ o vydání a odnětí věci důležité pro trestní řízení, § 82 až § 85a TŘ o domovní a osobní prohlídce, o prohlídce jiných prostor a pozemků, § 85b TŘ o provádění domovní prohlídky nebo prohlídky jiných prostor v místech, kde advokát vykonává advokacii, § 85c TŘ o provádění důkazu v bytě, obydlí, jiných prostorách a na pozemku, § 86 TŘ o zadržení zásilky, § 87b TŘ o sledované zásilce, § 88 TŘ o podmínkách, za nichž lze k důkazu použít odposlechu a záznamu telekomunikačního provozu, § 88a TŘ

o možnosti vyžádat k důkazu údaje o uskutečněném telekomunikačním provozu, § 158 odst. 6, § 211 odst. 6 a § 314d odst. 2 TŘ o důkazním významu úředního záznamu sepsaného o obsahu vysvětlení, atd. S dokazováním úzce souvisí i *operativně pátrací prostředky,* jejichž okruh a podmínky použití jsou soustředěny do ustanovení § 158b až § 158f TŘ a kterými jsou předstíraný převod, sledování osob a věcí a použití agenta (viz zejména možnost důkazního využití obrazových, zvukových a jiných záznamů získaných při použití operativně pátracích prostředků podle § 158b odst. 3 TŘ); v zákoně o Policii České republiky je pak obsažena právní úprava oprávnění k používání podpůrných operativně pátracích prostředků, tj. informátora, krycích prostředků, zabezpečovací techniky a zvláštních finančních prostředků (§ 72 až § 77 PolČR), jejichž využití může někdy směřovat i k následnému opatření procesně použitelných důkazů, a to i důkazů elektronických.

Způsob provádění důkazů, upravený v páté hlavě trestního řádu (§ 89 až § 118 TŘ), se uplatní *ve všech stadiích* trestního řízení a při všech úkonech orgánů činných v trestním řízení, jestliže se v rámci nich provádí dokazování a není-li zákonem jejich postup omezen na jiné úkony nebo jen na možnost provedení určitých důkazů (viz např. § 158 odst. 9, § 164 odst. 1, § 179b odst. 1, § 185 odst. 2, § 212, § 314d odst. 2, § 314q odst. 5 TŘ). To platí např. o výslechu zadrženého podezřelého (§ 76 odst. 5 TŘ), o výslechu svědka nebo rekognici prováděných jako neodkladný nebo neopakovatelný úkon (§ 158a TŘ), o výslechu svědka, jehož totožnost a podoba se utajuje (§ 55 odst. 2, § 101a, § 102a, § 165 odst. 2, 3, § 209 TŘ), o výslechu podezřelého ve zkráceném přípravném řízení (§ 179b odst. 3 TŘ), o provedení důkazu mimo hlavní líčení (§ 183a odst. 1 až 3 TŘ), o provádění důkazu policejním orgánem k žádosti státního zástupce nebo předsedy senátu (§ 179 odst. 2, § 183 odst. 1 TŘ) atd. Dokazování podle pravidel upravených v ustanoveních § 89 až § 118 TrŘ, popřípadě též podle dalších výše citovaných ustanovení, provádějí v podstatě *všechny orgány činné v trestním řízení,* tj. policejní orgán, státní zástupce i soud (soudce, senát, samosoudce), a to v rozsahu, který odpovídá stadiu trestního řízení, v němž každý z těchto orgánů působí (§ 2 odst. 5 TŘ). Obecným pravidlům stanoveným pro dokazování pak musejí vyhovovat i důkazy, které jsou vyhledány, opatřeny nebo prováděny *stranami trestního řízení,* např. podle § 89 odst. 2, § 110a, § 180 odst. 2, 3 a § 215 odst. 2 TŘ.

Tak, jako některé typy kriminality nejsou vázány jen na území jednoho státu, ani dokazování a opatřování důkazů není omezeno jen na území České republiky. Proto náš právní řád umožňuje využít i v trestním řízení *důkazy (důkazní prostředky), jejichž původ je v cizině,* resp. jejichž nositel, ať již jde o osobu nebo věc, se nachází v cizině (např. svědek vyslechnutý orgánem cizího státu, věc ohledaná orgánem cizího státu) nebo má svůj původ v cizině (např. listina vydaná orgánem cizího státu a zaslaná do České republiky). Takové důkazy jsou použitelné i v České republice,[55] jestliže byly opatřeny v souladu s právními předpisy cizího státu a nikoli v rozporu s ústavním pořádkem České republiky nebo s takovou zásadou právního řádu České republiky, na které je třeba bez výhrady trvat (§ 5 odst. 1 ZMJS). Důkazy se opatřují v cizině zpravidla dožádáním do ciziny (§ 39 a násl. ZMJS) včetně zvláštních druhů dožádání (§ 57 a násl. ZMJS), nebo mohou být opatřeny v cizině v souvislosti s převzetím trestního řízení z cizího státu (§ 112 a násl. ZMJS).

Zákonná ustanovení o dokazování tedy představují na jedné straně určitý *návod pro racionální postup* orgánů činných v trestním řízení při vytváření skutkového podkladu pro rozhodnutí a na druhé straně je jejich dodržování *zárukou zákonného procesu* vedeného proti obviněnému, předpokladem náležitého uplatnění jeho práv a podmínkou přípustnosti použití každého důkazu. Respektuje se zde tedy především zásada řádného zákonného procesu (§ 2 odst. 1 TŘ) a zásada zjištění skutkového stavu bez důvodných pochybností (§ 2 odst. 5 TŘ). V procesu dokazování se však uplatňují i *ostatní základní zásady* trestního řízení, zejména zásada vyhledávací, zásada presumpce neviny, zásada ústnosti a bezprostřednosti a zásada volného hodnocení důkazů.

II.2.2 Některé ústavní limity dokazování v trestním řízení

Vzhledem k tomu, že proces vyhledávání, opatřování a provádění důkazů v trestním řízení v mnoha směrech souvisí se zásahy do některých základních práv a svobod, vyplývají určité limity pro orgány činné v trestním řízení též z vnitrostátních a mezinárodních *norem o lidských právech a svobodách,* zejména z těch, které stanoví určité požadavky na spravedlivý trestní proces. V tomto směru se týkají dokazování zejména ustanovení čl. 95 odst. 1 a čl. 96 Ústavy, čl. 36 odst. 1, čl. 37, čl. 38 odst. 2 a čl. 40 odst. 4 LPS, čl. 14

55 Viz usnesení Vrchního soudu v Olomouci sp. zn. 5 To 187/2002, č. 11/2005 Sb. tr. rozh.

Mezinárodního paktu o občanských a politických právech (č. 120/1976 Sb.), čl. 6 EÚLP (č. 209/1992 Sb.) a čl. 15 Úmluvy proti mučení a jinému krutému, nelidskému či ponižujícímu zacházení nebo trestání (č. 143/1988 Sb.). Jinak je soud při zjišťování skutkového stavu věci zásadně vázán toliko zákonem[56] a musí být i v této činnosti nezávislý a nestranný.[57] Nesprávná realizace důkazního řízení pak může mít za následek porušení základních práv a svobod ve smyslu dotčení postulátů spravedlivého procesu.[58]

Jak vyplývá z charakteru trestního procesu, a především řízení před soudem, má zde zvláštní místo zejména ústavní princip *rovnosti stran* (čl. 96 odst. 1 Ústavy, čl. 37 odst. 3 LZPS). Podle judikatury Ústavního soudu však zásada rovnosti účastníků řízení (stran trestního řízení) neznamená, že by byl soud povinen vyhovět všem návrhům účastníků, případně že by měl dbát na to, aby důkazy provedené z jejich podnětu byly v určitém (úměrném) poměru; ustanovení čl. 6 odst. 3 písm. d) EÚLP neposkytuje absolutní právo na výslech každého svědka, jehož jmenovitě uvádí obhajoba.[59] Na druhé straně ovšem soud *nesmí nechat bez povšimnutí důkazní návrhy* stran, a i když neprovede jimi nabízené důkazy, musí se s neakceptovanými návrhy stran nebo s důkazy jimi opatřenými a předloženými ve svém rozhodnutí vypořádat a náležitě odůvodnit, proč nevyhověl těmto návrhům stran.[60] Důkazy vyhledané, opatřené nebo navržené některou ze stran pak nestačí jen *provést*, ale je třeba je odpovídajícím způsobem logicky a přesvědčivě *vyhodnotit*

56 Srov. nález Ústavního soudu sp. zn. III. ÚS 26/94, N 32/1 SbNU 241.

57 Viz usnesení Ústavního soudu sp. zn. Pl. ÚS 41/2000, U 7/21 SbNU 493. Viz také nález Ústavního soudu sp. zn. III. ÚS 628/2000, N 67/22 SbNU 87.

58 Viz souhrnně nález Ústavního soudu sp. zn. IV. ÚS 570/03, N 91/33 SbNU 377 a další judikaturu v tomto nálezu citovanou. Viz rovněž nález Ústavního soudu sp. zn. I. ÚS 2343/08, N 67/52 SbNU 663, nález Ústavního soudu sp. zn. IV. ÚS 1235/09, N 144/58 SbNU 207 a nález Ústavního soudu sp. zn. I. ÚS 864/11, N 116/61. K významu hodnocení důkazů v trestním řízení viz též nález Ústavního soudu sp. zn. IV ÚS 335/05, N 116/41 SbNU 453, nález Ústavního soudu sp. zn. I. ÚS 910/07, N 156/50 SbNU 389, nález Ústavního soudu sp. zn. III. ÚS 1104/08, N 65/52 SbNU 635 a nález Ústavního soudu sp. zn. I. ÚS 3094/08, N 103/53 SbNU 293.

59 Viz nález Ústavního soudu sp. zn. I. ÚS 32/95, N 40/5 SbNU 331.

60 Srov. nález Ústavního soudu sp. zn. III. ÚS 51/96, N 57/8 SbNU 69, nález Ústavního soudu sp. zn. I. ÚS 425/97, N 42/13 SbNU 305, nález Ústavního soudu sp. zn. III. ÚS 258/99, N 148/16 SbNU 99, nález Ústavního soudu sp. zn. II. ÚS 441/99, N 48/17 SbNU 337, nález Ústavního soudu sp. zn. III. ÚS 464/99, N 109/19 SbNU 63, nález Ústavního soudu sp. zn. I. ÚS 459/2000, N 89/27 SbNU 51, nález Ústavního soudu sp. zn. III. ÚS 26/03, N 22/32 SbNU 201, nález Ústavního soudu sp. zn. I. ÚS 733/01, N 26/32 SbNU 239, nález Ústavního soudu sp. zn. I. ÚS 2343/08, N 67/52 SbNU 663 a nález Ústavního soudu sp. zn. III. ÚS 3320/09, N 60/56 SbNU 643.

(§2 odst. 6 TŘ) a soud musí své hodnotící úvahy k nim uvést do odůvodnění rozhodnutí (§ 125 odst. 1, § 134 odst. 2 TŘ) tak, aby bylo i z tohoto hlediska přezkoumatelné.[61] Právní úprava vyšetřování a řízení před soudem nezná institut předběžného posuzování (hodnocení) důkazů, a proto není v pravomoci kteréhokoli orgánu činného v trestním řízení, aby prováděl podle vlastních kritérií předběžnou selekci (nabízených) důkazů a upravoval tak důkazní situaci podle vlastní úvahy a volby, případně z daných důkazů a priori preferoval ty, které potvrzují zvolenou skutkovou verzi.[62] Přitom podle judikatury Ústavního soudu *neakceptování důkazního návrhu* obviněného lze založit toliko třemi důvody: prvním je argument, podle něhož tvrzená skutečnost, k jejímuž ověření nebo vyvrácení je navrhován důkaz, nemá relevantní souvislost s předmětem řízení. Dalším je argument, podle kterého důkaz není s to ani ověřit, ani vyvrátit tvrzenou skutečnost, čili ve vazbě na toto tvrzení nedisponuje vypovídací potencí. Konečně třetím je pak nadbytečnost důkazu, tj. argument, podle kterého určité tvrzení, k jehož ověření nebo vyvrácení je důkaz navrhován, bylo již v dosavadním řízení bez důvodných pochybností (s praktickou jistotou) ověřeno nebo vyvráceno.[63]

Problematikou dokazování v trestním řízení se zabývá v mnoha souvislostech i *Evropský soud pro lidská práva* na podkladě stížností opřených zejména o ustanovení čl. 5 EÚLP (ochrana svobody a bezpečnosti), čl. 6 EÚLP (právo na spravedlivý proces) a čl. 8 EÚLP (ochrana rodinného a soukromého života), přičemž ve své obsáhlé judikatuře již formuloval řadu zobecňujících závěrů, jimiž ovlivnil jak právní úpravu některých otázek trestního řízení včetně dokazování v něm prováděného, tak i praxi orgánů činných v trestním řízení ve státech Rady Evropy včetně České republiky.[64]

61 Srov. nález Ústavního soudu sp. zn. III. ÚS 95/97, N 76/8 SbNU 231, usnesení Ústavního soudu sp. zn. I. ÚS 484/97, U 7/10 SbNU 361, nález Ústavního soudu sp. zn. III. ÚS 181/2000, N 175/20 SbNU 241, nález Ústavního soudu sp. zn. III. ÚS 463/2000, N 181/20 SbNU 267, nález Ústavního soudu sp zn. IV. ÚS 802/02, N 58/33 SbNU 89, nález Ústavního soudu sp. zn. I. ÚS 566/03, N 104/34 SbNU 99, nález Ústavního soudu sp. zn. III. ÚS 224/04, N 116/34 SbNU 213 a nález Ústavního soudu sp. zn. III. ÚS 1104/08, N 65/52 SbNU 635.

62 Srov. nález Ústavního soudu sp. zn. III. ÚS 617/2000, N 143/24 SbNU 27 a nález Ústavního soudu sp. zn. IV. ÚS 1526/08, N 188/51 SbNU 301.

63 Viz nález Ústavního soudu sp. zn. I. ÚS 733/01, N 26/32 SbNU 239.

64 K tomu viz souhrnně zejména publikace Kmec, J., Kosař, D., Kratochvíl, J., Bobek, M. *Evropská úmluva o lidských právech. Komentář. 1. vydání.* Praha: C. H. Beck, 2012; Repík, B. *Evropská úmluva o lidských právech a trestní právo.* Praha: Nakladatelství Orac, 2002; Čapek, J. *Evropská úmluva o ochraně lidských práv a základních svobod.* Praha: Linde Praha, 2010.

II.3 Subjekty dokazování

Trestní řád nevymezuje *subjekty dokazování,* tedy osoby, které se účastní procesu dokazování a vykonávají vliv na jeho průběh a výsledky svými úkony, k nimž je zákon opravňuje nebo zavazuje. Podle významu, jaký mají v rámci dokazování, lze považovat za subjekty dokazování:

a) *orgány činné v trestním řízení* (§ 12 odst. 1 TŘ), které rozhodují o předmětu a rozsahu dokazování, důkazy vyhledávají, zajišťují, provádějí, prověřují a hodnotí. V procesu dokazování mají stěžejní postavení, protože odpovídají za jeho řádný a zákonný průběh a organizují jej zároveň tak, aby mohly uplatnit svá práva v dokazování i ostatní subjekty. Pokud orgány činné v trestním řízení provádějí dokazování, činí tak zpravidla přímo samy, jen výjimečně prostřednictvím dožádaného orgánu (§ 53 a § 54 TŘ), resp. dožádáním do ciziny (§ 39 a násl. ZMJS) včetně zvláštních druhů dožádání (§ 57 a násl. ZMJS). Kromě orgánů činných v trestním řízení mohou za určitých okolností vyhledat, předložit nebo provést důkaz *i strany* (§ 89 odst. 2 věta druhá, § 215 odst. 2 TŘ);

b) *strany trestního řízení* (§ 12 odst. 6 TŘ), které mohou přímo poskytnout důkaz (výpověď obviněného, svědecká výpověď poškozeného) nebo navrhovat provedení důkazů a vyjadřovat se k nim, mohou samy vyhledat a předložit důkazy (viz § 89 odst. 2 věta druhá, § 110a, § 180 odst. 2, 3 TŘ), klást otázky vyslýchaným osobám (§ 215 odst. 1, 3 TŘ), přičemž státní zástupce, obžalovaný a jeho obhájce může na žádost sám provést před soudem důkaz, zejména výslech svědka nebo znalce (§ 215 odst. 2 TŘ);

c) *ostatní osoby,* pokud mají vliv na dokazování, např. znalec, který může podle § 107 odst. 1 věty šesté TŘ navrhnout provedení důkazů potřebných k podání posudku nebo může sám podle § 108 odst. 1 věty druhé a § 210 TŘ nadiktovat posudek nebo jeho doplněk do protokolu. Dále je subjektem ten, kdo je povinen předložit nebo vydat věc důležitou pro trestní řízení podle § 78 odst. 1 TŘ, která pak může být věcným důkazem, a na dokazování může mít vliv též konzultant (§ 157 odst. 3, § 183 odst. 2 TŘ), pokud přispívá ke správnému zaměření a rozsahu opatřovaných důkazů.

II.4 Předmět a rozsah dokazování v trestním řízení

II.4.1 Předmět dokazování

Předmětem dokazování se rozumí okruh skutečností, jež je nutné v trestním řízení dokazovat. Trestní řád ukládá orgánům činným v trestním řízení dokazovat v podstatě 3 okruhy skutečností:

a) okolnosti důležité pro rozhodnutí *ve věci samé* (které jsou významné z hlediska hmotného práva), tj. *skutkové okolnosti naplňující znaky trestného činu* spatřovaného ve stíhaném skutku, okolnosti nasvědčující nebo vyvracející, že jeho pachatelem je obviněný, důvody vylučující trestnost činu, okolnosti důležité pro uložení určitého opatření obviněnému (trestu, ochranného opatření, náhrady škody nebo nemajetkové újmy, resp. vydání bezdůvodného obohacení);

b) okolnosti důležité *pro postup trestního řízení*, např. okolnosti odůvodňující odročení hlavního líčení, přerušení trestního stíhání, odepření povinnosti svědčit atd.;

c) okolnosti, které *vedly* k trestné činnosti nebo *umožnily* její spáchání, a okolnosti důležité pro rozhodnutí o uplatněném nároku na *náhradu škody nebo nemajetkové újmy nebo na vydání bezdůvodného obohacení.*

U všech tří uvedených okruhů bude přicházet v úvahu i dokazování okolností důležitých pro hodnocení *věrohodnosti* důkazů a skutečností, které mají být *nepřímými* důkazy (viz níže podkapitolu II.7). Skutkový stav musí být spolehlivě prokázán také ve vztahu k okolnostem, které, pokud existují, vyvolávají nutnost *jiného rozhodnutí, než je rozhodnutí o vině a trestu* (případně též o náhradě škody nebo odčinění nemajetkové újmy, resp. o vydání bezdůvodného obohacení), např. nutnost přerušení trestního stíhání[65] či zastavení trestního stíhání,[66] resp. možnost rozhodnutí některým z alternativních způsobů – schválením dohody o vině a trestu (§ 175a a § 175b, § 314o až § 314s TŘ), podmíněným zastavením trestního stíhání (§ 307 TŘ), schválením narovnání (§ 309 a násl. TŘ) nebo odstoupením od trestního stíhání

65 Viz rozsudek Nejvyššího soudu sp. zn. 7 Tz 26/98, č. 28/1999 Sb. tr. rozh.

66 Srov. rozsudek Nejvyššího soudu sp. zn. 11 Tz 51/65, č. 7/1966 Sb. tr. rozh. a rozsudok Najvyššieho súdu sp. zn. 4 Tz 105/76, č. 28/1977 Sb. tr. rozh.

mladistvého (§ 70 ZSM). Podobně je třeba dokazováním vytvořit skutkový podklad pro jiné než meritorní rozhodnutí, např. o vrácení vydané či odňaté věci důležité pro trestní řízení (§ 80 odst. 1 TŘ).[67]

II.4.2 Rozsah dokazování

Pod pojmem *rozsah dokazování* lze rozumět stanovení hranice dokazování, tedy množství a kvality důkazů, jimiž má být prokázán ten okruh dokazovaných skutečností, který je vymezen předmětem dokazování. Negativně je pak rozsah dokazování vymezen i tím, které skutečnosti se v trestním řízení nedokazují, resp. je nelze dokazovat.

Okruh okolností, které bude nutné dokazovat v konkrétním případě, a to jak z hlediska předmětu, tak i z hlediska rozsahu dokazování, je v každé trestní věci závislý na skutečných podmínkách a okolnostech tohoto případu, na jeho povaze a rozsahu a na právě probíhajícím stadiu trestního stíhání. Proto např. pro zahájení trestního stíhání postačí méně důkazů než pro podání obžaloby a pro podání obžaloby zase méně než pro odsuzující rozsudek.[68] Podle výsledků prováděného dokazování se pak jeho okruh může zužovat nebo rozšiřovat. Různost konkrétních případů však nedovoluje vypracovat předem dané a obecně platné schéma určující vyčerpávajícím způsobem okruh dokazovaných okolností, což je důsledkem uplatnění zásady zjišťování skutkového stavu v potřebném rozsahu bez důvodných pochybností (§ 2 odst. 5 TŘ) a zásady volného hodnocení důkazů (§ 2 odst. 6 TŘ). Proto je věcí orgánu činného v trestním řízení, před nímž se právě řízení vede, aby si sám stanovil kvalitativní i kvantitativní meze dokazování, ovšem s vědomím důsledků pro případná další stadia téhož trestního řízení [viz např. možnost rozhodnutí soudu podle § 188 odst. 1 písm. e) TŘ]. Zjišťování okolností, které nejsou pro potřeby trestního stíhání nutné, pak zbytečně řízení protahuje, zatemňuje a odvádí pozornost od skutečností důležitých. V tomto smyslu nutno rovněž vykládat slova *v nezbytném rozsahu* v návětě ustanovení § 89 odst. 1 TŘ.[69] Jde o rozsah nezbytný pro rozhodnutí každého orgánu činného v trestním řízení tak, aby byl dostatečně zjištěn skutkový stav, o němž nejsou důvodné pochybnosti, a aby rozsah odpovídal potřebám

67 Srov. rozsudek Nejvyššího soudu sp. zn. 5 Tz 214/2001.
68 Srov. rozsudek Nejvyššího soudu sp. zn. 5 Tz 174/2001.
69 Srov. usnesení Nejvyššího soudu sp. zn. 3 Tz 62/91, č. 10/1993 Sb. tr. rozh.

příslušného orgánu činného v trestním řízení z hlediska toho rozhodnutí, do jehož vydání má dokazování vyústit.[70] V konkrétním případě může být obsah a rozsah dokazování prováděného určitým orgánem činným v trestním řízení *ovlivněn závazným právním názorem* nadřízeného orgánu, který rozhodoval o opravném prostředku (§ 149 odst. 6, § 264 odst. 1, § 265s odst. 1 a § 270 odst. 4 TŘ), dozorovým oprávněním státního zástupce [§ 174 odst. 2 písm. d) TŘ], rozhodnutím soudu o vrácení věci státnímu zástupci k došetření (§ 191 odst. 1, § 221 odst. 3 a § 260 TŘ), kasačním nálezem Ústavního soudu (§ 314h odst. 1 TŘ) nebo rozhodnutím Soudního dvora Evropských společenství o předběžné otázce (§ 9a odst. 4 TŘ).

Trestní řád vyžaduje, aby byly dokazovány všechny *podstatné okolnosti důležité pro trestní řízení,* které je nezbytné zjistit a prokázat, aby bylo možné učinit určité rozhodnutí nebo zvolit příslušný procesní postup. V zásadě zde *nestačí pouhé tvrzení stran*, proto i obsah doznání obviněného musí být ověřen dalšími věrohodnými důkazy.[71] Skutečnosti tzv. nepochybné či nesporné (viz § 120 odst. 3 OSŘ) trestní řád zpravidla nezná a v trestním řízení neplatí ani tzv. notoriety ve smyslu § 121 OSŘ. Výjimkou je zjednodušené řízení konané před samosoudcem po zkráceném přípravném řízení, v němž není třeba dokazovat *skutečnosti, které strany považují za nesporné* (viz § 314b odst. 2 věta první, § 314d odst. 2 věta druhá TŘ). Navíc i orgány činné v trestním řízení musí při vytváření poznatků o vnějším světě vycházet z ustálených pravidel myšlení a ze zkušeností, proto není třeba dokazovat ani v trestním řízení skutečnosti, které se podle obecné lidské zkušenosti považují za pravdivé, pokud o nich nevzniknou pochybnosti, např. že obviněný byl v době spáchání trestného činu příčetný, že písemnost došlá orgánu činnému v trestním řízení pochází od toho, kdo je v ní uveden jako podatel, že se na určitou osobu vztahuje působnost trestního zákoníku a trestního řádu apod. Vzniknou-li však i v těchto směrech pochybnosti, musí být proveden potřebný důkaz.

Ani v trestním řízení *nelze dokazovat* skutečnosti, o nichž bylo rozhodnuto způsobem závazným i pro trestní řízení nebo o kterých mohou rozhodovat

70 Viz rozsudek Krajského soudu v Plzni sp. zn. 4 To 167/63, č. 14/1964 Sb. tr. rozh.

71 Srov. rozsudek Nejvyššího soudu sp. zn. 7 Tz 11/68, č. 38/1968 Sb. tr. rozh. a nález Ústavního soudu sp. zn. I. ÚS 864/11, N 116/61 SbNU 695.

jen jiné orgány než orgány činné v trestním řízení, např. ohledně otázek týkajících se rodinněprávních věcí ve smyslu § 367 a násl. zákona č. 292/2013 Sb., o zvláštních řízeních soudních (viz § 9 odst. 2 TŘ). Jde zde o negativní vymezení předmětu a rozsahu dokazování. Předmětem dokazování nejsou ani právní normy České republiky, dále závazné a přímo použitelné normy práva Evropské unie a ani některé již shora zmíněné obecně známé skutečnosti.

Ustanovení § 89 odst. 1 TŘ pak uvádí v obecných rysech *okruh určitých okolností*, které bude třeba *pravidelně v každém trestním stíhání dokazovat,* ať budou zvláštnosti případu jakékoli. V trestním stíhání je tedy třeba v nezbytném rozsahu dokazovat zejména:

a) zda se stal skutek, v němž je spatřován trestný čin,
b) zda tento skutek spáchal obviněný, případně z jakých pohnutek,
c) podstatné okolnosti mající vliv na posouzení povahy a závažnosti činu,
d) podstatné okolnosti k posouzení osobních poměrů pachatele,
e) podstatné okolnosti umožňující stanovení následku, výše škody způsobené trestným činem a bezdůvodného obohacení,
f) okolnosti, které vedly k trestné činnosti nebo umožnily její spáchání.[72]

II.5 Důkaz, důkazní prostředek, demonstrativní výčet důkazních prostředků

V ustanovení § 89 odst. 2 TŘ podává trestní řád demonstrativní výčet důkazních prostředků, které slouží v trestním řízení k dokazování skutečností, jež jsou jeho předmětem, a umožňuje uplatnit důkazní aktivitu stran. Trestní řád však důsledně nerozlišuje mezi pojmy *důkaz*, *důkazní prostředek* a *pramen důkazu*, aniž by to činilo v praxi problémy, protože existuje úzká souvislost mezi uvedenými pojmy. Ustanovení § 89 odst. 2 TŘ obsahuje obecné vymezení okruhu důkazních prostředků a dále zakotvuje podíl stran na jejich opatřování.

72 Podrobněji k dokazování tohoto okruhu okolností viz v publikaci Šámal, P. a kol. *Trestní řád I. § 1 až 156. Komentář. 7. vydání.* Praha: C. H. Beck, 2013, s. 1324.

Důkazem se rozumí výsledek činnosti orgánu činného v trestním řízení při dokazování (např. obsah výpovědi vyslýchané osoby, obsah listiny, výsledek znaleckého zkoumání – obsah znaleckého posudku a odpověď znalce na položené otázky, výsledek získaný ohledáním atd.). Jde tedy o přímý poznatek získaný orgánem činným v trestním řízení o existenci či neexistenci určité okolnosti, která se má dokazovat (o předmětu dokazování). Jen o důkazy v tomto smyslu pak může orgán činný v trestním řízení opřít svá skutková zjištění, která jsou podkladem pro jeho rozhodnutí.

Důkazním prostředkem je procesní činnost orgánu činného v trestním řízení nebo oprávněné strany trestního řízení, která slouží k poznání skutečnosti, jež má být zjištěna. Důkazní prostředek je tedy nástroj k tomu, aby mohl orgán činný v trestním řízení dospět k přímému poznatku o předmětu dokazování, tj. k důkazu určité relevantní skutečnosti. V tomto smyslu jsou důkazními prostředky např. výslech obviněného, svědka, znalce, ohledání osoby nebo věci, čtení listiny atd.

Pramenem důkazů jsou nositelé informace, z níž se čerpá poznatek, který je předmětem dokazování. Prameny důkazů jsou buď osoby, nebo věci a podle tohoto hlediska lze důkazní prostředky rozdělit na osobní (výslech obviněného, svědků, znalců, ohledání osoby) a věcné (ohledávané věci, listiny, místo činu). Význam tohoto dělení je však sporný.

V ustanovení § 89 odst. 2 větě první TŘ jsou uvedeny příklady nejčastěji používaných důkazních prostředků v trestním řízení. V dalších ustanoveních (§ 90 a násl. TŘ) pak trestní řád upravuje podrobnosti pro dokazování těmito důkazními prostředky.

Trestní řád nepovažuje obecně některý druh důkazních prostředků nebo jeden z nich (např. znalecký posudek[73] nebo daktyloskopickou expertizu[74]) za průkaznější než jiný. Důkazní význam každého důkazního prostředku je závislý na okolnostech konkrétní trestní věci, na druhu, povaze a důkazní hodnotě ostatních ve věci získaných důkazních prostředků a na tom, jak sám o sobě a ve spojení s ostatními důkazy potvrzuje nebo vyvrací dokazovanou

73 Viz rozsudek Nejvyššího soudu sp. zn. 1 Tz 30/53, č. 56/1953 Sb. tr. rozh., rozsudek Nejvyššího soudu sp. zn. Tsf 1/72, č. 40/1972 Sb. tr. rozh., a rozsudek Nejvyššího soudu sp. zn. 5 Tz 175/2001.

74 Viz rozsudek Nejvyššího soudu sp. zn. 10 Tz 34/65, č. 46/1965 Sb. tr. rozh.

skutečnost. V zásadě *lze použít každého důkazního prostředku k dokazování jakékoli skutečnosti* důležité pro trestní řízení, protože zákon zpravidla nepředepisuje, kterým důkazním prostředkem by měla být dokazována určitá relevantní skutečnost. Jen výjimečně je stanoveno *použití určitého důkazního prostředku*; tak např. vyžaduje se odborné vyjádření nebo znalecký posudek podle § 105 TŘ, je-li k objasnění skutečnosti důležité pro trestní řízení třeba odborných znalostí, dále k prohlídce a pitvě mrtvoly je třeba vždy přibrat dva znalce podle § 105 odst. 4 TŘ, psychiatrický znalecký posudek podle § 115 až § 118 TŘ je nutný, je-li třeba vyšetřit duševní stav obviněného nebo svědka, ve zvláštních případech vyžadujících vědeckého posouzení je pak nezbytný znalecký posudek státního orgánu, vědeckého ústavu, vysoké školy nebo instituce specializované na znaleckou činnost podle § 110 TŘ.

Okruh důkazních prostředků výslovně uvedených v ustanovení § 89 odst. 2 TŘ je *jen demonstrativní* a může být v konkrétních případech doplněn i dalšími výslovně zde nezmíněnými důkazními prostředky, což zákon umožňuje nejen demonstrativním výčtem těch vyjmenovaných, ale i obecnou formulací, podle které za důkaz může sloužit *vše, co může přispět k objasnění věci*. Touto formulací je zároveň vyjádřeno určité omezení obecně stanoveného okruhu důkazních prostředků: důkaz musí mít *vztah* k objasňované věci a musí být *způsobilý* prokázat či vyvrátit dokazovanou skutečnost. Jinak tedy v podstatě žádný úkon, který může přispět k objasnění věci, nelze apriorně vyloučit z okruhu přípustných důkazních prostředků jen proto, že jde o úkon určitého druhu a že ho zákon výslovně neupravuje (viz též § 55 odst. 3 poslední větu TŘ). Má-li určitý důkazní prostředek obecné náležitosti úkonu podle trestního řádu (resp. neporušuje-li zákon ani ho neobchází) a je-li způsobilý k prokazování skutečností důležitých pro trestní řízení, lze ho použít jako důkaz, i když trestní řád nemá zvláštní úpravu postupu při provádění tohoto úkonu. Může jít např. o obsah *obrazového záznamu z kamerového systému*, který poškozený nainstaloval za účelem zjištění identity osoby poškozující jeho majetek,[75] o *zvukové, obrazové a jiné záznamy* osob podle § 158 odst. 3 písm. f) TŘ nebo takové záznamy získané při použití operativně pátracích prostředků v souladu s trestním řádem podle § 158b

75 Viz usnesení Nejvyššího soudu sp. zn. 3 Tdo 593/2009, č. 22/2010 Sb. tr. rozh. a usnesení Ústavního soudu sp. zn. IV. ÚS 2425/09, U 4/56 SbNU 841.

odst. 3 a § 158d odst. 7 TŘ[76] nebo při pořizování zvukového záznamu o průběhu hlavního líčení podle § 55b odst. 1 TŘ,[77] dále lze k důkazu použít záznam telekomunikačního provozu opatřený za splnění podmínek § 88 odst. 6 TŘ,[78] údaje o uskutečněném telekomunikačním provozu poskytnuté podle § 88a TŘ. Za důkaz mohou sloužit i soukromě pořízené obrazové nebo zvukové záznamy, byť byly opatřeny bez vědomí osob, jejichž osobní projevy jsou takto zaznamenány.[79] Použitelné jsou rovněž *elektronické důkazy*, např. v podobě různých záznamů na elektronických nosičích informací (např. v počítačích, na serverech, v mobilních telefonech, na přenosných záznamových médiích apod.).

Tak např. v jedné trestní věci byl k usvědčení pachatele, který po poškození zámku vstupních dveří neoprávněně vnikl do domu poškozeného, připuštěn i důkaz v podobě videozáznamu z bezpečnostní kamery, kterou si poškozený nainstaloval tak, aby snímala prostor před vchodem do domu. Nejvyšší soud zde dospěl mimo jiné k závěru, že s ohledem na ustanovení § 89 odst. 2 TŘ lze za důkaz použitelný v trestním řízení pokládat též obsah obrazového záznamu z kamerového systému, který poškozený nainstaloval za účelem zjištění identity osoby poškozující jeho majetek (např. jeho obydlí, jeho automobil). V takovém případě zpravidla nepředstavuje jednání poškozeného nepřípustný zásah do soukromí zaznamenané osoby, který by znamenal neúčinnost tohoto důkazu, i když instalaci záznamového zařízení a jeho provoz poškozený neoznámil Úřadu pro ochranu osobních údajů podle § 16 odst. 1, odst. 2 ZOOÚ. Přípustnost takto opatřeného důkazu

76 Viz nález Ústavního soudu sp. zn. II. ÚS 2806/08, N 15/56 SbNU 143.

77 Viz usnesení Nejvyššího soudu sp. zn. 8 Tdo 921/2009, č. 3/2011 Sb. tr. rozh.

78 Srov. usnesení Nejvyššího soudu sp. zn. 7 Tdo 638/2010, č. 56/2011 Sb. tr. rozh. a usnesení Vrchního soudu v Praze sp. zn. 2 To 144/03, č. 19/2004 Sb. tr. rozh. Ústavní soud však nálezem sp. zn. I. ÚS 3038/07, N 46/48 SbNU 549, nepřipustil k důkazu v trestním řízení odposlech a záznam telekomunikačního provozu opatřený podle tzv. zpravodajských zákonů, v konkrétním případě podle zákona č. 67/1992 Sb., o Vojenském obranném zpravodajství, ve znění pozdějších předpisů (nyní jde o zákon č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů). Základním důvodem byla podle Ústavního soudu skutečnost, že tyto jiné zákony stanoví mírnější podmínky k průlomu do ochrany soukromí než trestní řád.

79 Viz usnesení Nejvyššího soudu sp. zn. 5 Tdo 459/2007, č. 7/2008 Sb. tr. rozh.

je však nezbytné vždy posuzovat i s přihlédnutím k právu na soukromí zakotvenému v čl. 8 EÚLP a na nedotknutelnost osoby a jejího soukromí ve smyslu čl. 7 a čl. 10 odst. 2 LZPS.[80]

V jiné trestní věci byla jako jeden z důkazů využita k usvědčení pachatele též soukromá nahrávka telefonického rozhovoru pachatele s jinou osobou, která tuto nahrávku pořídila bez vědomí pachatele. Nejvyšší soud v tomto případě uzavřel, že s ohledem na ustanovení § 89 odst. 2 TŘ zásadně nelze vyloučit možnost, aby byl k důkazu použit i zvukový záznam, který byl pořízen soukromou osobou bez souhlasu osob, jejichž hlas je takto zaznamenán. Ustanovení § 88 TŘ o odposlechu a záznamu telekomunikačního provozu, jehož použití se pachatel (obviněný) domáhal, se zde neuplatní, a to ani analogicky. Přípustnost takového důkazu je však nezbytné vždy posuzovat též s ohledem na respektování práva na soukromí zakotveného v čl. 8 EÚLP, práva na nedotknutelnost osoby a jejího soukromí ve smyslu čl. 7 a čl. 10 odst. 2 LZPS.

Žádný druh důkazního prostředku nelze předem vyloučit, kromě případů, v nichž *přímo z trestního řádu* (nebo i z jiného právního předpisu) vyplývá *nepřípustnost* určitého důkazního prostředku, postupu nebo úkonu, resp. kde lze dovodit jeho nepřípustnost z některých souvislostí a za určitých okolností. Výslovně upraveným omezením je podle § 89 odst. 3 TŘ jen situace, kdy byl *důkaz získaný nezákonným donucením nebo hrozbou takového donucení*; tento důkaz nesmí být použit v řízení s výjimkou případu, kdy se použije jako důkaz proti osobě, která použila takového donucení nebo hrozby donucení. Jinak však český trestní řád – na rozdíl od některých zahraničních úprav – *neobsahuje* kromě ustanovení § 89 odst. 3 TŘ žádné další tzv. *vylučovací klauzule,* v nichž by byl výslovně stanoven výčet všech případů nepřípustných (zakázaných, neúčinných či nepoužitelných) důkazních prostředků, postupů a úkonů. Jejich nepřípustnost pak lze dovodit výkladem některých ustanovení, jak učinila judikatura nebo odborná literatura.[81] Tak např. podle § 88 odst. 1 věty třetí TŘ nelze použít získané informace o komunikaci mezi obhájcem

80 Viz výše zmíněné usnesení Nejvyššího soudu sp. zn. 3 Tdo 593/2009, č. 22/2010 Sb. tr. rozh., později potvrzené usnesením Ústavního soudu sp. zn. IV. ÚS 2425/09, U 4/56 SbNU 841.

81 V podrobnostech k takovým případům odkazujeme např. na publikaci Šámal, 2013a, op. cit., s. 1336-1340.

a obviněným při odposlechu a záznamu telekomunikačního provozu, podle § 88 odst. 6 věty třetí TŘ záznam telekomunikačního provozu nelze použít v jiné trestní věci bez splnění podmínek zde uvedených, podle § 158d odst. 1 TŘ nelze nijak použít poznatky zjištěné ze záznamu o komunikaci obviněného s obhájcem při sledování osob a věcí atd. Nepřípustný je i důkaz opatřený při provádění nezákonného procesního úkonu, např. získání listiny nebo jiného věcného důkazu při nepovolené domovní prohlídce a prohlídce jiných prostor nebo pozemků,[82] opatření zvukových záznamů rozhovorů osob v rozporu se zákonem,[83] získání a použití záznamu o odposlechu telefonických hovorů v rozporu s ustanovením § 88 TŘ, resp. jejich opatření podle jiných předpisů[84], získání zvukových, obrazových a jiných záznamů při použití operativně pátracích prostředků v rozporu s trestním řádem (§ 158b odst. 3 TŘ a contrario) apod.

II.6 Rozdělení důkazů

Teorie trestního práva procesního *dělí důkazy* podle různých kritérií:

a) podle vztahu k předmětu obvinění, a to na usvědčující a vyviňující (ospravedlňující),
b) podle vztahu pramene zpráv o dokazované skutečnosti k této skutečnosti, a to na původní (bezprostřední) a odvozené (prostředečné),
c) podle vztahu k dokazované skutečnosti (tedy podle toho, jaký je jejich poměr k závěru, který z nich vyvozuje orgán činný v trestním řízení), a to na přímé a nepřímé.

Každý důkaz z jedné z uvedených skupin může být zároveň kterýmkoli důkazem z hlediska jiného kritéria. Tak např. výpověď svědka o tom, že se mu těžce zraněná osoba A krátce před svou smrtí svěřila s tím, že jí zranění způsobila osoba B bodnutím nožem, je důkazem přímým, ale odvozeným. Zakrvácený nůž s otisky prstů osoby B nalezený na místě, kde došlo ke zranění osoby A, je důkazem nepřímým, ale původním.

82 Srov. nález Ústavního soudu sp. zn. III. ÚS 183/03, N 175/38 SbNU 399 a rozsudek Nejvyššího soudu sp. zn. 4 Tz 100/2006.

83 Viz usnesení Krajského soudu v Českých Budějovicích sp. zn. 4 To 354/94, č. 33/1995 Sb. tr. rozh.

84 Srov. rozsudek Vrchního soudu v Praze sp. zn. 2 To 73/2000, č. 55/2001 Sb. tr. rozh. a nález Ústavního soudu sp. zn. I. ÚS 3038/07, N 46/48 SbNU 549.

II.6.1 Důkazy usvědčující a vyviňující

Důkazy *usvědčující* prokazují okolnosti, které potvrzují obvinění, zejména spáchání stíhaného skutku obviněným, a svědčí tedy proti obviněnému. Důkazy *vyviňující* (ospravedlňující) potvrzují okolnosti, které vyvracejí obvinění, svědčí tedy ve prospěch obviněného, ať již ho zbavují viny úplně, nebo obvinění jen zeslabují. Toto dělení má význam pro správné vymezení rozsahu dokazování, protože orgány činné v trestním řízení jsou povinny bez návrhů stran stejně pečlivě *objasňovat okolnosti svědčící ve prospěch i v neprospěch obviněného* (§ 2 odst. 5, § 164 odst. 3 TŘ). V řízení před soudem pak státní zástupce zpravidla provádí důkazy podporující obžalobu (§ 180 odst. 3 TŘ), tj. důkazy usvědčující. Není přitom vyloučeno, že některý důkaz může současně obsahovat údaje usvědčující i údaje svědčící ve prospěch obviněného nebo že v průběhu trestního řízení se charakter důkazu usvědčujícího změní na ospravedlňující a opačně. Další význam uvedeného dělení vyplývá z toho, že podle čl. 6 odst. 3 písm. d) EÚLP má obviněný v rámci práva na spravedlivé soudní řízení též právo vyslýchat nebo dát vyslýchat svědky proti sobě a dosáhnout předvolání a výslechu svědků ve svůj prospěch za stejných podmínek jako svědků proti sobě.

Rozlišení usvědčujících a vyviňujících důkazů je důležité i vzhledem ke skutečnosti, že *obviněný nesmí být jakkoli donucován* (např. i hrozbou uložení pořádkové pokuty podle § 66 odst. 1 TŘ), aby aktivně poskytl (např. vydáním věci podle § 78 TŘ) orgánům činným v trestním řízení důkaz, resp. důkazní prostředek, *který ho usvědčuje* ze spáchání trestného činu, tj. platí zákaz nutit obviněného k sebeobviňování.[85] Není ovšem vyloučeno donucovat obviněného k tomu, aby pasivně strpěl opatření určitého usvědčujícího důkazu proti němu, resp. takový důkaz lze opatřit i přes odmítavý postoj obviněného (např. odnětím věci podle § 79 TŘ, sejmutím srovnávacího vzorku pachu podle § 114 odst. 2, 4 TŘ).

85 Viz zejména nález Ústavního soudu sp. zn. Pl. ÚS 29/2000, N 32/21 SbNU 285, nález Ústavního soudu sp. zn. II. ÚS 118/01, N 13/29 SbNU 101, nález Ústavního soudu sp. zn. I. ÚS 431/04, N 31/36 SbNU 347, nález Ústavního soudu sp. zn. II. ÚS 255/05, N 128/37 SbNU 623, nález Ústavního soudu sp. zn. I. ÚS 402/05, N 206/39 SbNU 185, nález Ústavního soudu sp. zn. II. ÚS 552/05, N 12/40 SbNU 103, nález Ústavního soudu sp. zn. I. ÚS 671/05, N 41/40 SbNU 341, nález Ústavního soudu III. ÚS 451/04, N 68/40 SbNU 677, nález Ústavního soudu sp. zn. III. 644/05, N 71/40 SbNU 697, stanovisko pléna Ústavního soudu sp. zn. Pl. ÚS-st. 30/10, ST 30/59 SbNU 595 (č. 439/2010 Sb.) a nález Ústavního soudu sp. zn. II. ÚS 2369/08, N 244/59 SbNU 489.

II.6.2 Důkazy původní a odvozené

Důkaz je *původním,* jestliže poznatek orgánu činného v trestním řízení je čerpán z přímého, bezprostředního pramene dokazované skutečnosti (např. výpověď svědka, který sám viděl událost, o které vypovídá, originál listiny). *Odvozený* důkaz znamená, že poznatek o dokazované skutečnosti je čerpán z pramene prostředečného, odvozeného (např. výpověď svědka, který slyšel vyprávět o předmětné události, opis listiny). Jde v podstatě o dělení podle toho, zda je či není zprostředkující nositel informací mezi původním pramenem zpráv o dokazované události, který byl v bezprostředním kontaktu s touto událostí, a orgánem činným v trestním řízení, který provádí dokazování a tím získává potřebné poznatky o dokazovaných skutečnostech.

Zásada bezprostřednosti (§ 2 odst. 12 TŘ) vyžaduje, aby orgány činné v trestním řízení použily k dokazování v první řadě důkazů původních, protože každý zprostředkující článek přináší riziko oslabení informační hodnoty důkazu (např. u svědků zapomenutí, zkreslení, nepochopení apod.). Odvozeného důkazu je nutno především použít ke zjištění a provedení důkazu původního, ke zjištění bezprostředního pramene dokazované skutečnosti (viz též § 101 odst. 2 věta třetí TŘ). Dále může být odvozenými důkazy prověřována věrohodnost důkazů původních (např. srovnáním listiny považované za její originál s ověřeným opisem této listiny, srovnáním obsahu svědecké výpovědi s tím, co o stejné události svědek uváděl jiným osobám, s nimiž se stýkal).

K dokazování skutečnosti důležité pro trestní řízení *lze použít i odvozeného* důkazu, zejména v případech, kdy původní důkaz již neexistuje nebo jej nelze opatřit (např. svědek, který přímo pozoroval událost, před výslechem zemřel nebo se natrvalo odstěhoval na neznámé místo do ciziny). Použití odvozených důkazů bude ovšem obtížnější a musí se projevit v pečlivém hodnocení takových důkazů. V souvislosti s tím bude zpravidla nezbytné zjistit i původní pramen důkazu a jeho kvalitu, protože na tom závisí hodnověrnost odvozeného důkazu.

II.6.3 Důkazy přímé a nepřímé

Přímým důkazem je takový, jenž umožňuje učinit přímý poznatek o dokazované skutečnosti, tj. o tom, zda se stala, popřípadě existuje, nebo se nestala či neexistuje. Přímý důkaz tedy přímo potvrzuje nebo vyvrací dokazovanou

skutečnost (např. výpověď svědka, který na vlastní oči viděl, jak obviněný vystřelil z pistole a tím smrtelně zranil poškozeného, přímo prokazuje skutečnost, že obviněný zastřelil poškozeného).

Důkaz *nepřímý* potvrzuje nebo vyvrací existenci určité dokazované skutečnosti pomocí skutečnosti jiné, která souvisí s dokazovanou skutečností jen nepřímo (např. výpověď svědka o tom, že slyšel vyhrožovat obviněného, že zastřelí poškozeného, který byl skutečně nalezen mrtvý, svědčí o úmyslném usmrcení poškozeného obviněným jen nepřímo, protože nedokazuje, že obviněný poškozeného zavraždil, ale lze na to usuzovat z takové výpovědi svědka). Stupeň vzdálenosti nepřímého důkazu od dokazované skutečnosti může být různý. Dokazování nepřímými důkazy není zásadně vyloučeno, je ovšem obtížnější a složitější než dokazování přímými důkazy. Otázka, zda je určitý důkaz přímým, nebo nepřímým, záleží na jeho vztahu k dokazované skutečnosti. Není rozhodná z hlediska použitelnosti tohoto důkazu před soudem, a to ani v tom smyslu, že by mu soud přikládal vzhledem k vadnosti jeho provedení menší význam.[86]

Jeden nepřímý důkaz nestačí k prokázání dokazované skutečnosti. K tomu musí být k dispozici více nepřímých důkazů; nepřímý důkaz má svoji důkazní hodnotu pouze ve spojení s jinými (byť rovněž nepřímými) důkazy. Nepřímé důkazy přitom musí tvořit ve svém souhrnu *logickou, ničím nenarušenou a uzavřenou soustavu vzájemně se doplňujících a na sebe navazujících nepřímých důkazů,* které vcelku shodně a spolehlivě dokazují určitou skutečnost a které jsou v takovém příčinném vztahu k dokazované skutečnosti, že z nich je možno vyvodit jen jediný závěr a současně vyloučit možnost jiného závěru.[87] Nepřímé důkazy vedoucí sice k důvodnému podezření vůči obviněnému, nevylučující však reálnou možnost, že pachatelem trestného činu mohla být i jiná osoba, nejsou dostatečným podkladem pro uznání viny obviněného.[88] Nepřímým důkazem nemůže být skutečnost, která nesouvisí s dokazovanou skutečností. Souvislost mezi skutečností, která má sloužit

86 Srov. usnesení Vrchního soudu v Praze sp. zn. 11 To 46/94, č. 45/1994 Sb. tr. rozh.

87 Srov. rozsudek Nejvyššího soudu sp. zn. 7 Tz 11/68, č. 38/1968 Sb. tr. rozh. a rozsudek Nejvyššího soudu sp. zn. 7 Tz 84/69, č. 38/1970 Sb. tr. rozh.

88 Srov. rozsudek Nejvyššího soudu sp. zn. 7 Tz 84/69, č. 38/1970 Sb. tr. rozh., nález Ústavního soudu sp. zn. II. ÚS 418/99, N 116/19 SbNU 113, nález Ústavního soudu sp. zn. I. ÚS 3094/08, N 103/53 SbNU 293 a nález Ústavního soudu sp. zn. III. ÚS 722/09, N 2/56 SbNU 11.

jako nepřímý důkaz, a dokazovanou skutečností, tedy to, co je u přímých důkazů zřejmé, se musí u nepřímých důkazů zjišťovat, protože dojem o této souvislosti může být vyvolán i náhodou.

Nepřímé důkazy *nelze* bez dalšího považovat za horší, méně věrohodné nebo méně spolehlivé. *Význam* nepřímých důkazů je i v tom, že umožňují prověřit nebo doplnit důkazy přímé, získat další (i přímé) důkazy, stanovit zaměření důkazního řízení a výběr důkazních prostředků.

II.7 Fáze procesu dokazování

Proces dokazování lze rozdělit do několika fází, jimiž jsou zejména:

a) *vyhledávání* důkazů, které je záležitostí především orgánů činných v trestním řízení, protože platí zásada vyhledávací (§ 2 odst. 5 TŘ), strany ovšem mají právo navrhovat důkazy, samy je vyhledat a předložit, proto skutečnost, že důkaz nevyhledal nebo nevyžádal orgán činný v trestním řízení, ale učinila tak některá ze stran, není důvodem k odmítnutí takového důkazu (§ 89 odst. 2 TŘ). Proces vyhledávání důkazů, resp. pátrání po nich, často probíhá s využitím operativně pátracích prostředků, jejichž okruh a podmínky použití upravuje trestní řád v ustanoveních § 158b až § 158f; jejich doplňkem jsou pak ustanovení § 72 až § 77 PolČR o podpůrných operativně pátracích prostředcích, které mohou rovněž sloužit k vyhledání důkazů použitelných v trestním řízení;

b) *provádění a procesní zajištění* důkazů zahrnuje procesní úkony, jimiž si orgány činné v trestním řízení způsobem stanoveným zákonem opatřují z pramene důkazu zprávy o skutečnostech významných pro věc a tyto zachycují v příslušném protokolu (§ 55 a násl., § 95, § 103, § 108 odst. 1 věta druhá, § 113 odst. 2 TŘ) nebo též jinak, např. fotodokumentací, zvukovým záznamem, videozáznamem, záznamem prostřednictvím výpočetní techniky na nosič informací [§ 52a, § 111a, § 158 odst. 3 písm. f) TŘ]. Podrobnosti o provádění důkazů jednotlivými důkazními prostředky upravují zejména ustanovení § 90 až § 118, § 209 až § 215 TŘ. Uplatní se zde především zásady bezprostřednosti a ústnosti (§ 2 odst. 11 a 12 TŘ). V případě *elektronických důkazních prostředků* může přicházet v úvahu podle povahy věci kombinace různých způsobů provedení důkazu, např. přečtení písemného

posudku znalce nebo jeho výslech o výsledku zkoumání určitého nosiče informací, přečtení písemného záznamu o obsahu elektronických informací, přehrání zvukového a/nebo obrazového záznamu z nosiče informací atd.;

c) *prověrka* důkazů, jejímž účelem je zjistit kvalitu pramene zpráv, spolehlivost a bezpečnost těchto zpráv na základě analýzy každého jednotlivého důkazu a jeho srovnání s důkazy ostatními, např. ověření, zda svědek mohl skutečně vidět z místa, kde se nacházel, to, o čem vypovídal – zde se mohou uplatnit zvláštní způsoby dokazování v podobě vyšetřovacího pokusu, rekonstrukce a prověrky na místě podle § 104c až § 104e TŘ včetně zachycení jejich průběhu a výsledku prostřednictvím obrazových a zvukových záznamů (§ 55 odst. 3 TŘ). Prověřováním důkazů a jejich rozborem se zjišťují a odstraňují rozpory mezi jednotlivými důkazy a objasňuje se jejich vzájemná spojitost a vztah k okolnostem případu;

d) *hodnocení* důkazů je vyvrcholením procesu dokazování a jeho nejvýznamnější fází. Uplatní se při něm zejména *zásada volného hodnocení důkazů* (§ 2 odst. 6 TŘ), přičemž se zde prolíná hodnocení důkazů s jejich prověrkou. Provedené důkazy netvoří ještě skutková zjištění; úplnost dokazování vytváří jen nezbytný podklad pro další myšlenkovou činnost záležející ve zhodnocení těchto důkazů podle § 2 odst. 6 TŘ a vytvoření závěrů o tom, zda, jak a k jakému skutku došlo, která osoba a za jakých časových, místních a dalších okolností spáchala tento skutek. Teprve tyto závěry, které pak příslušný orgán činný v trestním řízení vyjádří ve výroku svého meritorního rozhodnutí v tzv. skutkové větě, tvoří skutkový stav zjištěný takovým rozhodnutím.[89] Podobně to platí o jiné dokazované skutečnosti, než je skutek. Předpokladem správného hodnocení důkazů je nezkreslená (nedeformovaná) reprodukce informací obsažených v provedených důkazech, které se promítnou do konečného úsudku orgánu činného v trestním řízení.[90] Hodnocení důkazů je tedy myšlenkovou činností orgánů činných v trestním řízení, kterou tyto orgány na základě provedené analýzy přisuzují získanému důkazu určitou hodnotu, pokud

89 Srov. přiměřeně rozsudek Nejvyššího soudu sp. zn. 2 Tzf 3/88, č. 49/1989 Sb. tr. rozh.

90 Viz nález Ústavního soudu sp. zn. III. ÚS 398/97, N 64/11 SbNU 125, nález Ústavního soudu sp. zn. I. ÚS 910/07, N 156/50 SbNU 389 a nález Ústavního soudu sp. zn. III. ÚS 1104/08, N 65/52 SbNU 635.

jde o jeho závažnost, zákonnost a pravdivost:

- *závažností* důkazu je jeho upotřebitelnost pro zjištění skutkového stavu, vypovídá tedy o tom, do jaké míry určitý důkaz vzhledem ke svému obsahu poskytuje přímé nebo nepřímé poznatky o předmětu důkazu;
- *zákonností* důkazu se rozumí zjištění, zda byl získán z pramene, který stanoví nebo připouští zákon, zda byl opatřen a proveden příslušným orgánem činným v trestním řízení nebo oprávněnou stranou řízení, zda se tak stalo v odpovídajícím stadiu tohoto řízení a takovým postupem, který je v souladu s právními předpisy, resp. není s nimi v rozporu;
- *pravdivost* důkazu vyjadřuje, které závažné okolnosti, o nichž důkaz podává zprávu, lze považovat za existující a dokázané v souladu se skutečností; míra pravdivosti důkazu určuje zároveň jeho *věrohodnost*.

Hodnocení důkazu určuje jeho *důkazní moc*. V rámci něj je třeba zhodnotit každý jednotlivý důkaz i jejich souhrn, a to volně podle vnitřního přesvědčení orgánu činného v trestním řízení, který provádí dokazování, založeného na pečlivém uvážení všech okolností případu (§ 2 odst. 6 TŘ). Hodnocení důkazů provádí nezávisle každý orgán činný v trestním řízení, před nímž právě probíhá řízení a dokazování.[91] Výsledkem hodnocení důkazů je stanovení skutkového podkladu pro rozhodnutí orgánu činného v trestním řízení nebo pro jeho jiný postup. Jde-li o rozhodnutí, projeví se hodnocení důkazů v jeho odůvodnění [viz § 125 odst. 1, § 134 odst. 2, § 177 písm. d) TŘ].[92]

---

91 K nezávislosti soudů při hodnocení důkazů viz stanovisko trestného kolégia Najvyššieho súdu sp. zn. Tpj 20/89, č. 3/1990 Sb. tr. rozh. a rozsudek Vrchního soudu v Praze sp. zn. 2 To 116/2009.

92 Srov. též nález Ústavního soudu sp. zn. III. ÚS 181/2000, N 175/20 SbNU 241, nález Ústavního soudu sp. zn. III. ÚS 463/2000, N 181/20 SbNU 267, nález Ústavního soudu sp. zn. III. ÚS 628/2000, N 67/22 SbNU 87, nález Ústavního soudu sp. zn. III. ÚS 532/01, N 10/25 SbNU 69, nález Ústavního soudu sp. zn. IV. ÚS 37/03, N 81/33 SbNU 285, nález Ústavního soudu sp. zn. III. ÚS 224/04, N 116/61 SbNU 695, nález Ústavního soudu sp. zn. I. ÚS 455/05, N 210/39 SbNU 239 a nález Ústavního soudu sp. zn. III. ÚS 1104/08, N 65/52 SbNU 635.

Samozřejmostí je pak požadavek na ústavní konformitu hodnocení.[93]

Jednotlivé fáze procesu dokazování nejsou od sebe odděleny, ale úzce spolu souvisí a vzájemně se prolínají, proto je nelze v průběhu trestního řízení formálně rozlišovat.

II.8 Důkazní iniciativa stran

II.8.1 Možnost stran vyhledat, předložit nebo navrhnout důkaz

Ustanovení § 89 odst. 2 TŘ umožňuje procesním stranám z vlastní iniciativy *vyhledávat a předkládat důkazy nebo navrhovat provedení* určitých důkazů. Pro jejich provedení, prověrku a hodnocení se ovšem uplatní stejné zásady a pravidla jako pro důkazy opatřené orgány činnými v trestním řízení. To mimo jiné znamená, že použitelnost (přípustnost) důkazu, resp. důkazního prostředku, který vyhledala a předložila některá z procesních stran, bude závislá na jeho povaze a na dodržení zákonných požadavků kladených na jeho vyhledání, opatření a provedení. Jestliže by důkaz vyhledaný a předložený stranou vykazoval v těchto směrech podstatné vady, nebyl by zásadně přípustný (účinný).

Trestní řád v ustanovení § 89 odst. 2 větě druhé nedává bližší směrnice k tomu, kdy bude přicházet v úvahu vyhledání, kdy předložení a kdy jen návrh na provedení důkazu. Proto bude nepochybně záležet na druhu důkazu (důkazního prostředku), který je opatřován aktivitou strany. Každá ze stran trestního řízení (k jejich okruhu viz § 12 odst. 6 TŘ) je tedy oprávněna především *vyhledat* důkazy, tj. pátrat po pramenech důkazů a identifikovat jejich nositele tak, aby poté bylo možné využít důkazní hodnotu vyhledaných důkazních prostředků v procesu dokazování. V tomto smyslu mohou

[93] K ústavně konformnímu hodnocení důkazů viz nález Ústavního soudu sp. zn. III. ÚS 398/97, N 64/11 SbNU 125, nález Ústavního soudu sp. zn. Pl. ÚS 15/98, N 48/13 SbNU 341, nález Ústavního soudu sp. zn. III. ÚS 258/99, N 148/16 SbNU 99, nález Ústavního soudu sp. zn. III. ÚS 464/99, N 109/19 SbNU 63, nález Ústavního soudu sp. zn. III. ÚS 181/2000, N 175/20 SbNU 241, nález Ústavního soudu sp. zn. III. ÚS 463/2000, N 181/20 SbNU 267, nález Ústavního soudu sp. zn. III. ÚS 532/01, N 10/25 SbNU 69, usnesení Ústavního soudu sp. zn. Iv. ÚS 154/02, U 37/28 SbNU 447, nález Ústavního soudu sp. zn. I. ÚS 455/05, N 210/39 SbNU 239, nález Ústavního soudu sp. zn. I. ÚS 864/11, N 116/61 SbNU 695, nález Ústavního soudu sp. zn. III. ÚS 1076/08, N 144/50 SbNU 269, nález Ústavního soudu sp. zn. I. ÚS 910/07, N 156/50 SbNU 389, nález Ústavního soudu sp. zn. III. ÚS 1104/08, N 65/52 SbNU 635 a nález Ústavního soudu sp. zn. I. ÚS 3094/08, N 103/53 SbNU 293.

strany např. zjišťovat, které fyzické osoby byly svědky určité události, jež je předmětem dokazování, a vyzvat je, aby se dostavily k podání svědectví, nebo sdělit jejich jména a bydliště orgánu činnému v trestním řízení za účelem předvolání. Dále jsou strany oprávněny pátrat, jaké listiny mohou potvrdit nebo vyvrátit dokazovanou skutečnost a kde se nacházejí, na kterých osobách nebo věcech jsou stopy po trestném činu atd. Umožňuje-li to povaha důkazního prostředku (nositele důkazu), může ho strana orgánu činnému v trestním řízení, který provádí dokazování, přímo *předložit*. To znamená např. předložení znaleckého posudku, předložení listiny osvědčující dokazovaný stav, předložení věci s patrnými následky trestného činu nebo jeho stopami, předložení obrazových, zvukových nebo jiných záznamů zachycujících dokazované skutečnosti[94] apod. V určitých případech přichází v úvahu jen *návrh* na opatření a provedení důkazu, třeba i vyhledaného některou z procesních stran, pokud procesní strana sama není oprávněna provést takový druh důkazu, ale může učinit např. návrh na výslech svědka, na provedení konfrontace, rekognice apod. Konečně nejdůležitější procesní strany, tj. státní zástupce a obžalovaný nebo jeho obhájce, mohou v řízení před soudem – je-li jim to u hlavního líčení k jejich žádosti umožněno – samy *provádět* některé důkazy, zejména vyslýchat svědka nebo znalce podle § 215 odst. 2 TŘ. Strany však *nemohou relevantně hodnotit důkazy,* tj. procesně účinným způsobem vyvozovat z důkazních prostředků přímé poznatky o dokazovaných skutečnostech a tím vytvářet skutkový základ potřebný pro rozhodnutí; to je činnost vyhrazená jen orgánům činným v trestním řízení.

Podle § 110a TŘ dále platí, že předloží-li strana *znalecký posudek*, který má všechny zákonem požadované náležitosti a obsahuje doložku znalce o tom, že si je vědom následků vědomě nepravdivého znaleckého posudku, postupuje se při provádění tohoto důkazu stejně, jako by šlo o znalecký posudek vyžádaný orgánem činným v trestním řízení. Orgán činný v trestním řízení umožní znalci, jehož některá ze stran požádala o znalecký posudek, nahlédnout do spisu nebo mu jinak umožní seznámit se s informacemi potřebnými pro vypracování znaleckého posudku. Znalecký posudek předložený stranou je tedy *zásadně rovnocenný* se znaleckým posudkem již opatřeným orgány činnými v trestním řízení, pokud byl takový posudek zpracován, anebo ho

94 Srov. usnesení Nejvyššího soudu sp. zn. 5 Tdo 459/2007, č. 7/2008 Sb. tr. rozh.

může nahradit, jestliže orgány činné v trestním řízení zatím nepřibraly znalce ke zpracování (jiného) znaleckého posudku. Strana však *není oprávněna* místo orgánů činných v trestním řízení procesně přípustným způsobem vyslýchat znalce, nejde-li o případ uvedený v § 215 odst. 2 TŘ, proto nemůže být důkazem předloženým stranou protokol o „výslechu" znalce stranou (resp. znalecký posudek nadiktovaný do protokolu). Předloží-li strana písemně podaný posudek znalce podle § 110a TŘ, neznamená to, že takový důkaz musí být vždy proveden, ale orgán činný v trestním řízení může o něm – stejně jako o jiném předloženém důkazu – rozhodnout, že je *nadbytečný* (viz § 166 odst. 1 věta pátá, odst. 3, § 216 odst. 1 TŘ)[95], a to např. z důvodu, že je v něm řešena výlučně jiná odborná otázka, než která je nezbytná pro rozhodnutí. Nadbytečnost provedení takového důkazu a jeho odmítnutí *nemůže však záležet* jen ve skutečnosti, že ve věci byl k posouzení otázek, pro jejichž objasnění je třeba odborných znalostí, již opatřen znalecký posudek orgány činnými v trestním řízení. I posudek znalce předložený některou ze stran lze případně přečíst u hlavního líčení za podmínek § 211 odst. 5 TŘ, nebude-li nutný osobní výslech takového znalce (§ 108 TŘ). Předloží-li strana posudek znalce, nutno rovněž zjišťovat (stejně jako v případě, když je znalec přibrán orgánem činným v trestním řízení), zda není znalec v této věci vyloučen ve smyslu § 111 TŘ a § 11 ZnalZ.[96]

K posílení aktivity stran, zejména obviněného a poškozeného, v souvislosti s možností opatření znaleckého posudku pak směřuje též ustanovení § 151a TŘ, podle něhož lze požádat o to, aby v určitých případech *stát nesl náklady na znalecký posudek,* který vyžádá obviněný nebo poškozený.

Při vyhledávání a předkládání *jiných důkazních prostředků* (listiny, fotodokumentace, obrazové a zvukové záznamy, věcné důkazy, elektronické důkazy atd.) pak neplatí žádná zvláštní omezení a strany mohou samy tyto důkazy (důkazní prostředky) vyhledat, opatřit a předložit orgánům činným v trestním řízení, ovšem při respektování ochrany lidských práv a svobod. Tak např. obviněný nebo jeho obhájce nemůže svévolně vniknout do chráněného obydlí jiné osoby za účelem získání věcného důkazu, který by

95 K tomu srov. též usnesení Krajského soudu v Českých Budějovicích sp. zn. 4 To 475/94, č. 3/1996 Sb. tr. rozh.

96 Srov. rozsudok Najvyššieho súdu sp. zn. 4 Tz 98/76, č. 11/1977 Sb. tr. rozh. a rozsudek Nejvyššího soudu sp. zn. 5 Tz 63/2001, č. 4/2002 Sb. tr. rozh.

se tam mohl nacházet, ale k tomu je možné jen navrhnout využití institutu domovní prohlídky podle § 82 a § 83 TŘ, provedené příslušným orgánem činným v trestním řízení.

II.8.2 Zákaz odmítnout důkaz jen proto, že je výsledkem důkazní iniciativy strany

Důsledkem výše uvedené důkazní iniciativy stran je podle § 89 odst. 2 věty třetí TŘ, že *důvodem k odmítnutí důkazu není skutečnost, že ho nevyhledal nebo nevyžádal orgán činný v trestním řízení.* Orgán činný v trestním řízení tedy musí akceptovat důkaz vyhledaný, předložený nebo navržený některou ze stran. Rozhodnutí o tom, že odmítá provedení takového důkazu, však musí být opřeno výlučně *o jiné důvody*, které nespočívají jen v tom, kdo důkaz vyhledal nebo vyžádal. Neprovedení důkazu předloženého nebo navrženého některou ze stran proto může být odůvodněno např. tím, že jde o důkaz, který nemá vztah k projednávané věci (neprokazuje ani nevyvrací dokazované skutečnosti), jde o důkaz zatížený podstatnou vadou, pro kterou ho nelze provést nebo z něj vyvozovat skutkové závěry (např. znalecký posudek zpracoval podjatý znalec),[97] důkaz má potvrzovat tutéž skutečnost, k jaké již byl proveden jiný důkaz vyhledaný, předložený nebo navržený stejnou stranou, takže je nadbytečný apod.

Možnost obviněného předkládat důkazy opatřené vlastním přičiněním je důležitým prostředkem k reálnému zajištění jeho *práva na obhajobu* [viz čl. 6 odst. 3 písm. d) EÚLP], směřuje k posílení aktivity obviněného v trestním řízení a úzce souvisí s tzv. materiálním důkazním břemenem stran v tomto řízení.[98] Proto zejména soud nesmí nechat bez povšimnutí důkazní návrhy stran, a i když *neprovede* důkazy jimi vyhledané, předložené nebo navržené, musí o tom rozhodnout a s neakceptovanými návrhy stran a s jimi nabízenými důkazními prostředky se musí ve svém rozhodnutí *vypořádat a náležitě*

97 Viz rozsudek Nejvyššího soudu sp. zn. 5 Tz 63/2001, č. 4/2002 Sb. tr. rozh.

98 K tzv. materiálnímu důkaznímu břemenu viz podrobněji v publikaci Šámal, 2013a, op. cit., s. 1314.

odůvodnit, proč jim nevyhověl.[99] Důkazy vyhledané, předložené nebo navržené některou ze stran pak nestačí jen provést, ale je třeba je odpovídajícím způsobem logicky a přesvědčivě *vyhodnotit* (§ 2 odst. 6 TŘ) a soud musí své hodnotící úvahy uvést do odůvodnění rozhodnutí tak, aby bylo i z tohoto hlediska přezkoumatelné.[100] Právní úprava vyšetřování i řízení před soudem přitom nezná institut předběžného posuzování (hodnocení) důkazů, a proto není v pravomoci kteréhokoli orgánu činného v trestním řízení provádět podle vlastních kritérií předběžnou selekci (nabízených) důkazů a upravovat tak důkazní situaci podle vlastní úvahy a volby, případně z daných důkazů a priori preferovat ty, které potvrzují zvolenou skutkovou verzi.[101] Podle judikatury Ústavního soudu pak *neakceptování důkazního návrhu* obviněného lze založit toliko *třemi důvody*: prvním je argument, podle něhož tvrzená skutečnost, k jejímuž ověření nebo vyvrácení je navrhován důkaz, *nemá relevantní souvislost* s předmětem řízení. Dalším je argument, podle kterého důkaz není s to ani ověřit, ani vyvrátit tvrzenou skutečnost, čili ve vazbě na toto tvrzení *nedisponuje vypovídací potencí*. Konečně třetím je pak *nadbytečnost* důkazu, tj. argument, podle kterého určité tvrzení, k jehož ověření nebo vyvrácení je důkaz navrhován, bylo již v dosavadním řízení bez důvodných pochybností (s praktickou jistotou) ověřeno nebo vyvráceno.[102]

99 Srov. nález Ústavního soudu sp. zn. III. ÚS 51/96, N 57/8 SbNU 69, nález Ústavního soudu sp. zn. I. ÚS 425/97, N 42/13 SbNU 305, nález Ústavního soudu sp. zn. III. ÚS 258/99, N 148/16 SbNU 99, nález Ústavního soudu sp. zn. II. ÚS 441/99, N 48/17 SbNU 337, nález Ústavního soudu III. ÚS 464/99, N 109/19 SbNU 63, nález Ústavního soudu sp. zn. I. ÚS 459/2000, N 89/27 SbNU 51, nález Ústavního soudu sp. zn. I. ÚS 660/03, N 24/32 SbNU 219, nález Ústavního soudu sp. zn. IV. ÚS 802/02, N 58/33 SbNU 89, nález Ústavního soudu sp. zn. IV. ÚS 570/03, N 91/33 SbNU 377, nález Ústavního soudu sp. zn. I. ÚS 566/03, N 104/34 SbNU 99, usnesení Ústavního soudu sp. zn. I. ÚS 152/05, U 18/38 SbNU 541, nález Ústavního soudu sp. zn. I. ÚS 2343, N 67/52 SbNU 663 a nález Ústavního soudu sp. zn. III. ÚS 332/09, N 60/56 SbNU 643.

100 Srov. nález Ústavního soudu sp. zn. III. ÚS 95/97, N 76/8 SbNU 231, usnesení Ústavního soudu sp. zn. I. ÚS 484/97, U 7/10 SbNU 361, nález Ústavního soudu sp. zn. III. ÚS 181/2000, N 175/20 SbNU 241, nález Ústavního soudu sp. zn. III. ÚS 463/2000, N 181/20 SbNU 267, nález Ústavního soudu sp. zn. III. ÚS 628/2000, N 67/22 SbNU 87, nález Ústavního soudu sp. zn. III. ÚS 532/01, N 10/25 SbNU 69 a nález Ústavního soudu sp. zn. III. ÚS 1104/08, N 65/52 SbNU 635.

101 Viz nález Ústavního soudu sp. zn. III. ÚS 617/2000, N 143/24 SbNU 27.

102 Viz nález Ústavního soudu sp. zn. I. ÚS 733/01, N 26/32 SbNU 239.

II.9 Některé procesní úkony směřující k opatření elektronických důkazů

II.9.1 Obecně k problematice elektronických důkazů

Český trestní řád *nezná pojem elektronický důkaz*, resp. důkazní prostředek a ani neobsahuje žádné specifické procesní postupy či instituty, které by byly zaměřeny na zvláštnosti při opatřování elektronických důkazů. S možnostmi *využití elektronických dokumentů* však trestní řád na některých místech a v určitých případech výslovně počítá, např. jde-li o podání učiněné elektronicky (§ 59 odst. 1, 2 TŘ), o listiny, které obsahují skutečnosti, na něž se vztahuje povinnost mlčenlivosti advokáta, a kteréžto listiny podléhají zvláštní ochraně při provádění domovní prohlídky nebo prohlídky jiných prostor, v nichž advokát vykonává advokacii (§ 85b odst. 12 TŘ) apod. *Elektronickou povahu* některých opatřených či zafixovaných údajů je třeba předpokládat též např. při využití videokonferenčního zařízení při provádění určitých úkonů trestního řízení (§ 52a, § 111a TŘ), při pořizování obrazového a/nebo zvukového záznamu o prováděném úkonu trestního řízení jako zvláštního způsobu protokolace (§ 55a, § 55b TŘ), při odposlechu a záznamu telekomunikačního provozu (§ 88 TŘ), při vyžádání údajů o uskutečněném telekomunikačním provozu (§ 88a TŘ), v případě pořizování zvukových, obrazových a jiných záznamů získaných při použití operativně pátracích prostředků (§ 158b odst. 3 TŘ) atd., byť se v těchto případech mnohdy vyhotovuje i písemný protokol. Počítá se rovněž s doručováním do datové schránky (§ 62 odst. 1 věta první TŘ), což předpokládá existenci „písemnosti" v elektronické podobě, resp. její konverzi z listinné do této podoby, přičemž důkazem o takovém doručení jsou výstupy z elektronického systému datových schránek.

Pokud jde o *procesní postupy či instituty*, kterými lze opatřit elektronické důkazy (důkazní prostředky), v úvahu přichází některé z nich upravené příslušnými ustanoveními trestního řádu, popřípadě i jejich kombinace. Jde zejména o zajišťovací instituty v podobě vydání a odnětí věci (§ 78, § 79 TŘ), domovní prohlídky, prohlídky prostor nesloužících k bydlení a pozemků a osobní prohlídky (§ 82 až § 85b TŘ), o odposlech a záznam telekomunikačního provozu (§ 88 TŘ) včetně přeshraničního odposlechu (§ 64 ZMJS)

a vyžádání údajů o uskutečněném telekomunikačním provozu (§ 88a TŘ), dále jde o ohledání (§ 113 TŘ) nebo o využití posudku znalce či o odborné vyjádření (§ 105 až § 111 TŘ).

II.9.2 Vydání a odnětí věci

Jde o vydání nebo odnětí hmotné věci důležité pro trestní řízení, což jsou zajišťovací úkony ve vztahu k tzv. *doličné věci*. Považuje se za ni předmět, který by mohl být věcným důkazním prostředkem (§ 112 odst. 1 TŘ), listina, která může být listinným důkazem (§ 112 odst. 2 TŘ), s výjimkou některých listin uvedených v § 78 odst. 2 TŘ, a věc, ohledně které může být uložen trest propadnutí věci (§ 70 až § 72 TZ) nebo vysloveno zabrání věci (§ 101 TZ). Každý, kdo má u sebe takovou doličnou věc, je *povinen ji na vyzvání předložit* orgánu činnému v trestním řízení, a je-li ji nutno pro účely trestního řízení zajistit, je povinen ji na výzvu tomuto orgánu *vydat* (§ 78 TŘ). Tuto povinnost má *kdokoli*, nejen tedy obviněný, a nevyhoví-li této výzvě, může mu být hmotná věc odňata (§ 79 TŘ). Výzva k vydání hmotné věci důležité pro trestní řízení je opatřením a nemusí být učiněna písemně. Pokud povinný nevyhověl výzvě, lze ho k tomu nutit uložením pořádkové pokuty (§ 66 odst. 1 TŘ) anebo může příslušný orgán činný v trestním řízení (policejní orgán zpravidla potřebuje předchozí souhlas státního zástupce) dát příkaz, aby hmotná věc byla odňata. U obviněného se ovšem uplatní *zákaz sebeobviňování*, takže ho nelze nutit např. pořádkovou pokutou, aby aktivně poskytoval usvědčující důkazy proti sobě, a tedy ani k tomu, aby vydal doličnou věc, kterou má u sebe. Proto v případě, když obviněný dobrovolně nevydá doličnou věc, i bez předchozího uložení pořádkové pokuty je možné mu ji odejmout, což je povinen strpět (viz výše v kapitole II.6.1).

O vydání a odnětí hmotné věci se sepíše protokol (§ 55 odst. 1 TŘ), který musí obsahovat též dostatečně přesný popis této věci, aby umožnil určit její totožnost (§ 79 odst. 5 TŘ). Osobě, která vydala doličnou věc nebo které byla tato věc odňata, se o tom vydá písemné potvrzení nebo opis protokolu (§ 79 odst. 6 TŘ). Dokazování za použití doličné věci se provádí *předložením listin a jiných věcných důkazů stranám, svědkům a znalcům*, přičemž k návrhu strany soud přečte listiny (§ 213 TŘ), nebo se důkaz provádí též *ohledáním věci*, k němuž se zpravidla *přibere znalec* (§ 113 TŘ). Není-li již třeba vydané nebo odňaté věci k dalšímu řízení a nepřichází-li v úvahu její propadnutí nebo

zabrání, vrátí se tomu, kdo ji vydal, komu byla odňata nebo kdo na ni uplatnil právo. V případě pochybností se uloží do úschovy a za určitých okolností ji lze prodat (§ 80 odst. 1, 2 TŘ). Trestní řád dále upravuje nakládání s věcí, která byla získána nebo pravděpodobně získána trestným činem (§ 81 TŘ).

V souvislosti s elektronickými důkazy přichází v úvahu vydání a odnětí takových věcí, které mohou být nositeli různých informací a dat považovaných za elektronické důkazy. Jde zejména o počítače všech typů a provedení, tablety, mobilní telefony, ale též o samostatné nosiče elektronických informací v podobě externích pevných disků, USB paměťových prvků (tzv. flash disků), paměťových karet atd.

Pro úplnost je třeba ještě dodat, že trestní řád počítá i se *zajištěním nehmotné věci* podle § 79e TŘ.

II.9.3 Domovní prohlídka, prohlídka prostor nesloužících k bydlení a pozemků a osobní prohlídka

Jde o procesní instituty, které rovněž patří mezi *zajišťovací úkony*. Za splnění všech zákonných podmínek se jimi přípustným způsobem zasahuje do nedotknutelnosti obydlí a jiných prostor a do osobní svobody (čl. 12 odst. 2 LZPS, čl. 8 EÚLP). *Domovní prohlídka*, prohlídka *jiných prostor nesloužících k bydlení a pozemků* a *osobní prohlídka* jsou úkony trestního řízení, které směřují k zajištění osob a věcí v trestním řízení. Lze je vykonat, je-li důvodné podezření, že v bytě nebo jiné prostoře sloužící k bydlení nebo v prostorách nesloužících k bydlení nebo na pozemcích, které nejsou veřejně přístupné, *je osoba nebo věc důležitá pro trestní řízení* (§ 82 odst. 1, 2 TŘ), resp. že někdo má u sebe věc důležitou pro trestní řízení (§ 82 odst. 3 TŘ). Domovní prohlídku a prohlídku jiných prostor a pozemků je oprávněn nařídit jen předseda senátu a v přípravném řízení na návrh státního zástupce soudce. *Příkaz* musí být vydán písemně a musí být odůvodněn. Doručí se uživateli obydlí nebo dotčených prostor nebo pozemků, a nebyl-li zastižen při prohlídce, bezprostředně po odpadnutí překážky, která doručení brání (§ 83a odst. 1 TŘ). Osobní prohlídku je oprávněn nařídit předseda senátu a v přípravném řízení státní zástupce nebo s jeho souhlasem policejní orgán (§ 83b odst. 1 TŘ). Za určitých okolností může policejní orgán vykonat osobní prohlídku i bez příkazu nebo souhlasu (§ 83b odst. 4 TŘ).

Další podmínky provedení těchto prohlídek upravují ustanovení § 84 až § 85b TŘ. Osoba, u níž má být provedena taková prohlídka, je povinna strpět tento úkon, a neumožní-li jeho provedení, lze její odpor nebo vytvořenou překážku překonat (§ 85a TŘ). Do obydlí, do jiných (nebytových) prostor nebo na pozemek může policejní orgán mimo výkonu prohlídky též vstoupit v nezbytných případech (§ 83c TŘ) anebo lze na těchto místech provést rekonstrukci, rekognici, prověrku na místě nebo vyšetřovací pokus (§ 85c TŘ).

Při provádění domovní prohlídky nebo prohlídky jiných prostor, *v nichž advokát vykonává advokacii*, pokud se zde mohou nacházet listiny, které obsahují skutečnosti, na něž se vztahuje povinnost mlčenlivosti advokáta, je orgán provádějící tento úkon povinen vyžádat si součinnost České advokátní komory; orgán provádějící úkon je oprávněn seznámit se s obsahem těchto listin pouze za přítomnosti a se souhlasem zástupce České advokátní komory, kterého ustanoví její předseda z řad jejích zaměstnanců nebo z řad advokátů. Odmítne-li zástupce České advokátní komory udělit potřebný souhlas, musí být listiny za účasti orgánu provádějícího úkon, advokáta a zástupce České advokátní komory zabezpečeny tak, aby se s jejich obsahem nemohl nikdo seznámit, popřípadě je zničit nebo poškodit; bezprostředně poté musí být příslušné listiny předány České advokátní komoře. V případě odmítnutí souhlasu zástupce České advokátní komory lze tento souhlas nahradit na návrh orgánu, který nařídil domovní prohlídku nebo prohlídku jiných prostor, rozhodnutím soudce nejblíže nadřízeného soudu, u něhož působí předseda senátu nebo soudce, který je oprávněn podle § 83 odst. 1 a § 83a odst. 1 TŘ nařídit domovní prohlídku nebo prohlídku jiných prostor. Další podrobnosti stanoví § 85b TŘ.[103]

Nařízení a provedení domovní prohlídky a prohlídky jiných prostor nesloužících k bydlení může být mnohdy nezbytné i k opatření *elektronických důkazů*, jestliže je důvodný předpoklad, že se zde nacházejí nositelé takových důkazů v podobě počítačů různých druhů, prvky počítačových sítí, tablety, mobilní telefony, paměťové disky a karty atd. Totéž přiměřeně platí o osobní prohlídce, která přichází v úvahu, pokud lze důvodně předpokládat, že určitý nosič elektronického důkazu má u sebe nějaká osoba, která ho na výzvu dobrovolně nevydá.

103 Viz také Stanovisko trestního kolegia Nejvyššího soudu sp. zn. Tpjn 306/2014, č. 35/2015 Sb. tr. rozh.

II.9.4 Odposlech a záznam telekomunikačního provozu, vyžádání údajů o uskutečněném telekomunikačním provozu

Odposlech a záznam telekomunikačního provozu je dalším z úkonů směřujících k zajištění osob a věcí v trestním řízení. Může ho nařídit soud písemným a odůvodněným příkazem, je-li vedeno trestní řízení pro zločin, na který zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně 8 let, dále pro některý z trestných činů vyjmenovaných v § 88 odst. 1 TŘ nebo pro jiný úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva, pokud lze důvodně předpokládat, že v telekomunikačním provozu budou sděleny významné skutečnosti pro trestní řízení (§ 88 odst. 1, 2 TŘ). Odposlech a záznam telekomunikačního provozu provádí pro potřeby všech orgánů činných v trestním řízení Policie České republiky. Není přípustný mezi obhájcem a obviněným, jinak může být odposlouchávanou osobou obviněný nebo kterákoliv jiná osoba. Jeho provádění je časově omezeno dobou 4 měsíců, která však může být i opakovaně prodloužena. *Bez příkazu* soudu lze provádět odposlech a záznam telekomunikačního provozu se souhlasem účastníka odposlouchávané stanice, je-li vedeno trestní řízení pro trestné činy vyjmenované v § 88 odst. 5 TŘ (např. trestné činy obchodování s lidmi podle § 168 TZ, vydírání podle § 175 TZ nebo násilí proti skupině obyvatel a proti jednotlivci podle § 352 TZ). Záznam telekomunikačního provozu *lze použít jako důkazní prostředek* jen za předpokladu, že je k němu připojen protokol s uvedením údajů o místě, čase, způsobu a obsahu provedeného záznamu, jakož i o orgánu, který pořídil tento záznam. Za určitých okolností lze takový záznam použít k důkazu i v jiné trestní věci, než v které byl pořízen. Výsledky odposlechu a záznamu telekomunikačního provozu lze použít k důkazu jen tehdy, je-li prováděn podle trestního řádu, nikoli podle jiných zákonů.[104]

Po pravomocném skončení trestní věci státní zástupce nebo předseda senátu soudu prvního stupně podle § 88 odst. 8 TŘ *informuje* osobu, která je uživatelem odposlouchávaného zařízení, o nařízeném odposlechu a záznamu telekomunikačního provozu, nejde-li o výjimky uvedené v § 88 odst. 9 TŘ. Tato osoba může podat do 6 měsíců *návrh k Nejvyššímu soudu na přezkoumání zákonnosti* příkazu k odposlechu a záznamu telekomunikačního provozu,

104 Viz k tomu též nález Ústavního soudu sp. zn. I. ÚS 3038/07, N 46/48 SbNU 549.

přičemž Nejvyšší soud v řízení podle § 314l až § 314n TŘ usnesením buď vysloví, že zákon byl porušen, nebo vysloví, že zákon porušen nebyl; proti tomuto rozhodnutí není přípustný opravný prostředek.

Kromě odposlechu a záznamu telekomunikačního provozu lze v trestním řízení využít *příkaz ke zjištění údajů o telekomunikačním provozu* za podmínek § 88a TŘ, je-li k objasnění skutečností důležitých pro trestní řízení třeba zjistit údaje o uskutečněném telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat; tohoto příkazu není třeba v případě souhlasu uživatele telekomunikačního zařízení. Pokud jde o vydání příkazu a přezkoumání jeho zákonnosti, platí zde obdobný režim jako v případě odposlechu a záznamu telekomunikačního provozu.

II.9.5 Ohledání

Ohledání je jedním z důkazních prostředků. Konají ho orgány činné v trestním řízení, mají-li být přímým smyslovým pozorováním objasněny skutečnosti důležité pro trestní řízení. *Předmětem ohledání* může být jednak *fyzická osoba*, tj. obviněný, poškozený, jiný svědek, a jednak *věc* včetně místa činu, stop trestného činu a listin. Při zajišťování věci pro účely ohledání lze rozhodnout o povinnosti k předložení či vydání věci nebo o odnětí věci podle § 78 a § 79 TŘ, a to případně i pod sankcí pořádkové pokuty nebo jiného opatření podle § 66 TŘ. K ohledání se zpravidla přibere *znalec* a mohou být přibrány i jiné osoby, např. obviněný, poškozený nebo další svědci, zejména je-li třeba ověřit jejich údaje. O průběhu ohledání se sepíše protokol (§ 55 odst. 1 TŘ), který musí poskytovat úplný a věrný obraz předmětu ohledání, proto se k němu mají přiložit fotografie, náčrty a jiné pomůcky (§ 113 odst. 2 TŘ).

V souvislosti s *elektronickými důkazy* mohou být předmětem ohledání zejména věci, které jsou potenciálními nositeli takových důkazů, resp. důkazně významných informací a dat, a to v podobě počítačů různých druhů, prvků počítačových sítí, tabletů, mobilních telefonů, paměťových disků a karet atd.

II.9.6 Znalec

Znalec v trestním řízení je osoba rozdílná od procesních stran i od orgánů činných v trestním řízení, která má v trestním řízení v procesu

dokazování na podkladě svých *odborných znalostí* objasnit určitou skutečnost důležitou pro trestní řízení, jejíž objasnění vyžaduje takové odborné znalosti, např. z oboru zdravotnictví, psychologie, chemie, dopravy, ekonomiky, výpočetní techniky a informačních technologií atd. (§ 105 odst. 1 TŘ). O přibrání znalce lze rozhodnout teprve tehdy, nepostačí-li k objasnění skutečnosti důležité pro trestní řízení, která vyžaduje odborné znalosti, podání *odborného vyjádření*. O odborné vyjádření lze požádat i osobu, která je podle zvláštního zákona zapsána v seznamu znalců, a fyzickou nebo právnickou osobu, která má potřebné odborné předpoklady (§ 105 odst. 5 TŘ).

Výsledkem činnosti znalce je jeho *znalecký posudek*, který je jedním z důkazních prostředků a jímž znalec dává odpověď na objasňované odborné otázky, které mu zadal příslušný orgán činný v trestním řízení podle § 107 odst. 1 TŘ, popřípadě procesní strana podle § 110a TŘ. Znalec je zpravidla přibírán opatřením orgánu činného v trestním řízení, ale není vyloučeno předložení znaleckého posudku procesní stranou (§ 89 odst. 2, § 110a TŘ). Znalec musí být před podáním posudku poučen orgánem činným v trestním řízení podle § 106 TŘ. Jako znalec může vystupovat jen osoba zapsaná pro příslušný obor, popřípadě odvětví v seznamu znalců vedeném krajskými soudy a Ministerstvem spravedlnosti; jen výjimečně lze za splnění určitých podmínek ustanovit znalce nezapsaného do seznamu znalců. Překážkou účasti znalce jsou tytéž důvody, které brání výslechu svědka (§ 99 a § 100 TŘ), nebo podjatost znalce. Proti osobě znalce lze vznést námitky z důvodů, které stanoví zvláštní zákon, jímž je zákon č. 36/1967 Sb., o znalcích a tlumočnících, ve znění pozdějších předpisů (zejména pro podjatost). Vedle toho lze vznést námitky proti odbornému zaměření znalce nebo proti formulaci otázek položených znalci. Podrobnosti o řešení takových námitek stanoví § 105 odst. 3 TŘ.

Ve výjimečných, zvlášť obtížných případech, vyžadujících zvláštního vědeckého posouzení, se jako znalec přibírá *státní orgán, vědecký ústav, vysoká škola nebo instituce specializovaná na znaleckou činnost* (§ 110 TŘ). I tyto ústavy a instituce jsou zapsané v seznamu znalců vedeném Ministerstvem spravedlnosti. Zásadně postačí ustanovit jednoho znalce, nevyžaduje-li zákon dva znalce, jak je tomu např. podle § 105 odst. 4 TŘ při prohlídce a pitvě mrtvoly (§ 115 TŘ) nebo podle § 58 odst. 1 ZSM při vyšetření duševního stavu mladistvého v trestním řízení.

Znalec podává posudek pouze *o otázkách skutkových*, a to jen ve své odbornosti; není oprávněn řešit právní otázky ani provádět a hodnotit důkazy (§ 107 odst. 1 TŘ). Posudek znalce se skládá z nálezu (popis zkoumaného materiálu, popřípadě jevů, souhrn skutečností, k nimž znalec při úkonu přihlížel), z posudku (výčet otázek, na které má odpovědět, s odpověďmi na tyto otázky) a ze znalecké doložky. *Důkaz* se provede tak, že se znalec *vyslechne* do protokolu (§ 55 TŘ) nebo se při výslechu *odvolá na písemný posudek a stvrdí jej* (§ 108 odst. 1, § 210 TŘ) nebo se *protokol o výpovědi znalce nebo jeho písemný posudek přečte*, jestliže znalec byl před podáním posudku řádně poučen, nejsou pochybnosti o správnosti a úplnosti posudku a státní zástupce i obžalovaný s tím souhlasí, resp. není-li souhlas obžalovaného nutný (§ 211 odst. 5 TŘ). Pochybnosti o správnosti znaleckého posudku, jeho nejasnost nebo neúplnost se odstraní vysvětlením znalce nebo přibráním jiného znalce (§ 109 TŘ) a ve výjimečných, zvlášť obtížných případech, vyžadujících zvláštního vědeckého posouzení, i přibráním státního orgánu, vědeckého ústavu, vysoké školy nebo instituce specializované na znaleckou činnost k podání tzv. revizního znaleckého posudku (§110 TŘ). Znalec má nárok na znalečné, tj. na odměnu a náhradu nákladů účelně vynaložených v souvislosti se znaleckým posudkem. Nemajetný obviněný nebo poškozený mají právo žádat, aby bylo rozhodnuto o tom, že stát ponese náklady na znalecký posudek, který si vyžádal sám obviněný nebo poškozený (§ 151a TŘ).

Podá-li znalec nepravdivý, hrubě zkreslený nebo neúplný znalecký posudek nebo uvede-li před příslušným soudem či jiným orgánem nepravdu o okolnosti, která je podstatná pro jeho rozhodnutí, nebo takovou okolnost zamlčí, spáchá *trestný čin křivé výpovědi a nepravdivého znaleckého posudku* podle § 346 TZ.

Pokud jde o *elektronické důkazy*, znalecký posudek, resp. výslech znalce může být nezbytný zejména tam, kde bude třeba zjistit, zda určité zařízení (počítače různých druhů, prvky počítačových sítí, tablety, mobilní telefony, paměťové disky a karty atd.) vůbec obsahuje data či informace, které mohou být elektronickými důkazy, a pokud tomu tak je, jaký je jejich obsah. K tomu může být nezbytné i ohledání takových zařízení (věcí), popřípadě provedení některých jiných procesních úkonů (např. přehrání obrazového a zvukového záznamu).

II.9.7 Příklad využití různých procesních institutů při opatřování elektronických důkazů

Kombinaci ve využití různých důkazních postupů lze ilustrovat příkladem, je-li třeba získat elektronické důkazy o komunikaci obviněného s jinými osobami prostřednictvím jeho mobilního telefonu. Za tím účelem přichází v úvahu výzva k *vydání věci* (mobilního telefonu) podle § 78 TŘ s tím, že když obviněný dobrovolně nevydá svůj mobilní telefon, nelze ho k tomu nutit uložením pořádkové pokuty podle § 66 odst. 1 TŘ, neboť zde platí zákaz sebeobviňování a obviněný není povinen sám aktivně přispívat ke svému postihu. V takovém případě je třeba využít institut *odnětí věci* podle 79 TŘ, a jestliže by obviněný tvrdil, že mobilní telefon nemá u sebe, přichází v úvahu u něj nařízení a provedení *osobní prohlídky* podle § 82 odst. 3, § 83b, § 84 a § 85 TŘ, je-li zde důvodné podezření, že obviněný má mobilní telefon u sebe. Kdyby tomu tak nebylo a existovalo-li by důvodné podezření, že obviněný má mobilní telefon ve svém obydlí nebo v jiném prostoru nesloužícím k bydlení, bylo by možné nařídit a provést *domovní prohlídku nebo prohlídku jiných prostor* podle § 82 odst. 1, 2, § 83, § 83a, § 84 a § 85 TŘ. Pokud by byl takto mobilní telefon získán a jestliže by bylo nezbytné zjistit i průběh komunikace obviněného s jinými osobami podle údajů příslušného poskytovatele telekomunikačních služeb, musel by příslušný orgán činný v trestním řízení opatřit *příkaz ke zjištění údajů o uskutečněném telekomunikačním provozu* podle § 88a TŘ. Získaný mobilní telefon by mohl být i předmětem *ohledání věci* (§ 113 TŘ), kdyby měl důkazní význam i vnější stav mobilního telefonu (např. z hlediska jeho poškození), a vlastní informační obsah mobilního telefonu včetně jeho SIM karty by pak byl předmětem *znaleckého zkoumání nebo alespoň odborného vyjádření* (§ 105 a násl. TŘ), a to z hlediska existence či neexistence relevantních dat, která by byla použitelná jako elektronické důkazy.

II.10 Shrnutí kapitoly

Dokazování jako specifická procesní činnost má stěžejní význam pro každé trestní řízení. Tomu do jisté míry odpovídá i právní úprava procesu dokazování, která je obsažena především v různých ustanoveních *trestního řádu*, ale též v některých dalších normách. Nejde o úpravu zcela vyhovující, protože neobsahuje např. jasně stanovené limity pro přípustnost či nepřípustnost určitých

důkazních postupů a prostředků, ale ty vymezuje zpravidla jen judikatura soudů. Pozitivní změny lze však očekávat až od rekodifikace trestního řádu, která by měla přinést poněkud systematičtější a komplexnější úpravu důkazního práva. Stávající trestní řád obsahuje pouze *demonstrativní výčet důkazních prostředků* a připouští dokazování i prostřednictvím dalších, výslovně neupravených důkazních prostředků. To se týká i *elektronických důkazů (resp. důkazních prostředků)*, o nichž se trestní řád prakticky nikde nezmiňuje. V trestním řízení pak lze provádět dokazování i za pomoci elektronických důkazních prostředků, a to s využitím různých procesních postupů a institutů, jimiž jsou zejména vydání a odnětí věci důležité pro trestní řízení, domovní prohlídka, prohlídka jiných prostor a pozemků a osobní prohlídka, odposlech a záznam telekomunikačního provozu, vyžádání údajů o uskutečněném telekomunikačním provozu, ohledání a posudek znalce.

III DATA JAKO DŮKAZ V TRESTNÍM ŘÍZENÍ

Díky rapidnímu rozvoji využívání informačních a komunikačních technologií ve všech oblastech lidské činnosti je prostřednictvím výpočetní techniky zpracováváno a uchováváno stále větší množství informací[105]. Zvyšující se dostupnost výpočetní techniky, rostoucí počítačová gramotnost, rozšiřování dostupnosti internetu a rostoucí efektivita a kapacita zpracování počítačových dat vedou k tomu, že se mnoho lidských činností přesouvá do virtuálního prostoru. Dnes již není běžné posílat listovní zásilky, evidovat běžné faktury v šanonech nebo si vést knihu jízd jako sešit uložený v palubní desce služebního vozu. Všechny tyto informace jsou zpracovávány prostřednictvím počítačů a počítačových sítí. Je proto čím dál běžnější, že orgány činné v trestním řízení musejí při dokazování využívat informace uchované v počítačových datech.

Právo však do současné doby tento fakt reflektovalo spíše nedostatečně. Zákonná úprava trestního řízení je poněkud zastaralá, a ač prošla mnoha novelizacemi, jasnou odpověď na otázku, jak nakládat s daty jako s důkazem v trestním řízení, bohužel neposkytuje. Je proto třeba využívat interpretačních prostředků a na vznikající praktické situace flexibilně aplikovat existující procesní nástroje upravující dokazování v trestním řízení. To často staví orgány činné v trestním řízení do nelehké pozice. Tato kapitola shrnuje aktuální poznatky týkající se za prvé technických vlastností dat relevantních pro dokazování v trestním řízení a za druhé základních procesních postupů pro jejich využívání jako důkazů.

III.1 Prameny elektronických důkazů

Různá zařízení jsou způsobilá generovat či uchovávat data, která mohou být využitelná jako zdroj elektronických důkazů v trestním řízení. V závislosti na zdroji mohou mít taková data různý charakter a musí k nim být při dokazování různě přistupováno jak z technického, tak procesního hlediska.

105 Tento fakt lze demonstrovat na vývoji využívání internetu a počtu jeho uživatelů. Příslušné statistiky jsou dostupné např. z http://www.internetworldstats.com/emarketing.htm.

Tato podkapitola se věnuje pramenům elektronických důkazů, tedy jednotlivým technickým zařízením, která mohou být zdrojem dat využitelných v trestním řízení. Zabývá se jejich charakteristikou a technickými vlastnostmi, které mohou mít vliv na postupy aplikované v trestním řízení při zajišťování důkazů. Cílem kapitoly však není dokonale technicky popsat tato zařízení, nýbrž poskytnout obecný přehled nejvýznamnějších vlastností, které je třeba zohledňovat při nakládání s daty, která mají být využita k získání důkazů, a při využívání různých procesních nástrojů trestního práva při zajišťování takových dat.

III.1.1 Počítač

Jednoznačná definice pojmu počítač v podstatě neexistuje. Přestože si člověk pod tímto pojmem zpravidla představí osobní počítač nebo notebook, zahrnuje tento pojem daleko širší škálu různých zařízení. V nejobecnějším smyslu lze za počítač považovat přístroj, který může být naprogramován za účelem samostatné realizace aritmetických a logických operací. Oxford Dictionary například počítač definuje jako *„elektronické zařízení, které je schopné přijímat informace (data) v určité formě a provádět sekvenci operací v souladu s* přednastavenou, ale variabilní *sadou instrukcí (program) za účelem vytvoření výsledku v podobě informací nebo signálů"*[106]. Podobnou definici obsahuje také norma ČSN ISO/IEC 2382-1, která pod pojmem počítač chápe *„stroj na zpracování dat provádějící samočinné posloupnosti různých aritmetických a logických operací"*[107]. Pro potřeby tohoto textu se jako nejvhodnější jeví definice, která vychází z vlastností, které má počítač mít – tedy schopnost přijímat vstupní informace (1), samostatně informace zpracovávat (2), na základě takového zpracování vytvářet nové informace (3) a tyto poskytovat nebo uchovávat (4).

Aby mohl počítač vyžadované funkce vykonávat, obsahuje komponenty, které lze rozdělit do dvou základních kategorií – hardware a software.

Hardware jsou hmotné součásti počítače, které vykonávají předprogramované instrukce. Podle svého charakteru mají různé počítače různý hardware, jeho konfigurace se odvíjí především od zamýšleného účelu, pro který má

106 Překlad autor. Viz Oxford Dictionaries. *Computer* [online]. Dostupné z http://www.oxforddictionaries.com/definition/english/computer.

107 Viz Česká technická norma ČSN ISO/IEC 2382-1 - Informační technologie - Slovník Část 1: Základní termíny.

být počítač využíván, od požadovaného výkonu, spotřeby energie, míry zabezpečení nebo kapacity. Některé hardwarové součástí počítač obsahuje již z podstaty vždy – jde především o vstupní zařízení, kterým přijímá data (klávesnice, myš, scanner, síťová karta, modem, USB port, datové úložiště atd.), procesor, který provádí jejich zpracování, operační paměť, do které se dočasně ukládají zpracovávaná data, a výstupní zařízení, která mohou být shodná se zařízeními vstupními (monitor, tiskárna, síťová karta, USB port, datové úložiště atd.).

Vstupní a výstupní zařízení

Vstupní a výstupní zařízení v podstatě umožňují komunikaci informací s počítačem, který realizuje jejich zpracování. Nemusí se jednat pouze o nejběžnější zařízení jako klávesnice, monitor a podobně. Jelikož škála zařízení, která mohou být zahrnuta pod využitou definici počítače, je velmi široká, mohou být vstupními a výstupními zařízeními i nejrůznější čidla a senzory (teplotní, laserové, pohybové apod.), komunikační rozhraní (GPS moduly, rozhraní pro bezdrátovou komunikaci apod.) či stroje vykonávající výstupní instrukce. I samotná výstupní a vstupní zařízení mohou v sobě obsahovat samostatné počítače.

V souvislosti se zajišťováním důkazního materiálu mohou sloužit jako prostředek k zachycení důkazů získaných z dat zpracovávaných počítačem (například vytištěním, zobrazením na monitoru, pomocí datového přenosu) nebo mohou sloužit jako přímý zdroj důkazů (např. datová úložiště, tiskárny, které mohou ve své paměti uchovávat dříve vytištěné dokumenty, apod.).

Procesor

Procesor je v podstatě mozkem celého počítače. Provádí zpracování dat prostřednictvím aritmetických a logických operací. Některé počítače obsahují jeden procesor, jiné mohou obsahovat jejich větší množství. Procesory mohou také v rámci jednoho počítače mít rozdělené role, například CPU (centrální procesorová jednotka) může provádět základní operace, zatímco GPU (grafická procesorová jednotka) provádí výpočty pro grafické výstupy zpracování dat. Procesor sám o sobě zpravidla také obsahuje více součástí, těmi nejběžnějšími jsou aritmeticko-logická jednotka (ALU), která provádí vlastní výpočetní operace, kontrolní jednotka (CU), která řídí pohyb dat

v rámci procesoru, a procesorové rozhraní, které umožňuje komunikaci procesoru s ostatními součástmi počítače. Procesor je v rámci počítače zasazen do systému dalších dílčích součástí, které mezi sebou komunikují data a některá dočasně uchovávají. Tato komunikace je realizována v nešifrované formě.[108]

Z hlediska získávání důkazního materiálu je vhodné připomenout, že na různých hardwarových sběrnicích lze teoreticky zachycovat data, která jsou v rámci počítačového systému komunikována. Z takových dat je pak možné například získat šifrovací klíče k datovým úložištím. Specifickým nástrojem integrovaným především v přenosných počítačích je TPM čip (Trusted Platform Module), který funguje jako kryptoprocesor k bezpečnému uchovávání šifrovacích klíčů pro dešifrování dat z datových úložišť.[109]

Paměť

Paměť počítače je nezbytná pro uchovávání dat, nad kterými programy vykonávají operace. Paměť počítače má zpravidla formu integrovaného obvodu. Podle funkce, kterou v rámci počítače paměť vykonává, rozlišujeme:

- RAM (Random Access Memory), která umožňuje rychlý zápis i čtení dat využívaných programy. Do této paměti se uchovávají data systémového a aplikačního software a jimi zpracovávaná data tak, aby k nim bylo možno přistupovat rychle a segmentovaně. V případě, že je zašifrováno datové úložiště, je v této paměti uchováván zpravidla také dešifrovací klíč, který tak lze získat. Specifikem tohoto typu paměti je, že dokáže uchovávat data pouze, pokud je počítač v chodu. Se ztrátou elektrického napětí v paměťových modulech se ztrácí i v nich uchovaná data.
- ROM (Read Only Memory), která jako typ paměti umožňuje pouze čtení dat, neumožňuje však jejich zápis. Tato paměť je obvykle využívána k uchování základního řídícího software počítače (BIOS, Basic Input Output System) nebo k uchování firmware (software určený k řízení vestavěných systémů) některých specifických počítačových systémů.

108 Více k fungování procesoru počítače viz např. Young, R. *How computers work: processor and main memory. 2nd ed.* S. l.: Roger Young, 2009.

109 Tento typ čipu je v podstatě považován za standard a například jej obsahují v podstatě všechny počítače, které jsou certifikovány pro provoz operačního systému Windows. TPM je však také zdrojem kontroverzí. Více detailů viz Kinney, Steven L. *Trusted platform module basics using TPM in embedded systems*. Oxford: Newnes, 2006.

- EPROM (Erasable Programmable Read Only Memory), je zpravidla využívána podobně jako ROM, tedy v běžném režimu pouze pro čtení. Umožňuje však i zápis dat, například za účelem aktualizace obsaženého software či firmware. Data z této paměti se při vypnutí počítače neztratí.

V rámci trestního řízení mohou být data z paměti počítače zajímavým zdrojem důkazního materiálu především z toho důvodu, že se v nich zpravidla uchovávají v nešifrované podobě. Paměť RAM obsahuje aktuálně zpracovávaná data a za běhu se v ní uchovává také dešifrovací klíč k šifrovaným datovým úložištím. I paměti EPROM mohou teoreticky obsahovat data uživatele. Jsou dokonce známy případy, kdy keylogger kód[110] v BIOSu přímo do EPROM ukládal zachycená hesla. Získávání dat však především v případě RAM není jednoduché a mnohdy ani možné bez kompromitace dat. Při vypnutí počítače se totiž data ztrácí.

Software

Software lze chápat jako počítačové programy, které obsahují instrukce zpracovávané hardwarem. Pojem software není jednoznačně definovaný. Některé zdroje definují software jako všechny součásti počítače, které nejsou hardware. Tato definice je však pro potřeby tohoto textu příliš široká, protože kromě počítačových programů, které obsahují strojový kód a instrukce pro hardware, zahrnuje také data, která jsou prostřednictvím software zpracovávána (dokumenty). Ač je hranice mezi počítačovým programem a dokumentem mnohdy jen těžko identifikovatelná (například dokument HTML[111] může obsahovat dynamické prvky, které lze považovat za počítačové programy), je vhodné pro naše potřeby tyto dvě kategorie rozlišit.

110 Keylogger je typ malware, který sleduje, jaké klávesy byly během používání počítače stisknuty. Tyto údaje pak může uchovávat nebo sám analyzovat a vyhledávat v takto získaném řetězci znaků přístupová hesla. V citovaném případě bylo specifické, že toto prováděl škodlivý kód přímo v BIOSu a získaná hesla uchovával ve vlastní paměti EPROM. To proto, že útočník věděl, že společnosti a instituce často likvidují zastaralé datové nosiče, ale zbytek hardware prodávají. Je tak snadnější se k heslům dostat.

111 HTML (hypertext markup language) je značkovací jazyk využívaný pro tvorbu webových stránek. Stručně o HTML viz Písek, S. *HTML: tvorba jednoduchých internetových stránek. 2., aktualiz. a dopl. vyd.* Praha: Grada, 2006.

Za software tedy můžeme považovat taková počítačová data, která mají charakter počítačového programu, jenž obsahuje instrukce, na základě kterých procesor realizuje výpočetní a logické operace.

Software může být zachycen v několika formách, z nichž nejdůležitější jsou zdrojový a strojový kód. Strojový kód jsou binární data obsahující instrukce srozumitelné pro procesor, který podle nich vykonává zadané operace. Strojový kód ale není příliš srozumitelný pro člověka a jeho sestavování by bylo komplikované. Proto se počítačové programy vytváří pomocí takzvaného zdrojového kódu, což je striktně formátovaný text popisující algoritmus počítačového programu. Aby mohl být takto vytvořený text zpracován procesorem, musí být přeložen do strojového kódu pomocí kompilátoru.

Software lze rozdělit do dvou základních kategorií. Na systémový software, který řídí chod počítačového systému a umožňuje provoz druhé kategorie – aplikačního software, který plní v rámci počítačového systému specifické funkce.

Systémový software

Systémový software je navržen tak, aby řídil fungování hardware a aby vytvářel platformu pro provoz aplikačního software. Za systémový software lze považovat v první řadě firmware, což jsou počítačové programy obsažené přímo v hardware. Zpravidla jsou uchované v paměti ROM nebo EPROM a řídí fungování konkrétní součásti počítačového systému nebo zařízení (např. BIOS[112], programy řídící fungování řadičů, periferních zařízení apod.). V jistém smyslu vyšší kategorií jsou operační systémy, které kromě toho, že hardware řídí, také zprostředkovávají přístup k hardwarovým zdrojům aplikačnímu software a uživateli. Operační systém obsahuje jádro a ovladače, které komunikuje s hardware, a pomocné systémové nástroje pro správu operačního systému (řízení oprávnění, bezpečnosti, šifrovací nástroje, utility apod.).

Pro dokazování je z hlediska systémového software podstatná především otázka kompatibility. Aplikační software kompilovaný pro určitý systémový

112 BIOS (basic input-output system) je zjednodušeně firmware osobních počítačů uložený na čipu, který je součástí základní desky počítače. Zajišťuje inicializaci a konfiguraci hardware počítače, aby umožnil spuštění operačního systému.

software totiž často není možné provozovat na jiném, stejně tak k některým formátům dokumentů nebo datům uchovaným na datových úložištích s určitým formátem nelze přistupovat na všech systémových software (viz níže).

Aplikační software

Aplikační software jsou počítačové programy, které využívají rozhraní a prostředky nabízené systémovým software a umožňují uživateli provádět určité specifické aktivity. Jedná se především o kancelářské balíky, software pro práci s multimédii, grafické programy, vývojové nástroje, informační systémy, software sloužící k řízení strojů apod. Aplikační software může být distribuován jako multiplatformní, tedy takový, který je možné provozovat na více různých systémových software. Často je však pro provoz určitého aplikačního software nutné mít k dispozici počítač s určitým systémovým software (například některé počítačové programy lze využívat na platformě Windows, ale neexistuje jejich verze pro Mac OS). Je-li aplikační software distribuován ve strojovém kódu (binární podoba), pak jej lze zpravidla provozovat pouze na určitém systémovém software. Některé programy jsou však distribuovány v podobě zdrojového kódu, který si pak systémový software kompiluje do strojově čitelné a kompatibilní binární podoby.[113]

III.1.2 Datová úložiště

Existuje mnoho druhů datových úložišť. Některá jsou zabudována přímo v počítači (interní), jiná lze k počítači připojovat podle potřeby (externí).

Jako interní datová úložiště slouží vedle počítačové paměti (RAM, ROM, EPROM) zpravidla především pevné disky (HDD, Hard Disk Drive) nebo SSD disky (Solid State Drive).

Pro externí datová úložiště je užíván pojem datový nosič, neboť tato úložiště jsou mobilní a mohou být připojována podle potřeby k různým počítačovým nosičům. Jako datové nosiče mohou být využívány nejen pevné disky a SSD disky, ale také například flashové USB paměti nebo optické disky (CD/DVD/BluRay). Za externí datová úložiště se vedle datových nosičů považují také úložiště dostupná v síti (například NAS – Network-attached

[113] Kompilací se rozumí překlad ze zdrojového kódu čitelného pro člověka do kódu strojového, srozumitelného pro počítač. K tomu slouží počítačové programy zvané kompilátory.

storage). Jde zpravidla o datová úložiště připojená k počítačové síti, ke kterým přistupují různé počítače. Data tak mohou být využívána distribuovaně.

Pevné disky obsahují rotující kotouče, na které se pohyblivými hlavami pomocí magnetické indukce zaznamenávají data. Naproti tomu SSD disky neobsahují pohyblivé části a jsou sestaveny z integrovaných nevolatilních paměťových čipů typu flash. SSD disky díky svojí rychlosti a nízké spotřebě postupně nahrazují pevné disky. Pevné disky i SSD disky jsou k počítači připojeny prostřednictvím určitého rozhraní, nejčastěji SATA, PCI Express či PCMCIA – jde o fyzicky se lišící konektory, které umožňují komunikaci se sběrnicí, prostřednictvím které jsou informace přenášeny do procesoru.

Flash USB paměti mají podobný charakter jako SSD disky, jde o čipy postavené na shodné technologii. Jejich výhodou je, že je lze prostřednictvím USB (Universal Serial Bus) připojit k různým počítačům a pohodlně tak transportovat data.

Konečně optická média mají charakter kotoučů, které obsahují reflexní vrstvu, do které jsou zaznamenávána binární data. Pro jejich čtení a zápis je nutné, aby měl počítač speciální zařízení – optickou mechaniku. Jednotlivé typy optických datových nosičů se liší podle hustoty zápisu respektive kapacity (CD – cca 700 MB, DVD – cca 5 až 17 GB, BluRay – cca 25 až 100 GB). Optické disky mohou být určeny pouze pro čtení zaznamenaných dat (CD-ROM, DVD-ROM či BD-ROM), může jít o disky určené k jednorázovému zápisu (CD-R, DVD-R či BD-R) nebo mohou umožňovat opakovaný přepis dat (CD-RW, DVD-RW, BD-RE).

Všechny typy datových úložišť v počítači zpravidla plní stejnou funkci: jsou na nich uchovávána data, především počítačové programy (operační systém a aplikační software) a dokumenty, a to strukturovaně v podobě souborů a adresářů.

Data uchovávaná v datových úložištích jsou logicky strukturovaná. V první úrovni mohou být disky rozděleny na oddíly (partition), které představují logické celky pro uchovávání dat. Tyto celky jsou potom naformátovány pro uchovávání dat za využití určitého souborového systému (file system), který v podstatě definuje, jak jsou na disku data organizována. Souborových systémů existuje poměrně velké množství a různé systémové software jsou

schopné pracovat s různými souborovými systémy. Některé typy firmware (například firmware kamerových systémů) dokonce někdy obsahují proprietární souborové systémy a k datům tak lze přistupovat pouze prostřednictvím konkrétního zařízení.

III.1.3 Počítačová síť

Pod pojmem počítačová síť chápeme technické prostředky, které realizují nebo asistují výměnu dat mezi počítači. Počítačové sítě lze mnoha způsoby kategorizovat, neboť jich existuje velké množství.

V současné době je síťová komunikace postavena především na referenčním modelu ISO/OSI, který síťovou komunikaci rozděluje na vrstvy, které plní různé funkce v rámci zajištění spolehlivé, bezpečné a rychlé komunikace. V rámci tohoto modelu se fyzická vrstva sítě skládá z takzvaných nodů, těmi může být vedle komunikujících zařízení (počítače, servery, mobilní zařízení atd.) také síťový hardware (routery, switche, brány apod.). Taková zařízení mohou být přímo spojena nebo mohou pro komunikaci využívat širší infrastrukturu sítě. V dnešní době nejvyužívanější sadou protokolů pro síťovou komunikaci je tzv. TCP/IP, která je rozdělena na 4 vrstvy a využívána rovněž pro provoz sítě Internet.

Jedná se o decentralizovaný model, který rozděluje datovou komunikaci na pakety, které jsou samostatně zasílány infrastrukturou sítě na úrovni síťové vrstvy na unikátní adresy IP uchované v hlavičce datového paketu. Každý počítač v síti má svoji IP adresu, která je využívána pro komunikaci dat, samotné pakety pak proudí sítí přes množství nodů, přičemž nikdy není předem přesně známa cesta, kterou bude komunikace mezi dvěma zařízeními vést.

Na transportní vrstvě je pak v hlavičce uchován port, pomocí kterého se komunikace směruje pro různé aplikace v rámci komunikujícího zařízení. Pro tuto vrstvu jsou využívány protokoly TCP (transmission control protocol), který obsahuje kontroly a tak zajišťuje spolehlivou komunikaci (využívá se pro komunikaci, která je závislá na spolehlivosti přenosu – soubory, e-maily apod.) a UDP (user datagram protocol), který je využíván pro rychlou komunikaci s nižší spolehlivostí (například pro služby VoIP, streaming videa apod.).

Na aplikační vrstvě pak řídí komunikaci samotné protokoly aplikací využívajících síťový přenos (HTTP – přenos hypertextových dokumentů, IMAP – přenos e-mailů, atd.). Na aplikační vrstvě dochází také k šifrování datové komunikace.

Z hlediska dokazování je podstatné, že při komunikaci nedochází pouze k přenosu obsahových dat, ale také k přenosu a vytváření dat provozních, které se váží k jednotlivým vrstvám. Ta mohou poskytovat informace o tom, odkud a kam byla data přenášena, prostřednictvím jakého protokolu, zda byla šifrovaná, případně mezi jakými aplikacemi ke komunikaci docházelo.

Síťovou komunikaci lze rovněž odposlouchávat, a to prostřednictvím takzvaného sniffovacího zařízení nebo software, který je strategicky umístěn tak, aby přes něj proudila zájmová komunikace. Odposlouchávání lze provádět na různých vrstvách komunikace a lze tak získat nejen obsah komunikovaných dat ale i provozní metadata. Pokud je však komunikace na aplikační vrstvě šifrovaná, nedojde k přístupu k obsahovým datům.

III.1.4 Cloud

Cloud computing je termín, který popisuje myšlenku distribuovaného využívání výpočetních zdrojů. Je založen na využívání skupin vzdálených serverů a počítačové sítě za účelem vytvoření centralizovaného úložiště dat a umožnění online přístupu k počítačovým službám a zdrojům. Nejde tedy o konkrétní technologii, ale spíše o způsob využívání počítačových technologií zmíněných výše. Tato myšlenka je založena na globálním charakteru počítačové sítě Internet, prostřednictvím kterého jsou propojovány jednotlivé servery a datová úložiště do logického celku. Jednu z často využívaných definic pojmu cloud computing nabízí Národní institut pro standardy a technologie USA: *„Cloud computing je model umožňující teritoriálně neomezený, pohodlný, on-demand přístup k množině konfigurovatelných výpočetních zdrojů (např. sítím, serverům, datovým úložištím, aplikacím a službám), které mohou být okamžitě poskytnuty nebo upraveny s minimálním úsilím ze strany uživatele a bez potřeby aktivního zásahu ze strany poskytovatele služeb.“*[114]

114 Překlad autora. Viz Mell, P., Grance, T. National Institute Of Standards And Tehchnology. *The NIST Definition of Cloud Computing.* 2011. Dostupné z: http://dx.doi.org/10.6028/NIST.SP.800-145.

Na straně poskytovatele tedy může existovat různé množství zařízení rozmístěných po celém světě, ke kterým uživatel přistupuje jako k celku z jednoho nebo více bodů. Z hlediska uživatele tedy nezáleží na fyzickém umístění jeho dat, ta mohou v rámci cloudu podle potřeby migrovat a uživatel k nim přistupuje stále stejným způsobem. K datům, zdrojům a aplikacím v cloudu lze navíc teoreticky přistupovat z kteréhokoliv zařízení připojeného do příslušné sítě, uživatel je tak může využívat prostřednictvím webového prohlížeče nebo specifického aplikačního software ze svého počítače, mobilního telefonu nebo třeba tabletu. Kromě toho je také výhodou cloudu možnost škálování zdrojů. Vyžaduje-li uživatel větší výpočetní výkon nebo kapacitu úložiště, může jej získat okamžitě pouhou změnou konfigurace služby. Zdroje jsou tak využívány efektivněji.

Z technického hlediska existují tři typy distribučního modelu cloudových služeb:

- IaaS (infrastructure as a service, infrastruktura jako služba), ve kterém uživatel získá přístup k čistému výpočetnímu výkonu nebo k datové kapacitě bez implementace platformy nebo software, cena se zpravidla odvíjí od nakoupeného procesorového času nebo od nakoupeného úložného prostoru;
- PaaS (platform as a service, platforma jako služba), kde si uživatel kromě výpočetního výkonu a úložného prostoru platí také přístup ke zdroji nástrojů nebo knihoven, které tvoří platformu pro implementaci software uživatele;
- SaaS (software as a service, software jako služba), v případě tohoto modelu si uživatel platí provoz konkrétního software v určitém rozsahu. Není tedy podstatným kritériem poskytnutý výpočetní výkon, ale rozsah, ve kterém je umožněno využití software, provozovaného správcem cloudu na jeho vlastní infrastruktuře.[115]

V současné době je ohledně právní povahy cloudu a způsobů přístupu k důkaznímu materiálu v něm uchovanému vedena široká diskuse na mezinárodní úrovni. Jelikož jsou taková data delokalizovaná a provozovatel cloudu je zpravidla usídlen mimo území ČR, je mnohdy jejich zajišťování poměrně náročné a v některých případech v podstatě nemožné. Fungování moderních

115 Viz Winkler, J. R., Meine B. (eds.) *Securing the Cloud Cloud Computer Security Techniques and Tactics.* Burlington: Elsevier Science, 2011.

cloudových služeb má však specifika, která mohou naopak při zajišťování důkazního materiálu být výhodná. Často například dochází prostřednictvím cloudového úložiště nebo informačního systému k synchronizaci dat. Pokud je získán přístup k zařízení, se kterým k synchronizaci dochází, lze při využití vhodných procesních nástrojů získat přístup nejen k datům aktuálně v cloudu dostupným, ale rovněž lze sledovat jejich změnu v čase.

III.2 Charakteristika dat jako elektronických důkazních prostředků

Důkazními prostředky, z nichž orgány činné v trestním řízení (resp. jiné osoby) mohou čerpat důkazy, vyjmenovává trestní řád v § 89 odst. 2.[116] Důkazem je podle jeho dikce vše, co může přispět k objasnění věci. Tuto obecnou definici doplňuje o demonstrativní výčet jednotlivých prostředků – výpovědi, znalecké posudky, věci, listiny a ohledání. Ač trestní řád nikde výslovně neodděluje pojmy důkaz a důkazní prostředek, teorie trestního práva považuje důkaz za informaci o věci a důkazní prostředek jako zdroj této informace. Důkazní prostředek tak lze vymezit jako „zdroj, z něhož orgán činný v trestním řízení důkazy čerpá (výpovědi osob, věci)“[117]. Za elektronický důkazní prostředek lze tedy považovat vše, co může sloužit jako zdroj relevantní informace a co je uchováno v elektronické podobě – tedy především data. Data jako elektronické důkazní prostředky lze chápat jako nezpracovaná fakta a údaje bez přidané interpretace či analýzy. Samotné důkazy, tedy informace, jsou data, která byla interpretována tak, aby měla nějaký smysl pro jejich zpracovatele, resp. v našem případě pro dokazování v trestním řízení.

Pojem elektronické důkazní prostředky není v současném platném právu České republiky nikde definován a vlastně ani zmíněn. Ani právní teorie nám v současné době neposkytne uspokojivou definici. Ač je často pro elektronické důkazní prostředky využívána analogie[118], jako nejvhodnější se jeví

116 Viz Jelínek, J. *Trestní právo procesní. 1. vyd. podle novelizované právní úpravy účinné od 1. 1. 2010.* Praha: Leges, 2010.

117 Viz Císařová, D., Fenyk, J., Gřivna, T. et al. *Trestní právo procesní. 5. vyd.* Praha: ASPI, 2008, s. 284.

118 Viz Mason, S. *International electronic evidence.* London: British Institute of International and Comparative Law, 2008.

definovat je pomocí jejich specifických vlastností. Jedním z hlavních znaků, který je charakteristický pro data jako elektronické důkazní prostředky, je to, že jsou informace v nich uchovávány v podobě, která je bez dalších nástrojů pro běžného člověka obtížně smyslově vnímatelná. Ze základního binárního zobrazení dat[119] nedokáže člověk běžně získat žádnou relevantní informaci, a proto je za účelem jejich interpretace nutno využít nějakého elektronického zařízení, které je schopné tato data převést do podoby vnímatelné lidskými smysly.

Nejobecněji lze v tomto smyslu elektronické důkazní prostředky definovat jako takové „důkazní prostředky, k jejichž převodu do podoby srozumitelné pro člověka je třeba použít nějaké elektronické zařízení“[120].

Výše uvedené vymezení pojmu je velmi obecné, k jeho bližšímu pochopení je tedy vhodné si elektronické důkazní prostředky rozdělit do určitých kategorií, které jsou pro běžného člověka lépe uchopitelné.

Na běžném datovém úložišti se nacházejí dvě hlavní kategorie dat. První jsou taková data, která přímo obsahují nějaké informace. Ta můžeme obecně rozdělit na elektronické dokumenty, metadata těchto dokumentů nebo provozní data vytvořená aplikacemi. Elektronické dokumenty obsahují informace, které v nich aktivně zachytil člověk. Jedná se tedy například o textové dokumenty, tabulky, texty na webových stránkách, digitální fotografie, audio a video záznamy a podobně. K těmto informacím pak aplikace, prostřednictvím kterých dokumenty vznikají, zpravidla přidávají takzvaná metadata. Metadata obsahují doplňující informace o dokumentu, například dobu jeho pořízení, kdo jej pořídil, jaká verze jakého programu jej vytvořila. Kromě metadat aplikace vytvářejí také další data, která přímo nesouvisejí s aktivitou realizovanou člověkem. Může jít o různá provozní a pomocná data, která aplikace vytvářejí jako produkt svojí funkcionality. K těmto aplikačním datům můžeme řadit různé logy, automaticky pořizované záznamy nebo například data uložená v palubním počítači automobilů nebo data vytvářená počítači a síťovými prvky při datové komunikaci. Specifickou kategorií

119 Strojový kód obsahuje pouze hodnoty 1 a 0, sled těchto dvou hodnot je definován standardy, které umožnují elektronickým zařízením jejich zpětnou interpretaci do člověkem vnímatelné podoby.

120 Více k definici viz Kočí, M. *Elektronické důkazní prostředky*. Brno: Masarykova univerzita, 2012. Diplomová práce.

aplikačních dat jsou dočasné soubory a obsah cache. Tato data si uchovávají především internetové prohlížeče za účelem rychlejšího načítání webových stránek a obsahují fragmenty navštívených webů. Díky těmto souborům se dá dohledat historie prohlížeče, i když dojde ke smazání logů. Tyto různé typy elektronických dat mají různou míru vlivu člověka na jejich obsah, různou míru automatizace jejich vzniku, a proto i různou důkazní spolehlivost. Data, která vytvářejí aplikace automaticky a která nelze jednoduše uživatelsky upravovat, budou mít patrně větší důvěryhodnost než samotné elektronické dokumenty, které lze snadno a rychle editovat.

Druhou kategorií jsou aplikace, tedy data, která mají v počítačových systémech určitou dynamiku, která určují co a jak má systém dělat. Tyto aplikace zprostředkovávají nebo realizují tvorbu klasických dat obsahujících informace, ale také realizují zpětnou interpretaci již vytvořených dat do smyslově vnímatelné podoby. Aplikace zpravidla v současné praxi nejsou zahrnuté do rozsahu dokazování[121] a u běžně využívaných aplikací se způsob jakým vytvářejí nebo interpretují data, zpravidla nerozporuje.

III.2.1 Smyslová vnímatelnost důkazů[122]

Jak napovídá zvolená definice elektronických důkazních prostředků, k jejich převodu do pro člověka smyslově vnímatelné podoby je nutné využít nějakého elektronického zařízení. Různých elektronických zařízení s různou funkcionalitou existuje obrovské množství, proto je důležité pro získávání důkazu z elektronického důkazního prostředku zvolit takové, které je pro daný typ prostředku vhodné a které umožní získat z něj maximální množství informací.

K demonstraci tohoto konstatování si můžeme nastínit modelovou situaci, kdy je zajištěn kompaktní disk. Zařízení, která mohou kompaktní disk

121 Rozsah dokazování je primárně vymezen v ust. § 89 odst. 1 TŘ podle nějž je třeba okolnosti důležité pro trestní řízení dokazovat v „nezbytném rozsahu". Jelikož se zpravidla pro interpretaci elektronických dat využívají aplikace se standardní funkcionalitou a nepředpokládá se, že by byly nějak upraveny, nedokazuje se, jak aplikace zpracovává vstupní data a zda z nich získává autentické a úplné informace.

122 Koncept úvodní části této podkapitoly byl publikován v STUPKA, Václav. Elektronické důkazní prostředky. In KALVODOVÁ, Věra a Milana HRUŠÁKOVÁ. *Dokazování v trestním řízení - právní, kriminologické a kriminalistické aspekty*. Brno: Masarykova univerzita, 2015. S. 311-320.

přehrát, je celá řada, ale kvalita a kvantita informací, které nám poskytnou, je různá. Jestliže se jedná o hudební CD, můžeme jej přehrát v přehrávači a zjistit tak, jaké obsahuje audio záznamy. Toto CD ale může současně obsahovat i další data[123], která však hudební přehrávač neumí interpretovat, a tak zůstanou skrytá.

Podobným případem může být i webová stránka, která se obvykle zobrazuje prostřednictvím standardního webového prohlížeče, jenž provede kompilaci zdrojového kódu stránky a zobrazí ji podle svého algoritmu. Když se k dokazování využije pouze výtisk takto interpretované stránky, připravujeme se o podstatné informace, které mohou být obsaženy ve zdrojovém kódu nebo v metadatech[124]. Různé webové prohlížeče navíc mohou jeden a ten stejný zdrojový kód interpretovat různě[125].

Podobně tomu může být také například u smluvních dokumentů vytvořených v textovém editoru. Nejenže mohou mít při využití dnešních technologií dynamický charakter a jejich obsah se tak může podle uživatelských instrukcí měnit, ale změny mohou nastávat i nechtěně. Běžným příkladem je otevření dokumentu v jiném software, než ve kterém byl vytvořen (typicky například dokument vytvořený v MS Word otevřený v LibreOffice, nebo v jiném open source nástroji). Často v takových případech dochází ke změnám nejen ve formátování nebo číslování odstavců, ale také ke změně obsahu (například nejsou vidět komentáře apod.). To může mít na právní interpretaci takového dokumentu značný vliv.

Volba interpretačního prostředku, tedy elektronického zařízení a aplikace, je tak v případě elektronických důkazních prostředků kriticky důležitá, může totiž velmi ovlivnit i samotný výsledek dokazování[126]. Proto je při dokazování nutné vhodně pracovat s datovými formáty.

123 Vedle hudební stopy lze na jedno CD zapsat také stopy datové. Ty mohou obsahovat například videosoubory, elektronické dokumenty nebo například fotky.

124 Ve zdrojovém kódu mohou být skryty i podstatné informace, poměrně často se do něj tvůrce webu podepisuje nebo do něj vkládá svoje komentáře. Často se podle zdrojového kódu dá také zjistit, prostřednictvím jakého software byl vytvořen, nebo dokonce i identita jeho tvůrce.

125 Jednotlivé webové prohlížeče i jejich jednotlivé verze používají ke zpracování zdrojového kódu různé algoritmy, a proto se může výsledné zobrazení webové stránky mírně lišit. A to i po obsahové stránce.

126 Více příkladů k problematice volby interpretačních prostředků viz Newman, R. *Computer Forensics: Evidence Collection and Management.* Auerbach publications, 2007.

III.2.2 Datové formáty

Datový formát nebo formát souboru obvykle určuje význam dat uchovaných v datovém souboru. Datových formátů je veliké množství, některé jsou navrženy pro uchovávání jen jednoho druhu dat (např. JPEG pro uchovávání statických obrázků nebo TXT pro neformátovaný text), jiné mohou sloužit jako kontejner pro uchovávání více druhů dat v jednom souboru (např. MKV – multimediální kontejner, který je schopen pojmout různá audio a video data) nebo může jít o balíčky určené pro archivaci nebo kompresi jakýchkoliv dat (např. ZIP – může obsahovat i více zkomprimovaných souborů a adresářů). Formát souboru lze rozeznat několika způsoby. Tím nejjednodušším je rozeznávání podle přípony souboru. Soubory mnoha operačních systémů obsahují příponu (text za tečkou v názvu souboru), pomocí jejíhož znění lze často rozeznat datový formát (.txt.jpg.docx apod.). Toto rozeznávání však mnohdy není příliš spolehlivé. Předně, některé operační systémy a aplikační software s příponami nepracují, a navíc lze příponu snadno změnit. Může k tomu dojít omylem nebo záměrně, když někdo chce například zastřít skutečný obsah souboru. Dále lze datový formát souboru rozeznat podle hlavičky souboru, která v některých typech obsahuje informaci o datovém formátu, nebo podle metadat, které k souboru umožňuje ukládat souborový systém datového úložiště. Stále častěji jsou pro identifikaci datového formátu souboru využívány takzvané MIME typy, kdy je mimo soubor (například v hypertextovém odkazu) uvedeno, jaký má zdrojový soubor mít formát.

Datový formát souboru je důležité znát při analýze elektronických stop proto, aby bylo možné zvolit vhodný technický nástroj pro přístup k obsaženým informacím. Pro mnoho datových formátů existuje specifikace, která popisuje, jak jsou v souboru data strukturována a jak k nim správně a bezztrátově přistupovat. Stále je však i mnoho datových formátů, které specifikaci nemají, ať už proto, že ji nikdo nevypracoval, nebo proto, že strukturu dat považuje tvůrce za svoje obchodní tajemství[127].

[127] To byl velmi dlouho případ formátů využívaných nativně kancelářským balíkem MS Office – jejich soubory DOC, XLS a podobně neměly dostupnou specifikaci. Proto open source kancelářské balíky dokázaly zobrazovat tyto soubory pouze omezeně, neboť byly závislé na reverse engineeringu samotných souborů.

Některé datové formáty dokáže bez problému zpracovat velké množství různých aplikací, neboť jsou velmi dobře známé nebo zdokumentované nebo obsahují jednoduše strukturovaná a snadno dostupná data. Jiné, především složité a nedokumentované datové formáty je naopak možné zpracovat jen prostřednictvím nativní aplikace, která původní soubor vytvořila. Při vytěžování důkazů z elektronických důkazních prostředků je proto vždy vhodné zajistit si adekvátní technické a programové vybavení pro plnohodnotné zobrazení konkrétních souborů. Mnohdy však může jít o velmi náročný úkol, který je nutné svěřit znalci, který provede plnohodnotnou forenzní analýzu souboru.

III.2.3 Šifrování

Šifrování je postup, kterým jsou data v čitelné podobě převedena do podoby nečitelné tak, aby bylo za pomoci klíče možné data převést zpět do čitelné podoby. Tento postup je využíván především k zajištění důvěrnosti dat, ke kterým má po jejich zašifrování přístup pouze držitel dešifrovacího klíče. Šifrování může být realizováno symetricky, kdy klíč, podle kterého se data šifrují, je stejný jako ten, který se využívá k jejich dešifrování, nebo asymetricky, kdy se uplatňuje veřejný klíč k zašifrování dat a privátní klíč, pomocí kterého lze data dešifrovat.

Jedná se nástroj, který je v současné době v oblasti informačních technologiích čím dál častěji využíván. Šifrování se uplatňuje různými způsoby. Lze například zašifrovat konkrétní soubory, celé datové nosiče nebo datovou komunikaci realizovanou mezi dvěma zařízeními. Pro šifrování jsou využívány různé algoritmy, kterých je poměrně velké množství. Různé typy šifrování pak poskytují různou míru zabezpečení. Některé algoritmy jsou slabé nebo zastaralé a dešifrování jimi zabezpečených dat je relativně jednoduché i bez dešifrovacího klíče. Jiné jsou velmi sofistikované a získání přístupu k jimi zabezpečeným datům je prakticky nemožné.

Šifrování tak představuje pro orgány činné v trestním řízení často poměrně zásadní překážku při využívání elektronických důkazů. Zajištěná data, která jsou zašifrovaná silným algoritmem, jsou při nedostupnosti dešifrovacího klíče prakticky nepoužitelná. Je-li algoritmus dešifrovatelný, mohou se orgány činné v trestním řízení pokusit o jejich dekrypci. V takovém

případě jsou zpravidla využívány služby znalce nebo je realizována kriminalistická expertiza. Pokud dekrypce bez klíče možná není, je nutné získat šifrovací klíč. Ten ale v ČR není podezřelý či obviněný povinen vydávat. Klíče však často lze získat i jinak, například mohou být uchovány v zajištěných zařízeních nebo na datových nosičích.

III.3 Nakládání s elektronickými důkazy

III.3.1 Zajišťování elektronických dat

Aby mohl být důkaz využit v trestním řízení, ať už ve prospěch nebo neprospěch obviněného, musí být zajištěn zákonnou cestou bez podstatných vad. Existence podstatné vady v procesním postupu orgánů činných v trestním řízení může totiž mít za následek absolutní nebo relativní neúčinnost důkazu. Takový důkaz pak nemůže být zohledněn při dokazování a je tudíž pro trestní řízení bezcenný.

Jelikož je trestní řád i přes velké množství jeho novelizací poněkud zastaralou normou, je třeba k zajišťování elektronických důkazních prostředků často využívat nepříliš vhodné procesní nástroje, jejichž úprava je kreativně vykládána tak, aby pokryla i případy elektronických důkazních prostředků trestním řádem nepředpokládaných.

Mnohdy je tak realizován postup v praxi netestovaný, respektive legislativně a judikatorně nezachycený, u kterého existuje riziko, že bude jeho prostřednictvím získaný důkaz pro potřeby trestního řízení nevyužitelný. Jasné limity nastavuje § 89 odst. 3 TŘ, podle nějž je absolutně nepřípustný takový důkaz, který byl získán nezákonným donucením. To se vztahuje jak na způsob získání zařízení či datových nosičů, tak i na získání samotných dat, ať už z jakéhokoliv zdroje. Důkazy však mohou být v trestním řízení absolutně či relativně neúčinné i z jiných důvodů – především v případě, že je orgánem činným v trestním řízení zvolen nevhodný procesní prostředek k zajištění elektronické stopy. To totiž může být vyhodnoceno jako podstatná vada postupu orgánů činných v trestním řízení, která způsobuje absolutní či relativní (pokud může být vada odstraněna) neúčinnost získaných důkazů.[128]

128 Srov. např. Musil, J., Kratochvíl, V., Šámal, P. *Kurs trestního práva: trestní právo procesní. 3. přeprac. a dopl. vyd.* Praha: C. H. Beck, 2007.

Za pomoci zkušeností z praxe a výkladu právní úpravy procesních nástrojů však zpravidla lze dojít k závěrům, jak různé typy elektronických důkazních prostředků zákonně zajišťovat tak, aby byly využitelné při dokazování.

K počítačovým datům se lze dostat v zásadě třemi základními způsoby:

- zajištěním zařízení nebo datových nosičů, na kterých jsou počítačová data uchovávána (počítače, datové nosiče, mobilní telefony apod.);
- získáním přímého přístupu k počítačovým datům uchovaným v počítačových systémech (volně dostupných, pomocí poskytnutých přístupů, pomocí přihlášeného zařízení, prostřednictvím překonání bezpečnostního opatření apod.);
- získáním počítačových dat od poskytovatelů služeb (např. uživatelských dat uchovaných u poskytovatele či provozních a lokalizačních údajů).

Zajištění zařízení a datových nosičů

Jednou z nejefektivnějších metod získání přístupu k zájmovým datům, která mohou obsahovat důkazy využitelné v trestním řízení, je zajištění zařízení nebo datového nosiče, na kterém jsou data přímo uchovávána.

Zajištění věci, za kterou je považován rovněž počítačový systém nebo nosič informací, je navíc i z procesního hlediska poměrně snadné, vztahuje se na ni totiž ediční povinnost vyplývající z ust. § 78 TŘ. Podle té má ten, kdo má u sebe věc důležitou pro trestní řízení, kterou je nutno zajistit, povinnost ji v přípravném řízení vydat na vyzvání státního zástupce nebo policejního orgánu. Takovou osobou nemusí být vlastník dané věci, ale může jí být kdokoliv, kdo ji má u sebe, tedy například provozovatel server housingu, poskytovatel služby, zaměstnavatel apod. Držitel věci rovněž musí být poučen o následcích neuposlechnutí výzvy k vydání věci. Pokud jí přesto nevyhoví, může mu být kromě uložení pořádkového opatření předmětná věc na základě rozhodnutí státního zástupce či policejního orgánu (po předchozím souhlasu státního zástupce) i odňata. Odnětí věci by měla být přítomna nezúčastněná osoba a o celém úkonu (vydání i odnětí) musí být pořízen protokol, ve kterém bude detailně zachyceno, jaká věc byla zajištěna (včetně popisu příslušenství), a to tak, aby taková věc nemohla být zaměněna za jinou. Rovněž musí být osobě, která věc vydává, nebo které je věc odňata,

vystaveno potvrzení, případně jí musí být poskytnut opis protokolu, do kterého je třeba splnění této povinnosti zachytit.

Vydání i odnětí věci je do určité míry omezeno v § 78 odst. 2 TŘ, podle kterého takto nemůže být zajištěn dokument, jehož obsah se týká okolnosti, o které platí zákaz výslechu (utajované informace podle zákona č. 412/2005 Sb. nebo informace, pro které platí státem stanovená nebo uznaná mlčenlivost – osobní údaje, advokátní data apod.). Neznamená to však například, že by takto vůbec nemohl být zajištěn datový nosič nebo zařízení, které takové dokumenty obsahuje podle tvrzení povinné osoby. Shodně se vyjádřil i Ústavní soud když konstatoval, že by existenci takového dokumentu měl zjistit sám orgán činný v trestním řízení při zkoumání zajištěných dat ve spolupráci se znalcem, s odvoláním na znění § 2 odst. 5 TŘ. [129]

Zařízení nebo nosiče informací obsahující zájmová data je možné také zajišťovat v rámci domovní prohlídky nebo prohlídky jiných prostor. Oba typy prohlídek je oprávněn nařídit předseda senátu a v přípravném řízení na návrh státního zástupce také soudce. Jde o rozhodnutí *sui generis*, proti kterému není přípustné odvolání. Samotný příkaz musí být písemný a odůvodněný. Podobně jako při vydání a odnětí věcí je třeba při prohlídkách provádět zajištění zařízení a nosičů s náležitou odbornou péčí a protokol, který musí být při prohlídce pořízen, by měl obsahovat detailní technickou specifikaci nejen zajištěných věcí, ale i postupu příslušného orgánu. I z toho důvodu by měly takové prohlídky probíhat za účasti náležitě vyškoleného vyšetřovatele nebo znalce.

Praktický postup při zajišťování zařízení a datových nosičů by měl respektovat požadavky na zdrženlivost a přiměřenost orgánů činných v trestním řízení, zakotvených v § 2 odst. 1 a § 52 TŘ, na straně jedné a požadavky na efektivní a bezpečné zajištění důkazního materiálu, vycházející z vlastností dat a zařízení popsaných výše, na straně druhé. Je-li zajišťován samostatný datový nosič nepřipojený k zařízení nebo vypnuté zařízení, pak je postup relativně jednoduchý. Tyto věci se náležitě identifikují do protokolu a zapečetí do antistatického vaku. Zařízení by měla být zajišťována tak, aby přístup k datům v nich uchovaným v budoucnu mohl mít jako první znalec. Proto je vhodné zapečetit veškerá rozhraní zařízení nebo rovnou zařízení vložit

129 Viz usnesení Ústavního soudu sp. zn. IV. ÚS 2/02, U 11/25 SbNU 385.

do vaku nebo boxu umožňujícího zapečetění. Pokud však policejní orgán zajišťuje zařízení, které je v provozu, je postup poněkud komplikovanější. Odpojením a vypnutím zařízení by totiž mohlo dojít nejen ke ztrátě některých dat, ale i ke ztrátě přístupu k datům dostupným na vzdáleném úložišti, nebo dokonce ke ztrátě přístupu k datům v zařízení, která jsou zašifrována. Před odpojením zařízení by tedy mělo dojít k protokolovanému ohledání věci dle § 113 TŘ, v rámci kterého bude ověřeno, zda je zařízení zabezpečeno šifrováním, zda je jeho prostřednictvím možný přístup do vzdálených služeb nebo zda neexistuje nějaká jiná překážka, která by mohla bránit úspěšné forenzní analýze zařízení. V průběhu ohledání je vhodné pořídit fotodokumentaci nebo videozáznam a přiložit je k pořízenému protokolu.

Po ohledání je třeba zařízení zajistit takovým způsobem, aby nemohlo dojít ke kompromitaci dat jejich smazáním nebo úpravou. Měly by proto být odpojeny veškeré periferie, zařízení by mělo být kompletně vypnuto a zapečetěno do antistatického vaku. Je-li to možné, je rovněž vhodné zajišťovat celá zařízení, nikoliv pouze demontovaná datová úložiště nebo bitové kopie dat. Jejich zpřístupnění totiž může být na zařízení vázáno (např. využitím TPM čipu). Tento postup však nelze volit vždy. Kdyby zajištění zařízení mělo představovat neodůvodněný zásah do základních práv a svobod jejich držitele, je vhodné provést toliko ohledání nebo zajistit pouze otisky datových nosičů. Vždy je třeba brát v úvahu specifika a okolnosti konkrétního případu a vzít v úvahu možnost následného využití institutů vydání a odnětí věci.

Získání přístupu ke vzdáleným datům

Druhým způsobem, kterým lze získat elektronické důkazy, je získání dat ze vzdálených úložišť nebo služeb. To lze opět provést několika způsoby.

Prvním a nejjednodušším způsobem je získání informací volně dostupných v síti. Není-li překonáváno žádné bezpečnostní opatření, lze v podstatě bez dalšího přistupovat k obsahu dostupnému v prostředí Internetu a pořizovat z něj důkazní prostředky. Je třeba dodržovat pravidla stanovená pro ohledání věcí dle § 112 TŘ – především sepsat důkladný protokol. Při zajišťování je však rovněž třeba mít na vědomí specifické vlastnosti elektronických dat a dynamické fungování internetu. Především by měla být pořizována vhodná dokumentace. Například při ohledání webové stránky sice

lze dokumentaci pořizovat v podobě fotografií nebo printscreenů, nicméně tak nedojde k zajištění maximálního možného množství důkazního materiálu, proto lze doporučit s ohledem na dynamičnost webu rovněž uchování zdrojového kódu stránky.

K datům, která nejsou volně dostupná v síti, lze získat přístup prostřednictvím přístupových údajů poskytnutých dobrovolně ať už při výslechu, během podání vysvětlení nebo jiným způsobem.

Jelikož jde v tomto případě o data volně nedostupná a tedy nějakou formou zabezpečená, je nutné je považovat za písemnosti a záznamy uchovávané v soukromí ve smyslu ustanovení o operativním pátracím prostředku sledování osob a věcí v § 158d odst. 3 TŘ. K obsahu takových dat mohou orgány činné v trestním řízení přistupovat jen na základě předchozího povolení soudce, nebo pokud s tím výslovně souhlasí ten, do jehož práv a svobod je tím zasahováno (§ 158d odst. 6 TŘ). Mají-li navíc taková data být využita jako důkaz v trestním řízení, je nutné o jejich pořízení sepsat řádný protokol. Ten by měl obsahovat i informaci o tom, jak orgán činný v trestním řízení přístup získal, a výslovný souhlas osoby jej poskytující.[130]

Získávají-li však orgány činné v trestním řízení přístupové údaje jiným způsobem (např. nálezem, uložené na zajištěném zařízení apod.), od jiné osoby než té, do jejíchž práv a svobod má být zasahováno, nebo chtějí-li přistupovat k takovým datům po překonání technického bezpečnostního opatření, jde o poměrně zásadní zásah do práv a svobod, pro takový případ je proto stanoven poměrně vysoký standard kontroly. Je především nutný souhlas soudce získaný na základě písemné žádosti dle § 158d odst. 3 TŘ. Nesnese-li věc odkladu, může k datům přistoupit policejní orgán i bez souhlasu, o který je ale povinen dodatečně požádat. Pokud na základě této žádosti neobdrží ani dodatečný souhlas do 48 hodin, musí pořízená data zničit. I v tomto případě platí, že mají-li být získaná data využita při dokazování, je nutné pořídit protokol.

Poslední variantou, jak získat přístup k datům vzdáleně zabezpečeně uchovaným, je prostřednictvím zařízení, které je k přístupu způsobilé. Typicky může jít o počítače, mobilní telefony, tablety či jiná zařízení, ve kterých jsou uchovány přístupové údaje ke službě nebo které jsou ke službě připojeny (např. dlouhodobě prostřednictvím nainstalovaného klienta nebo cookies prohlížeče).

130 Shodně nález Ústavního soudu sp. zn. III. ÚS 3844/13.

V případech, kdy jsou na zajištěném zařízení toliko uchovány přístupové údaje, je situace stejná, jako když jsou tyto údaje získány jinak, a aplikuje se tedy ustanovení § 158d TŘ o sledování věcí popsané výše.

Zdánlivě se tato situace neliší od situace, kdy je ke vzdálené službě zařízení připojeno. Existuje však i jiný výklad, vycházející ze specifického chápání pojmu počítač, resp. počítačový systém ve výkladu k § 230 TZ[131], který počítačový systém chápe jako: *„[…] jakékoli zařízení nebo skupina vzájemně propojených nebo souvisejících zařízení, z nichž jedno nebo více provádí na základě programu automatické zpracování dat. […] Pojem počítač je někdy používán jako synonymum počítačového systému.“*[132]

Je-li takto z hlediska trestního práva chápán obsah pojmu počítač, mohl by být obsah propojených zařízení (cloudového úložiště, nebo služby) považován za jeho součást. Přístup k takovým datům by tak byl možný bez dodatečného povolení v rámci přístupu k počítačovému systému zajištěnému v souladu se zákonem (postupem dle § 78, § 79, § 82, nebo § 113 TŘ). S tímto velmi extenzivním výkladem pojmu počítač se však neztotožňujeme, a přístup ke vzdálené službě připojené k zajištěnému zařízení doporučujeme realizovat teprve na základě souhlasu soudce získaného v souladu s ust. § 158d odst. 3 TŘ, neboť nepochybně jde o samostatný přístup do soukromého virtuálního prostoru.

Specifické postavení mají data, která nejsou staticky uchovávána prostřednictvím vzdálené zabezpečené služby nebo úložiště, ale která jsou nebo byla předmětem elektronické komunikace, tedy například data z e-mailu či chatovacích a komunikačních služeb (Skype, ICQ, Viber, Google Hangouts, Facebook Messenger apod.). Podle výkladového stanoviska Nejvyššího státního zastupitelství č. 1/2015[133] je totiž nutné zajišťovat elektronickou komunikaci v reálném čase jen v rámci odposlechu a záznamu telekomunikačního provozu postupem podle § 88 odst. 1 TŘ, neboť se tato stejně

131 S tímto stanoviskem jsme se setkali na několika odborných konferencích věnujících se problematice zajišťování elektronických důkazních prostředků.

132 Viz výklad k § 230 v Šámal, P. Trestní zákoník II. § 140 až 421. Komentář. 2. vydání Praha: C. H. Beck, 2012.

133 Výkladové stanovisko Nejvyššího státního zastupitelství č. 1/2015, ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek. Dostupné z http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2015/1_SL_760-2014.pdf.

jako telekomunikační provoz uskutečňuje v sítích elektronických komunikací a jde o obsahová data. Současně dle citovaného stanoviska platí, že jednorázové zajištění dat obsažených ve schránkách komunikačních nástrojů se provádí prostřednictvím operativně pátracího prostředku sledování věci dle § 158d odst. 3 TŘ, neboť taková data mají charakter záznamů uchovávaných v soukromí. Komplikovanější situace nastává v případě, že daná služba zahrnuje zároveň funkce úložiště i komunikačního prostředku. V takové situaci je třeba aktuálně přítomná data zajistit postupem dle § 158d odst. 3 TŘ a další sledování komunikace s účtem realizovat dle § 88 TŘ. Příkladem takové služby může být například Facebook - při prvním přístupu do služby dojde k zajištění již přítomných dat, pokud však existuje zájem na dalším zajišťování údajů o komunikaci příslušné virtuální identity, je třeba postupovat podle právní úpravy odposlechu a záznamu telekomunikačního provozu.

Získání dat od ISP

Data, která mohou být neocenitelným zdrojem důkazů v trestním řízení, mohou být získávána také přímo od poskytovatelů informačních služeb. Při volbě procesního nástroje, prostřednictvím kterého budou data zajišťována, je z hlediska trestního procesu zohlednit dvě základní hlediska.

Prvním hlediskem je charakter poskytovatele, od kterého data žádáme. Poskytovatelé informačních služeb se totiž dají rozdělit na dvě základní skupiny. Na poskytovatele telekomunikačních služeb dle zákona č. 127/2005 Sb., o elektronických komunikacích a na poskytovatele služeb informační společnosti dle zákona č. 480/2004 Sb., o některých službách informační společnosti. Poskytovatelem telekomunikačních služeb myslíme podnikatele zajišťujícího veřejnou komunikační síť nebo poskytujícího veřejně dostupnou službu elektronických komunikací ve smyslu ZEK, tedy subjekty, které provozují infrastrukturu veřejné komunikační sítě nebo které poskytují připojení k takové síti. Poskytovatelem služeb informační společnosti je pak subjekt, který elektronickými prostředky (prostřednictvím sítě elektronických komunikací) zpravidla úplatně poskytuje jakoukoliv službu na individuální žádost uživatele podanou elektronickými prostředky. Pod tuto poměrně

širokou definici spadají v podstatě všechny služby poskytované na internetu, které pracují s uživatelskými daty – e-mailové služby, sociální sítě, hostingy, diskusní servery, filehostingy, cloudové služby, vyhledávače apod.

Druhým zmiňovaným hlediskem je charakter dat. Různá data totiž podléhají různé míře ochrany, a je tedy nutné volit i různé procesní nástroje. Podle charakteru se pak data uživatelů zpracovávaných poskytovateli informačních služeb dělí především na obsahová data, která během využívání služby vložil uživatel, obsahová data o komunikaci uživatele či provozní a lokalizační údaje a různá jiná metadata.

Jsou-li od poskytovatele služby vyžadována data neobsahující informace, která jsou předmětem povinnosti mlčenlivosti, lze je vyžádat při využití institutu dožádání upraveného v § 8 odst. 1 TŘ. Podle něj je kdokoliv povinen bez zbytečného odkladu a, nestanoví-li zvláštní předpis jinak, bez úplaty vyhovovat dožádáním orgánů činných v trestním řízení při plnění jejich úkolů. Tímto postupem lze získat různá data, například obsahová, která uživatel zveřejnil, informace o uživatelských účtech, logy zaznamenávané poskytovatelem, na něž se nevztahuje telekomunikační tajemství, informace o fungování služby, různá metadata apod. Kromě toho lze tímto způsobem získávat i data, která mají podobný charakter jako provozní a lokalizační údaje, ale nejsou dožadována od poskytovatele telekomunikačních služeb dle ZEK. Taková data ale nesmějí obsahovat například osobní údaje nebo utajované informace podle zvláštních zákonů. Plnění této povinnosti totiž povinná osoba může odmítnout pouze s odkazem na povinnost zachovávat tajnost utajovaných informací nebo státem uloženou nebo uznanou povinnost mlčenlivosti.

Pokud jsou od poskytovatele vyžadována data, která uživatel uchovává ve službě zabezpečené nějakým bezpečnostním opatřením (typicky jménem a heslem), pak mají tato data charakter záznamů uchovávaných v soukromí a při přístupu k nim je třeba postupovat podle § 158d odst. 3 TŘ popsaného výše.

Specifické postavení mají provozní a lokalizační údaje ve smyslu § 90 a 91 ZEK. Jde o údaje zpracovávané pro potřeby přenosu zprávy sítí elektronických komunikací nebo pro její účtování a údaje zpracovávané v síti elektronických komunikací nebo službou elektronických komunikací, které

určují zeměpisnou polohu telekomunikačního koncového zařízení uživatele veřejně dostupné služby elektronických komunikací. Tyto údaje má poskytovatel telekomunikačních služeb za podmínek stanovených v ZEK povinnost po určitou dobu uchovávat. K těmto údajům lze přistupovat za specifických podmínek upravených v § 88a TŘ nařídí-li jejich vydání soudce na žádost státního zástupce. Tohoto nástroje je však možno využít jen při stíhání vyjmenovaných trestných činů a je-li dosažení sledovaného účelu jinak ztížené nebo znemožněné.[134]

Jiné ochrany požívají data, která jsou obsahem telekomunikačního provozu (obsahová data komunikovaná prostřednictvím sítí elektronických komunikací) – na ně se totiž váže takzvané telekomunikační tajemství. Odposlech neboli zachytávání takových dat během jejich přenosu je možný jenom za podmínek stanovených v § 88 TŘ. Stejně jako v předchozím případě lze tento procesní nástroj využít toliko při stíhání vyjmenovaných trestných činů a je-li dosažení sledovaného účelu jinak ztížené nebo znemožněné. Je zde rovněž vyžadováno nařízení soudce na návrh státního zástupce. Podle ustanovení o odposlechu je dle výše citovaného výkladového stanoviska NSZ č. 1/2015 nutno postupovat i při zajišťování dat o komunikaci uživatelů služeb informační společnosti do budoucna.[135]

Specifickým postupem, který mohou orgány činné v trestním řízení vůči ISP uplatňovat, je dožádání zachování dat. Díky charakteru dat a vlastnostem služeb na internetu může být vyšetřování trestného činu snadno zmařeno nedostatečnou pružností orgánů činných v trestním řízení, neboť zájmová data mohou být pachatelem velmi snadno a rychle zlikvidována. Některé procesní nástroje však předpokládají určitý procesní postup, který nějakou dobu trvá, a během této doby může dojít ke smazání předmětných dat. Proto může policejní orgán formou prostého dožádání dle § 8 odst. 1 uložit provozovateli služby, aby u sebe uchovával zálohu dat uživatele (i těch, které uživatel smaže) až do doby, než bude rozhodnuto soudcem o povolení přístupu k nim. Využívá-li například pachatel e-mailovou schránku jako zápisník, do kterého ukládá údaje o svojí trestné činnosti, a policie chce tyto

134 K problematice data retention více viz kapitola VII níže.
135 Tato problematika je opět detailněji popsaná v kapitole VIII níže.

údaje pro potřeby vyšetřování získat, musí žádat o povolení soudu ve smyslu § 158d odst. 3 TŘ. Aby nedošlo ke ztrátě těchto dat, může policejní orgán operativně uložit provozovateli služby, aby uchoval zálohu takových dat.

III.3.2 Analýza dat

Získání elektronických důkazních prostředků je teprve prvním krokem v procesu dokazování prostřednictvím elektronických dat. Data jako taková mají díky svému charakteru jen minimální vypovídací hodnotu. Teprve ve chvíli, kdy jsou interpretována na informace, je možné začít hovořit o důkazu. Vzhledem k vlastnostem dat a elektronických zařízení je, jak je naznačeno výše, poměrně technicky náročné nejen vyhodnocovat jejich informační obsah, ale mnohdy jej i v množství dat identifikovat. K těmto úkonům lze nicméně využívat více či méně technicky sofistikované nástroje pro forenzní analýzu.

Důkazy lze z elektronických důkazních prostředků tedy získat mnoha způsoby a jejich volba se bude odvíjet od technických vlastností předmětného důkazního prostředku, schopností a zkušeností vyšetřovatele či znalce, od jejich technického vybavení a pochopitelně i od konkrétních skutkových okolností. Je pochopitelně nesmysl využívat služeb znalce, je-li například potřeba toliko zachytit jako důkaz obsah volně dostupné webové stránky, takový postup by totiž byl nejen zbytečně komplikovaný, ale také velmi neekonomický. Možnosti analýzy jsou také závislé na způsobu zajištění elektronického důkazního prostředku. Je-li realizován nesprávně, může dojít k technickému znehodnocení dat nebo k jejich kompromitaci, proto lze naopak doporučit v případech, ve kterých to vyžadují okolnosti, přizvat znalce i například k domovní prohlídce nebo odnětí věci.

Prvním a patrně nejběžnějším způsobem, jak je z dat v elektronickém zařízení získáván důkazní materiál, je prosté ohledání elektronického zařízení a dat v něm pomocí vstupních a výstupních komponent zařízení, v případě počítače například pomocí klávesnice, myši, monitoru, případně tiskárny. Stejně tak lze ohledat data dostupná online, například prostřednictvím počítače vyšetřovatele. Vyšetřovatel při ohledání v takových případech v podstatě běžným způsobem zachází se zařízením a využívá jeho vestavěných funkcionalit k seznámení se s jeho informačním obsahem. Tento postup je pak

zachycen do protokolu, který je opatřen průvodní dokumentací v podobě fotografií či výtisků a následně slouží jako listinný důkaz. Výhody tohoto postupu jsou zřejmé – je velmi rychlý, nenáročný na organizaci, zařízení nemusí být zajištěno a není třeba žádných dodatečných technických analytických pomůcek. Nevýhodou je naopak snížená důkazní síla takto pořízeného důkazu. Vzhledem k technickému charakteru zařízení může totiž docházet ke znehodnocování dat v něm uložených, lze navíc z mnoha důvodů vycházejících z vlastností počítačových systémů napadat věrohodnost takto získaného důkazu. Z těchto důvodů je při využití tohoto postupu nutné pořizovat skutečně detailní a kvalitně zpracovanou dokumentaci. Druhá nevýhoda spočívá v tom, že takto prostou analýzou mohou být přehlédnuty informace, které mohou být pro výsledek trestního řízení klíčové. Data totiž lze mnoha způsoby maskovat či skrývat a jejich dohledání je pak možné jen za využití sofistikovaných nástrojů a postupů.

Data jako důkazní prostředky ale nabízí také jednu zásadní výhodu. Dají se totiž v podstatě v neomezené míře pořizovat jejich bezztrátové kopie. Je-li tedy k analýze k dispozici zařízení nebo nosič obsahující data, je možné je extrahovat tak, že se vytvoří jejich kopie. Při analýze takto extrahovaných dat pak nedochází k jejich modifikaci ani znehodnocování na zdrojovém zařízení. Extrakce se zpravidla provádí standardním využitím funkcionalit systému či na něm instalovaných aplikací – především vykopírování souborů. Výhodou je, že takto dojde k získání celého obsahu dostupných dat, ze kterého pak mohou být efektivněji získávány například skryté informace nebo informace na první pohled a prostřednictvím na zařízení dostupných aplikací nedostupné. Nevýhodou je, že ani při tomto postupu nejsou získávána úplně všechna data, ale pouze ta, která jsou dostupná spuštěnému systému nebo aplikačnímu software. Například na pevném disku počítače může však být mnohem více dostupných dat – smazaná data nebo data ve skrytých oddílech disku. Taková data jsou zajištěna pouze, pokud je pořízena bitová kopie celého úložiště. K tomu jsou využívány speciální forenzní pomůcky – hardwarové i softwarové. Může jít například o k tomu vybavený počítač, ke kterému se připojí pevný disk demontovaný ze zkoumaného

přístroje, spustí se v režimu čtení a vykopírují se z něj veškerá dostupná data. Rovněž se provede kontrolní součet nad obsahem disku, aby bylo možné prokázat, že v průběhu extrakce nedošlo k žádnému zásahu do dat.

Takto extrahovaná zařízení mohou být analyzována vyšetřovatelem, nicméně aby byla zachována co nejvyšší důkazní síla získaného důkazu, měl by následnou analýzu dat provádět odborník. Proto bývají pro tyto účely využíváni znalci, kteří na základě stanovených otázek k posouzení vyhotoví znalecký posudek, jenž se později u soudu provádí jako listinný důkaz.

Podle ustanovení § 105 odst. 1 TŘ rozhodne orgán činný v trestním řízení o přibrání znalce, je-li k objasnění skutečností důležitých pro trestní řízení třeba odborných znalostí, případně je možné v jednodušších případech vyžádat odborné vyjádření. V případech analýzy elektronických důkazních prostředků se přistupuje k přibrání znalce poměrně často, neboť jsou vyžadovány odborné znalosti, většinou v oboru kybernetika – výpočetní technika. Mnohdy je rovněž znalec přibrán k úkonům popsaným výše, neboť jeho odborné znalosti a vybavení může být nutné pro úspěšné a účelné zajištění důkazních prostředků či informací o technickém charakteru ohledávaného zařízení.

Nejčastějším způsobem využití služeb znalce je však vypracování znaleckého posudku, ve kterém se znalec vyjadřuje k otázkám, které mu zadavatel (zpravidla orgán činný v trestním řízení) pokládá, přičemž se znalec vyjadřuje pouze k technické stránce věcí – důkazy nehodnotí ani se nevyjadřuje k otázkám právním. Zpravidla jsou znalci zadány takové otázky, které směřují k technickému charakteru dat a k jejich obsahu. Často se tak znalec vyjadřuje k hardwarovému či softwarovému vybavení počítače, k existenci určitých zájmových dat na úložišti, ke spolehlivosti a identifikaci zajištěných dat či k vlastnostem zařízení a sítí.

Ani využití znaleckých posudků jako prostředků k provádění elektronických důkazů však není bezproblémové. Předně, znalci svoje služby poskytují úplatně, a jelikož je k jejich vykonávání nejen v oblasti informačních a komunikačních technologií často třeba velmi drahého a komplikovaného vybavení, i náklady znalce jsou vysoké. Není tudíž ekonomicky možné služeb znalců

využívat u každého elektronického důkazu. Nejen že by to bylo nákladné, ale znalců navíc není tolik, aby mohli pokrýt rostoucí poptávku po znaleckých posudcích v případě dokazování elektronickými důkazy.

Dalším problémem je přinejmenším v oboru kybernetika - výpočetní technika právní úprava znalecké činnosti zachycená v zákoně o znalcích a tlumočnících. Ten totiž na osoby znalců i na znaleckou činnost klade velmi mírné požadavky. Znalcem může být dle § 4 ZnalZ jmenován kdokoliv, kdo je českým občanem (1), má potřebné zkušenosti v oboru (2), absolvuje speciální výuku, je-li stanovena (3), má osobní předpoklady pro výkon znalecké činnosti (4) a se svým jmenováním souhlasí (5). O jmenování znalce rozhoduje ministr spravedlnosti nebo předseda krajského soudu, kteří však nemají k dispozici žádný aparát ani kontrolní mechanismus, který by jim umožňoval posoudit, zda je splněna podmínka absolvování speciální výuky. Odborná kvalifikace znalců je tak často zajištěna jen do určité míry, což má mnohdy za důsledek vznik znaleckých vyjádření a posudků s vpravdě tristní kvalitou. Ač jsou možnosti měření kvality znaleckých posudků velmi omezené a nejsou k dispozici ani solidní studie, které by tuto tezi podporovaly, ozývá se stále více hlasů, které kvalitu znaleckých posudků a potažmo znalců kritizují.[136] S tímto poznatkem příliš nekoresponduje to, že k odvolání nedostatečně odborně vybavených znalců dochází velmi zřídka[137], ani to, že soudy přistupují k obsahu znaleckých posudků často poměrně nekriticky.

Do určité míry by mohl tyto problémy řešit nový zákon o znalcích, jehož věcný záměr počítá se stanovením kvalifikačních předpokladů podle oborů a rovněž s povinnými vstupními testy. Domníváme, se že by mohlo pomoci větší zapojení oborových organizací, především Komory soudních znalců, která by mohla kvalitu znalců na základě zákonného zmocnění garantovat.

III.3.3 Provádění a hodnocení elektronických důkazů

Aby mohly být elektronické důkazy využity ke svému účelu a poskytnout soudu informace důležité pro trestní řízení, musí být před soudem

136 Zde vycházíme ze zkušenosti autorů. Kvalita znaleckého zkoumání je často kritizována i samotnými znalci. Srov. např. Tiskový odbor MSp. Rozhovor: Deset otázek k připravovanému zákonu o znalcích a tlumočnících. Dostupné z http://www.pravniprostor.cz/clanky/ostatni-pravo/k-deset-otazek-k-pripravovanemu-zakonu-o-znalcich-a-tlumocnicich.

137 Musil, J. Hodnocení znaleckého posudku. *Kriminalistika*, 2010, č. 3.

provedeny. Díky výše zmíněným specifikům dat je provádění elektronických důkazů poněkud problematické. Elektronické důkazy jsou obvykle provedeny jako listinné či věcné důkazy dle § 112 TŘ, to však není vždy možné. Nelze si dost dobře představit, že by před soudem byl bez dalšího proveden důkaz například zdrojovým kódem. U náročnějších typů elektronických důkazů je proto často dle § 105 TŘ vyžádáno odborné vyjádření, které může poskytnout kdokoliv s potřebnými odbornými předpoklady[138]. Jelikož mají státní orgány na rozdíl od soukromníků povinnost poskytovat odborná vyjádření bezúplatně, jsou k tomuto účelu často využíváni příslušníci Policie ČR. Jestliže není odborné vyjádření díky komplexitě elektronického důkazu dostačující, může být dle § 105 TŘ rovněž přibrán znalec.

Určitou překážkou při provádění elektronických důkazů v řízení před soudem může do budoucna být technická vybavenost soudů. Některé druhy elektronických důkazů není snadné zachytit vytisknutím na papír nebo popsáním do protokolu. Vzhledem ke specifikům elektronických důkazů navíc dochází při tisku mnohdy ke ztrátě podstatných informací. Domníváme se proto, že bude stále více růst tlak na to, aby bylo v trestních řízeních možné provádět elektronické důkazy bezprostředně. Informace z datových struktur, obsahy cloudových služeb či počítačové simulace apod. by mohly být provedeny přímo před soudem, a ne zprostředkovaně prostřednictvím listinných důkazů nebo znaleckých posudků.

V současné době jsou však služby znalce při dokazování elektronickými důkazními prostředky nezastupitelné.

Pro hodnocení elektronických důkazů je rozhodující možnost jejich ztotožnění, respektive spojení označené osoby s obsahem elektronického důkazu. Ať již jde o vytvořený dokument, zaslaný e-mail, provozní a lokalizační údaje nebo obsahová data z komunikace, je vždy nutné ztotožnit zdroj těchto dat. Zpravidla je proto třeba spojit data s konkrétním zařízením a následně zařízení s konkrétním uživatelem. Judikatura[139] se ve složitějších případech zpravidla spoléhá na další podpůrné nepřímé důkazy, které ve své kombinaci svědčí o ztotožnění elektronického důkazu. V závislosti na typu

138 Často se pro tyto účely využívá služeb znalců nebo uznávaných autorit v oboru, např. odborníků z akademické sféry.

139 Viz např. usnesení Nevyššího soudu sp. zn. 5 Tdo 1136/2014.

elektronického důkazu může být takových podpůrných důkazů celá řada, nejčastějšími však patrně budou provozní a lokalizační údaje, různá metadata, znalecké posudky, elektronické podpisy, svědecké výpovědi nebo faktické okolnosti konkrétního případu.

V případě dokumentu zaslaného prostřednictvím komunikačního protokolu uchovávaného na zajištěném zařízení, lze z metadat dokumentu zjistit dobu jeho vytvoření nebo uložení v zajištěném zařízení, následně vyžádat provozní a lokalizační údaje vztahující se k zařízení a na jejich základě je možné identifikovat odesílající zařízení. Pokud je odesílající zařízení zabezpečeno tak, že k němu má přístup jen jedna osoba, lze odesílatele identifikovat na základě takové faktické okolnosti. Jinak lze rovněž odesilatele ztotožnit pomocí svědecké výpovědi svědka, který odesílatele viděl v době určené pomocí provozních a lokalizačních údajů pracovat se zařízením. Je-li dokument opatřen zaručeným, nebo uznávaným elektronickým podpisem, lze autora ztotožnit přímo prostřednictvím něj. Eventuálně lze využít služeb znalce, který z obsahu dokumentu pomocí nástrojů forenzní lingvistiky identifikuje autora.[140] Způsobů a kombinací způsobů je tak poměrně rozsáhlé množství a záleží především na schopnostech a zkušenostech vyšetřovatele, do jaké míry je schopen tyto podpůrné důkazy kombinovat.

III.4 Shrnutí kapitoly

Tato kapitola byla věnována otázce využití počítačových dat jako důkazu v trestním řízení. Jelikož je stále více informací zpracováváno prostřednictvím výpočetní techniky ve formě dat, stále častěji musí orgány činné v trestním řízení nakládat s daty, které jsou cenným zdrojem důkazního materiálu. Vzhledem k historickému vývoji trestního práva procesního však tyto orgány často pracují se zastaralou právní úpravou a naráží tak na limity procesních nástrojů trestního práva k práci s důkazy.

Máme-li se bavit o datech jako důkazu v trestním řízení, je třeba se nejdříve zabývat jejich zdroji, povahou a vlastnostmi. Proto byla v této kapitole první část textu věnována zařízením, která mohou sloužit jako zdroj dat. Ta

140 Konkrétnější postupy jsou zpracovány v následujících kapitolách.

v první řadě shrnula, jaká zařízení jsou být využitelná jako zdroj důkazního materiálu, jaká je jejich technická charakteristika, jaké mají funkce a především jaké kategorie dat z nich lze získávat.

Následně se text zabýval charakterem dat jako předmětu dokazování v trestním řízení. Byl zohledněn především jejich technický charakter a z něj vyplývající limity a praktické překážky, se kterými se při dokazování daty v trestním řízení můžeme setkat. V neposlední řadě se výklad věnoval rovněž právní povaze dat z hlediska dokazování v trestním řízení.

Následující části kapitoly se pak věnovaly konkrétním procesním nástrojům trestního práva využívaným při zpracování dat jako důkazního materiálu. První podstatnou otázkou je, jak data vlastně vhodně zajistit. Jak bylo z výkladu patrné, je k tomuto účelu možné využít hned několik procesních nástrojů, jejichž volba bude především záležet na tom, z jakého zdroje mají být elektronické důkazy získány. Jinak je totiž třeba postupovat při zajištění dat uchovaných na nosiči, nebo zařízení, jinak při zajištění dat uchovaných ve vzdálených úložištích „svépomocí" nebo za součinnosti ISP. V podstatě ve všech případech jsou však v podstatě „ohýbány" existující procesní nástroje pro potřeby získání konkrétních dat, neboť specializovaný prostředek jednoduše neexistuje. Dále byla diskutována problematika analýzy zajištěných dat za účelem získání důkazů a jejích praktických a technických specifik, a především otázka znaleckého zkoumání a jeho nedostatků. Poslední část kapitoly je pak věnována provádění a hodnocení elektronických důkazů a především problematice jejich ztotožňování. Velmi palčivým problémem totiž je i při kvalitním zajištění elektronického důkazu spojit jej s konkrétním pachatelem.

Tato kapitola slouží jako úvod, který si klade za cíl shrnout základní technické a právní poznatky související s využíváním elektronických důkazů v trestním řízení. Následující kapitoly pak detailněji probírají specifické kategorie elektronických důkazů, se kterými praxe nejčastěji pracuje.

IV DOKAZOVÁNÍ E-MAILEM

IV.1 Vysvětlení pojmu

IV.1.1 E-mail – pojem

Pro způsob odesílání, doručování a přijímání zpráv mezi uživateli počítačů přes elektronické komunikační systémy, tedy pro elektronickou poštu, se vžil zkrácený výraz e-mail. V dnešní době zdaleka nejde pouze o textové soubory, neboť přílohou e-mailu může být v podstatě jakýkoliv datový soubor, pokud to jeho velikost dovoluje. Zákon elektronickou poštu definuje jako textovou, hlasovou, zvukovou nebo obrazovou zprávu poslanou prostřednictvím veřejné sítě elektronických komunikací, která může být uložena v síti nebo v koncovém zařízení uživatele, dokud ji uživatel nevyzvedne.[141]

Ačkoliv elektronická pošta svým pojmem a většinou i grafickým ztvárněním evokuje podobnost s fyzickými poštovními zásilkami, ve skutečnosti má s poštou v tradičním slova smyslu čím dál méně společného. Této iluze, vytvořené pro lepší pochopení a pohodlí uživatelů, se doposud víceméně držela i judikatura, avšak dříve nebo později bude třeba, aby opustila klidné vody „poštovních schránek" a hovořila výhradně o počítačovém systému, nosičích informací a elektronických komunikacích. Avšak vzhledem k tomu, že elektronická pošta svou základní myšlenkou vychází z dopravování tradičních poštovních zásilek, některé podobnosti zde zůstávají.

Elektronická pošta se uskutečňuje prostřednictvím veřejné komunikační sítě, a přestože technicky prochází cizími počítači předtím, než dosáhne cíle, jde o soukromou komunikaci mezi konkrétními a předem určenými subjekty. Jedná se o komunikaci důvěrnou[142], přičemž ochrany požívá samotný obsah zpráv elektronické pošty.[143] E-mailové adresy, kterým chybí propojení

141 § 2 písm. b) ZSIS.
142 § 89 ZEK; Čl. 7 odst. 1, Čl. 10, Čl. 13 LZPS.
143 Stanovisko trestního kolegia Nejvyššího soudu, sp. zn. Tpjn 300/2012, č. 20/2013 Sb. tr. rozh.

s určitou osobou, stejné ochrany nepožívají, přestože i jejich zneužití je zákonem zakázáno.[144]

IV.1.2 E-mail – princip

Pro srovnání „tradiční" a elektronické pošty je nutno načrtnout alespoň základní princip fungování e-mailu, ačkoliv se přitom nelze vyhnout značné míře zjednodušení.

V zásadě platí, že každý uživatel elektronické pošty je vybaven účtem neboli e-mailovou schránkou, což je de facto vymezené místo na disku. Uživatel svoji e-mailovou schránku zobrazuje a spravuje typicky buď prostřednictvím tzv. poštovního či e-mailového klienta (např. MS Outlook, Netscape Mail, Eudora, Pegasus, KMail, AppleMail, Thunderbird, Lotus, The Bat!), nebo pomocí webového rozhraní přes webový prohlížeč (např. Internet Explorer, Mozilla Firefox, Opera), což je charakteristické pro tzv. freemailové služby.

Je nutné si uvědomit, že elektronická pošta je zajišťována spoluprací více specializovaných programů, z nichž některé zůstávají před uživatelem obvykle skryty a zabývají se pouze vlastním přenosem zpráv, zatímco jiné uživatel bezprostředně vnímá, neboť mu umožňují zprávy číst, editovat apod. Uživatelské a přenosové programové složky a celý komplex programů zajišťujících chod elektronické pošty se obecně označuje jako *Electronic Mail System*, který může mít více podob.[145]

Typicky však, pokud uživatel zamýšlí odeslat e-mail ze svého účtu, zpracuje zprávu v uživatelském rozhraní (často nazývaném *Mail User Agent* – MUA), jehož funkce spočívá v připojení se k e-mailové schránce, do které je e-mail uložen ve formátu vhodném pro další zpracování. Uživatel příkazem k odeslání dá pokyn programu MUA, aby pomocí SMTP protokolu (*Simple Mail Transfer Protocol*; je určený pro samotnou výměnu zpráv mezi počítači připojenými k Internetu) předal zprávu serveru MTA (*Mail Transfer Agent*), který provozuje poskytovatel internetových služeb odesílatele. Servery MTA se starají o vlastní přenos zpráv a za tímto účelem mohou používat různé protokoly, k jejichž vzájemné spolupráci jsou pak vytvářeny různé přechodové

144 § 93 ZEK.

145 Viz Peterka, J. Elektronická pošta II. *Computer World*, 1994, roč. 4, č. 9, s. 3. Dostupné také online z: http://www.earchiv.cz/a94/a409c110.php3.

brány. Server MTA podle části e-mailové adresy (např. adresat@urad.cz) za znakem @, tedy podle názvu domény, vyhledá tento název na serveru domény „urad.cz“ DNS (*Domain Name System*), který mu odpoví záznamem (tzv. MX záznamem), ve kterém uvede správný server pro výměnu elektronické pošty pro danou doménu; v uvedeném příkladu by šlo o „mx.urad.cz“. Server MTA odesílatele následně předá pomocí protokolu SMTP zprávu MTA serveru adresáta, který ho doručí do cílové e-mailové schránky.

Existuje poměrně mnoho způsobů, jakými si adresát může svoji e-mailovou poštu vybírat a číst. Může si například pomocí protokolu POP3 stáhnout do svého počítače celé zprávy nebo může pracovat se zprávami pomocí protokolu IMAP (v současné době se používá protokol IMAP4), který je optimalizován k použití v dlouhodobě připojeném režimu. V případě protokolu IMAP zůstávají zprávy uloženy na serveru a stahují se, jen pokud je třeba. Adresát se také může přihlásit k serveru „mx.urad.cz“ a zprávu přečíst přímo, anebo k přečtení zprávy užívat webmailové služby.

Je třeba opětovně uvést, že v systému elektronické pošty existuje mnoho možností, zvláštností a překážek. Odlišnost fungování e-mailu od klasické pošty je však již na tomto místě zcela zjevná.

IV.1.3 Vlastnosti e-mailu

a) Neformálnost – snadnost vytvoření e-mailu i možnost jeho odeslání ze zařízení, jako je mobilní telefon, který má téměř každý neustále v dosahu, svádí uživatele k větší neformálnosti v kompozici i v obsahu elektronické pošty. Mnoho zpráv například vůbec neobsahuje podpis. Pokud se nejedná o formální komunikaci, je pravděpodobnější, že autor bude mít sklon k větší uvolněnosti, čímž může pisatel vyjevit mnohé o svojí identitě i povahových rysech.

b) Odlišná trvanlivost - zatímco papírový vzkaz nebo dopis lze skartovat nebo spálit, život datových souborů nekončí stiskem tlačítka delete. Místo, které např. na hard disku zabírala e-mailová zpráva, je označeno jako nevyužité, a dokonce i po jeho přepsání mohou i na několika místech zůstat fragmenty původního souboru, a to díky způsobu, kterým se dnes běžně zařízení používají; přepínání mezi současně běžícími aplikacemi (multitasking) totiž plní paměť RAM dočasnými

soubory, které se po jejím zaplnění začnou odkládat na pevný disk. Zde se pak mohou nacházet fragmenty souborů, včetně e-mailové komunikace.[146]

c) Jednoduchost pozměnění a podvržení – e-mail je jakožto elektronický soubor citlivější a může být úmyslně nebo neúmyslně pozměněn, třeba jen zapnutím počítače, který přepíše existující soubory. Většina poštovních programů umožňuje editaci textu doručené zprávy a další adresát, kterému je tato zpráva dále poslána, nemá běžným způsobem možnost tuto změnu rozpoznat.[147] Vzhledem k tomu, že je možné pozměnit vlastnosti souborů nebo i metadata, automaticky neexistuje předpoklad pravosti e-mailů, jako tomu je častěji u dokumentů ve fyzicky psané podobě.

d) Objem a přehlednost – v porovnání s papírovými dokumenty nezabírá e-mail žádné místo, přestože jeho přílohy mohou obsahovat obrovské množství dat a informací. Na rozdíl od doručených papírových dokumentů však doručené e-maily nejsou zpravidla tříděny, a pokud ano, pak často ve vytištěné podobě s minimální možností jejich pozdějšího ověření.

e) Nestálost – pokud je e-mailová zpráva psána v jazyce HTML, je možné do ní vkládat hypertextové odkazy směřující k externím zdrojům. Ačkoliv se pak obsah takové zprávy může měnit v závislosti na změně obsahu externího zdroje, kontrolní součet souboru bude stejný. Možnost automatického stahování externího obsahu je většinou omezena bezpečnostním nastavením e-mailových klientů a webových rozhraní. Pokud tomu tak není, může být do zprávy z externího zdroje včleněn různorodý objekt včetně takového, který se jeví jako běžný text zprávy, nebo může obsah takového objektu být na první pohled zcela skrytý.

146 Srovnej případ Kanada. Rozsudek Nejvyššího soudu Britské Kolumbie ze dne 24. 8. 1994 sp. zn. C872267 ve věci *Prism Hospital Software Inc. v. The Hospital Records Institute*. Dostupné z http://www.canlii.org/en/bc/bcsc/doc/1994/1994canlii1308/1994canlii1308.html.

147 Garrett, C. K. Admissibility of Electronic Information. *The Journal of Kansas Bar Association*, 2002, roč. 71., s. 33.

IV.2 Zajištění a uchování důkazního prostředku

Od příchodu mobilních telefonů s datovým připojením se policejní orgány mohou setkat s elektronickou poštou doručenou a uloženou na mobilních zařízeních takřka při každém zadržení osoby, každé domovní prohlídce. Doručené e-mailové zprávy se kvůli svému obsahu pochopitelně těší velkému zájmu policie, avšak rozmach mobilních technologií vedl k nejednotné praxi policejních orgánů a státních zástupců, která se však postupně sjednocuje, a to níže uvedeným způsobem.

IV.2.1 Zajištění obsahu e-mailové komunikace uskutečněné do té doby, než se datový nosič dostal do moci orgánů činných v trestním řízení

Datový nosič se může dostat do moci orgánů činných v trestním řízení legální cestou např. vydáním či odnětím věci (podle § 78, § 79 TŘ), při domovní prohlídce nebo při prohlídce jiných prostor a pozemků (§ 83, § 83a tr. řádu), osobní prohlídce (83 b TŘ), nálezem na místě činu při ohledání (§ 113 TŘ) nebo při jiných procesních úkonech učiněných z iniciativy orgánů činných v trestním řízení. Do jejich dispozice se může dostat také dobrovolným vydáním, ať už při provádění některých již uvedených procesních úkonů nebo například z iniciativy oznamovatele, který policii předá datový nosič nebo celé zařízení jako důkaz k podpoře svých tvrzení.

Uvedená ustanovení trestního řádu v sobě obsahují zákonem dovolené donucení směřující k získání věci pro účely trestního řízení, v tomto případě datového nosiče, a obsahují i zpřísněné postupy, kterými je možno takovou hmotnou věc získat. Tyto zákonem předepsané postupy v sobě již obsahují omezení daná orgánům činným v trestním řízení, např. v § 78 TŘŘ povinnost osobu vyzvat, upozornit na následky nevyhovění, sankcionovat dle § 66 TŘ a teprve v případě, že věc nebude na vyzvání vydána, může být odňata dle § 79 TŘ. Hmotná věc je důležitá pro trestní řízení kvůli objasnění všech skutkových okolností. Zákon přitom nepředepisuje žádnou další proceduru a neklade omezení k ohledání a expertnímu kriminalistickému zkoumání takové věci – v tomto případě datového nosiče. Závěr, podle něhož by policejní orgán mohl zajistit externí hard disk některým z příkladem uvedených postupů, ale bez dalšího povolení soudu by nemohl zkoumat jeho obsah, včetně například uložených zpráv elektronické pošty, není logický.

E-mailovou komunikaci nacházející se na datovém nosiči zde lze z právního hlediska s jistou dávkou opatrnosti přirovnat k obsahu poštovní schránky. Není důvod, aby údaje předávané prostřednictvím elektronických komunikací požívaly rozdílné ochrany než údaje předávané prostřednictvím poštovního styku, neboť obojí spadá do údajů chráněných v oblasti soukromí jakožto ústavně zaručeného práva podle čl. 7 odst. 1, čl. 10 a čl. 13 LZPS a článku 8 odst. 1 EÚLP, kdy navíc požívají zvláštní ochrany v průběhu přepravy od odesílatele k adresátovi. Na právnickou nebo fyzickou osobu, která jako podnikatel zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací (zjednodušeně poskytovatelé telefonních služeb a internetu) zajišťuje i elektronické komunikace, dopadá podle § 89 ZEK povinnost zajistit organizačně a technicky důvěrnost zpráv a s nimi spojených provozních a lokalizačních údajů, resp. povinnost zachovávat mlčenlivost o nich. Zatímco ochrana soukromí zaručená Listinou trvá, zvláštní povinnost mlčenlivosti poskytovatele služeb elektronických komunikací ve vztahu k orgánům činným v trestním řízení je časově omezená a je navázána na trvání právního vztahu mezi ním a uživatelem služeb.

Zvláštní omezení této povinnosti mlčenlivosti ve vztahu k orgánům činným v trestním řízení, které jim dovoluje získávat informace vznikající v souvislosti s poskytováním uvedených služeb na základě trestním řádem stanovených postupů, je vymezeno tak, že trvá po dobu, po níž se musí orgány činné v trestním řízení za účelem zjištění obsahu těchto informací dovolávat součinnosti s poskytovatelem služeb elektronických komunikací, neboť jen tyto subjekty (a nikoli adresát) jsou uvedenou zvláštní povinností mlčenlivosti vázány. Rozhodující je, že jde o informace, které pocházejí z této služby a že jejich zdrojem je pro orgán činný v trestním řízení její poskytovatel. Ochrana těchto informací, předávaných prostřednictvím elektronických komunikací, existující v podobě zvláštní povinnosti mlčenlivosti, pomíjí okamžikem, kdy jsou takové informace doručeny jejich oprávněnému příjemci – poté mohou orgány činné v trestním řízení zprávy doručené přímo na mobilní telefon nebo jakýkoliv datový nosič těchto informací (ať už jsou uloženy v paměti či na SIM kartě, na externím disku nebo v operačním systému přístroje) zajistit a zkoumat stejně tak, jako lze zajistit a přečíst dopis či telegram, který držitel poštovní licence řádně doručil jejich adresátovi.

Uvedené lze tedy shrnout tak, že ke zjištění obsahu elektronické komunikace uložené na datovém nosiči a uskutečněné do doby, než se tento datový nosič dostal do moci orgánů činných v trestním řízení, není třeba zvláštních postupů, například příkazu soudce podle § 88 TŘ.[148]

IV.2.2 Zjištění obsahu e-mailové komunikace uložené na datovém nosiči uskutečněné v době po jeho zajištění orgány činnými v trestním řízení

V praxi často dochází k situacím, že jsou na zajištěné zařízení (počítač, mobilní telefon) doručovány zprávy elektronické pošty i poté, co se zařízení dostalo do moci orgánů činných v trestním řízení. Skutečnost, že policie disponuje s daným zařízením, ji však v žádném případě neopravňuje ke vstupu do práv uživatele služeb elektronických komunikací. Ochrana informací předávaných prostřednictvím elektronických komunikací, existující v podobě zvláštní povinnosti mlčenlivosti, stále trvá, neboť adresát zpráv elektronické pošty se s nimi právě vinou zásahu orgánů činných v trestním řízení nemohl seznámit. Stejnou ochranu bude třeba přiznat v případě zpráv elektronické pošty, které byly doručeny poté, co byl adresát zadržen, vzat do vazby nebo mu bylo jinak ze strany orgánů činných v trestním řízení znemožněno se zařízením disponovat. Nejedná se o stejnou situaci, jaká nastane zajištěním datového nosiče, jeho ohledáním a zjištěním, jaké doručené informace již obsahuje. Zajištění počítače nebo mobilního telefonu neopravňuje orgány činné v trestním řízení, aby i do budoucna bez dalšího využívaly jako důkazní materiál docházející e-maily a další údaje chráněné v rámci práva na ochranu soukromí a dalších práv. Zajištění věci pro účely trestního řízení není prostředkem pro získání informací, které teprve v budoucnu budou do věci nějakým způsobem vneseny, respektive není prostředkem pro odposlech a záznam telekomunikačního provozu ve smyslu § 88 TŘ, ale právním nástrojem pro nalezení a zajištění informací důležitých pro trestní řízení, jejichž je věc nositelem v době zajištění.

148 Viz Výkladové stanovisko Nejvyššího státního zastupitelství č. 4/2005, 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. Dostupné z http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2005/stanovisko%204-2005.pdf.

Ke zjištění obsahu e-mailové elektronické komunikace uskutečněné v době po zajištění datového nosiče orgánem činným v trestním řízení je proto třeba příkazu soudce podle § 88 TŘ, pokud již předmětný příkaz nebyl vydán před zajištěním datového nosiče a příkaz je stále platný.

Nejvyšší soud se touto problematikou zabýval na základě stížnosti pro porušení zákona podané ministrem spravedlnosti v případu, ve kterém jedna z podezřelých osob na vyzvání vyšetřovatele vydala mobilní telefon, který byl následně podroben kriminalistickému zkoumání a měl být mimo jiné zjištěn obsah registru SMS zpráv. Nejvyšší soud přisvědčil argumentům ministra spravedlnosti ve prospěch obviněného v tom smyslu, že „zjištění obsahu registru SMS zpráv" nesmí zahrnovat zprávy, které došly na zařízení až po jeho vydání. [149]

V praxi se vyskytly i názory[150], že „údaje o telekomunikačním provozu, které jsou předmětem důvěrnosti komunikací anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat" ve smyslu § 88a TŘ je možno mimo provozních a lokalizačních údajů, uchovávaných podle § 97 odst. 3 ZEK, vztáhnout i na samotný obsah zpráv a o jeho zpřístupnění žádat postupem dle § 88a trestního řádu.[151] Ačkoliv pojmosloví § 88a nepostihuje všechny v úvahu přicházející formy elektronické komunikace a s ohledem na novelizace ZEK a dalších předpisů je již zastaralé, je třeba § 88a interpretovat za využití právě těchto předpisů.

Podle § 136 odst. 20 písm. b) ZEK obsahuje-li zvláštní právní předpis ustanovení o údajích o telekomunikačním provozu, rozumí se tím provozní a lokalizační údaje související s přenášenou zprávou podle tohoto zákona. Podle § 97 odst. 3 ZEK je právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací povinna uchovávat po dobu 6 měsíců provozní a lokalizační údaje, které jsou vytvářeny nebo zpracovávány při zajišťování jejích veřejných komunikačních sítí a při poskytovávání jejích veřejně dostupných služeb elektronických komunikací. Současně je tato právnická nebo fyzická

149 Viz Usnesení Nejvyššího soudu sp. zn. 7 Tz 9/2000. Pro úplnost je však třeba zmínit i odlišné rozhodnutí Vrchního soudu v Olomouci sp. zn. 5 To 42/2010.

150 Jedná se o nepublikované rozsudky okresních soudů v Jihlavě a v Rakovníku.

151 Srov. Behr, T., Kohout, J. Elektronická pošta a její záznam pro trestní řízení. *Trestněprávní revue*, 2011, č. 4, s. 101.

osoba povinna zajistit, aby při plnění povinností podle věty první a druhé nebyl uchováván obsah zpráv a takto uchovávaný dále předáván. Z toho lze jednoznačně dovodit, že obsah zpráv elektronické pošty nespadá pod provozní a lokalizační údaje (definované zvlášť v § 90 a 91 ZEK) a podnikatel v elektronických komunikacích (§ 8 odst. 2 ZEK) obsah nesmí uchovávat a není oprávněn jej poskytnout. Znění § 88a odst. 1 trestního řádu „údaje o telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat," je nutno interpretovat právě v kontextu § 97 odst. 3 ZEK a § 4 ZOOÚ.

Doručením zprávy příjemci končí elektronický komunikační provoz podléhající důvěrnosti komunikací a součinnost od podnikatele poskytujícího služby elektronické komunikace směřující ke zjištění obsahu zpráv lze, stejně jako v případě odposlechu, požadovat pouze v době přenosu, a to na základě příkazu soudce podle § 88 odst. 1 TŘ.

Zvláštní kategorii tvoří otázka vymahatelnosti povinnosti umožnit soudem nařízený odposlech a záznam zpráv, případně uchovávat provozní a lokalizační údaje (§ 97 odst. 1, 3 ZEK) u fyzických a právnických osob poskytujících služby elektronickými prostředky[152], které nejsou současně podnikateli v elektronických komunikacích (§ 8 odst. 2 ZEK). Jedná se především o některé provozovatele freemailových služeb, kteří však často provozní a lokalizační údaje uchovávají pro obchodní a marketingové účely. Z hlediska postupu v trestním řízení však není důvod činit u těchto osob výjimku, když se ústavně zaručená ochrana telekomunikačního tajemství a práva na ochranu soukromí vztahuje i na služby poskytované těmito fyzickými a právnickými osobami.[153]

IV.2.3 Zjišťování obsahu e-mailové schránky

Příměr poštovní a e-mailové schránky může být zavádějící z technického i z právního hlediska. Je zcela běžné, že jeden uživatel má zřízeno více e-mailových účtů, ke kterým přistupuje buď zvlášť, nebo z jednoho místa.

152 Viz § 2 písm. a) ZSIS.

153 Viz Výkladové stanovisko Nejvyššího státního zastupitelství č. 1/2015, ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek. Dostupné z http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2015/1_SL_760-2014.pdf.

Služba Gmail například umožňuje centralizovat poštu z více e-mailových účtů do jedné schránky. Navíc je možné přímo z rozhraní Gmailu odesílat zprávy tak, že jako odesílatel není v hlavičce označen uživatel Gmailu (např. *uživatel@gmail.com*), ale jedna ze synchronizovaných schránek, kterou uživatel vlastní (z rozhraní Gmailu je tedy možno odesílat e-maily s adresou např. *uživatel@seznam.cz*).

V e-mailové schránce se navíc mohou nacházet jak zprávy doručené a odeslané, tak koncepty zpráv, ale i zprávy nežádoucího spamu ve zvláštní složce, stejně jako zprávy v koši, které jsou po určité době automaticky trvale smazány. Technická odlišnost od klasické poštovní schránky je zde tedy více než zjevná.

Obsah e-mailové schránky je plně v dispozici jejího uživatele, který má za použití různých prostředků možnost e-mailové zprávy ve schránce zachovat, automaticky je podle různých filtrů a nastavení posílat na další účty nebo je pravidelně vymazávat. Jedná se o komunikaci ukončenou a uloženou v rámci virtuálního soukromého prostoru, e-mailové schránce, z vůle jejího uživatele. Rozhodující v tomto případě není, zda si uživatel e-mailové schránky e-mail přečetl, ale to, zda tuto možnost měl, a pokud ne, zda tomu bylo vinou ingerence orgánů činných v trestním řízení, případně, zda přečtení bránily objektivní překážky spočívající mimo vůli uživatele.

K rozdílné ochraně obsahu zpráv při probíhající komunikaci a po doručení či ukončení této komunikace se vyslovil Nejvyšší soud ČR při posuzování zásahu do tajemství dopravovaných zpráv.[154] Ochrana se podle Nejvyššího soudu poskytuje dopravované zprávě v době jejího „podávání", tedy v průběhu doručování, kdy počátek tohoto procesu je ohraničen odesláním zprávy z počítače odesílatele a okamžikem doručení zprávy do e-mailové schránky příjemce. Doručením je proces dopravy zprávy ukončen a v e-mailové schránce zpráva také zůstává, pokud ji adresát neodstraní. Přístup do e-mailové schránky je chráněn heslem a její uživatel má přitom povětšinou možnost s obsahem schránky disponovat z kteréhokoli počítače připojeného k internetu. Doručené zprávy nacházející se v e-mailové schránce jsou tedy již zcela v dispozici příjemce. Nastavení e-mailové schránky zpravidla také umožňuje, aby si její uživatel nechal zasílat oznámení o doručení zprávy, obsahující současně i část jejího textu, na mobilní telefon nebo jiné

154 Viz usnesení Nejvyššího soudu sp. zn. 11 Tdo 349/2009.

zařízení (např. na tzv. „chytré hodinky“), a adresát tak může být bezprostředně informován o části nebo o celém obsahu e-mailu, aniž by k tomu potřeboval počítač. Nastavením (např. v aplikaci Outlook) je možno dosáhnout také toho, že zpráva je po uplynutí určitého času automaticky označena jako přečtená a automaticky jsou odesílány potvrzení o přečtení. Pokud by tedy ochrana probíhající elektronické komunikace byla vázána na okamžik přečtení e-mailu adresátem, nebylo by zřejmé, jak v takovém případě tento okamžik určit.

Nejvyšší soud dospěl k závěru, že pokud by zákonodárce zamýšlel rozšířit v tomto směru trestněprávní ochranu tak, jak vyplývá z právního názoru zaujatého soudy nižších stupňů v nyní projednávané věci, měl by možnost formulovat toto ustanovení přesněji a výslovně v něm uvést, že zpráva se má za doručenou až po jejím přečtení, vyslechnutí či jiném poznání jejího obsahu příjemcem, nebo jinak výslovně stanovit konec ochrany tajemství takové zprávy.

Za situace, kdy orgány činné v trestním řízení nemají k dispozici datový nosič, na kterém je elektronická komunikace uložena, a potřebují za účelem objasnění skutkových okolností zjistit obsah elektronické komunikace uložené v e-mailové schránce, mohou do tohoto soukromého prostoru zasáhnout na základě povolení sledování osob a věcí soudem podle § 158d odst. 1 a 3 TŘ v rozsahu specifikovaném v soudním rozhodnutí, neboť obsah e-mailové schránky lze považovat za jiné záznamy uchovávané v soukromí za použití technických prostředků.

K výše uvedenému závěru prozatím neexistuje bohatší judikatura, nicméně ho již jednou podpořil Ústavní soud ČR, který konkrétně uvedl, že: *„Sledováním osob a věcí se dle citovaného ustanovení (158d trestního řádu) rozumí získávání poznatků o osobách a věcech prováděné utajovaným způsobem nebo jinými prostředky. Z dikce zákona jasně vyplývá, že v rámci tohoto úkonu lze pořizovat záznamy nejrůznějšího druhu a se souhlasem soudce může být v přiměřené míře zasahováno do práva na soukromí dotčených osob. 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 na těchto zařízeních uložená, jejichž otisk lze pořídit za využití utajené*

operativně pátrací techniky. Pořízení otisku elektronických dat lze povolit postupem dle § 158d odst. 3 tr. řádu, pokud jde o data na sledovaných počítačích již uložená, nikoli o data telekomunikačního provozu."[155]

Z názoru Ústavního soudu lze dovodit, že zjištění aktuálního obsahu e-mailové schránky se může vztahovat nejen na odeslané e-mailové zprávy, ale i na e-maily ve složce odstraněných zpráv a na rozepsané a doručené zprávy, včetně těch, které si příjemce doposud nepřečetl, pokud tuto možnost objektivně měl.

Pro možnost použití postupu podle § 158d odst. 3 TŘ nepřímo hovoří i další judikatura Nejvyššího soudu, která co do účelu připodobňuje odposlech a záznam telekomunikačního zařízení k operativně pátracím prostředkům podle § 158 b a násl. TŘ, neboť se v obou případech jedná o zajišťovací instituty. V širším smyslu totiž i odposlechy a záznamy telekomunikačních zařízení v trestním řízení slouží k předcházení, odhalování a objasňování trestné činnosti, jakož i k pátrání po skrývajících se pachatelích, pátrání po hledaných nezvěstných osobách a po věcných důkazech.[156]

K volbě postupu podle § 158d odst. 3 TŘ vedou i konkrétní případy, ve kterých pachatelé z organizované zločinecké skupiny mezi sebou komunikovali prostřednictvím složky rozepsaných zpráv na jediném e-mailovém účtu, ke kterému všichni znali přístupové heslo. V takovém případě nešlo o odesílání a doručování zpráv elektronické pošty mezi uživateli e-mailových účtů, a nelze proto hovořit o probíhající elektronické komunikaci, případně volit postup dle § 88 TŘ.

Orgány činné v trestním řízení postupem dle § 158d odst. 3 TŘ tedy mohou pořídit otisk elektronických dat uložených na sledovaných počítačích. V žádném případě však nesmí jít o cílené zneužití postupu dle § 158d odst. 3 TŘ k získání dat telekomunikačního provozu (kde je třeba volit postup dle § 88a TŘ) nebo k faktickému sledování probíhajícího telekomunikačního provozu (postup podle § 88 TŘ). Přes časovou působnost příkazu dle § 158d je však možno vidět i slabinu této právní konstrukce, neboť si lze představit, že policejní orgány budou sváděny k tomu, aby vstupovaly

155 Viz usnesení Ústavního soudu sp. zn. III. ÚS 3812/2012, U 10/71 SbNU 573.
156 Viz usnesení Nejvyššího soudu sp. zn. 8 Tdo 109/2014.

do schránky několikrát, nebo dokonce nepřetržitě po dobu trvání platnosti příkazu, což se fakticky rovná soudem neschválenému odposlechu probíhající komunikace.

Otázkou zajištění obsahu e-mailové schránky uloženého na e-mailovém serveru poskytovatele se zabýval také německý ústavní soud.[157] Na rozdíl od Nejvyššího soudu ČR dospěl k závěru, že obsah e-mailového účtu chráněného heslem, ke kterému má přístup pouze uživatel, je chráněn telekomunikačním tajemstvím ve smyslu Čl. 10.1 Základního zákona SRN. Tuto ochranu je podle německého ústavního soudu nutno takovému e-mailovému účtu přiznat proto, že jeho uživatel nemá technické prostředky k tomu, aby zabránil poskytovateli v předání e-mailů třetím osobám (státní orgány nevyjímaje). Nedostatek technických možností na straně uživatele a nutnost „spoléhat se na poskytovatele" si žádá ochranu telekomunikačním tajemstvím, která vyvažuje relativně snadnou dostupnost obsahu e-mailového účtu státním orgánům. Není přitom důležité, zda jde o e-maily nepřečtené, rozepsané nebo přečtené a ponechané v e-mailové schránce. Pokud uživatel ponechá e-mail po přečtení ve schránce na e-mailovém serveru poskytovatele, nedává tím současně souhlas k tomu, aby k jeho datům měla přístup třetí strana. Ochranu telekomunikačního tajemství Čl. 10.1 Základního zákona SRN nelze podle ústavního soudu SRN vykládat úzce ve smyslu definice uvedené v § 3 německého zákona o telekomunikacích[158], ale je třeba ji vztáhnout na celý komunikační proces a na právo uživatele, aby do tohoto procesu nevstupovaly třetí strany. Ústavní soud SRN však současně dodává, že ustanovení německého trestního řádu o zajištění věci[159] je aplikovatelné i na obsah e-mailové schránky na serveru poskytovatele, a není tedy v takovém případě nutné žádat např. o povolení odposlechu, přestože je zasahováno do telekomunikačního tajemství. Podle soudu jde v případě zajištění věci o jasná a určitelná pravidla, která jsou v souladu se Základním zákonem SRN.

157 Srov. Německo. Rozhodnutí Federálního ústavního soudu SRN ze dne 16. 6. 2009 sp. zn. 2 BvR 902/06. Dostupné z http://www.hrr-strafrecht.de/hrr/bverfg/06/2--bvr-902-06-1.php.

158 Srov. zákon SRN o telekomunikacích *(Telekommunikationsgesetz)* v platném znění.

159 Srov. § 94 a násl. německého trestního řádu *(Strafprozessordnung)* v platném znění.

IV.2.4 Zjišťování probíhající e-mailové komunikace

Ačkoliv proces „doručování" zprávy elektronické pošty z původního do koncového zařízení zpravidla trvá řádově vteřiny, je zřejmé, že pomocí technických zařízení je možno zprávu v tomto procesu zachytit, případně zkopírovat a následně přečíst. Úvahy českých soudů nad otázkou ochrany zpráv „dopravovaných" telekomunikačním provozem byly podrobně rozvedeny výše v této kapitole. Soudy na ochranu obsahu zpráv elektronické pošty pohlížejí z hlediska etapy „přepravy" a momentu, kdy již zpráva byla doručena.

V případě etapy přepravy, tedy „doručování" zprávy elektronické pošty, zákonodárce stanovil zpřísněné podmínky pro ochranu tajemství těchto zpráv v podobě povinnosti podnikatelů zajišťujících veřejné komunikační sítě nebo poskytujících veřejně dostupné služby elektronických komunikací zajistit technicky a organizačně důvěrnost zpráv a s nimi spojených provozních a lokalizačních údajů, které se přenášejí prostřednictvím jejich veřejné komunikační sítě a veřejně dostupných služeb elektronických komunikací.

Pro zjištění obsahu těchto zpráv proto bude nezbytné použít postup předpokládaný § 88 TŘ. Stejný postup, jak již bylo uvedeno, musí orgány činné v trestním řízení zvolit ke zjištění obsahu e-mailové elektronické komunikace uskutečněné až poté, co se datový nosič dostane legální cestou do jejich moci.

IV.3 Forenzní analýza

Zprávy elektronické pošty jsou nejčastěji policejním orgánům jako důkaz předkládány z iniciativy poškozených, svědků anebo i podezřelých osob a mívají různorodou formu (a v návaznosti na to i důkazní hodnotu) podle možností a znalostí jednotlivců.

Mnoho informací je dostupných i při zběžné kontrole, např. kromě položek viditelných v každé zprávě, lze po otevření celé hlavičky e-mailu zjistit množství dalších údajů.

Tyto údaje mohou v hlavičce vypadat například takto:

Received: from mailing.eproof.be (mailing.eproof.be [178.208. 36. 23])
by email-smtpd5.go.seznam.cz (Seznam SMTPD 1. 2. 99) with ESMTP;
Thu, 29 Jan 2015 20:58:31 +0100 (CET)

Received: from eproof.be (178.208. 38. 166.static.hosted.by.combell.com [178.208. 38. 166])
(authenticated bits=0)
by com-mailing003.srv.combell-ops.net (8. 14. 5/8. 14. 5) with SMTP id t0TJl8vY005126
for ouvex@seznam.cz; Thu, 29 Jan 2015 20:47:08 +0100
Date: Thu, 29 Jan 2015 20:47:08 +0100
Message-Id: <201501291947.t0TJl8vY005126@com-mailing003.srv.combell-ops.net>
Subject: New routes in 2015
MIME-Version: 1.0
Content-type: text/html; charset=iso-8859-15
To: <ouvex@seznam.cz>
From: Brussels Airport <brussels-airport@eproof.be>
Reply-to: Brussels Airport <marketingnews@brusselsairport.be>

Údaje uvedené v hlavičce pak mají tento význam:

„Received" – adresa e-mailového serveru a IP odesílatele (v tomto případě jde o IP adresu skutečně se nacházející v Bruselu v Belgii); další „Received" ukazuje cestu, kudy e-mail putoval. Položka „Date" obsahuje datum a čas odeslání, včetně časového pásma. „Message-Id" – jedinečné identifikační číslo zprávy. „Subject" – stručný popis předmětu zprávy. „Content-type" – určuje kódování obsahu – text/plain nebo text/html a znakovou sadu. Známé položky „To" a „From" definují adresy příjemce a odesílatele ve formátu „jméno" nebo „adresa" a položka „Reply-to" označuje nastavenou adresu odesílatele pro odpověď.

Setkat se můžeme s dalšími údaji, jako jsou např.: „Mime-version" – značí, že je zpráva formátována ve standardu MIME. Údaje ve formátu „X – údaj" označují další parametry, které používají různé programy, ale nejsou specifikovány v MIME (např. „X-Mailer: PHP" – identifikuje program, který byl použit pro odeslání). Typicky zde najdeme data antispamových programů a firewallu (např.: „X-Barracuda-URL: https://172. 31. 255.12:425/cgi-mod/mark.cgi" – označuje IP adresu Firewallu Barracuda Spam Firewall, který zprávu zpracoval. Zjištěný typ antispamového programu pak může být cenným poznatkem při ověřování pravosti e-mailu.

Pokud zprávy technicky zajišťuje policejní orgán sám, ať už jde o dobrovolné vydání, nebo o nucené zajištění, nejčastěji je uloží na uzavřené CD ROM a provede kontrolní součet hash kódů. Připojená legenda nemá na úrovni Policie ČR unifikovanou podobu, avšak může znít například takto:

> *Předmětná e-mailová zpráva byla zajištěna na HDD služebního počítače poškozeného A. U., systém Microsoft Windows, a byla uložena pod názvem „01AUmessage" na uzavřeném CD ROM, které je přílohou č. 5 spisu. Dne dd.mm.rrrr byla vytvořena kontrolní suma MD5 souboru – „ 8c106b9d372ba6826cd97d4823a516d6". Poškozený A.U. byl zajištění přítomen.*

Zvláštní situace nastává v případě, kdy je obsah zpráv šifrován. V takovém případě je třeba dešifrování, pokud je možné, jehož výsledkem je v kladném případě znalecký posudek nebo výsledek kriminalistické expertizy. V České republice nemůže být podezřelý či obviněný nucen, aby vydal hesla či šifrovací klíče, avšak je třeba upozornit na to, že v jiných zemích EU tomu tak být nemusí. Na základě příkazu belgického vyšetřujícího soudce musí každý (tedy i obviněný) čitelným způsobem zpřístupnit počítačový systém[160] (v daném případě jde však spíše o legislativní chybu belgického zákonodárce). V Anglii je nerespektování soudního příkazu k vydání dešifrovacích klíčů a hesel dokonce trestným činem. Důkazy získané tímto způsobem v zahraničí by však v trestním řízení v ČR byly nepoužitelné pro rozpor zahraničního procesního postupu se základními zásadami trestního řízení.

IV.4 Provedení důkazu

E-mail je záznamem o komunikaci mezi uživateli, který má, jakožto důkaz v trestním řízení, prokázat konkrétní skutkovou okolnost. Tedy, pro stranu, která tento důkaz předkládá, existuje nutnost prokázat logické spojení mezi důkazem a právní skutečností, která má být prokázána.

Přísně vzato, e-mail opatřený elektronickým podpisem doručený do datové schránky je důkazem pouze toho, že „nějaká osoba, která má přístup k privátnímu klíči, odněkud odeslala e-mail do dané datové schránky". Podobně zpochybnit lze v konečném důsledku takřka jakýkoliv důkaz. Naopak,

160 Srov. Čl. 88quater odst. 1 belgického trestního řádu (*Code d'Instruction Criminelle) v platném znění.*

za situace, kdy strany řízení před soudem nebudou vznášet pochybnosti o tom, že jde o pravou a původní zprávu elektronické pošty, soud nemá a priori důvod takový e-mail podrobovat dalšímu zkoumání.

Problém tkví v autorství a autentičnosti e-mailu a v tom, zda jej soud a strany řízení jako konkrétní důkaz zpochybňují. Možností zfalšování e-mailu, včetně metadat, je mnoho, a to od těch nejprimitivnějších (editace hlavičky nebo obsahu e-mailu) přes nápaditější (využití webových stránek umožňujících odeslat e-mail z libovolné e-mailové adresy; zfalšování IP adresy apod.) až po sofistikované využití schopností útočníka a/nebo k tomu uzpůsobeného softwaru (např. ovládnutím cizího počítače a odeslání zprávy přímo z něj). Někdy však velmi prostá metoda, kdy pachatel někde získá zaznamenané heslo a příležitost k přístupu k počítači oběti, může být z důkazního hlediska tou nejproblematičtější. Zmínit je třeba i nepřeberné možnosti anonymizace, například přes anonymizační remailery, využitím sítí Tor nebo I2P a šifrování v těchto sítích nebo za pomoci šifrovacího softwaru. Mimo technických parametrů zprávy elektronické pošty je však e-mail jako důkaz nutno zkoumat především ve vztahu k osobě pisatele, času a okolnostem, za kterých byl napsán, jakož i v logické souvislosti s dalšími shromážděnými důkazy.

> Při ověřování e-mailu jakožto důkazu v trestním řízení tedy půjde v první řadě o to, zda za autora e-mailu lze skutečně považovat osobu označenou jako jeho původce (jako odesílatele nebo osobu pod zprávou podepsanou). Pokud je autorství e-mailu sporné, může k jeho určení sloužit řada nepřímých důkazů, například:
>
> 1. Svědecká výpověď. Svědek mohl vidět psaní nebo odesílání e-mailu, mohl si jej se svolením pisatele přečíst apod.
> 2. Znalecký posudek. V souvislosti s určením osoby, která je skutečným autorem e-mailu přichází v úvahu především forenzní lingvistika, jejímž úkolem je jazyková analýza a interpretace psaného i mluveného textu. Forenzní znalec určí významné osobnostní rysy původce textu s cílem hledání této osoby ulehčit anebo v ideálním případě přiřadit autorství textu konkrétní osobě. Forenzní lingvistika tedy zkoumá otisk osobnosti autora do textu, za kterým stojí, a napomáhá tím jeho odhalení. Jedná se o doplnění jiných kriminalistických metod, nicméně v řetězci nepřímých důkazů může tento postup významně přispět k odhalení autora e-mailu, potažmo pachatele trestného činu.

3. Úprava, obsah, podstata, vnitřní uspořádání a další charakteristické rysy zprávy, a to v souvislosti s konkrétními okolnostmi případu.
4. Možnost fyzického přístupu pisatele ke konkrétnímu zařízení (počítač, mobilní telefon); znalost přístupových hesel.
5. Parametry hlavičky e-mailu (viz výše kapitola IV.3).
6. Záznamy o datovém provozu – od poskytovatele internetových služeb, případně od správce sítě – zde záleží na správci a na používaném softwaru. Hlavičky na mailserveru většinou obsahují jenom informace „From", „To" a maximálně předmět zprávy. Vypovídající hodnotu mají také ověřovací systémy (např. DKIM), pokud jsou na mailserveru spuštěny.
7. Odeslání z datové schránky náležející konkrétnímu uživateli.
8. Elektronický podpis.

IV.5 Hodnocení důkazu

V souvislosti s určováním autorství e-mailu je třeba poukázat na úvahy Nejvyššího správního soudu, který rozhodoval v případu kasační stížnosti podané proti rozsudku Krajského soudu, kterým byla zamítnuta správní žaloba a bylo potvrzeno rozhodnutí městského úřadu o vině ze spáchání přestupku proti občanskému soužití a uložení pokuty.[161] Ve věci bylo nejprve vedeno řízení trestní, ale skutek byl později překvalifikován na přestupek. Šlo o to, že stěžovatel měl založit jistý e-mailový účet a z něj na určitou e-mailovou adresu zaslat fotografie (akty) s vyobrazením osoby P. B., čímž ji měl vystavit v posměch. Stěžovatel v průběhu celého správního řízení namítal, že skutečnost, že e-mail odešel z IP adresy přidělené jeho telefonnímu číslu, ještě neznamená, že uvedený e-mail skutečně odeslal, a odeslání e-mailu popřel. Poukazoval na možnosti zneužití osobního počítače třetí osobou a jeho ovládnutí, jakož i na fenomén phishingu, a uváděl osobu P., která měla mít v rozhodné době přístup k jeho počítači, jakož i motiv k tomu, aby stěžovatele poškodila.

Nejvyšší správní soud dal stěžovateli za pravdu v tom, že pokud je prokázáno, že z jeho počítače odešel e-mail, neznamená to automaticky, že autorem

161 Viz rozsudek Nejvyššího správního soudu č. j. 8 As 10/2006-48.

e-mailu je stěžovatel, a uvádí hned několik způsobů, jakým mohla jiná osoba předmětný e-mail odeslat. Současně soud konstatuje, že důkazu o odeslání e-mailu z IP adresy přidělené pevné telefonní lince, jejímž prostřednictvím je realizováno připojení k internetu, je nutno přiznat určitou relevanci. Soud v této souvislosti uvádí: „*Jedná se totiž v zásadě o nepřímý důkaz, který lze s jistou mírou zjednodušení připodobnit důkazu svědčícímu o tom, že dopravní přestupek byl spáchán při jízdě určitým konkrétním dopravním prostředkem. V takovém případě také nelze majitele daného dopravního prostředku bez dalšího považovat za pachatele přestupku, avšak důkaz o tom, že přestupek byl spáchán např. jeho vozidlem, jistě představuje významné vodítko, které může za pomoci dalších nepřímých důkazů vyústit v to, že je uznán vinným.*“[162]

Jestliže má IP adresa za určitých okolností představovat osobní údaj,[163] na jehož základě lze přímo či nepřímo identifikovat konkrétní osobu, je možné takový údaj použít jako nepřímý důkaz v přestupkovém řízení. Nepřímých důkazů svědčících o vině stěžovatele bylo shromážděno více, avšak právě vzhledem k tomu, že šlo o důkazy nepřímé, soud v tomto případě důsledně zkoumal, zda tyto důkazy tvoří ucelený, logicky provázaný řetězec.

Jeho části tvořila skutečnost, že stěžovatel měl přístup k počítači, na kterém byly uloženy předmětné citlivé fotografie, a to v rodinném domku, kde bydlel. Znalec dále potvrdil, že složka s fotografiemi byla na tomto počítači v rozhodné době vypálena na CD ROM. V původně vedeném trestním řízení stěžovatel uvedl, že PC, ze kterého byl předmětný e-mail odeslán, užívá sám, nicméně později tvrdil, že k počítači měl přístup také pan P., který však takovou možnost popřel. Řetězec těchto důkazů vedl orgány rozhodující v předchozích řízeních k závěru o vině stěžovatele ze spáchání přestupku.

Nejvyšší správní soud však nalezl zásadní rozpor mezi výpovědí stěžovatele, podle níž měl k jeho počítači v inkriminovanou dobu přístup pan P. a měl praktickou možnost doličný e-mail z tohoto počítače odeslat, a opačným tvrzením pana P, kterým uvěřil i krajský soud. Stěžovatel přitom prezentoval v průběhu řízení tvrzení, kterými věrohodnost výpovědi pana P. zpochybňoval. E-mailovou korespondencí pana P., vytištěnou ze svého

162 Viz Rozsudek Nejvyššího správního soudu č. j. 1 As 90/2008–189.
163 Viz Rozhodnutí SDEU ve věci Promusicae, sp. zn. C-275/06.

počítače, dokládal tvrzení, že pan P. měl na jeho počítači založenou e-mailovou schránku a pracoval na něm, a následně poukazoval na to, že pan P. měl motiv k tomu ho poškodit, neboť se o to už v minulosti opakovaně snažil. V rámci konfliktu s rodinou stěžovatele pan P. dokonce použil i střelnou zbraň, za což byl trestně stíhán. Krajský soud se však v odůvodnění svého rozsudku s těmito skutečnostmi nevypořádal.

S odkazem na své předchozí rozhodnutí Nejvyšší správní soud opětovně poukazoval na to, že nepřímé a vzájemně se podporující důkazy musí tvořit logickou a ničím nenarušovanou soustavu a musí spolehlivě prokazovat všechny okolnosti spáchaného skutku. Tato soustava nepřímých důkazů má nad vší rozumnou pochybnost stavět najisto, že se jednání dopustil právě ten, kdo má být za nezákonné jednání postižen, a současně vylučovat možnost jiného závěru.

> V souvislosti s autentizací e-mailu je pro srovnání možno zmínit názor Odvolacího soudu státu Albama v USA, který rovněž dospěl k názoru, že e-mail může být jako důkaz ověřen jednak obecnými technickými rozlišovacími znaky e-mailů, ale také svou úpravou, obsahem, podstatou, vnitřním uspořádáním, případně jinými vlastnostmi charakteristickými pro e-maily. Soud uvádí:
>
> *„V některých případech se domnělý odesílatel vlastně k autorství plně či zčásti doznal nebo byl při psaní viděn. V jiných případech provozní záznamy poskytovatele internetových služeb ukázaly, že zpráva má původ v počítači nebo mobilním telefonu domnělého odesílatele, a to za takových okolností, kdy lze mít důvodně za to, že pouze domnělý odesílatel mohl mít k počítači nebo mobilnímu telefonu přístup. Někdy komunikace obsahovala takové informace, které mohl znát pouze domnělý odesílatel, někdy tento domnělý odesílatel odpověděl při výměně elektronické komunikace takovým způsobem, že v okolnostech naznačil, že je ve skutečnosti autorem určité komunikace, která byla sporná. A v některých případech to byly jiné zvláštní okolnosti tak příznačné pro fakta konkrétního případu, že zjevně stačily k autentizaci.“*[164]
>
> Uvedený rozsudek navazoval na řadu rozsudků soudů USA týkajících se ověřování dokumentů, z nichž některé výpověď svědka berou jako běžný

164 Viz Spojené státy. Rozsudek Trestního odvolacího soudu státu Alabama ze dne 21. 11. 2014 sp. zn. CR-13-1039 ve věci Robert N. Culp, Jr. v. State of Alabama. Dostupné z: http://law.justia.com/cases/alabama/court-of-appeals-criminal/2014/cr-13-1039.html.

způsob k autentizaci e-mailu.[165] Dále hovoří o autentizaci přes jeho specifickou podobu, obsah a kontext – předmětné e-maily například obsahovaly přesné informace o předchozích aktivitách obžalovaného a znaky spjaté s jeho osobou (zpráva byla podepsána přezdívkou, kterou již dříve používal v komunikaci se svědky) nebo se obsah e-mailů shodoval s obsahem telefonických rozhovorů svědků a obžalovaného.

IV.6 Shrnutí

Elektronická pošta se stala nejběžnějším způsobem obchodního i soukromého písemného styku. Přestože její obrazová podoba a základní myšlenka vychází z principu tradičních poštovních zásilek, její fungování a nepřeberné možnosti se od tradiční pošty stále více odlišují. Jde o důvěrnou komunikaci chráněnou jednak tzv. telekomunikačním tajemstvím a jednak právem na soukromí, což má svůj odraz v použití adekvátních procesních nástrojů při zajišťování obsahu elektronické pošty. Judikatura nejvyššího a ústavního soudu dává probíhající e-mailovou komunikaci pod ochranu telekomunikačního tajemství, které dále nerozšiřuje (po vzoru Federálního ústavního soudu SRN) na „spící" obsah e-mailového účtu, nebo na obsah datového nosiče, na kterém jsou zprávy elektronické pošty uloženy; soudy takovému obsahu přisuzují pouze ochranu právem na soukromí, což má odraz v možnosti použití např. ustanovení o sledování osob a věcí.

Vzhledem k nemalým technickým možnostem falzifikace e-mailu je v případě sporu o jeho pravost nutno zkoumat technické údaje, počínaje rozšířenou hlavičkou e-mailu a konče daty aplikací. Stejně tak je ale třeba ověřovat autenticitu e-mailu skrze „otisk osobnosti" autora zprávy, k čemuž může dopomoci například forenzní lingvistika. Konečně, pravost e-mailu může prokázat i soustava vzájemně se doplňujících nepřímých důkazů v podobě okolností, za nichž byl e-mail odeslán, výpovědí svědků nebo možnosti fyzického přístupu domnělého autora ke konkrétnímu zařízení.

Písemné zprávy nepochybně přetrvají, ať už bude jejich budoucí podoba a způsob zasílání jakýkoliv. Čím lépe a podrobněji se zákonodárce, soudy

165 Viz Spojené státy. Rozsudek Odvolacího soudu 11. obvodu USA ze dne 15. 12. 2000 sp. zn. No. 98-6994 ve věci United States v. Siddiqui. Dostupné z http://caselaw.findlaw.com/us-11th-circuit/1493241.html.

a odborná veřejnost seznámí s podstatou, možnostmi a různorodými vlastnostmi e-mailu, tím samozřejmější bude předkládání zpráv elektronické pošty jako důkazu v trestním řízení.

V DOKAZOVANIE OSOBNÝM PROFILOM A WEBOVOU PREZENTÁCIOU

V.1 Vysvetlenie pojmov

Dokazovanie skutočností v trestnom konaní pomocou informácií vyťažených z osobného profilu sociálnej siete a webovej prezentácie predstavuje v súčasnosti problém procesného postupu orgánov činných v trestnom konaní. Webová prezentácia, ktorá je neodmysliteľne spojená s priekopníckymi začiatkami širokého využitia internetu, a od nej neskôr odvodený osobný profil v sociálnej sieti, je nositeľom užitočných informácii, ktoré nepochybne môžu slúžiť ako vhodný dôkazný materiál v trestnom konaní o rôznorodých skutkoch. Je možné konštatovať, že tuzemská súdna prax sa už pokúša vysporiadať s fenoménom sociálnych sietí a súvisiacich digitálnych stôp. Desiatky súdnych rozhodnutí obsahujú tvrdenia strán alebo sa inak odvolávajú na tento elektronický dôkaz, často nahradený listinným výpisom komunikácie, fotografie alebo stav štatútu z portálu sociálnej siete.[166] Za účelom získania skutkových poznatkov tak boli podrobené skúmaniu komunikácie, obsahy fotografií alebo sociálne väzby užívateľov sociálnych portálov alebo webových prezentácií. Je na mieste sa spýtať, akú povahu má dôkaz získaný z týchto prostriedkov a aké je jeho správne vykonanie podľa platného procesného trestného práva?

V nasledujúcej kapitole bude osvetlená technická povaha osobného profilu vyskytujúceho sa na najčastejšie dostupných sociálnych sieťach. Paralelne bude vysvetlený proces fungovania webovej stránky so špecifickým obsahom – osobnou prezentáciou. Pre potreby využitia týchto dôkazných

166 Viac ako 15 rozhodnutí Najvyššieho súdu ČR v trestných veciach okrajovo odkazuje na dôkaz alebo inú skutočnosť pochádzajúcu zo sociálnej siete Facebook (viď http://nsoud.cz/Judikatura/judikatura_ns.nsf/$$WebSearch1?SearchView&Query=%5BARozhodnutiRT%5D%3Dfacebook & SearchMax=1000 & pohled=1 & start=1 & Count=15). Taktiež existujú 4 rozhodnutia Ústavneho súdu ČR, ktoré v texte uvádzajú skutočnosti pochádzajúce zo sociálnej siete Facebook (viď http://nalus.usoud.cz/Search/). Nižšie súdy s týmto typom zdroja dôkazu pracujú častejšie. Napr. prostredníctvom portálu www.otvorenesudy.sk je možné na Slovensku nájsť viac ako 350 výsledkov (rozhodnutí nižších súdov, ktoré sú povinne zverejňované) po zadaní kľúčového slova „Facebook" (viď http://www.otvorenesudy.sk/decrees/search?utf8=&q=facebook).

prostriedkov je nutné priblížiť procesné otázky ich zaistenia a uchovávania v zmysle platnej zákonnej úpravy. Navyše, forenzná analýza tohto typu dôkazného prostriedku predstavuje kľúčovú časť celého dôkazného procesu, ktorý je zavŕšený vykonaním a hodnotením takto získaných dôkazov.

V.1.1 Sociálna sieť

Za sociálnu sieť sa považuje každá webová stránka prístupná verejnosti pomocou webového prehliadača (na PC alebo mobilnom zariadení), ktorej primárnym cieľom je nadväzovanie, udržiavanie a rozširovanie sociálnych väzieb medzi užívateľmi. Ďalším cieľom je zdieľanie obsahu (text, fotky, obrázky, hudba, videá, správy, atď.). Sociálne siete sa zväčša delia na súkromne (napr. Facebook) alebo profesné (napr. LinkedIn). Avšak toto delenie sa v posledných rokoch vytráca. Poskytovatelia služieb sociálnych sietí (ďalej len ako „poskytovatelia") pochopili, že model nadväzovania profesných kontaktov (ponuka platených služieb) a model postavený na platenej reklame pri voľne dostupných zábavných službách môžu často splývať, resp. čerpať výhody jeden od druhého. Napriek tejto skutočnosti je charakter sociálnej sieti a jej zameranie (orientácia na koncového užívateľa) stále významné pre prvotné rozhodnutie o voľbe dôkazného prostriedku.[167] V tuzemskej vyšetrovacej praxi sa je možné najčastejšie stretnúť s vyťažovaním informácií zo sociálnych sietí, akými sú Facebook, Google+ (ktorý je súčasťou ekosystému aplikácií Google) a Lide.cz. Či už ide o páchateľa trestného činu, svedka alebo obeť, tieto siete môžu ponúknuť veľké množstvo digitálnych stôp.

Ďalším významným aspektom pre selekciu dôkazného prostriedku je štát pôvodu sociálnej siete, resp. jurisdikcia pod ktorú spadá poskytovateľ (alebo jeho server). Taktiež to je jeho ochota alebo skúsenosť v spolupráci pri vydávaní potrebných údajov.

---

167 Je možné uvažovať o tom, že profesná sieť LinkedIn (známa svojou stavbou osobného profilu v podobe formy životopisu) bude mať u bežného užívateľa väčšiu dôveru pravdivosti zverejnených a dostupných informácii ako sieť Facebook. Samotná podstata tejto siete je založená na vytváraní profesných kontaktov a sprostredkovaní zamestnania. Avšak je potrebné dodať, že aj (pôvodne študentská) sieť Facebook približuje pracovný trh jej užívateľom. Navyše, nedávno zaviedla kontroverzné pravidlá používania „reálnych mien". Viď Facebook.com, Help Center: What names are allowed on Facebook? Dostupné z: https://www.facebook.com/help/112146705538576.

Súčasná odborná trestná literatúra radí sociálne siete medzi prostriedky, ktoré sú podobné sieťam elektronických komunikácií (napr. v prípade zákazu styku s určitými osobami v zmysle § 88d TŘ).[168] Navyše, sociálna sieť má charakter služby informačnej spoločnosti v zmysle ZSIS.[169]

Medzi najväčšie zahraničné sociálne siete v súčasnosti patria:[170]

Meno	Účel	Počet užívateľov	Rok spustenia	Spolupráca pri vydávaní údajov
Google+	Všeobecný	1.600 mil.	2011	Áno
Facebook	Všeobecný (fotky, video, blogy, aplikácie)	1.440 mil.	2004	Áno
Twitter	Všeobecný, mikro-bloging, RSS	645 mil.	2006	Áno
Qzone	Všeobecný (Čína)	480 mil.	2005	n/a
Sina Weibo	Všeobecný, mikrobloging (Čína)	300 mil.	2009	n/a
Habbo	Všeobecný, teenagerský (Fínsko)	268 mil.	2000	Áno
VK	Všeobecný (fotky, video, blogy, aplikácie) – Rusko a bývalé sovietske republiky	250 mil.	2006	n/a
Tumblr	Mikrobloging	227 mil.	2007	n/a
LinkedIn	Profesná sieť	200 mil.	2003	Áno

Význam sociálnych sieti je neprehliadnuteľný. Podľa posledných prieskumov, dve tretiny domácich používateľov internetu v ČR navštevujú sociálne siete a z toho štyri pätiny aspoň raz denne. Štvrtina užívateľov aspoň raz denne niečo okomentuje na sociálnych sieťach a nahrá na internet aspoň raz týždenne vlastnoručne vytvorený obsah.[171] Medzi tri najväčšie české soci-

168 *„Mezi obdobné prostředky (jako síť elektronických komunikací) lze řadit všechny obdobné typy propojení počítačů (mobilních telefonů, smartphonů nebo tabletů) do sítě založené na přístupu na dálku, např. tedy i prostřednictvím nejrůznějších komunikačních systémů (ICQ, Miranda apod.). Patří sem nepochybně i Facebook, Twitter a systémy podobné."* Viď Šámal, 2013a, op. cit., s. 1252.

169 Viď §2 ods.1 písm. a) ZSIS.

170 Viď List of social networking websites. Dostupné z: http://en.wikipedia.org/wiki/List_of_social_networking_websites.

171 Viď Lupač, P., Chrobáková, A., Sládek, J. *Internet v České republice 2014*. Praha: Filozofická fakulta Univerzity Karlovy v Praze. Dostupné z: http://www.worldinternetproject.net/_files/_/193_report_wip_czr2014_v1.pdf.

álne siete v súčasnosti patria Lidé.cz (všeobecná sociálna sieť), Spolužáci.cz (určený pre bývalých spolužiakov) a online zoznamka Libimseti.cz.[172]

Užívatelia internetu už dávno uprednostňujú sociálne siete pred pôvodnými službami, akými sú obyčajný email alebo chat. Sociálne siete tieto služby suplujú a pod jednou strechou v inovatívnom kabáte prinášajú komplexné softvérové riešenia. Príkladom môže byť sociálna sieť Google+, ktorá je súčasťou ekosystému aplikácií Google a predstavuje prístup k službám, akými sú webová prezentácia užívateľa, diskusné fórum, email, chat, VoIP, manažment súborov, úložný priestor, hry a kancelárske nástroje, atď. Preto si je potrebné túto skutočnosť uvedomiť v prípade získavania informácii z osobného profilu a analyzovať všetky prepojené služby ponúkané poskytovateľom alebo oprávnenou treťou osobou integrovanou do sociálnej siete s prepojením na skúmaný účet.[173]

V.1.2 Osobný profil na sociálnej sieti

Zámerom registrácie užívateľa v sociálnej sieti je zdieľať vybrané údaje (často osobnej povahy, napr. meno, adresa, vzdelanie, profesia, stav, národnosť, dátum narodenia, bydlisko, aktivity, záľuby atď.) ďalším užívateľom tejto siete. Množina týchto údajov, či už zadaných počas registrácie alebo neskôr upravených v priebehu existencie účtu, spolu s nahratými grafickými médiami (fotky, obrázky, videá, atď.), publikovanými textami a súbormi (blog, mikroblog, knižnica nahratých súborov, atď.), zoznamom prepojení (kontakt list) a súvisiacimi informáciami o interakciách (wall príspevky alebo odpovede, geolokácie atď.), predstavuje celistvý osobný profil užívateľa sociálnej siete.[174]

Osobný profil užívateľa je ďalej prepojený s prevádzkovými údajmi (napr. záznamy miesta a času prihlásenia, IP adresy, dĺžka spojenia, typ web

172 Viď České sociální sítě. Dostupné z: http://cs.wikipedia.org/wiki/Sociáln%C3%AD_s%C3%ADť.

173 Príkladom môže byť množstvo pripravovaných aplikácií pre sociálnu sieť Facebook, ktoré sú technicky, ale aj právne, previazané s pôvodným poskytovateľom sociálnej siete. Viď Facebook Developers. Dostupné z: https://developers.facebook.com.

174 Avšak je potrebné mať na pamäti, že žiaden z týchto údajov nemusí byť pravdivý. Napr. pri bezplatnom registrovaní účtu v sieti Facebook je potrebné vyplniť nasledujúci minimálny štandard: meno, priezvisko, email alebo tel. číslo mobilu, heslo, pohlavie a dátum narodenia. Jediná informácia, ktorá podlieha verifikácii, je email alebo mobilné číslo.

prehliadača, posledná príchodzia a odchodzia web stránka, atď.) a metadátami súborov, ktoré sú zväčša nedostupné pre samotného užívateľa.[175] Navyše, osobný profil užívateľa nemusí byť sprístupnený širokej internetovej verejnosti. Takmer každá sociálna sieť obsahuje možnosť zamedziť verejnosti vidieť takýto profil, resp. jeho výstupy.

Z právneho hľadiska je obtiažne určiť povahu sociálnej siete. Ide čiastočne o verejný, čiastočne o súkromný priestor. Voľba je ponechaná na technických parametroch systému a prípadnej možnosti výberu užívateľa sprístupniť tento priestor tretím osobám. Ústavný súd vo svojom rozhodnutí k povahe sociálnej siete Facebook uviedol nasledujúce:[176]

> *„Povaha sociální sítě Facebook není dle názoru Ústavního soudu jednoznačně soukromá či veřejná. Vždy záleží na konkrétních uživatelích, jakým způsobem si míru soukromí na svém profilu, případně přímo u jednotlivých příspěvků, nastaví. Teoreticky může uživatel prostřednictvím této sítě komunikovat pouze s jediným dalším uživatelem, a to aniž by tuto komunikaci mohli vidět, či do ní zasahovat, ostatní uživatelé. Taková komunikace by pak jistě mohla být považována za ryze soukromou, byť uskutečněnou prostřednictvím sociální sítě využívané miliardou uživatelů, stejně jako je za soukromou možno považovat emailovou komunikaci dvou osob, uskutečněnou např. prostřednictvím emailové služby Gmail (www.gmail.com), kterou taktéž využívají miliony uživatelů (obdobně v České republice např. emailová služba dostupná na stránkách www.seznam.cz). Uživatel sociální sítě Facebook však má možnost učinit svůj profil také zcela veřejným a tedy přístupným všem uživatelům sociální sítě Facebook, případně i všem uživatelům sítě internet. Tato možnost je hojně využívána např. politickými stranami, zájmovými skupinami, umělci, poskytovateli služeb, obchodníky a dalšími, jejichž cílem je prezentovat se prostřednictvím sociální sítě Facebooku co nejširšímu počtu uživatelů internetu. Toto nastavení ale volí i část „běžných" uživatelů."*

V nadväznosti na toto rozhodnutie je nutné spomenúť ešte jeden prípad, ktorý riešil právnu povahu sociálnej siete. Najvyšší súd sa zaoberal tým, či sociálna sieť a prejavy poslanca na nej, sú prejavy v rámci poslaneckej

175 V tejto časti odkazujeme na kapitolu VII tejto publikácie o dokazovaní prevádzkovými a lokalizačnými údajmi.

176 Viď nález Ústavního soudu sp. zn. III. ÚS 3844/13.

snemovne, a to z dôvodu jeho vyňatia z právomoci orgánov činných v trestnom konaní:[177]

„Nejvyšší soud, pohybujíc se v takto určeném legislativním a výkladovém rámci, konstatuje, že text, uveřejněný na uživatelském profilu internetové sociální sítě facebook jako písemné vyjádření myšlenek obviněného, tehdy poslance Parlamentu ČR, nenaplňuje znaky projevu poslance na půdě sněmovní komory. Nešlo totiž o projev v rámci soutěže politických sil, diskusí při legislativním procesu, jakéhokoli jednání pléna či orgánů sněmovny. Nemohlo ani jít o výkon poslaneckého mandátu ve sněmovně. Veřejně přístupné uživatelské profily internetových sociálních sítí, ostatně stejně jako obecně přístupné internetové stránky, mají v současné době nepochybně již charakter masových komunikačních prostředků, rovnocenných s tiskem, rozhlasem a televizí. Pokud se poslanec Parlamentu rozhodne či je vyzván prezentovat své myšlenky veřejně v prostředcích veřejné komunikace a tyto jsou cíleně zaměřeny právě a jedině vůči veřejnosti, vně sněmovního prostředí, jde o občanské projevy podléhající veřejné kontrole, kritice. V demokratickém společenském zřízení lze zde proto předpokládat občanskou záruku svobodné společnosti proti případným excesům výkonné či soudní moci."

V.1.3 Webová prezentácia

V nadväznosti na osobný profil sociálnej siete je potrebné uviesť, že pôvodná webová prezentácia (web stránka) prestala byť doménou internetových nadšencov a ustupuje informatívnovizuálnym prezentáciám komerčných alebo neziskových subjektov. Navyše web stránky plnia množstvo iných úloh, predstavujú informačné zdroje alebo prístupné brány k internetovým web aplikáciam. Web stránka môže obsahovať všetky vyššie uvedené prvky typické pre osobný profil užívateľa sociálnej siete, ale rovnako často obsahuje aj ďalšie technické údaje spojené s jej užívateľom. Vlastnosťou web stránky je existencia doménového mena (pod ktorým je identifikovateľná) a súvisiaci WHOIS zápis.[178]

177 Viď usnesení Nejvyššího soudu č. j. 3 Tcu 33/2014-26.

178 WHOIS (z angličtiny, who is? - Kto je?) je označenie pre prístupnú databázu a službu, ktorá slúži na evidenciu údajov o majiteľoch internetových domén a IP adries. Tie často môžu odhaliť komplexné pozadie registrovaných web stránok. Niektoré súkromné spoločnosti (napr. domaintools.com) sa zameriavajú na ukladanie historických údajov z týchto databáz, ukladanie historických screenshotov (webhistory.org), čo umožňuje pomerne ľahké vyhľadávanie alebo reverzný výpis (napr. všetky domény jednej spoločnosti alebo majiteľa). Viď Whois. Dostupné z: http://en.wikipedia.org/wiki/Whois.

Pod pojmom web stránka je možné rozumieť jeden alebo viacero súborov (dokumentov) s obsahom presne špecifikovaného kódu (napr. HTML, XHTML), ktoré sa distribuujú prostredníctvom verejnej siete internet (za pomoci HTTP protokolu) z jedného miesta (web servera) a ich výstupy sú zobraziteľné pomocou URL v štandardnom webovom prehliadači (napr. Internet Explorer, Safari, Firefox, atď.). Súbor všetkých dostupných stránok vytvára celosvetovú webovú sieť (world web site).

Web stránka je pomerne široký pojem. Pre účely trestného konania je nutné považovať za web stránku akýkoľvek zdroj informácie čitateľnej a dostupnej na internete alebo intranete prostredníctvom protokolu HTTP/S v štandardnom webovom prehliadači. Navyše, výtlačok (tzv. printscreen) web stránky predstavuje v poslednej dobe jeden z najčastejších dôkazných prostriedkov (v podobe listiny), aj keď často nesprávnym spôsobom interpretovaný. Získané informácie z web stránky môžu byť obsahové (text web stránky) alebo technické (metadáta súborov, v ktorých je stránka naprogramovaná, logy, databázové súbory atď.). Pre potreby tejto kapitoly bude potrebné skúmať možnosti správneho zaistenia a uchovávania web stránok s údajmi potrebnými pre trestné konanie.[179]

V závere je potrebné dodať, že osobný profil sociálnej siete je *de facto* tiež spustiteľná web stránka. Navyše, aj web stránka môže byť v správe tretej osoby – poskytovateľa web hostingu. Preto ak sa v tejto kapitole bude hovoriť o osobnom profile sociálnej siete užívateľa, pokiaľ nie je uvedené inak, má sa na mysli aj web stránka.

V.2 Zaistenie a uchovávanie dôkazného prostriedku

V.2.1 Oprávnená osoba

Oprávnenou osobou v prípade trestného konania pre zaistenie a uchovávanie dôkazného prostriedku osobného profilu sociálnej siete alebo web stránky bude v prvom rade policajný orgán, štátny zástupca alebo súd.

179 V tejto časti odkazujeme na kapitolu VII tejto publikácie o dokazovaní prevádzkovými a lokalizačnými údajmi.

Je potrebné uviesť, že aj advokát (obhajca) má právo v zmysle platných právnych predpisov vyhľadávať dôkazy pre svojho mandanta, avšak v rámci trestného konania je toto právo značne limitované.[180]

Obmedzenie pochádza aj zo strany poskytovateľov, ktorí nemajú žiadnu právnu povinnosť spolupracovať s tuzemským advokátom (opačný prístup je v prípade angloamerického práva, kde advokát za asistencie súdu získava dôkazy aj v trestnom konaní).

Súčasná právna úprava v prípade využitia zaisťovacieho prostriedku v prípravnom konaní alebo konaní pred súdom počíta so všeobecnou edičnou povinnosťou dotknutej osoby zakotvenou v § 78 TŘ.

V praxi sa často tento inštitút využíva spolu s domovou prehliadkou podľa ustanovení § 82 až § 85 b, resp. § 158d ods. 3 TŘ[181] v prípade nedobrovoľného zaistenia elektronických dôkazných prostriedkov. Platný trestný poriadok nerobí rozdiel v otázkach zaistenia dôkazných prostriedkov medzi vecou a elektronicky uloženou informáciou, resp. dátami. Orgány činné v trestnom konaní sa bežne k dôkazom dostávajú prostredníctvom vyťažovania zaistených elektronických nosičov (vecí) za využitia odbornej znaleckej expertízy. Avšak táto koncepcia je v prípade dôkazného prostriedku zo sociálnej siete alebo webovej stránky prekonaná. Kyberpriestor v súčasnosti predstavuje nový fenomén, ktorý umožňuje virtualizovanie dát do takej podoby, že tie sú ťažko fyzicky lokalizovateľné.[182] Čo je však dôležitejšie, zaistenie dát

180 Súčasná úprava vyhľadávanie dôkazov advokátom je obsiahnutá najmä v § 41 ods.1 a 2 a § 89 ods. 2 TŘ. Predmetnú problematiku upravuje aj Výkladové stanovisko Nejvyššího státního zastupitelství č. 9/2004, ke sjednocení výkladu zákonů a jiných právních předpisů k postupu státních zástupců ohledně výkonu práva obhájce (advokáta) postupem podle § 89 odst. 2 věty druhé trestního řádu vyhledávat a předkládat důkazy nebo navrhovat provedení důkazů. Dostupné z: http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2004/stanovisko%209-2004.pdf.

181 *„Aktuální obsah e-mailové schránky je určován vůlí uživatele a lze jej zjišťovat postupem podle § 158d odst. 3 trestního řádu, který je možno považovat za zákonnou licenci prolamující ústavně zaručené právo na ochranu soukromí v e-mailové schránce se nacházejících záznamů, a to podle platné právní úpravy v případě trestního řízení pro kterýkoli úmyslný trestný čin."* Viď Výkladové stanovisko Nejvyššího státního zastupitelství č. 1/2015, ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek. Dostupné z http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2015/1_SL_760-2014.pdf.

182 Napr. cloud systém, ktorý využíva serverové farmy po celom svete a ani sám správca tohto systému nevie, kde sa nachádza ten ktorý sektor disku s požadovanou informáciou, nakoľko tieto môžu byť v neustálom pohybe.

na rozdiel od zaistenia veci (napr. celého hard disku počítača) môže priniesť omnoho šetrnejší a precíznejší zásah do práv vyšetrovaného. Ide o vyjadrenie zásady zdržanlivosti a primeranosti, resp. minimalizácie a subsidiarity, ktoré sú vlastné trestnému právu.[183]

Zaujímavou otázkou je to, že drvivá väčšina informácií osobných profilov sociálnej siete je uložená v počítačovej databáze. Ide o typický prípad, kedy sa na jednom dátovom nosiči nachádza väčšie množstvo dát, často s vecou nesúvisiacich. Preto je nevyhnutná prvotná selekcia, a to nie je len z pohľadu náhrady škody plynúcej v prípade obmedzenia činnosti poskytovateľa (zaistenie celého dátového nosiča), ale aj z pohľadu ochrany práv ostatných účastníkov sociálnej siete.

Navyše, c*onditio sine qua non* pre odňatie veci je aj to, že nejde o listinu, ktorej obsah sa týka okolnosti, o ktorej platí zákaz výsluchu, ibaže došlo k oslobodeniu od povinnosti zachovať vec v tajnosti alebo k oslobodeniu od povinnosti mlčanlivosti (napr. klient pozbaví povinnosti mlčanlivosti svojho advokáta). Podľa výkladového stanoviska najvyššieho štátneho zastupiteľstva, dátové nosiče nie sú listinou v zmysle § 112 TŘ a preto sa na ne nevzťahuje ustanovenie § 78 ods. 2 TŘ:[184]

> *„Úvodem je třeba konstatovat, že pojem „listinných důkazů" je vymezen v ustanovení § 112 odst. 2 tr. ř. tak, že „listinnými důkazy jsou listiny, které svým obsahem prokazují nebo vyvracejí dokazovanou skutečnost, vztahující se k trestnému činu nebo k obviněnému". Bližší výklad tohoto pojmu nečinil v dřívější době žádných potíží, neboť listina byla skutečně materiálně listinou (soukromou či veřejnou) v „papírové" formě. Teprve s rozvojem výpočetní techniky a rozšířením technických nosičů informací, kterými lze rozumět jakákoli média používaná v procesu automatizovaného zpracování dat k záznamům dat a informací, vznikl problém, zda tyto nosiče informací lze považovat za listinné*

183 Viď Kolouch, J. Zajišťovací úkony a důkazní prostředky využitelné v rámci boje s kybernetickou trestnou činností. Dostupné z: https://csirt.cesnet.cz/Dokumenty?action=AttachFile & do=get & target=Zajistovaci+ukony-RTF.pdf.

184 Viď Výkladové stanovisko Nejvyššího státního zastupitelství č. 9/2001, k zajišťování počítačů a jiných nosičů informací při domovní prohlídce a prohlídce jiných prostor a pozemků. Dostupné z: http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2001/stanovisko%209-2001.pdf. Viď Výkladové stanovisko Nejvyššího státního zastupitelství č. 1/2015, ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek. Dostupné z http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2015/1_SL_760-2014.pdf.

důkazy ve smyslu § 112 odst. 2 tr. ř., při jejichž vydání je nezbytné respektovat ustanovení § 78 odst. 2 tr. Ř. Je třeba připustit, že formulace ustanovení § 112 odst. 2 tr. ř. v současné době nevyhovuje změněné situaci v oblasti zpracovávání dat a informací. Ze znění tohoto ustanovení nelze však dovodit, že počítačová technika a další záznamová média jsou svojí povahou listinou. Listinou se záznamy na nosiči informací stanou teprve poté, kdy jsou skutečně z nosiče informací do listinné podoby převedeny."

Otázkou ostáva, či je možné aplikovať na zaistenie dôkazov zo sociálnych sietí a webových prezentácii aj procesný postup nariadenia odposluchu a záznamu telekomunikačnej prevádzky. Nakoľko systém sociálnej siete môže vykazovať znaky telekomunikačnej prevádzky, môže orgán činný v trestnom konaní žiadať o zachytenie každej budúcej informácie, a to len za splnenia podmienok (v prípade „obsahového" záznamu) podľa § 88 ods.1 TŘ alebo v prípade zaistenia telekomunikačných údajov (prevádzkové údaje, akými sú IP adresa, čas a dĺžka pripojenia, atď.) podľa § 88a TŘ.

Nariadiť odpočúvanie a záznam telekomunikačnej prevádzky v prípade dát prenášaných na sociálnej sieti je oprávnený predseda senátu a v prípravnom konaní na návrh štátneho zástupcu sudca. V prípade zistenia prevádzkových údajov (údaje o telekomunikačnej prevádzke, ktoré sú predmetom telekomunikačného tajomstva alebo na ktoré sa vzťahuje ochrana osobných a odkazových dát) a ak nemožno sledovaný účel dosiahnuť inak alebo ak bolo by inak jeho dosiahnutie podstatne sťažené, nariadi v konaní pred súdom ich vydanie súdu predseda senátu a v prípravnom konaní nariadi ich vydanie štátnemu zástupcovi alebo policajnému orgánu sudca na návrh štátneho zástupcu. Takýto príkaz musí byť vydaný písomne a musí byť odôvodnený. Problémy môže predstavovať obtiažna špecifikácia užívateľskej adresy či zariadenia a osoby používateľa (účtu), ktoré musia byť v príkaze presne uvedené.[185] Príkaz musí obsahovať tiež dobu, po ktorú bude odpočúvanie a záznam telekomunikačnej prevádzky vykonávaný, ktorá nesmie byť dlhšia ako štyri mesiace.

185 Súdna prax taktiež riešila otázku príkazu k domovej prehliadke podľa § 83 odst. 1 TŘ, kde bol priestor okrem iného identifikovaný nesprávnou IP adresou. Ústavný súd ČR v konkrétnom prípade vo svojom odôvodnení uviedol, že *„napadený příkaz k domovní prohlídce vyhovoval zákonným požadavkům, neboť z něj bylo zřejmé, kdo jej vydal, o podezření z jakého trestného činu se jednalo, kde se měla prohlídka vykonat, kdo mohl být pachatelem trestné činnosti a rovněž jaké byly důvody vzniku podezření ze spáchání konkrétního trestného činu. Pochybení v podobě nesprávně uvedené IP adresy nebylo takového rázu, aby, přihlédnuto k okolnostem případu, zakládalo pochybnosti o důvodnosti nařízení domovní prohlídky, resp. činilo příkaz k domovní prohlídce nepřezkoumatelným."* Viď Usnesení Ústavního soudu sp. zn. IV. ÚS 3225/09.

V neposlednom rade príkaz musí obsahovať konkrétne skutkové okolnosti, ktoré vydanie tohto príkazu, vrátane doby jeho trvania, odôvodňujú.

V prípade ak je potrebné získať obsah, resp. súvisiace prevádzkové údaje osobného profilu alebo webovej prezentácie uloženej na zahraničnom servery (typické komerčné služby Google+, Facebook, LinkedIn, ktoré majú svoje sídlo a servre v USA) je potrebné, aby orgány činné v trestnom konaní postupovali cestou právnej pomoci. Buď pôjde o vykonávanie jednotlivých úkonov právnej pomoci na základe medzinárodnej zmluvy alebo o realizáciu právnej pomoci bez zmluvného základu. Príkladom môže byť spolupráca členských štátov EÚ, kde základom sú články 82 a 86 Zmluvy o fungovaní Európskej únie. Dňa 29. mája 2000 Rada ministrov EÚ schválila Dohovor o vzájomnej pomoci v trestných veciach, ktorého cieľom je podporovať spoluprácu medzi justičnými, policajnými a colnými orgánmi v rámci Únie doplňovaním ustanovení v existujúcich právnych nástrojoch. Taktiež významnú rolu zohráva aj budapeštiansky Dohovor o počítačovej kriminalite zo dňa 23. 11. 2001. V neposlednom rade ide o Dohovor o vzájomnej pomoci v trestných veciach medzi členskými štátmi EÚ, vypracovaný Radou v súlade s článkom 34 Zmluvy o EÚ. Justičná spolupráca v trestných veciach v rámci EÚ stojí na dvoch kľúčových princípoch: na uznávaní rozsudkov a súdnych rozhodnutí a taktiež na zbližovaní právnych predpisov členských štátov. Ide najmä o úpravu v prípade príkazu na zaistenie majetku a dôkazov v prípade zaisťovania elektronických dôkazov v pôsobnosti cudzieho prevádzkovateľa sociálnej siete. Vyjadrenie týchto princípov vo sfére dokazovania bolo zavŕšené v smernici Európskeho parlamentu a Rady 2014/41/EÚ z 3. apríla 2014 o európskom vyšetrovacom príkaze v trestných veciach.

K otázkam zaistenia elektronického dôkazu sa vyjadril aj slovenský Ústavný súd, ktorý vo veci výberu nástrojov vo svetle existencie trestného inštitútu „uchovania a vydania počítačových údajov" vyslovil, že:[186]

> *„Záujem štátu na ochrane pred zločinnosťou zakladajúci legitímnosť zásahov do práva na súkromie pri realizácii niektorých inštitútov podľa štvrtej hlavy prvej časti Trestného poriadku („Zaistenie osôb a vecí") musí byť uvedený do rovnováhy so závažnosťou*

186 Viď Slovensko. Rozhodnutí Ústavního soudu Slovenské republiky ze dne 25. 8. 2010 sp. zn. III. ÚS 68/2010. Dostupné z https://www.ustavnysud.sk/SearchRozhodnutiav01/rozhod.do?urlpage=dokument & id_spisu=355658.

zásahu do tohto práva. Znamená to zvoliť pri realizácii zásahu čo najmiernejší prostriedok, ktorý je súčasne spôsobilý zabezpečiť dosiahnutie sledovaného cieľa. Samotná právna úprava obsiahnutá v Trestnom poriadku na túto požiadavku reflektuje a určuje na dosiahnutie špecifického cieľa (získanie počítačových údajov dôležitých pre objasnenie trestnej činnosti) prostriedok zaručujúci požadovanú proporcionalitu, ktorým je úkon uchovania a vydania počítačových údajov zakotvený v ustanoveniach § 90 Trestného poriadku. Je nepochybné, že ide o prostriedok, ktorého realizácia predstavuje zásah menšej intenzity v porovnaní so situáciou, keby sa na dosiahnutie cieľa zvolil inštitút vydania, resp. odňatia veci. Napokon to potvrdzuje aj rozdielny režim realizácie uvedených prostriedkov. Vyzvať podľa § 89 ods. 3 Trestného poriadku na vydanie veci je policajt oprávnený bez toho, aby potreboval príkaz či súhlas prokurátora. K odňatiu veci podľa § 91 ods. 1 Trestného poriadku môže policajt pristúpiť na základe vlastného príkazu vydaného po predchádzajúcom súhlase prokurátora, bez predchádzajúceho súhlasu prokurátora môže policajt vydať príkaz len vtedy, ak predchádzajúci súhlas nemožno dosiahnuť a vec neznesie odklad. Naproti tomu na realizáciu úkonu uchovania a vydania počítačových údajov podľa § 90 Trestného poriadku potrebuje policajt nevyhnutne príkaz prokurátora ako orgánu vykonávajúceho dozor nad dodržiavaním zákonnosti pred začatím trestného stíhania a v prípravnom konaní (§ 230 Trestného poriadku). Policajt v danom konkrétnom prípade pre účely získania počítačových údajov zvolil prostriedok – zaistenie samotného počítačového vybavenia (z obsahu zápisnice nie je zrejmé, či išlo o úkon vydania alebo odňatia veci), ktorý pre tento účel zákonná úprava neumožňuje, jeho postup preto treba považovať za nelegálny."

V neposlednom rade je potrebné uviesť, že orgány činné v trestnom konaní by mali mať vypracovanú metodiku (*guidelines, best practices*) pre zaisťovanie a uchovávanie elektronických dôkazov.[187] Tieto interné pravidla sú často jediným spätným kontrolným mechanizmom v prípade nesprávneho zaobchádzania s elektronickým dôkazom v trestnom konaní, a to zo strany nadriadeného orgánu, súdu alebo inej dotknutej osoby. Aj keď tieto pravidlá nebudú verejné (napr. interné predpisy zaisťovania elektronických dôkazov Polície

187 Ide o podobné odporúčania, aké publikuje Európska komisia v prípade miestneho šetrenia hospodárskej súťaže (dawn raid) a o spôsobe zaisťovania elektronických dôkazov. Viď European Commission: Explanatory note to an authorisation to conduct an inspection in execution of a Commission decision under Article 20(4) of Council Regulation No 1/2003. Dostupné z: http://ec.europa.eu/competition/antitrust/legislation/explanatory_note.pdf alebo Štandardy ISO. Viď ISO/IEC 27037:2012, Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence. Dostupné z: http://www.iso.org/iso/catalogue_detail?csnumber=44381.

ČR), ich obsah je významný pre samotné trestné konanie a správny postup kriminalistických expertov. Metodika by mala rovnako obsahovať presný postup v prípade zaisťovania údajov z osobného profilu sociálnej siete a web stránky s aspektom zahraničnej spolupráce. Na druhú stranu, väčšina veľkých poskytovateľov sociálnych sietí publikuje odporúčania pre štátne orgány, akým spôsobom majú požadovať sprístupnenie údajov v prípade trestného konania (*best practices for law enforcements authorities*). V nasledujúcej podkapitole budú osvetlené práve tieto odporúčania.

V.2.2 Povinná osoba

Z pohľadu práva je poskytovateľ sociálnej siete a poskytovateľ web hostingu, resp. systému pre web stránky (blog, mikro blog, atď.) v rovnakom právnom postavení. Často ide o poskytovateľa služby v informačnej spoločnosti.[188] Zaujímavá je tu otázka jurisdikcie vo vzťahu k zahraničným prevádzkovateľom. Podľa odbornej literatúry je jurisdikcia trestného orgánu delokalizovaných právnych vzťahov v kyberpriestore určená miestom protiprávneho následku.[189]

Ako už bolo uvedené, viacerí poskytovatelia sociálnych sietí publikujú odporúčania pre štátne orgány a rovnako sprístupňujú správy transparentnosti.[190] Ide o prehľadné a anonymné štatistiky o dožiadaní štátov a štátnych orgánov smerujúcich k vydaniu údajov a informácií o jednotlivých užívateľoch.[191] Tieto odovzdávané dáta často slúžia ako dôkazné prostriedky v trestnom konaní alebo ako poznatky bezpečnostných služieb (tzv. informačnotechnické prostriedky).

---

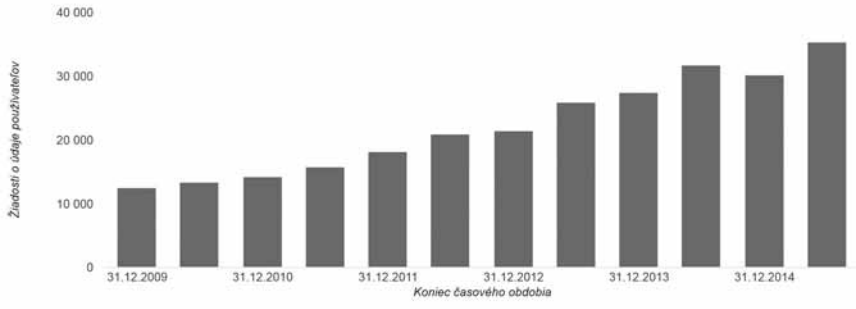
188 Viď § 2 odst. 1 písm. d) ZSIS.

189 Viď Marek, T. Autonomie vůle a soukromí na Facebooku. *Právní rozhledy*, 2015, č. 6, s. 196.

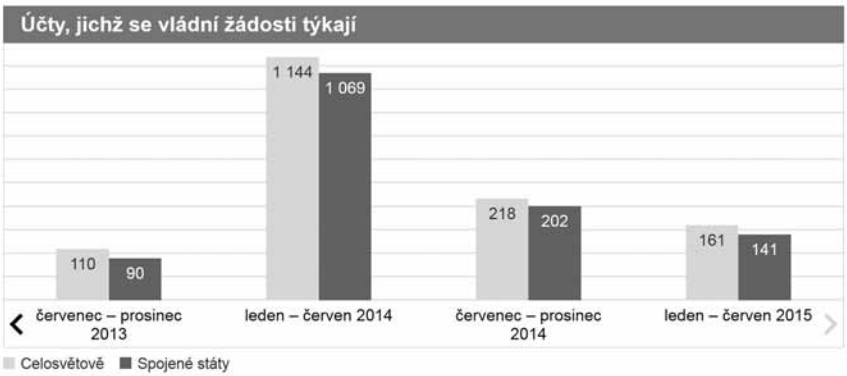
190 Medzi prvými to bola spoločnosť Google (rok 2010), potom Twitter, Microsoft, Verizon, AT & T, Apple, Dropbox, Facebook, Yahoo and CloudFlare. Každá z týchto spoločnosti v súčasnosti zverejňuje správu transparentnosti o tom, ako sprístupňuje svoje dáta tretím osobám. Viď Transparency report. Dostupné z: http://en.wikipedia.org/wiki/Transparency_report.

191 Je potrebné dodať, že viaceré spoločnosti sú nútené pripúšťať nielen žiadosti orgánov štátnej správy, ale aj žiadosti súkromných osôb na odstránenie škodlivého obsahu. Príkladom môže byť medializovaný prípad španiela Maria Gonzalesa proti spoločnosti Google Inc., ktorý dosiahol stiahnutie odkazov na webové stránky o jeho osobe z výsledkov vyhľadávania, viď rozhodnutí SDEU ve věci Google Spain, sp. zn. C-131/12.

Príkladom správy transparentnosti je štatistika spoločnosti Google Inc., ktorá vypovedá o rastúcom trende dopytov štátnych orgánov za posledných päť rokov (oproti roku 2009 išlo o takmer dvojnásobné zvýšenie dopytov):[192]



Obdobný trend potvrdzujú aj iné spoločnosti. Príkladom môže byť profesná sociálna sieť LinkedIn:[193]

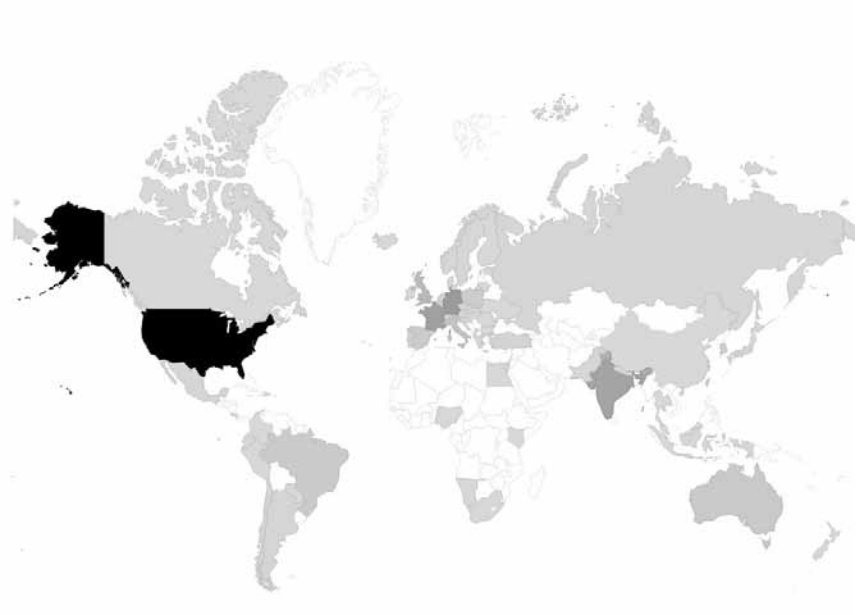


Je zrejmé, že žiadosti o sprístupnenie dát neprichádzajú len z krajiny sídla poskytovateľa sociálnej sieti alebo webovej prezentácie. Práve naopak, ide o strhujúci zápas množstva lokálnych jurisdikcií o výkon práva

192 Viď Informácie o transparentnosti. Žiadosti od vládnych orgánov a súdov. Dostupné z: http://www.google.com/transparencyreport/userdatarequests/?hl=sk.

193 Viď Our Transparency Report. Dostupné z: https://www.linkedin.com/legal/transparency.

v kyberpriestore, v ktorom je ťažké určiť rozhodné právo. Spoločnosť Google udáva, že v roku 2014 obdržala dopyty z vyše 70 štátov:[194]



Google Transparency Report – Penetrácia krajín žiadajúcich o informáciu od januára do júna 2014[195]

194 Zaujímavým momentom je, že americká vláda na základe zákona (FISA, Section 702 a Patriot Act Section 215, resp. National Security letters) neumožňuje spoločnostiam zverejniť presné číslo dopytov. Tie to väčšinou obchádzajú zakomponovaním týchto údajov do iných reportov alebo vágnym určením číslovky, napr. 0-999 atď. Viď Why the transparency report is necessary in the fight for privacy. Dostupné z: http://venturebeat.com/2013/09/12/transparency-reports.

195 Napr. z ČR to bolo 99 žiadostí, v ktorých definičná autorita vyhovela v 57%. Tieto žiadosti sa týkali 154 účtov. Zo SR prišlo 29 žiadostí, v ktorých definičná autorita vyhovela 7%. Tieto žiadosti sa týkali 50 účtov. Graf autora na základe dostupných dát. Viď Requests for user information. Dostupné z: http://www.google.com/transparencyreport/userdatarequests.

Za zmienku stojí taktiež prehľad žiadosti z ČR na spoločnosť Google Inc.:[196]

	Žiadosti o údaje používateľov	Používatelia alebo účty	Percento žiadostí, v prípade ktorých boli predložené niektoré údaje
Júl až december 2014	**117**	**163**	**50 %**
Právne žiadosti	117	163	50 %
Žiadosti o uchovanie informácií	4	10	—
Január až jún 2014	**99**	**154**	**57 %**
Júl až december 2013	**74**	**88**	**39 %**
Január až jún 2013	**63**	**67**	**41 %**
Júl až december 2012	**51**	**84**	**31 %**
Január až jún 2012	**44**	**44**	**32 %**
Júl až december 2011	**—**	**—**	**—**
Január až jún 2011	**—**	**—**	**—**
Júl až december 2010	**—**	**—**	**—**
Január až jún 2010	**—**	**—**	**—**
Júl až december 2009	**—**	**—**	**—**

Zo štatistiky spoločnosti Facebook Inc. je rovnako zrejmý výrazný nárast žiadostí v minulom kalendárnom roku:[197]

Rok	Počet žiadostí OČTK	Počet dotknutých účtov	Percento vyhovenia
2013 (1/2)	10	13	60,00%
2013 (2/2)	14	19	78.57%
2014 (1/2)	11	12	27.27%
2014 (2/2)	22	132	54.55%

Všeobecne poskytovatelia v rámci spolupráce so štátnymi orgánmi štandardne akceptujú nasledujúce skupiny žiadosti:

- Žiadosti od štátnych orgánov týkajúce sa odstránenia obsahu
- Žiadosti týkajúce sa porušenia autorských práv
- Žiadosť o poskytnutie informácií o používateľoch

196 Napr. z ČR to bolo 99 žiadostí, v ktorých definičná autorita vyhovela v 57%. Tieto žiadosti sa týkali 154 účtov. Zo SR prišlo 29 žiadostí, v ktorých definičná autorita vyhovela 7%. Tieto žiadosti sa týkali 50 účtov. Graf autora na základe dostupných dát. Viď Requests for user information. Dostupné z: http://www.google.com/transparencyreport/userdatarequests.

197 Viď Goverment requests report. Dostupné z: https://govtrequests.facebook.com/country/Czech%20Republic/2014-H2.

Žiadosť o poskytnutie informácií o používateľoch je ťažiskovým nástrojom pre získanie relevantných elektronických dôkazov. Prevádzkovatelia môžu spolupracovať tak vo veciach civilného práva (napr. v angloamerickom práve ide o inštitút ediscovery), tak aj vo veciach trestného práva procesného. Tieto žiadosti je možné rozdeliť na žiadosti pochádzajúce zo štátu sídla poskytovateľa (napr. USA, členský štát EÚ – najčastejšie Írsko) a žiadosti mimo tento štát. Je pravidlom, že žiadosť musí byť vždy doplnená právoplatným a vykonateľným rozhodnutím štátneho orgánu.

Typické rozhodnutia súdnych orgánov (v USA podľa anglo-amerického práva), na ktoré odkazujú napr. Google, Facebook, LinkedIn v prípade vydania informácií z účtu užívateľa, sú:[198]

Predvolanie (Subpoena)

- ide o výsledok zjednodušeného procesu získavania prevádzkových údajov
- je vydané bez predchádzajúceho odsúhlasenia sudcom či úradníkom so súdnou právomocou
- predvolanie smeruje iba k špecifickému druhu prevádzkových informácii (taxatívne zákonom stanovených)
- vydáva sa v trestnoprávnych a občianskoprávnych záležitostiach
- Spoločnosť Google k tomuto nástroju uvádza, že „platné predvolanie týkajúce sa vašej adresy v službe Gmail nás môže donútiť k odhaleniu mena, ktoré ste uviedli pri vytváraní účtu, a adries IP, z ktorých ste účet vytvorili a z ktorých ste sa prihlásili alebo odhlásili (vrátane dátumu a času). Na prvý pohľad sa zdá, že zákon ECPA umožňuje orgánu vlády predvolaním alebo súdnym príkazom (viď popis nižšie) donútiť poskytovateľa komunikačných služieb k odhaleniu obsahu určitého typu emailov alebo iného druhu obsahu. Spoločnosť Google však v prípade obsahu služby Gmail a ďalších služieb vyžaduje príkaz k prehliadke vystavený na základe zákona ECPA. Sme totiž presvedčení, že len tak je to v súlade so štvrtým dodatkom Ústavy Spojených štátov, ktorý zakazuje neopodstatnenú prehliadku či konfiškáciu."

198 Viď Requests for user information. Legal process. Dostupné z: http://www.google.com/transparencyreport/userdatarequests/legalprocess.

Súdny príkaz na základe zákona ECPA (ECPA Court Order)

- ide o zložitejší proces získavania prevádzkových a čiastočne aj obsahových údajov;
- väčšinou tu je potrebný výslovný súhlas sudcu najčastejšie podľa trestného procesného práva;
- žiadateľ musí pred súd predložiť konkrétne fakty dokazujúce, že požadované informácie sú relevantné a podstatné pre prebiehajúce vyšetrovanie trestného činu;
- spoločnosť Google k tomuto nástroju uvádza, že „orgán vlády môže získať na základe takého súdneho príkazu tie isté informácie ako na základe predvolania a dodatočné podrobnejšie informácie o používaní účtu. K tým môže patriť adresa IP, ktorá je priradená ku konkrétnemu emailu odoslanému z daného účtu alebo sa použila na zmenu hesla k účtu, (s dátumom a časom) a časť hlavičky emailu, ktorá nie je súčasťou obsahu emailu, napríklad pole „Od:“, „Komu:“ a „Dátum“. Súdny príkaz na základe zákona ECPA je možné získať iba v prípade trestnoprávneho vyšetrovania.“

Príkaz k prehliadke (Search Warrant)

- je to výstup z najprísnejšieho procesu získavania obsahových údajov;
- žiadateľ musí získať súhlas súdu a musí preukázať dôvodné podozrenie, že „kontraband alebo určité informácie súvisiace so zločinom sa aktuálne nachádzajú na konkrétnom mieste, ktorého prehliadka sa požaduje“;
- príkaz k prehliadke musí špecifikovať miestá, ktoré majú byť prehľadané, ako aj cieľ hľadania;
- podľa spoločnosti Google „s príkazom k prehliadke je možné vynútiť sprístupnenie tých istých informácií ako s predvolaním na základe zákona ECPA či súdnym príkazom, ale aj sprístupnenie informácií o vyhľadávacích dopytoch používateľa alebo súkromného obsahu uloženého v účte Google, ako sú správy služby Gmail, dokumenty, fotografie či videá YouTube. Príkaz k prehliadke na základe zákona ECPA je k dispozícii iba v prípade kriminálneho vyšetrovania. Vo videu nižšie je uvedený prehľad, ako kontrolujeme a reagujeme na príkazy k prehliadke na základe zákona ECPA.“

Povolenie odpočúvania (Wiretap)

- je to najkomplikovanejší spôsob získavania (zaznamenávanie) obsahových údajov v reálnom čase – ide o odpočúvanie obsahu komunikácie v reálnom čase (odpočúvanie a záznam telekomunikačnej prevádzky);
- vyšetrujúci orgán/OČTK musí preukázať, že a) používateľ sa dopustil zločinu uvedeného v zákone o odpočúvaní Wiretap Act, b) cieľom odpočúvania je získať informácie o danom zločine, c) odpočúvané telefónne číslo alebo účet súvisia s daným zločinom, a navyše súd musí stanoviť, že všetky „štandardné spôsoby vyšetrovania tohto zločinu zlyhali (alebo by pravdepodobne zlyhali), prípadne že sú predovšetkým príliš nebezpečné na to, aby sa realizovali";
- je si nutné uvedomiť, že existujú zákonné obmedzenia týkajúce sa doby (lehoty) na zákonné odpočúvania a tiež požiadaviek na informovanie odpočúvaných používateľov (za akých môžu byť s povolením oboznámení).

Povolenie sledovania prichádzajúcej alebo odchádzajúcej komunikácie (Pen Register, and Trap and Trace)

- ide o pomerne jednoduchý proces získavania prevádzkových údajov v reálnom čase (IP, web adresa, logy, atď.);
- žiadateľ musí preukázať, že informácie, ktoré sa získajú, budú relevantné pre aktuálne prebiehajúce vyšetrovanie trestného činu (opäť ako možnosť pre OČTK v trestnom konaní);
- zaujímavosťou je, že spoločnosť Google sa domnieva, že v tomto prípade ide o príliš nízky štandard ochrany práv jej užívateľov, a preto začala spolupracovať so združením Digital Due Process s cieľom zabezpečiť to, aby tieto povolenia podliehali súdnej kontrole.

V prípade ak sa tuzemský orgán činný v trestnom konaní rozhodne využiť inštitút právnej pomoci na základe medzinárodnej dohody o vzájomnej právnej pomoci (napr. prostredníctvom Ministerstva spravodlivosti USA), často musia jeho rozhodnutia alebo rozhodnutia súdov splniť vyššie uvedené štandardy (minimálne s nimi korešpondovať). Je potrebné dodať, že internetový poskytovatelia sa môžu rozhodnúť dobrovoľne spolupracovať, a to aj bez formálneho medzinárodného postupu právnej pomoci.

Ide o prejav transparentnosti a právomoci poskytovateľa v kyberpriestore týkajúceho sa sociálnych sietí.[199]

V.3 Forenzná analýza

Odborná zahraničná literatúra v prípade forenznej analýzy „internetových dát" hovorí o nasledujúcich krokoch:[200]

- vyhodnotenie získaných dát
- experimentovanie (pripustenie nových neortodoxných techník)
- spájanie informácií a hľadanie vzájomných súvislostí
- validácia (overovanie faktov a skutočností)

Forenzná analýza dát získaných od poskytovateľov sociálnych sietí je predovšetkým determinovaná výberom technického spôsobu odovzdania dát orgánom činným v trestnom konaní.

V prípade dobrovoľného odovzdania požadovaných dát ide o proces:

- odovzdania dátového nosiča (HDD, USB, CD, DVD, atď.) spolu s preberacím protokolom nebo
- sprístupnenia vzdialeného úložiska s požadovanými dátami (SFTP, zabezpečená web stránka, SSH prístup, atď.) a verifikovateľným logovacím systémom;
- a následnú kriminalistickú analýzu vykonanú povereným súdnym znalcom.

V prípade nedobrovoľného zaistenia požadovaných dát ide často o odňatie dátových nosičov (HDD, USB, CD, DVD, atď.), resp. celých počítačových systémov (hardware) a servov. Taktiež nie je vylúčená možnosť kopírovania dát na mieste. Rovnako môže ísť o zaistenie priestorov (zapečatenie) a následnú analýzu tam nájdených počítačov (serverov).

Pri týchto úkonoch je nutné apelovať na uvedenú zásadu zdržanlivosti a primeranosti, resp. minimalizácie a subsidiarity, ktorá sa premieta aj do práce poverených súdnych znalcov alebo znaleckých organizácii. Špecifikum

199 Napr. spoločnosť Google uvádza, že *„údaje používateľa môže v reakcii na platný právny proces zo strany orgánov vlád iných krajín ako USA poskytnúť dobrovoľne, pokiaľ sú tieto žiadosti v súlade s medzinárodnými normami, americkým právom, pravidlami spoločnosti Google a zákonmi krajiny, z ktorej žiadosť pochádza."* Viď Requests for user information. Legal process. Dostupné z: http://www.google.com/transparencyreport/userdatarequests/legalprocess.

200 Viď Mason, S. *Electronic evidence*. London: LexisNexis. 2010, s. 65.

skúmaných dát z osobných profilov je ich previazanosť s cudzími dátami (nezaujatými osobami), ku ktorým je nutné pristupovať obzvlášť opatrne. Navyše, je možné doplniť, že skúmané dáta by v čase konania mali byť uložené na objektívne verifikovateľnom zdroji (napr. elektronický spis) s tým, že každá zo strán by mala presne stanovené práva a povinnosti pri nahliadaní, resp. nakladaní s obsahom. Je zrejmé, že tieto úskalia sa dnes pomerne často odbíjajú znaleckým dokazovaním, ktoré si však žiada neúnosné časové nároky na priebeh sporu a často zbytočne, resp. nezákonne prejudikuje právne otázky.

V.4 Vykonanie dôkazu

Každý dobre vykonaný dôkaz by mal predstavovať záruku reflektovania minulých dejov. Slovami Holländera *„fair spôsob vedenia dôkazného konania (ktoré je v trestnom procese spojené s aplikáciou najmä zásad rovnosti zbraní, prezumpcie neviny, práva na obhajobu, in dubio pro reo) sleduje jednak nachádzanie pravdy v konflikte proti sebe stojacich strán, a jednak snahu o minimalizáciu dôkazných chýb, justičných omylov, a tým aj minimalizáciu prijímania nespravodlivých rozhodnutí"*.[201] Je preto zrejmé, že existuje úzka väzba kategórie pravdivosti na povahu konania, akým je práve vykonanie dôkazu prostredníctvom elektronického dôkazného prostriedku.

Súd v trestnom konaní bude vykonávať dôkazy získané zo sociálnych sietí alebo web stránok najmä na základe ustanovení § 112 TŘ (ako listinný dôkaz), § 105 TŘ (znalecké posudky, odborné vyjadrenia, resp. § 101 TŘ (ako výsluch svedka) alebo § 113 TŘ (ako obhliadku). Avšak súčasná prax často spočíva v tom, že výkonanie dôkazu osobného profilu alebo web stránky sa ohraničuje na tlač získaných informácií do listinnej podoby a jej predloženie súdu.[202] Z technického pohľadu sa tak zbytočne stráca širšia

201 Viď Holländer, 2006, op. cit., s. 204.

202 Typicky to je napr. v prípade stalkingu keď *„Soudy obou stupňů vyšly především z doslovného znění obsahu výhrůžky, aniž by důsledně hodnotily okolnosti, za nichž jí bylo užito, a to ve spojení s poznatky o chování obviněného k poškozené. Soud prvního stupně z výpovědi svědkyně K. T., s níž korespondují i záznamy komunikace mezi ní a obviněným na facebooku založené ve spise, zjistil, že v komunikaci s ní se obviněný ve dnech 11. 2. a 12. 2. 2009 vyjádřil tak, že „ju zabije", přičemž z kontextu jeho sdělení bylo patrné, že tím míní poškozenou a že tak chce učinit za vulgární nadávky, jimiž ho označila právě poškozená (č. l. 29, 30).* "Viď usnesení Nejvyššího soudu sp. zn. 8 Tdo 1082/2011.

suma informácií (metadáta súborov, zdrojový kód, atď.), ktoré nie sú síce okamžite viditeľné, ale môžu predstavovať zaujímavý zdroj informácií. Ústavný súd sa už dávnejšie zaoberal požiadavkami zákazu deformácie dôkazov a uviedol, že:[203]

> *„Podle názoru Ústavního soudu musí obecný soud dodržet vysoký standard i tam, kde jde o hodnocení vypovídací schopnosti a hodnověrnosti důkazu samotného. Jdeli o hodnocení důkazů, procesní předpisy sice ponechávají volnost soudci obecného soudu, avšak nemůže jít o volnost absolutní, nevázanou na zkušenostmi prověřenou pravděpodobnost určitých skutečností. Důkaz musí být odrazem skutečných událostí a situací, což má garantovat, aby byl jednotlivec uznán vinným na podkladě objektivních a skutečnosti odpovídajících zjištění, protože pouze ona jsou způsobilá ospravedlnit krajní opatření spočívající ve zbavení jednotlivce jeho osobní svobody (nález Ústavního soudu, sp. zn. IV. ÚS 335/05, Sbírka nálezů a usnesení, svazek 41, str. 453). Právě z tohoto důvodu lze formulovat určité principy vážící se k provádění a hodnocení důkazů, např. princip opomenutého důkazu, princip možnosti verifikace důkazů směřujících proti obžalovanému či zásadu zákazu deformace důkazů; aplikace těchto principů je dovoditelná i z nálezu Ústavního soudu, sp. zn. III. ÚS 398/97, Sbírka nálezů a usnesení, svazek 11, str. 125, v němž jde o zákaz vyvozování z důkazu takových skutkových zjištění, která při racionálním zhodnocení z provedeného důkazu nevyplývají, a nejsou podporována ani obecnou zkušeností.“*

Ďalšou vlastnosťou elektronického dôkazu je aj to, že elektronický záznam sa môže pomerne jednoducho a nepozorovane (automaticky) modifikovať alebo zmeniť. A to aj v čase jeho vykonávania. Takáto zmena je spôsobená povahou alebo okolnosťami, za ktorých bolo s týmto záznamom nakladané. Inak povedané, už len samotným kopírovaním záznamu dát sa môže kontaminovať ich obsah.[204] Kľúčom k správnemu vykonávaniu elektronických dôkazov je pochopenie vlastnosti – volatility elektronického dôkazného prostriedku samotným súdom. Ide o správne chápanie dôkazného procesu od počiatočnej fázy – zaisťovania počítačových údajov, až po hodnotenie dôkazov.

---

203 Viď nález Ústavního soudu sp. zn. I. ÚS 3094/08, N 103/53 SbNU 293.

204 Ústavný súd už dávnejšie uviedol, že *„účelem trestního řízení není jen náležité zjištění trestných činů a potrestání pachatelů, nýbrž i projednání věcí s plným šetřením práv a svobod zaručených Listinou a mezinárodními smlouvami o lidských právech a základních svobodách, jimiž je Česká republika vázána“*. Viď nález Ústavního soudu sp. zn. II. ÚS 889/10, N 237/59 SbNU 405.

V.5 Hodnotenie dôkazu

Za dôkazný prostriedok je možné označiť zákonom upravený spôsob získania informácie (skutočnosti, ktorá má byť zistená – porov. § 89 ods. 1 TŘ). Za dôkaz môže slúžiť všetko, čo môže prispieť k objasneniu veci, najmä výpovede obvineného a svedkov, znalecké posudky, veci a listiny dôležité pre trestné konanie a ohliadka. Ako už bolo uvedené, každá zo strán môže dôkaz vyhľadať, predložiť alebo jeho vykonanie navrhnúť. Skutočnosť, že dôkaz nevyhľadal alebo nevyžiadal orgán činný v trestnom konaní, nie je dôvodom na odmietnutie takéhoto dôkazu.

Pre dokazovanie elektronickými dôkaznými prostriedkami bude prilieha-vosť voľby právnej normy súdom okrem iného závislá aj na tom, ako dobre bude zistená samotná skutková podstata prostredníctvom vykonávania takýchto dôkazov. Trestné procesné právo týkajúce sa otázky dokazovania je vystavané na zásade voľného hodnotenia dôkazov, avšak len za predpokladu dodržania ostatných právnych zásad Podľa Holländera má dokazovanie pre právne rozhodovanie okrem noetickej podstaty práve aj funkciu presvedčovania a argumentovania[205]. Tá je vlastná elektronickému vykonávaniu dôkazov. Neraz video alebo zvuk, resp. správa vo svojej vlastnej podobe vyzerajú ako zrkadlo reality minulých dejov. Preto je možné tiež hovoriť aj o oceňovaní dôkazu, resp. hľadaní jeho sily[206]. Tento proces je sfinalizovaný síce predložením úplného súhrnu dôkazov, avšak správna bonifikácia dôkaz-ných partikularít je o to viac dôležitejšia ak ide o použitie elektronických dôkazných prostriedkov.

Podľa Vladimíra Smejkala elektronické dôkazy majú jednu zásadnú slabinu: *„ťažko ich priraďujeme ku konkrétnej osobe, pretože dokázať, kto „mal ruky na klávesnici" je možné len s využitím elektronického podpisu alebo iných autentizačných metód (použitie hesla, SMS, čipové karty atď.). Našťastie sú zvyčajne súčasťou kruhu ďalších, hoci nepriamych dôkazov a môžu aj v tomto prípade zohrať dôležitú úlohu v rámci príslušného konania."*[207] Práve informácie z osobných profilov (web stránok)

205 Viď Holländer, 2006, op. cit., s. 195.

206 Viď Boguszak, J., Čapek, J., Gerloch, A. *Teorie práva*. Praha: Eurolex Bohemia, 2001, s. 132.

207 Viď Smejkal, V. Elektronické důkazy – současnost či budoucnost českého soudnictví? Dostupné z: http://www.bulletin-advokacie.cz/elektronicke-dukazy-soucasnost-ci-budoucnost-ceskeho-soudnictvi.

môžu často priniesť ďalšie nepriame dôkazy, ktoré nasvedčujú dokazovaným skutočnostiam.

Nedávno riešený problém vytvorenia falošného facebookového profilu (trestný čin poškodzovania cudzích práv) zdôraznil dôležitý aspekt hodnotenia elektronických dôkazov v nadväznosti na ujmu práv poškodenej:[208]

> *„Není žádných pochyb o tom, že zpřístupnění fotografií, na nichž je poškozená zachycena nahá při provádění soulože bez souhlasu poškozené širokému okruhu osob, a to způsobem vyvolávajícím dojem, že tyto fotografie zpřístupnila samotná poškozená, vážnou újmu na uvedených právech poškozené způsobuje. O tom ostatně svědčí i popis dopadu jednání obviněného na poškozenou obsažený ve výpovědi poškozené, ale i dalších svědků. Pokud jde o tvrzení obviněného o absenci znaku uvedení v omyl, nelze se s tímto ztotožnit. Obviněný založil facebookový profil na jméno poškozené, uvedl zde kontaktní údaje na ni a zveřejnil její fotografie. Jednoznačně tímto způsobem byly osoby, kterým k profilu bylo umožněno přistoupit, uváděny v omyl ohledně majitele profilu. Obdobné závěry platí i o dopisech, které obviněný psal jménem poškozené v první osobě s uvedením adresy poškozené jako odesílatele na obálkách. Rovněž pokud soud prvního stupně dochází k závěru, že obviněný využil omylu poškozené, která nepředpokládala, že její intimní fotografie pořízené s jejím souhlasem obviněný tímto způsobem zneužije, je možno se s takovým závěrem ztotožnit. […] Nejvyšší soud po prostudování předmětného spisového materiálu zjistil, že soudy srozumitelně popsaly subjekty uvedené v omyl, jakož i subjekt, jemuž byla způsobena újma na právech a rovněž podrobně vyložily, proč bylo jednání obviněného JUDr. PhDr. I. S., PhD. kvalifikováno jako přečin poškození cizích práv podle § 181 odst. 1 písm. a), b) tr. zákoníku, ale také to, v čem spočívala vážná újma na právech a komu byla způsobena. Nutno uvést, že intenzita škodlivého následku rozhodně nebyla v posuzovaném případě zanedbatelná, neboť poškozená J. T. byla zveřejněním jejích intimních fotografií zesměšněna, v souvislosti s inkriminovanými dopisy musela podávat vysvětlení svým nadřízeným, byly prověřovány její odměny a byla řešena i její bezpečnostní prověrka u Národního bezpečnostního úřadu. Při posouzení uplatněné právní námitky proto Nejvyšší soud dospěl k závěru, že znaky skutkové podstaty přečinu poškození cizích práv podle § 181 odst. 1 písm. a), b) tr. zákoníku byly naplněny.“*

Možno na záver už len dodať, že v priebehu trestného konania je nutné postaviť výsledky dokazovania do svetla poznania, ktoré bude založené na úsilí priblížiť sa zhode myšlienky so skutočnosťou (minulým dejom) v tej miere, ktorá zodpovedá požiadavkám overovania, tak aj falzifikovania, ktoré

208 Viď usnesení Nejvyššího soudu sp. zn. 4 Tdo 815/2014.

je možné v určitej dobe na túto mieru priblíženia položiť.[209] Tieto požiadavky overovania, tak aj falzifikovania, musia primárne vychádzať zo zásad a princípov trestného práva, avšak rovnako musia brať v zreteľ existujúce technikality dôkazov pochádzajúcich z osobných profilov sociálnych sietí alebo webových prezentácii.

V.6 Námety de lege ferenda

Ako zásadný námet *de lega ferenda* je možné uviesť úvahu nad existenciou elektronického spisu v trestnom procese. Za dodržania podmienok technologickej neutrality, elektronický spis má potenciál priniesť mimoriadne zaujímavú platformu na riadne vykonávanie elektronických dôkazov, ktoré môže miestami nabúrať a prestavať už zažité partikularity procesného práva dôkazných prostriedkov. Vzhľadom na zvyšujúcu sa početnosť nehmotných elektronických dôkazných prostriedkov je povinnosťou každého praktikujúceho právnika brať na zreteľ citlivosť a volatilitu elektronických dôkazov. Preto virtualizácia súdneho spisu predstavuje stabilnú konštrukciu ochrany týchto základných povinností a napomáha pri zachovaní elementárnej podstaty tohto inštitútu zvyšovať dynamiku prístupu k informáciám pre zúčastnene procesné strany.

V.7 Zhrnutie

V uvedenej kapitole bolo popísané, akým spôsobom je možné získať, analyzovať, vykonať a hodnotiť elektronický dôkaz pochádzajúci z osobných profilov sociálnych sietí alebo webových stránok. Tieto „internetové dôkazy" ukazujú špecifickú vlastnosť *ubiquity* kyberpriestoru, t.j. vlastnosť bez previazanosti na lokálnu jurisdikciu a jej právne zásady a princípy. Nepochybne, právny proces vydávania dát bude podliehať najmä jurisdikcii sídla prevádzkovateľa alebo jeho pobočky. Na jej postup sa bude ďalej vzťahovať národné, ale aj medzinárodné právo. Otázkou však ostáva, čo ak právo štátu žiadateľa je v rozpore s právom štátu prevádzkovateľa a zároveň neexistuje žiadna medzinárodná zmluva alebo medzinárodným právom uznaná zásada ako postupovať. Môže sa zdať, že národné alebo medzinárodné

[209] Viď Holländer, 2006, op. cit., s. 201.

právo vystupuje ako záchytný bod alebo garancia tradičných hodnôt. Avšak nie je možné ich automaticky premietať do virtuálnej sféry bez ďalšieho. Treba si totiž uvedomiť, že v prípade vydávania dát požíva prevádzkovateľ pomerne vysokú mieru samostatnej rozhodovacej právomoci. Už výber technológie pre spracovanie a odovzdanie požadovaných dát reguluje to, aký rozsah bude mať zásah do práv dotknutého subjektu. Navyše, zahraničný poskytovateľ určuje aj procedúru prijatia žiadosti, jej spracovania a príp. odovzdania zaistených dát. Týmto sa stáva definičnou autoritou v pravom zmysle slova. Ovplyvňuje nie len regulovaného užívateľa, ale aj prípadné výsledky trestného vyšetrovania v prípade dopytu o poskytnutie dát.

VI DOKAZOVÁNÍ PROVOZNÍMI A LOKALIZAČNÍMI ÚDAJI

VI.1 Vysvětlení pojmu

Blanketní uchovávání provozních a lokalizačních údajů představuje styčný bod mezi povinností zajistit důvěrnost přenášené komunikace, povinností uchovávat některé údaje o této komunikaci a procesními oprávněními některých subjektů veřejné moci k takto uchovávaným datům přistupovat. Poskytovatelé telekomunikačních služeb nesmí zpracovávat obsah přenášené komunikace s poukazem na základní práva obsažená v čl. 10 a čl. 13 LZPS a čl. 8 EÚLP (dále také „Úmluva"), což je na zákonné úrovni upraveno v § 89 ZEK Povinnost zajistit technicky i organizačně důvěrnost zpráv se vztahuje i na provozní a lokalizační údaje se zprávami spojené.[210] Obsah zpráv nemůže poskytovatel uchovávat za žádných okolností, zákon však v některých případech ukládá povinnost uchovávat provozní a lokalizační údaje.

VI.1.1 Povinné subjekty

Přijetím Směrnice 2006/24/ES byly členské státy Evropské unie zavázány přijmout národní legislativu, která by umožnila uchovávání provozních a lokalizačních údajů jako zákonnou výjimku z výše uvedených práv. Účelem uchovávání bylo vyšetřování, odhalování a stíhání trestných činů, jak uvádí recitál 11 Směrnice. Recitál 10 Směrnice pak zmiňoval přímou souvislost s bojem proti terorismu, resp. s útoky v Londýně v roce 2005. Členské státy tak musely zajistit uchovávání údajů potřebných k dohledání a identifikaci zdroje sdělení, údaje potřebné k identifikování adresáta sdělení, údaje potřebné k identifikaci komunikačního vybavení uživatelů nebo jejich údajného komunikačního vybavení a údaje potřebné ke zjištění polohy mobilního komunikačního zařízení. Povinnými subjekty jsou dle § 94 odst. 1 ZEK

[210] Praktický rozdíl mezi samotným obsahem komunikace a provozními a lokalizačními údaji je možné popsat analogií s obálkou, kdy na obálce jsou údaje, které umožňují doručení dopisu (tedy dohledání zamýšleného příjemce komunikace) a které jsou, na rozdíl od obsahu dopisu, veřejně viditelné.

právnické nebo fyzické subjekty zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací. Vzhledem ke znění poslední věty § 2 písm. n) ZEK je nutné si uvědomit, že pod pojem služeb elektronických komunikací spadají i služby informační společnosti, které spočívají zcela nebo převážně v přenosu signálů po sítích elektronických komunikací.

Povinnými subjekty pak jsou samozřejmě telefonní operátoři, v případě internetových služeb je však v praxi situace komplikovanější. Obecně lze říci, že se jedná pouze o poskytovatele připojení.[211] Klíčovým pro určení povinného subjektu tak je, jestli poskytuje zároveň s jinými (webovými) službami i služby připojení. V případě, že dochází k poskytování připojení, se tak subjekt stává povinným a musí uchovávat údaje v rozsahu stanoveném Vyhláškou Ministerstva průmyslu a obchodu č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů (dále jen „vyhláška"). Např. v případě ust. § 2 odst. 3 vyhlášky je subjekt poskytující služby připojení a webové služby povinen uchovávat údaje o přenosech zpráv elektronické pošty. Subjekt poskytující pouze služby webové pak údaje v souladu s vyhláškou uchovávat nemusí.

V praktické rovině se zdá být celkem problematickým postavení poskytovatelů Wi-Fi připojení. V případě neveřejných Wi-Fi se poskytovatel, za použití gramatického výkladu § 2 písm. j) ZEK, nestává subjektem povinným uchovávat provozní a lokalizační údaje. Pokud je ale poskytováno veřejně přístupné Wi-Fi, dochází k naplnění definice služby elektronických komunikací.[212] Mělo by tak následovat splnění povinnosti uchovávat provozní a lokalizační údaje, ke kterému však často nedochází. Lze totiž konstatovat, že kdyby všichni tito poskytovatelé zažádali o náhradu nákladů podle § 97 odst. 7 ZEK, představovalo by to značnou administrativní zátěž pro celý aparát. Zároveň si lze jen těžko představit, že by údaje byly orgány činnými

211 Iuridicum Remedium. *Co dělají provideři a telefonní operátoři s našimi daty? Studie praxe poskytovatelů internetových a telekomunikačních služeb (ISP).* Dostupné z: http://slidilove.cz/sites/default/files/Studie%20ISP_final.pdf.

212 Technická realita zde říká, že subjekt, se kterým má dané např. restaurační zařízení smlouvu o poskytnutí připojení, přiřadí restauračnímu zařízení veřejnou IP adresu (může jich být i více). Na provozovateli restauračního zařízení by pak mělo být, aby dle vlastního logu provozu umožnil orgánům činným v trestním řízení další postup. Subjekt, který smluvně zajišťuje připojení, totiž již nemá přístup k IP adresám za NATem.

v trestním řízení po této skupině subjektů vyžadovány. Mezi orgány činnými v trestním řízení převládá názor,[213] že je nutné striktně odlišovat mezi osobami podnikajícími v režimu ZEK a osobami podnikajícími ZSIS. Osoby podnikající podle ZEK mají povinnost chránit telekomunikační tajemství. Tímto postupem se dá dojít k závěru, že orgány činné v trestním řízení se od poskytovatelů veřejné Wi-Fi sítě údaje nikdy získat nepokusí, protože je nepovažují za subjekty, které by byly povinné je uchovávat. Tímto způsobem tak výkladem dochází ke korekci gramatického výkladu § 2 písm. n) ZEK.

VI.1.2 Rozsah povinnosti

Povinnost či možnost specifickým způsobem uchovávat provozní a lokalizační údaje se odehrává v několika rovinách. Nejvíce diskutabilní z nich je národní legislativa, vytvořená implementací Směrnice 2006/24/ES. V současné době představuje národní implementaci[214] této povinnosti § 97 odst. 3 a odst. 4 ZEK, které stanovuje povinným subjektům povinnost uchovávat provozní a lokalizační údaje po dobu 6 měsíců.[215]

Provozní údaje jsou ustanovením § 90 ZEK definovány jako jakékoli údaje zpracovávané za účelem přenosu zprávy sítí nebo za účelem účtování.[216] Příkladmo se tak jedná o informace o názvech, číslech nebo adresách, které poskytuje odesílatel sdělení nebo uživatel spojení za účelem přenosu sdělení a jakýkoli převod těchto informací sítí, po které se sdělení přenáší, za účelem provedení přenosu. Lokalizačními údaji se dle § 91 ZEK rozumí jakékoli zpracovávané údaje určující zeměpisnou polohu koncového

213 Implicitně potvrzený v rámci Výkladové stanovisko Nejvyššího státního zastupitelství č. 1/2015, ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek. Dostupné z http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2015/1_SL_760-2014.pdf.

214 Byť byla směrnice zneplatněna, tato úprava původně vznikla jako její implementace.

215 Pro zmapování vývoje tohoto ustanovení a na něj navazujících procesních oprávnění orgánů činných v trestním řízení viz Myška, 2013, op. cit., s. 64-81.

216 Definice přitom odpovídá mezinárodním dokumentům. Provozními údaji se dle čl. 1 písm d) Úmluvy o počítačové kriminalitě (104/2013 Sb. m. s.) rozumí *„jakákoli počítačová data vztahující se ke komunikaci prostřednictvím počítačového systému, vytvořená počítačovým systémem, jakožto součástí komunikačního řetězce, uvádějící původ, cíl, cestu, čas, datum, objem nebo trvání komunikace nebo typ příslušné služby."* Dle čl. 2 písm. b) Směrnice 2002/58/ES se pak jedná o *„jakékoli údaje zpracovávané pro účely přenosu sdělení sítí elektronických komunikací nebo pro jeho účtování"*.

zařízení uživatele veřejně dostupné služby elektronických komunikací.[217] Zde se např. jedná o zeměpisnou šířku, délku a nadmořskou výšku koncového zařízení, dále pak informaci o směru pohybu, úrovni přesnosti lokalizačních informací, identifikaci síťové buňky, ve které je zařízení umístěno v určitém časovém bodu. Přesnou specifikaci metadat, která musí povinné subjekty uchovávat, stanovuje prováděcí předpis, kterým je Vyhláška. § 2 Vyhlášky stanovuje rozsah uchovávání provozních a lokalizačních údajů v závislosti na tom, zda se jedná o veřejné telefonní sítě s přepojováním okruhů, veřejné mobilní telefonní sítě, nebo sítě elektronických komunikací.

V rámci současné diskuze, která předcházela dubnovému ostře sledovanému rozhodnutí SDEU ve spojených případech C-293/12 a C-594/12 a pokračuje i po něm, se otevřela otázka budoucnosti uchovávání provozních a lokalizačních údajů. Zrušená Směrnice 2006/24/ES nebyla jediným harmonizačním opatřením dopadajícím na tuto oblast, ale částečně do ní vstoupila i Směrnice 2002/58/ES, resp. národní implementace v ní obsažených čl. 6 a čl. 9. Tyto články jsou reflektovány v § 90 a § 91 ZEK. § 90 odst. 2 ZEK stanovuje povinnost smazat vytvářená provozní a lokalizační data, jakmile nejsou potřebná pro přenos zpráv, s výjimkou následujících odstavců. Výjimkou je obecně nutnost uchovávat data po dobu, po kterou je možné vyúčtování poskytnutí služby právně napadnout nebo tuto platbu právně vymáhat. V tomto případě se jedná o obecnou tříletou promlčecí lhůtu podle § 629 odst. 1 zákona č. 89/2012 Sb., občanský zákoník. § 91 ZEK pak dává poskytovateli možnost uchovávat anonymizované lokalizační údaje za účelem poskytování služeb s přidanou hodnotou, k čemuž je ale zapotřebí získat souhlas.

Obecně se tak dá říci, že i v případě možného odstranění nejvíce diskutabilní povinnosti stanovené § 97 odst. 3 a odst. 4 ZEK budou existovat metadata, která mohou být využita orgány činnými v trestním řízení. Metadata uchovávaná za účelem vyúčtování podle § 90 ZEK zůstávají k dispozici minimálně po dobu 3 let. Teoreticky může být doba uchovávání ještě prodloužena, protože v případě zahájení sporu podle § 129 odst. 3 ZEK musí být

217 Dle evropské legislativy, resp. dle čl. 2 písm. c) Směrnice 2002/58/ES, *„jakékoli údaje zpracovávané v síti elektronických komunikací, které určují zeměpisnou polohu koncového zařízení uživatele veřejně dostupné služby elektronických komunikací."*

metadata uchována do doby jeho rozhodnutí. Při načasování zahájení sporu ke konci promlčecí lhůty je tedy možné podle délky trvání sporu uchovat data i za hranici tří let. Rozsah takto uchovávaných metadat je menší, než je rozsah stanovený Vyhláškou, ale Nejvyšší soud dovodil povinnost uchovávat za účelem vyúčtování i URL adresy: [218]

> *„Z hmotněprávní úpravy obsažené v ustanovení § 64 odst. 1 zákona o elektronických komunikacích vyplývá, že osoba poskytující služby elektronických komunikací má ve sporu s účastníkem, popřípadě uživatelem veřejně dostupné služby elektronických komunikací o úhradu ceny za poskytnutou službu břemeno tvrzení, že účastníku (uživateli) poskytl veřejně dostupnou službu elektronických komunikací v rozsahu a kvalitě odpovídajícím ceně, kterou mu za službu vyúčtoval a která byla platná v době poskytnutí služby, a důkazní břemeno, pokud jde o prokázání tohoto tvrzení.*
>
> *[…]*
>
> *Důkazem k prokázání tvrzení žalobce o obsahu poskytnuté datové služby mohly být nejen záznamy o tzv. URL adresách (o adresách webových stránek navštívených účastníkem v době datového spojení), které žalobce mohl (aniž by tím – jak správně dovodil odvolací soud - porušoval ustanovení čl. 10 Listiny základních práv a svobod) zpracovávat jako provozní údaje nezbytné pro vyúčtování ceny za poskytnutou službu do konce doby, během níž mohlo být vyúčtování ceny právně napadeno nebo úhrada mohla být vymáhána (srov. § 90 odst. 1 a 3 zákona o elektronických komunikacích), ale i jiné důkazní prostředky, kterými bylo možné zjistit obsah datové služby poskytnuté účastníku a které jsou příkladmo uvedeny v ustanoveních § 51 odst. 1 správního řádu a § 125 větě první, o. s. ř.“* [219]

Tvrzení, že by v případě sjednané paušální náhrady za použití služeb nebylo nutné uchovávat data za účelem vyúčtování dle § 90 ZEK, není dle Nejvyššího soudu relevantní. Dokázání prostého objemu přenesených dat nepostačuje ke splnění povinnosti stanovené § 64 odst. 2 ZEK. Nejvyšší soud zde fakticky nutí poskytovatele služby uchovávat obsahová data z důvodu opatrnosti a unesení důkazního břemene budoucího sporu plynoucího z vyúčtování služby. Uchovávání záznamu o URL adresách tak není dle Nejvyššího soudu porušením čl. 10 LZPS. Jestli by tento závěr obstál

218 Detailní anotaci tohoto rozhodnutí, jakož i souvisejících rozhodnutí nižších instancí, podává Stupka, Václav. Uchovávání provozních a lokalizačních údajů pro účely vyúčtování poskytnutých služeb elektronických komunikací. *Revue pro právo a technologie,* 2014, roč. 4, č. 8.

219 Viz rozsudek Nejvyššího soudu sp. zn. 21 Cdo 2058/2012.

při přezkumu Ústavním soudem, zůstává otázkou. A contrario je nutné říci, že pokud by ústavní přezkum uzavřel neústavnost uchovávání za tímto účelem, operátor by byl v problematické pozici a nebyl by schopný efektivně chránit vlastní majetková práva.

Tato verze uchovávání provozních údajů mimo režim § 97 odst. 3 a 4 ZEK je sice do určité míry použitelná, ale neobsahuje lokalizační údaje a i skladba provozních údajů je odlišná. Určitá míra použitelnosti zde tak je zejména díky SNejvyššímu soudu. URL adresami je totiž možné vytvářet vzorce chování (připojení na konkrétní účty na sociálních sítích a následné připojení např. na stránky obsahující dětskou pornografii), ale to vyžaduje velkou neopatrnost pachatele. Navíc jen minimum povinných subjektů uchovává URL adresy.

VI.2 Zajištění a uchování důkazního prostředku

Jak bylo řečeno výše, váže se k povinnosti uchovávat provozní a lokalizační údaje i specifický procesní postup orgánů činných v trestním řízení, který je nutné využívat při zajišťování legálních důkazních prostředků. Použití zde nachází ústavní maxima obsažená v čl. 2 odst. 3 Ústavy, že státní moc lze uplatňovat pouze v případech, v mezích a způsobem, který stanoví zákon. Orgány, kterým dle § 97, odst. 3 ZEK náleží zákonné zmocnění k přístupu k uchovávaným metadatům, představují orgány činné v trestním řízení, jejichž zákonnému zmocnění pak odpovídá procesní postup uvedený v § 88a TŘ.[220]

Impulzem k formulaci původního[221] znění tohoto ustanovení a jeho uvedení do TŘ novelou č. 265/2001 Sb. byl Ústavní soud, který vztáhl ochranu podle čl. 13 LZPS i na provozní a lokalizační údaje, nejenom na obsah zpráv.[222] Za pomoci analogie tak dovodili nezbytnost orgánů činných trestním řízení

220 Orgány činné v trestním řízení samozřejmě nejsou jedinými oprávněnými subjekty, ale další subjekty uvedené v § 97 odst. 3 ZEK, tedy Bezpečnostní informační služba, Vojenské zpravodajství a Česká národní banka nejsou pro účely tohoto textu relevantními subjekty.

221 Později derogovaného nálezem Ústavního soudu sp. zn. Pl. ÚS 24/11, N 217/63 SbNU 483 (43/2012 Sb.).

222 Konkrétně se jednalo o nálezy Ústavního soudu sp. zn. II. ÚS 502/2000, N 11/21 SbNU 83 a sp. zn. IV. ÚS 536/2000, N 29/21 SbNU 251.

postupovat při přístupu k těmto údajům podle § 88 tehdy účinného TŘ, který, stejně jako dnes, upravoval procesní postup v případě nasazení obsahových odposlechů. Po novele TŘ č. 273/2012 Sb. dosáhl § 88a dnešní podoby.

Možnosti postupu jsou tak v současné době dvě. Možnost získání údajů bez souhlasu sledované osoby je podmíněna kumulativním splněním níže uvedených podmínek, což při podání písemné a odůvodněné žádosti vede k vydání soudního příkazu. Příkazu není potřeba, pokud je získán souhlas uživatele, k němuž se mají poskytnuté údaje vztahovat dle § 88a odst. 4 TŘ.

K uplatnění institutu bez souhlasu osoby[223] tedy musí být kumulativně splněny následující podmínky:

1. Řízení je vedeno pro
   a) úmyslný trestný čin s horní hranicí sazby nejméně tři roky nebo
   b) pro některý z trestných činů porušení tajemství dopravovaných zpráv dle § 182 tz, pro trestný čin podvodu dle § 209 TZ, pro trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 TZ, pro trestný čin opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat dle § 231 TZ, pro trestný čin nebezpečného vyhrožování dle § 353 TZ, pro trestný čin nebezpečného pronásledování dle § 354 TZ, pro trestný čin šíření poplašné zprávy dle § 357 TZ, pro trestný čin podněcování k trestnému činu dle § 364 TZ, pro trestný čin schvalování trestného činu dle § 365 TZ nebo
   c) pro úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva.

223 Těchto je naprostá většina. V roce 2011 se jednalo o 97,3 %, v roce 2012 to bylo 85,4 % a v roce 2013 pak 95,9 %.
Viz Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR za rok 2011. Dostupné z http://www.mvcr.cz/soubor/ppr-2261-13-cj-2012-0099ta-analyza-2012-final-ver-pdf.aspx, s. 167.
Dále viz Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR za rok 2012. Dostupné z http://www.mvcr.cz/soubor/analyza-odposlechu-a-zaznamu-pdf.aspx, s. 143.
Viz také Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR za rok 2013. Dostupné z http://www.mvcr.cz/soubor/ppr-102-31-cj-2014-990390-analyza-odposlechu-a-sledovani-za-rok-2013-pdf.aspx, s. 133.

2. Sledovaného účelu nelze dosáhnout jiným způsobem, popř. by jiný postup dosažení účelu podstatně stěžoval.
3. Vydání údajů musí nařídit předseda senátu nebo samosoudce (v přípravném řízení soudce dle § 26 TŘ).

Oproti původně derogované úpravě je v současné době zakotvena povinnost informovat uživatele, o němž byly provozní a lokalizační údaje vyžádány, samozřejmě pokud je znám. Toto opatření představuje záruku, že subjekt, jehož údaje jsou předávány, bude mít určitou možnost obrany. V České republice se jedná o možnost podat ve lhůtě šesti měsíců Nejvyššímu soudu návrh na přezkoumání zákonnosti příkazu ke zjištění údajů o telekomunikačním provozu. Tato záruka představuje promítnutí aktuálního výkladu čl. 8 EÚLP do českého práva.

Podrobnosti o přístupu orgánů činných v trestním řízení k údajům o telekomunikačním provozu obsahuje ust. § 3 vyhlášky. Ten stanoví, že s příkazem soudu je nutné obrátit se na kontaktní pracoviště, kterým je ÚZČ.[224] Jakoukoli snahu orgánů činných v trestním řízení obcházet tuto proceduru neformálním postupem nebo postupem dle § 8 TŘ je nutné vnímat jednoznačně negativně. Vyhověním žádosti o součinnost se totiž povinný subjekt vystavuje riziku správní sankce, hlavně je ale takto získaný důkaz důkazem nepřípustným. § 88a TŘ zde navíc nepředstavuje lex specialis pouze ve vztahu k § 8 TŘ, ale i k povinnostem stanoveným v § 158 odst. 9 TŘ. Co se pak týká rozsahu údajů, jejichž poskytnutí je možné vyžádat dle § 88a odst. 1, jedná se pouze o údaje uchovávané podle § 97 odst. 3 a 4 ZEK. Žádné jiné údaje není tímto postupem možné vyžádat.[225]

Podle vyhlášky dochází k předání údajů ve formě datového souboru. K prokázání jeho autentičnosti se dle ust. § 3 odst. 4 používá uznávaného elektronického podpisu nebo elektronické značky nebo je v případě paralelní

224 Dle Závazného pokynu policejního prezidenta č. 186/2011, o vyžadování odposlechu a záznamu telekomunikačního provozu a údajů o uskutečněném telekomunikačním provozu, ve znění závazného pokynu policejního prezidenta č. 139/2012. Ten je veřejnosti nedostupný a ani autorům se dokument nepodařilo získat. Jeho existence je nicméně očividná z policejní statistik uvedených v předchozí poznámce pod čarou.

225 Viz Výkladové stanovisko Nejvyššího státního zastupitelství č. 1/2015, ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek. Dostupné z http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2015/1_SL_760-2014.pdf.

listinné či elektronické komunikace možné použít i průvodní dopisy. Zpráva o uskutečněném komunikačním provozu může tedy být poskytnuta v listinné podobě nebo v elektronické podobě umožňující dálkový a nepřetržitý přístup.[226]

VI.3 Forenzní analýza

Forenzní analýza je v případě provozních a lokalizačních údajů z velké části přímo na poskytovateli, který tyto údaje povinně uchovává. Na rozdíl od obsahových odposlechů je možné údaje počítačově zpracovávat za pomocí specializovaného software. Z některých automaticky zpracovávaných údajů je možné usuzovat i přímo na obsah komunikace.[227]

Je zajímavým faktem, že § 88a TŘ představuje, minimálně na základě interpretace Vrchního soudu v Olomouci, účinnou překážku pro některé druhy forenzní analýzy. Pokud například plyne z povahy vyžadovaného znaleckého posudku, že na jeho základě dojde ke zjištění dat o uskutečněném telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství, je před pověřením znalce tímto úkonem potřeba postupovat dle § 88a TŘ a vyžádat si příkaz soudu, což dovodil Vrchní soud v Olomouci:[228]

> *„V této souvislosti je nutno poukázat na rozhodnutí Ústavního soudu, sp. zn. II. ÚS 502/2000, podle kterého je soukromí každého člověka hodno ochrany ve smyslu čl. 13 Listiny základních práv a svobod nejen ve vztahu k vlastnímu obsahu zpráv podávaných telefonem, ale i ve vztahu k údajům o volaných číslech, datu a čase hovoru, době jeho trvání, v případě mobilní telefonie o základových stanicích zajišťujících hovor. Tyto údaje jsou nedílnou součástí telekomunikace uskutečněné prostřednictvím telefonu. Jestliže ústavní pořádek České republiky připouští průlom této ochrany, děje se tak pouze a výlučně v zájmu ochrany demokratické společnosti, případně v zájmu ústavně zaručených práv a svobod jiných; sem spadá především nezbytnost daná obecným zájmem na ochraně společnosti před trestnými činy a na tom, aby takové činy byly zjištěny a potrestány. Přípustný je tedy pouze zásah do základního práva nebo svobody člověka ze strany státní moci, jestliže jde o zásah nezbytný ve výše uvedeném smyslu. K tomu, aby nebyly překročeny meze nezbytnosti, musí existovat systém adekvátních a dostatečných záruk, skládající se z odpovídajících právních předpisů a účinné kontroly jejich dodržování."*

226 Viz Šámal, 2013a, op. cit., s. 1224.
227 Srov. Myška, 2013, op. cit., s. 23.
228 Viz usnesení Vrchního soudu v Olomouci sp. zn. 5 To 42/2010.

Pokud by tedy výstupem forenzní analýzy zajištěných důkazních prostředků měly být provozní a lokalizační údaje, je nutné jejich použití jako důkazního prostředku legitimizovat postupem podle § 88a TŘ. Toto ustanovení se tedy, podle interpretace Vrchního soudu v Olomouci, nevztahuje pouze na samotnou žádost k subjektům povinným uchovávat provozní a lokalizační údaje podle § 97 odst. 3 ZEK. Mělo by se vztahovat obecně na přístup k jakýmkoliv údajům, které jsou předmětem komunikačního tajemství nebo na něž se vztahuje ochrana osobních a zprostředkovacích údajů, jak lze ostatně dovodit výše uvedeným gramatickým výkladem § 88a odst. 1 TŘ.

Toto rozhodnutí je, zejména z pohledu procesního práva, jen těžko udržitelné. Soudní příkaz podle § 88a ost. 1 TŘ totiž přikazuje konkrétnímu subjektu, který drží provozní a lokalizační údaje, aby je dal k dispozici orgánům činným v trestním řízení. Dle shora uvedeného přístupu Vrchního soudu by adresátem musel být obviněný. K zajištění přístroje obsahujícího provozní a lokalizační údaje navíc došlo na základě jiného procesního postupu a jeho automatická nelegitimita v případě forenzní analýzy např. zajištěného telefonu by zbytečně zatěžovala zúčastněný aparát. Považujeme to za jeden z projevů schizofrenie současného TŘ, který na rozdíl od některých zahraničních úprav neobsahuje ustanovení o zajištění dat, nemluvě o tom, že používat k argumentaci nález Ústavního soudu sp. zn. II. ÚS 502/2000 ve chvíli, kdy došlo k zásadní diskontinuitě zejména zavedením § 88a TŘ, je chybné. I když tedy argumentace zvolená Vrchním soudem působí prospěšně z hlediska ochrany soukromí, je nutné ji považovat za nešťastný exces.

VI.4 Provedení důkazu

Jak je výše uvedeno, důkazem, který je možno provést, je zpráva o zjištění údajů o uskutečněném telekomunikačním provozu. Ta může být provedena v podobě listinné nebo v podobě elektronické. V obou případech je samozřejmě v souladu s výkladem účinné právní úpravy[229] nutné zajistit možnost ověření pravosti a pravdivosti prováděného důkazu. Vyhláška v tomto případě přímo upravuje způsoby poskytnutí důkazního prostředku orgánům činným v trestním řízení včetně několika způsobů ověření pravosti a pravdivosti

229 Viz § 112 a § 213 TŘ.

datového souboru. Dle § 3 odst. 4 písm. a) vyhlášky se tak používá uznávaný elektronický podpis nebo uznávaná elektronická značka připojená k poskytnutému datovému souboru nebo některý ze způsobů ověření autentičnosti mimo samotný datový soubor. Dále se jedná dle § 3 odst. 4 písm b), c), d) a e) o průvodní dopisy v elektronické nebo listinné podobě, které obsahují identifikaci poskytnutých souborů a údaje pro ověření jejich správnosti nebo úplnosti. Provedením tohoto důkazu je tak možné podložit některá tvrzení vznesená v průběhu řízení – jedná se např. o uskutečnění telefonického kontaktu nebo o přistoupení k obsahu z určitého stroje.

V tomto bodě považují autoři za nutné poznamenat, že praxe provádění tohoto důkazu znaleckým posudkem za situace, kdy by postačilo provést důkaz listinou, jak se v některých případech na soudech děje, není dlouhodobě udržitelnou.

VI.5 Hodnocení důkazu

Jak bylo výše zmíněno, je nutné vnímat jakoukoli snahu orgánů činných v trestním řízení obcházet § 88a TŘ negativně, protože se tím vytváří nezákonný důkaz, který neobstojí tváří v tvář účinné obhajobě. Vzhledem k nepřímé povaze důkazu provozními a lokalizačními údaji to nemusí mít pro řízení fatální následky, přesto se tím vytváří prostor pro zpochybnění některých závěrů z dokazování plynoucích.

Provozní a lokalizační údaje dle české judikatury nevedou k identifikaci konkrétní osoby jako pachatele nebo osoby zúčastněné na trestném činu, protože vedou vždy pouze k identifikaci komunikujícího přístroje. De facto se tak jedná pouze o jeden ze článků důkazního řetězce. Ani označení provozního a lokalizačního údaje jako osobního údaje nemůže pro účely trestního řízení vést k jednoznačné identifikaci osoby. V případě mobilního čísla se jedná o osobní údaj,[230] přesto není možné bez dalšího dovodit, že uskutečnění telefonického kontaktu z určitého telefonního čísla bez pochyb identifikuje držitele čísla jako volajícího. Pro účely trestního řízení se nejedná o dostatečné ztotožnění, byť se pro účely správního práva jedná o osobní údaj.

230 Srov. rozsudek Nejvyššího správního soudu sp. zn. 9 As 34/2008, č. 1844/2009 Sb. rozh. NSS.

Nejkomplikovanějším je použití IP adresy, kde je navíc nutné rozlišovat mezi IP adresou statickou a dynamickou. Dynamickou IP adresou se částečně řeší nedostatek veřejných IP adres, kdy je za pomoci NATu jedna veřejná IP adresa přiřazena více koncovým uživatelům. DHCP protokol automaticky přiřadí IP adresu skupině přístrojů, nicméně i v tomto případě poskytovatelé připojení vědí, komu je jaká adresa v daný okamžik přiřazena. Podle WP29 se v případě dynamické IP adresy jedná o osobní údaj, protože poskytovatel internetového připojení je schopen identifikovat uživatele za pomoci přiměřených prostředků, kterými jsou logy[231], a dynamickou IP adresu je tak možné při specifikaci času přiřadit konkrétnímu stroji. Tento nepřímý důkaz, sám o sobě menší vypovídající hodnoty, tedy identifikuje konkrétní stroj. Až dalším procesním postupem je možné dosáhnout na další důkazy, např. cestou zajištění počítače či mobilního telefonu. Ač tento závěr nezbytně nutně komplikuje práci orgánů činných v trestním řízení, je nutné na něm trvat. Snaha spojit IP adresu s konkrétní osobou vedla v některých případech v minulosti snad až k nechtěně humorným excesům:[232]

> *„Přestože tato zřejmě na počítači obviněného občas pracovala, vzhledem k jejímu vzdělání a zájmům šlo nejpravděpodobněji o prohlížení snadno přístupného obsahu jako např. webových stránek. Sdílení souborů vyžaduje hlubší zkušenosti s prací na počítači, které L. Š. nemá. Má je naopak obviněný, který je dokonce zaměstnán ve výrobě počítačových komponent. Ze stejných důvodů je soud přesvědčen i o tom, že programové vybavení nalezené na pevných discích počítače obviněného a na jeho CD a DVD discích užíval obviněný a zhotovil jeho rozmnoženiny. O tom, že data na těchto médiích spravoval obviněný a nikoliv jeho družka do značné míry svědčí i skutečnost, že se na nich nachází i pornografie – srov. audiovizuální dílo pojmenované „porno – Jenna.Jameson – Baby doll".*

Spojovat zařízení s osobou podpůrným užitím genderového stereotypu však není pravidlem. V dnešní době lze již odkázat i na některé případy ilustrující kvalitní práci vedoucí ke ztotožnění konkrétní osoby jako uživatele konkrétního identifikovaného stroje:[233]

231 Viz Opinion 4/2007, on the concept of personal data, Article 29 Data Protection Working Party. Dostupné z http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

232 Jedná se o shrnutí závěrů nižších soudů obsažených v usnesení Nejvyššího soudu sp. zn. 5 Tdo 31/2010.

233 Viz usnesení Nejvyššího soudu sp. zn. 4 Tdo 1482/2012.

„Dokazováním bylo zjištěno, že autorem předmětných e-mailů byl právě obviněný, toto vyplynulo z elektronické podoby těchto e-mailů, které v tzv. hlavičce obsahují i IP adresu, ze které byly e-maily odesílány, z šetření týkajícího se subjektů, kterým byly jednotlivé IP adresy přiděleny a z šetření týkajícího se založení a užívání všech tří e-mailových adres. Ze znaleckého posudku Mgr. Pavlíka a dále z listinných důkazů pak vyplynula vazba mezi počítačem v domácnosti obviněného a počítačem na pracovišti obviněného (kterou měl obviněný přidělenu do 20. 12. 2008) a od tohoto data (20. 12. 2008) na jedné straně a zjištěnými e-mailovými schránkami […]. To koresponduje se zjištěním, že z IP adres počítače obviněného na pracovišti a na tyto adresy byl veden provoz v inkriminovaném období a to nejen předmětné e-maily […], ale i obsáhlejší provoz, který by odpovídal pracovnímu nasazení obviněného. Současně bylo z tohoto počítače korespondováno uvedenými e-mailovými adresami […] Za tohoto stavu není nic nelogického na závěru soudů, že pachatelem činu byl obviněný. Soudy došly k tomuto závěru postupem, při kterém hodnotily důkazy v souladu s jejich obsahem […]. Své hodnotící úvahy soudy jasně, srozumitelně a logicky vysvětlily.“

I když tedy mají metadata velkou vypovídací hodnotu, není možné tvrdit, že bez dalšího jednoznačně identifikují konkrétní osobu jako pachatele nebo osobu zúčastněnou na trestném činu. Logickému vysvětlení návaznosti nepřímých důkazů je nutné věnovat zvýšenou pozornost.

VI.6 Náměty de lege ferenda

Po rozhodnutí SDEU ve spojených případech C-293/12 a C-594/12, kterým došlo ke zrušení Směrnice 2006/24/ES, je nutné věnovat značnou pozornost budoucnosti uchovávání provozních a lokalizačních údajů. Některé členské země EU totiž na rozsudek zareagovaly zrušením své národní úpravy. [234] Jak jsme výše uzavřeli, toto nemusí a nebude znamenat konec uchovávání provozních a lokalizačních údajů. S přihlédnutím k povinnostem stanoveným v § 90 ZEK budou data v limitované míře dostupná i nadále. Pokud by došlo ke zrušení § 97 odst. 3 a 4 ZEK, jednalo by se pro orgány činné v trestním řízení o komplikaci, nikoli však o fatální záležitost. Fatální záležitostí pro ochranu práv a svobod by na druhé straně mohlo být zrušení § 88a TŘ. Ten je dáván přímo do souvislosti s povinností uchovávat provozní a lokalizační údaje pro účely orgánů činných v trestním řízení

234 Viz Harašta, J., Myška, M. Budoucnost data retention. *Trestněprávní revue*, 2015, č. 10.

a dalších subjektů. Jak jsme ale výše dovodili, jeho význam jde daleko za toto úzké vnímání a ve své podstatě naopak zvyšuje současný standard ochrany základních práv. Stejně jako v minulosti by jeho zrušení mohlo navíc zasáhnout do probíhajících řízení, s čímž se v minulosti vypořádal Ústavní soud přímo ve zrušujícím nálezu sp. zn. Pl. ÚS 24/11[235], což ale nakonec stejně nezabránilo opakovaným řízením.[236]

Jako alternativa současné úpravy uchovávání provozních a lokalizačních údajů dle § 97 odst. 3 a 4 ZEK je prosazován tzv. quick-freeze, kterým dojde na žádost orgánů činných v trestním řízení k zajištění údajů uchovávaných podle § 90 ZEK.[237] Výhodou by v českém prostředí mohla být dlouhá doba uchovávání, daná tříletou promlčecí lhůtou. Zajímavou alternativou se jeví také digitální otisky připojujícího se přístroje pomocí vyhodnocení použitého prohlížeče – tato metoda vyhodnocující verzi prohlížeče a použití specifických zásuvných modulů (pluginů) je prezentována jako velice úspěšná. Dosahuje vysoké míry úspěšnosti při identifikaci a vykazuje jen minimum falešně pozitivních identifikací.[238] Tyto způsoby nejsou orgánům činným v trestním řízení neznámé. Je možné získávat z těchto údajů důkazy použitelné pro trestní řízení. Jedná se však pouze o náhražku uchovávání provozních a lokalizačních údajů. K tomu totiž v současné době opravdu neexistuje žádný ekvivalent.

VI.7 Shrnutí kapitoly

Tato kapitola obsahovala rozbor problematiky významu provozních a lokalizačních údajů jako důkazního prostředku. Problematika uchovávání provozních a lokalizačních údajů a přístupu k nim je celoevropsky předmětem zájmu nejen odborné veřejnosti, ale i častých odborných diskuzí a ústavněprávního přezkumu. Důvodem je mimořádná kontroverze tohoto nástroje, který představuje, jak již potvrdily národní soudy i SDEU, mimořádný zásah

235 Viz odst. 59 zmiňovaného nálezu Ústavního soudu sp. zn. Pl. ÚS 24/11.
236 Viz usnesení Ústavního soudu sp. zn. III. ÚS 2797/12.
237 Podrobněji Myška, 2013, op. cit., s. 106-107.
238 Eckersley, P. How unique is your web browser? In: Attalah, M. J., Hopper, N. J. (eds.). *Privacy Enhancing Technologies*. Springer, 2010, s. 1-18. Výzkum uzavřel, že 94,2% prohlížečů používajících Flash nebo Javu je unikátních.

do vybraných lidských práv. Zároveň ale poskytuje nutné důkazy, bez kterých by orgány činné v trestním řízení v současné době nebyly schopné efektivně vykonávat a plnit své základní funkce.

Jakýkoli přístup k provozním a lokalizačním údajům tak musí splnit relativně přísné ústavněprávní kautely, tedy zejména probíhat zákonnou cestou, a to dle příslušného ustanovení TŘ v závislosti na povaze podnikatelské činnosti uchovávajícího subjektu (k tomu více i v kapitole IX). Aby totiž mohly být tyto údaje použity před soudem jako důkaz, musí být shromážděny a analyzovány v souladu s účinnou právní úpravou.

Zásadním problémem provozních a lokalizačních údajů je také jejich povaha jako nepřímého důkazu, protože u některých těchto údajů (zcela typicky např. v případě IP adresy) nedochází k přímé identifikaci člověka, ale pouze k identifikaci konkrétního komunikujícího zařízení. S tímto faktem, se kterým se pojí i povaha provozního a lokalizačního údaje jako nepřímého důkazu, se zatím české soudy vyrovnávají. Je tedy nutné klást zvláštní důraz na adekvátní zasazení těchto údajů do důkazního řetězce další činností orgánů činných v trestním řízení.

VII DOKAZOVÁNÍ ODPOSLECHEM

Jedním z velmi efektivních nástrojů získávání důkazního materiálu je odposlech a záznam telekomunikačního provozu. Tento nástroj, historicky využívaný především k odposlechu přenosu hlasové komunikace, se v dnešní době stále více využívá k zajišťování obsahu dat přenášených v elektronických sítích. Vzhledem k technologické neutralitě síťové platformy může být obsahem těchto dat prakticky cokoliv – od hlasových a obrazových záznamů přes dokumenty až po kryptoměny. Vzhledem ke specifikům fungování elektronických sítí a obsahu, který je po nich přenášen, představuje často odposlech a záznam takového přenosu technickou i právní výzvu.

Není pochyb o tom, že využití tohoto nástroje představuje významný zásah do práva na soukromí jednotlivce, které zaručuje Listina základních práv a svobod. V čl. 13 LZPS stanoví, že tajemství zpráv a záznamů uchovávaných v soukromí, zasílaných poštou nebo jiným způsobem či podávaných telefonem, telegrafem nebo jiným zařízením se zaručuje. K porušení této ochrany však i podle Listiny dojít může, a to v případech a způsobem, který stanoví zákon.

Trestní řád je jedním z předpisů, které umožňují zásah do ochrany telekomunikačního tajemství a které stanovují předpoklady a podmínky, jež možnost takového zásahu podmiňují. Klíčovým ustanovením TŘ je v tomto smyslu § 88, který upravuje odposlech a záznam telekomunikačního provozu. Ač je jeho úprava historicky směřována především ke komunikaci hlasové či faxové, umožňuje rovněž odposlech komunikace datové. Rychlý vývoj technologií však ani v tomto případě není právní úprava schopna reflektovat, a proto je při využívání § 88 pro získávání důkazů z datového přenosu často poněkud problematické. Tato kapitola se proto věnuje pojmovým nejednoznačnostem právní úpravy a využitím odposlechem získaných dat jako důkazu v trestním řízení.

VII.1 Vysvětlení pojmu

Odposlech a záznam telekomunikačního provozu, upravený v § 88 TŘ, je zajišťovací institut trestního práva, který za stanovených podmínek

umožňuje orgánům činným v trestním řízení zasahovat do tajemství zpráv podávaných prostřednictvím telekomunikačních zařízení a získávat z nich skutečnosti důležité pro trestní řízení.

Za účelem technologické neutrality však tato právní úprava žádným způsobem nedefinuje pojmy odposlechu, záznamu či telekomunikačního provozu. V odborné literatuře jsou poskytovány různé definice těchto pojmů.

VII.1.1 Odposlech a záznam

Odposlech je možno chápat obecně jako záměrné, utajené a současné vnímání obsahu komunikace, zprostředkované telekomunikačními zařízeními (nebo sítěmi), a záznam jako souběžné zachycení obsahu probíhající komunikace na nosičích záznamu, které umožňují jeho uchování a následnou reprodukci[239]. Odposlech a záznam lze tedy zjednodušeně chápat jako soudem aprobovaný postup orgánů činných v trestním řízení, které v reálném čase sledují a zachycují probíhající telekomunikační provoz za účelem získání informací důležitých pro trestní řízení.

Na tomto místě je vhodné rovněž dodat, že za zákonný odposlech je považován jen takový odposlech, který byl pořízen policejním orgánem. Je však otázka, zda je přípustný odposlech pořízený jednou z komunikujících stran. Ústavní soud konstatoval, že: *„Jestliže soudy připustily provedení důkazu přečtením záznamu telefonických hovorů proti výslovnému nesouhlasu jednoho z účastníků hovoru, došlo tím k zásahu do jeho základního práva na ochranu tajemství zprávy podávané telefonem podle čl. 13 Listiny základních práv a svobod – a důsledně vzato i do základního práva stěžovatele na spravedlivý proces podle čl. 36 odst. 1 Listiny základních práv a svobod – a důkaz jako takový je třeba považovat za nepřípustný.“*[240] Na druhou stranu, opačný postoj lze sledovat v usnesení Nejvyššího soudu sp. zn. 5 Tdo 459/2007, který konstatuje, že *„[s] ohledem na ustanovení § 89 odst. 2 tr. ř. zásadně nelze vyloučit možnost, aby byl k důkazu použit i zvukový záznam, který byl pořízen soukromou osobou bez souhlasu osob, jejichž hlas je takto zaznamenán. Ustanovení § 88 tr. ř. se zde neuplatní, a to ani analogicky. Přípustnost takového důkazu je však nezbytné vždy posuzovat též s ohledem na respektování práva na soukromí, zakotveného*

239 Viz Musil, 2007, op. cit., s. 363. Obdobně též Novotná, J. K některým otázkám dokazování odposlechem a záznamem telekomunikačního provozu. *Trestněprávní revue*, 2003, č. 10, s. 290 a násl.

240 Viz usnesení Ústavního soudu sp. zn. ÚS 191/05 N 161/42 SbNU 327.

v čl. 8 Úmluvy o ochraně lidských práv a základních svobod, práva na nedotknutelnost osoby a jejího soukromí ve smyslu čl. 7 odst. 1 a čl. 10 odst. 2 Listiny základních práv a svobod."[241] Lze tedy dovodit, že využití záznamu pořízeného jednou komunikující stranou jako důkazu v trestním řízení není zcela vyloučené. Bude však vždy podrobeno testu proporcionality, který bude hodnotit míru zásahu do soukromí a důsledky využití záznamu pro trestní řízení.

VII.1.2 Telekomunikační provoz

Poněkud problematičtější je jednoznačné definování poměrně širokého pojmu telekomunikační provoz. Tradičně byl tento pojem chápan jako obsah komunikace mezi osobami realizovaný prostřednictvím mobilních či pevných telefonů, faxu, vysílaček a podobných přístrojů. S technologickým rozvojem se však i tento pojem vyvíjel. Nyní tak pod něj patrně lze zahrnout všechny druhy komunikace realizované prostřednictvím telekomunikačních sítí a sítí elektronických komunikací, včetně komunikace mezi počítači či jinými zařízeními. Bude se tedy mimo jiné jednat i o veškerý provoz prostřednictvím IP protokolů nezávisle na tom, zda zahájení a obsah takové komunikace volí člověk, nebo počítač. Tento přístup vychází z chápání důvěrnosti komunikací definované v ZEK, který v § 89 odst. 1 stanoví, že *„[p]odnikatelé zajišťující veřejné komunikační sítě nebo poskytující veřejně dostupné služby elektronických komunikací jsou povinni zajistit technicky a organizačně důvěrnost zpráv a s nimi spojených provozních a lokalizačních údajů, které se přenášejí prostřednictvím jejich veřejné komunikační sítě a veřejně dostupných služeb elektronických komunikací. Zejména nepřipustí odposlech, ukládání zpráv nebo jiné druhy zachycení nebo sledování zpráv a s nimi spojených údajů osobami jinými, než jsou uživatelé, bez souhlasu dotčených uživatelů, pokud zákon nestanoví jinak.*"[242] Přestože se toto rozhodnutí věnuje toliko komunikaci telefonické, jeho závěry lze zobecnit a aplikovat i na odposlech přenosu datového.

Obecně tedy lze telekomunikační provoz definovat jako jakoukoliv komunikaci přenášenou prostřednictvím veřejných sítí elektronických komunikací mezi konečným počtem uživatelů. Jelikož je díky technickým vlastnostem těchto sítí nemožné předem zjistit, jaká data bude datový přenos obsahovat,

241 Viz usnesení Nejvyššího soudu sp. zn. 5 Tdo 459/2007, č. 7/2008 Sb. tr. rozh.
242 Viz § 89 odst. 1 ZEK.

lze uzavřít, že jakýkoliv odposlech datové komunikace ve veřejných sítích by měl být orgány činnými v trestním řízení prováděn pouze na základě a v souladu s vydaným příkazem k odposlechu a záznamu telekomunikačního provozu.

Kromě samotného obsahu pojmu telekomunikační provoz je rovněž potřeba vyrovnat se s otázkou, kdy jsou konkrétní data jeho předmětem, respektive ohraničit dobu, kdy jsou přenášená data chráněná důvěrností komunikací, tedy kdy je zahájen a ukončen jejich přenos. Tato otázka není judikatorně jednoznačně vyřešena, lze nicméně analogicky vycházet z chápání tajemstvím dopravovaných zpráv.

Proto lze za telekomunikační provoz považovat data, která jsou prostřednictvím sítí elektronických komunikací přepracována od okamžiku jejich odeslání ze zdrojového zařízení do okamžiku jejich přijetí zařízením cílovým. Tuto tezi podporuje i Ústavní soud, který ve svém usnesení[243] konstatoval, že jsou-li data po svém přenosu uložená v cílovém počítači, nejde již o data telekomunikačního provozu.

Poněkud specifická je situace, kdy je adresátovi elektronické komunikace orgány činnými v trestním řízení znemožněno seznámit se s obsahem komunikace. Tato situace může nastat v mnoha případech, například bylo-li zajištěno jediné zařízení nebo jediný nástroj, kterým lze k obsahu telekomunikačního provozu získat přístup, nebo využívají-li orgány činné v trestním řízení k získávání obsahu telekomunikačního provozu zajištěný nástroj[244]. V takové situaci nemá adresát možnost seznámit se s obsahem komunikace, a proto je v takové situaci ochrana telekomunikačního tajemství rozšířena i na obsah uchovaný po svém technickém doručení. Potřebují-li tedy orgány činné v trestním řízení sledovat budoucí příchozí telekomunikační provoz pomocí zařízení nebo nástroje získaného vydáním nebo odnětím věci při domovní nebo osobní prohlídce nebo například postupem podle

243 Viz usnesení Ústavního soudu ČR ze dne 3. 10. 2013 sp. zn. III. ÚS 3812/2012, U 10/71 SbNU 573.

244 Získá-li například policie přístup k obsahu e-mailové schránky postupem podle § 158d odst. 3 a dále tento přístup využívá ke sledování příchozí pošty. Více viz kapitola IV. Jiným příkladem může být situace, kdy policie zajistí mobilní telefon, nebo počítač, prostřednictvím kterého sleduje příchozí datovou komunikaci. Více také kapitola VIII. této publikace.

§ 158d TŘ, musí být nejdříve vydán příkaz k odposlechu a záznamu telekomunikačního provozu podle § 88 TŘ. Tento přístup podporuje rovněž judikatura Nejvyššího soudu[245] a výkladové stanovisko Nejvyššího státního zastupitelství[246].

Zajímavou otázkou je problematika odposlechu telekomunikačního provozu, jehož součástí je komunikace, která neměla být součástí přenosu. Debata o této otázce vznikla po rozhodnutí Městského soudu v Praze[247], který se věnoval zákonnosti důkazu získaného odposlechem, který obsahoval komunikaci zachycenou v blízkosti mobilního telefonu při vytáčení volaného čísla. Podle vyjádření techniků mobilní telefon odesílá do sítě mikrofonem zachycené zvuky ještě před zahájením komunikace mezi dvěma stanicemi a do určité míry tedy funguje jako prostorový odposlech. Městský soud rozhodl, že i takto získaný obsah je krytý příkazem k odposlechu a záznamu telekomunikačního provozu a že je možné takový důkaz považovat za zákonný. Tento přístup je však poněkud problematický, neboť nikdo pravděpodobně nepředpokládá, že telefon ještě před zahájením komunikace s druhou stranou hovoru odesílá poskytovateli zachycené okolní zvuky. Zatím však není dostupná další judikatura, která by se této problematice blíže věnovala.

VII.2 Zajištění a uchování důkazního prostředku

VII.2.1 Příkaz k odposlechu a záznamu telekomunikačního provozu

Odposlech a záznam telekomunikačního provozu nařizuje v trestním řízení předseda senátu (v přípravném řízení trestním pak soudce na návrh státního zástupce) příkazem, který má povahu rozhodnutí *sui generis*. Může být vydán v řádně zahájeném trestním řízení pro zákonem kvalifikovanou trestnou činnost, a to jen tehdy, je-li doložen relevantními podklady, odůvodňujícími

245 Viz usnesení Nejvyššího soudu sp. zn. 7 Tz 9/2000.

246 Srov. Výkladové stanovisko Nejvyššího státního zastupitelství č. 4/2005, 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. Dostupné z http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2005/stanovisko%204-2005.pdf.

247 Viz rozhodnutí Městského soudu v Praze sp. zn. 42 T 8/2013.

podezření, že ke spáchání trestného činu připouštějícího nařízení odposlechu[248] skutečně došlo, dochází anebo že k němu v budoucnosti velmi pravděpodobně dojde[249].

Často bývají odposlechy realizovány rovněž ve fázi prověřování, tedy ještě před zahájením trestního stíhání. Jedná se o úkony, na které je pohlíženo jako na neodkladné či neopakovatelné dle § 160 odst. 4 TŘ. V takovém případě pak musí protokol o provedení odposlechu obsahovat rovněž odůvodnění, na základě jakých skutečností byl za neodkladný či neopakovatelný považován.

Návrh na vydání příkazu k odposlechu a záznamu telekomunikačního provozu nemá zákonem stanovenou formu ani obsah, nicméně ze zavedené praxe a z obsahu Závazného pokynu policejního prezidenta o plnění úkolů v trestním řízení[250] lze identifikovat následující obsahové náležitosti příkazu:

a) identifikátor zařízení nebo uživatele, je-li znám,
b) stručné vyhodnocení skutkového stavu předmětné trestní věci,
c) odůvodnění provedení odposlechu a záznamu,
d) jestliže je trestní řízení vedeno pro trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva, pak odkaz na tuto smlouvu,
e) popis trestného činu a jeho trestněprávní kvalifikaci,
f) seznam příkazů k odposlechu a záznamu telekomunikačního provozu, které byly v minulosti ke stejnému identifikátoru vydány,
g) vlastní návrh na nařízení odposlechu a záznamu telekomunikačního provozu.

Základní požadavky na obsah příkazu odposlechu a záznamu telekomunikačního provozu obsahuje samotný trestní řád, podle kterého musí být odůvodněn popisem skutkových okolností, musí obsahovat odkaz na trestný čin, pro který je vedeno trestní řízení, musí obsahovat identifikátor zařízení či osoby, pokud je známa, a stanovení doby, po kterou má být odposlech

248 Odposlech je přípustný u zločinů, na které zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně osm let, u taxativně vyjmenovaných trestných činů v § 88 odst. 1 TŘ a u jiných úmyslných trestných činů, k jejichž stíhání zavazuje vyhlášená mezinárodní smlouva.

249 Viz Nález Ústavního soudu sp. zn. II. ÚS 615/06, N 88/45 SbNU 291.

250 Čl. 67 Závazného pokynu policejního prezidenta č. 30/2009, o plnění úkolů v trestním řízení, ze dne 21. dubna 2009. Dostupný online z http://www.pecina.cz/files/pokyn2.pdf.

prováděn[251]. Obecným náležitostem příkazu se věnoval rovněž Ústavní soud ve svém nálezu sp. zn. II. ÚS 615/06[252]. V tomto rozhodnutí Ústavní soud konstatoval, že příkaz k odposlechu a záznamu telekomunikačního provozu musí být odůvodněn relevantními stopami, na základě kterých lze s vysokou pravděpodobností předpokládat, že byl spáchán trestný čin. Samotná existence trestního oznámení tak Ústavní soud nepovažuje za dostatečné odůvodnění vydání příkazu. Rozhodnutí rovněž konstatuje, že příkaz musí být individualizovaný ve vazbě ke konkrétní osobě nebo zařízení a musí specifikovat, jaké informace důležité pro trestní řízení mají být odposlechem získány. ÚS rovněž kritizoval praxi, kdy bývají příkazy vydávány, aniž by bylo dostatečně vyhodnoceno, zda existují materiální podmínky k jejich vydání.

Z výše řečeného lze tedy odvodit, že by příkaz k odposlechu a záznamu telekomunikačního provozu měl obsahovat následující:

a) vlastní příkaz k zahájení odposlechu,
b) identifikátor zařízení či osoby, je-li známa,
c) označení trestného činu, pro který je vedeno trestní řízení (včetně případného odkazu na vyhlášenou mezinárodní smlouvu, která k jeho stíhání zavazuje),
d) stanovení doby, po kterou má být odposlech prováděn (maximálně 4 měsíce),
e) odůvodnění vydání příkazu k odposlechu včetně popisu skutkového stavu,
f) účel odposlechu, respektive specifikace informací důležitých pro trestní řízení, které mají být prostřednictvím odposlechu získány,
g) vysvětlení, proč neexistuje jiný způsob, jak tyto informace získat, respektive proč by jinak bylo jejich získání značně ztíženo.

Odposlech a záznam telekomunikačního provozu může být rovněž nařízen bez příkazu orgánem činným v trestním řízení. To však jen v případě, že je vedeno trestní řízení pro taxativně vyjmenované trestné činy[253] a pokud s tím uživatel odposlouchávaného zařízení souhlasí. V takovém případě může být odposlech zahájen na základě příkazu policejního orgánu, který

251 Viz § 88 odst. 2 TŘ.
252 Viz nález Ústavního soudu sp. zn. II. ÚS 615/06, N 88/45 SbNU 291.
253 Taxativní výčet obsahuje § 88 odst. 5 TŘ.

získá předchozí písemný souhlas od uživatele zařízení. Takový příkaz by měl obsahovat podobné náležitosti jako příkaz soudu.

VII.2.2 Provádění odposlechu

Odposlech provádí pro potřeby orgánů činných v trestním řízení Policie ČR[254], konkrétně specializovaný ÚZČ. Tento útvar provádí kromě odposlechů rovněž sledování osob a věcí a další specializované úkony. Je k tomu technicky a personálně vybaven. Organizačně jde o servisní složku Policie s centrálou v Praze, která má v jednotlivých krajích svoje expozitury.

Tomuto útvaru je příkaz k odposlechu a záznamu telekomunikačního provozu zaslán současně s žádostí o jeho provedení, jež obsahuje číslo spisu, ke kterému má být odposlech přiřazen.

Konkrétní postupy a technické nástroje využívané ÚZČ při realizaci odposlechů jsou utajované. Odposlech však probíhá za součinnosti subjektů provozujících veřejné komunikační sítě nebo veřejně dostupné služby elektronických komunikací podle ZEK (dále též „provozovatelé"). Tyto subjekty mají v souladu s § 97 ZEK zřídit a zabezpečit v určených bodech své sítě rozhraní pro připojení koncového telekomunikačního zařízení pro odposlech a záznam zpráv.

Konkrétní technická pravidla pro instalaci takového zařízení a jeho provoz definuje prováděcí vyhláška k ZEK[255]. Provozovatel je při budování nebo obměně sítě povinen vyzvat ke vznesení žádosti o vybavení sítě nebo služby rozhraním pro připojení zařízení pro odposlech. Pokud ÚZČ žádost vznese, zpracuje provozovatel po konzultaci s ÚZČ návrh variant technického řešení, které obsahují odůvodnění a stanovení výše nákladů na jejich realizaci. ÚZČ vybere variantu řešení a ve spolupráci s provozovatelem vyhotoví záznam, který obsahuje informace o zvoleném řešení, způsobu platby a postupu instalace.[256] Náklady na instalaci a provoz nese Policie ČR.[257]

254 Dle § 19 PolČR.

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

256 Srov. § 7 tamtéž.

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

Samotný odposlech se realizuje dvěma základními způsoby – aktivací již instalovaného zařízení k odposlechu, nebo instalací zařízení v připojovacím bodě. K aktivaci instalovaného zařízení dochází vzdáleně na základě pokynu vázaného na základě identifikátoru určujícího uživatele nebo zařízení[258], zachycený telekomunikační provoz je pak přímo zpřístupněn, respektive uchováván ÚZČ.[259] Není-li účelné tento postup využívat (například z ekonomických důvodů), využívá se k odposlechu připojovacích bodů, které zřizují provozovatelé a do kterých pak může ÚZČ připojovat svoje zařízení pro odposlech. Konkrétní technická specifika jsou předmětem dohody mezi ÚZČ a provozovatelem.[260] Pokud provozovatelé telekomunikační provoz ve svých sítích šifrují, musí poskytovat klíče nebo musí zařízení pro odposlech instalovat do segmentů sítě, kde komunikace neprobíhá šifrovaně. V případě, že k šifrování dochází mimo provozovatelovy sítě, je policii zpřístupňována komunikace v zašifrované podobě.[261]

ÚZČ patrně využívá k realizaci odposlechů i další autonomní technické nástroje, především jde-li o odposlech realizovaný mimo sítě elektronických komunikací nebo ve službách informační společnosti. Je rovněž známo, že ÚZČ využívá specializovaných technických nástrojů pro dešifrování provozu nebo pro přístup k němu, jejich konkrétní specifika však známa nejsou[262].

Za nepřípustný je považován odposlech komunikace mezi obhájcem a obviněným. Policejní orgán je povinen záznam s takovou zachycenou komunikací zničit a informace, které tímto způsobem získal, nijak nepoužít. Toto omezení se však nevztahuje na komunikaci mezi podezřelým a jeho obhájcem ani obecně na komunikaci mezi advokátem a jeho klientem. Tato

258 Tím může být například účastnické číslo, elektronická adresa, fyzická adresa a jméno, čísla IMEI nebo IMSI, IP adresa, MAC adresa apod.

259 Viz § 9 a násl. vyhlášky č. 336/2005 Sb.

260 Viz § 14 tamtéž.

261 Viz § 8 tamtéž.

262 Příkladem mohou být nástroje využívané ÚZČ, které dodávala italská společnost Hacking Team. Informace o této spolupráci byly zveřejněny po napadení této společnosti hackery a zveřejnění její obchodní korespondence. Viz např. Útok na Hacking Team vyvolal dusno. Jejich software používá i česká policie. Dostupné z: http://www.lidovky.cz/utok-na-hacking-team-vyvolal-dusno-jejich-software-pouziva-i-ceska-policie-1tn-/zpravy-svet.aspx?c=A150716_175531_ln_zahranici_mct.

situace je některými autory považována za problematickou mimo jiné z toho důvodu, že se většina odposlechů realizuje ještě před zahájením trestního stíhání jako neodkladný a neopakovatelný úkon.[263]

VII.2.3 Ukončení odposlechu a nakládání se zaznamenaným telekomunikačním provozem

Standardně se odposlech ukončuje uplynutím doby stanovené v příkazu k odposlechu. Policejní orgán má však rovněž povinnost průběžně výsledky odposlechu vyhodnocovat, a jestliže vyhodnotí, že důvody k vydání příkazu k odposlechu již pominuly, musí jej okamžitě ukončit. Dobu odposlechu však lze rovněž prodlužovat, a to pokud o tom na základě vyhodnocení dosavadního průběhu odposlechu rozhodne soud. Prodlužovat se může i opakovaně, vždy na dobu maximálně 4 měsíců.

Po skončení odposlechu policejní orgán vyhodnotí jeho průběh. Jestliže záznamy neobsahují informace důležité pro trestní řízení, pak všechny záznamy o odposlechu vyšetřovatel i ÚZČ zničí po 3 letech od pravomocného skončení věci a pořídí o této skutečnosti protokol. Pokud naopak záznamy informace důležité pro trestní řízení obsahují, převezme policejní orgán všechny záznamy od ÚZČ.

Zbývající záznamy, které neobsahují informace důležité pro trestní řízení, jsou označeny a uloženy tak, aby nemohlo dojít k jejich zneužití. Tato skutečnost a místo uložení se pak uvede do protokolu.

Pořízené záznamy pak mohou být využity i v jiném trestním řízení, to ale jenom za předpokladu, že je toto trestní řízení vedeno pro některý z trestných činů, pro který lze vydat příkaz k odposlechu nebo pokud k tomu dá souhlas uživatel odposlouchávaného zařízení.

Výstupem záznamu telekomunikačního provozu mohou být rovněž hrubá či zašifrovaná data. Ta nejsou jako taková srozumitelná pro člověka, a je proto nutné využít technologických nástrojů či odborných postupů ke zpřístupnění informací, které obsahují. Proto bývá záznam telekomunikačního provozu následně předmětem kriminalistické expertizy nebo znaleckého zkoumání. Výstupem je v takovém případě znalecký posudek, který je využitelný jako důkaz v trestním řízení.

263 Viz např. Jelínek, J., Uhlířová, M. *Obhájce v trestním řízení*. 1. vydání. Praha: Leges, 2011, s. 260.

Bezodkladně po pravomocném skončení věci, ve které došlo k odposlechu a záznamu telekomunikačního provozu, musí být o jeho nařízení informována osoba, které se odposlech týkal, tedy pochopitelně jen v případě, že je známa. Informace musí obsahovat označení soudu, který příkaz vydal, délku trvání odposlechu a datum jeho ukončení. Součástí musí být rovněž poučení o právu podat ve lhůtě šesti měsíců návrh na přezkoumání zákonnosti příkazu k odposlechu a záznamu telekomunikačního provozu.[264] V situacích vymezených v zákoně se pak informace o provedeném odposlechu předávat nemusí.[265]

VII.3 Forenzní analýza

Předmětem odposlechu mohou být rovněž data z telekomunikačního provozu. Jelikož není znám postup, jakým jsou taková data útvarem zvláštních činností zajišťována, lze jen těžko hodnotit, jakými postupy jsou z těchto dat získávány informace důležité pro trestní řízení. Je-li totiž například toliko prováděno prosté odchytávání datové komunikace v určitém segmentu sítě, bude obsahem záznamu velké množství pro člověka jen těžko srozumitelných dat. Ty mohou kromě samotného obsahu komunikace obsahovat velké množství metadat, provozních a lokalizačních údajů, dat aplikací apod. Předpokladem jejich efektivního využití pro trestní řízení tak je analýza těchto dat za využití pokročilých forenzních nástrojů.

Je proto velmi pravděpodobné, že v těchto případech bude probíhat znalecké zkoumání zajištěných dat. Taková forenzní analýza je však značně technicky komplikovaná, proto pro ni bezezbytku platí limity znaleckého zkoumání formulované v kapitole III výše. Především je problematické pokládání otázek, na které má znalec ve svém posudku odpovědět. Musí se v nich totiž zohlednit například způsob zachycování telekomunikačního provozu, vlastnosti různých úrovní datové komunikace a technických protokolů, prostřednictvím kterých jsou data přenášena, či metod šifrování datového přenosu.

Předpokladem zadávání takových znaleckých posudků by tak měla být přinejmenším předchozí konzultace se znalcem, který může posoudit charakter získaných dat a limity jejich analýzy.

264 Viz § 88 odst. 8 TŘ.
265 Viz § 88 odst. 9 TŘ.

VII.4 Provedení důkazu

Předpokladem provedení důkazu záznamem telekomunikačního provozu je pořízení protokolu o uskutečnění tohoto úkonu, který splňuje zákonem stanovené náležitosti. Těmi jsou dle § 88 odst. 6 TŘ:

- údaje o místě, času, způsobu a obsahu jeho provedení;
- údaj o osobě, která záznam pořídila, nebo údaj o tom, že záznam byl pořízen automaticky bez účasti konkrétní osoby.

Protokol musí pochopitelně obsahovat také obecné náležitosti, definované v § 55 TŘ:

- pojmenování soudu, státního zástupce nebo jiného orgánu provádějícího úkon,
- místo, čas a předmět úkonu,
- jméno a příjmení úředních osob a jejich funkce, kteří se úkonu zúčastnili,
- stručné a výstižné vylíčení průběhu úkonu, z něhož by bylo patrné i zachování zákonných ustanovení upravujících provádění úkonu,
- návrhy stran, udělené poučení, popřípadě vyjádření poučených osob,
- námitky stran nebo vyslýchaných osob proti průběhu úkonu nebo obsahu protokolu.

Nesplnění těchto náležitostí, zejména pokud jde o údaje o místě, času, způsobu provedení záznamu, jakož i orgánu, který záznam pořídil, lze však odstranit, a to i v řízení před soudem, stejným způsobem jako v případě odstranění formálních nedostatků protokolu sepsaného o jakémkoliv jiném úkonu trestního řízení (např. výslechem osob, které se provedení úkonu zúčastnily, popř. jej provedly, a to v postavení svědka). Takový postup nelze považovat na nepřípustnou manipulaci se záznamy telekomunikačního provozu a nevymyká se ani možnostem soudu, takže věc nevyžaduje další šetření.[266]

Pokud byl záznam telekomunikačního provozu následně podroben znaleckému zkoumání, může být rovněž využit znalecký posudek jako listinný důkaz, respektive výpověď znalce. K tomu dochází, jsou-li předmětem odposlechu data. V takovém případě se na provedení důkazu bez dalšího uplatní závěry zmíněné v kapitole III výše.

266 K tomu srov. usnesení Vrchního soudu v Praze sp. zn. 4 To 3/01, č. 56/2001 Sb. tr. rozh.

VII.5 Hodnocení důkazu

Z hlediska hodnocení důkazů získaných odposlechem a záznamem telekomunikačního provozu je problémem, podobně jako u ostatních elektronických důkazů, ztotožnění. Ačkoliv je v případě odposlechu telefonických hovorů praxe již v podstatě stabilizována, u záznamu elektronické komunikace je situace poněkud problematičtější a je třeba přihlédnout k jejím specifikům. Data totiž nelze jednoduše ztotožnit analýzou hlasu komunikujících stran[267]. Na druhou stranu, nástrojů využitelných ke ztotožnění elektronické komunikace je značné spektrum a jejich technický charakter umožňuje využívat různé jejich kombinace. Praktická aplikace pak závisí na individuálních znalostech a zkušenostech vyšetřovatele. Za nejběžnější nástroje pak lze považovat:

- znalecký posudek – znalecký posudek je nejefektivnější nástroj při hodnocení zajištěných elektronických dat, jeho základním nedostatkem je však nákladnost. Měla-li by být jakákoliv zaznamenaná elektronická komunikace předmětem znaleckého posudku, bylo by to velmi nákladné a neodůvodnitelné z hlediska ekonomie procesu. Více ke znaleckým posudkům viz předchozí kapitoly.
- metadata datového přenosu – přenos elektronických dat díky technickým vlastnostem počítačových sítí generuje relativně velké množství metadat, které mohou být i automatizovaně analyzovány a využity ke ztotožnění zaznamenaného přenosu. Metadaty v tomto případě myslíme nejen informace obsažené v přenášených datech, ale rovněž data přenosu, která generují jednotlivá zařízení, prostřednictvím kterých jsou data přenášena. V tomto ohledu mohou být velmi užitečná data získaná z dohledových pracovišť kybernetické bezpečnosti, o kterých pojednává kapitola IX níže.
- provozní a lokalizační údaje – podobnou úlohu jako metadata datového přenosu mohou plnit provozní a lokalizační údaje získané postupem podle § 88a TŘ od provozovatelů sítí elektronických

267 Na tomto místě je vhodné připomenout, že pokud byl obviněný řádně seznámen s právem nevypovídat, a i přesto se sám vypovídat při hlavním líčení rozhodl, nemůže namítat nezákonnost postupu soudu, který takto pořízený zvukový záznam použil jako srovnávací materiál pro účely vypracování znaleckého posudku. Posudek znalce je pak důkazem v trestním řízení, který lze použít ve smyslu § 89 odst. 2 TŘ. K tomu viz usnesení Nejvyššího soudu sp. zn. 8 Tdo 921/2009, č. 3/2011 Sb. tr. rozh.

komunikací. Máme-li zachycená data a známe jejich logický zdroj a cíl, pak lze pomocí provozních a lokalizačních údajů zjistit fyzickou polohu těchto zařízení. Blíže k tomu viz kapitolu VII výše.

- elektronické identifikátory – za elektronické identifikátory lze považovat různé údaje od elektronických podpisů přes e-mailové adresy a IP adresy až po údaje uložené v cookies webového prohlížeče. Díky těmto údajům lze podle jejich charakteru komunikaci přiřadit konkrétnímu zařízení nebo uživateli.
- svědecká výpověď – svědecká výpověď může být užitečná především v situaci, kdy bylo pomocí ostatních nástrojů identifikováno zařízení, s nímž pak lze na základě svědeckých výpovědí spojit uživatele, například když jej někdo viděl v příslušné době s daným zařízením manipulovat.
- časové značky – jde o specifický druh metadat, která spojují data s určitým časovým okamžikem, například datum a čas vytvoření souboru, datum a čas uskutečnění datového přenosu, nebo datum a čas přístupu k počítačovému systému.

VII.6 Shrnutí kapitoly

Odposlech a záznam telekomunikačního provozu je velmi efektivní pro získávání důkazů v trestním řízení. Přestože byl tento nástroj konstruován pro získávání obsahu především telefonické či faxové komunikace, je v současné době využíván i k zajišťování přenášených dat. To přináší mnoho výzev nejen z hlediska výkladu platného práva. Telekomunikační provoz totiž může v podstatě obsahovat jakýkoliv druh dat, proto je forenzní analýza a celkově využívání při dokazování technicky a procesně náročné. Komunikace je navíc stále častěji šifrovaná, což znamená další překážku, se kterou se musí orgány činné v trestním řízení vyrovnat.

Tato kapitola se věnovala definici pojmů odposlech, záznam a telekomunikační provoz, neboť jde o pojmy legislativně nedefinované a doktrinálně nedostatečně zachycené. Dále byl v textu věnován prostor postupu při odposlechu a záznamu telekomunikačního provozu od podání návrhu a vydání příkazu k jeho realizaci přes vlastní technické postupy při jeho provádění útvarem zvláštních činností policie až po analýzu získaného záznamu

a jeho provedení a hodnocení jako důkazu před soudem. Cílem bylo obecně zachytit současně aplikované postupy a nastínit překážky, které při aplikaci institutu odposlechu na datový provoz vznikají.

V současné době bohužel neexistuje zavedená praxe, adekvátní judikatura či doktrína ani dostatečně dostupné technické nástroje, které by tyto překážky efektivně odstraňovaly. Proto je více než žádoucí, aby se právní věda a praxe tímto tématem nadále zabývaly a hledaly cesty jak nastavit procesní postupy k efektivnímu využívání odposlechu v trestním řízení při současném šetření základních práv a svobod.

VIII DOKAZOVÁNÍ DATY Z MOBILNÍCH KOMUNIKAČNÍCH ZAŘÍZENÍ[268]

VIII.1 Vysvětlení pojmu

Zatímco ještě v devadesátých letech byl mobilní telefon technologickým výstřelkem, dnes existuje více aktivních mobilních telefonů, než je na světě lidí.[269] Spolu s množstvím mobilních telefonů se rovněž závratně rozšiřují jejich funkce a s tím souvisí nárůst objemu ukládaných dat. Zatímco na konci dvacátého století mobilní telefony obsahovaly pouze malé množství telefonních čísel a SMS zpráv, dnes jsou běžně vybaveny vlastní pamětí či paměťovými kartami s kapacitou v řádech desítek gigabytů. I v důsledku rozvoje rychlého mobilního internetu je dnes evidentní, že mobilní telefon je zdaleka nejčastěji využívaným osobním elektronickým zařízení, které vytváří otisk svého uživatele. S rozšiřujícím se využitím mobilních telefonů se pak přirozeně zvyšuje i četnost případů, kdy mobilní telefony a data v nich uložená hrají roli v rámci trestního řízení.

Mobilní telefon může být při trestné činnosti *hmotným předmětem útoku*, kdy je odcizen, poškozen nebo úmyslně zničen, *prostředím,* ve kterém byl trestný čin spáchán (například byl telefon při neoprávněném přístupu infikován virem), ale i *nástrojem ke spáchání trestné činnosti* (například při vydírání, nebezpečném pronásledování nebo aktivaci výbušného systému). Mobilní telefon je také nezřídka nástrojem k organizování trestné činnosti, a to ať už se jedná o přípravu či samotnou realizaci. Avšak i pokud mobilní telefon nehraje žádnou z uvedených rolí, může být cenným zdrojem dalších kriminalisticky relevantních informací, které povedou k jiným důkazům, případně potvrdí nebo vyvrátí ostatní důkazy. Množství dat rovněž umožňuje vytvořit přesvědčivý psychologický profil podezřelé osoby. Každá dílčí informace získaná z mobilního telefonu může mít v konkrétním trestním řízení

268 Koncept této kapitoly byl publikován jako Pejčochová, A., Elbert, T. Mobilní telefon v trestním řízení. *Kriminalistika*, 2015, roč. 48, č. 3 a Pejčochová, A., Elbert, T. Provedení a hodnocení důkazu získaného z mobilního telefonu. *Kriminalistika*, 2015, roč. 48, č. 3.

269 Viz Number of mobile phones to exceed world population by 2014. *Dostupné z:* http://www.digitaltrends.com/mobile/mobile-phone-world-population-2014.

význam. Neomezené možnosti využití mobilního telefonu pak může s jistou nadsázkou ilustrovat i rozsudek Nejvyššího soudu, dle kterého byl mobilní telefon v konkrétním případě užit jako zbraň.[270]

K získání důkazu v rámci trestního řízení lze dle § 89 odst. 2 TŘ využít vše, co může přispět k objasnění věci, to jest pochopitelně i elektronické důkazy v podobě různých záznamů na elektronických nosičích informací.[271] Ty se mohou nacházet nejenom v paměti telefonu, ale také na vložené paměťové kartě (např. typu microSD) nebo na SIM kartě.[272] Informace, které jsou zde uloženy, obsahují záznamy o volání (odchozí, příchozí, zmeškané hovory a v některých případech i délku hovoru), kontakty (jména, telefonní čísla a případně i jejich fotografie, adresy či data narození), SMS zprávy (včetně údajů o odeslání a doručení), MMS (multimediální) zprávy, záznamy v kalendáři (datum, čas, místo a předmět schůzky), úkoly, poznámky, fotografie (včetně Exif dat[273]), audio (např. záznamy z funkce diktafon či vlastní nahrávky telefonních hovorů) a video. Nadto mobilní telefon samozřejmě může sloužit i jako pouhé přenosné paměťové médium pro libovolná data v takřka jakémkoliv souborovém formátu.

Relevantní však v konkrétním případě může být i samotné nastavení mobilního telefonu, jako je jeho datum a čas, jazyk nebo konkrétní vyzváněcí melodie, která například mohla být zaslechnuta svědkem na místě činu. Dále se může jednat o informace o párování telefonu s jinými telefony či zařízeními pomocí technologie Bluetooth nebo pomocí jiných rozhraní. Propojení mobilního telefonu s okolním prostředím navíc stále častěji zajišťuje rádiová bezdrátová NFC technologie, díky které se mobilní telefon využívá jako bezkontaktní platební prostředek (tzv. služba mobilní/digitální peněženky). Některé mobilní telefony navíc ukládají seznam základnových

270 Srov. Usnesení Nejvyššího soudu sp. zn. 3 Tdo 553/2006. Pachatel použil mobilní telefon k opakovaným úderům směřujícím vůči citlivé, resp. zranitelné části těla poškozené. Telefon měl tak za daných skutkových okolností povahu zbraně ve smyslu ustanovení § 89 odst. 5 zákona č. 140/1961 Sb., trestní zákon (v současnosti § 118 TZ).

271 Viz Šámal, 2013a, op. cit., s. 1336.

272 SIM karta (z anglického „subscriber identity module“) je účastnická identifikační karta která slouží pro identifikaci účastníka v mobilní síti.

273 Exif data jsou metadata připojená k jednotlivým fotografiím. Tato data obsahují například datum a přesný čas pořízení fotografie, informace o přístroji, kterým byla fotografie pořízena, a nastavení přístroje v okamžik pořízení fotografie. Pokud je funkce aktivována, mohou tato data obsahovat i přesnou GPS polohu přístroje v době pořízení fotografie.

stanic (tzv. BTS stanice), skrz které se v minulosti připojily do telefonní sítě. I takový záznam umožňuje zjistit pohyb přístroje, potažmo jeho majitele, v konkrétním čase. Moderní mobilní telefony zpravidla obsahují také GPS modul. Ten, pokud je aktivovaný, generuje ještě přesnější informace o pohybu přístroje. Telefon může navíc obsahovat nejenom informace o uskutečněném pohybu, ale v rámci navigačních služeb také o plánovaném pohybu v podobě zadané cílové destinace a trasy.

Už výše uvedený rozsah dat obsažených v mobilním telefonu naznačuje, že mobilní telefon se svými funkcemi vyrovnal počítači. Tuto skutečnost pak podtrhuje fakt, že mobilní telefon se stal plnohodnotným nástrojem pro využití internetových služeb. Z telefonu tak lze vytěžit rovněž historii prohlížených stránek či historii využití internetového připojení obecně (objem dat, využití základnových stanic atp.). Dokonce i samotná vyhledávaná slova či slovní spojení mohou být nezřídka pro trestní řízení podstatná. Tyto informace rovněž poskytnou uložené záložky (odkazy na internetové stránky), soubory cookies (typicky generované stránkami online bankovnictví, při nakupování přes e-shop či při rezervaci ubytování a letenek). K využití mobilního internetu navíc mnohdy slouží lokální bezdrátové sítě a mobilní telefon tak může obsahovat informace o konkrétním Wi-Fi spotu včetně IP adresy routeru apod., a tím pádem opět poskytnout přesnou informaci o pohybu konkrétní osoby.

Vedle dat týkajících se využití internetu pak důležité informace mohou skrývat rovněž nerozmanitější aplikace na mobilním telefonu, které využívají internetových služeb. V první řadě se bude jednat o e-mailové aplikace, které mohou obsahovat nejenom samotné e-maily a jejich přílohy, ale také seznam kontaktů uživatele. Zásadní informace se mohou nacházet rovněž v aplikacích služeb typu instant messaging,[274] jako je například Facebook či WhatsApp.[275] Jakékoliv další aplikace pak mohou obsahovat cenné

274 Internetová služba, která zpravidla ukazuje uživatelům ostatní uživatele (kontakty), kteří jsou v daný okamžik připojeni, a umožňuje jim zaslat textové či audio zprávy nebo jakékoliv soubory či geolokační údaje. Aplikace zejména obsahuje uložené kontakty a mnohdy také obsah proběhnuvší komunikace.

275 Dále například Viber, Skype, ICQ, Windows Live Messenger, Yahoo Messenger či Google Talk. Jelikož dostat se k těmto datům, která jsou zpravidla zpracovávána servery v zahraničí, je pro orgán činný v trestním řízení takřka nemožné bez přístupu k mobilnímu telefonu, jsou právě tyto komunikační kanály na rozdíl od SMS zpráv často využívány při nelegálních aktivitách.

informace o komunikaci, lokaci či alespoň informaci o tom, že mobilní telefon byl v daný okamžik užíván.

S daty získanými z mobilních telefonů bezprostředně souvisí odposlechy a záznam telekomunikačního provozu, respektive údaje o telekomunikačním provozu, které lze podle § 88 a 88a TŘ získat od mobilního operátora či přímo při přenosu dat. Vedle odposlechů (telefonátu, SMS i dat) se jedná především o provozní a lokalizační údaje o telefonátu (s kým, kdy a jak dlouho trval), o SMS zprávě (mezi kým a kdy), o datovém provozu a o přibližném pohybu telefonního přístroje v čase podle připojení na konkrétní základnové stanice.[276] Povinnost uchovávat tyto údaje po dobu 6 měsíců a povinnost poskytnout tyto údaje na požádání policejnímu orgánu (a jiným subjektům) upravuje zejména TŘ a ZEK.[277] Jelikož se však nejedná o data získaná přímo z mobilního telefonu, zajištění těchto dat či dokazování těmito daty není předmětem této kapitoly.[278] Zdánlivě podobnou problematiku dat uložených mimo mobilní telefon, ale přístupných skrz zajištěný mobilní telefon (zejména problematika cloudcomputingu), adresujeme v kapitole VIII.4.

Na závěr úvodní části je třeba si uvědomit, že z právního pohledu mobilní telefon v konkrétních případech vykazuje stejné charakteristiky jako například phablet, tablet, GPS navigace či notebook. Řada zde rozebíraných témat, jako je například heslování, získávání dat uložených v cloudu či přiřazení jednání individuální osobě (uživateli), se rovněž kryje s problematikou forenzní analýzy klasických stolních počítačů. Současně tyto otázky mohou být v budoucnosti kladeny nejenom v souvislosti s uvedenými nástroji, ale rovněž ve vztahu ke stále populárnějším a rozmanitějším produktům typu wearable, tj. zařízením, která člověk nosí na sobě (např. sporttestery a jiná monitorovací zařízení, drobné kamery či přímo minipočítače, jako je Google Glass apod.). V nejširší rovině témata zde probíraná korespondují s rostoucím fenoménem tzv. internetu věcí. Rysy komunikačního zařízení,

276 Rozsah uchovávaných informací stanoví § 2 vyhlášky č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů.

277 Je třeba upozornit, že celou platnou právní úpravu významně zpochybnil rozsudek SDEU ve věci Digital Rights Ireland a Seitlinger a další, sp. zn. C-293/12 a C-594/12. K tomu blíže Komárek, J. Soudní dvůr EU – duben 2014. *Soudní rozhledy*, 2014, č. 6, s. 229.

278 Data úzce související s užíváním mobilních telefonů lze navíc hledat i jinde než u mobilních operátorů (s mobilním telefonem synchronizované počítače, provozovatelé online aplikací, Wi-Fi hot spoty, NFC platební terminály atd.).

které může zanechat datovou stopu, totiž dnes stále častěji mají i samotné věci, jejichž primárním účelem není komunikace mezi lidmi (viz integrované GPS moduly v dopravních prostředcích na jedné straně a implantované RFID čipy ve zvířatech či lidech na straně druhé).

VIII.2 Zajištění a uchování důkazního prostředku

OČTŘ se může mobilního telefonu, jako kterékoliv jiné věci důležité pro trestní řízení, zmocnit celou řadou způsobů. Aby však mohl být důkaz v trestním řízení využit, musí být zajištěn postupem v souladu s trestním řádem.

Mobilní telefon je nezřídka *nalezen* u oběti trestného činu či na jiném místě ohledání (§ 113 TŘ). Pokud s mobilním telefonem disponuje určitá osoba, předseda senátu a v přípravném řízení státní zástupce nebo přímo policejní orgán mohou podle § 78 TŘ vyzvat takovou osobu k *vydání* mobilního telefonu jakožto věci důležité pro trestní řízení. Osobou povinnou k vydání věci nemusí být přímo uživatel daného mobilního telefonu, ale může jí být přirozeně kterákoliv osoba, která má mobilní telefon u sebe (např. zaměstnavatel může být vyzván k vydání služebního telefonu svého bývalého zaměstnance). V případě, že není nutné pro účely trestního řízení mobilní telefon zajistit, může OČTŘ namísto vydání požadovat jeho *předložení*. Je-li to technicky možné, mobilní telefon lze v takovém případě ohledat (vytěžit) bezprostředně při předložení na místě samém.

Nevyhoví-li osoba výzvě k vydání mobilního telefonu, může jí být přístroj *odejmut* podle § 79 TŘ. O tom musí být osoba poučena již ve výzvě k vydání věci. K odnětí je třeba příkaz předsedy senátu a v přípravném řízení příkaz státního zástupce nebo policejního orgánu s předchozím souhlasem státního zástupce. Mobilní telefon je možné jakožto věc důležitou pro trestní řízení zajistit také *při domovní prohlídce a při prohlídce jiných prostor a pozemků* podle § 82 a násl. TŘ. Výhodou domovních a jiných prohlídek je zpravidla přítomnost kriminalistického technika, který jednak určí, co vše je třeba zajistit, a jednak provede zajištění samotné dostatečně kvalifikovaně (viz dále).

Rovněž není vyloučeno, že policejní orgány namísto mobilního telefonu získají pouze data v něm uložená, a to bez vědomí uživatele. Dle § 158d

odst. 3 TŘ může být *sledováním* zjišťován obsah záznamů uchovávaných v soukromí na základě předchozího povolení soudce. Možnost využít § 158d odst. 3 TŘ k získání otisku elektronických dat (v daném případě z počítače) potvrdil také Ústavní soud.[279] Pokud se tedy policejnímu orgánu bez vědomí majitele podaří fyzicky se na omezenou dobu mobilního telefonu zmocnit, může jej vytěžit v souladu s uvedeným ustanovením. Teoreticky je rovněž možné, že si policejní orgán zajistí přístup k datům uloženým v mobilním telefonu na dálku, a to například pomocí utajené aplikace v mobilním telefonu.

Co se týká samotného praktického postupu při zajišťování mobilního telefonu, je v první řadě třeba mobilní telefon zajistit tak, aby nedošlo ke smazání ani změně obsažených dat. Mobilní telefony jsou dynamická zařízení a jejich hodnota jako důkazního prostředku tak může být snadno znehodnocena. Přístroj je zpravidla připojen do sítě mobilního operátora a eventuálně rovněž přes Wi-Fi či Bluetooth. Prostřednictvím těchto spojení mobilní telefon neustále odesílá a přijímá data v podobě nových zpráv a aktualizací jednotlivých aplikací. Veškeré důkazy v mobilním telefonu jsou tak náchylné k přepisu novými daty. Stejně tak neodborné propojení mobilního telefonu s počítačem může vést k přepisu dat (např. vlastním obsahem z počítače). Při expertní manipulaci po zajištění mobilního telefonu se zpravidla tzv. klonuje SIM karta, což slouží k zamezení komunikace mobilního telefonu se sítí. Nedochází tedy k promazání některých záznamů, které mají vazbu na poslední vloženou SIM kartu (například odchozí/příchozí a zmeškané volání).

Některé mobilní telefony mohou být navíc na dálku úmyslně smazány nebo zablokovány. Pro nejfrekventovanější mobilní přístroje typu iPhone a telefony s operačním systémem Android a Windows Phone jsou pro případ ztráty či krádeže telefonu běžně dostupné aplikace umožňující vzdálenou lokalizaci a rovněž smazání telefonního přístroje na dálku. Stejně tak zařízení BlackBerry může být na dálku smazáno příslušným správcem. Tyto služby samozřejmě mohou být a jsou zneužívané i v případech, kdy je mobilní telefon zajištěn pro účely trestního řízení.[280]

279 Viz usnesení Ústavního soudu sp. zn. III. ÚS 3812/2012, U 10/71 SbNU 573.

280 Viz Smartphones ‚remotely wiped' in police custody, as encryption vs. law enforcement heats up. Dostupné z: http://www.zdnet.com/smartphones-remotely-wiped-in-police-custody-as-encryption-vs-law-enforcement-heats-up-7000034521.

Mobilní telefon je tedy třeba neprodleně zajistit proti přepisu uložených dat. S ohledem na množství různých přístrojů a zejména jejich individuální nastavení přirozeně nelze určit jeden postup nebo nástroj, který by byl optimální ve všech případech. Lze však obecně doporučit při zajištění mobilního telefonu zamezit jeho veškeré vnější komunikaci. Nejjednodušším způsobem, jak toho docílit, je mobilní telefon vypnout či ještě lépe odpojit jeho baterii. Tento krok však představuje riziko, že telefon bude při opětovném zapnutí uzamčen, a tedy veškerá extrakce dat bude potenciálně ohrožena, nebo (u starších typů telefonů) může dojít ke smazání nastaveného data a času. Jako vhodnější postup se proto jeví aktivace tzv. letového módu, který přeruší veškerá bezdrátová spojení mobilního telefonu, avšak telefon neuzamkne. Tímto módem disponuje většina moderních přístrojů. Není-li možné z jakéhokoliv důvodu tento mód aktivovat, lze spojení přerušit vložením mobilního telefonu do Faradayova sáčku, který mobilní telefon odstíní na základě principu Faradayovy klece. Nevýhodou tohoto postupu je, že mobilní telefon se zpravidla rychleji vybíjí a může tak opět dojít k jeho vypnutí a uzamčení.

Dojde-li z jakéhokoliv důvodu k uzamčení telefonu nebo je-li telefon uzamčen již při jeho zajištění, odvíjí se možnost překonat zámek zejména od toho, zda se jedná o uzamčení SIM karty, či samotného přístroje. SIM karta mobilního telefonu je nezřídka chráněna osobním identifikačním číslem, tzv. PIN („personal identification number“). V případě opakovaného (trojího) chybného zadání PIN je třeba zadat namísto PIN tzv. PUK („PIN unlock key“). PUK, který na rozdíl od PIN nemůže uživatel změnit, je možné vyžádat od mobilního operátora.

Praxe zde není jednotná v tom, zda je mobilní operátor povinen poskytnout PUK na základě prostého dožádání policejního orgánu ve smyslu § 8 odst. 1 TŘ, nebo zda je nezbytné, aby soud nejprve vydal příkaz k odposlechu a záznamu telekomunikačního provozu podle § 88 TŘ. Samotný PUK není chráněn důvěrností komunikací podle § 89 ZEK, jelikož není zprávou ani s ní spojeným provozním či lokalizačním údajem přenášeným prostřednictvím veřejné komunikační sítě. Stejně tak, co se týká dat uložených na uzamčené SIM kartě, domníváme se i s ohledem na níže uvedenou

judikaturu[281], že tato data nejsou, až na výjimky v podobě nepřečtených SMS zpráv, chráněna režimem § 88 ani § 88a TŘ. Dle našeho názoru by proto měl mobilní operátor poskytnout policejnímu orgánu PUK k zákonně zajištěné SIM kartě na základě prostého dožádání podle § 8 odst. 1 TŘ.

Podstatnější překážkou při sběru dat, než je uzamčení SIM karty prostřednictví kódu PIN, je uzamčení přímo samotného telefonu (nejenom pomocí alfanumerického kódu, ale např. také pomocí dnes velmi populárního kreslení gesta (tzv. „pattern lock"), případně dokonce zašifrování obsahu mobilního telefonu. Jelikož jsou taková hesla volena samotnými uživateli[282] a ve většině případů k nim neexistuje obdoba kódu PUK, nelze při jejich překonání spoléhat na pomoc mobilního operátora. Stejně tak vytvoření klonu SIM karty pochopitelně neovlivní heslo nastavené přímo v telefonu. Nejedná-li se tedy o pouhé uzamčení SIM karty a heslo nebylo zjištěno jiným způsobem, musí policejní orgány spoléhat na metody odemknutí či dešifrování bez znalosti hesla. Takové řešení je však přirozeně časově, a tedy i finančně náročné. Teoretickou možností je samozřejmě i požadovat odemknutí či dešifrování přímo od výrobce mobilního telefonu nebo dané aplikace. Výrobce je však v zásadě vždy mimo jurisdikci OČTŘ, a tedy jen velmi těžko dostupný. Výrobci navíc obecně nemají zájem na takové spolupráci, a proto se snaží naprogramovat telefony tak, aby nebylo v jejich možnostech takovou spolupráci OČTŘ vůbec poskytnout.[283]

V ideálním případě poskytne heslo samotný uživatel telefonu. V tuzemsku však na rozdíl od jiných států[284] není možné obviněného nutit k vydání hesla.

281 Viz usnesení Nejvyššího soudu sp. zn. 7 Tz 9/2000.

282 S výjimkou přednastavených hesel telefonu, která jsou společná pro daný typ přístroje. Tato hesla jsou však zpravidla uživateli změněna.

283 Viz např. veřejně dostupná informace na toto téma od společnosti Apple, dle které mobilní telefony s operačním systémem iOS 8 nemůže společnost ani na žádost státních orgánů odemknout. Apple Inc. Our commitment to customer privacy doesn't stop because of a government information. Dostupné z: https://www.apple.com/privacy/government-information-requests.

284 Například ve Spojeném království lze obviněného donutit k poskytnutí hesla pod hrozbou až dvou let vězení za pohrdání soudem podle Regulation of Investigatory Powers Act 2000. Kritici kontroverzního předpisu mimo jiné logicky namítají, že obviněný nemusí požadované heslo vůbec znát anebo jej prostě může zapomenout.

Dle článku 40 odst. 4 LZPS má obviněný právo odepřít výpověď, a proto nesmí být v žádném případě nucen nejen k výpovědi, ale ani k jinému aktivnímu jednání, kterým by přispíval k obstarání důkazu proti své osobě.[285]

> Ohledně možnosti přinutit obviněného k poskytnutí hesla existuje poměrně rozsáhlá judikatura ve Spojených státech amerických. Zda a kdy pátý dodatek Ústavy, který zakotvuje právo odmítnout svědectví proti sobě samým, chrání obviněné i před žádostí k poskytnutí hesla,[286] není sice zatím zcela jednoznačné, avšak není bez zajímavosti, že panuje shoda na povinnosti obviněného poskytnout otisk prstu, je-li zařízení uzamčeno tímto otiskem (např. funkce Touch ID od Applu). Soudy mimo jiné argumentovaly, že se jedná o obdobný úkon, jako je donucení k poskytnutí vzorku DNA, krve, ale i jakékoliv jiné věci. Smyslem pátého dodatku totiž je ochrana proti mučení a vynucenému doznání viny. Pátý dodatek proto dopadá pouze na informaci, která je vědomostí obviněného, a nikoliv na vydání věci byť se jedná o otisk prstu.[287] S ohledem na stanovisko pléna českého Ústavního soudu,[288]dle kterého nelze např. na sejmutí pachové stopy, odebrání vzorku vlasů či bukální stěr, které nevyžadují aktivní jednání podezřelého, pohlížet jako na úkony, jimiž by byl podezřelý donucován k ústavně nepřípustnému sebeobviňování, lze předpokládat, že by české soudy vyřešily tuto otázku obdobně a donucení k poskytnutí otisku prstu posvětily.[289]

Současně s mobilním telefonem je vhodné zajistit i veškeré jeho příslušenství. Zejména jakákoliv související média (paměťové karty), propojovací kabely, CD s drivery a souvisejícím software, papírovou dokumentaci, ale i veškerá zařízení, se kterými se mobilní telefon mohl párovat, tzn. především osobní počítač, se kterým byl mobilní telefon synchronizován a ve

---

285 Viz stanovisko pléna pléna Ústavního soudu sp. zn. Pl. ÚS-st. 30/10, ST 30/59 SbNU 595 (č. 439/2010 Sb.).

286 Viz Google and Apple Won't Unlock Your Phone, But a Court Can Make You Do It. Dostupné z: http://www.wired.com/2014/09/google-apple-wont-unlock-phone-court-can-make.

287 Viz Cops can make you unlock your smart phone with fingerprint, says judge. Dostupné z: http://mashable.com/2014/10/30/cops-can-force-you-to-unlock-phone-with-fingerprint-ruling.

288 Viz Stanovisko pléna Ústavního soudu sp. zn. Pl. ÚS-st. 30/10, ST 30/59 SbNU 595 (č. 439/2010 Sb.).

289 Naopak podle usnesení Krajského soudu v Hradci Králové sp. zn. 10 To 319/2008 nelze obviněného žádným způsobem, tedy ani hrozbou uložení pořádkové pokuty, donucovat k tomu, aby poskytl srovnávací hlasovou nahrávku, například pro účely zpracování znaleckého posudku z oboru kriminalistiky, odvětví audioexpertiza. Obdobně také nález Ústavního soudu sp. zn. III. ÚS 528/06, N 159/47 SbNU 75.

kterém tak pravděpodobně lze dohledat zálohy obsahu mobilního telefonu. Zatímco příslušenství telefonu může usnadnit následnou forenzní analýzu, párovaná zařízení mohou jednak potvrdit data obsažená na mobilním přístroji a jednak mohou obsahovat i data, která již byla z mobilního telefonu vymazána.

Mobilní telefon i související zajištěné věci je přirozeně nutné správné zdokumentovat. K identifikaci mobilního telefonu slouží především 15místné číslo IMEI (zkratka pro „international mobile equipment identity"),[290] které výrobce přiděluje GSM zařízením a lze jej nalézt zpravidla pod baterií. Pokud IMEI kód není čitelný nebo není žádoucí v důsledku odpojení baterie mobilní telefon vypnout, lze IMEI kód vyvolat na displeji zadáním univerzálního kódu *#06#. Ostatní součásti, jako jsou zejména SIM karty a paměťové karty, je možné zpravidla dokumentovat pomocí natištěného sériového čísla. Mobilní telefony, stejně jako ostatní zajištěné důkazy, by měly být vloženy do pytlů a zapečetěny tak, aby se vyloučila případná manipulace před forenzní analýzou. K tomu slouží především řádná dokumentace v celém procesu zajišťování důkazu.

VIII.3 Forenzní analýza

Kromě výše naznačené šíře, kvality a množství dat, jež běžně obsahují moderní mobilní telefony, mají tyto přístroje z pohledu OČTŘ i některé další přednosti. V mobilních telefonech je totiž uloženo i velké množství informací, o nichž uživatelé zpravidla ani netuší, že jsou zaznamenávány. Důkazy pak mohou být dohledány ve smazaných, avšak nepřepsaných souborech nebo jejich fragmentech, v datech uložených v operační (dočasné) paměti RAM nebo v záznamech činnosti jednotlivých aplikací na mobilním telefonu. Díky použití flashové paměti také data na mobilním telefonu spíše, než je tomu u klasických počítačů s pevným diskem, vydrží vysoké teploty, tlak a nárazy. I zcela zničený a zdánlivě bezcenný mobilní telefon tak mnohdy může stále obsahovat cenná data. K tomu, aby mohla být smazaná data převedena do vnímatelné podoby, se formou opatření dle § 105

290 Na zařízeních s CDMA kódováním, využívaných zejména v Severní Americe, je namísto IMEI uvedeno tzv. MEID („mobile equipment identifier").

odst. 1 TŘ vyžádá odborné vyjádření nebo znalecký posudek.[291] Mobilní telefon předaný spolu s příslušenstvím znalci již musí být zajištěn proti změně dat, tak jak je uvedeno v kapitole o zajištění. Předmětem znaleckého zkoumání mohou být pouze informace zaznamenané v mobilním telefonu ještě před okamžikem zajištění. Výsledky znaleckého zkoumání jsou přijímány jako důkaz ve formě odborného vyjádření nebo znaleckého posudku a rovněž se řídí příslušnou normou, upravující postavení znalců a znaleckých pracovišť.

Forenzní analýza digitálních dat[292] z mobilních telefonů má mnoho podob a nelze určit jedinou správnou a obecně aplikovatelnou metodu. Okolnosti a požadavky každého případu jsou jedinečné, a navíc volba metody závisí nejen na konkrétním přístroji, jeho nastavení a technologických možnostech expertních pracovišť, ale často také na znalostech a zkušenostech samotného znalce. Aby však výsledky analýzy mohly být použity jako důkaz, musí vždy splňovat základní vlastnosti forenzního zkoumání, jako jsou přezkoumatelnost procesu, objektivita znalce a zachování integrity důkazu.[293]

Samotnou forenzní analýzu dat lze rozdělit na fázi extrakce, tj. získání dat z mobilního telefonu, a fázi analýzy, tj. interpretaci získaných dat a jejich převedení do formátu použitelného v rámci trestního řízení. Co se týká samotné extrakce, lze rozlišit tři základní metody: manuální, logickou a fyzickou.[294]

Manuální extrakce se provádí pomocí přístupu přes uživatelské rozhraní mobilního telefonu. K přístupu a zkoumání hledaných dat je tedy využito displeje či kláves a nabídky telefonu. Informace, která se zobrazí na displeji telefonu, je poté zaznamenána prostým nafocením nebo přepisem.

291 Vyhotovení odborného posudku expertizními pracovišti v rámci PČR (OKTE - Odboru kriminalistické techniky a expertiz při jednotlivých Krajských ředitelstvích Policie České republiky a KÚP - Kriminalistického ústavu Praha) je někdy z časových důvodů nahrazováno spoluprací se soukromými znalci, a to i přesto, že úplata za takové specializované služby není ani zdaleka nepatrná.

292 Blíže k pojmu forenzní analýzy digitálních dat viz Selinšek, L. Některé právní aspekty forenzní analýzy digitálních dat. *Acta Universitatis Carolinae*, 2008, č. 4, s. 132.

293 Tato zásada znamená, že veškeré způsoby práce se zajištěnými daty musí být prováděny takovým způsobem, ze kterého je zřejmé, že nedošlo k úmyslné nebo neúmyslné manipulaci nebo změně.

294 Viz Casey, E. et al. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Third Edition.* Academic Press, 2011. Kapitola 20.1 - Digital Evidence on Mobile Devices. Dostupné z: http://booksite.elsevier.com/9780123742681/Chapter_20_Final.pdf.

Tím vzniká odvozený důkaz. Výstupem by měl být protokol o ohledání, který se v řízení před soudem provede jako listinný důkaz. Jelikož touto metodou mohou OČTŘ důkaz zajistit samy bez součinnosti znalce, je tato metoda hojně využívaná.

Logická extrakce spočívá v získání kopie dat logické struktury objektů (např. adresářů a souborů). Během tohoto postupu se tedy data importují do počítače prostřednictvím originálního propojovacího kabelu (zpravidla USB kabel) a specializovaného forenzního nástroje či pouze přes originální software od výrobce nebo zcela prostě zkopírováním souborů z mobilního telefonu připojeného k počítači jako přenosný disk (USB mass storage). Výhodou logické extrakce je nepochybně to, že na rozdíl od manuální extrakce takřka nedochází k přímé manipulaci s přístrojem, což posiluje integritu důkazu. Touto metodou je také získáno větší množství dat než pomocí manuální extrakce.

Fyzická extrakce umožňuje získání všech reálně existujících dat nezávisle na souborovém a operačním systému mobilního telefonu. Touto metodou lze získat i smazaná data, která doposud nebyla přepsána daty novými.

Fyzická, stejně jako logická extrakce je prováděna pomocí forenzních nástrojů, které tvoří softwarová a někdy i hardwarová[295] řešení. Obecně je vhodná kombinace více nástrojů, jelikož každý má jiné možnosti, výhody a nevýhody. Jsou-li navíc data získána z více nástrojů, lze jednu analýzu potvrdit druhou. Pomocí těchto nástrojů jsou zajištěna „hrubá data", která tyto nástroje dále umí zpracovat do podoby a struktury použitelné a srozumitelné pro další analýzu. Fyzické extrakce lze také docílit pomocí forenzních metod prováděných přes tzv. flasher boxy, bootloadery, JTAG body/rozhraní či doslova prostřednictvím fyzického vyjmutí paměťového čipu (označovaném jako tzv. Chip-Off metoda). Použití těchto vesměs invazivních metod je jednak časově a technicky náročné, ale může také na mobilním telefonu způsobit nevratné změny či ho zcela znehodnotit (zejména v případě vyjmutí čipu). V souladu se zásadou přiměřenosti trestního řízení je tak třeba důsledně zvážit nasazení těchto metod nejenom s ohledem

295 Mezi nejpopulárnější zařízení patří XRY, UFED, CellDEK, Oxygen ForensicSuite či iXAM. Výrobci jsou rozmístěni po celém světě, a tak některá zařízení jsou spolehlivější při práci s evropskými přístroji, jiná s čínskými apod.

na osobnostní, ale i vlastnická práva majitele přístroje. Jelikož fyzickou i logickou extrakci budou zpravidla provádět expertní pracoviště, provedení takto získaných důkazů proběhne obvykle výslechem znalce a čtením znaleckého posudku.

VIII.4 Provedení důkazu

Data získaná z mobilního telefonu, který je mnohdy nerozlučným pomocníkem v ruce podezřelého přímo při páchání trestné činnosti nebo alespoň během každodenního života podezřelého nebo jeho oběti, mohou mít zásadní význam pro dokazování kterékoliv ze skutečností dokazovaných v rámci trestního řízení dle § 89 TŘ.[296]

Pro samotné provedení důkazů pomocí dat získaných z mobilních telefonů jsou relevantní zejména ustanovení § 112 TŘ o věcných a listinných důkazech a § 105 TŘ o odborných vyjádřeních a znaleckých posudcích. Zcela vyloučen však není ani postup podle § 113 TŘ, upravujícího ohledání, či podle § 101 TŘ o výslechu svědka. Důkazy z mobilních telefonů jsou zpravidla provedeny jako věcné či listinné důkazy přímo v podobě fotografií displeje mobilního telefonu či jiných záznamů dat vyvolaných z takového přístroje. Případně, pokud se jedná o data, která nelze získat prostou manuální extrakcí, se zadá vyhotovení znaleckého posudku a důkaz se provede výslechem znalce. Vypracování znaleckého posudku je také preferováno vždy, pokud to časový rámec trestního řízení a požadavek přiměřenosti s ohledem na závažnost vyšetřovaného trestného činu umožňují. Důkaz získaný z nezávislého znaleckého posudku je totiž pro soud přirozeně přesvědčivější než důkaz vyplývající z dat manuálně extrahovaných policejním orgánem.

Zcela klíčovou problematikou dokazování daty z mobilních telefonů je však zákonnost takovýchto důkazů. Stejně jako v případě jakýchkoliv jiných důkazů nelze elektronické důkazy, které byly získány nezákonným způsobem, provést. Je zřejmé, že pokud bude mobilní telefon zajištěn nezákonným

296 Podle § 89 odst. 1 TŘ se v nezbytném rozsahu dokazuje nejenom, zda se stal trestný čin a zda jej spáchal obviněný, ale také podstatné okolnosti mající vliv na posouzení povahy a závažnosti činu, osobních poměrů pachatele a následků trestného činu. Dále se dokazují také okolnosti, které vedly k trestné činnosti nebo umožnily její spáchání, tzv. kriminogenní faktory, jejichž zjištění je nezbytné pro uložení konkrétního postihu pachatele, ale i obecně pro prevenci trestné činnosti.

donucením, nesmí být podle § 89 odst. 3 TŘ ani data z takového přístroje použita při dokazování. Avšak důkaz může být nepřípustný i z celé řady jiných důvodů, které trestní řád takto výslovně neuvádí. V trestním řízení totiž nelze využít ani ty důkazy, při jejichž vyhledávání, opatřování nebo provádění došlo k jakémukoliv jinému porušení právního předpisu, pokud toto porušení současně představuje podstatnou vadu řízení ve smyslu ustanovení o odvolání § 258 odst. 1 písm. a) TŘ.[297] Zákonnost důkazu je tak třeba vždy posuzovat samostatně v každém jednotlivém případě.

Obecně lze uvést, že zajištěné mobilní telefony jsou v rámci trestního řízení vnímány jako jakékoliv jiné hmotné věci a stejně tak jsou posuzována i data v nich uložená. To znamená, že obdobně, jako když je v souladu se zákonem zajištěn například soubor dokumentů, diář či fotoalbum, policejní orgány mohou vytěžit veškerá data, která jsou uložena přímo v zajištěném mobilním telefonu. Takto získané důkazní prostředky z mobilního telefonu pak mohou být použity k provedení důkazu v rámci trestního řízení před soudem.

Tento výklad potvrzuje rovněž Nejvyšší soud, dle kterého jsou sama ustanovení § 78 a 79 TŘ o povinnosti k vydání věci, respektive o odnětí věci, dostatečným zákonným podkladem pro prolomení ochrany tajemství zpráv dle čl. 13 LZPS.[298] V případě, že byla zpráva již příjemci předána (doručena) a je v jeho dispozici, zvýšená ochrana, kterou požívala v průběhu přepravy (v podobě ustanovení § 86 a násl. TŘ o zadržení a otevření zásilky a § 88 TŘ o odposlechu), dle Nejvyššího soudu končí.

Aplikační praxi potvrzuje i výkladové stanovisko Nejvyššího státního zastupitelství z roku 2005.[299] Podle tohoto stanoviska při zajištění telefonu jako věci důležité pro trestní řízení nepotřebuje policejní orgán k odposlechu, respektive k záznamu telekomunikačního provozu příkaz soudce, vydaný podle ustanovení § 88 či 88a TŘ jedná-li se o zjištění obsahu údajů

297 Výčet konkrétních ustanovení a hlavně judikatury k nepřípustnosti důkazu lze nalézt v komentáři Šámal, 2013a, op. cit., s. 1337 a násl.

298 Viz usnesení Nejvyššího soudu, sp. zn. 7 Tz 9/2000.

299 Viz Výkladové stanovisko Nejvyššího státního zastupitelství č. 4/2005, 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. Dostupné z http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2005/stanovisko%204-2005.pdf.

zprostředkovaných (doručených) volanému (oprávněnému účastníkovi telekomunikačního provozu) již předtím, než mobilní telefon získal do své moci policejní orgán. To znamená, že v zásadě veškerá data uložená v mobilním telefonu při jeho zajištění mohou být využita jako důkazní prostředek. Stejné závěry pak obsahuje rovněž pokyn nejvyšší státní zástupkyně ze dne 21. 9. 2009.[300]

V souladu se shora uvedeným je tedy zřejmé, že dostatečným zákonným podkladem pro využití dat z mobilního telefonu v rámci trestního řízení je vedle vydání a odnětí telefonu také příkaz k domovní a osobní prohlídce či k prohlídce jiných prostor a pozemků podle § 82 a násl. TŘ. V případě nálezu mobilního telefonu pak nelze logicky aplikovat ochranu tajemství jiných písemností podle čl. 13 LZPS, jelikož nalezené záznamy, na rozdíl od výslovné dikce čl. 13 LZPS, nejsou uchovávány v soukromí. Z toho plyne, že v případě nálezu také pochopitelně není třeba, aby státní zástupce či soud vydával příkaz k zajištění dat.

Jedná-li se o zprávy nepřečtené, a tedy i zprávy doručené až po zajištění přístroje, respektive i údaje o příchozím hovoru nebo jiném datovém provozu proběhnuvším až po zajištění přístroje, je třeba aplikovat § 88 TŘ[301] (případně § 88a TŘ, pokud by se mělo jednat pouze o údaje o telekomunikačním provozu). V těchto případech je třeba zprávy považovat za dosud nedoručené písemnosti, jejichž otevření je zásahem do tajemství zpráv podávaných telefonem, a s těmito informacemi se lze seznámit pouze při splnění zákonných podmínek (závažná trestná činnost, subsidiarita a důvodnost) na základě příkazu soudce. Uvedené pochopitelně platí i pro nevyzvednuté zprávy v hlasové schránce.[302] V případě nevyzvednutých zpráv z hlasové

300 Viz Pokyn obecné povahy Nejvyšší státní zástupkyně č. 8/2009, o trestním řízení. Dostupné z http://www.nsz.cz/images/stories/PDF/POP/trest/1_SL_902-205_2.pdf.

301 Viz Výkladové stanovisko Nejvyššího státního zastupitelství č. 4/2005, 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. Dostupné z http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2005/stanovisko%204-2005.pdf.

302 Pokud by se však jednalo o již v minulosti adresátem vyslechnuté (vyzvednuté) hlasové zprávy, zvláštní ochrany dopravovaných zpráv již nepožívají a lze je jakožto záznam uchovávaný v soukromí zajistit postupem podle § 158d odst. 3 TŘ. Viz dále jiná data uložená mimo mobilní telefon (cloud).

schránky je však tím spíš nutný příkaz soudu k odposlechu podle § 88 TŘ, jelikož tyto zprávy se na rozdíl od nepřečtených SMS zpráv ani nenacházejí přímo v zajištěném mobilním telefonu. Hlasové zprávy totiž mohou být prostřednictvím mobilního telefonu pouze vyzvednuty z úložišť operátora. Je proto zřejmé, že právní důvod zajištění mobilního telefonu (odejmutí, domovní prohlídka atp.) nemůže v žádném případě pokrýt data nacházející se mimo telefon. Obdobně je nutné posuzovat i jiná data přístupná skrz mobilní telefon, avšak uložená mimo něj, tak jak je popsáno dále.

Je však třeba upozornit, že dle stanoviska Nejvyššího státního zastupitelství z roku 2015[303] je nezbytné, aby byl příkaz k odposlechu dán ještě předtím, než vůbec dojde k samotné komunikaci. Nejvyšší státní zastupitelství správně uvádí, že ohledně obsahu samotné komunikace se nelze spoléhat na analogickou aplikaci § 88a TŘ, jelikož dané ustanovení dopadá pouze na údaje o uskutečněném telekomunikačním provozu, tj. například na provozní a lokalizačních údaje uchovávané podle § 93 odst. 3 a 4 zákona o elektronických komunikacích. Zdá se však, že Nejvyšší státní zastupitelství poněkud ukvapeně vyloučilo rovněž aplikaci § 88 TŘ o odposlechu a záznamu telekomunikačního provozu. Ve stanovisku tak uvádí, že na rozdíl od údajů o telekomunikačním provozu obsah zpráv „není podnikatel v elektronických komunikacích oprávněn uchovávat, a tudíž ani oprávněn poskytnout". Nejvyšší státní zastupitelství pak dovozuje, že § 88 TŘ lze využít pouze v reálném čase probíhající komunikace. U služeb informační společnosti je však naopak veškerá komunikace (proběhnuvší či teprve probíhající) zaznamenávána a tyto záznamy jsou dále uchovávány. V opačném případě by ani nebylo možné služby, které nezprostředkovávají komunikaci v reálném čase, jako je zejména e-mail či služby typu „messenger", poskytovat. Pokud byl záznam komunikace proveden a uložen v zajištěném mobilním telefonu, není dle našeho názoru důvod, aby nebyl takový záznam,

303 Viz Výkladové stanovisko Nejvyššího státního zastupitelství č. 1/2015, ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek. Dostupné z http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2015/1_SL_760-2014.pdf.

se kterým se adresát dosud neměl možnost seznámit, po vydání příkazu soudu k odposlechu a záznamu telekomunikačního provozu podle § 88 TŘ využit v trestním řízení.[304]

Při využívání dat z mobilních telefonů je však ještě palčivější otázka ochrany soukromí ve vztahu k datům, která jsou dostupná skrz zajištěný mobilní telefon, avšak uložena jsou mimo něj na externích úložištích, jak je tomu zejména v případě cloudových aplikací (např. e-mail a aplikace typu Facebook) či cloudových uložišť (jako je např. iCloud, Dropbox či Google Drive), dnes již zcela běžně instalovaných v moderních mobilních telefonech. Mobilní telefon je v těchto případech jakousi přístupovou bránou k potenciálně neomezenému množství dat uložených na internetové síti. Mobilní telefon může být v okamžiku zajištění přihlášený na konkrétní cloudové služby nebo může být nastaven tak, že si přímo pamatuje přístupové údaje k těmto službám. Skutečnost, že je tato přístupová brána v podobě mobilního telefonu otevřena dokořán, zcela jistě nedává policejnímu orgánu oprávnění vstoupit. Stejně tak jako když orgán činný v trestním řízení nalezne u podezřelé osoby klíče od bytu, není z tohoto titulu oprávněn vstoupit do bytu a provést domovní prohlídku, není nepochybně ani orgán, který zajistí mobilní telefon, oprávněn bez dalšího procházet data uložená mimo mobilní telefon.

Domníváme se proto, že policejní orgán by si měl vždy před analýzou dat uložených mimo mobilní telefon zajistit předchozí povolení soudce podle § 158d odst. 3 TŘ, který upravuje podmínky sledování osob a věcí. Dané ustanovení mimo jiné pamatuje i na zjišťování obsahu záznamů uchovávaných v soukromí za použití technických prostředků. Stanovisko Nejvyššího státního zastupitelství z roku 2015 shodně uvádí, že tento operativně pátrací úkon na základě soudního povolení může být proveden, např. jedná-li se o e-mailovou schránku za účelem zjištění rozepsaných zpráv, odeslaných zpráv, nikoliv trvale odstraněných zpráv a přijatých zpráv, včetně

304 Souhlas soudce podle § 8 odst. 5 TŘ ke zbavení povinnosti mlčenlivosti, který navrhuje využít v uvedeném stanovisku Nejvyšší státní zastupitelství, může být relevantní, budou-li údaje vyžadovány přímo od zprostředkovatele, nikoliv budou-li tyto údaje čerpány ze zajištěného mobilního telefonu. I pokud se však orgány činné v trestním řízení budou muset obrátit na zprostředkovatele, měl by být s ohledem na ústavně chráněná práva aplikován přísnější režim § 88 TŘ o odposlechu a záznamu telekomunikačního provozu.

těch, které si příjemce doposud nepřečetl, pokud tuto možnost objektivně měl.[305] Pokud by povolení podle § 158d odst. 3 TŘ nebylo zajištěno, takto získaný důkazní prostředek by byl pro účely trestního řízení jakožto nezákonně získaný zcela bezcenný, a by se nadto osoba extrahující data z cloudu svým počínáním mohla dopustit trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací ve smyslu § 230 TZ. V případě dat uložených mimo mobilní telefon, která zachycují dosud nedoručenou komunikaci (např. nepřečtený e-mail či jiná fakticky adresátovi nedoručená zpráva), bude nezbytné v souladu s výše uvedenými závěry ohledně zpráv doručených až po zajištění mobilního telefonu postupovat podle § 88 TŘ o odposlechu a záznamu telekomunikačního provozu.

Otázka zajištění dat v cloudu se pochopitelně v posledních letech stává zcela klíčovou pro celou disciplínu digitální forenzní analýzy.[306] Sdílené výpočetní kapacity jsou s rozvojem rychlého internetu stále více populární a veškerá data se z důvodu vyšší efektivity přesouvají z lokálně umístěných počítačů či mobilních telefonů a jiných zařízení na servery poskytovatelů online služeb. Nicméně situace, kdy nelze k takovým datům zajistit přístup prostřednictvím mobilního telefonu a je třeba využít spolupráci se zprostředkovateli, nejsou předmětem této kapitoly zaměřené na obsah mobilních telefonů. Na druhou stranu je nutné upozornit, že i programy běžící tzv. v cloudu mnohdy instalují klienta (program) na paměť mobilního telefonu. Část dat se tak vždy nahrává na paměť mobilního telefonu. Mobilní telefon zejména při těchto operacích slouží jako jakési průtokové úložiště dat, kdy nejnovější data vytěsňují data nejstarší. Typicky může paměť mobilního telefonu obsahovat e-maily doručené a odeslané během posledních několika týdnů apod. Takto uložená data může nepochybně policejní orgán bez dalšího využít, stejně jako jakákoliv jiná data uložená v řádně zajištěném mobilním telefonu, tak, jak je uvedeno shora.

305 Viz Výkladové stanovisko Nejvyššího státního zastupitelství č. 1/2015, ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek. Dostupné z http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2015/1_SL_760-2014.pdf.

306 Blíže k technickým i právním úskalím forenzní analýzy v rámci „cloudu" lze doporučit Quick, D., Martini, B., Choo, R. *Cloud Storage Forensics*. Elsevier Inc., 2014, s. 5 a násl.

Co se týká dat uložených v mobilním telefonu, není z právního pohledu podstatné, zda jsou tato data uložena v integrované paměti telefonu, na vložených paměťových kartách či na SIM kartě. Zatímco operační systém telefonu včetně jeho nastavení bude zpravidla uložen přímo v integrální paměti, paměťová karta bude mnohdy obsahovat média (audio-video záznamy), ale také mobilní aplikace a jimi generovaná data. Na SIM kartě mobilního telefonu mohou být uloženy zejména SMS zprávy, kontakty a poslední volaná čísla. Vedle toho SIM karta vždy také obsahuje unikátní číslo IMSI („international mobile subscriber identity"), které jednoznačně identifikuje účastníka či přesněji řečeno SIM kartu v rámci telekomunikační sítě po celém světě.

Na tomto místě je třeba uvést, že i veškerá data uložená přímo v mobilním telefonu, která nepodléhají ochraně dopravovaných zpráv, jako je tomu např. u nepřečtených zpráv či zpráv doručených až po zajištění, se s jejich rostoucím rozsahem a detailem stávají čím dál tím citlivější, a tedy hodna ochrany. Přes shora uvedený trend cloudových služeb se se zvyšující paměťovou kapacitou mobilních telefonů enormně zvyšuje rozsah uložených dat. Zatímco tak v nedávné minulosti mohly mobilní telefony uchovávat pouze omezený počet SMS zpráv, dnes jsou paměťové možnosti v tomto ohledu takřka neomezené a mobilní telefony běžně obsahují všechny doručené a odeslané SMS zprávy, které se v mobilním telefonu nashromáždily od jeho uvedení do provozu. Údaje o telekomunikačním provozu, uložené v mobilním telefonu, jsou současně rozsáhlejší než kdy dříve. Například telefony typu iPhone a mobilní telefony s operačním systémem Android ukládají seznam všech využitých základnových stanic. Tyto telefony tak běžně obsahují poměrně detailní historii pohybu přístroje v místě a čase. V návaznosti na konkrétní nastavení telefonu může nadto přístroj paralelně ukládat i rozsáhlá data synchronizovaná s cloudovými službami (např. e-maily či kalendáře).

> Právě s ohledem na stále rostoucí kvalitu a kvantitu dat uložených v mobilním telefonu Nejvyšší soud Spojených států amerických v rozhodnutí Riley v. California[307] dovodil, že k prohledání dat uložených v zajištěném mobilním telefonu je třeba soudní příkaz vždy. Dle odůvodnění totiž mobilní

307 Viz Spojené státy. Rozhodnutí Nejvyššího soudu Spojených států amerických ze dne 25. 6. 2014 ve věci Riley v. California. Dostupné z http://www.scotusblog.com/case-files/cases/riley-v-california/.

> telefony v dnešní době mnohdy obsahují navýsost soukromé informace a pouhá skutečnost, že technologie umožnila tyto informace nosit neustále při sobě, nezbavuje jedince práva na jejich ochranu. Rozhodnutí je sice třeba číst v kontextu amerického principu „search incident to a lawful arrest", dle kterého osobní prohlídka zadržené osoby probíhá zejména kvůli zajištění bezpečnosti policejního orgánu, i tak je však trend větší ochrany dat obsažených přímo v mobilním telefonu nepřehlédnutelný, a český zákonodárce by proto měl o této problematice uvažovat *de lege ferenda*.

Uvedená omezení zákonnosti důkazů ve smyslu trestního řádu, respektive zákonné postupy obstarání důkazů, se přirozeně neaplikují na data získaná soukromou osobou. Důkaz přitom může podle § 89 odst. 2 TŘ vyhledat, předložit nebo jeho provedení navrhnout každá ze stran.[308] Osoba odlišná od OČTŘ nepostupuje podle ustanovení trestního řádu a není tak při získávání dat omezena trestním řádem. Jako důkaz tak může být v trestním řízení použit například i audio záznam pořízený na mobilní telefon bez souhlasu osoby, jejíž hlas byl zaznamenán. Přípustnost takového důkazu je však nezbytné vždy posuzovat s ohledem na respektování práva na soukromí. Dle soudu tedy taková informace může sloužit jako důkaz jen za podmínky, *„že zásah do soukromí je odůvodnitelný převažujícím zájmem na straně toho, kdo informaci popsaným způsobem opatřil a následně použil.*"[309] Současně jakákoliv účast státních orgánů na obstarání důkazu mimo rámec trestního řádu zpravidla povede k nepřípustnosti takto získaného důkazu.[310]

Nadto Ústavní soud v minulosti uvedl,[311] že za významnou okolnost k tomu, aby mohl být k důkazu použit i zvukový záznam, který byl pořízen soukromou osobou bez souhlasu osob, jejichž hlas je zaznamenán, je nutné považovat především to, zda důkaz v podobě například zvukového záznamu

---

308 Dle § 12 odst. 6 TŘ se stranou rozumí ten, proti němuž se vede trestní řízení, zúčastněná osoba a poškozený a v řízení před soudem též státní zástupce a společenský zástupce; stejné postavení jako strana má i jiná osoba, na jejíž návrh nebo žádost se řízení vede nebo která podala opravný prostředek.

309 Viz usnesení Nejvyššího soudu sp. zn. 8 Tdo 908/2013.

310 Zásah do soukromí za účasti policejních orgánů (v daném případě zadržený podezřelý nájemný vrah ve spolupráci s policií nahrál telefonát obviněnému, ve kterém podezřelý s obviněným rozebral detaily vraždy) shledal Evropský soud pro lidská práva v rozporu s článkem 8 EÚLP ve svém rozsudku ESLP ve věci A. proti Francii, stížnost č. 14838/89.

311 Viz usnesení Ústavního soudu sp. zn. II. ÚS 143/06.

na mobilním telefonu svědka stojí v konkrétní věci osamocen v rámci hodnocení otázky viny pachatele, anebo zda má soud k dispozici jiné důkazy, které významným způsobem nasvědčují důvodnosti obvinění a s nimiž je zvukový záznam v obsahové shodě.

Je třeba také podotknout, že i k obsahu, který je ve skutečnosti uložen přímo v mobilním telefonu a současně není kryt tajemstvím dopravovaných zpráv, či také k důkazním prostředkům předloženým stranami řízení musí OČTŘ vždy přistupovat nanejvýš zdrženlivě. Dle § 2 odst. 4 TŘ lze při provádění úkonů trestního řízení zasahovat do lidských práv a svobod jen v odůvodněných případech, na základě zákona a pouze v míře nezbytné pro zajištění účelu trestního řízení. Tato zásada přiměřenosti (zdrženlivosti) se sice již přímo promítá například do § 88 odst. 1 TŘ, který stanoví, v jakých případech lze využít odposlech, či do § 158 b odst. 2 TŘ, který upravuje subsidiaritu použití operativně pátracích prostředků, avšak jakožto základní zásadu trestního řízení je ji třeba zohlednit a respektovat v rámci celého trestního řízení.

Tato zásada přiměřenosti, která úzce souvisí s principem presumpce neviny, musí být aplikována zejména s ohledem na rušení práva na soukromí ve smyslu čl. 10 odst. 3 a čl. 13 LZPS i čl. 8 EÚLP. Při zajištění věci, jako je mobilní telefon, současně dochází k výraznému zásahu do vlastnického práva zaručeného čl. 11 LZPS. Dotčená osoba je totiž nejenom zbavena věci, která má v případě nejmodernějších chytrých telefonů leckdy nikoliv nepatrnou hodnotu, ale hlavně je zbavena možností vykonávat své vlastnické právo k věci, kterou do té doby používala takřka neustále a zpravidla i víc než jakoukoliv jinou jednu konkrétní věc. Při hodnocení přípustnosti důkazu a jeho provedení by tak měly hrát roli i otázky na přiměřenost zásahu do těchto ústavně chráněných práv.

VIII.5 Hodnocení důkazu

Dle zásady volného hodnocení důkazů, zakotvené v § 2 odst. 6 TŘ, OČTŘ hodnotí důkazy podle svého vnitřního přesvědčení, založeného na pečlivém uvážení všech okolností případu jednotlivě i v jejich souhrnu. Zákon tedy

nestanoví míru důkazů potřebných k prokázání určité skutečnosti ani váhu či důkazní sílu jednotlivých důkazů.[312] To platí i pro elektronické důkazy.

Zatímco každý důkaz, ať již se jedná o svědeckou výpověď či ohledání hmotné věci, lze nepochybně zmanipulovat, u elektronických důkazů je pro laika zpravidla obtížné podezření z manipulace správně vyhodnotit. Aby bylo minimalizováno podezření z manipulace přímo ze strany OČTŘ či znalců, je v první řádě nezbytné důkazní prostředek správně zajistit a následnou forenzní analýzu řádně zdokumentovat. Vedle toho je třeba se také zabývat otázkou, zda data získaná z mobilního telefonu mohou být v konkrétním případě potvrzena i jinými daty. Kromě zcela na mobilním telefonu nezávislých informací (např. svědecká výpověď) může být věrohodnost důkazu z mobilního telefonu nezřídka potvrzena zejména provozními a lokalizačními údaji od mobilního operátora, synchronizovanými daty (např. v počítači či cloudu) nebo daty z druhého komunikačního zařízení, s nímž zajištěný přístroj navázal spojení.

Stejně jako u jiných telekomunikačních prostředků bývá dále ověření autenticity důkazního prostředku v podobě dat z mobilních telefonů komplikováno potřebou prokázat určitou aktivitu na elektronickém přístroji konkrétní osobě. Vždy je možné setkat se s námitkami, že zařízení použil někdo jiný. Mobilní telefon je však například na rozdíl od osobního počítače vysoce individuální zařízení, a možnosti prokázat konkrétní činnost konkrétní osobě jsou proto zpravidla širší.

To se potvrdilo i v případě čtyř telefonátů o uložení bomb na Hlavním nádraží v Praze v roce 2003. Obžalovaný byl dostatečně identifikovaný na základě znaleckého posudku z kriminalistické audioexpertizy a zjištění, že krátce před inkriminovanými událostmi i následně po nich hovořil z telefonu, ze kterého byly volány předmětné poplašné zprávy, s různými svými přáteli a známými, přičemž tyto telefonáty byly navíc zaměřeny v místech, které se shodovaly s místy ubytování a zaměstnání obžalovaného.[313]

Bez zajímavosti není, že se znalecký posudek dle názoru Ústavního soudu dostatečně vypořádal také s časovým odstupem, který byl vzhledem k věku obviněného nepodstatný, a rovněž i s handicapem chybějící zubní protézy

312 Viz Šámal, 2013a, op. cit., s. 40-41.
313 Viz usnesení Nejvyššího soudu sp. zn. 4 Tz 24/2013.

obviněného. Znalecký posudek z oboru fonoskopie označil obžalovaného za pravděpodobného mluvčího předmětných telefonátů a znalecký posudek z audioexpertizy vyloučil jako možné mluvčí další dva podezřelé. Ústavní soud však ohledně tohoto případu také zdůraznil,[314] že závěr o vině postavily soudy na jiných důkazech než na znaleckém posudku v oboru kriminalistika-audioexpertiza.

Je evidentní, že shora uvedené obavy z neautentičnosti elektronického důkazu mnohdy nemusí hrát v rámci celého trestního řízení velkou roli. Data z mobilních telefonů se totiž zpravidla osvědčila spíše jako důkazy nepřímé, které až spolu s dalšími důkazy tvoří ucelený, spojitý a na sebe navzájem navazující řetěz důkazů vedoucí ke zjištění skutkového stavu věci, o němž nejsou důvodné pochybnosti. Data z mobilních telefonů také mnohdy pouze vyvrací vymyšlenou verzi podezřelého a mohou vést podezřelého k doznání.

VIII.6 Shrnutí kapitoly

Tato kapitola naznačila prostřednictvím dnes nejcharakterističtějšího mobilního komunikačního zařízení, mobilního telefonu, jak se neustále zvyšuje potenciál těchto zařízení jakožto důkazních prostředků v rámci trestního řízení. Je to dáno nejenom nárůstem jejich počtu, ale hlavně tím, že se dramaticky rozšiřuje jejich funkčnost a s tím související paměťová kapacita. Mobilní telefon byl popsán jako dynamické zařízení, které neustále mění svůj obsah a vyžaduje tak odborné zacházení jak při zajištění, tak při následném uchování a forenzní analýze. Metody extrakce dat v rámci forenzní analýzy lze rozlišit na manuální, logickou a fyzickou extrakci. Zatímco fyzická extrakce je nejvíce sofistikovanou formou umožňující nejširší akvizici dat, manuální extrakce je pro svoji snadnost a tedy i rychlost zpravidla preferována. S rostoucí sofistikovaností mobilních komunikačních zařízení a jejich lepší ochranou budou i na forenzní analýzu kladeny rostoucí nároky. Aby mohly být výsledky forenzní analýzy mobilních telefonů použity v řízení před soudem, musí být analyzovaná data shromážděna v souladu s platnými právními předpisy. Spornou se v tomto ohledu zdá být zejména otázka oprávnění k přístupu k datům uloženým mimo mobilní telefon, např. v cloudu,

314 Usnesení Ústavního soudu sp. zn. I. ÚS 413/06.

prostřednictvím zajištěného mobilního telefonu. Stejně tak zůstává otázkou, zdali by obecně data uložená na mobilním telefonu neměla požívat širší ochrany než dosud. Je stále více evidentní, že pouhá analogická aplikace zavedených trestněprávních institutů na dokazování daty z mobilních komunikačních zařízení na jedné straně neposkytuje jednoznačné odpovědi orgánům činným v trestním řízení a na druhé straně nechrání dostatečně ústavně garantovaná lidská práva.

IX DOKAZOVÁNÍ DATY Z DOHLEDOVÝCH SYSTÉMŮ KYBERNETICKÉ BEZPEČNOSTI

IX.1 Vysvětlení pojmu

Jedním z klíčových prvků kybernetické bezpečnosti je funkční dohledové pracoviště, které, zjednodušeně řečeno, představuje tým odborníků na problematiku kybernetické bezpečnosti. Tato pracoviště se často označují jako CSIRT, CERT nebo CIRC s tím, že tato označení se používají do značné míry zaměnitelně. V České republice působí v současné době těchto týmů hned několik, ať už se jedná o týmy mezinárodně akreditované,[315] neakreditované[316] či jiné.[317]

Jednotlivé týmy nemají stejnou povahu ani stejnou oblast působení. Existenci některých z nich přímo předpokládá ZKB. Možnost konkrétních subjektů ustavit vlastní dohledové pracoviště kybernetické bezpečnosti ale není závislá na žádné centrální autoritě. V širším slova smyslu totiž za dohledové pracoviště můžeme považovat i obecné kapacity některých subjektů dedikované řešení bezpečnostních incidentů. Procedury, které by zakládaly existenci dohledového pracoviště v jeho současném úzkém chápání,[318] nemusí být přítomny a dohledové pracoviště tak ani nemusí být formálně označováno.

315 Mezi akreditované jako Trusted Introducer patří CESNET-CERTS (od 2008), CSIRT-MU (od 2011), CSIRT.CZ (od 2011), CZ.NIC-CSIRT (od 2010) a GOVCERT.CZ (od 2014). Za další zastřešující organizace dohledových pracovišť pak můžeme považovat např. Forum Incident Response and Security Teams (FIRST) nebo European Network and Information Security Agency (ENISA).

316 Mezi zařazené na seznam Trusted Introducer, ale neakreditované patří 2CCSIRT (od 2014), ACTIVE24-CSIRT (od 2012), ALEF-CSIRT (od 2015), CASABLANCA.CZ-CSIRT (od 2014), CDT-CERT (od 2014), Coolhousing CSIRT (od 2014), CSIRT Merit (od 2015), CSIRT-VUT (od 2014), CSOB-Group-CSIRT (od 2014), DIAL-CERT (od 2013), FORPSI-CSIRT (od 2015), ISPA CSIRT (od 2015), KAORA-CSIRT (od 2015), O2.cz CERT (od 2014), SEBET (od 2014) a SEZNAM.CZ-CSIRT (od 2013), WEB4U-CSIRT (od 2015).

317 V ČR se jedná zejména o CIRC-MO.

318 Jak popsáno např. ENISA. *Good Practice Guide for Incident Management*. Dostupné z: https://www.enisa.europa.eu/activities/cert/support/incident-management/files/good-practice-guide-for-incident-management.

Můžeme tak rozlišovat mezi vládními pracovišti,[319] národními pracovišti,[320] interními týmy přidruženými ke vzdělávacím a výzkumným institucím,[321] poskytovatelům služeb informační společnosti,[322] finančním společnostem,[323] nekomerčním subjektům[324] a případnými dalšími.[325] Tyto týmy mají kromě odlišné povahy, i odlišné okruhy působnosti[326], které mohou být určené rozsahem IP adres[327], identifikací autonomního systému[328], identifikací domén[329] nebo slovním popisem.[330] Vymezené pole působnosti jednoho týmu se může překrývat s jinými týmy,[331] což samozřejmě může způsobovat problémy, které je nutné řešit na úrovni dohody mezi týmy navzájem.[332]

Hlavní úlohou dohledových pracovišť je zajištění bezpečnosti svěřených sítí a k naplnění tohoto účely týmy spolupracují mezi sebou navzájem i s dalšími zástupci bezpečnostní komunity.

IX.1.1 Vládní CERT

V rámci struktury dohledových pracovišť má specifické postavení vládní CERT, jehož existenci předepisuje ZKB v § 20 a který představuje součást NBÚ. Roli vládního CERTu plní v současné době GovCERT.cz v rámci Národního centra kybernetické bezpečnosti v Brně. Vládní CERT se svými nařizovacími a kontrolními pravomocemi působí pouze na informační a komunikační systémy, jejichž funkčnost má pro Českou republiku zásadní

319 Viz ZKB § 20.
320 Viz ZKB § 17.
321 Např. CESNET-CERTS, CSIRT-MU, CSIRT-VUT.
322 Např. 2CCSIRT, ACTIVE24-CSIRT, CASABLANCA.CZ-CSIRT, CDT-CERT, O2.cz CERT, SEBET, SEZNAM.CZ-CSIRT.
323 Např. CSOB-Group-CSIRT.
324 Např. CZ.NIC-CSIRT.
325 Např. ze strany Trusted Introducer neakreditovaný SKY-CERT (Estonsko), jehož vznik se datuje přibližně do doby, kdy společnost eBay získala Skype Technologies.
326 Viz ENISA, op. cit., s. 14-19.
327 Pro CSIRT-MU se jedná např. o rozsah 147.251. 0. 0/16, tedy 147.251. 0. 0 až 147.251.255.255.
328 Např. pro O2.cz CERT se jedná o AS5610, 20884, 28725, 51154.
329 Např. pro CDT-CERT se jedná o *.cdt.cz, *.cd-t.cz, *.cd.cz.
330 Pro CZ.NIC např. *„Polem působnosti týmu CSIRT.CZ je celá Česká republika, tzn. všichni uživatelé a všechny sítě provozované v České republice se nachází ve sféře vlivu CSIRT.CZ“*. CZ.NIC. O nás. Dostupné z: https://www.csirt.cz/page/882/o-nas/.
331 Např. povinnosti stanovené v § 8 ZKB, dále vztah mezi institucionálním dohledovým pracovištěm a pracovištěm poskytovatele konektivity.
332 Srov. ENISA, op. cit., s. 19. Toto samozřejmě může hrát roli při případné snaze zajistit důkazní prostředek.

význam. Jedná se primárně o prvky kritické informační[333] a komunikační[334] infrastruktury a o významné informační systémy.[335] Vládní CERT v souladu se zákonem zejména přijímá hlášení o kybernetických bezpečnostních incidentech. V souvislosti s těmito incidenty pak postiženým subjektům poskytuje metodickou podporu a součinnost. Jako vládní dohledové pracoviště přijímá podněty od všech subjektů druhově vymezených v § 3 písm. c), d) a e) ZKB i údaje od národního CERTu. Dá se tedy předpokládat, že v jeho rámci bude možné zajistit důkazy o bezpečnostních incidentech, které se udály v rámci uvedených povinných subjektů.

IX.1.2 Národní CERT

Dalším pracovištěm se specifickým postavením v rámci systému kybernetické bezpečnosti je národní CERT. Jeho existenci předepisuje ZKB v § 17 a má být reflexí poptávky soukromoprávních subjektů po centralizovaném řešení sběru informací o kybernetické bezpečnosti, které by mělo soukromoprávní povahu.[336] Úlohu národního CERTu plní CSIRT.cz. Ten poskytuje, stejně jako vládní CERT, metodiku a asistenci při účinném řešení různých typů kybernetických bezpečnostních incidentů v rámci systémů, které jsou pro chod státu dostatečně důležité, aby byly zakomponovány do systematiky ZKB, ale zároveň nepodléhají vládnímu CERTu – zejména se jedná o poskytovatele služby elektronických komunikací[337] a o osoby zajišťující významnou síť.[338] Národní CERT tak nedisponuje žádnými exekutivními pravomocemi, ale funguje právě za účelem vyhodnocování a metodické podpory subjektů, které jsou stanoveny zákonem, a subjektů, které mají zájem o možnost kolektivní obrany před kybernetickými hrozbami. Soukromoprávní povaha národního CERTu[339] tak má, v porovnání s vládním dohledovým

333 Viz § 3 písm. c) ZKB.
334 Viz § 3 písm. d) ZKB.
335 Viz § 3 písm. e) ZKB.
336 Polčák mluví o aspektu autonomie vůle, kterým se vytváří možnost dobrovolné spolupráce soukromoprávních subjektů, které by jinak nebyly povinnými subjekty podle ZKB – srov. Polčák, R. Kybernetická bezpečnost jako aktuální fenomén českého práva. *Revue pro právo a technologie,* 2015, roč. 5, č. 11, s. 110.
337 Viz § 3 písm. a) ZKB.
338 Viz § 3 písm. b) ZKB.
339 Za projev je možné považovat § 8 ZKB v kombinaci s vyhláškou 316/2014 Sb., kdy § 8 odst. 4 stanovuje, že náležitosti a způsoby hlášení stanoví vyhláška, ta tak ale činí pouze pro hlášení vládnímu CERTu (tedy hlášení od povinných subjektů v § 3 písm. c) až e) a nikoli národnímu CERTu (hlášení povinných subjektů v § 3 písm. b).

pracovištěm, umožnit výrazně větší flexibilitu v neočekávaných situacích, kdy bude nutné implementovat kvalitativně nová řešení či postupy v krátkém čase. Na rozdíl od vládního CERTu totiž není národní CERT, vzhledem ke své soukromoprávní povaze, vázán zásadou o zakázanosti výslovně nedovoleného jednání. Národní CERT totiž uzavřením veřejnoprávní smlouvy[340] mezi provozovatelem tohoto dohledového pracoviště a NBÚ nenabývá veřejnoprávní povahy. Zachování soukromoprávní povahy tak vede k předpokládané vyšší míře flexibility a snadnější spolupráci s obdobnými pracovišti na mezinárodní úrovni. V tom všem je národní CERT jako subjekt soukromého práva limitován pouze zákonnými zákazy. Jedná se tak o ryze soukromoprávní aktivitu, která je provozována ve veřejném zájmu. Tomuto pracovišti pak ze zákona hlásí bezpečnostní incidenty subjekty druhově vymezené v § 3 písm. b) ZKB a Národní CERT je dále bez uvedení ohlašovatele předává vládnímu CERTu.

IX.1.3 Další dohledová pracoviště

Český právní řád existenci žádných dalších dohledových pracovišť přímo nepředpokládá. V duchu jejich výše uvedené povahy jako důležitého prvku zajištění kybernetické bezpečnosti ale samozřejmě existují. Kromě pracovišť při vzdělávacích institucích, poskytovatelích služeb informační společnosti, finančních společnostech a nekomerčních subjektech mohou existovat i pracoviště v širším slova smyslu. Jejich činnost pak může být založena pracovněprávním zařazením jejich členů nebo mohou existovat pracoviště poskytující funkci dohledového pracoviště jako služby na smluvním základě.

Všechny tyto subjekty jsou jednoznačně soukromoprávní povahy a jako takové se řídí stejnými principy jako shora uvedený národní CERT. Zároveň je ale nutné si uvědomit, že se jedná o dohledová pracoviště provozovaná konkrétními právnickými osobami za účelem ochrany vlastní informační infrastruktury. Celý režim fungování je zde tak výrazně odlišný od vládního nebo národního dohledového pracoviště. Ve vztahu k infrastruktuře je vykonávána bezprostřední kontrola – možnost případného získávání informací je tak širší ve vztahu ke klientskému provozu i ve vztahu k vlastním zaměstnancům. Sběr těchto údajů pak musí být vždy v souladu s příslušnými zákonnými předpisy.

340 Viz § 159 a násl. zákona č. 500/2004 Sb., správního řádu. § 19 ZKB.

Nakolik jsou tato dohledová pracoviště vázána ZKB a VKB, nelze zcela jednoduše určit. Na první pohled tedy, zejména z hlediska zajišťování důkazních prostředků, nemusí být zcela jisté, nakolik má subjekt možnost sběru informací o incidentech přímo danou ZKB.[341] V ZKB se totiž pro dohledová pracoviště povinných subjektů nachází explicitní zákonné zmocnění pro zpracování osobních údajů, např. IP adres zdrojů bezpečnostních incidentů.[342] V případě chybějícího zákonného zmocnění je pak nutné zkoumat, nakolik je dohledovému pracovišti tato možnost dána v intencích oprávněného zájmu nebo zákoníku práce v případě sledování provozu na vnitřní síti. Na povahu některých dohledových pracovišť, jejichž existenci zákon přímo nepředpokládá, je možné usuzovat s poměrně velkou mírou jistoty.[343] U každého pracoviště je ale nutné tuto povahu vždy pečlivě vyhodnotit.

IX.2 Zajištění a uchování důkazního prostředku

IX.2.1 Zajištění důkazního prostředku v rámci vlastní infrastruktury

Shora uvedené rozlišení mezi jednotlivými typy dohledových pracovišť má určitý vliv z hlediska procesního postupu při zajištění důkazního prostředku. Hraje totiž roli, zda se jedná o dohledová pracoviště povinná předávat hlášení o bezpečnostním incidentu dle ZKB, či nikoli. Dle našeho názoru mohou v zásadě nastat tři situace. V první z nich dohledové pracoviště náleží k subjektu, který je povinným dle ZKB. Ve druhé situaci dohledové pracoviště náleží k subjektu, který dle ZKB povinným není, zároveň ale tento subjekt podniká podle ZEK. Poslední situace pak nastává ve chvíli, kdy dohledové pracoviště náleží k subjektu, který není povinným dle ZKB a zároveň nepodniká podle ZEK.

341 Subjekty druhově vymezené v § 3 písm. b) ZKB, subjekty druhově vymezené v § 3 písm. c), d) a e) ZKB s náležitostmi hlášení uvedenými v § 32 a příloze č. 5 VKB.

342 IP adresy je totiž de lege lata nutné za určitých situací považovat za osobní údaje. Dynamická IP adresa může být osobním údajem také, ale pouze za situace, kdy jsou k dispozici i logy ze systému poskytovatele internetové konektivity. Srov. Rozsudek SDEU ve věci SABAM, sp. zn. C-70/10. Poměrně jasnou předběžnou otázku ve vztahu k IP adrese pak položil německý Bundesgerichtshof ve věci C-582/14, nicméně na odpověď bude nutné vyčkat. Viz také Harašta, J., Míšek, J. IP adresy v kybernetické bezpečnosti. *Revue pro právo a technologie*, 2015, č. 12, s. 29-34.

343 Např. CDT-CERT jako dohledové pracoviště ČD-Telematika, a. s. může být dohledovým pracovištěm prvku kritické infrastruktury, DIAL-CERT jako dohledové pracoviště Dial Telecom, a. s. může být dohledovým pracovištěm osoby zajišťující významnou síť podle § 3 písm. b) ZoKB.

Jak bylo výše uvedeno, v prvním případě se jedná zejména o subjekty typově vymezené v § 3 písm. b), c), d) a e) ZKB. Tyto subjekty mají v souladu s § 8 ZKB povinnost hlásit kybernetické bezpečnostní incidenty bezodkladně po jejich detekci. Součástí tohoto hlášení by tak mělo být zejména uvedení IP adresy, která byla zdrojem incidentu. Informační toky v rámci ZKB jsou pak nastaveny tak, že u těchto typů subjektů bude informace o okolnostech incidentu vždy předána vládnímu CERTu.[344] K těmto údajům je pak možné přistupovat v souladu v § 8 odst. 1 TŘ. Jelikož tyto údaje slouží ke splnění zákonné povinnosti, je jejich sběr možný a nehrozí tak problém se zákonností takto získaného důkazu.

Ve chvíli, kdy subjekt, jehož potřebám dohledové pracoviště slouží, není povinným podle ZoKB, ale zároveň se jedná o subjekt podnikající dle ZEK, je nutné důkazní prostředek zajišťovat odlišným způsobem. V prvé řadě nebude informace o incidentu povinně předána národnímu nebo vládnímu dohledovému pracovišti. V řadě druhé se pak, v případě již zmíněné IP adresy, jedná o údaj, který podléhá legislativě o uchovávání provozních a lokalizačních údajů. Celá problematika uchovávání provozních a lokalizačních údajů je složená ze dvou složek, tedy povinnosti údaje držet a práva k nim specifickým způsobem přistupovat.[345] Takto shromážděné údaje tedy také slouží ke splnění zákonné povinnosti, ale aby mohly být použity jako zákonný důkaz, je nutné, aby k nim OČTŘ přistupovaly pomocí specifického procesního institutu. Při zajišťování tohoto důkazního prostředku je tak nutné trvat na postupu v souladu s § 88a TŘ.

Poslední možností je, že dohledové pracoviště slouží potřebám subjektu, který není povinným subjektem dle ZKB a zároveň nepodniká podle ZEK. Zde je možné přistupovat k údajům podle § 8 odst. 1 TŘ, ale je zde zřejmě nejvíce problematických aspektů ve vztahu k zákonnosti takto opatřeného důkazu, mj. ve vztahu k pracovněprávním předpisům. Vzhledem k dostupným analytickým nástrojům, používaným na síti, je z technického hlediska možnost vykonávat nad provozem plošnou heuristickou a behaviorální analýzu poměrně bezproblémová. Hlavním problémem zde ale může být

344 U subjektu povinného dle § 3 písm. b) půjde informace cestou před národní CERT a z hlášení bude odstraněna informace o navrhovateli.

345 Srov. kapitolu VII. této publikace.

provádění monitorování takovým způsobem, aby byly případné důkazy využitelné i pro trestní řízení a nestaly se pro případnou nezákonnost použitého monitorovacího prostředku oním pověstným plodem otráveného stromu. Jakkoli totiž současná rozhodovací praxe nasvědčuje,[346] že konstatování nepřípustnosti důkazu na základě zprostředkovaného zásahu do práv[347] je pouze přepjatý formalismus, s touto námitkou se zcela jistě bude nutné kvalifikovaně vyrovnat. Dozor nad dodržováním interních předpisů ve vztahu k používání zařízení připojených do sítě je sice možné vykonávat, zároveň ale nesmí docházet ke sledování obsahu zasílaných zpráv.[348] Při podezřelé aktivitě zjištěné na základě metadat je pak již možné argumentovat konkrétním podezřením a monitorovat již podstatně sofistikovaněji další aspekty provozu souvisejícího s tímto strojem či uživatelským účtem.

Ve vztahu k údajům o subjektech, se kterými je zevnitř sítě komunikováno, je pak nutné posuzovat účel, za kterým je IP adresa zpracovávána. Při chybějícím explicitním zákonném zmocnění v ZKB a při chybějících povinnostech uchovávat provozní a lokalizační údaje podle ZEK je tak nutné uchýlit se k odůvodnění podle § 5 odst. 2 písm. e) ZOOÚ.[349] Aby takto opatřený důkaz nepředstavoval důkaz nezákonný, je nutno vypořádat se s podmínkami obsaženými v tomto ustanovení tak, aby bylo možné uzavřít, že sběr osobních údajů probíhal v souladu se ZOOÚ. Toto opatření tak musí být nezbytné za účelem naplnění chráněného zájmu.[350]

346 Srov. např. nález Ústavního soudu sp. zn. Pl. ÚS 47/13.

347 Viz rozsudek Nejvyššího soudu sp. zn. 21 Cdo 1009/98, č. 39/1999 Sb. civ. rozh.

348 Srov. § 316 odst. 2 zákona č. 262/2006 Sb., zákoníku práce. Viz také Polčák, R., Říha, Z., Malinka K. Právní aspekty interních směrnic – část I. *Data Security Management*, 2015, roč. 19, č. 2 a Polčák, R., Říha, Z., Malinka K. Právní aspekty interních instrukcí – část II. *Data security management*, 2015, roč. 19, č. 3.
Srov. Stanovisko Úřadu pro ochranu osobních údajů č. 2/2009, ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště. Dostupné z https://www.uoou.cz/files/stanovisko_2009_2.pdf.
Také Vidrna, J., Koudelka, Z. Zaměstnanci v objektivu kamer: právní aspekty monitoringu zaměstnanců. Praha: C. H. Beck, 2013, s. 106.

349 Jedná se o národní implementaci článku 7 písm. f) Směrnice 95/46/ES.

350 Zájem musí být v souladu s národním právem i právem EU jasně artikulovatelný tak, aby dovolil provést test proporcionality proti zájmům subjektu údajů. Také nesmí být pouze spekulativní. Srov. Opinion 6/2014, on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, Article 29 Data Protection Working Party. Dostupné z http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

IX.2.2 Zajištění důkazu aktivním protiopatřením

Často diskutovanou problematikou je možnost aktivního protiopatření, někdy nazývaného též hack-back.[351] Jakkoli se může jednat o přitažlivou možnost, přináší poměrně hodně problémů, a to nejen ve vztahu k legálnosti důkazů v rámci této akce získaných.

Jedním z problémů je, že v současné době neexistuje žádná obecně uznávaná taxonomie aktivních protiopatření. Některé náznaky se začínají ve vztahu k právu objevovat,[352] ale ačkoli navrhované taxonomie často reflektují požadavky praxe, je problém jejich použitelnost v praxi ověřit. Z hlediska výkonných orgánů pak zřejmě je možné dovodit možnost využití aktivních protiopatření na základě obecných oprávnění příslušného orgánu provádějícího toto protiopatření, nicméně ani tuto domněnku zatím praxe nemohla prověřit. Hranice těchto oprávnění jsou totiž velice vágní.[353] Použití aktivních protiopatření je omezováno často mlhavými hranicemi vlastní institucionální legitimity[354] – v případě armády se bude jednat o ochranu suverenity a celistvosti území, v případě orgánů činných v trestním řízení pak o agendu vyšetřování a stíhání trestných činů a o ochranu veřejného pořádku. Jaká konkrétní aktivní protiopatření tak je možné použít, zůstává otázkou, která nemá jasnou ani jednoduchou odpověď.

Absence obecně uznávané taxonomie přitom není jediným problémem. České trestní právo totiž spočívá na formálním pojetí trestného činu, kdy je za trestný považován každý čin, který vykazuje pojmové znaky činu trestného.[355] Tato definice je doplněna materiálním korektivem v § 12 odst. 2 TZ, který zajišťuje subsidiaritu trestní represe. Trestní odpovědnost lze uplatňovat pouze v případech společensky škodlivých, kdy nepostačuje uplatnění odpovědnosti podle jiného právního předpisu. Konstatovat nicméně nedostatečnou společenskou škodlivost je možné pouze výjimečně v případech,

351 K pojmu obecně Kesan, J. P., Hayes, C. M. Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace. *Harvard Journal of Law And Technology*, roč. 25, č. 2, s. 431.

352 Např. taxonomie sestavená v rámci semináře Leibnizovy nadace, dostupná z http://drops.dagstuhl.de/opus/volltexte/2014/4442/pdf/dagrep_v003_i011_p193_s13482.pdf.

353 Viz Polčák, 2015c, op. cit., s. 142-143.

354 Tamtéž.

355 Těmi jsou, kumulativně, protiprávnost, naplnění znaků skutkové podstaty trestného činu a obecné znaky pachatele.

v nichž není vhodné trestněprávní represi uplatňovat. Jestli tomu tak bude ve chvíli aktivního protiopatření, nelze v tuto chvíli jednoznačně říci. Získávání údajů o útočníkovi totiž v rámci některých aktivních protiopatření může spadat pod rozsah kybernetické kriminality.

§ 230 TZ, které bude na tuto situaci zřejmě dopadat, totiž bude zahrnovat, minimálně tedy z hlediska formálních znaků, i akce dohledového centra. Toto ustanovení v zásadě obsahuje dvě skutkové podstaty – první v odst. 1 představuje ochranu důvěrnosti počítačových dat a počítačového systému nebo jejich částí. Ochrana zde směřuje proti ohrožení důvěrnosti.[356] Ochrana integrity a dostupnosti dat je až sekundární. Aby mohlo být jednání kvalifikováno touto skutkovou podstatou, musí být splněny především dvě podmínky – musí být překonáno bezpečnostní opatření a současně musí být takto získaný přístup k počítačovému systému neoprávněný. Získání přístupu zde představuje takové jednání, které umožní pachateli volnou dispozici s počítačovým systémem nebo nosičem informací nebo využití jeho informačního obsahu.[357] Oprávněnost přístupu k počítačovému systému bude nutné posuzovat ad hoc, nicméně lze předpokládat, že ze strany CERT týmu se o oprávněný přístup jednat nebude – jedná se totiž o přístup, který tvůrce systému očividně nezamýšlel ostatním uživatelům umožnit. Druhá skutková podstata v rámci § 230 odst. 2 TZ pak primárně chrání integritu a dostupnost počítačových dat a systémů – jedná se tak o prostředek ochrany před neoprávněnými zásahy, které mohou mít vliv na existenci, kvalitu a správnost dat a chrání před neoprávněným užíváním uložených dat. Znakem zde není překonání bezpečnostního opatření nebo neoprávněnost přístupu k systému. K případnému získání důkazů ze systému útočníka totiž bude nutné využít některých chyb nebo obecně přinutit systém, aby se choval nestandardně. Formální znaky trestného činu tak mohou být naplněny.

Dle našeho názoru v situacích, kdy bude provedeno aktivní protiopatření směřující pouze k získání údajů, které budou použitelné pro trestní řízení, pojetí trestního práva jako ultima ratio zabrání nástupu trestněprávní odpovědnosti. Nebude vhodné ani účelné trestněprávní represi uplatňovat.

356 Triáda CIA – Srov. Graham, J., Howard, R., Olson, R. (eds.) *Cyber Security Essentials*. Boca Raton: CRC Press, 2011.

357 Srov. Šámal, 2012, op. cit., s. 2308.

Takové jednání totiž není možné považovat za společensky škodlivé a tím by tyto důkazy neměly být prohlášeny za nepřípustné, a to zejména ve chvíli, kdy orgány činné v trestním řízení nemají často vlastní kapacitu ke sběru důkazů tímto způsobem. Za zásadní argument totiž považujeme konstatování, že nelze rezignovat na úlohu orgánů činných v trestním řízení v oblasti kyberkriminality.

IX.2.3 Uchování důkazního prostředku

Co se týká uchování důkazního prostředku pro pozdější použití v rámci trestního řízení, vzhledem k chybějícím prověřeným standardům nakládání s elektronickými důkazy se otevírá značná možnost pro účelové namítání manipulace s důkazy. Než dojde k ustavení standardů, kterými se oblast může řídit, je nutné využít postupy, které jsou nám známy z jiné oblasti získávání důkazů od soukromých subjektů a jejich uchovávání. Zejména vyhláška č. 357/2012 o uchovávání, předávání a likvidaci provozních a lokalizačních údajů poskytuje nástroje, kterými je možné spolehlivosti dosáhnout, a analogické použití principů v ní zakotvených tak lze jen doporučit.

Autentičnost by měla být prokazována uznávaným elektronickým podpisem, elektronickou značkou nebo v budoucnosti elektronickou pečetí. Integrita dat by pak měla být zajištěna kontrolním součtem tak, aby s ním již nebylo možné žádným způsobem manipulovat.[358] Dá se navíc předpokládat, že soukromé subjekty nebo jejich specializovaná pracoviště budou disponovat nástroji umožňujícími sběr elektronických důkazů, bezpečné uložení a nezměnitelnost, které budou sofistikovanější, než budou mít k dispozici orgány činné v trestním řízení. Prokázat existující standardizaci a technická zabezpečení důkazního prostředku soudci se může ukázat jako problematické, ale nelze zde než apelovat na nutnost pragmatického přístupu a odmítání případných účelových argumentací obhajoby.

358 V rámci řešení bezpečnostního incidentu se tak dá předpokládat dodržení standardního postupu, tedy vyřešení incidentu a pro případ potřeby zajištění výstupu z forenzní analýzy i původních data ve formě otisku opatřeného kontrolním součtem tak, aby s ním nebylo možné manipulovat.

IX.3 Forenzní analýza

Forenzní analýza důkazních prostředků sebraných dohledovými centry kybernetické bezpečnosti bude z velké části přímo na poskytovateli těchto údajů, tedy na samotném dohledovém centru kybernetické bezpečnosti bez ohledu na jeho povahu. Vzhledem ke způsobům, jakým budou údaje sbírány[359], je jejich použití v této podobě v podstatě nemožné. Jedním z hlavních cílů dohledových pracovišť je vytváření informací, na základě kterých je možné přijímat konkrétní opatření. Strukturaci dat (tedy forenzní analýzu) bude tedy dohledové pracoviště pro svoji činnost vytvářet každopádně a v případě jejich náležité dokumentace a za použití některého z existujících standardů zřejmě nebude problém výsledek této analýzy přijmout za důkaz.[360]

IX.4 Provedení důkazu

Důkazem, který je v tuto chvíli možno provést by měla být zpráva o údajích zajištěných v rámci řešení incidentu. Opět je možné opřít se o podobné postupy, které jsou známé z oblasti uchovávání provozních a lokalizačních údajů. Zřejmě největším problémem je bezprostřednost důkazního prostředku.

V rámci informačního toku mezi subjektem povinným dle ZKB a OČTŘ tak bude žádoucí opatřit důkaz přímo od původního subjektu, a to bez ohledu na možnost jeho opatření v důsledku splnění povinnosti vůči vládnímu CERTu.[361] Provádění důkazu opatřeného od vládního CERTu může vést k posouzení tohoto důkazu pouze jako odvozeného, což bude dále umenšovat již tak nepřímou identifikační povahu IP adresy, která bude zřejmě nejčastěji předávaným údajem. Důkaz opatřený od vládního CERTu tak nemusí být považován za důkaz z pramene co nejbližšího zjišťované skutečnosti. Opět se zde otevírá možnost k judikatorní interpretaci, ale také

359 Např. NetFlow.

360 Jedná se tedy o přechod mezi low-level informacemi v podobě převážně strojově generovaných dat a detekčními indikátory – za detekční identifikátory je možné považovat IP adresu „útočícího" stroje atp. ENISA, *Actionable Information for Security Incident Response*. Dostupné z: http://www.enisa.europa.eu/activities/cert/support/actionable-information/actionable-information-for-security, s. 5-8.

361 Srov. rozdělení důkazů v kapitole II.6.

i k účelovým námitkám obhajoby. Orgány činné v trestním řízení by tak měly v případě možnosti zajistit důkazní prostředek přímo u subjektu, který incident hlásil, a tím dosáhnout jeho provedení jako důkazu bezprostředního.

IX.5 Hodnocení důkazu

Vzhledem k povaze získaných údajů bude zřejmě nejproblematičtější záležitostí použití získané IP adresy – stejně jako v případě uchovávání provozních a lokalizačních údajů se totiž jedná o nepřímý důkaz, a je navíc nezbytně nutné rozlišovat mezi statickou a dynamickou IP adresou. V případě získání IP adresy přístupového bodu (nebo MAC adresy stroje) je tak možné přes poskytovatele konektivity pátrat po daném přípojném místě. Jedná se ale o nepřímý důkaz a navíc o důkaz, který v tomto případě pouze uvádí do pohybu další postupy orgánů činných v trestním řízení. Opět se tedy jedná o metadata, na základě kterých je nutné činit konkrétní další procesní úkony ze strany orgánů činných v trestním řízení, které budou směřovat k zajištění dalších důkazů a zejména k zajištění kompletního obrazu spáchaného činu a kompletního důkazního řetězce, který umožní použití nepřímých důkazů tak, aby bylo možné dosáhnout odsouzení případného pachatele.[362]

IX.6 Náměty de lege ferenda

Zcela jistě je nezbytně nutné postupně dojít k vyjasnění oprávnění dohledových center kybernetické bezpečnosti ve všech podobách – jak součástí NBÚ v podobě Národního centra kybernetické bezpečnosti (resp. pracoviště GovCERT.cz), tak soukromoprávní platformy předpokládané zákonem a provozované ve veřejném zájmu v podobě CSIRT.CZ i dalších soukromoprávních platforem, vykonávajících určitou činnost na síti na základě pracovněprávního vztahu jednotlivých členů těchto týmů nebo na základě smluvního vztahu s externími subjekty. V úvahu připadá vyjasnění standardní podoby některých postupů a automatizování spolupráce s OČTŘ a aprobace existujících standardů spolupráce mezi dohledovými pracovišti. Za druhou možnost vedoucí k vyjasnění těchto kontur, zejména z pohledu

362 Srov. výklad věnovaný nepřímým důkazům v kapitolách I.7, III.3.3, IV.4, IV.5 a VI.5.

pragmatického, bude zřejmě možné považovat i chování subjektů samotných – dohledová centra tak mohou přímo svým disciplinovaným chováním přispět k tomu, že na ně bude orgány činnými v trestním řízení nahlíženo jako na vítanou asistenci a nikoli jako na nedisciplinované „kovboje" zneužívající specifické postavení v síti. Neexistence ustálené interpretační praxe v tuto chvíli způsobuje sice nejasnost, na druhou stranu ale umožňuje realizaci ambicí soukromých subjektů – způsob, který zvolí pro určité jednání, se může zpětně projevit v právní kvalifikaci jejich vlastního jednání. Dá se tedy říci, že v současné době nevyjasněných možností mají jednotlivá dohledová centra (nicméně stále s důrazem zejména na dohledová centra, jejichž existenci přímo předpokládá ZoKB) možnost stanovit normu pro odlišení jednání fakticky běžných od takových, která za běžná považovat nelze. Příkaz k eliminaci excesů typu svévole nicméně zůstává v platnosti a pragmatickým přístupem jej nelze vyloučit.

IX.7 Shrnutí kapitoly

Tato kapitola obsahovala rozbor problematiky důkazů daty z dohledových systémů kybernetické bezpečnosti. S rostoucí pozorností, která se kybernetické bezpečnosti dostává, bude dle našeho názoru růst i význam tohoto specifického důkazního prostředku. V současné době je možné konstatovat, že ZKB usnadnil povinným subjektům situaci při zpracovávání údajů, které jsou de lege lata považované za osobní (např. IP adresy). ZKB nicméně správně nevymezil, že dohledové centrum mohou provozovat pouze subjekty dle tohoto zákona povinné, a tak se postupy orgánů činných v trestním řízení musejí odvíjet dle režimu, ve kterém subjekty držící údaje podnikají. Pro subjekty podnikající podle ZoEK tak bude nutné použít pro získání údajů postup dle § 88a TŘ, pro subjekty vykonávající svoji podnikatelskou činnost mimo působnost tohoto zákona pak dle § 8 odst. 1 TŘ. Činnost dohledových center, ať už předpokládaných ZKB či nikoli, každým pádem představuje oblast, která se bude doktrinálně i judikatorně v našem prostředí teprve ustalovat. Instituty umožňující orgánům činným v trestním řízení pracovat s daty získanými dohledovými centry nicméně existují a není jediný důvod, proč je nepoužívat.

Summary

It is not entirely common to speak specifically in Continental Europe about the law of evidence. Issues related to discovery, forensic analysis or presentation of evidence at courts are normally tackled here not separately but rather as integral component of procedural disciplines, e.g. civil or criminal procedure. In that respect, the authors of this book decided for a bit unusual step by trying to specifically discuss only legal problems arising of the need to use digital evidence in common forms of criminal procedure.

This book, however, is not based on commonly accepted cliché that digital evidence represents novel and highly specialized topic. Websites, e-mails, wiretapped calls or traffic data are for considerable time being used as standard evidence not just in specific cases of cybercrime but in almost any kind of criminal investigation and/or court proceedings. In that sense, the aim of the book is not just to creatively elaborate on specific high-tech forms of digital evidence (e.g. on data gathered by computer security incident response teams) but also to simply summarize recent court practice in the use of aforementioned common forms of digital evidence in the Czech criminal procedure..

General part of the book consists of the theory of evidence (still not significantly present in the Czech law), explanation of statutory grounds of law of evidence in criminal procedure and general discussion of the use of data as evidence in criminal procedure. Special parts of the book are dedicated to procedural issues in discovery, forensic analysis and use of different types of digital evidence, whereas particular forms of digital evidence were chosen namely upon the level of their recent practical use at criminal courts.

The guiding principle of Czech law of evidence is referred to as free consideration of evidence. It means there are only very few rigorous statutory rules regulating discovery of evidence, its admissibility or the way in which it is to be considered by the court. Instead particular rules, courts are given quite a discretion when assessing the evidence and the only limitation is then general logics and empirical rationality. This system provides for significantly less certainty when it comes to use of evidence at courts. On the other

hand, it provides for flexibility for cases when new forms of evidence are to be used, including those arising from the use of information and communication technologies.

This book, however, is not aimed at comparing the free consideration of evidence to rules of evidence or other standards found in different legal cultures. It rather tries to provide for empirically backed academic understanding of standard ways in which different forms of digital evidence is or should be used at Czech courts. Consequently, the main aim of the book is to provide for greater certainty as to the use of digital evidence in a situation when particular statutory provisions are either entirely missing or not functioning in contemporary criminal cases.

Out of specific forms of digital evidence, we decided to particularly discuss e-mails, personal profiles on social networks, websites, traffic data (namely those compulsorily processed upon data retention obligations), wiretapped calls and other transmissions, data discovered from mobile communication devices and data acquired by different kinds of computer security incident response teams.

Each of special chapters tries to keep the same structure, i.e. legal issues in discovery of evidence, forensic analysis, use of evidence in preparatory and court criminal proceedings and the consideration of evidence by the court. Common issues discussed across different topics include namely information privacy and related questions of proportionality of fundamental rights and subsequent admissibility of evidence. Specific issues depend mostly on technical nature of different types of digital evidence and include questions arising of nonstandard forms of gathering of digital evidence (e.g. using exploits or different hacking techniques), its trusted storage or communication of evidence including international data transfers among different bodies of procedural criminal law.

The authors of this book include Czech and Slovak academics, police investigators, a Supreme Court justice and a member of Supreme Prosecution service. This mixture is aimed at providing for balanced view combining doctrinal or academic understanding of problematic issues with practical experience and pragmatic approach needed for everyday use of respective conclusions.

Seznam použitých zkratek

CERT	Computer Energency Response Team
CIRC	Computer Incident Response Capacity
CSIRT	Computer Security Incident Response Team
EÚLP	Evropská úmluva o lidských právech
LZPS	Listina základních práv a svobod
NBÚ	Národní bezpečnostní úřad
OČTŘ	orgány činné v trestním řízení
PolČR	zákon č. 273/2008 Sb., o policii České republiky, ve znění zákona č. 64/2014 Sb.
SDEU	Soudní dvůr Evropské Unie
TŘ	zákon č. 141/1961 Sb., trestní řád, ve znění zákona č. 86/2015 Sb.
TZ	zákon č. 40/2009 Sb., trestní zákoník, ve znění zákona č. 165/2015 Sb.
ÚZČ	Útvar zvláštních činností služby kriminální policie a vyšetřování
VKB	vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti
WP29	Article 29 Working Party
ZEK	zákon č. 127/2005, o elektronických komunikacích, ve znění zákona č. 250/2014 Sb.
ZKB	zákon č. 181/2014 Sb., o kybernetické bezpečnosti
ZMJS	zákon č. 104/2013 Sb., o mezi národní justiční spolupráci ve věcech trestních, ve znění zákona č. 86/2015 Sb.
ZnalZ	zákon č. 36/1967 Sb., o znalcích a tlumočnicích, ve znění zákona č. 444/2011 Sb.
ZOOÚ	zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění zákona č. 250/2014 Sb.
ZSIS	zákon č. 480/2004, o některých službách informační společnosti, ve znění zákona č. 89/2012 Sb.
ZSM	zákon č. 218/2003 Sb., o soudnictví ve věcech mládeže, ve znění zákona č. 86/2015 Sb.

Literatura a další použité zdroje

Monografie

Anderson, T., Schum, D., Twinning, W. *Analysis of Evidence*. Cambridge: Cambridge University Press, 2005.

Boguszak, J., Čapek, J., Gerloch, A. *Teorie práva*. Praha: Eurolex Bohemia, 2001.

Casey, E. et al. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Third Edition*. Academic Press, 2011.

Císařová, D., Fenyk, J., Gřivna, T. et al. *Trestní právo procesní. 5. vyd.* Praha: ASPI, 2008.

Čapek, J. *Evropská úmluva o ochraně lidských práv a základních svobod*. Praha: Linde Praha, 2010.

Del Mar, M., Twining, W. (eds.) *Legal Fictions in Theory and Practice*. Heidelberg: Springer International Publishing, 2015.

Engliš, K. *Malá logika*. Praha: Melantrich, 1947.

Fryšták, M. *Dokazování v přípravném řízení*. Brno: Masarykova univerzita, 2014.

Glenn, P. *Legal Traditions of the World*. New York: Oxford University Press, 2004.

Graham, J., Howard, R., Olson, R. (eds.) *Cyber Security Essentials*. Boca Raton: CRC Press, 2011.

Hobbes, T. *Leviathan, Or, the Matter, Forme, & Power of a Common-Wealth, Ecclesiastical and Civill*. Project Gutenberg, 2009.

Holländer, P. *Filosofie práva*. Plzeň: Aleš Čeněk, 2006.

Hunter, R. *World Without Secrets*. New York: John Wiley and Sons, 2002.

Jelínek, J. *Trestní právo procesní. 1. vyd. podle novelizované právní úpravy účinné od 1. 1. 2010*. Praha: Leges, 2010.

Jelínek, J., Uhlířová, M. *Obhájce v trestním řízení. 1. vydání*. Praha: Leges, 2011.

Kant, I. *Critique of Pure Reason. Přel. Meiklejohn, J. M. D.* Project Gutenberg, 2003.

Kinney, Steven L. *Trusted platform module basics using TPM in embedded systems*. Oxford: Newnes, 2006.

Kmec, J., Kosař, D., Kratochvíl, J., Bobek, M. *Evropská úmluva o lidských právech. Komentář. 1. vydání.* Praha: C. H. Beck, 2012.

Knapp, V. *O možnosti použití kybernetických metod v právu.* Praha: Nakladatelství Československé akademie věd, 1963.

Lévy, P. *Becoming Virtual – Reality in the Digital Age.* New York: Plenum Trade, 2002.

Macur, J. *Důkazní břemeno v civilním soudním řízení.* Brno: Masarykova univerzita, 1995.

Macur, J. *Kompenzace informačního deficitu procesní strany v civilním soudním sporu.* Brno: Masarykova univerzita, 2000.

Macur, J. *Zásada projednací v civilním soudním řízení.* Brno: Masarykova univerzita, 1997.

Mason, S. *Electronic evidence.* London: LexisNexis. 2010.

Mason, S. *International electronic evidence.* London: British Institute of International and Comparative Law, 2008.

Musil, J., Kratochvíl, V., Šámal, P. *Kurs trestního práva: trestní právo procesní. 3. přeprac. a dopl. vyd.* Praha: C. H. Beck, 2007.

Myška, M. *Právní aspekty uchovávání provozních a lokalizačních údajů.* Brno: Masarykova univerzita, 2013.

Newman, R. *Computer Forensics: Evidence Collection and Management*. Auerbach publications, 2007.

Oakshott, M. *On Human Conduct*. Oxford: Oxford University Press, 1975.

Paliwala, A. (ed.) *History of Legal Informatics*. Zaragoza: Prensas de Universitarias de Zaragoza, 2010.

Písek, S. *HTML: tvorba jednoduchých internetových stránek. 2., aktualiz. a dopl. vyd.* Praha: Grada, 2006.

Polčák, R. *Internet a proměny práva*. Praha: Auditorium, 2012.

Quick, D., Martini, B., Choo, R. *Cloud Storage Forensics*. Elsevier Inc., 2014.

Repík, B. *Evropská úmluva o lidských právech a trestní právo.* Praha: Nakladatelství Orac, 2002.

Solove, D. *The Digital Person*. New York: New York University Press, 2004.

Šámal, P. a kol. *Trestní řád I. § 1 až 156. Komentář. 7. vydání.* Praha: C. H. Beck, 2013.

Šámal, P. a kol. *Trestní řád III. § 215 až 471. Komentář. 7. vydání.* Praha: C. H. Beck, 2013.

Šámal, P. *Trestní zákoník II. § 140 až 421. Komentář. 2. vydání* Praha: C. H. Beck, 2012.

Šámal, P. *Základní zásady trestního řízení v demokratickém systému*. Praha: SEVT, 1992.

Šámal, P. *Základy trestního řízení v demokratickém systému*, 2. vyd. Praha: Codex Bohemia, 1999 .

Vidrna, J., Koudelka, Z. *Zaměstnanci v objektivu kamer: právní aspekty monitoringu zaměstnanců.* Praha: C. H. Beck, 2013.

Višinskij, J. A. *Theorie soudních důkazů v sovětském právu*. Praha: Mír, 1950.

Weinberger, O. *Alternative Action Theory*. Dordrecht: Springer Science+Business Media, 1998.

Wiener, N. *Cybernetics: On the Control and Communication in the Animal and the Machine*. Cambridge: MIT Press, 1961.

Winkler, J.R., Meine B. (eds.) *Securing the Cloud Cloud Computer Security Techniques and Tactics*. Burlington: Elsevier Science, 2011.

Wood, A. *Kantian Ethics*. Cambridge: Cambridge University Press, 2008.

Young, R. *How computers work: processor and main memory. 2nd ed.* S.l.: Roger Young, 2009.

Odborné články

Ariens, M. S. The Law of Evidence and the Idea of Progress. *Loyola of Los Angeles Law Review*, 1992, roč. 25, č. 3.

Behr, T., Kohout, J. Elektronická pošta a její záznam pro trestní řízení. *Trestněprávní revue*, 2011, č. 4.

Donelly, C. R. The Law of Evidence: Privacy and Disclosure. *Louisiana Law Review*, 1954, roč. 14, č. 2.

Eckersley, P. How unique is your web browser? In: Attalah, M. J., Hopper, N. J. (eds.). *Privacy Enhancing Technologies.* Springer, 2010.

Garrett, C. K. Admissibility of Electronic Information. *The Journal of Kansas Bar Association*, 2002, roč. 71.

Harašta, J., Míšek, J. IP adresy v kybernetické bezpečnosti. *Revue pro právo a technologie*, 2015, č. 12.

Harašta, J., Myška, M. Budoucnost data retention. *Trestněprávní revue*, 2015, roč. 5, č. 10.

Kesan, J. P., Hayes, C. M. Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace. *Harvard Journal of Law And Technology*, roč. 25, č. 2.

Komárek, J. Soudní dvůr EU – duben 2014. *Soudní rozhledy*, 2014, č. 6.

Krongold, H. L. A Comparative Perspective on the Exclusion of Relevant Evidence: Common Law and Civil Law Jurisdictions. *Dalhousie Journal of Legal Studies*, 2003, roč. 12.

Lenhoff, A. The Law of Evidence – A Comparative Study Based Essentially on Austrian and New York Law. *The American Journal of Comparative Law,* 1954, roč. 3, č. 3.

Marek, T. Autonomie vůle a soukromí na Facebooku. *Právní rozhledy*, 2015, č. 6.

Musil, J. Hodnocení znaleckého posudku. *Kriminalistika,* 2010, č. 3.

Nissan, E. Can You Measure Circumstantial Evidence? The Background of Probative Formalisms for Law. *Information and Communications Technology Law*, 2001, roč. 10, č. 2.

Novotná, J. K některým otázkám dokazování odposlechem a záznamem telekomunikačního provozu. *Trestněprávní revue*, 2003, č. 10.

Polčák, R. Getting European data protection off the ground. *International Data Privacy Law*, 2014, roč. 4, č. 4.

Polčák, R., Říha, Z., Malinka K. Právní aspekty interních směrnic – část I. *Data Security Management*, 2015, roč. 19, č. 2.

Polčák, R., Říha, Z., Malinka K. Právní aspekty interních instrukcí – část II. *Data Security Management*, 2015, roč. 19, č. 3.

Polčák, R. Kybernetická bezpečnost jako aktuální fenomén českého práva. *Revue pro právo a technologie,* 2015, č. 11.

Rubinstein, I. Regulating Privacy by Design. *Berkeley Technology Law Journal*, 2012, roč. 26, č. 3.

Selinšek, L. Některé právní aspekty forenzní analýzy digitálních dat. *Acta Universitatis Carolinae*, 2008, č. 4.

Shannon, C. E. A Mathematical Theory of Communication. *The Bell Systems Technical Journal*, 1948, roč. 27, č. 3.

Shapira, R. Economic Analysis of the Law of Evidence: A Caveat. *Cardozo Law Review*, 1998, roč. 19, č. 5.

Schwartz, P. M. The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures. *Harvard Law Review*, 2013, roč. 126, č. 7.

Stupka, Václav. Uchovávání provozních a lokalizačních údajů pro účely vyúčtování poskytnutých služeb elektronických komunikací. *Revue pro právo a technologie,* 2014, roč. 4, č. 8.

Thayer, E. R. Observations on the Law of Evidence. *Michigan Law Review*. 1915, roč. 13, č. 5.

Walton, J. Notes on the Law of Evidence. *Medico-Legal Journal*, 1904, roč. 2, č. 1.

Weinberger, O. Logické a metodologické základy důkazu v oboru práva. *Stát a právo*, 1967, č. 13.

Judikatura

Publikovaná rozhodnutí českých soudů

Nález Ústavního soudu sp zn. IV. ÚS 802/02, N 58/33 SbNU 89, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. I. ÚS 2343/08, N 67/52 SbNU 663, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. I. ÚS 3094/08, N 103/53 SbNU 293, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. I. ÚS 32/95, N 40/5 SbNU 331, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. I. ÚS 402/05, N 206/39 SbNU 185, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. I. ÚS 425/97, N 42/13 SbNU 305, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. I. ÚS 431/04, N 31/36 SbNU 347, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. I. ÚS 455/05, N 210/39 SbNU 239, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. I. ÚS 459/2000, N 89/27 SbNU 51, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. I. ÚS 566/03, N 104/34 SbNU 99, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. I. ÚS 660/03, N 24/32 SbNU 219, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. I. ÚS 671/05, N 41/40 SbNU 341, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. I. ÚS 733/01, N 26/32 SbNU 239, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. I. ÚS 864/11, N 116/61 SbNU 695, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. I. ÚS 910/07, N 156/50 SbNU 389, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. II. ÚS 118/01, N 13/29 SbNU 101, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. II. ÚS 2369/08, N 244/59 SbNU 489, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. II. ÚS 255/05, N 128/37 SbNU 623, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. II. ÚS 2806/08, N 15/56 SbNU 143, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. II. ÚS 418/99, N 116/19 SbNU 113, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. II. ÚS 441/99, N 48/17 SbNU 337, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. II. ÚS 502/2000, N 11/21 SbNU 83, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. II. ÚS 552/05, N 12/40 SbNU 103, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. II. ÚS 615/06, N 88/45 SbNU 291, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. II. ÚS 889/10, N 237/59 SbNU 405, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. III. ÚS 1076/08, N 144/50 SbNU 269, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. III. ÚS 1104/08, N 65/52 SbNU 635, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. III. ÚS 181/2000, N 175/20 SbNU 241, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. III. ÚS 183/03, N 175/38 SbNU 399, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. III. ÚS 224/04, N 116/34 SbNU 213, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. III. ÚS 258/99, N 148/16 SbNU 99, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. III. ÚS 26/03, N 22/32 SbNU 201, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. III. ÚS 26/94, N 32/1 SbNU 241, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. III. ÚS 332/09, N 60/56 SbNU 643, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. III. ÚS 398/97, N 64/11 SbNU 125, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. III. ÚS 451/04, N 68/40 SbNU 677, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. III. ÚS 463/2000, N 181/20 SbNU 267, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. III. ÚS 464/99, N 109/19 SbNU 63, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. III. ÚS 51/96, N 57/8 SbNU 69, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. III. ÚS 528/06, N 159/47 SbNU 75, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. III. ÚS 532/01, N 10/25 SbNU 69, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. III. ÚS 617/2000, N 143/24 SbNU 27, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. III. ÚS 628/2000, N 67/22 SbNU 87, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. III. ÚS 644/05, N 71/40 SbNU 697, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. III. ÚS 722/09, N 2/56 SbNU 11, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. III. ÚS 95/97, N 76/8 SbNU 231, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. IV. ÚS 1235/09, N 144/58 SbNU 207, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. IV. ÚS 1526/08, N 188/51 SbNU 301, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. IV. ÚS 335/05, N 116/41 SbNU 453, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. IV. ÚS 37/03, N 81/33 SbNU 285, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. IV. ÚS 536/2000, N 29/21 SbNU 251, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. IV. ÚS 570/03, N 91/33 SbNU 377, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. IV. ÚS 767/05, N 81/41 SbNU 67, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. IV. ÚS 802/02, N 58/33 SbNU 89, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. Pl. ÚS 14/94, N 14/3 SbNU 73 (55/1995 Sb.), dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. Pl. ÚS 15/98, N 48/13 SbNU 341, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. Pl. ÚS 24/11, N 217/63 SbNU 483 (43/2012 Sb.), dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. Pl. ÚS 29/2000, N 32/21 SbNU 285, dostupné z http://nalus.usoud.cz.

Rozsudek Krajského soudu v Plzni sp. zn. 4 To 167/63, č. 14/1964 Sb. tr. rozh., dostupné z http://beck-online.cz.

Rozsudek Nejvyššího soudu sp. zn. 1 Tz 30/53, č. 56/1953 Sb. tr. rozh., dostupné z http://beck-online.cz.

Rozsudek Nejvyššího soudu sp. zn. 10 Tz 34/65, č. 46/1965 Sb. tr. rozh., dostupné z http://beck-online.cz.

Rozsudek Nejvyššího soudu sp. zn. 11 Tz 51/65, č. 7/1966 Sb. tr. rozh., dostupné z http://beck-online.cz.

Rozsudek Nejvyššího soudu sp. zn. 2 Tzf 3/88, č. 49/1989 Sb. tr. rozh., dostupné z http://beck-online.cz.

Rozsudek Nejvyššího soudu sp. zn. 5 Tz 63/2001, č. 4/2002 Sb. tr. rozh., dostupné z http://www.nsoud.cz.

Rozsudek Nejvyššího soudu sp. zn. 7 Tz 11/68, č. 38/1968 Sb. tr. rozh., dostupné z http://beck-online.cz.

Rozsudek Nejvyššího soudu sp. zn. 7 Tz 26/98, č. 28/1999 Sb. tr. rozh., dostupné z http://beck-online.cz.

Rozsudek Nejvyššího soudu sp. zn. 7 Tz 84/69, č. 38/1970 Sb. tr. rozh., dostupné z http://beck-online.cz.

Rozsudok Najvyššieho súdu sp. zn. 4 Tz 98/76, č. 11/1977 Sb. tr. rozh., dostupné z http://beck-online.cz.

Rozsudok Najvyššieho súdu sp. zn. 4 Tz 105/76, č. 28/1977 Sb. tr. rozh., dostupné z http://beck-online.cz.

Rozsudek Nejvyššího soudu sp. zn. Tsf 1/72, č. 40/1972 Sb. tr. rozh., dostupné z http://beck-online.cz.

Rozsudek Nejvyššího správního soudu sp. zn. 9 As 34/2008, č. 1844/2009 Sb. rozh. NSS, dostupné z http://nssoud.cz.

Rozsudek Vrchního soudu v Praze sp. zn. 2 To 73/2000, č. 55/2001 Sb. tr. rozh., dostupné z http://beck-online.cz.

Stanovisko pléna Ústavního soudu sp. zn. Pl. ÚS-st. 30/10, ST 30/59 SbNU 595 (č. 439/2010 Sb.), dostupné z http://nalus.usoud.cz.

Stanovisko trestného kolégia Najvyššieho súdu sp. zn. Tpj 20/89, č. 3/1990 Sb. tr. rozh., dostupné z http://beck-online.cz.

Stanovisko trestního kolegia Nejvyššího soudu sp. zn. Tpjn 300/2012, č. 20/2013 Sb. tr. rozh., dostupné z http://www.nsoud.cz.

Stanovisko trestního kolegia Nejvyššího soudu sp. zn. Tpjn 306/2014, č. 35/2015 Sb. tr. rozh., dostupné z http://www.nsoud.cz.

Usnesení Krajského soudu v Českých Budějovicích sp. zn. 4 To 475/94, č. 3/1996 Sb. tr. rozh., dostupné z http://beck-online.cz.

Usnesení Krajského soudu v Českých Budějovicích sp. zn. 4 To 354/94, č. 33/1995 Sb. tr. rozh., dostupné z http://beck-online.cz.

Usnesení Nejvyššího soudu sp. zn. 3 Tdo 593/2009, č. 22/2010 Sb. tr. rozh., dostupné z http://www.nsoud.cz.

Usnesení Nejvyššího soudu sp. zn. 3 Tz 62/91, č. 10/1993 Sb. tr. rozh., dostupné z http://beck-online.cz.

Usnesení Nejvyššího soudu sp. zn. 5 Tdo 459/2007, č. 7/2008 Sb. tr. rozh., dostupné z http://www.nsoud.cz.

Usnesení Nejvyššího soudu sp. zn. 7 Tdo 638/2010, č. 56/2011 Sb. tr. rozh., dostupné z http://www.nsoud.cz.

Usnesení Nejvyššího soudu sp. zn. 8 Tdo 921/2009, č. 3/2011 Sb. tr. rozh., dostupné z http://www.nsoud.cz.

Usnesení Ústavního soudu sp. zn. I. ÚS 152/05, U 18/38 SbNU 541, dostupné z http://nalus.usoud.cz.

Usnesení Ústavního soudu sp. zn. I. ÚS 484/97, U 7/10 SbNU 361, dostupné z http://nalus.usoud.cz.

Usnesení Ústavního soudu sp. zn. III. ÚS 3812/2012, U 10/71 SbNU 573, dostupné z http://nalus.usoud.cz.

Usnesení Ústavního soudu sp. zn. IV. ÚS 154/02, U 37/28 SbNU 447, dostupné z http://nalus.usoud.cz.

Usnesení Ústavního soudu sp. zn. IV. ÚS 2/02, U 11/25 SbNU 385, dostupné z http://nalus.usoud.cz.

Usnesení Ústavního soudu sp. zn. IV. ÚS 2425/09, U 4/56 SbNU 841, dostupné z http://nalus.usoud.cz.

Usnesení Ústavního soudu sp. zn. Pl. ÚS 41/2000, U 7/21 SbNU 493, dostupné z http://nalus.usoud.cz.

Usnesení Ústavního soudu sp. zn. ÚS 191/05 N 161/42 SbNU 327, dostupné z http://nalus.usoud.cz.

Usnesení Vrchního soudu v Praze sp. zn. 4 To 3/01, č. 56/2001 Sb. tr. rozh., dostupné z http://beck-online.cz.

Usnesení Vrchního soudu v Olomouci sp. zn. 5 To 187/2002, č. 11/2005 Sb. tr. rozh., dostupné z http://beck-online.cz.

Usnesení Vrchního soudu v Praze sp. zn. 11 To 46/94, č. 45/1994 Sb. tr. rozh., dostupné z http://beck-online.cz.

Usnesení Vrchního soudu v Praze sp. zn. 2 To 144/03, č. 19/2004 Sb. tr. rozh., dostupné z http://beck-online.cz.

Rozhodnutí publikovaná mimo sbírky

Nález Ústavního soudu sp. zn. I. ÚS 4793/12, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. I. ÚS 173/13, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. I. ÚS 2726/14, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. III. ÚS 3844/13, dostupné z http://nalus.usoud.cz.

Nález Ústavního soudu sp. zn. Pl. ÚS 47/13, dostupné z http://nalus.usoud.cz.

Rozhodnutí Městského soudu v Praze sp. zn. 42 T 8/2013. Dostupné na: http://www.pecina.cz/files/Rozsudek_MS-P_30.4.2014.pdf.

Rozsudek Nejvyššího soudu sp. zn. 21 Cdo 2058/2012, dostupné z http://www.nsoud.cz.

Rozsudek Nejvyššího soudu sp. zn. 4 Tz 100/2006, dostupné z http://www.nsoud.cz.

Rozsudek Nejvyššího soudu sp. zn. 5 Tz 174/2001, dostupné z http://beck-online.cz.

Rozsudek Nejvyššího soudu sp. zn. 5 Tz 175/2001, dostupné z http://beck-online.cz.

Rozsudek Nejvyššího soudu sp. zn. 5 Tz 214/2001, dostupné z http://beck-online.cz.

Rozsudek Nejvyššího správního soudu č. j. 1 As 90/2008–189, dostupné z http://www.nssoud.cz.

Rozsudek Nejvyššího správního soudu č. j. 8 As 10/2006–48, dostupné z http://www.nssoud.cz.

Rozsudek Vrchního soudu v Praze sp. zn. 2 To 116/2009, dostupné z http://beck-online.cz.

Usnesení Krajského soudu v Hradci Králové sp. zn. 10 To 319/2008, dostupné z http://beck-online.cz.

Usnesení Nejvyššího soudu č. j. 3 Tcu 33/2014-26, dostupné z http://beck-online.cz.

Usnesení Nejvyššího soudu sp. zn. 11 Tdo 349/2009, dostupné z http://www.nsoud.cz.

Usnesení Nejvyššího soudu sp. zn. 3 Tdo 553/2006, dostupné z http://www.nsoud.cz.

Usnesení Nejvyššího soudu sp. zn. 3 Tdo 567/2013, dostupné z http://www.nsoud.cz.

Usnesení Nejvyššího soudu sp. zn. 4 Tdo 1482/2012, dostupné z http://www.nsoud.cz.

Usnesení Nejvyššího soudu sp. zn. 4 Tdo 815/2014, dostupné z http://www.nsoud.cz.

Usnesení Nejvyššího soudu sp. zn. 4 Tz 24/2013, dostupné z http://www.nsoud.cz.

Usnesení Nejvyššího soudu sp. zn. 5 Tdo 31/2010, dostupné z http://www.nsoud.cz.

Usnesení Nejvyššího soudu sp. zn. 7 Tz 9/2000, dostupné z http://beck-online.cz.

Usnesení Nejvyššího soudu sp. zn. 8 Tdo 1082/2011, dostupné z http://www.nsoud.cz.

Usnesení Nejvyššího soudu sp. zn. 8 Tdo 109/2014, dostupné z http://www.nsoud.cz.

Usnesení Nejvyššího soudu sp. zn. 8 Tdo 1189/2014, dostupné z http://www.nsoud.cz.

Usnesení Nejvyššího soudu sp. zn. 8 Tdo 908/2013, dostupné z http://www.nsoud.cz.

Usnesení Nevyššího soudu sp. zn. 5 Tdo 1136/2014, dostupné z http://www.nsoud.cz.

Usnesení Ústavního soudu sp. zn. I. ÚS 413/06, dostupné z http://nalus.usoud.cz.

Usnesení Ústavního soudu sp. zn. II. ÚS 143/06, dostupné z http://nalus.usoud.cz.

Usnesení Ústavního soudu sp. zn. III. ÚS 2797/12, dostupné z http://nalus.usoud.cz.

Usnesení Ústavního soudu sp. zn. IV. ÚS 3225/09, dostupné z http://nalus.usoud.cz.

Usnesení Vrchního soudu v Olomouci sp. zn. 5 To 42/2010, dostupné z http://kraken.slv.cz/VSOL5To42/2010.

Rozhodnutí SDEU a ESLP

Rozhodnutí ESLP ve věci Gäfgen v. Německo, stížnost č. 22978/05.

Rozhodnutí ESLP ve věci Kennedy v. Spojené království, stížnost č. 26839/05.

Rozhodnutí ESLP ve věci Uzun v. Německo, stížnost č. 35623/05.

Rozhodnutí ESLP ve věci Weber a Saravia v. Německo, stížnost č. 54934/00).

Rozhodnutí SDEU ve věci Google Spain, sp. zn. C-131/12.

Rozhodnutí SDEU ve věci Promusicae, sp. zn. C-275/06.

Rozsudek ESLP ve věci A. proti Francii, stížnost č. 14838/89.

Rozsudek SDEU ve věci Digital Rights Ireland a Seitlinger a další, sp. zn. C-293/12 a C-594/12.

Rozsudek SDEU ve věci SABAM, sp. zn. C-70/10.

Rozhodnutí zahraničních soudů

Kanada. Rozsudek Nejvyššího soudu Britské Kolumbie ze dne 24. 8. 1994 sp. zn. C872267 ve věci Prism Hospital Software Inc. v. The Hospital Records Institute. Dostupné z http://www.canlii.org/en/bc/bcsc/doc/1994/1994canlii1308/1994canlii1308.html.

Německo. Rozhodnutí Federálního ústavního soudu SRN ze dne 16. 6. 2009 sp. zn. 2 BvR 902/06. Dostupné z http://www.hrr-strafrecht.de/hrr/bverfg/06/2-bvr-902-06-1.php.

Slovensko. Rozhodnutí Ústavního soudu Slovenské republiky ze dne 25. 8. 2010 sp. zn. III. ÚS 68/2010. Dostupné z https://www.ustavnysud.sk/SearchRozhodnutiav01/rozhod.do?urlpage=dokument & id_spisu=355658.

Spojené státy. Rozhodnutí Nejvyššího soudu Spojených států amerických ze dne 25. 6. 2014 ve věci Riley v. California. Dostupné z http://www.scotusblog.com/case-files/cases/riley-v-california/.

Spojené státy. Rozsudek Odvolacího soudu 11. obvodu USA ze dne 15. 12. 2000 sp. zn. No. 98-6994 ve věci United States v. Siddiqui. Dostupné z http://caselaw.findlaw.com/us-11th-circuit/1493241.html.

Spojené státy. Rozsudek Trestního odvolacího soudu státu Alabama ze dne 21. 11. 2014 sp. zn. CR-13-1039 ve věci Robert N. Culp, Jr. v. State of Alabama. Dostupné z: http://law.justia.com/cases/alabama/court-of-appeals-criminal/2014/cr-13-1039.html.

Stanoviska

Opinion 4/2007, on the concept of personal data, Article 29 Data Protection Working Party. Dostupné z http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

Opinion 6/2014, on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, Article 29 Data Protection Working Party. Dostupné z http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

Pokyn obecné povahy Nejvyšší státní zástupkyně č. 8/2009, o trestním řízení. Dostupné z http://www.nsz.cz/images/stories/PDF/POP/trest/1_SL_902-205_2.pdf.

Stanovisko Úřadu pro ochranu osobních údajů č. 2/2009, ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště. Dostupné z https://www.uoou.cz/files/stanovisko_2009_2.pdf.

Výkladové stanovisko Nejvyššího státního zastupitelství č. 1/2015, ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek. Dostupné z http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2015/1_SL_760-2014.pdf.

Výkladové stanovisko Nejvyššího státního zastupitelství č. 4/2005, 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. Dostupné z http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2005/stanovisko%204-2005.pdf.

Výkladové stanovisko Nejvyššího státního zastupitelství č. 9/2001, k zajišťování počítačů a jiných nosičů informací při domovní prohlídce a prohlídce jiných prostor a pozemků. Dostupné z: http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2001/stanovisko%209-2001.pdf.

Výkladové stanovisko Nejvyššího státního zastupitelství č. 9/2004, ke sjednocení výkladu zákonů a jiných právních předpisů k postupu státních zástupců ohledně výkonu práva obhájce (advokáta) postupem podle § 89 odst. 2 věty druhé trestního řádu vyhledávat a předkládat důkazy nebo navrhovat provedení důkazů. Dostupné z: http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2004/stanovisko%209-2004.pdf.

ELEKTRONICKÉ DŮKAZY V TRESTNÍM ŘÍZENÍ

**doc. JUDr. Radim Polčák, Ph.D., JUDr. František Púry, Ph.D.,
JUDr. Jakub Harašta, Mgr. Tomáš Abelovský, Mgr. Tomáš Elbert,
Mgr. Petr Klement, JUDr. Matěj Myška, Ph.D.,
Alena Pejčochová, M. A., Mgr. Václav Stupka**

Vydala Masarykova univerzita v Brně roku 2015
Spisy Právnické fakulty MU č. 542 (řada teoretická, Edice Scientia)

Ediční rada: J. Kotásek (předseda), J. Bejček, J. Hurdík, V. Kalvodová,
V. Kratochvíl, P. Mrkývka, R. Polčák, N. Rozehnalová

Tisk: Point CZ, s.r.o., Milady Horákové 890/20, 602 00 Brno
1. vydání, 2015

ISBN 978-80-210-8073-7