UNIVERZITA KARLOVA

Právnická fakulta

Simona Krákorová

Dokazování elektronickými důkaznímі prostředky

Diplomová práce

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

Katedra trestního práva

Datum vypracování práce (uzavření rukopisu): 18. června 2019

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

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 151 895 znaků včetně mezer.

_____

Simona Krákorová

V Praze dne 18. června 2019

Obsah

ÚVOD

Pro společnost 21. století je naprosto charakteristické stále výraznější propojení každodenního života a nejrůznějších technologií. Značná část mezilidské komunikace, ať už v zaměstnání či v ostatních oblastech života, se odehrává ve virtuálním světe a pro mnoho z nás je takřka nepřestavitelná existence bez internetu.[1]

Neustále se rozvíjející oblast informačních a komunikačních technologií se přirozeně projevuje i v oblasti trestního práva. Pachatelé dnes při páchání trestné činnosti využívají širokou škálu zařízení (od běžných mobilních telefonů přes software umožňující odblokování elektronického zabezpečení vozidel po hackerské programovací nástroje). Elektronické důkazní prostředky se tak objevují v souvislosti s téměř všemi druhy trestné činnosti, nikoliv jen v rámci počítačové kriminality.[2]

Tomuto stavu se musí přizpůsobit i orgány činné v trestním řízení tak, aby byla zachována důvěra společnosti v právní stát, který je schopen zajistit ochranu bezpečnosti a veřejného pořádku. Nabízí se však otázka, zda těmto orgánům aktuální právní úprava umožňuje adekvátně reagovat na výzvy nové informační doby. Zda současná úprava dokazování a institutů s dokazováním souvisejících umožňuje orgánům činným v trestním řízení rychle a efektivně zajišťovat elektronické důkazní prostředky a potažmo získané důkazy užít pro usvědčení pachatelů. Cílem této práce je zhodnotit současnou právní úpravu, její specifika, a navrhnout případné změny, které se v daných oblastech jeví jako vhodné.

Aktuální právní úprava vykazuje problémy v několika směrech. Za problematickou skutečnost považuji, že příslušné orgány často zajišťují elektronické důkazní prostředky prostřednictvím postupů, které uspokojivě nezaručují ochranu práv a svobod jednotlivců. V oblasti zajišťování těchto důkazních prostředků navíc často není jasné, jakou cestou se mají příslušné orgány vydat. Tuto situaci sice částečně napravuje judikatura spolu s výkladovými stanovisky Nejvyššího státního zastupitelství (dále jen „NSZ“), nicméně

[1] Samotný pojem internet není v české legislativě definován. Dle údajů Českého statistického úřadu bylo v roce 2018 připojeno k internetu více než 80 % českých domácností, [online], [cit. 10. 5. 2019], dostupné: https://www.czso.cz/documents/10180/61508128/0620041809.pdf/8ea8ced6-6822-4f5a-bf29-a57279ac93e7?version=1.3

[2] SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7, s. 697

absence závaznosti výkladových stanovisek může vést k určitým odchylkám v praxi příslušných orgánů.

Významné nedostatky se objevují v souvislosti se zajišťováním údajů od provozovatelů sociálních sítí a služeb souvisejících. V této oblasti došlo k rozvinu jakési přímé spolupráce osob soukromého práva s orgány činnými v trestním řízení. Tato spolupráce je však postavena především na dobrovolnosti dotčených subjektů nežli na adekvátním zákonném základě. Daná praxe se ustálila především v důsledku neefektivní legislativy, jež nedovoluje rychlé a účinné (zejména přeshraniční) zajištění elektronických důkazních prostředků. Otázkou však zůstává, zda splňuje tato praxe požadavky na zaručení nezbytné úrovně ochrany jedinců před neoprávněným nakládáním s jejich údaji.

Na úrovni Evropské unie (dále jen „EU“) se v současné době projednává iniciativa, která si klade za cíl zakotvit přímou spolupráci orgánů veřejné moci a poskytovatelů služeb informační společnosti a elektronických komunikací prostřednictvím předávání a uchovávání elektronických důkazů. V této souvislosti taktéž EU iniciovala vyjednávání dohody se Spojenými státy americkými (dále jen „USA“) o přeshraničním přístupu k elektronickým důkazům v trestních věcech. Současně došlo na úrovni Rady Evropy k zahájení vyjednávání druhého dodatkového protokolu k Úmluvě o počítačové kriminalitě z Budapešti.[3] Všechny výše uvedené iniciativy se mají oprostit od v současnosti klíčového hlediska umístění dat, a to po vzoru nové legislativy USA, tzv. CLOUD Act. Zakotvení navrhovaných principů by zřejmě mohlo vést k nápravě výše uvedené situace. Nicméně, je nezbytné se zabývat důsledky přijetí takovéto legislativy a současně i problematikou jejího právního základu.

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

1. Pojem elektronický důkazní prostředek

1.1 Právní úprava dokazování v českém právním řádu

Procesem dokazování se v trestním právu procesním rozumí: *„zákonem upravený postup orgánů činných v trestním řízení, jehož úkolem je umožnit poznání skutečností důležitých pro rozhodnutí, tedy vyhledat důkazy o nich, tyto důkazy provést, získané poznatky procesně zajistit a zhodnotit.“* Procesní normy, které proces dokazování upravují se nazývají *důkazní právo.*[4]

Během procesu dokazování se střetává veřejný zájem společnosti na usvědčení pachatelů trestné činnosti se zájmem na spravedlivém projednání a rozhodnutí věci, v širším smyslu s právem na spravedlivý proces.[5] Východisko pro právo na spravedlivý proces poskytuje článek 6 Evropské úmluvy o ochraně lidských práv a základních svobod (dále jen „Úmluva“).[6] V souvislosti s dokazováním je nezbytné brát v úvahu judikaturu Evropského soudu pro lidská práva (dále jen „ESLP“), zejména tu týkající se právě článku 6. Východiska spravedlivého procesu nalezneme i v dalších dokumentech, kterými je Česká republika (dále jen „ČR“) vázána na základě čl. 10 Ústavy ČR (dále jen „Ústava“), tj. v Úmluvě proti mučení a jinému krutému, nelidskému či ponižujícímu zacházení nebo trestání[7] či v Mezinárodním paktu o občanských a politických právech[8], aj. Na vnitrostátní úrovni vychází právo na spravedlivý proces z Ústavy[9], a to z čl. 95 odst. 1 a čl. 96 a z Listiny základních lidských práv a svobod (dále jen „Listina“)[10], konkrétně z čl. 36 odst. 1, čl. 37, čl. 38 odst. 2 a čl. 40 odst. 4.

Procesní činnost orgánů činných v trestním řízení, nazvaná dokazování, je podrobněji upravená v trestním řádu v části první, v hlavě páté (§ 89 až § 118). Ustanovení hlavy páté obsahují především obecnou právní úpravu dokazování společnou

---

[4] JELÍNEK, J., Trestní právo procesní. 5. vydání. Praha: Leges, 2018, ISBN 978–80–7502–278–3 s. 363
[5] ZAORALOVÁ, P. Procesní použitelnost důkazů v trestním řízení a její meze. Praha: Leges, 2018. Teoretik. ISBN 978-80-7502-310-0., s. 27 a násl.
[6] Sdělení federálního ministerstva zahraničních věcí č. 209/1992 o sjednání Úmluvy ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících.
[7] Vyhláška ministra zahraničních věcí č. 143/1988 Sb. o Úmluvě proti mučení a jinému krutému, nelidskému či ponižujícímu zacházení nebo trestání
[8] Vyhláška ministra zahraničních věcí č. č. 120/1976 Sb. o Mezinárodním paktu o občanských a politických právech a Mezinárodním paktu o hospodářských, sociálních a kulturních právech
[9] Ústavní zákon č. 1/1993 Sb., Ústava České republiky
[10] Usnesení předsednictva České národní rady č. 2/1993 Sb. o vyhlášení Listiny základních práv a svobod jako součástí ústavního pořádku České republiky

pro všechna stadia trestního řízení, neupravují tedy dokazování vyčerpávajícím způsobem.

Pro proces dokazování mají velký význam i další ustanovení trestního řádu. Jedná se v první řadě o základní zásady trestního řízení (§ 2 trestního řádu), zejména zásada presumpce neviny, zásada materiální pravdy, zásada vyhledávací, zásada bezprostřednosti a ústnosti, zásada volného hodnocení důkazů a zásada přiměřenosti. Význam mají taktéž pravidla týkající se jednotlivých stádií trestního řízení. Před zahájením trestního stíhání hrají významnou roli neodkladné a neopakovatelné úkony[11] či operativně pátrací prostředky[12]. Nelze se obejít ani bez procesních úkonů, jako je vyžadování vysvětlení, odborného vyjádření, ohledání věci, či ohledání místa činu policejním orgánem, aj.[13] (§ 158 odst. 3 trestního řádu).

Pro elektronickou formu důkazních prostředků pak hrají nezastupitelnou roli zajišťovací instituty, jejichž specifika podrobněji rozebírám v druhé kapitole své diplomové práce. Jedná se zejména o právní úpravu odposlechu a záznamu telekomunikačního provozu, zjišťování údajů o telekomunikačním provozu, operativně pátracího prostředku sledování osob a věcí, institutu vydání a odnětí věci důležité pro trestní řízení a provádění domovní prohlídky, prohlídky jiných prostor a pozemků. V některých případech lze využít i ohledání věci. Pro analýzu zajištěných pramenů elektronických důkazů pak bude zpravidla přizván znalec.

1.1.1 Základní pojmy týkající se dokazování

Důkazním prostředkem se ve fázi dokazování v rámci trestního řízení rozumí: *„zdroj, z něhož orgán činný v trestním řízení důkazy čerpá.“*[14] Dle Jelínka lze důkazní prostředek definovat jako: *„vlastní procesní činnost orgánu činného v trestním řízení, která slouží podle trestního řádu k poznávání skutečnosti.“*[15] Jedná se tedy o formu procesního poznávání. Důkazním prostředkem jsou např. ohledání osob a věcí, výslech

[11] § 158 odst. 3 písm. i), odst. 9, § 158a, § 160 odst. 4, § 179b odst. 1 trestního řádu
[12] § 158b a násl. trestního řádu
[13] § 158 odst. 3 trestního řádu
[14] FENYK, J., GŘIVNA, T. a CÍSAŘOVÁ, D., Trestní právo procesní. 6., aktualiz. vyd. Praha: Wolters Kluwer, 2015. ISBN 978-80-7478-750-8
[15] JELÍNEK, J., Trestní právo procesní. Op. cit., s. 361

osob, výslech znalce, přehrání audiozáznamu, promítnutí audiovizuálního záznamu, či například přečtení obsahu e-mailové komunikace.[16]

Důkazem se rozumí výsledek, který byl orgánem činným v trestním řízení v rámci procesu dokazování získán o předmětu důkazu z důkazního prostředku. Jedná se tedy o obsah procesního poznání, tj. obsah listin, obsah výpovědi, obsah komunikace zasílané prostřednictvím elektronické pošty, výsledek znaleckého zkoumání.[17] Důkaz lze definovat jako *„přímý poznatek získaný orgánem činným v trestním řízení o existenci či neexistenci určité okolnosti, která se má dokazovat.“*[18] Skutečnost, která má být procesem dokazování zjištěna je označena pojmem *předmět důkazu*. *Pramenem důkazů*, či nositelem důkazu pak rozumíme osoby a věci, které jsou s důkazem spjaty.[19]

Předně je vhodné uvést, že jak trestní řád, tak praxe pojmy důkazní prostředek a důkaz nerozlišují, což může vést k určitým problémům. Například, zákon v ustanovení § 89 odst. 2 trestního řádu hovoří o výpovědi obviněného a svědků jako o důkazu, ačkoliv dle nauky výpověď odpovídá spíše pojmu důkazní prostředek.[20] Dle Jelínka však nemá tato skutečnost vzhledem k úzké souvislosti pojmů důkaz a důkazní prostředek nepříznivé důsledky, a to proto, že je očividné, kdy je kladen větší důraz na formu poznání a kdy na jeho obsah.[21]

Druhý odstavec ustanovení § 89 trestního řádu stanoví, že *„za důkaz může sloužit vše, co může přispět k objasnění věci.“* Co do možnosti využití určitého druhu důkazního prostředku tak existuje pouze logické omezení, a to, že důkaz má mít souvislost s dokazovanou skutečností, kterou může prokázat či vyvrátit.[22] Totéž ustanovení následně názorně uvádí některé přípustné důkazní prostředky, tj. výpovědi obviněného a svědků, znalecké posudky, věci a listiny důležité pro trestní řízení a ohledání. Je ponecháno na orgánech činných v trestním řízení, jaké další nástroje k objasnění skutkového stavu věci použijí. Z dikce zákona lze tedy dovodit, že orgány činné

[16] JELÍNEK, J., Trestní právo procesní. Op. cit., s. 361
[17] Ibid
[18] ŠÁMAL, P. Trestní řád: komentář. 7., dopl. a přeprac. vyd. V Praze: C.H. Beck, 2013. Velké komentáře. ISBN 978-80-7400-465-0. s.1308-1394
[19] JELÍNEK, J., Trestní právo procesní. Op. cit., s. 361
[20] Ibid, ZAORALOVÁ, P.: Procesní použitelnost důkazů v trestním řízení a její meze. Op. cit., s. 29.
[21] JELÍNEK, J., Trestní právo procesní. Op. cit., s. 362
[22] ŠÁMAL, P. Trestní řád: komentář. Op. cit., s.1308-1394

v trestním řízení mohou k objasňování skutečností důležitých pro trestní řízení použít i poměrně širokou škálu elektronických důkazních prostředků.

O otázce vhodnosti demonstrativního výčtu důkazních prostředků se však vedou určité diskuze. Mezi autory, kteří se přiklánějí k přechodu na výčet taxativní patří i Jelínek. Dle Jelínka by bylo vhodné do budoucna zavést taxativní výčet důkazních prostředků, jelikož by taková právní úprava byla jednoznačně *in favorem* principu právní jistoty a ochrany práv fyzických a právnických osob.[23] Proti tomu lze však argumentovat, že zavedení taxativního výčtu by mohlo činit potíže v souvislosti s rozvojem nových forem důkazních prostředků, kdy na tento vývoj by nebyl schopen efektivně reagovat zákonodárce. Otázkou tedy zůstává, zda namísto nové legislativní úpravy není vhodnější ponechat výklad forem důkazních prostředků judikatuře soudů.

Orgány činné v trestním řízení si prostřednictvím dokazování obstarávají skutkový podklad tak, aby mohly co nejpřesněji a nejvěrněji zrekonstruovat skutek, a tento postup je klíčový pro následné rozhodování soudu o vině a trestu. Postupují v souladu se zásadou materiální pravdy, tak: *„aby byl zjištěn skutkový stav věci, o němž nejsou důvodné pochybnosti, a to v rozsahu, který je nezbytný pro jejich rozhodnutí.*“[24]

Subjekty dokazování trestní řád nevymezuje, nicméně obecně se jedná o orgány činné v trestním řízení (§ 12 odst. 1 trestního řádu), které jsou povinny samy na základě vyhledávací zásady důkazy aktivně zjišťovat, zajišťovat, provádět a hodnotit; a dále o strany trestního řízení, u kterých není vyloučena součinnost a osoby ostatní, tj. např. znalec či specializovaný konzultant.

Nauka rozděluje důkazy na základě rozdílných kritérií. To však neznamená, že by zákon některému důkazu přiznával větší váhu než jinému. V souladu se zásadou volného hodnocení důkazů hodnotí orgány činné v trestním řízení důkazy dle svého vnitřního přesvědčení založeného na pečlivém uvážení všech okolností případu, a to jednotlivě i v jejich souhrnu. Důkazy lze dle nauky rozdělit[25]:

a) na *usvědčující* a *ospravedlňující*, a to dle vztahu k předmětu obvinění; přičemž důkazy usvědčující prokazují okolnosti svědčící proti obviněnému a potvrzují

---

[23] JELÍNEK, J., K chybějící právní úpravě tzv. prostorového odposlechu v trestním řádu, Bulletin advokacie 7-8/2018, s. 13
[24] § 2 odst. 5 trestního řádu
[25] JELÍNEK, J., Trestní právo procesní. op. cit., s. 382 a násl.; ŠÁMAL, P. Trestní řád: komentář. op. cit., s.1308-1394

obvinění; ospravedlňující důkazy na druhou stranu prokazují okolnosti, svědčící ve prospěch obviněného, nehledě na to, zda jeho obvinění jen zeslabují nebo zcela vyvracejí. Obviněný je oprávněn v rámci práva na spravedlivý proces dle Úmluvy *"vyslýchat svědky proti sobě a má právo dosáhnout předvolání a výslechu osob svědčících v jeho prospěch."*[26] Současně platí, že obviněný nesmí být donucován k poskytování důkazů ve svůj neprospěch na základě zásady *nemo tenetur se ipsum accusare.*[27]

b) na *původní* a *odvozené*, a to dle vztahu pramene zpráv o dokazované skutečnosti k této skutečnosti. Toto dělení závisí na tom, zda je nebo není mezi původním pramenem zpráv o dokazované události, který byl v bezprostředním kontaktu s takovou událostí, a orgánem, který provádí dokazování, zprostředkující nositel informací. Původní důkaz je získán z pramene bezprostředního, tj. z výpovědi svědka, originálu listiny. Odvozený důkaz je naopak získán z pramene odvozeného (prostředečného), tj. např. výpověď svědka o událostech, kterých se nezúčastnil, ale doslechl se o nich[28]. Odvozené důkazy jsou problematické vzhledem k jejich omezené věrohodnosti, a to například právě u odvozené svědecké výpovědi. Přesto však nelze odvozené důkazy v rámci procesu dokazování opomíjet, jelikož mohou často sloužit k získání důkazu původního.[29]

c) na *přímé* a *nepřímé,* a to dle vztahu k dokazované skutečnosti. Přímý důkaz přímo potvrzuje nebo vyvrací dokazovanou skutečnost. Nepřímý důkaz dokazuje jinou skutečnost, ale takovou, ze které je možno usuzovat, zda se stala či nestala skutečnost, o jejíž důkaz jde.[30] Nezřídka mívá orgán činný v trestním řízení k dispozici pouze důkazy nepřímé, jejichž vztah k dokazované skutečnosti je mnohdy vzdálený. Přesto může být o vině a trestu rozhodnuto na základě výlučně nepřímých důkazů, a to za předpokladu, že „*tvoří ve svém souhrnu logickou, ničím*

---

[26] Článek 6 odst. 3 písm. d) Úmluvy

[27] Zásadě „nemo tenetur" je věnována pozornost v judikatuře ESLP, přičemž v rozsudku ve věci Jalloh vs. Německo ze dne 11.7.2006 zakotvil soud test, zda postup orgánů činných v trestním řízení potlačuje princip zákazu sebeobviňování, jehož prvky jsou dle bodu 101 daného rozsudku: povaha a stupeň donucení, existence relevantních záruk v řízení a to, jak je takto získaný materiál použít. Zásadě zákazu sebeobviňování se věnuje rozsáhlá judikatura českých soudů, např. nález Ústavního soudu, sp. zn. II. ÚS 255/05 ze dne 23. 6. 2005, nález Ústavního soudu, sp. zn. II. ÚS 2369/08 ze dne 9. 12. 2010, Stanovisko pléna Ústavního soudu Pl.ÚS-st. 30/10 ze dne 30. 11. 2010

[28] V angloamerickém právním systému se tento institut označuje jako tzv. „hearsay evidence"

[29] JELÍNEK, J., Trestní právo procesní. Op. cit., s.382. a násl.; ŠÁMAL, P. Trestní řád: komentář. Op. cit., s.1308-1394

[30] Ibid

nenarušenou a uzavřenou soustavu."[31] Nepřímým důkazem je např. nález daktyloskopické stopy nebo výsledek pachové zkoušky.[32] Z judikatury Nejvyššího správního soudu (dále jen „NSS") lze dovodit, že důkazy o skutečnosti, zda došlo k odeslání zprávy v rámci elektronické pošty, či prostřednictvím komunikační aplikace tzv. instant messagingu (komunikace v rámci aplikací Facebook Messenger či Viber, atd.) z IP adresy přidělené určitému telefonnímu číslu, jehož je účastník uživatelem, bude mít charakter nepřímého důkazu. Skutečnost, že ze zařízení uživatele odešla určitá komunikace totiž automaticky neznamená, že sám uživatel je autorem takové komunikace.[33]

1.2 Elektronický důkazní prostředek

Pojem elektronický důkazní prostředek nebo elektronický důkaz český právní řád nezná[34]. Pokud by zákonodárce v rámci plánované rekodifikace trestního řízení uvažoval o zakotvení taxativního výčtu důkazních prostředků, bylo by z hlediska *de lege ferenda* jistě nezbytné definovat právě pojem těch elektronických. Prostým důvodem je skutečnost, že nějakou formu elektronického důkazu lze vypátrat v souvislosti s většinou páchané trestné činnosti.

Je vhodné poznamenat, že v platné právní úpravě již existují ustanovení, která předpokládají využití elektronických zařízení v rámci trestního řízení, např. § 52a trestního řádu upravuje možnost využití videokonferenčního zařízení při provádění úkonů trestního řízení. Ačkoliv zavedení obdobných institutů není bez kritiky, využití elektronických zařízení dané úkony nepopiratelně usnadňuje a urychluje, což napomáhá naplňovat zásady rychlosti, potažmo hospodárnosti trestního řízení. Například možnost výslechu prostřednictvím videokonferenčního zařízení se v praxi jeví jako velmi přínosná, především pokud je třeba vyslechnout osobu, jež pobývá v cizině[35].

---

[31] Rozhodnutí Nejvyššího soudu České socialistické republiky, sp. zn. 7 Tz 84/69, ze dne 24. 3. 1970, publikováno jako R 38/1970 – I.
[32] Rozhodnutí Nejvyššího soudu, sp. zn. 5 Tdo 1207/2016, ze dne 21. 9. 2016, publikováno jako R 46/2017, a Rozhodnutí Nejvyššího soudu, sp. zn. 4 Tz 107/2002, ze dne 15. 4. 2003 publikováno jako SR 12/2003 v Soudních rozhledech, 12/2003
[33] Rozhodnutí Nejvyššího správního soudu, č.j. 1 As 90/2008-189 ze dne 4. 2. 2009
[34] POLČÁK, R., PÚRY, F. a HARAŠTA, J. Elektronické důkazy v trestním řízení. Brno: Masarykova univerzita, 2015. ISBN 978-80-210-8073-7, s. 94
[35] Část pražských soudců se k videokonferencím zatím staví zdrženlivě, Česká justice [online], [cit. 12. 4. 2019], dostupné: http://www.ceska-justice.cz/2017/08/cast-prazskych-soudcu-se-k-videokonferencim-zatim-stavi-zdrzenlive/

Dle dosavadní literatury lze obecně elektronické důkazní prostředky definovat jako *„důkazní prostředky, k jejichž převodu do podoby srozumitelné pro člověka je třeba použít nějaké elektronické zařízení*.“[36] Východiskem pro tuto definici je především charakter dat jakožto elektronických důkazních prostředků a jejich uchovávání v podobě pro člověka jeho smysly jen těžko uchopitelné. Data, ve smyslu dat počítačových, pak lze definovat například jako *„jakékoliv vyjádření faktů, informací nebo pojmů vhodné pro zpracování v počítačovém systému, včetně programu způsobilého zapříčinit provedení funkce počítačovým systémem.“*[37] Obecně jsou data zdrojem relevantní informace uchované v elektronické podobě. Aby byl člověk schopný předmětným datům porozumět, je nezbytné je interpretovat pomocí nějakého nástroje, tj. elektronického zařízení.[38]

Pro srovnání dále uvádím, jak na definici elektronických důkazních prostředků či elektronických důkazů nahlíží zahraniční literatura. Je nezbytné poznamenat, že v angloamerickém systému nebývá rozlišováno mezi pojmy důkaz a důkazní prostředek.[39]

Mason navrhuje následující definici: *„data, se kterými je nakládáno, která jsou uložena či sdělovaná zařízením, počítačem, počítačovým systémem či přenášena prostřednictvím komunikačního systému, která jsou způsobilá učinit skutkové tvrzení jedné strany více, či méně pravděpodobným, než by tomu tak bylo bez nich.“*[40]

Pojem data zde zahrnuje jak data ve formě digitální, tak výstupy z analogového zařízení. Na rozdíl od dalších definic[41] zahrnují obě výše uvedené jak analogové, tak

---

[36] KOČÍ, M. Elektronické důkazní prostředky. Brno: Masarykova univerzita, 2012. Diplomová práce, na tuto definici odkazuje ve své publikaci i Polčák, viz. POLČÁK, R., PÚRY, F. a HARAŠTA, J. Elektronické důkazy v trestním řízení. Op. cit., s.95

[37] Jedná se o definici počítačových data dle čl. 1 písm. b) Sdělení Ministerstva zahraničních věcí, č. 104/2013 Sb. m. s., o sjednání Úmluvy o počítačové kriminalitě

[38] POLČÁK, R., PÚRY, F. a HARAŠTA, J. Elektronické důkazy v trestním řízení. Op. cit., s. 95

[39] Výkladový slovník GARNER, B. (eds.) et al. A. Black's Law Dictionary. 8. vyd., St. Paul (MN, USA): Thomson West, 2004. s. 595

[40] V originále: *„data (comprising the output of analogue devices or data in digital form) that is manipulated, stored or communicated by any manufactured device, computer or computer system or transmitted over a communication system, that has the potential to make the factual account of eitther party more probable or less probable than it would be without the evidence.“*
MASON, S., SENG, D., Electronic evidence, 4th edition, 4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017, ISBN 978-1-911507-07-9 s. 19

[41] Např. definice Caseyho: „*jakákoliv data přenášená za použití počítače, která prokazují či vyvracejí domněnku, jak se stal trestný čin nebo, která adresují závažné elementy trestného činu jako jsou úmysl či důkaz o nevině.“* CASEY, E., Digital Evidence and Computer Crime, 3. vydání, Academic Press 2011, s. 7

digitální zařízení, přičemž druhá definice poskytuje následně jejich demonstrativní výčet. Může se jednat o zařízení v nejrůznějších formách, příkladmo osobní počítač, mobilní telefon, bezdrátový telekomunikační systém, navigační systémy, zařízení, které jsou součástí oděvu či domácnosti (např. smartwatch). Obě definice taktéž berou v potaz pouze informace relevantní pro určitý zákonem předvídaný postup státních orgánů, tj. je splněna podmínka souvislosti s dokazovanou skutečností.

Mason si klade za cíl především stanovit definici obecnou, ačkoliv nemusí být plně v souladu s terminologií počítačové vědy a upozorňuje, že s ohledem na velmi rychlý vývoj informačních technologií, je velmi složité stanovit vhodnou definici, která by nebyla dříve či později překonána, či naopak, která není pro potřeby důkazního práva příliš abstraktní.[42]

1.3 Charakter dat jakožto digitálních stop

V terminologii kriminalistiky představují data jeden z druhů digitálních stop (vedle stop technických). Pod pojmem digitální stopa si lze představit: *„jakoukoliv informaci s vypovídající hodnotou pro danou relevantní událost, uloženou či přenášenou v digitální podobě.“* Data lze rozdělit to tří kategorií: na systémová, programová a uživatelská. Vymezení dat pak představuje podmínku pro počítačovou kriminalistickou expertízu. [43]

Při zajišťování digitálních stop a při jejich následné manipulaci musí mít dotčené orgány na paměti jejich specifickou povahu. Takové stopy jsou nestálé, volatilní a mohou být snadno pozměněny nebo dokonce ztraceny, a to v některých případech i prostým vypnutím výpočetní techniky.

Problematiku zajišťování digitálních stop lze demonstrovat na případu ESLP, *Khodorkovskiy a Lebedev proti Rusku*. Ruský úřad generálního prokurátora zde v rámci řízení zajistil mimo jiné pevné disky z několika počítačů, přičemž tyto pevné disky byly přezkoumány vyšetřovateli na půdě úřadu generálního prokurátora za účasti nezúčastněných osob a poté byly předány expertům za účelem extrakce dat. Takto extrahované informace pak byly prezentovány vnitrostátnímu soudu ve formě výtisků.

---

[42] MASON, S., SENG, D., editors. Electronic Evidence. Op. cit., s. 19
[43] PORADA, V., POLÁK, P. et al. Kriminalistika. Plzeň: Aleš Čeněk, 2015. ISBN 978-80-7380-558-6, s. 77

Žalobci k tomuto tvrdili, že mezi informacemi, které se nacházely na pevných discích v době jejich zajištění a informacemi, které byly předloženy soudu došlo k rozporu. Žalobci dále uvedli, že předmětné pevné disky nebyly v době jejich uchování na půdě generální prokuratury řádně zabaleny a zapečetěny, a tudíž, že mohlo dojít k modifikaci uložených dat. ESLP k námitkám žalobců uvedl, že v souvislosti se zajišťováním a přezkoumáváním předmětných důkazů nebyla zjištěna žádná zásadní chyba, která by vedla k nepoužitelnosti takových důkazů před soudem, a to ačkoliv předmětné pevné disky opravdu zapečetěny nebyly.[44] Proti danému rozhodnutí Mason namítá, že došlo ze strany soudu k závažnému nepochopení důležitosti dodržování určitých standardů při manipulaci s digitálními stopami.[45] Dle mého názoru by měly především existovat určité jasně stanovené standardy pro nakládání s prameny elektronických důkazů, konkrétně si lze představit vytvoření interních instrukcí příslušných orgánů, čímž by byla zaručena možnost zpětné kontroly ze strany nadřízených orgánů a soudu, který bude důkazy hodnotit. A to v případě podezření, že s předmětnými prameny nebylo řádně zacházeno. V souvislosti s výše uvedeným případem je nasnadě poznamenat, že zapečetění pevných disků je poměrně snadno proveditelné pro zajištění integrity důkazu účinné opatření.

Problémem digitálních stop je tedy snadná možnost jejich pozměnění či zničení. Tento problém lze demonstrovat na příkladech zařízení pro uchovávání dat. V praxi se běžně pro uchování dat používají tzv. pevné disky (magnetické mechanické disky), jejichž princip je již od 60. let minulého století v zásadě stejný, přičemž primární výhoda použití pevných disků spočívá v jejich relativně nízké ceně. Modernější technologií pro ukládání dat jsou tzv. SSD (Solid-state drive) disky, které jsou oproti prvně zmíněným rychlejší, méně energeticky náročné a odolnější vůči podmínkám okolního prostředí. V případě klasických pevných disků dochází k faktickému odstranění „smazaných“ dat až zápisem dat nových, a je tedy poměrně složité kompletně odstranit uložená data. Pro expertní analytiky tak není velkým problémem tato „smazaná“ data obnovit. Systém SSD disků však funguje na zcela jiném principu, kdy dochází k přepisování „neužitečných“ bloků dat, což vede k fyzickému výmazu dat, které již obnovit nelze.[46] To samozřejmě

[44] Rozsudek ESLP Khodorkovskiy a Lebedev proti Rusku ze dne 25. 7. 2013, (č. 11082/06 13772/05), bod. 72 a 181
[45] MASON, S., SENG, D., editors. Electronic Evidence. Op. cit., s. 289
[46] BELL, G. B., BODINGGTON, R., Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery? 2010

činí problémy, jelikož narušení integrity důkazů může působit potíže při jejich uplatňování před soudem, a nakonec může vést až k jejich nepoužitelnosti.

1.3.1 Nové přístupy k analýze dat

V souvislosti s problematikou zajišťování a analýzy digitálních stop se v posledních letech dostalo mezi zahraničními autory pozornosti tzv. metodě třídění. Tato metoda zahrnuje řadu specifických procesů souvisejících s nakládáním s digitálními stopami v rámci vyšetřování.[47]

Za výhodu této metody autoři považují včasnost identifikace, analýzy a interpretace digitálních stop. Je tedy využitelná především v souvislosti s trestnou činností, kdy sehrává čas kruciální roli, např. v případech únosů dětí. Metodu zmiňuji, jelikož je již nyní využívána ve zdravotnických zařízeních, kdy je třeba alokovat omezené zdroje za účelem roztřídění pacientů do určitých skupin na základě jejich potřeby okamžitého ošetření. Metodě se věnuje řada autorů, kteří navrhují různá konkrétní řešení, a ty novější pak implementují jednu z oblastí umělé inteligence, tzv. strojové učení.[48]

Jeden z původních modelů metody třídění představuje tzv. terénní přístup.[49] Jak již napovídá jeho název, podstatou tohoto přístupu je identifikace, analýza a interpretace stop v krátkém časovém úseku, bez nutnosti přemisťování elektronických zařízení do laboratoře. K úspěšné aplikaci metody je nezbytné náležité technické vybavení a expert schopný velmi efektivně analyzovat předmětná data. Dle autorů má tento postup následující fáze:

1. V počáteční fázi je nutné stanovit vyšetřovací verze, stanovit si známé a neznámé proměnné, zajistit náležité technické a personální vybavení.
2. Následuje fáze tzv. třídění, která spočívá v identifikaci a roztřídění potencionálních pramenů důkazů (paměťových médií, počítačů, aj. na základě kritéria rychlosti možnosti extrakce relevantních dat a na základě kritéria přednosti volatilních dat (typicky data v operační paměti).

[47] MASON, S., SENG, D., editors. Electronic Evidence. Op. cit., s. 286
[48] GADE, S., MANE, V., Survey on „Triage-based" Digital Forensic Models, International Journal of Engineering Research in Computer Science and Engineering (IJCSE), Vol 3, Issue 7, červenec 2016
[49] ROGERS, M. K., GOLDMAN, J., MISLAN R., WEDGE T., Computer Forensic Field Triage Process Model, Conference on Digital Forensic, Security and Law, 2006

3. Po nalezení relevantního poznatku je nezbytné prokázat spojení mezi tímto poznatkem a určitou osobou. V této fázi je nezbytné určit, kolik osob mělo přístup k elektronickému zařízení. S tím souvisí počet uživatelských profilů a skutečnost, zda byly tyto profily používány jednou či více osobami. K tomu je nezbytné dát do souvislosti údaje nalezené v metadatech souborů s údaji o čase, kdy měla či neměla určitá osoba přístup k elektronickému zařízení.
4. V další fázi je nalezený poznatek definován metadaty obsahující informace o tom, kdy byly dotčené dokumenty vytvořeny, změněny nebo zobrazeny. Díky tomu lze kvalifikovat, kdy určitá osoba zařízení používala. Dále v této fázi probíhá identifikace a analýza aplikačního softwaru a datových souborů, které byly používány během relevantních časových období. Během determinace časové osy jsou významné i např. tzv. cookies či cache.[50] K výše uvedenému je však nutno uvést, že systémové hodiny mohou vykazovat určité nepřesnosti a mohou být snadno nastaveny samotným uživatelem.
5. Následuje fáze, kdy je zjišťována internetová aktivita. Analytik bude především zjišťovat, jak tyto aktivity souvisejí s případem.
6. V poslední fázi je nezbytné přizpůsobit proces specifikům dané trestné činnosti, např. v případě trestných činů souvisejících s majetkovou kriminalitou se mohou nacházet na datovém nosiči dokumenty obsahující faktury či jiné záznamy, významné ale mohou být i nejrůznější uživatelské aplikace.

Zjevná nevýhoda toho přístupu spočívá v možnosti opomenutí či přehlédnutí důležité stopy. Proto, jak autoři upozorňují, není vyloučena následná podrobná analýza zajištěných pramenů důkazů v laboratoři.[51]

Dle výkladového stanoviska NSZ č. 9/2001 závisí rozhodnutí o tom, zda bude obsah nosičů zjišťován přímo na místě, při provádění domovní prohlídky nebo prohlídky jiných prostor a pozemků nebo, zda budou takové nosiče zajištěny a podrobněji analyzovány na expertním pracovišti, na množství zajištěných datových nosičů a na složení týmu prohlídku provádějící. Zejména závisí na skutečnosti, zda se úkonu účastní

[50] Cookies jsou krátké soubory dat, které jsou standardně ukládané do webového prohlížeče, sloužící především k vytvoření stavové komunikace na webu, zaznamenávají např. informace o nastavení jazyka. Jejich účelem je především zefektivnění dalších návštěv webových stránek. Cache znamená vyrovnávací paměť, kam jsou dočasně ukládána data, za účelem jejich rychlejšího znovunačtení.
[51] ROGERS, M. K., GOLDMAN, J., MISLAN R., WEDGE T., Computer Forensic Field Triage Process Model, Conference on Digital Forensic, Security and Law, 2006

znalec.[52] Ten se účastní takového úkonu jako konzultant, jelikož on sám není oprávněn zajišťovat důkazní prostředky, k tomu jsou oprávněny jen policejní orgány.

Pro srovnání dále uvádím novější a z technologického hlediska zajímavější přístup k tzv. metodě třídění, model automatizované analýzy a kategorizace dat, který funguje na principech strojového učení. Strojové učení („*machine learning*“) je jedna z oblastí informatiky, zabývající se umělou inteligencí. Tato oblast se především věnuje problematice algoritmů, které umožňují počítačovému systému „učit se“.[53]

Dle autorů má model automatizované analýzy a kategorizace následující fáze:

1. První fáze spočívá v zajištění digitální stopy, v této fázi dochází k vytvoření klonové kopie zkoumaného pramene důkazu, např. paměťového média. Současně je třeba zajistit integritu média tak, aby byla zaručena možnost opětovného provedení analýzy.
2. V následné fázi dochází k extrakci relevantní informace o uživateli zkoumaného média. Zjišťují se uživatelovy návyky, dovednosti, zájmy. Předmětem zájmu je instalovaný software, webová historie, statistiky souborů, metadata souborů, prohlížeč událostí, atd.
3. Ve třetí fázi dochází k identifikaci informací souvisejících s trestnou činností, tj. například přítomnost nelegálního pornografického materiálu, nelegálně instalovaného softwaru, aj.
4. Tyto informace jsou následně vytěžovány za účelem kategorizace zkoumaného pramene důkazů na základě relevance jeho obsahu, přičemž základem pro tuto fázi jsou algoritmy strojového učení, tzv. WEKA. WEKA je software v programovacím jazyce Java, který používá velké množství algoritmů provádějících analýzu dat a prediktivní modelování. Kategorizaci předchází fáze učení. Aby byl software schopný provést danou kategorizaci, je nezbytné jej naučit analyzovat digitální zařízení a předpovídat závislou proměnnou, tj. třídu (zda souvisí s trestným činem či nikoliv). K tomu je nezbytné nejdříve vytvořit

[52] Výkladové stanovisko Nejvyššího státního zastupitelství č. 9/2001 ze dne 13. 6. 2001 k zajišťování počítačů a jiných nosičů informací při domovní prohlídce a prohlídce jiných prostor a pozemků
[53] MARTURANA, F., TACCONI, S., A machine learning-based Triage methodology for automated categorization of digital media, Digital investigation, Vol. 10, Sept. 2013

tréninkovou sadu, skládající se z reprezentativních vzorků zařízení, která již byla klasifikována a je u nich znám vztah k trestnému činu[54].

Ačkoliv umělá inteligence stále více proniká do všech oblastí lidského života, využití plně automatizované analýzy namísto podrobného expertního zkoumání je stále v počátcích svého vývoje. Situace, kdy by byl lidský faktor zcela nahrazen umělou inteligencí bude zřejmě ještě v horizontu několika let spíše nepředstavitelný. Nicméně, již v současnosti můžeme uvažovat o variantě, kdy podobná metoda pomůže vyšetřovatelům učinit objektivní a informované rozhodnutí. V této podobě lze uvažovat, že by umělá inteligence mohla doplnit klasické metodologické postupy policejních orgánů v souvislosti s určitou specifickou skupinou trestné činnosti, kde se využití obdobných metod jeví jako přínosné.

[54] MARTURANA, F., TACCONI, S., A machine learning-based Triage methodology for automated categorization of digital media, Digital investigation, Vol. 10, Sept. 2013

2 Významné procesní instituty sloužící k zajištění elektronických důkazních prostředků

Jak již bylo uvedeno výše, trestní řád nabízí postupy, kterými mohou orgány činné v trestním řízení zajišťovat elektronická zařízení, či přímo data, ať už ve formě obrazových, zvukových či jiných záznamů, které mohou následně sloužit jako důkazní prostředky v rámci trestního řízení. Cílem této kapitoly je představit dané postupy a jejich specifika, potažmo problémy, které jsou spojeny s jejich aplikací na jednotlivé situace.

2.1 Odposlech a záznam telekomunikačního provozu

Odposlech a záznam telekomunikačního provozu představuje jeden z nejúčinnějších nástrojů pro opatřování důkazů a následného usvědčování pachatelů té nejzávažnější trestné činnosti a vzhledem k jeho roli v řadě mediálně známých kauz se jedná o institut, který je vnímán do jisté míry i laickou veřejností, ačkoliv v médiích může docházet k záměně „klasických" odposlechů s institutem sledování osob a věcí na základě § 158d odst. 3 trestního řádu, jehož problematice se věnuji níže.

Na úvod je vhodné uvést, že technickou realizaci odposlechů a záznamu telekomunikačního provozu provádí pro všechny orgány činné v trestním řízení Útvar zvláštních činností Služby kriminální policie a vyšetřování Policie ČR za součinnosti poskytovatelů služeb elektronických komunikací a konkrétní postupy tohoto útvaru podléhají utajenému režimu.[55] Za vyhodnocení odposlechu a záznamu telekomunikačního provozu je odpovědný policejní orgán, jelikož ten má k záznamu přístup jako první. Ačkoliv se tato činnost policejního orgánu vyznačuje významnou samostatností, garantem zákonnosti zůstává státní zástupce, jehož povinností je průběžně se seznamovat s vyhodnocením záznamu odposlechu.[56]

Tento postup získávání informací komunikovaných v reálném čase prostřednictvím sítí elektronických komunikací je upraven v trestním řádu ustanovením § 88. Jedná se o velmi citelný zásah do základních práv a svobod, konkrétně do práva na ochranu

[55] POLČÁK, R., PÚRY, F. a HARAŠTA, J. Elektronické důkazy v trestním řízení. Op. cit., s. 188
[56] Výkladové stanovisko Nejvyššího státního zastupitelství č. 1/2018 ze dne 11. 5. 2018 ke sjednocení výkladu zákonů a jiných právních předpisů při výkonu působnosti státního zastupitelství podle § 12 odst. 2 zákona č. 283/1993 Sb., o státním zastupitelství, ve znění pozdějších předpisů k problematice pořizování a nakládání s odposlechem a záznamem telekomunikačního provozu

soukromí. Z toho důvodu jsou zákonem upraveny striktní limitující podmínky, které musí být při využívání tohoto postupu respektovány. Prvně, postup lze užít jen v souvislosti s trestním řádem specificky vymezenými trestnými činy.[57]

Odposlech a záznam telekomunikačního provozu je možné realizovat na základě příkazu, který je oprávněn vydat předseda senátu a v přípravném řízení na návrh státního zástupce soudce. Příkaz má povahu rozhodnutí *sui generis*, přičemž proti němu není přípustný opravný prostředek. Z tohoto důvodu jsou kladeny přísnější nároky na obsahové a formální náležitosti takového příkazu, které doplňuje nad rámec zákona judikatura.[58]

V roce 2017 bylo Nejvyšším soudem (dále jen „NS“) vydáno významné usnesení (v souvislosti s mediálně známým případem Davida Ratha), kdy bylo dovozeno, že formální nedostatky příkazů je nutné posuzovat z formálně-materiálního hlediska, které vychází z principu materiálního právního státu. Soud dovodil, že formální nedostatky neznamenají automaticky nezákonnost příkazu, pokud jsou *věcně odůvodněny konkrétními skutkovými okolnostmi obsaženými v odůvodnění příkazů*. NS taktéž stanovil, že stejný požadavek se uplatní i u obdobných úkonů, tj. např. povolení ke sledování osob a věcí.[59] Soud tak v předmětném rozhodnutí vyjádřil, že náležitosti příkazu nelze posuzovat přepjatě formalistickým způsobem, který neodpovídá soudobé koncepci demokratického právního státu, aniž by tím současně snižoval požadavek na kvalitu příkazů.

Významnou otázku tvoří současně náležitosti návrhu státního zástupce na vydání příkazu k odposlechu. Dle výkladového stanoviska NSZ č. 1/2018 by měl takový návrh co do obsáhlosti a podrobnosti splňovat vyšší standard, jelikož úkolem takového návrhu je přesvědčit soud o jeho důvodnosti.[60]

Povolení odposlechu může následovat až po vniku důvodného podezření, že se nějaká osoba dopustila protiprávního jednání, a takové podezření je nezbytné podepřít

---

[57] Dle §88 odst. 1 trestního řádu je možné využít odposlechu je-li vedeno trestní řízení pro zločin, na který zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně osm let, dále v případě konkrétních trestných činů vypočtených v daném ustanovení nebo v případě jiného úmyslného trestného činu, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva. Zákonem č. 287/2018 Sb. došlo k rozšíření okruhu takových trestných činů.

[58] Usnesení Nejvyššího soudu ze dne 7. 6. 2017, sp. zn. 6 Tz 3/2017-II., uveřejněné pod č. 4156/2017 Sbírky soudních rozhodnutí a stanovisek, část trestní, dostupné na www.nsoud.cz

[59] Ibid

[60] Výkladové stanovisko Nejvyššího státního zastupitelství č. 1/2018 op. cit.

relevantními skutečnostmi.[61] Naopak, není tedy možné odposlech realizovat jen za účelem nahodilého odhalování trestné činnosti.

V případech vymezených v § 88 odst. 5 trestního řádu může orgán činný v trestním řízení nařídit odposlech a záznam telekomunikačního provozu i bez příkazu, s tím však musí souhlasit uživatel odposlouchávané stanice. Zde je nutné především rozlišovat pojmy účastník a uživatel. Účastníkem se rozumí osoba, která s poskytovatelem služby uzavřela smlouvu, kdežto uživatelem je každý, kdo danou službu využívá[62], kdy uživatelů bude zpravidla ve vztahu k telekomunikačnímu zařízení více, naopak účastník bude zpravidla jeden. Jako příklad může sloužit situace, kdy v souvislosti s domácí telefonní stanicí dá svolení dcera, jejíž otec uzavřel s poskytovatelem služby smlouvu.

Aby mohl být záznam telekomunikačního provozu použit jako *důkaz* je nezbytné k němu připojit protokol s uvedením údajů o místě, času, způsobu, o obsahu provedeného záznamu, jakož i o orgánu, který záznam pořídil.[63] Dle judikatury je absence údajů o místě, času, způsobu a obsahu pouze formální vadou, kterou lze zhojit v řízení před soudem, např. provedením dodatečného výslechu osob, zúčastněných na provedení zaprotokolovaného úkonu.[64] Zde lze namítnout, že v případě absence výše uvedených náležitostí, mohou vyvstat pochybnosti o tom, zda nedošlo k pořízení záznamu až po lhůtě uvedené v příkazu.[65] Na druhou stranu je třeba vzít v úvahu, že záznamy jsou vytvářeny pomocí automatického systému, nikoliv přímo konkrétní osobou a připojený protokol může být orgány činnými v trestním řízení vyhotoven i opožděně.

O nařízení odposlechu státní zástupce nebo policejní orgán a v řízení před soudem předseda senátu soudu prvého stupně následně dotčené osoby informují, přičemž informovaným osobám je zaručena následná ochrana před nezákonným zásahem orgánu veřejné moci prostřednictvím možnosti obrátit se na NS s návrhem na přezkoumání zákonnosti příkazu.[66]

---

[61] Nález Ústavního soudu ze dne 23. 05. 2007, sp. zn. II. ÚS 615/06, uveřejněné pod č. 88/2007 USn. Sbírky nálezů a usnesení ÚS, 45/2007
[62] Dle § 2 písm. a) a b) č. 127/2005 o elektronických komunikacích
[63] § 88 odst. 6 a 55 trestního řádu
[64] Usnesení Nejvyššího soudu ČR ze dne 8. 4. 2009, sp. zn. 3 Tdo 1301/2008
[65] ZAORALOVÁ, P. Procesní použitelnost důkazů v trestním řízení a její meze. Op. cit., s. 236
[66] § 88 odst. 8 trestního řádu

2.1.1 Aplikovatelnost ustanovení o odposlechu a záznamu telekomunikačního provozu

Výsledkem „tradiční“ podoby odposlechu a záznamu telekomunikačního provozu je zpravidla audiozáznam zachycující rozhovor účastníků odposlouchávané stanice. Audiozáznam pořizuje automatizované zařízení a zaznamenává se na nepřepisovatelné přenosné datové médium.[67] Po ukončení odposlechu dochází k vytvoření dvou datových nosičů, přičemž archivní nosič obsahuje záznam všech nahraných informací a důkazní nosič obsahuje pouze záznamy, které mají důkazní hodnotu. Právě tento důkazní nosič bude opatřen protokolem. V souladu s § 88 odst. 6 trestního řádu je policejní orgán povinen archivní nosič označit a spolehlivě jej uschovat tak, aby byla zajištěna ochrana před neoprávněným zneužitím. Ze stanoviska NSZ vyplývá, že policejní orgány postupují poměrně často v rozporu se zákonem, kdy do trestního spisu nezřídka kdy přikládají spolu s protokolem i archivní nosiče. Tato situace vede k neoprávněnému narušení práv třetích osob na ochranu soukromí.[68]

Pokud však budeme uvažovat o jiných variantách odposlechu, jejichž výstupem zpravidla budou nějaká data, bez expertní analýzy jen těžko člověku srozumitelná, bude takový výstup zpravidla zkoumat znalec či expertní pracoviště, aby byly poznatky získané odposlechem využitelné jako důkaz v trestním řízení.[69] Jako důkaz pak bude sloužit posudek znalce.

Mimo typické využití odposlechu telefonické komunikace přichází v úvahu i zajištění dat, která jsou přenášena elektronickými sítěmi v reálném čase. Pojem telekomunikační provoz dnes již neznamená pouze obsah telefonické komunikace, která je realizovaná prostřednictvím pevných linek či mobilních telefonů. V současné době zahrnuje tento pojem veškeré způsoby komunikace, které se uskutečňují v sítích elektronických komunikací, tj. zjevně i komunikace mezi výpočetní technikou.[70] To s sebou samozřejmě přináší řadu otázek. Takovou je například, jak je z časového hlediska ohraničena ochrana přenášených dat? K tomu lze užít výklad ÚS. Totiž že data, která jsou

[67] Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR za rok 2017, [online], [cit. dne 13. 4. 2019], dostupné na https://www.mvcr.cz/clanek/odposlechy-zaznamy-telekomunikacniho-provozu-a-sledovani-osob.aspx
[68] Výkladové stanovisko Nejvyššího státního zastupitelství č. 1/2018 op. cit.
[69] POLČÁK, R., PÚRY, F. a HARAŠTA, J.. Elektronické důkazy v trestním řízení. Op. cit., s. 190
[70] Ibid, s. 181 a násl.

v datovém nosiči již uložená, nejsou již předmětem telekomunikačního provozu, a tedy již nepožívají zvýšené ochrany.[71]

Pokud orgán činný v trestním řízení zajistí v rámci řádně provedené domovní prohlídky, či za použití jiných úkonů datové nosiče jako věci důležité pro trestní řízení, má oprávnění zkoumat data, která byla na datovém nosiči uložena k datu uvedeném v příkazu k takovému úkonu, a to bez toho, aby k zjišťování těchto dat musel opatřovat příkaz soudce.[72] V situaci, kdy budou na předmětný zajištěný nosič přicházet další sms zprávy, či zprávy prostřednictvím elektronické pošty či komunikace prostřednictvím nejrůznějších komunikačních aplikací (tzv. instant messaging), není již možné jejich obsah zjišťovat bez dalšího. Pokud by orgány činné v trestním řízení chtěly zjišťovat obsah komunikace v reálném čase, která byla uskutečněna až po zajištění takových datových nosičů, je nezbytné postupovat dle § 88 trestního řádu, a to s ohledem na skutečnost, že taková komunikace, uskutečňovaná v síti elektronických komunikací, podléhá telekomunikačnímu tajemství.[73]

Postup dle § 88 trestního řádu se uplatní také v případě zjišťování komunikace, která se odehrává v rámci elektronické pošty v reálném čase, přičemž orgány činné v trestním řízení nemají k dispozici žádný datový nosič a klíčová tak bude spolupráce s poskytovatelem služeb elektronických komunikací.[74]

V praxi však může nastat situace, kdy budou dané orgány namísto odposlechu zajišťovat údaje o obsahu takových e-mailových schránek až zpětně na základě příkazu dle § 158d odst. 3 trestního řádu a tento postup pak bude případně opakován. Z pohledu orgánů činných v trestním řízení je tento způsob jednodušší a především úspornější, nicméně otázkou zůstává nakolik je také legální. K postupu dle § 158d odst. 3 trestního řádu v souvislosti s obsahem elektronické pošty viz. níže.

---

[71] Usnesení Ústavního soudu ČR ze dne 3. 10. 2013 sp. zn. III. ÚS 3812/2012, uveřejněno pod č. 10/2013 ve Sbírce nálezů a usnesení ÚS, č. 71/2013

[72] Stanovisko Nejvyššího státního zastupitelství č. 4/2005 ze dne 6. června 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

[73] Tento závěr vychází ze stanoviska Nejvyššího státního zastupitelství č. 1/2015 ze dne 26. ledna 2015 ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek, dále z Usnesení Nejvyššího soudu ze dne 15. 12. 2000, sp. zn. 7 Tz 9/2000, publikováno pod č. 2091/2000

[74] Ibid

Problematika sledování e-mailové komunikace v reálném čase (s tím související problematika sledování dalších moderních komunikačních kanálů) není v současné právní úpravě jasně vymezena a podmínky použití přiléhavých institutů jsou ponechávány judikatuře, potažmo výkladovým stanoviskům NSZ. Nicméně, současná právní úprava odposlechu a záznamu telekomunikačního provozu se zdá být pro zajištění takové komunikace přiléhavá a striktní limity použití takového postupu zaručují legitimitu intenzivních zásahů do autonomní sféry jednotlivců. Problém však může nastat na straně příslušných orgánů, které se mohou s ohledem na absenci závaznosti výkladových stanovisek od tohoto postupu odchylovat.

2.2 Zjištění údajů o telekomunikačním provozu

Postup dle § 88a trestního řádu poskytuje orgánům činným v trestním řízení velmi účinný nástroj pro zjišťování informací o pachatelích trestné činnosti, a to do té míry, že ve spojení s právní úpravou tzv. *data retention* na základě zákona o elektronických komunikacích (dále jen „ZEK“)[75] umožňuje sestavit detailní komunikační profil jednotlivce, včetně záznamu o jeho pohybu. Pokud jde o charakter těchto dat jako důkazních prostředků, ve většině případů se jedná o důkazy nepřímé, především představují vodítka na počátku vyšetřování.[76] Pojem *data retention* reprezentuje povinnost primárně mobilních operátorů a poskytovatelů internetového připojení preventivně a plošně uchovávat provozní a lokalizační údaje svých uživatelů po dobu šesti měsíců zejména pro potřeby orgánů činných v trestním řízení.

Stejně jako v případě odposlechů lze tento postup využít jen ve vztahu k taxativně vyjmenovanému okruhu trestných činů (oproti odposlechům je možnost využití širší).[77] Primární odlišnost institutů zjištění údajů o telekomunikačním provozu a odposlechů pak spočívá v charakteru zajišťovaných informací. V rámci odposlechů dochází k zachycení samotného obsahu komunikace v reálném čase, naproti tomu zjištění údajů o telekomunikačním provozu se vztahuje k tzv. vedlejším údajům o již uskutečněné

[75] Zákon č. 127/2005 Sb., zákon o elektronických komunikacích a o změně některých souvisejících zákonů
[76] Nález Ústavního soudu ze dne 14. 5. 2019, sp. zn. Pl. ÚS 45/17, publikováno jako ÚS 1148/2019
[77] Postup je využitelný, je-li trestní řízení vedeno pro úmyslný trestný čin, na který zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně tři roky, pro taxativně vymezený okruh trestných činů uvedený v daném ustanovení nebo pro úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva, kterou je ČR vázána

komunikaci. Dikcí zákona se těmito vedlejšími rozumí provozní a lokalizační údaje (jinak lze taktéž hovořit o metadatech).

Postup konkrétněji zasahuje do práva na informační sebeurčení[78] vycházející z čl. 10 odst. 3 Listiny, které spočívá v garanci ochrany před neoprávněným shromažďování či jiným zneužíváním osobních údajů a do komunikační svobody vycházející z čl. 13 Listiny.[79] ÚS dovodil, že v určitých případech představují vedlejší údaje o komunikaci dokonce cennější důkazní prostředek než její obsah. Vedlejší údaje lze totiž strojově analyzovat a predikovat tak budoucí chování jedince.[80]

Provozní a lokalizační údaje vedou k ztotožnění zdroje a příjemce komunikace; typicky údaje týkající se data, času, délky a způsobu komunikace, konkrétně telefonní číslo, datum a čas odeslání sms zprávy, typ připojení, IP adresa, identifikátor protokolu elektronické pošty aj.[81].

Vydání údajů o telekomunikačním provozu nařizuje předseda senátu/samosoudce a v přípravném řízení soudce na návrh státního zástupce.[82] Jako důkaz pak bude v trestním řízení sloužit zpráva poskytovatele služeb o zjištění údajů o uskutečněném telekomunikačním provozu.[83]

Jako reakce na dosavadní judikaturu ESLP byl do trestního řádu zakotven požadavek na informování osoby uživatele, jehož se daná věc týkala, po vynesení pravomocného rozhodnutí ve věci, o nařízení sdělení údajů o uskutečněném telekomunikačním provozu.[84] Povinnost informovat uživatele mají orgány činné v trestním řízení v závislosti na fázi trestního řízení v níž došlo k pravomocnému skončení věci. Ve třetím odstavci ustanovení § 88a trestního řádu jsou pak vypočteny situace, kdy příslušné orgány povinnost uživatele o nařízení informovat nemají, např. poskytnutím informace by mohlo dojít ke zmaření účelu trestního řízení, či v případě

---

[78] Informační sebeurčení je konkretizováno v nařízení Evropského parlamentu a rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen „GDPR“)
[79] srov. nález sp. zn. II ÚS 789/06 ze dne 27. 9. 2007 (N 150/46 SbNU 489)
[80] Nález Ústavního soudu ze dne 14. 5. 2019, sp. zn. Pl. ÚS 45/17, publikováno jako ÚS 1148/2019
[81] Vyhláška č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů
[82] § 88a odst. 1 trestního řádu
[83] ŠÁMAL, P. Trestní řád: komentář. Op. cit., s. 1222 - 1237
[84] Srov. nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/10, publikováno ve Sbírce nálezů a usnesení ÚS, 60/2011, pod č. 52/2011 Usn.

ohrožení bezpečnosti státu, života, zdraví, práv a svobod osob.[85] Zde je třeba poznamenat, že ze strany orgánů činných v trestním řízení by určitě nemělo docházet k nadužívání vymezených důvodů.

Dotčeným osobám je následně poskytnuta garance ochrany práv v podobě možnosti obrátit se na NS s návrhem na přezkum zákonnosti soudního příkazu v souladu s § 88a odst. 2 trestního řádu. Ve vztahu k poskytnutí údajů o uskutečněném telekomunikačním provozu může nastat samozřejmě i situace, kdy sám uživatel telekomunikačního zařízení poskytne svolení, přičemž tento souhlas pak nahrazuje funkci příkazu.[86]

2.2.1 Data retention

Osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací, tj. právě výše zmínění mobilní operátoři a poskytovatelé datového připojení, jsou současně dle ZEK povinny preventivně a plošně uchovávat provozní a lokalizační údaje po dobu šesti měsíců a na požádání je bez zbytečného odkladu poskytnout orgánu činnému v trestním řízení pro účely a při splnění podmínek stanovených trestním řádem. Dále jsou tyto osoby povinny poskytnout provozní a lokalizační údaje Policii ČR např. pro účely pátrání po pohřešované osobě či za účelem ztotožnění nalezené mrtvoly, dále Bezpečnostní informační službě, Vojenskému zpravodajství a České národní bance pro účely stanovené zákonem.[87]

Právní úprava *data retention* (plošného uchovávání dat) přitom prošla zajímavým vývojem. Původní znění § 97 ZEK, které vycházelo z dnes již neexistující *data retention* směrnice[88], bylo posouzeno ÚS jako ústavně nekonformní, a došlo k derogaci části tohoto ustanovení. ÚS předchozí právní úpravě vytýkal především fakt, že přesně nevyplývalo, jaké orgány jsou oprávněny vyžádat si uchované údaje a také absenci jasně vymezeného legitimního cíle. To mělo za následek nadužívání tohoto postupu ze strany policejních

[85] ŠÁMAL, P. Trestní řád: komentář. Op. cit., s. 1192 - 1221
[86] § 88a odst. 4 trestního řádu
[87] §97 odst. 3 zákona č. 127/2005, rozsah těchto údajů, způsob předávání a likvidace stanoví blíže vyhláška č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů
[88] Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES byla zrušena Soudním dvorem EU (C-293/12 a C-594/12) „*Digital Rights Ireland Ltd"* ze dne 8. 4. 2014

orgánů i k odhalování méně závažné trestné činnosti.[89] Na konci roku 2011 došlo k derogaci původního znění § 88a trestního řádu, přičemž ÚS konstatoval, že meze základního práva na informační sebeurčení byly vyjádřeny příliš široce a neurčitě, když podmínka po daný postup zněla: *„musí vést k objasnění skutečností důležitých pro trestní řízení“.*[90]

Na jaře letošního roku se ÚS komplexně vyjádřil k otázce ústavní konformity současné právní úpravy *data retention* a § 88a trestního řádu. Soud došel k závěru, že stávající úpravu lze aplikovat ústavně konformním způsobem a není tak důvod pro její zrušení. Jeden z hlavních argumentů pro zachování současně platné úpravy zní, že absence legislativně upraveného principu *data retention* by vedla pouze k tomu, že se příslušné orgány budou uchylovat k alternativám, které mohou narušit soukromí jednotlivců ještě více invazivním a nepředvídatelným způsobem. Soud vyjádřil tezi, že současně platný rámec představuje *„menší zlo“*, než *„legislativní stín“*, který by nastal v případě zrušení. ÚS současně zkoumal, zda neexistují méně invazivní prostředky, které umožňují dosáhnutí téhož účelu. Došel k závěru, že využití provozních a lokalizačních údajů vhodnou alternativu nemá, a to i přesto, že zároveň uvádí srovnání se zahraničím, kde právě minimálně inspirační zdroje existují.[91] Domnívám se, že právní úprava sousedního Německa, kde došlo k výraznému omezení doby uchování dat a současně se zde uplatňují různá pravidla pro přístup k uchovaným datům v závislosti k závažnosti trestné činnosti, zaručuje vyšší standart ochrany za současného zachování efektivity daného nástroje. Je nutné podotknout, že ÚS současně uvedl, že uchování dat po dobu šesti měsíců nevybočuje z evropského rámce, což ale dostatečně neodůvodnil.

Dle většinového názoru pléna představuje plošné uchovávání údajů: *„snahu státu neztratit v době informační společnosti krok,“*[92] tak aby měly příslušné orgány k dispozici efektivní nástroje k zajištění ochrany bezpečnosti státu a jeho obyvatel. Domnívám se, že naplnění této teze lze docílit pouze za současného nastavení dostatečně omezujících podmínek proti neoprávněnému nakládání s údaji, jak uvádí v disentu Šimáčková.

---

[89] Nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/10, publikováno ve Sbírce nálezů a usnesení ÚS, 60/2011, pod č. 52/2011 USn.
[90] Nález Ústavního soudu ze dne 20. 12. 2011, sp.zn. Pl. ÚS 24/11, publikováno ve Sbírce nálezů a usnesení ÚS, 63/2011, pod č. 217/2011 USn.
[91] Nález Ústavního soudu ze dne 14. 5. 2019, sp. zn. Pl. ÚS 45/17, publikováno jako ÚS 1148/2019
[92] Ibid

Otázku, zda za současného stavu neabsentují potřebné záruky proti neoprávněnému nakládání se shromažďovanými údaji rozebírá Šimáčková podrobně. Problém stávající úpravy spočívá dle odlišného stanoviska zejména ve skutečnosti, že povinnost shromažďovat dotčené údaje náleží soukromým komerčním subjektům, kdy v podstatě chybí kontrola ze strany státu. Zákonodárce by měl respektovat minimální standart ochrany a zakotvit do právního řádu konkrétní a obecně platné záruky, konkrétní povinnosti shromažďujících subjektů, zejména konkrétní technická opatření.[93] Současně je třeba vzít v úvahu možnost zneužití shromažďovaných údajů ze strany soukromých subjektů právě ve spojení s možností automatizovaného profilování a předvídání chování jednotlivce. Tato praxe se dostala do centra pozornosti například v souvislosti v kauzou Cambridge Analytica.[94] Pro upřesnění je však nutné uvést, že právní úprava *data retention* se týká primárně mobilních operátorů a nedopadá na služby informační společnosti, tj. služby instant messagingu, apod.

Na závěr bych ráda poznamenala, že současně nastavená právní úprava § 88a trestního řádu nebere v úvahu situaci zajištění provozních a lokalizačních údajů týkajících se komunikace mezi obhájcem a obviněným. Na druhou stranu, údaje o tom, že obviněný v určitou dobu komunikoval se svým obhájcem s největší pravděpodobností nebudou pro orgány činné v trestním řízení nijak zvlášť využitelné.

2.3 Sledování osob a věcí

Jeden z druhů operativně pátracích prostředků – sledování osob a věcí – je upraven v části druhé, hlavy deváté trestního řádu, ustanovením § 158d. Jedná se o postup, který je v souvislosti se zajišťováním elektronických důkazů poměrně široce využitelný, např. pro zjišťování aktuálního obsahu elektronické pošty. Jedná se však také o institut, který přináší řadu problémů. Jedním z těch nejmarkantnějších je nedostatečná právní úprava sledování, kdy jsou pořizovány audiovizuální záznamy. Jak vyplývá

[93] Nález Ústavního soudu ze dne 14. 5. 2019, sp. zn. Pl. ÚS 45/17, publikováno jako ÚS 1148/2019, odlišné stanovisko

[94] CADWALLADR, C., GRAHAM-HARRISON, E., Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, [online], [cit. dne 2. 6. 2019], Dostupné na: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

z analýzy Policie ČR, v roce 2017 byl tento operativně pátrací prostředek využit v souvislosti s 1 120 živými spisy.[95]

S ohledem na povolovací režim rozlišit tři kategorie sledování:

- Prosté sledování;
- Sledování, při kterém jsou pořizovány zvukové, obrazové nebo jiné záznamy;
- Sledování, při kterém je zasahováno do nedotknutelnosti obydlí, do listovního tajemství nebo zjišťován obsah jiných písemností a záznamů uchovávaných v soukromí za použití technických prostředků.[96]

Prosté sledování není v souvislosti s elektronickými důkazními prostředky příliš významné, proto se v následujícím textu se zaměřuji na specifika zbývajících dvou kategorií.

2.3.1 Sledování, při kterém jsou pořizovány zvukové, obrazové nebo jiné záznamy

Právě tento postup představuje v poslední době v odborných kruzích poměrně diskutované téma, a to především z toho důvodu, že aktuální právní úprava se jeví jako zcela neodpovídající. Tento způsob sledování bývá označován jako tzv. prostorový odposlech. Dle Jelínka lze pojem vymezit jako: *„utajené získávání informací pomocí speciálních, pro tyto účely sestrojených technických prostředků a zařízení zaznamenávající obraz, zvuk, přesný pohyb i činnost sledovaných osob v reálném čase a prostoru.“*[97] Jinými slovy lze tento postup popsat jako sledování obrazu a/či zvuku na místě, kde je to z technického hlediska proveditelné. Ke sledování tak může docházet kdekoliv ve veřejném prostoru, v kavárenských a restauračních prostorách, ale i na pracovišti, a to za stejných povolovacích podmínek.[98] Ke sledování samozřejmě může docházet i v obydlí či ve vozidle, to však již bude spadat již do třetí, přísnější kategorie povolování. Provádění tohoto úkonu tak zcela zřejmě významně zasahuje do základních

[95] Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR za rok 2017, [online], [cit. dne 13. 4. 2019], dostupné na https://www.mvcr.cz/clanek/odposlechy-zaznamy-telekomunikacniho-provozu-a-sledovani-osob.aspx
[96] GŘIVNA, T. In: JELÍNEK, Jiří a kol. Dokazování v trestním řízení v kontextu práva na spravedlivý proces. Praha: Leges, 2018. ISBN 978-80-7502-287-5, s. 314 a násl.
[97] JELÍNEK, Jiří, K chybějící právní úpravě tzv. prostorového odposlechu v trestním řádu, Bulletin advokacie 7-8/2018, s. 13
[98] Ibid

lidských práv a svobod, jejichž ochrana je zaručena Listinou, zejména do práva na ochranu soukromí.

Pokud srovnáme účinky tzv. prostorového odposlechu ve smyslu zásahů do základních práv a svobod s postupy dle § 88 a § 88a trestního řádu, nutně dojdeme k závěru, že jejich intenzita je přinejmenším srovnatelná. Jejich povolovací režim však nastavuje naprosto odlišný standard ochrany. Sledování, při němž dochází k pořizování zvukových, obrazových nebo jiných záznamů je podmíněno pouze písemným povolením státního zástupce, přičemž omezení s ohledem na okruh trestných činů, kdy lze institut použít je značně širší, než u „klasického" odposlechu, jelikož institut lze použít v souvislosti s jakýmkoliv *úmyslným* trestným činem. Navíc lze tento postup v neodkladných případech zahájit i bez povolení. To je ale korigováno povinností policejního orgánu o povolení dodatečně požádat a pokud jej neobdrží do 48 hodin, povinností takové sledování ukončit, případný záznam zničit a informace, které se v této souvislosti dozvěděl, nijak nepoužít.

Autoři, kteří se touto problematikou v poslední době zabývají se přiklání k tomu, aby byla do trestního řádu zakotvena právní úprava tzv. prostorových odposlechů srovnatelným způsobem, jak je tomu právě u postupů dle § 88 a § 88a trestního řádu, nejlépe postavit ho jim naroveň. To především zakotvením soudního dohledu nad povolováním a zúžením okruhu trestných činů v jejichž souvislosti by bylo možné tento prostředek použít.[99] Další navrhují současně za účelem naplnění požadavků ESLP přistoupit k začlenění informační povinnosti vůči osobě, jíž se sledování týkalo, po pravomocném skončení věci.[100] S tím souvisí i zakotvení možnosti obrátit se na NS s návrhem na přezkum zákonnosti příkazu, s čímž trestní řád nyní nepočítá.

Při provádění tzv. prostorových odposlechů tedy dochází k intenzivním zásahům do ústavně garantovaných práv a svobod člověka. Ačkoliv většina ústavně zaručených práv není neomezitelná, takové omezení musí respektovat princip minimalizace zásahů do základních práv a svobod, přičemž musí být šetřeno jejich podstaty a smyslu v souladu s 4 odst. 4 Listiny. Tyto podmínky podle mého názoru současná právní úprava nesplňuje. Považuji za vhodné zakotvit minimálně vydání příkazu na základě povolení soudu.

---

[99] GŘIVNA, T., In: JELÍNEK, Jiří a kol. Dokazování v trestním řízení v kontextu práva na spravedlivý proces. Op. cit, s. 320

[100] ZAORALOVÁ, P. Procesní použitelnost důkazů v trestním řízení a její meze. Op. cit., s. 257

Ve prospěch zakotvení soudního příkazu se vyjádřila i Stálá komise pro použití použití odposlechů a záznamů telekomunikačního provozu, použití sledování osob a věcí a rušení provozu elektronických komunikací, kdy v roce 2017 požádala vládu o návrh zákona, jímž mělo dojít ke zpřísnění podmínek postupu dle § 158d odst. 2 trestního řádu.[101]

2.3.2 Sledování, kdy dochází k zásahu do ústavně garantovaných práv a svobod

Nyní se budu zaobírat třetí situací, tj. sledováním, při kterém je zasahováno do nedotknutelnosti obydlí, do listovního tajemství nebo zjišťován obsah jiných písemností a záznamů uchovávaných v soukromí za použití technických prostředků. K realizaci tohoto postupu je nezbytné povolení soudce, vydávané zejména na návrh státního zástupce.[102] Povolení je možné vydat jen na žádost (policejního orgánu či státního zástupce), která musí být odůvodněná podezřením na konkrétní trestnou činnost a jsou-li známy, též údaji o osobách či věcech, které mají být sledovány. ÚS k tomuto uvedl, že nepostačí jen vyslovení takového podezření, ale je nezbytné, aby bylo dán do souvislosti vztah sledované osoby a konkrétní trestné činnosti, k níž se podezření vztahuje.[103]

Konkrétně se zaměřím na význam toho institutu v souvislosti se zajišťováním obsahu e-mailových schránek. Elektronická pošta tvoří v současnosti jeden z nejvýznamnějších způsobů mezilidské komunikace, ačkoliv jej v rámci soukromého života dnes již nahrazují spíše webové komunikační aplikace, v rámci pracovního života tvoří prozatím nejvýznamnější komunikační platformu. Současně je tento prostředek využíván také pachateli trestné činnosti a údaje týkající se e-mailových schránek jsou tak předmětem zájmu orgánů činných v trestním řízení. Definici elektronické pošty v českém právním řádu obsahuje zákon č. 480/2004, o některých službách informační společnosti (dále jen „ZNSIS“). Dle § 2 písm. b) daného zákona se elektronickou poštou rozumí*: „textová, hlasová, zvuková nebo obrazová zpráva poslaná prostřednictvím veřejné sítě*

[101] Viz. Usnesení Stálé komise pro kontrolu použití odposlechů a záznamů telekomunikačního provozu, použití sledování osob a věcí a rušení provozu elektronických komunikací z 26. schůze ze dne 23. února 2017
[102] ŠÁMAL, P. Trestní řád: komentář. Op. cit., s. 2001-2011
[103] Nález Ústavního soudu, sp. zn. II.ÚS 2806/08 ze dne 27. 1. 2010, N 15/56 SbNU 143

elektronických komunikací, která může být uložena v síti nebo v koncovém zařízení uživatele, dokud ji uživatel nevyzvedne.“[104]

Orgány činné v trestním řízení musí brát v úvahu specifické vlastnosti tohoto způsobu komunikace, jelikož obsah elektronické pošty je do jisté míry pozměnitelný, a proto mu nelze přiřadit stejnou úroveň věrohodnosti jako například listinné zprávě zaslané prostřednictvím pošty, ačkoliv právě k běžné poštovní komunikaci bývá e-mail často přirovnáván.[105]

Praxe byla postavena před problém, jakým způsobem získávat data z e-mailových schránek. V této souvislosti je především nutné rozlišit následující situace:

- Situace zjišťování obsahu e-mailových schránek v reálném čase a zjišťování obsahu elektronické komunikace, která bude uskutečněna po zajištění datového nosiče orgány činnými v trestním řízení – v tomto případě je nutné postupovat dle ustanovení o odposlechu, viz. výše, v kapitole 2.1.
- Situace zjišťování aktuálního obsahu e-mailových schránek ze zajištěného datového nosiče – datové nosiče budou orgány činnými v trestním řízení zajišťovány prostřednictvím odnětí, vydání věci, či v rámci domovní prohlídky. Po zajištění bude zpravidla následovat expertní zkoumání dotčených věcí, přičemž zákon nestanovuje další omezující podmínky pro provádění takových zkoumání, např. právě uložených zpráv elektronické pošty.[106]
- Situace zjišťování aktuálního obsahu e-mailových schránek, pokud orgány činné v trestním řízení nemají k dispozici datový nosič.

V souvislosti s postupem dle § 158d odst. 3 trestního řádu nás bude zajímat třetí situace, tedy zjištění obsahu, aniž by měly orgány činné v trestním řízení datový nosič k dispozici. Z aktuálního obsahu e-mailové schránky lze zjistit přijaté a odeslané zprávy, koncepty rozepsaných zpráv, a prostřednictvím odborné analýzy i zprávy, které byly uživatelem již smazané. Charakteristickým rysem elektronické pošty je, že uživatel e-mailové schránky může k jejímu obsahu přistoupit z jakéhokoliv počítače či obdobného zařízení po zalogování, tj. po zadání přístupového jména a hesla. E-mailová schránka má tedy povahu jakéhosi *„quasi datového internetového úložiště“* a její obsah podléhá

[104] Zákon č. 480/2004 Sb. o některých službách informační společnosti a o změně některých zákonů
[105] POLČÁK, R., PÚRY, F. a HARAŠTA, J. Elektronické důkazy v trestním řízení. Op. cit., s. 177 a násl.
[106] Ibid, s. 121

ústavní ochraně soukromí a listovního tajemství. Dikcí zákona se jedná o jiné záznamy uchovávané v soukromí za použití technických prostředků.[107] K režimu povolení přístupu k aktuálnímu obsahu elektronické pošty přistupovaly orgány činné v trestním řízení v minulosti rozdílně, ačkoliv většina se klonila spíše k přístupu dle § 158d odst. 3 trestního řádu, v některých případech byl volen režim dle § 88a trestního řádu či dokonce dle ustanovení o součinnosti § 8 odst. 1 trestního řádu. Na roztříštěnou rozhodovací praxi reagovalo NSZ vydáním výkladového stanoviska č. 1/2015. V něm bylo vyloženo, že v případě zajišťování aktuální obsahu e-mailových schránek mají jít orgány činné v trestním řízení právě postupem dle § 158d odst. 3 trestního řádu, jelikož poskytovatelé služby elektronické pošty neukládají preventivně obsah schránky, ten je zajišťován ve stavu ke dni, kdy jej poskytovatel zachytí dle příkazu. Postup dle § 8 trestního řádu nelze užít k prolomení ústavně zaručených práv, a postup k zjištění údajů o telekomunikačním provozu není vhodný k zajištění obsahu elektronické komunikace.[108] Ve stanovisku bylo taktéž poukázáno na usnesení ÚS, kdy bylo vyvozeno, že *„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“*[109] Z toho bylo analogicky dovozeno, že postup se uplatní i v případě obsahu elektronické pošty.

Je vhodné poznamenat, že stanovisko nepočítá se skutečností, že hlavičky e-mailových zpráv obsahují provozní a lokalizační údaje, např. IP adresy. Což vyvolává otázku, zda je za použití § 158d odst. 3 trestního řádu zajištěna dostatečná ochrana práv jednotlivců.

Aby bylo možné záznamy pořízené při sledování použít jako důkaz, je nezbytné k nim připojit protokol. [110]

---

[107] 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
[108] Výkladové stanovisko Nejvyššího státního zastupitelství, č. 1/2015 op. cit.
[109] Nález Ústavního soudu, sp. zn. III.ÚS 3812/12 ze dne 3. 10. 2013, U 10/71 SbNU 573
[110] § 158d odst. 7 trestního řádu

2.4 Vydání a odnětí věci

Neopomenutelný postup používaný k zajišťování elektronických důkazů je institut upravený v ustanoveních § 78 a 79 trestního řádu, tedy vydání a odnětí věci. Jedná se o jeden z nejčastějších postupů, který orgány činné v trestním řízení k zajištění důkazů používají. Je tomu tak zejména proto, že data důležitá pro trestní řízení se často nacházejí na komponentech nejrůznější výpočetní techniky, tedy v počítačích, v mobilních telefonech, na různých paměťových médiích. Tyto předměty jsou pak věcmi důležitými pro trestní řízení. Kdo má takové věci u sebe, bude mít na vyzvání ediční povinnost vůči orgánu činném v trestním řízení. Ediční povinnost se však nevztahuje na nosič informací, jehož obsah se týká skutečností, o nichž platí zákaz výslechu, pokud nedojde ke zproštění povinnosti mlčenlivosti. Uplatní se zde také *zásada zákazu sebeobviňování*, kdy nelze obviněného donucovat k vydání důkazu, který svědčí v jeho neprospěch.[111]

Zde bych chtěla poukázat na zakotvení nové skutkové podstaty trestného činu maření spravedlnosti do trestního zákoníku, zákonem č. 287/2018 Sb. Dle § 347a trestního zákoníku nyní hrozí trest odnětí svobody až na dvě léta za jednání, kdy osoba předloží v řízení před soudem padělaný či pozměněný *věcný či listinný* důkazní prostředek v úmyslu, aby byl použit jako pravý, anebo důkazní prostředek padělá či pozmění v úmyslu použít ho jako pravý. Nová právní úprava sice není v zásadě v rozporu se zásadou zákazu sebeobviňování, nicméně se může jevit jako poněkud nelogická. Pokud nemůže být obviněný trestán za křivou výpověď, nabízí se otázka, z jakého důvodu by měl být trestán, pokud bude svá tvrzení podporovat falešnými důkazy.

Pokud není výzvě k předložení věci vyhověno, může orgán činný v trestním řízení přistoupit k razantnějšímu řešení, které je na místě v případě, že osoba dobrovolně nesplní ediční povinnost. Příkaz k odnětí věci vydává předseda senátu a v přípravném řízení státní zástupce nebo policejní orgán. Pokud odnětí věci nevykoná orgán příkaz vydávající, provede tento úkon dle § 79 trestního řádu policejní orgán s předchozím souhlasem státního zástupce, či sám, pokud věc nesnese odkladu. O provedení výše uvedených úkonů se sepíše protokol v souladu s § 55 odst. 1 trestního řádu.[112]

---

[111] HERZEG, J., Zásada „nemo tenetur" a práva obviněného v trestním řízení, Bulletin advokacie 1-2/2010, s. 38

[112] POLČÁK, R., PÚRY, F. a HARAŠTA, J. Elektronické důkazy v trestním řízení. Op. cit., s. 74

2.5 Domovní prohlídka, prohlídka jiných prostor a pozemků, vstup do obydlí, jiných prostor a pozemků

Je-li důvodného podezření, že se v určitém obydlí či jiných prostorách nachází věci důležité pro trestní řízení, což jsou v případě elektronických důkazních prostředků zejména komponenty výpočetní techniky, datové nosiče, a jiné, je možné, aby za účelem jejich zajištění provedl policejní orgán domovní prohlídku či prohlídku jiných prostor a pozemků, a to v souladu s podmínkami stanovenými trestním řádem v § 82 a násl. Pokud existuje důvodné podezření, že takové věci má u sebe určitá osoba, je možné vykonat v souladu s § 82 odst. 3 trestního řádu osobní prohlídku. Na místě bude zpravidla přítomen kriminalistický technik, který zajistí správnou manipulaci s předmětnou technikou tak, aby nedošlo ke kontaminaci zařízení a ztrátě významných dat.[113]

Tyto postupy opět představují významný zásah do základních lidských práv a svobod, tudíž je nezbytné respektovat přesně vymezená pravidla při jejich provádění. Následkem jejich nedodržení je totiž absolutní neúčinnost důkazu, tedy jeho nepoužitelnost pro účely trestního řízení.[114] Při provádění prohlídek se střetává právo na nedotknutelnost obydlí a právo na respektování soukromého života se zájmem na ochraně demokratické společnosti před trestnou činností. Domovní svoboda taktéž velmi úzce souvisí s nedotknutelností osobní integrity jedince.

Čl. 12 Listiny ve svém druhém odstavci možnost provedení domovní prohlídky pro účely trestního řízení přímo předpokládá. Prohlídku nařizuje pouze soud, a to předseda senátu nebo v přípravném řízení na návrh státního zástupce soudce.[115] S ohledem na výjimečný charakter takového zásahu je nezbytné, aby byl příkaz dle § 83 odst. 1 trestního řádu a § 83a odst. 1 trestního řádu soudem náležitě odůvodněn, přičemž za nedostačující odůvodnění je považováno prosté odkázání na zákonná ustanovení, bez toho, aby bylo zřejmé, na základě jakých skutkových okolností byl takový příkaz vydán.[116] Podle § 83a trestního řádu je provedení prohlídky jiných prostor nebo pozemků

---

[113] POLČÁK, R., PÚRY, F. a HARAŠTA, J. Elektronické důkazy v trestním řízení. Op. cit., s. 201

[114] K následkům nedodržení zákonných podmínek osobní prohlídky se vyjádřil Nejvyšší soud ve svém usnesení ze dne 4. 8. 2010, sp. zn., 7 Tdo 783/2010, publikováno v Souboru trestních rozhodnutí NS, č. 70/2010, pod č. T 1331, analogicky lze dovodit, že se vztáhne i institut domovní prohlídky a prohlídky jiných prostor a pozemků

[115] §83 odst. 1 a 83a odst. 1 trestního řádu

[116] Nález Ústavního soudu ze dne 28. 4. 2009, sp. zn. I. ÚS 536/06, publikováno ve Sbírce nálezů a usnesení ÚS, č. 53/2009, pod č. 100/2009 USn.

možné i policejním orgánem bez příkazu, a to za podmínek, že vydání příkazu nelze předem dosáhnout a věc nesnese odkladu nebo pokud uživatel dotčených prostor nebo pozemků písemně prohlásí, že s prohlídkou souhlasí, a své prohlášení předá policejnímu orgánu.

S ohledem na zákonnost příkazu je zajímavé usnesení ÚS, sp. zn. IV. ÚS 3225/09 ze dne 14. 12. 2011. V daném případě bylo v odůvodnění příkazu uvedeno podezření, že z IP adresy Z uživatele X bylo přistupováno do schránky elektronické pošty XX@XX.cz, z níž odcházel a do níž přicházel obsah mající povahu dětské pornografie. IP adresa Z však byla nesprávná, chybou státního zástupce byla převzata z jiného spisu. Soud však dovodil, že tato chyba neměla vliv na zákonnost příkazu, a to proto, že podstatné bylo především to, že domovní prohlídka měla být provedena u uživatele IP adresy X, z níž se pachatel připojoval do výše uvedené schrány elektronické pošty. Ačkoliv v příkazu k nařízení domovní prohlídky byla uvedená adresa s uživatelem nesouvisející, z obsahu spisu vyplývalo, že prověřování policejního orgánu skutečně směřovalo vůči IP adrese X.[117]

Domovní prohlídka může být vykonána i jako neodkladný a neopakovatelný úkon, tedy ještě před zahájením trestního stíhání. Aby byl takový postup proveden v souladu se zákonem, je nutné, aby byl příkaz k domovní prohlídce vydán s odůvodněním toho, že jde o neodkladný a neopakovatelný úkon.[118] O provedení neodkladného a neopakovatelného úkonu se pořídí protokol, kde je vždy nezbytné uvést, na základě jakých skutečností byl úkon za neodkladný a neopakovatelný považován.[119] K této problematice se vyjadřuje i výkladové stanovisko NSZ č. 2/2017. Zde je vyjádřeno, že při tzv. testu činnosti trojí kontroly (policejní orgán-státní zástupce-soud) je pro posouzení legality neodkladnosti a/nebo neopakovatelnosti třeba zhodnotit, zda byl policejním orgánem podán řádně odůvodněný návrh státnímu zástupci a následně soudci. Současně je klíčové, zda je neodkladnost či neopakovatelnost řádně zachycena ve spisovém materiálu.[120]

---

[117] Usnesení Ústavního soudu ze dne 14. 12. 2011, sp. zn. IV. ÚS 3225/09, publikováno pod č. ÚS 3555/2011

[118] Nález Ústavního soudu, sp. zn. IV. ÚS 1780/07, publikováno ve Sbírce nálezů a usnesení ÚS, č. 50/2008, pod č. 147/2008 USn.

[119] § 160 odst. 4 trestního řádu

[120] Výkladové stanovisko Nejvyššího státního zastupitelství č. 2/2017 ze dne 30. 8. 2017 ke sjednocení výkladu zákonů a jiných právních předpisů k některým otázkám postupu státního zástupce při podávání návrhů a provádění domovních prohlídek a prohlídek jiných prostor a pozemků

V souvislosti se zajišťováním počítačů a jiných datových nosičů při provádění domovní prohlídky a prohlídky jiných prostor a pozemků bylo NSZ vypracováno výkladové stanovisko.[121] To vyjádřilo premisu, že za splnění podmínek trestního řádu pro nařízení domovní prohlídky a obdobně, lze zajistit výpočetní techniku a datová média, i pokud existuje možnost, že se na takových zařízeních nacházejí informace, které nesouvisejí s trestním řízením a ke kterým se váže povinnost mlčenlivosti. Stanovisko se též vyjádřilo k otázce, zda má být prohlédnutí datových nosičů vykonáno na místě, či až následně v prostorách expertního pracoviště, a to tak, že na tuto otázku neexistuje paušální odpověď a vždy bude záležet na okolnostech, jako je například přítomnost příslušného znalce.[122] V případě zajištění datových nosičů, kdy existuje předpoklad dokumentů podléhajících mlčenlivosti, může nastat problém nedostatečného zabezpečení takových nosičů. Při neodborném nakládání s datovými nosiči současně hrozí ztráta potencionálně důležitých dat.

V souvislosti se státem uznanou povinností mlčenlivostí je zajímavá problematika domovních prohlídek nebo prohlídek jiných prostor, v nichž advokát vykonává advokacii, konkrétně otázka rozsahu situací, kdy jsou orgány činné v trestním řízení povinny postupovat dle § 85b trestního řádu. Ten stanoví, že při provádění prohlídky „*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 úkon povinen vyžádat si součinnost České advokátní komory*.“

Pokud zástupce Komory odmítne udělit souhlas k seznámení orgánů činných v trestním řízení s předmětným obsahem, je možné takový souhlas nahradit rozhodnutím příslušného soudce.[123] Taková situace nastala v případě, kterému se věnuje usnesení Městského soudu v Praze ze dne 9. 7. 2014. Soud zde jazykovým výkladem daného ustanovení došel k názoru, že úložiště serverů externí účetní společnosti není místem, kde advokát vykonává advokacii, potažmo, že takovým místem nejsou ani jiné prostory sloužící k úschově datových serverů. Dle názoru soudu je třeba k situacím, na které se vztahuje ochrana dle § 85b trestního řádu přistupovat restriktivně.[124] Soud tedy tímto

---

[121] Výkladové stanovisko Nejvyššího státního zastupitelství č. 9/2001 ze dne 13. června 2001 k zajišťování počítačů a jiných nosičů informací při domovní prohlídce a prohlídce jiných prostor a pozemků
[122] Ibid
[123] § 85b odst. 3 trestního řádu
[124] Usnesení Městského soudu v Praze ze dne 9. 7. 2014, sp. zn. Nt 615/2014, publikováno v Bulletinu advokacie, 11/2014 jako BA11/2014, s. 51

výkladem vyloučil z ochrany nejen datová uložiště, ale i prostory jako například hotelové pokoje či restaurační zařízení. Tento závěr však neodpovídá realitě, kdy v dnešní době není výjimkou, že advokáti poskytují služby např. i během doby dovolené.

V souvislosti s výše uvedenou problematikou vydáno sjednocující stanovisko NS, sp. zn. Tpjn 306/2014, ve kterém byl vyjádřen názor opačný. Dle názoru soudu se postup podle § 85b trestního řádu *„uplatní i u ostatních v úvahu přicházejících míst vztahujících se k výkonu advokacie, v nichž lze ukládat, zpracovávat a využívat informace o klientech, jichž se dotýká povinnost mlčenlivosti advokáta“.* Daný postup se tedy uplatní i ve vztahu k vlastním uložištím dat, které se mohou nacházet mimo místo běžného výkonu advokátní praxe, ale i k uložištím umožňující dálkový přístup, jako jsou cloudové a hostingové služby.[125] Soud došel k tomuto názoru teleologickým výkladem předmětného ustanovení. Byl tedy vzat v úvahu jeho účel, který zjevně směřuje k rozšíření ochrany klientů advokátů, nikoliv k jejímu zúžení.

Podle mého názoru by bylo vhodné nahradit či doplnit slovo listiny v rámci znění § 85b odst. 1 trestního řádu například pojmem dokumenty, což lépe odpovídá současné realitě, kdy se dnes téměř veškerá dokumentace související s výkonem advokacie nalézá v elektronické podobě. V současnosti navíc advokátní kanceláře stále více využívají služeb cloudových uložišť, jejichž nespornou výhodou je, že mimo velkého úložného prostoru poskytují velmi vysokou úroveň ochrany dat.

2.6 Uchování dat důležitých pro trestní řízení

Pokud je třeba zachovat elektronický důkaz a předejít jejího zničení či pozměnění, mají nově orgány činné v trestním řízení k dispozici speciální ustanovení, které umožňuje nařídit osobě, která má určitá data ve své moci, uchování těchto dat po určitou dobu v nezměněné podobě.[126] Nové ustanovení § 7b trestního řádu vychází z mezinárodních závazků, konkrétně je reakcí na požadavky Úmluvy o počítačové kriminalitě. Tatáž novela zakotvila ustanovení § 65a ZMJS, které umožňuje přeshraniční uchování dat.

Z dikce § 7b trestního řádu lze rozlišit dvě potencionální situace. Na základě prvního odstavce lze subjektům, které drží či mají pod kontrolou určitá data nařídit, aby

[125] Stanovisko Nejvyššího soudu ze dne 25. 6. 2015, Tpjn 306/2014, uveřejněno pod č. R 35/2015 tr. ve Sbírce soudních rozhodnutí a stanovisek, 7/2015
[126] Institut byl zakotven novelou trestního řádu, zákonem č. 287/2018 Sb., který je účinný od 1. 2. 2019

tato data uchovaly po určitou dobu v nezměněné podobě. Doba nesmí přesáhnout 90 dnů. Současně musí být splněny dva předpoklady. Data musí být důležitá pro trestní řízení a je nezbytné zabránit jejich ztrátě, zničení či pozměnění. V příkazu lze současně nařídit utajení informace o tom, že došlo k nařízení uchování. Utajení je opodstatněné zejména, kdy se řízení nachází ve fázi prověřování a prozrazení by jeho průběh mohlo ohrozit.[127]

Na základě druhého odstavce pak lze nařídit znemožnění přístupu k těmto datům, aby bylo zabráněno v pokračování či opakování v trestné činnosti. Tato situace jde nad rámec požadavků Úmluvy o počítačové kriminalitě.[128]

Pojem *„data důležitá pro trestní řízení"* představuje pro trestní řád novinku. Jedná se o počítačová a provozní data, která jsou uložena v počítačovém systému či na nosiči informací, u nichž hrozní ztráta, zničení či pozměnění. Z účelu ustanovení lze dovodit, že se jedná zejména o data uchovávána po krátkou dobu.[129]

Tato data musí být v příkazu specifikována a konkrétně označena. K vydání příkazu je oprávněn předseda senátu a přípravném řízení státní zástupce nebo policejní orgán. Policejní orgán však musí mít k takovému kroku předchozí souhlas státního zástupce. Bez předchozího souhlasu státního zástupce může policejní orgán vydat příkaz jen za předpokladu, že věc nesnese odkladu a souhlasu nelze dosáhnout.[130]

Osobou mající data důležitá pro trestní řízení pod kontrolou či taková data držící bude typicky správce dat. Jelikož data důležitá pro trestní řízení téměř vždy obsahují osobní údaje, dotýká se tato právní úprava i problematiky ochrany osobních údajů. Dle terminologie GDPR se správcem dat rozumí: *„fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů"*[131] GDPR současně stanoví povinnost správce uchovávat osobní údaje jen po dobu nezbytně nutnou k účelu zpracování.[132] Což se s novou právní úpravou nepochybně střetává. Na druhou stranu jistě do menší míry než právní úprava *data retention*. Správcem dat, vůči kterému budou žádosti o uchování dat

---

[127] Důvodová zpráva, č. 287/2018 Dz, k zákonu č. 287/2018 Sb. kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a některé další zákony [online], str. 34-38, 50-52 [cit. 21. 3. 2019], Dostupné z: https://www.psp.cz/sqw/text/tiskt.sqw?O=8&CT=79&CT1=0
[128] DOSTÁL, O., Zajišťování důkazů u počítačové kriminality – dožádání, vydání věci a prohlídky (1. díl), Trestněprávní revue, 3/2019, s. 66
[129] Důvodová zpráva, č. 287/2018 Dz, op. cit.
[130] § 7b trestního řádu
[131] Čl. 4, bod. 7 GDPR
[132] Čl. 5, bod. 1 e) GDPR

směřovat, bude typicky poskytovatel služeb informační společnosti a poskytovatel služeb elektronických komunikací.[133]

Služby informační společnosti jsou upravené tzv. e-commerce[134] směrnicí, transponovanou do českého právního řádu ZSIS.[135] Mezi předmětné služby se pak řadí takzvané *mere conduit, catching* a *hosting.*

Mere conduit: nebo-li služba datového připojení, jinak definována jako prostý přenos dat, je v zásadě službou, díky které může uživatel využívat internetové připojení, tj. Wi-Fi, 4G, LTE připojení. Poskytovatelem bude zpravidla operátor, či v případě veřejně přístupných sítí ten, kdo danou síť provozuje, např. univerzity, provozující síť Eduroam.[136] Dále do této kategorie spadají i poskytovatelé služeb tzv. instant messagingu, přičemž okamžitý přenos zpráv se odehrává a aplikacích jako jsou WhatsApp, Facebook Messenger, Viber a obdobně[137], dále služby VoIP, kterou lze popsat jako telefonování skrze internet, tedy např. Skype.

Catching: tato služba spočívá v automatickém dočasném meziukládání dat, což umožňuje snížení komunikační zátěže při vyhledávání a přenosu těchto dat dalšími uživateli. Typickým poskytovatelem bude tzv. *proxy cache provider* či poskytovatel služeb *internetových vyhledávačů.*[138]

Hosting: tato služba spočívá v ukládání informací poskytnutých uživatelem, pod tímto pojmem tedy nalezneme provozovatele datových a webových uložišť. Do této kategorie patří i sociální sítě, on-line tržitště či komunitní portály, cloudová uložiště. Konkrétně se jedná např. o Youtube, Facebook, Hellspy, atd.[139]

Právní úpravu týkající se poskytovatelů služeb elektronických komunikací najdeme v ZEK. Mezi takové služby patří telekomunikační provoz zajišťovaný veřejnými

---

[133] Důvodová zpráva, č. 287/2018 Dz, op. cit.
[134] Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu)
[135] Zákon č. 480/2004 Sb. o některých službách informační společnosti a o změně některých zákonů
[136] KORBEL, F., Ne-odpovědnost poskytovatelů služeb informační společnosti v digitálním světě, Právní prostor, 17. 5. 2018, MAISNER, M.: Zákon o některých službách informační společnosti. Komentář. 1. vydání. Praha: C. H. Beck, 2016, s. 39-49
[137] HARAŠTA, J. Obecná prevenční povinnost poskytovatele služeb informační společnosti ve vztahu k informacím ukládaným uživatelem, Právní rozhledy 17/2014, s. 590
[138] MAISNER, M.: Zákon o některých službách informační společnosti. Komentář. Op. cit., s. 50-59, dále Harašta, J. Obecná prevenční povinnost poskytovatele služeb informační společnosti ve vztahu k informacím ukládaným uživatelem, Právní rozhledy 17/2014, s. 590
[139] MAISNER, M.: Zákon o některých službách informační společnosti. Komentář. 1. Op. cit., s. 60-98

telefonními sítěmi, dále služby elektronických komunikací, které jsou zajišťované prostřednictvím veřejných komunikačních sítí, realizovaných na základě přenosu informací, tj. služby na internetu, jako je například e-mailová komunikace.[140]

Představuje však nová právní úprava pro orgány činné v trestním řízení přelomovou novinku? Nikoliv, samotná žádost orgánů činných v trestním řízení o tzv. „zmražení dat" je již zavedenou praxí. Dosud však oprávněné orgány využívaly obecného ustanovení o součinnosti, tj. §8 odst. 1 trestního řádu[141], jehož účelem je spíše zjišťování údajů obecnějšího charakteru, bez vazeb na konkrétní osoby. Například zjištění skutečnosti, jakým způsobem funguje určitý program. Současně si lze představit, že toto ustavení lze užít k získání veřejných údajů z uživatelského profilu na sociální síti.[142]

Je tak zjevné, že zakotvením speciálního pravidla, jež stanovuje transparentní povolovací podmínky, dochází k posílení ochrany práv a svobod jednotlivců před libovůlí orgánů veřejné moci. Pravidlo dle §8 odst. 1 trestního řádu v případě absence speciálního ustanovení mnohdy představuje jakýsi univerzální recept. Nicméně v případě, kdy existuje speciální právní úprava, je nezbytné, aby orgány činné v trestním řízení postupovaly v souladu. Protiústavnost důkazů získaných v rozporu s tímto pravidlem lze analogicky dovozovat z judikatury ÚS, která vyjádřila tuto tezi ve vztahu § 8 odst. 1 a § 88a trestního řádu.[143]

Vystačit si při získávání údajů o uživatelích s prostým dožádáním neobstojí ani ve světle judikatury ESLP. V případě Benedik proti Slovensku[144], který se týkal rozšiřování dětské pornografie za použití peer-to-peer sítě, si slovinské policejní orgány vyžádaly (pouhým dožádáním bez povolení soudu) od poskytovatele datového připojení údaje týkající se určité IP adresy. Poskytnuté údaje vedly ke ztotožnění stěžovatele a na základě důkazů zajištěných při domovní prohlídce byl stěžovatel odsouzen. ESLP v daném případě dovodil, že ochrana soukromí ve smyslu čl. 8 Úmluvy se vztahuje i na online aktivity. Soud taktéž dovodil, že v daném případě chyběly dostatečné záruky proti zásahu do práva na soukromí a dovodil, právo stěžovatele bylo porušeno.

---

[140] § 2 písm. h), i), k) zákona č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů
[141] KOLOUCH, J., CyberCrime. Praha: CZ.NIC, z. s. p. o., 2016, ISBN 978-80-88168-18-8, s. 416.
[142] DOSTÁL, O., Zajišťování důkazů u počítačové kriminality – dožádání, vydání věci a prohlídky (1. díl), Trestněprávní revue, 3/2019, s. 66
[143] Ibid
[144] Rozsudek ESLP Benedik proti Slovinsku, č. 62357/14.

Účelem výše rozebraného příkazu je ochrana dat. Za problematické považuji, že v případech, kdy se osoba, vůči ní takový příkaz směřuje, nejeví jako důvěryhodná, je zřejmě lepší přikročit přímo k jejich zajištění. Dle dosavadní zkušenosti kpt. Mgr. Terezy Andělové[145] dotčené subjekty zatím na příkaz reagují velmi pomalu (tzn. v řádech několika týdnů) a přímé zajištění dat se zatím jeví jako rychlejší a efektivnější. Lze však předpokládat, že se jedná pouze o přechodný stav, který ustane, až se dotčené subjekty naučí na novinku reagovat.

Lze si taktéž představit, že tzv. „zmražení dat" by mohlo po vzoru např. Slovenska za současné úpravy podmínek přístupu k datům na základě § 88a trestního řádu představovat vhodnou alternativu k dosavadní právní úpravě *data retention*.

Na závěr bych ráda poznamenala, že na úrovni EU pokračuje proces k přijetí nového nařízení, které cílí na zakotvení evropského předávacího a uchovávacího příkazu elektronických důkazů, k tomu ale blíže v poslední kapitole této diplomové práce.

2.7 Shrnutí

Ačkoliv nejsou výše uvedené postupy bez problémů, jejich do jisté míry obecná povaha umožňuje, aby byly užity k zajišťování elektronických důkazních prostředků. Konkretizace situací jejich využitelnosti je ponechávána judikatuře soudů a výkladovým stanoviskům NSZ. Zde bych však ráda poznamenala, že vzhledem k nezávaznosti výkladových stanovisek, může docházet k jejich nerespektování ze strany orgánů činných v trestním řízení.

Zavedením tzv. předběžného uchovávacího příkazu byl zakotven institut, který může podle mého názoru do jisté míry sloužit jako alternativa k plošnému preventivnímu uchování údajů na základě § 97 odst. 3 a 4 ZEK.[146] Z hlediska *de lege ferenda* by bylo za účelem posílení ochrany práv jednotlivců vhodné přistoupit k zostření podmínek použití § 88a trestní řádu. Lze si představit například odstupňování přístupu k datům v závislosti na závažnosti trestné činnosti.

Ráda bych dodala, že výše uvedené postupy bývají ze strany orgánů činných v trestním řízení často kombinovány. Typicky si lze představit situaci, kdy bude na

[145] Vrchní komisařka Služby kriminální policie a vyšetřování Odboru analytiky a kybernetické kriminality Policie ČR, KŘP Plzeňského kraje
[146] Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů

základě informací z odposlechů či zjišťování údajů o telekomunikačním provozu provedena domovní prohlídka, při níž se bude zajišťovat výpočetní technika. Pro analýzu zabavené výpočetní techniky pak bude přibrán znalec. V případě zabavení datových nosičů, typu CD-Rom, např. pro podezření z přechovávání dětské pornografie bude na místě i ohledání takových CD-Romů ze strany policejního orgánu. Ze statistiky Policie ČR vyplývá, že poměrně časté je taktéž kumulativní užití odposlechů a sledování osob a věcí v téže věci. V roce 2017 tomu tak bylo v souvislosti s 477 živými spisy.[147]

[147] Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR za rok 2017, [online], [cit. dne 13. 4. 2019], dostupné na https://www.mvcr.cz/clanek/odposlechy-zaznamy-telekomunikacniho-provozu-a-sledovani-osob.aspx

3 Dokazování pomocí informací ze sociálních sítí

3.1 Pojem sociální síť

Sociální sítě, či sociální média tvoří celosvětový komunikační fenomén moderní doby.[148] Z pohledu českého práva jsou společnosti poskytující služby sociálních sítí poskytovatelé služeb informační společnosti spadající pod zákonné ustanovení § 5 ZNSIS, tj. ustanovení upravující tzv. *hosting.*[149] Uživatelé zpravidla využívají tyto komunikační platformy za účelem sdílení svých osobních údajů s dalšími uživateli. Mezi základní osobní údaje, které uvádí každý uživatel při registraci patří jméno, příjmení, adresa, pohlaví, datum narození a číslo mobilního telefonu nebo e-mailová adresa.[150] Tyto údaje samozřejmě nemusí odpovídat realitě, verifikaci totiž u většiny poskytovatelů podléhá jen e-mailová adresa nebo telefonní číslo. Dále už je na každém, jakým způsobem a v jakém rozsahu umožní ostatním uživatelům dané služby tzv. nahlédnout do svého soukromí.

Sociální sít lze charakterizovat jako veřejně dostupnou webovou stránku, jejímž primárním účelem je navazování, udržování a rozvíjení sociálních vazeb mezi jejími uživateli. Můžeme rozlišovat určité kategorie sociálních sítí, nicméně v řadě případů se rozdělení již stírá. Například platforma LinkedIn.com představuje typického zástupce profesní sociální sítě s profily potencionálních adeptů na zaměstnance, na druhou stranu větší platformy poskytují široký prostor pro realizaci ve více rovinách.[151]

Většina sociálních sítí umožňuje svým uživatelům určit, jaké údaje budou či nebudou sdílet s dalšími uživateli, tj. nastavit míru svého soukromí. S tím také souvisí povaha sociální sítě a jaké důsledky může tato povaha představovat pro postup orgánů činných v trestním řízení. ÚS zaujal k této problematice stanovisko, že povahu sociální sítě (v daném případě se jednalo o platformu Facebook) nelze generalizovat a nelze předem říci, že její povaha je výlučně soukromá či veřejná. Záleží na každém jednotlivci, který je uživatelem, jakým způsobem nastaví míru svého soukromí.[152] *Ad absurdum* lze

[148] Dle zprávy ČSÚ přesáhl v roce 2018 počet Čechů majících profil na některé sociální sítí hranici 50%, [online], [cit. 10. 5. 2019], dostupné: https://www.czso.cz/csu/czso/vice-nez-polovina-cechu-pouziva-socialni-site

[149] Dle §5 zákona č. 480/2004 Sb. o některých službách informační společnosti, více viz kapitola 2.6

[150] POLČÁK, R., PÚRY, F. a HARAŠTA, J. Elektronické důkazy v trestním řízení. Op. cit., s. 142 a násl.

[151] Ibid

[152] Nález Ústavního soudu ze dne 30. 10. 2014, sp. zn. III. ÚS 3844/13, publikováno ve Sbírce nálezů a usnesení ÚS, 75/2014, pod č. 201/2014 USn.

uvažovat o situaci, kdy uživatel zvolí u svých příspěvků takové nastavení, že by k nim měla přístup pouze jediná další osoba. Tuto situaci pak lze připodobnit k soukromé konverzaci na síti, a ochrana by zde tedy byla poskytována přímo v ústavní rovině. Na druhou stranu si může uživatel zvolit takové nastavení, že jeho obsah bude přístupný velmi širokému okruhu osob, přičemž tato varianta je běžná u profilů politicky angažovaných osob. Podle povahy toho, kterého uživatelského profilu se pak musí lišit i přístup dotčených orgánů.

Výše uvedená teze byla pak promítnuta v dalším rozhodnutí, které se týkalo právě výroků politicky angažované osoby na sociální sítí. V daném případě zveřejnil poslanec Parlamentu ČR Otto Chaloupka trestně postižitelný výrok na svém uživatelském profilu, když se nalézal na půdě Poslanecké sněmovny. ÚS dospěl k závěru, že takový výrok nepožívá výsad poslanecké imunity, jelikož se nejedná o projev poslance na půdě sněmovní komory. V daném nálezu byla pak poprvé formulována pravidla pro výklad nestíhatelnosti členů parlamentu za projevy učiněné v komoře parlamentu.[153]

Sociální média poskytují současně prostor, kde se jejich uživatelé mohou anonymně realizovat, což vytváří u řady z nich dojem, že jejich činy v kyberprostoru, včetně názorových komentářů s nenávistným podtextem, nemají trestněprávní následky v reálném světě. Tuto problematiku si dovolím demonstrovat na případu, kdy obviněná osoba na veřejně přístupné počítačové sítí ze svého uživatelského profilu, okomentovala následující příspěvek (veřejně přístupný): *„Aktualizováno video: v kamionech se tísnily mezi nákladem zboží rodiny běženců,“* slovy, *„a my na ně budeme platit… proč ty autobusy radši nezapálili...“* Soud postoupil věc usnesením k projednání jako přestupek proti veřejnému pořádku. NS však tato usnesení zrušil a věc přikázal k novému projednání a rozhodnutí soudu prvního stupně, kdy nepřisvědčil závěrům soudu o nízké společenské škodlivosti spáchaného skutku.[154] V obdobných případech však nastává problém, kdy ze strany příslušných orgánů není možné obdobné situace zcela efektivně prošetřovat. A to zejména s ohledem na mimořádné množství takových situací. Současně se obávám, že právě s ohledem na množství takových případů může docházet k exemplárnímu potrestání usvědčených pachatelů, za účelem odstrašení pachatelů potencionálních.

---

[153] Nález Ústavního soudu, sp. zn. I. ÚS 3018/14, 16. 6. 2015, publikováno ve Sbírce nálezů a usnesení ÚS, 77/2015, pod č. 111/2015 USn.
[154] Usnesení Nejvyššího soudu ze dne 31. 1. 2019, č.j. 6 Tdo 72/2019-19

Mimo výše uvedené, tvoří významnou část kriminality páchané prostřednictvím sociálních sítí tvoří ta související se zneužíváním dětí. S ohledem na skutečnost, že uživateli těchto platforem jsou často nezletilí, nikoliv ojediněle osoby mladší patnácti let[155], výjimkou nejsou situace, kdy se společensky škodlivého jednání dopustí právě tyto osoby. Spolu s rozmachem sociálních medií není již pro děti nijak složité vytvořit audiovizuální záznamy nejrůznější povahy a následně jej sdílet s dalšími uživateli. Jako v případě, kdy nezletilá Y, toho času jedenáctiletá, zaslala dobrovolně video, které zobrazovalo nezletilou Y zcela nahou, provádějící úkony erotické povahy, nezletilému X. Nezletilý X. následně prostřednictvím aplikace Facebook Messenger přeposlal toho video čtyřem mladistvým a dvěma nezletilým osobám. Státní zástupce následně podal návrh na uložení opatření nezletilému pro spáchání činu jinak trestného podle § 90 zákona o soudnictví ve věcech mládeže[156], s to přečinu výroby a jiného nakládání s dětskou pornografií. NS zde připustil, že předmětné video bylo pornografickým dílem zobrazujícím dítě. K subjektivní stránce nezletilého X. však uvedl, že: *„subjektivní stránku nezletilého X je třeba posuzovat i se zřetelem na tuto povahu rozšířené informační platformy Facebooku a na to, že vlivem vývoje nových technologií je pro děti jednoduché vytvořit vlastní i autopornografické dílo (nezletilá jej vytvořila nahráním pomocí tabletu) a následně ho sdílet mezi své kontakty uvnitř internetové sociální sítě. Jejich cílem však obecně není ohrozit vývoj dětí či se nějak účastnit na jejich sexuálním zneužívání.“…..* *„Jako v tomto případě jde spíše o formu snahy se určitým způsobem vyjádřit, předvést, zviditelnit anebo na sebe jinak upozornit, a to i způsoby, které nejsou vždy vhodné, neodpovídají obecné slušnosti nebo vkusu apod. a mohou i hraničit s trestným jednáním. Je však třeba vždy zvažovat, zda je nezbytné a účelné vést děti za ně k trestní či jiné odpovědnosti.“*[157] NS tedy upozornil právě na skutečnost, že děti využívající služeb informační společnosti si nemusí vždy dostatečně uvědomovat závažnost situace a je tak třeba k obdobným případům přistupovat s největší uvážlivostí, za šetření osobnosti všech zúčastněných.

[155] Zákon č. 110/2019 Sb., zákon o zpracování osobních údajů v souvislosti v nabídkou služby informační společnosti nově požaduje pro souhlas se zpracováním údajů dovršení věku 15ti let.
[156] Zákon č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže, ve znění pozdějších předpisů
[157] Usnesení Nejvyššího soud, sp. zn. 8 Tdo 1106/2017, ze dne 25. 10. 017, publikováno ve Sbírce soudních rozhodnutí a stanovisek, 9/2018, pod č. R 42/2018 tr.

3.2 Postup orgánů činných v trestním řízení vůči provozovatelům sociálních sítí

Nejvýznamnější provozovatelé sociálních sítí jsou zpravidla usídleni v zahraničí, většina z nich v USA, přičemž data, která mají pod kontrolou, uchovávají v datových centrech napříč celým světem. V případech vyšetřování trestné činnosti, kdy je nezbytné zajistit data, nad kterými vykonávají kontrolu tyto společnosti, se tedy obecně uplatní mechanismy mezinárodní právní pomoci a v případě států v rámci EU evropský vyšetřovací příkaz.[158] Nicméně, již pouhé zjištění, ve které zemi se vlastně určitá data nacházejí představuje pro dotčené orgány značný problém. Zvláště v případě, kdy někteří provozovatelé data neustále přesouvají mezi data centry.[159]

Postup prostřednictvím výše uvedených mechanismů současně prodlužuje zajištění potřebných dat do takové míry, že nakonec může dojít k situaci, kdy získané údaje již postrádají využitelnost. Právě délka celého procesu vyústila ve vznik jakési paralelní cesty přímé spolupráce orgánů činných v trestním řízení a některých provozovatelů sociálních sítí. Tyto společnosti si současně vytvořily vlastní pravidla pro poskytování údajů o uživatelích (např. *law enforcement guidlines* v případě společnosti Facebook[160]).

Přímá spolupráce českých orgánů veřejné moci a poskytovatelů služeb funguje v praxi tak, že orgány činné v trestním řízení zasílají příkazy dle trestního řádu (např. k zjištění údajů o telekomunikačním provozu dle § 88a trestního řádu) poskytovatelům daných služeb prostřednictvím Národní centrály proti organizovanému zločinu (dále jen „NCOZ“), která zajišťuje jejich překlad. NCOZ pak zajišťuje komunikaci se zahraničními poskytovateli, jelikož funguje jako kontaktní bod pro kybernetickou kriminalitu a kontaktní místo pro počítačové hlášení závadného obsahu a závadových aktivit v síti internet.[161]

Je nutné zdůraznit, že tato praxe je možná pouze, pokud dotčené společnosti údaje poskytnou dobrovolně. Jinak je třeba jít cestou mezinárodní justiční spolupráce. V případech, kdy budou orgány činné v trestním řízení požadovat součinnost českých

[158] K tomu podrobněji v poslední kapitole
[159] Takto činní např. Google
[160] [online], [cit. 9. 6. 2019], Dostupné na: https://www.facebook.com/safety/groups/law/guidelines/
[161] VOKUŠ, J. Kyberkriminalita, Zveřejněné informace za rok 2019, [online], [cit. dne 3. 6. 2019], dostupné na: https://www.policie.cz/clanek/zverejnene-informace-2019-kyberkriminalita.aspx

poskytovatelů, kdy jsou data fakticky uložena na území ČR, uplatní se ustanovení českého právního řádu. Zjišťování provozních a lokalizačních údajů je, jak bylo výše uvedeno, zákonem přímo upraveno. V souvislosti s aktuálně uloženými obsahovými údaji zpravidla využívají orgány činné v trestním řízení stejně jako v případě zajišťování obsahu elektronické pošty postup dle § 158d odst. 3 trestního řádu, popřípadě postup dle § 88 trestního řádu pro komunikaci v reálném čase.[162]

Současně je nutné uvést, že cestu dobrovolné spolupráce nelze dle zkušenosti Policie ČR využít při zajišťování jakýchkoliv údajů, ale pouze těch neobsahových.[163] Údaje o obsahu lze tedy dožadovat výhradně prostřednictvím mezinárodní justiční spolupráce. Neobsahovými údaji rozumíme dle dikce české legislativy lokalizační a provozní údaje.

Dle dokumentu Evropské komise právo USA umožňuje tamním poskytovatelům služeb informační společnosti přímou spolupráci s orgány veřejné moci ze zahraniční. Na rozdíl od práva EU[164] právo USA neobsahuje generální ustanovení, které by zakazovalo předání osobních údajů do jiných jurisdikcí i v případě absence dostatečných záruk ochrany údajů.[165]

Jinak je ale daná praxe především reakcí dotčených poskytovatelů na Úmluvu o počítačové kriminalitě. Ta stanoví, že:

„Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby umožnila svým příslušným orgánům nařídit poskytovateli služby nabízejícímu své služby na území strany, aby předložil ty informace o odběrateli vztahující se k těmto službám, které jsou v jeho držení nebo pod jeho kontrolou.“[166]

---

[162] Konzultace s vrchní komisařkou kpt. Mgr. Terezou Andělovou Služby kriminální policie a vyšetřování Odboru analytiky a kybernetické kriminality Policie ČR, KŘP Plzeňského kraje
[163] Ibid
[164] Nařízení Evropského parlamentu a rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
[165] Doporučení pro rozhondutí Rady o zmocnění k zahájení jednání za účelem dosažení dohody mezi Evropskou unií a Spojenými státy americkými o přeshraničním přístupu k elektronickým důkazům pro justiční spolupráci v trestních věcech, dostupné: https://ec.europa.eu/info/sites/info/files/recommendation_council_decision_eu_us_e-evidence.pdf, s. 2 a The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens STUD, dostupné: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/519215/IPOL_STU%282015%29519215_EN.pdf, viz. § 2701 a násl. zákona o elektronické komunikaci a soukromí z roku 1986
[166] Čl. 18 odst. 1 písm. b) Úmluvy o počítačové kriminalitě

Dotčení poskytovatelé tedy dobrovolně spolupracují především z toho důvodu, že očekávají do budoucna zakotvení této povinnosti do národního zákonodárství smluvních stran.

K využití cesty přímé spolupráce byly současně vyzvány členské státy EU v roce 2016, po zhodnocení dohody o vzájemné pomoci mezi EU a USA.[167]

Ačkoliv, pro orgány činné v trestním řízení je do tato praxe do jisté míry výhodná, jelikož jim umožňuje získat potřebná data v relativně krátkém časovém úseku, zdá se, že v těchto případech došlo k jakési rezignaci na požadavek zákonnosti. Skutečnost, že se orgány činné v trestním řízení vlastně řídí interními instrukcemi soukromých subjektů vyvolává otázku, do jaké míry je zajištěna ochrana práva na soukromí dotčených uživatelů. Současně fakt, že se orgány veřejné moci přizpůsobily interním politikám společností spravujících sociální sítě poukazuje i na značně silné postavení takových společností, a to v globálním měřítku. Na druhou stranu jsou orgány činné v trestním řízení s ohledem na absenci efektivních právních nástrojů vlastně nuceny se k této cestě uchylovat.

Situaci jakéhosi legislativního vakua by mohla vyřešit navrhovaná unijní legislativa, která předpokládá možnost zajištění dat přímo od poskytovatelů dotčených služeb. K té se blíže vyjadřuji v poslední kapitole své diplomové práce.

Současně by podle mého názoru, *de lege ferenda,* bylo vhodné do trestního řádu zakotvit institut, který by přímo počítal se zajišťováním obsahových údajů týkající se poskytovatelů služeb informační společnosti, v jehož rámci by byly rozlišovány situace zajišťování aktuálně uložených dat a situace, kdy se zjišťuje obsah on-line do budoucna.

[167] Review of the 2010 EU-US MLA Agreement - Examination of draft texts ze dne 7 dubna 2017, [online], [cit. dne 13. 5. 2019] dostupné na: http://statewatch.org/news/2016/apr/eu-council-eu-usa-mutual-legal-assistance-review-07403-07-04-16.pdf

3.3 Postup zajišťování elektronických důkazních prostředků v souvislosti s nakládáním s dětskou pornografií

Jak již bylo naznačeno výše, osobní profil uživatele je spojen s obsahovými a neobsahovými údaji. Ty neobsahové hrají významnou roli zejména na počátku celého procesu odhalování osoby pachatele trestné činnosti. Takovými údaji se rozumí například IP adresy či telefonní číslo uživatele.[168]

Níže se zaměřuji blíže na specifika postupů orgánů činných v trestním řízení při odhalování trestné činnosti související s nakládáním s dětskou pornografií ve vztahu k sociálním sítím.

Odhalování takových trestných činů zpravidla začíná po trestním oznámení. To činí často rodič dítěte, které se stalo obětí sexuálního nátlaku apod. Dále jej může činit zaměstnavatel osoby, u níž existuje podezření, že se dopustila protiprávního jednání. Pro trestnou činnost páchanou za pomocí sociálních médií je však typická situace, kdy oznámení činí samotný poskytovatel služby. Jednotlivé platformy zjišťují preventivně přítomnost závadného obsahu za pomocí algoritmů, které jej detekují.[169]

Jak uvádím v předchozí kapitole, některé údaje poskytují dotčené společnosti i bez formálního postupu mezinárodní právní pomoci, prostřednictvím cesty přímé spolupráce. Typicky se jedná o údaje jako jsou IP adresy či registrační e-mail a telefonní číslo uživatele. Pokud však příslušný orgán potřebuje získat obsah korespondence uživatelů, údaje o platebních kartách či údajů typu cookies musí postupovat cestou mezinárodní právní pomoci.

Pokud tedy např. Facebook detekuje přítomnost závadného obsahu na uživatelském profilu či v rámci komunikačních aplikací uživatelů nacházejících se kdekoliv na světě, učiní zpravidla hlášení neziskové organizaci Národní centrum pro ztracené a zneužívané děti (*National Center for missing and exploited children)*. Ta úzce spolupracuje s mezinárodním centrem pro ztracené a zneužívané děti (*International Center for missing and exploited children)* a bezpečnostními složkami po celém světě[170],

---

[168] K neobsahovým údajům neboli údajů lokalizačním a provozním více v kapitole 2.2

[169] DAVIS, A., New Technology to Fight Child Exploitation [online], [cit. dne 10. 6. 2019], dostupné na: https://newsroom.fb.com/news/2018/10/fighting-child-exploitation/

[170] Informace pro bezpečnostní složky, [online], [cit. 9. 6. 2019] viz.: https://www.facebook.com/safety/groups/law/guidelines/

např. mezinárodní organizací kriminální policie, Interpolem. Pokud se bude jednat o trestnou činnost s následkem či podezřelým pachatelem na území EU, následuje notifikace Europolu, který vyhodnotí, jakému členskému státu informaci následně předat. V případě ČR bude kontaktní institucí NCOZ, odbor kybernetické kriminality, která pak o daných případech informuje věcně a místně příslušné útvary Policie ČR.[171]

Počáteční notifikace od provozovatelů služeb sociálních sítí obsahuje zpravidla registrační údaje dotyčného účtu a IP adresy, ze kterých bylo přistupováno k takovému účtu. Po vyhodnocení oznámení může policejní orgán přistoupit k sepsání úředního záznamu o zahájení úkonů trestního řízení a případně činí potřebná šetření k odhalení skutečností, které nasvědčující tomu, že byl spáchán trestný čin a směřující ke ztotožnění pachatele (§158 trestního řádu).

Pokud dojde orgán činný v trestním řízení k závěru, že je nezbytné zajistit urychlené uchování dat, je nově možné realizovat tzv. předběžný uchovávací příkaz. V případě tuzemských poskytovatelů, kteří spravují data na území ČR postupují nyní příslušné orgány dle § 7b trestního řádu. Jak již bylo uvedeno výše, před zakotvením toho institutu, bylo ke stejnému účelu využíváno obecné ustanovení o součinnosti § 8 trestního řádu. Zajímavá situace nastává právě v případě cesty dobrovolné spolupráce s provozovateli sociálních sítí. V takovém případě pro získání údajů o uživatelích od provozovatele, a to bez ohledu na to, kde se dotčená data nacházejí fyzicky, taktéž postačí vydání příkazů podle trestního řádu, přeložené do jazyka společnosti, tj. zpravidla jazyka anglického. A to i přes skutečnost, že existují zákonné postupy pro zajištění dat na mezinárodní úrovni dle ZMJS.

Po tom, co dojde k uchování předmětných údajů, vygeneruje provozovatel identifikační číslo vztahující se k těmto údajům, které poskytne policejnímu orgánu.

V případě přímé spolupráce následuje zpravidla příkaz k zjištění údajů o telekomunikačním provozu dle § 88a trestního řádu. Tento úkon bude v obdobných případech zpravidla vykonáván jako neodkladný a neopakovatelný úkon ještě před zahájením trestního stíhání. Tímto způsobem budou zajištěny registrační údaje uživatele, tj. e-mailová adresa, telefonní číslo, dále tzv. logovací údaje a IP adresy. Tlumočníkem

[171] Závazný pokyn policejního prezidenta ze dne 21. dubna 2009 o plnění úkolů v trestním řízení k organizaci výkonu služby, součinnosti, příslušnosti policejních orgánů1) a k provádění některých úkonů podle zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů

přeložený příkaz dle § 88a trestního řádu zasílá NCOZ stejně jako žádost o uchování dat přímo konkrétním poskytovatelům.[172]

Pokud bude takový postup možný, dojde po získání relevantních údajů od provozovatele sociální sítě, k vyžádání informací, na základě § 88a trestního řádu od českého poskytovatele služby datového připojení, a to za účelem ztotožnění podezřelého. V případě, že zjištěné informace povedou v jejich vzájemné souvislosti k určité osobě, provede policejní orgán domovní prohlídku v souladu s § 82 a násl. trestního řádu.

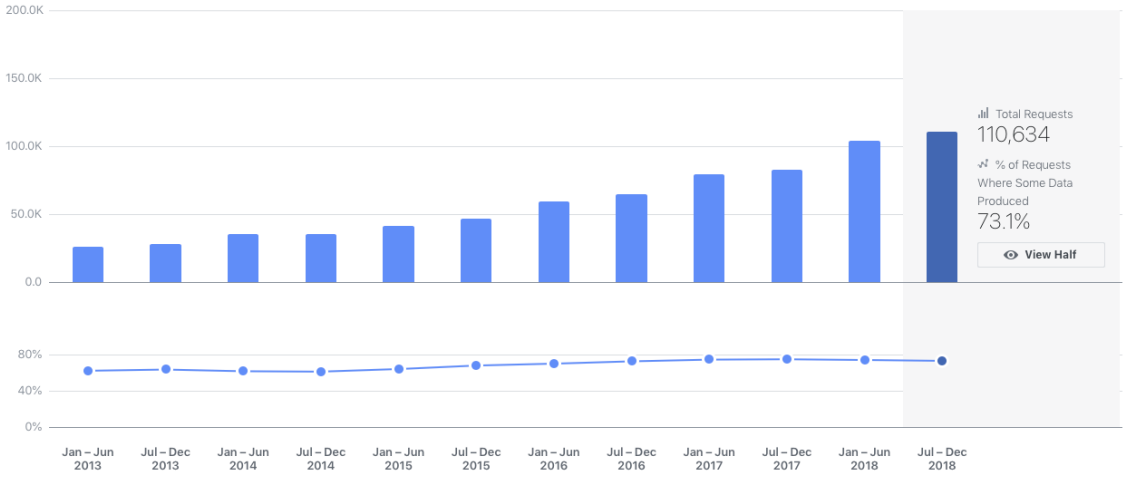
V rámci domovní prohlídky zajišťuje policejní orgán v obdobných případech zpravidla veškerou výpočetní techniku a datové nosiče jako jsou externí disky. Při výkonu tohoto úkonu však musí policejní orgán dbát zásady přiměřenosti a zdrženlivosti dle § 2 odst. 1, potažmo § 52 trestního řádu. Jak bylo již demonstrováno v první kapitole této diplomové práce, je současně nezbytné efektivně zabezpečit zabavená zařízení pro účely forenzní analýzy prováděné znalcem. Zpravidla budou zajištěny klonové otisky disků a disky budou poté zapečetěny. Aby bylo zabráněno případné ztrátě relevantních dat, zapříčiněné odpojením zařízení, které je stále v provozu, od zdroje, je vhodné provést na místě ohledání v souladu s § 113 trestního řádu. Ohledáním lze taktéž případně zajistit přístup do vzdálených uložišť.[173]

Výpočetní technika a další nosiče dat budou zpravidla předány znalci k provedení forenzní analýzy a znalecké posudky pak budou sloužit jako důkazní prostředek.

3.3.1 Statistické údaje

V souvislosti s poskytováním informací o uživatelích vnitrostátním orgánům vytváří poskytovatelé služeb každoroční zprávy, ve kterých uvádí statistické údaje týkající se jednotlivých států.[174] Jak je vidět z níže uvedeného grafu, například celkový počet žádostí vnitrostátních orgánů vůči společnosti Facebook má globálně vzestupnou tendenci.

[172] Konzultace s vrchní komisařkou kpt. Mgr. Terezou Andělovou Služby kriminální policie a vyšetřování Odboru analytiky a kybernetické kriminality Policie ČR, KŘP Plzeňského kraje
[173] POLČÁK, R., PÚRY, F. a HARAŠTA, J. Elektronické důkazy v trestním řízení. Op. cit., s. 103
[174] Statistiky žádostí týkající se dat uživatelů společnosti Facebook. [online], [cit. dne 10. 6. 2019] Ke stažení na: https://transparency.facebook.com/government-data-requests



Významně taktéž globálně narůstá počet žádostí o uchování uživatelských údajů za účelem jejich pozdějšího získání. Orgány ČR zaslaly společnosti Facebook v roce 2018 celkem 331 žádostí o „uchování dat“, v roce 2017 to bylo 208 žádostí.[175] I z těchto důvodů hodnotím zakotvení postupů tzv. předběžného uchování dat do trestního řádu a ZMJS jako pozitivní krok, který směřuje k zajištění vyšší míry ochrany práv jednotlivců a současně k zajištění vyšší míry transparentnosti postupů orgánů činných v trestním řízení.

[175] Nejnovější dostupné statistiky se týkají druhého pololetí pololetí 2018. Ke stažení na: https://transparency.facebook.com/government-data-requests

3.3.2 Praktický příklad

Na závěr této kapitoly bych ráda uvedla reálný případ související s trestnou činností páchanou za pomocí sociální sítě, kdy byl za pomocí elektronických důkazních prostředků dopaden pachatel. Případ je pro účely této diplomové práce anonymizován.

Matka devítileté holčičky podala trestní oznámení na neznámého pachatele. Bylo zjištěno, že mezi obětí a osobou XY došlo k prvotní komunikaci přes poměrně neznámou platformu Omegle, přičemž pachatel XY nejdříve z oběti vylákal intimní fotografie, jež mu nejprve poslala oběť dobrovolně. Další komunikace mezi pachatelem XY a obětí se odehrávala v rámci platforem Facebook Messenger a Skype. Když oběť nechtěla zaslat pachateli další fotografie, ten počal oběti vyhrožovat, že již zaslané fotografie zveřejní na sociálních sítích. Prvním úkonem ve věci bylo podání vysvětlení ze strany nezletilé. Následovala žádost poskytovatelům služeb zaslaná prostřednictvím NCOZ o tzv. zmražení dat na základě § 8 trestního řádu a dále následoval příkaz k zjištění údajů o telekomunikačním provozu dle § 88a trestního řádu. Na základě zjištěných okolností byl pachatel XY ustanoven podezřelým. Vzhledem k důvodnému podezření, že v obydlí podezřelého se nachází věc důležitá pro trestní řízení, byla provedena domovní prohlídka, při níž došlo k zajištění jednoho osobního počítače, mobilního telefonu a několika kusů CD-ROMů. Na základě analýzy těchto datových nosičů znalcem bylo zjištěno, že podezřelý komunikoval s cca dalšími 60 osobami mladistvými či nezletilými přes platformy Skype, Instagram, Messenger, WhatsApp. V daném případě se podařilo ztotožnit cca 50 % poškozených osob, přičemž trestná činnost byla zjištěna v souvislosti s dalšími 11 nezletilými. Pachatel byl usvědčen ze zvlášť závažného zločinu sexuálního nátlaku dle §186 odst. 1, odst. 5 trestního zákoníku v jednočinném souběhu s přečinem zneužití dítěte k výrobě pornografie dle § 193 odst. 1 trestního zákoníku.

Na případu pachatele XY je lze demonstrovat, jak sociální sítě usnadňují páchání trestné činnosti související s dětskou pornografií. Pachatel XY, pocházející z Rožnova po Radhoštěm prostřednictvím sociálních médií kontaktoval oběti po celém území ČR, přičemž první oběť byla ztotožněná v Plzni.

3.4 Shrnutí

Sociální sítě představují v současné době jakýsi paralelní svět, kde dochází k významným střetům práv a svobod jednotlivců. Významně se zde střetává svoboda

projevu s právem na ochranu soukromí. Nicméně, chováním jednotlivců tzv. „na síti“ nezřídka dochází i k narušování veřejného zájmu na ochraně společnosti před trestnými činy, přičemž toto jednání často představuje významný zásah do osobnosti jednotlivců. Jistá míra anonymity tohoto virtuálního světa zřejmě otupuje morální zábrany jedinců, což se projevuje v nejrůznějších projevech vůči skupinám osob.

V případech vyšetřování trestné činnosti páchané za pomocí sociálních sítí hraje významnou roli doba, za jakou se orgánům činným v trestním řízení podaří získat relevantní údaje k dopadení pachatele. Rychlé zajištění údajů však stojí v kolizi se skutečností, že jsou potřebné údaje často fyzicky spravovány na zahraničních serverech a nezřídka bývají přesouvány napříč celým světem. Zákonné postupy jsou v důsledku toho velmi neefektivní. Tyto faktory zavdaly v oblasti neobsahových údajů příčinu ke vzniku dobrovolné spolupráci vyšetřujících orgánů a společností spravujících údaje o uživatelích. Tato praxe však není z hlediska zajištění práv jednotlivců ideální a ukazuje na potřebu nových legislativních opatření. Situaci by snad mohla vyřešit navrhovaná unijní legislativa, které se podrobněji věnuji v následující části diplomové práce.

Nicméně problémy existují i ve vztahu k poskytovatelům, kteří jsou usazeni v ČR. Jak jsem uvedla výše, bylo by podle mého názoru zakotvit do trestního řádu ustanovení, které by umožňovalo orgánům činným v trestním řízení zajišťovat obsahové údaje týkající se komunikace uskutečňované prostřednictvím „moderních“ komunikačních platforem. Takový postup by ideálně zahrnul jak komunikaci prostřednictvím elektronické pošty, tak komunikaci prostřednictvím sociálních sítí, přičemž s ohledem na ochranu soukromí a listovního tajemství by bylo třeba trvat na zakotvení přísných limitujících podmínek pro takový postup.

Při odhalování trestné činnosti související s nakládáním s dětskou pornografií tvoří významné vodítko IP adresy serverů, z nichž se dotčené osoby připojují. Ve valné většině případů souvisejících s dětskou pornografií pachatelé své IP adresy nešifrují, a tak jsou poměrně snadno odhalitelní. Problém pak nastává v případě, kdy pachatel využije dnes běžně dostupného aplikačního softwaru, který IP adresu změní a odhalení pachatelů se stane značně ztíženým. Tak však činní většina sofistikovanějších pachatelů kybernetické kriminality.

4 Přístup k problematice elektronických důkazních prostředků na mezinárodní úrovni

Rychlý rozvoj informačních technologií a komunikačních služeb je samozřejmě předmětem zájmu i na mezinárodní a unijní úrovni. To především proto, že bezhraniční povaha internetu si žádá efektivní nástroje právní pomoci mezi státy a současně také spolupráce s osobami soukromého práva. Jak uvádím výše, potencionální důkazy ve formě údajů týkajících se uživatelů online služeb se totiž často nacházejí mimo jurisdikci státu, kde byl spáchán trestný čin.

V současnosti jsou pro zajišťování elektronických důkazů, které se nacházejí mimo jurisdikci státu, v němž probíhá trestní řízení, využívány instituty evropského vyšetřovacího příkazu ve vztahu k zemím EU (mimo Irsko a Dánsko) a mechanismus mezinárodní právní pomoci ve vztahu k zemím ostatním. Stávající mechanismy však vykazující jeden podstatný problém. A to dobu jejich uskutečnění. Vyřízení evropského vyšetřovacího příkazu trvá zpravidla 120 dní (ačkoliv v odůvodněných případech může trvat i delší dobu) a mezinárodní právní pomoc se v průměru řeší cca 10 měsíců.[176] To samozřejmě není vzhledem k nestálé povaze elektronických důkazů příliš optimální. Významný problém pro zajištění elektronických důkazů představuje také jejich umístění. A to zvláště v případech, kdy dochází k neustálému přesouvání dat uživatelů napříč data centry po celém světě.

Za účelem zefektivnění procesu zajištění elektronických důkazů nacházející se v jiné jurisdikci přistoupila EU k návrhu nařízení a související směrnice, jejichž účelem je zakotvení mechanismů zjednodušeného přístupu k takovým důkazům. Současně je v souvislosti s elektronickými důkazy na úrovni Rady Evropy projednáván dodatkový protokol k Úmluvě o počítačové kriminalitě. S ohledem na významnou roli USA, jakožto domovské země nejvýznamnějších společností v odvětví služeb informační společnosti, pak EU cílí na uzavření dohody týkající se zjednodušeného přeshraničního přístupu k elektronickým důkazům.

[176] Zákon č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních, Čl. 12 Směrnice Evropského parlamentu a Rady 2014/41/EU ze dne 3. dubna 2014 o evropském vyšetřovacím příkazu v trestních věcech

4.1 Evropská unie

Na úrovni EU byla dne 17. dubna 2018 navržena nová legislativa ve formě nařízení pro oblast justiční spolupráce v trestních věcech. Účelem navrhované právní úpravy je zakotvení evropského předávacího a uchovávacího příkazu za účelem zajištění a uchování elektronických důkazů, které se nacházejí v odlišné jurisdikci. Cílem návrhu je zavést cestu přímé spolupráce vnitrostátních orgánů a osob soukromého práva, bez zahrnutí zahraničních orgánů veřejné moci. Současně byla navržena směrnice, stanovující pravidla pro jmenování právních zástupců za účelem shromažďování důkazů v trestním řízení.[177] Návrh legislativy prochází momentálně v rámci řádného legislativního procesu fází prvního čtení (Rada EU). Není tedy zatím jasné, jaká bude závěrečná podoba, i přesto bych si však plánovanou úpravu dovolila níže představit a zhodnotit její problémy. Pro upřesnění je vhodné uvést, že návrh nepočítá se sledováním údajů v reálném čase, týká se pouze informací již uložených.[178]

Výše uvedené návrhy reflektují potřebu změnit stávající právní stav, který se v oblasti zajišťování a předávání elektronických důkazů mezi jednotlivými státy vyznačuje značnou neefektivitou, a to především v důsledku neúnosně dlouhé doby vyřízení. Vzhledem k neustálému zrychlování v online prostředí může přetrvání současného stavu do budoucna způsobit úpadek důvěry v právní stát. Současný právní rámec nezohledňuje volatilní povahu elektronických důkazů. Po komplikovaném a zdlouhavém vyřízení celého procesu může snadno dojít k tomu, že zajištění důkaz již není v daném trestním řízení vůbec potřeba. Další problém aktuálně platného rámce představuje neefektivní spolupráce veřejného a soukromého sektoru.[179] Je však otázkou, do jaké míry může navrhované nařízení tento problém vyřešit. Významnou otázkou stávající i budoucí právní úpravy je pak problematika umístění údajů a jejich lokalizace.

---

[177] Návrh nařízení Evropského parlamentu a rady o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech COM/2018/225 final - 2018/0108 (COD) a návrh směrnice Evropského parlamentu a rady, kterou se stanoví harmonizovaná pravidla pro jmenování právních zástupců za účelem shromažďování důkazů v trestním řízení, COM/2018/226 final - 2018/0107 (COD)

[178] Ibid

[179] Důvodová zpráva, č. COM/2018/225 final - 2018/0108 (COD) k návrhu nařízení Evropského parlamentu a rady o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech, Ve Štrasburku dne 17. 4. 2018, [online], [cit. 27. 3. 2019], Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1559736463321&uri=CELEX%3A52018PC0225, s. 7

Je však vhodné upozornit, že navrhovaná legislativa již zakotvené mechanismy přeshraniční spolupráce nenahrazuje, pouze je v určitých oblastech doplňuje.

Informace by tedy dle navrhované legislativy měly být poskytovány orgánům v dožadujícím státě přímo poskytovatelem služby, a to bez nezbytné spolupráce orgánů státu, v jehož jurisdikci se údaje nacházejí. Tento prvek představuje poměrně významný zvrat vzhledem k současné koncepci pojetí přeshraničního zajištění důkazů. Stejný trend se však objevil i v USA spolu s novým zákonem, tzv. CLOUD Act.[180] Důvodová zpráva tento odklon odůvodňuje tak, že stát, kde jsou údaje umístěny zásadně nemá nad takovými údaji žádnou kontrolu.[181]

Ve prospěch návrhu lze argumentovat, že v případech, kdy jsou data přesouvána z jednoho data centra v jednom státě do druhého v naprosto odlišném státě, příslušné orgány nejsou prakticky schopny taková dat zajistit. Na druhou stranu je třeba položit si otázku, zda není tímto způsobem zasahováno do suverenity toho, kterého státu. Protiargument, že obdobným opatřením může dojít ke snížení ochrany soukromí, se zřejmě v rámci EU, kde je nastaven společný rámec ochrany osobních údajů, neuplatní.

Postupy se uplatní i v případě, kdy poskytovatel není usazen ani zastoupen v zemi EU, pouze poskytuje na jejím území služby.[182]

V návrhu je definován pojem elektronických důkazů, a to jako: „*důkazy uložené v elektronické podobě poskytovatelem služeb nebo jeho jménem v době obdržení certifikátu předávacího nebo uchovávacího příkazu, sestávající z uložených údajů o účastníkovi, údajů o přístupu, údajů o transakcích a údajů o obsahu.*“[183] Tato definice zahrnuje dvě kategorie údajů. Prvně jde o tzv. neobsahové údaje, tj. údaje o účastníkovi, údaje o přístupu, údaje o transakcích. V zásadě jde o provozní a lokalizační údaje. Druhou kategorií jsou pak údaje o obsahu. Dle důvodové zprávy k návrhu je nezbytné, aby se navrhovaná úprava týkala všech výše uvedených kategorií. Provozní a lokalizační údaje jsou totiž, jak bylo již demonstrováno v předchozí kapitole, významným zdrojem poznání

[180] Podrobněji níže.
[181] Důvodová zpráva, k návrhu nařízení Evropského parlamentu a rady o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech, Ve Štrasburku dne 17. 4. 2018, Op. cit., s. 13
[182] Buďto mají provozovnu nebo služby využívá významný počet uživatelů
[183] Čl. 2 odst. 6 Návrhu nařízení Evropského parlamentu a rady o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech

totožnosti pachatele. Na druhou stranu údaje o obsahu mohou tvořit důležité indicie týkají se spáchaného skutku.[184]

Ze srovnání s vnitrostátním právním rámcem je zjevné, že s ohledem na charakter těchto dat se liší i intenzita zásahu do soukromí jednotlivých osob. Proto také navrhovaná úprava rozlišuje jednotlivé kategorie data a stanoví různé podmínky pro vydávání, respektive uchovávání. Tzv. neobsahové údaje bude možné vydat v souvislosti s jakýmkoliv trestným činem, kdežto údaje o obsahu jen v souvislosti s trestnými činy s horní hranicí trestní sazby v délce nejméně tří let či v souvislosti s trestnými činy výslovně uvedenými v návrhu (u takových trestných činů je předpoklad, že důkazy budou výlučně v elektronické formě). Předpokladem pro vydání příkazů je princip vzájemnosti, tedy existence obdobného opatření ve vztahu ke stejnému trestnému činu ve vydávajícím státě.[185]

Uchovávacím příkazem se dle návrhu rozumí „*závazné rozhodnutí vydávajícího orgánu členského státu nutící poskytovatele služeb nabízejících služby v Unii a usazeného nebo zastoupeného v jiném členském státě uchovávat elektronické důkazy vzhledem k následné žádosti o předání údajů.*“[186] Poskytovatelem služeb se pak rozumí fyzická či právnická osoba, která je poskytovatelem služeb elektronických komunikací, služeb informační společnosti či např. poskytovatelé IP adres, názvů domén, atd[187] (legislativa se dotkne i sociálních sítí, VoIP, instant messagingu, cloudových služeb, atd.).

Vydáním uchovávacího příkazu lze zamezit ztrátě či pozměnění důležitých údajů v případě, kdy lze předpokládat, že získání údajů vyžaduje delší čas. Prakticky si lze jeho využitelnost představit v případě, kdy budou data dožadovány prostřednictvím evropského vyšetřovacího příkazu, ten totiž není limitován z hlediska závažnosti trestné činnosti. Po přijetí příkazu má adresát uchovat údaje označené v příkazu bez zbytečného odkladu a na takovou dobu, která je nutná k jejich předání. Pokud však vydávající orgán nezašle následně žádost o předání uchovaných údajů, musí je adresát uchovávat nejdéle

---

[184] Důvodová zpráva, k návrhu nařízení Evropského parlamentu a rady o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech, Ve Štrasburku dne 17. 4. 2018, Op. cit., s. 14

[185] ŠÁMAL, P. Trestní řád: komentář. Op. cit., s. 4079 - 4080

[186] Čl. 2 odst. 2 Návrhu nařízení Evropského parlamentu a rady o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech

[187] Čl. 2 odst. 3 Návrhu nařízení Evropského parlamentu a rady o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech

po dobu šedesáti dnů. Návrh počítá se státním zástupcem, jakožto orgánem příslušným k vydání příkazu.[188]

Jak uvádím v druhé kapitole této diplomové práce, ČR již institut tzv. předběžného uchovávacího příkaz zakotvila na základě požadavků Úmluvy o počítačové kriminalitě. A to jak do trestního řádu, tak do ZMJS ve vztahu k datům uloženým v zahraničí. Dle právní úpravy v ZMJS se přeložená žádost o uchování dat posílá prostřednictvím NCOZ *cizozemskému orgánu.*[189] Dle § 2 písm. c) ZMJS se cizozemským orgánem rozumí: *„justiční nebo jiný orgán cizího státu, který je podle mezinárodní smlouvy nebo právního řádu cizího státu příslušný k mezinárodní justiční spolupráci"*[190]. Zde je tedy patrný rozdíl mezi nově zakotveným institutem a institutem dle navrhovaného nařízení. V současné době je nezbytné spolupracovat s vnitrostátními orgány v dožádaném státě, což je fáze, kterou navrhovaná legislativa neobsahuje.

Evropským předávacím příkazem se dle návrhu rozumí: *„závazné rozhodnutí vydávajícího orgánu členského státu nutící poskytovatele služeb nabízejícího služby v Unii a usazeného nebo zastoupeného v jiném členském státě předat elektronické důkazy."*[191] Znatelným rozdílem, oproti současnému stavu, představují lhůty, ve kterých musí adresát poskytnout dožádané údaje. Běžná lhůta je 10 dnů a v naléhavých případech[192] je lhůta pouze 6 hodin.[193]

Návrhu je ze strany členských států vytýkáno, že se nezabývá přímým přístupem k elektronickým důkazům ani jejich sledováním v reálném čase.[194] Proti tomu lze však namítnout, že takové postupy jsou extrémním zásahem do základních práv a svobod a tvorba efektivní legislativy, která by obsahovala nezbytné záruky, by s největší

[188] Důvodová zpráva, k návrhu nařízení Evropského parlamentu a rady o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech, Ve Štrasburku dne 17. 4. 2018, Op. cit., s. 17
[189] Viz znění § 65a zákona č. 104/2013, o mezinárodní justiční spolupráci ve věcech trestních
[190] § 2 písm. c) zákona č. 104/2013, o mezinárodní justiční spolupráci ve věcech trestních
[191] Čl. 2 odst. 1 Návrhu nařízení Evropského parlamentu a rady o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech
[192] Je bezprostředně ohrožen život, tělesná integrita, či kritická infrastruktura
[193] Čl. 9 Návrhu nařízení Evropského parlamentu a rady o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech
[194] E-evidence a) Regulation on European Production and Preservation Orders for e-evidence b) Directive on legal representatives for gathering evidence = Policy debate, č. ST 9418 2018 INIT ze dne 29. 5. 2018 [online], [cit. dne 13. 5. 2019], dostupné: http://data.consilium.europa.eu/doc/document/ST-9418-2018-INIT/en/pdf

pravděpodobností představovala velmi zdlouhavý proces. Současně lze předpokládat, že by k této otázce nebylo dosaženo potřebného konsenzu.

4.1.1 CLOUD ACT

V souvislosti s navrhovanou unijní legislativou bych ráda zmínila zákon USA, který byl přijat na jaře loňského roku, tzv. „CLOUD Act“. Tento zákon totiž zakotvil povinnost poskytovatelů služeb z USA vyhovovat příkazům vnitrostátních orgánů a sdělovat údaje o obsahu bez ohledu na to, kde se vlastně tato data fyzicky nacházejí.

Otázku, zda je poskytovatel služby elektronické pošty povinen předat federálním orgánům na základě příkazu vydaného dle zákona o uloženém obsahu komunikace (Stored Communiactions Act) obsah komunikace, kdy se ale samotná data nacházejí na serveru mimo jurisdikci USA, řešil i Nejvyšší soud USA ve sporu United States v. Microsoft. Corp.[195] Ačkoliv se spor stal s ohledem na přijetí nového zákona bezpředmětným, argumentace stran jistě stojí za povšimnutí, v jejím světle lze podrobit přezkumu i na připravovanou legislativu EU.

Společnost Microsoft poskytuje službu e-mailové komunikace nazvanou „Outlook.com“, přičemž údaje související s jednotlivými účty jsou uchovávány na serverech po celém světě. V roce 2013 byl vydán příkaz k zajištění údajů týkajících se určitých uživatelských účtů s ohledem na důvodné podezření, že předmětné uživatelské účty jsou používány pro páchání trestné činnosti související s pašováním drog. Společnost Microsoft však odmítla takové údaje poskytnout, jelikož byly uloženy v datovém centru, které se fyzicky nacházelo v irském Dublinu. Případ byl předložen vládou k rozhodnutí Nejvyššímu soudu USA po tom, co soud druhé instance nepřipustil, že by příkaz umožnil zajistit data uložená v zahraničí. Vláda argumentovala, že je nesmírně zatěžující pokaždé podat žádost do určitého státu, i přesto, že se údaje týkají občana USA, který se dopustil protiprávního jednání na území USA, a jeho údaje navíc spravuje společnost, která je usazena v USA. Dále tvrdila, že v některých případech není v silách federálních orgánů zjistit skutečnou lokaci umístění dat.[196] Současně upozornila na skutečnost, že některé země nejsou ochotné s USA spolupracovat, a tudíž by mohlo docházet k tomu, že zločinní

[195] Rozhodnutí Nejvyššího soudu USA ve věci Spojené státy proti Microsoft Corp. ze dne 17. 4. 2018, No. 17-2 (per curiam)
[196] SCHWARTZ, Paul M., Legal Access to the Global Cloud, UC Berkeley Public Law Research Paper, 118 Columbia Law Review, 20. 6. 2017, s. 1695

aktéři budou uchovávat své údaje právě v těchto zemích.[197] Microsoft na druhou stranu argumentovat, že tento výklad znamená významný zásah do práva na soukromí. Současně by měl takový příkaz místně neomezenou povahu, a tudíž z daném případě USA zasahuje do suverenity jiného státu.[198]

CLOUD Act rovněž předpokládá uzavření tzv. výkonných dohod s jinými státy, na jejichž základě by poskytovatelé z USA byly povinni poskytnout údaje o obsahu přímo těmto státům, resp. jejich orgánům.[199]

4.2 Spolupráce s USA

V současné době se spolupráce v oblasti zajišťování důkazů mezi ČR a USA řídí mezinárodní smlouvou o vzájemné právní pomoci v trestních věcech z roku 2000.[200] Po přijetí Lisabonské smlouvy, a tedy po zavedení právní subjektivity EU vstoupila v roce 2010 v platnost Dohoda o vzájemné právní pomoci mezi EU a USA[201], na niž reagovala Dodatková úmluva o vzájemné právní pomoci v trestních věcech mezi ČR a USA.[202]

Ve světle nového zákona CLOUD Act se však jeví jako vhodné přistoupit k uzavření nové dohody mezi EU a USA. V únoru 2019 doporučila Evropská Komise zahájit jednání za účelem dosažení dohody mezi EU a USA o přeshraničním přístupu k elektronickým důkazům pro justiční spolupráci v trestních věcech.

Cílem návrhu je zakotvit pravidlo, aby mohly poskytovatelé předmětných služeb odpovídat na žádosti vnitrostátních orgánů ohledně obsahových a neobsahových údajů přímo, a to bez ohledu na umístění relevantních dat. Iniciativa rovněž předpokládá zajištění vzájemné reciprocity.[203] Dohoda by tedy ve vztahu k USA mohla vymezit právní rámec přímé spolupráce, která v oblasti neobsahových údajů v současné sobě funguje

---

[197] DASKAL, J., Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0, Stanford Law Review online, Volume 71, květen 2010, s. 10
[198] Ibid
[199] Ibid
[200] Sdělení Ministerstva zahraničních věcí o sjednání Smlouvy mezi Českou republikou a Spojenými státy americkými o vzájemné právní pomoci v trestních věcech č. 40/2000 Sb. m. s.
[201] Sdělení Ministerstva zahraničních věcí o sjednání Dohody o vzájemné právní pomoci mezi Evropskou unií a Spojenými státy americkými č. 5/2010 Sb. m. s.
[202] Sdělení Ministerstva zahraničních věcí o sjednání Dodatkové úmluvy o vzájemné právní pomoci v trestních věcech mezi Českou republikou a Spojenými státy americkými 7/2010 Sb. m. s.
[203] Doporučení pro rozhodnutí Rady o zmocnění k zahájení jednání za účelem dosažení dohody mezi Evropskou unií a Spojenými státy americkými o přeshraničním přístupu k elektronickým důkazům pro justiční spolupráci v trestních věcech, [online], [cit. dne 20. 3. 2019], dostupné: https://ec.europa.eu/info/sites/info/files/recommendation_council_decision_eu_us_e-evidence.pdf

paralelně k cestě mezinárodní justiční spolupráce. Současný stav netransparentního procesu vzbuzuje pochyby o zajištění odpovídající úrovně ochrany soukromí dotčených osob. Iniciativa současně předpokládá umožnění přímé předání obsahových údajů, což by značně urychlilo práci vnitrostátních orgánů a současně míří na zakotvení jasných pravidel v případě kolize norem.[204]

4.3 Rada Evropy

V roce 2013 ratifikovala ČR budapešťskou Úmluvu o počítačové kriminalitě, dokument Rady Evropy, který zakotvuje právní rámec boje s počítačovou kriminalitou a současně směřuje k zakotvení efektivního režimu mezinárodní spolupráce. V současné době je smluvními stranami Úmluvy o počítačové kriminalitě 63 států (z toho 26 členů EU), včetně států mimo Radu Evropy (např. USA). V souvislosti s Úmluvou o počítačové kriminalitě byly zřízeny pracovní skupiny zabývající se problematikou přístupu vnitrostátních orgánů k elektronickým důkazům.[205] Na základě doporučení pracovní skupiny pro cloudové důkazy bylo přistoupeno k přípravě druhého dodatkového protokolu k Úmluvě o počítačové kriminalitě, jehož účelem je nastavení právního rámce spolupráce států v souvislosti s elektronickými důkazy a taktéž zakotvení mechanismu přímé spolupráce s poskytovateli služeb usazených v jiné jurisdikci.

Záměrem připravovaného protokolu je podle všeho změna v koncepci zajišťování údajů, kdy místo uložení údajů již nebude rozhodujícím faktorem. Pro upřesnění je vhodné dodat, že vztah Úmluvy o počítačové kriminalitě a EU jako celku je takový, že EU je pozorovatelskou organizací Výboru pro Úmluvu o počítačové kriminalitě a aktivně se účastní projednávání plánovaného dodatkového protokolu, aby zajistila soulad s unijní legislativou.[206]

[204] Ibid
[205] Cloud Evidence Group a Transborder group
[206] Doporučení pro rozhodnutí Rady o zmocnění k účasti na jednání o druhém dodatkovém protokolu k Úmluvě Rady Evropy o kyberkriminalitě (CETS č. 185)ze dne 5. února 2019

4.4 Shrnutí

Je zjevné, že současně nastavený právní rámec spolupráce států v oblasti předávání důkazů již v souvislosti se zajišťováním elektronických důkazů nepostačuje, a to zejména v důsledku neúnosně dlouhé doby vyřizování příslušných příkazů. Na úrovni EU by situaci zřejmě mohla vyřešit navrhovaná legislativa. Ta přichází s poměrně inovativními principy. Míří na zakotvení přímé spolupráce vnitrostátních orgánů a poskytovatelů služeb, kteří spravují data, tj. elektronické důkazní prostředky. Současně cílí na změnu v koncepci zajišťování takových důkazů. Nebere totiž v potaz hledisko umístění dat.

Problematický však může být právní základ navrhované právní úpravy. To je dle důvodové zprávy postaveno na zásadě vzájemného uznávání vycházející z článku 81 Smlouvy o fungování Evropské unie (dále jen „SFEU“). Otázkou zůstává, do jaké míry lze zásadu vzájemného uznávání chápat i jako spolupráci mezi vnitrostátními orgány a osobami soukromého práva. Dále je otázkou, proč by měla být tato problematika regulována formou nařízení, když například institut evropského vyšetřovacího příkazu je upraven směrnicí a především, podle čl. 82 odst. 2 SFEU mohou být harmonizační pravidla vzájemné přípustnosti důkazů mezi členskými státy stanovena jedině ve formě směrnic.

Prostřednictvím nového zákona „CLOUD Act“ bylo hledisko umístění dat opuštěno i v USA. A stejnou cestou se vydává i iniciativa směřující k přijetí druhého dodatkového protokolu k Úmluvě o počítačové kriminalitě. S ohledem na obsah iniciativy směřující k přijetí dohody mezi EU a USA v oblasti elektronických důkazů je patrný trend, který směřuje v zakotvení přímé spolupráce vnitrostátních orgánů a poskytovatelů služeb. Na jednu stranu se tento postup jeví jako velmi efektivní a do jisté míry i jako nevyhnutelný. Je však nezbytné nastavit dostatečné záruky transparentnosti takového procesu, aby nedocházelo k zásahům do práv a svobod uživatelů.

Závěr

Vytyčeným cílem diplomové práce bylo posoudit, zda současná právní úprava umožňuje orgánům činným v trestním řízení adekvátně reagovat na výzvy nové informační doby. Dále analyzovat, zda mají příslušné orgány k dispozici dostatečně efektivní nástroje k zajišťování elektronických důkazních prostředků a současně zhodnotit, zda je zajištěna dostatečná ochrana před neodůvodněnými zásahy orgánů veřejné moci do práv a svobod jednotlivců. Problematika byla uvozena vymezením pojmu elektronický důkazní prostředek a současně pojednáním o specifikách dat, jež je nezbytné vzít v úvahu při jejich zajišťování a následné analýze. V této souvislosti byly nastíněny moderní přístupy k analýze dat, využívající umělou inteligenci a jejich potenciální role v rámci vyšetřování v blízké budoucnosti.

Právní úprava zajišťovacích institutů na jedné straně příliš nereaguje na technologický vývoj společnosti. Nicméně, jejich obecná povaha umožňuje jejich nadčasovou aplikaci v různých situacích. Zejména instituty vydání a odnětí věci, jakož i domovní prohlídka a související představují pro orgány činné v trestním řízení efektivní nástroje pro zajištění elektronických důkazních prostředků. Významnou otázkou tedy především zůstává, zda dostatečně zaručují ochranu jednotlivce.

Zejména institut odposlechu a záznamu telekomunikačního provozu nastavuje striktní limitující podmínky, jež takovou ochranu poskytují. Problematika *Data retention*, neboli plošného preventivního sběru provozních a lokalizačních údajů, byla v nedávné době předmětem podrobného přezkumu ze strany ÚS. Závěr o ústavní konformitě současně platného právního rámce lze však podrobit kritice. Sledování prakticky veškeré populace ČR prováděné soukromými subjekty bez potřebných záruk proti neoprávněnému shromažďování a zneužití údajů totiž představuje vzhledem ke stupni technologického vývoje pro soukromí jedince větší ohrožení než kdykoliv v minulosti.

Za problematické považuji současné nastavení podmínek pro uplatnění sledování, při kterém dochází k pořizování zvukových, obrazových nebo jiných záznamů. Vývoj sledovacích technologií umožňuje využití tohoto postupu v širokém okruhu situací, a to velmi invazivním způsobem. V této oblasti je tedy patrná potřeba legislativní změny, nejlépe po vzoru podmínek pro uplatnění institutu odposlechu a záznamu telekomunikačního provozu. V rámci druhé kapitoly bylo současně rozebráno, jakým způsobem se praxe staví k zajišťování obsahu elektronické pošty. Výkladové stanovisko

NSZ dovozuje, že pro zajištění aktuálního obsahu e-mailové schránky mají jít orgány činné v trestním řízení cestou soudního příkazu k povolení sledování osob a věcí. Výkladové stanovisko však nebere v potaz skutečnost, že hlavičky e-mailových zpráv obsahují taktéž provozní a lokalizační údaje.

V rámci třetí kapitoly podrobněji rozebírám postup orgánů činných v trestním řízení při odhalování trestné činnosti v prostoru sociálních sítí. V úvodu analyzuji existující judikaturu soudů ve vztahu k pojmu sociální síť. V důsledku nedostatečně efektivní právní úpravy, zejména přeshraničního zajišťování elektronických důkazů, vznikl jakýsi paralelní systém přímé spolupráce s poskytovateli online služeb, založený zejména na dobrovolnosti osob soukromého práva, které mají údaje pod kontrolou. V třetí kapitole rozebírám důvody vniku přímé spolupráce, jakož i její důsledky. Problém dané praxe spočívá zejména ve skutečnosti, že není zajištěna dostatečná transparentnost celého procesu, což vede k oslabení práv a svobod uživatelů online služeb. Současně není postaveno najisto, jaké instituty českého právního řádu mají být užity k zajišťování obsahových údajů ze sociálních sítí a jiných komunikačních platforem.

Rozborem postupu dotčených orgánů v souvislosti s páchání trestné činnosti související se zneužíváním dětí docházím k závěru, že postup zjišťování údajů o telekomunikačním provozu hraje v těchto případech významnou roli, jelikož údaj o IP adrese představuje často prvotní vodítko v rámci zjišťování totožnosti pachatele.

Ačkoliv aktuální právní úprava není s ohledem na technologický rozvoj ideální a trpí řadou nedostatků, na základě mezinárodních závazků došlo k implementaci nových procesních postupů s přímou vazbou na elektronické důkazní prostředky a vzhledem k projednávaným záměrům na mezinárodní úrovni lze předpokládat, že tento trend bude pokračovat. Navrhovaná unijní legislativa směřuje k umožnění přímé spolupráce orgánů činných v trestním řízení a poskytovatelů služeb informační společnosti a elektronických komunikací. Pozitivně hodnotím, že navrhovaná legislativa má upustit od hlediska umístění dat, jako významného faktoru při dožádání dat důležitých pro trestní řízení. Za vzor si přitom bere novou legislativu USA, která je rozebírána v závěrečné pasáži poslední části.

Seznam použitých zkratek

ČR	Česká republika
ESLP	Evropský soud pro lidská práva
EU	Evropská unie
GDPR	Nařízení Evropského parlamentu a rady 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
Listina	Usnesení předsednictva ČNR č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součástí ústavního pořádku České republiky, ve znění pozdějších ústavních zákonů
NCOZ	Národní centrála proti organizovanému zločinu
NS	Nejvyšší soud
NSS	Nejvyšší správní soud
NSZ	Nejvyšší státní zastupitelství
SFEU	Smlouva o fungování Evropské unie
Trestní řád	Zákon č. 141/1961 Sb., o trestním řízení soudním
Úmluva	Evropská úmluva o ochraně lidských práv a svobod
USA	Spojené státy americké
Ústava	Ústava České republiky
ÚS	Ústavní soud

ZEK	Zákon č. 127/2005 Sb., o elektronických komunikacích
ZNSIS	Zákon č. 480/2004 Sb., o některých službách informační společnosti

Seznam použitých zdrojů

Seznam použité literatury

Monografie a komentáře

- CASEY, E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3. vydání, 2011.
- COHEN, F. Digital Forensic Evidence Examination, 4. vydání, 2010.
- FENYK, J., GŘIVNA, T. a CÍSAŘOVÁ, D. Trestní právo procesní. 6., aktualiz. vyd. Praha: Wolters Kluwer, 2015. ISBN 978-80-7478-750-8.
- JELÍNEK, J. a kol. Dokazování v trestním řízení v kontextu práva na spravedlivý proces. Praha: Leges, 2018. ISBN 978-80-7502-287-5.
- JELÍNEK, J., Trestní právo procesní. 5. vydání. Praha: Leges, 2018, ISBN 978–80–7502–278–3.
- KOLOUCH, J., CyberCrime. Praha: CZ.NIC, z. s. p. o., 2016, ISBN 978-80-88168-18-8.
- MAISNER, M. Zákon o některých službách informační společnosti: komentář. V Praze: C.H. Beck, 2016. Beckovy komentáře. ISBN 978-80-7400-449-0.
- MASON, S., and SENG, D editors. Electronic Evidence. School of Advanced Study, University of London, 2017, 4. vydání ISBN 978-1-911507-07-9.
- POLČÁK, R., PÚRY, F. a HARAŠTA, J. Elektronické důkazy v trestním řízení. Brno: Masarykova univerzita, 2015. ISBN 978-80-210-8073-7.
- PORADA, V., POLÁK, P. et al. Kriminalistika. Plzeň: Aleš Čeněk, 2015. ISBN 978-80-7380-558-6.
- SMEJKAL, V. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7.
- ŠÁMAL, P. Trestní řád: komentář. 7., dopl. a přeprac. vyd. V Praze: C.H. Beck, 2013. Velké komentáře. ISBN 978-80-7400-465-0.
- ZAORALOVÁ, P. Procesní použitelnost důkazů v trestním řízení a její meze. Praha: Leges, 2018. Teoretik. ISBN 978-80-7502-310-0.

Odborné články

- BELL, B., BODDINGTON, R., Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery?, Journal of Digital Forensics, Security and Law: Vol 5, 3/2010.
- DASKAL, J., Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0, Stanford Law Review online, 71/2010.
- DOSTÁL, O., Zajišťování důkazů u počítačové kriminality – dožádání, vydání věci a prohlídky (1. díl), Trestněprávní revue, 3/2019.
- GADE, S., MANE, V., Survey on „Triage-based" Digital Forensic Models, International Journal of Engineering Research in Computer Science and Engineering (IJCSE), Vol 3, 7/2016.
- HARAŠTA, J. Obecná prevenční povinnost poskytovatele služeb informační společnosti ve vztahu k informacím ukládaným uživatelem. Právní rozhledy, Nakladatelství C.H. Beck, 2014, roč. 22, č. 17.
- HERZEG, J., Zásada „nemo tenetur" a práva obviněného v trestním řízení, Bulletin advokacie 1-2/2010.
- JELÍNEK, J., K chybějící právní úpravě tzv. prostorového odposlechu v trestním řádu, Bulletin advokacie 7-8/2018.
- KORBEL, F., Ne-odpovědnost poskytovatelů služeb informační společnosti v digitálním světě, Právní prostor, 17. 5. 2018.
- MARTURANA, F., TACCONI, S., A machine learning-based Triage methodology for automated categorization of digital media, Digital investigation, 10/2013.
- ROGERS, M. K., GOLDMAN, J., MISLAN R., WEDGE T., Computer Forensic Field Triage Process Model, Conference on Digital Forensic, Security and Law, 2/2006.
- SCHWARTZ, Paul M., Legal Access to the Global Cloud, UC Berkeley Public Law Research Paper, 118 Columbia Law Review, 20. 6. 2017.

Důvodové zprávy

- Důvodová zpráva, č. 287/2018 Dz, k zákonu č. 287/2018 Sb. kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a některé další zákony [online], str. 34-38, 50-52 [cit. 21. 3. 2019], Dostupné z: https://www.psp.cz/sqw/text/tiskt.sqw?O=8&CT=79&CT1=0.
- Důvodová zpráva, č. COM/2018/225 final - 2018/0108 (COD) k návrhu nařízení Evropského parlamentu a rady o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech, Ve Štrasburku dne 17. 4. 2018, [online], [cit. 27. 3. 2019], Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1559736463321&uri=CELEX%3A52018PC0225.

Seznam použitých právních předpisů a mezinárodních smluv

- Ústavní zákon č. 1/1993 Sb., Ústava České republiky
- Usnesení předsednictva České národní rady č. 2/1993 Sb. o vyhlášení Listiny základních práv a svobod jako součástí ústavního pořádku České republiky
- Zákon č. 141/1961, trestní řád
- Zákon č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních
- Zákon č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže
- Zákon č. 127/2005 Sb., zákon o elektronických komunikacích
- Zákon č. 480/2004 Sb. o některých službách informační společnosti
- Zákon č. 287/2018 Sb. kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a některé další zákony
- Zákon č. 110/2019 Sb., zákon o zpracování osobních údajů
- Vyhláška č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů
- The Clarifying Lawful Overseas Use of Data Act or CLOUD Act (H.R. 4943)
- Sdělení Ministerstva zahraničních věcí ČR č. 104/2013 Sb. m. s., o sjednání Úmluvy o počítačové kriminalitě
- Vyhláška ministra zahraničních věcí č. 143/1988 Sb. o Úmluvě proti mučení a jinému krutému, nelidskému či ponižujícímu zacházení nebo trestání

- Vyhláška ministra zahraničních věcí č. č. 120/1976 Sb. o Mezinárodním paktu o občanských a politických právech a Mezinárodním paktu o hospodářských, sociálních a kulturních právech
- Sdělení federálního ministerstva zahraničních věcí č. 209/1992 o sjednání Úmluvy ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících.
- Sdělení Ministerstva zahraničních věcí o sjednání Smlouvy mezi Českou republikou a Spojenými státy americkými o vzájemné právní pomoci v trestních věcech č. 40/2000 Sb. m. s.
- Sdělení Ministerstva zahraničních věcí o sjednání Dohody o vzájemné právní pomoci mezi Evropskou unií a Spojenými státy americkými č. 5/2010 Sb. m. s.
- Sdělení Ministerstva zahraničních věcí o sjednání Dodatkové úmluvy o vzájemné právní pomoci v trestních věcech mezi Českou republikou a Spojenými státy americkými 7/2010 Sb. m. s.
- Nařízení Evropského parlamentu a rady 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
- Směrnice Evropského parlamentu a Rady 2014/41/EU ze dne 3. dubna 2014 o evropském vyšetřovacím příkazu v trestních věcech
- Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu)

Seznam použitých internetových zdrojů

- Statistika týkající se počtu českých domácností připojených k internetu, [online], [cit. 10. 5. 2019], dostupné: https://www.czso.cz/documents/10180/61508128/0620041809.pdf/8ea8ced6-6822-4f5a-bf29-a57279ac93e7?version=1.3.

- Statistika týkající se počtu Čechů používající sociální sítě, [online], [cit. 10. 5. 2019], dostupné: https://www.czso.cz/csu/czso/vice-nez-polovina-cechu-pouziva-socialni-site.
- CADWALLADR, C., GRAHAM-HARRISON, E., Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, [online], [cit. dne 2. 6. 2019], Dostupné na: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.
- Část pražských soudců se k videokonferencím zatím staví zdrženlivě, Česká justice [online], [cit. 12. 4. 2019], dostupné: http://www.ceska-justice.cz/2017/08/cast-prazskych-soudcu-se-k-videokonferencim-zatim-stavi-zdrzenlive/.
- Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR za rok 2017, [online], [cit. dne 13. 4. 2019], dostupné na https://www.mvcr.cz/clanek/odposlechy-zaznamy-telekomunikacniho-provozu-a-sledovani-osob.aspx.
- Informace pro bezpečnostní složky od společnosti Facebook, [online], [cit. 9. 6. 2019] dostupné na: https://www.facebook.com/safety/groups/law/guidelines/.
- Doporučení pro rozhodnutí Rady o zmocnění k zahájení jednání za účelem dosažení dohody mezi Evropskou unií a Spojenými státy americkými o přeshraničním přístupu k elektronickým důkazům pro justiční spolupráci v trestních věcech, [online], [cit. dne 20. 3. 2019], dostupné: https://ec.europa.eu/info/sites/info/files/recommendation_council_decision_eu_us_e-evidence.pdf.
- Review of the 2010 EU-US MLA Agreement - Examination of draft texts ze dne 7 dubna 2017, [online], [cit. dne 13. 5. 2019], dostupné na: http://statewatch.org/news/2016/apr/eu-council-eu-usa-mutual-legal-assistance-review-07403-07-04-16.pdf.
- Statistiky žádostí týkající se dat uživatelů společnosti Facebook. [online], [cit. dne 10. 6. 2019] Ke stažení na: https://transparency.facebook.com/government-data-requests.

- E-evidence a) Regulation on European Production and Preservation Orders for e-evidence b) Directive on legal representatives for gathering evidence = Policy debate, č. ST 9418 2018 INIT ze dne 29. 5. 2018 [online], [cit. dne 13. 4. 2019], dostupné: http://data.consilium.europa.eu/doc/document/ST-9418-2018-INIT/en/pdf.
- VOKUŠ, J. Kyberkriminalita, Zveřejněné informace za rok 2019, [online], [cit. dne 3. 6. 2019], dostupné na: https://www.policie.cz/clanek/zverejnene-informace-2019-kyberkriminalita.aspx.
- DAVIS, A., New Technology to Fight Child Exploitation [online], [cit. dne 10. 6. 2019], dostupné na: https://newsroom.fb.com/news/2018/10/fighting-child-exploitation/.

Seznam použité judikatury

- Rozhodnutí Nejvyššího soudu České socialistické republiky, sp. zn. 7 Tz 84/69, ze dne 24. 3. 1970, publikováno jako R 38/1970 – I.
- Usnesení Nejvyššího soudu ze dne 15. 12. 2000, sp. zn. 7 Tz 9/2000, publikováno pod č. 2091/2000.
- Nález Ústavního soudu, sp. zn. II. ÚS 255/05 ze dne 23. 6. 2005, publikováno ve Sbírce nálezů a usnesení ÚS, 37/2005, pod č. 128/2005 USn.
- Nález Ústavního soudu ze dne 23. 05. 2007, sp. zn. II. ÚS 615/06, publikováno ve Sbírce nálezů a usnesení ÚS, 45/2007, pod č. 88/2007 USn.
- Nález Ústavního soudu ze dne 25. 8. 2008, sp. zn. IV. ÚS 1780/07, publikováno ve Sbírce nálezů a usnesení ÚS, č. 50/2008, pod č. 147/2008 USn.
- Rozhodnutí Nejvyššího správního soudu, č.j. 1 As 90/2008-189 ze dne 4. 2. 2009, publikováno pod č. NSS 153/2009.
- Usnesení Nejvyššího soudu ze dne 8. 4. 2009, sp. zn. 3 Tdo 1301/2008, publikováno pod č. NS 4823/2009.
- Nález Ústavního soudu ze dne 28. 4. 2009, sp. zn. I. ÚS 536/06, publikováno ve Sbírce nálezů a usnesení ÚS, č. 53/2009, pod č. 100/2009 USn.

- Nález Ústavního soudu, sp. zn. II.ÚS 2806/08 ze dne 27. 1. 2010, publikováno ve Sbírce nálezů a usnesení ÚS, 56/2010, pod č. 15/2010 USn.
- Usnesení Nejvyššího soudu ze dne 4. 8. 2010, sp. zn., 7 Tdo 783/2010, publikováno v Souboru trestních rozhodnutí NS, č. 70/2010, pod č. T 1331.
- Nález Ústavního soudu, sp. zn. II. ÚS 2369/08 ze dne 9. 12. 2010, publikováno ve Sbírce nálezů a usnesení ÚS, 59/2010, pod č. 244/2010 USn.
- Nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/10, publikováno ve Sbírce nálezů a usnesení ÚS, 60/2011, pod č. 52/2011 USn.
- Usnesení Ústavního soudu ze dne 14. 12. 2011, sp. zn. IV. ÚS 3225/09, publikováno pod č. ÚS 3555/2011.
- Nález Ústavního soudu ze dne 20. 12. 2011, sp.zn. Pl. ÚS 24/11, publikováno ve Sbírce nálezů a usnesení ÚS, 63/2011, pod č. 217/2011 USn.
- Nález Ústavního soudu, sp. zn. III.ÚS 3812/12 ze dne 3. 10. 2013, publikováno ve Sbírce nálezů a usnesení ÚS, 71/2013, pod č. 10/2013 Usu.
- Usnesení Městského soudu v Praze ze dne 9. 7. 2014, sp. zn. Nt 615/2014, publikováno v Bulletinu advokacie, 11/2014 jako BA11/2014, s. 51.
- Nález Ústavního soudu ze dne 30. 10. 2014, sp. zn. III. ÚS 3844/13, publikováno ve Sbírce nálezů a usnesení ÚS, 75/2014, pod č. 201/2014 USn.
- Nález Ústavního soudu, sp. zn. I. ÚS 3018/14, 16. 6. 2015, publikováno ve Sbírce nálezů a usnesení ÚS, 77/2015, pod č. 111/2015 USn.
- Stanovisko Nejvyššího soudu ze dne 25. 6. 2015, Tpjn 306/2014, publikováno pod č. R 35/2015 tr. ve Sbírce soudních rozhodnutí a stanovisek, 7/2015.
- Rozhodnutí Nejvyššího soudu, sp. zn. 5 Tdo 1207/2016, ze dne 21. 9. 2016, publikováno jako R 46/2017, a Rozhodnutí Nejvyššího soudu, sp. zn. 4 Tz 107/2002, ze dne 15. 4. 2003 publikováno jako SR 12/2003 v Soudních rozhledech, 12/2003.
- Usnesení Nejvyššího soudu ze dne 7. 6. 2017, sp. zn. 6 Tz 3/2017-II., publikováno ve Sbírce soudních rozhodnutí a stanovisek, 4156/2017, část trestní.

- Usnesení Nejvyššího soud ze dne 25. 10. 2017, sp. zn. 8 Tdo 1106/2017, publikováno ve Sbírce soudních rozhodnutí a stanovisek, 9/2018, pod č. R 42/2018 tr.
- Usnesení Nejvyššího soudu ze dne 31. 1. 2019, č.j. 6 Tdo 72/2019, publikováno pod č. NS 517/2019.
- Nález Ústavního soudu ze dne 14. 5. 2019, sp. zn. Pl. ÚS 45/17, publikováno pod č. ÚS 1148/2019.
- Rozsudek ESLP Benedik proti Slovinsku ze dne 24. 4. 2018 (č. 62357/14).
- Rozsudek ESLP ve věci Jalloh vs. Německo ze dne 11. 7. 2006 (č. 54810/00).
- Rozsudek ESLP ve věci Khodorkovskiy a Lebedev proti Rusku ze dne 25. 7. 2013 (č. č. 11082/06 a 13772/05).
- Rozhodnutí Nejvyššího soudu USA ve věci Spojené státy proti Microsoft Corp. ze dne 17. 4. 2018, No. 17-2 (per curiam).

Seznam výkladových stanovisek Nejvyššího státního zastupitelství

- Výkladové stanovisko Nejvyššího státního zastupitelství č. 9/2001 ze dne 13. 6. 2001 k zajišťování počítačů a jiných nosičů informací při domovní prohlídce a prohlídce jiných prostor a pozemků.
- Výkladové stanovisko Nejvyššího státního zastupitelství č. 4/2005 ze dne 6. června 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.
- Výkladové stanovisko Nejvyššího státního zastupitelství č. 1/2015 ze dne 26. ledna 2015 ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek.
- Výkladové stanovisko Nejvyššího státního zastupitelství č. č. 2/2017 ze dne 30. 8. 2017 ke sjednocení výkladu zákonů a jiných právních předpisů k některým

otázkám postupu státního zástupce při podávání návrhů a provádění domovních prohlídek a prohlídek jiných prostor a pozemků.

- Výkladové stanovisko Nejvyššího státního zastupitelství č. 1/2018 ze dne 11. 5. 2018 ke sjednocení výkladu zákonů a jiných právních předpisů při výkonu působnosti státního zastupitelství podle § 12 odst. 2 zákona č. 283/1993 Sb., o státním zastupitelství, ve znění pozdějších předpisů k problematice pořizování a nakládání s odposlechem a záznamem telekomunikačního provozu.

Seznam ostatních zdrojů

- GARNER, B. (eds.) et al. A. Black's Law Dictionary. 8. vyd., St. Paul (MN, USA): Thomson West, 2004.
- KOČÍ, M. Elektronické důkazní prostředky. Brno: Masarykova univerzita, 2012. Diplomová práce.
- Usnesení Stálé komise pro kontrolu použití odposlechů a záznamů telekomunikačního provozu, použití sledování osob a věcí a rušení provozu elektronických komunikací z 26. schůze ze dne 23. února 2017.
- Doporučení pro rozhodnutí Rady o zmocnění k účasti na jednání o druhém dodatkovém protokolu k Úmluvě Rady Evropy o kyberkriminalitě (CETS č. 185) ze dne 5. února 2019.
- Závazný pokyn policejního prezidenta ze dne 21. dubna 2009 o plnění úkolů v trestním řízení k organizaci výkonu služby, součinnosti, příslušnosti policejních orgánů1) a k provádění některých úkonů podle zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.
- Konzultace s vrchní komisařkou kpt. Mgr. Terezou Andělovou Služby kriminální policie a vyšetřování Odboru analytiky a kybernetické kriminality Policie ČR, KŘP Plzeňského kraje.

Název diplomové práce

Dokazování elektronickými důkazními prostředky

Abstrakt

Diplomová práce se zabývá dokazováním elektronickými důkazními prostředky v rámci trestního procesu. Význam problematiky zajišťování této kategorie důkazních prostředků se spolu s rozvojem technologií významně prohlubuje. Pachatelé rozličných druhů trestné činnosti totiž za sebou v současnosti zanechávají digitální stopu téměř ve všech případech. V diplomové práci se tak autorka zaměřuje na otázku, zda lze takové elektronické důkazní prostředky efektivně zajišťovat. Současně si klade otázku, zda při zajišťování nedochází k excesivním zásahům do základních práv a svobod jednotlivců. Z toho důvodu rozebírá specifika jednotlivých zajišťovacích institutů. S tím související problematiku *data retention* neboli plošného preventivního uchování údajů rozebírá ve světle nejnovější judikatury Ústavního soudu a polemizuje o možných změnách stávající právní úpravy. Pozornost je mimo jiné věnována i novému institutu, jenž předpokládá předběžné uchování dat důležitých pro trestní řízení na základě příkazu dle trestního řádu. Autorka se dále věnuje otázce zajišťování obsahu elektronické pošty. V neposlední řadě rozebírá dílčí problémy jednotlivých postupů pro zajišťování důkazních prostředků, pro příklad nevhodně nastavené limitující podmínky sledování osob a věcí, při němž dochází k pořizování zvukových, obrazových a jiných záznamů.

V diplomové práci je současně nastíněna problematika zajišťování údajů od provozovatelů sociálních sítí. Autorka zde přibližuje způsob dobrovolné spolupráce, který se v této oblasti vyvinul v reakci na neefektivní zákonnou úpravu. Pozornost je věnována možnému řešení v podobě předkládané unijní legislativy, potažmo iniciativy dohody mezi Evropskou unií a Spojenými státy americkými, které reagují na nový zákon Spojených států tzv. CLOUD Act. Tento předpis zakotvil povinnost poskytovatelů online služeb vyhovovat příkazům federálních orgánů a sdělovat uživatelské údaje bez ohledu na to, kde se vlastně tato data fyzicky nacházejí. Autorka se tak v poslední části diplomové práce věnuje navrhovaným principům a jejich přínosu.

Klíčová slova

Elektronické důkazní prostředky, orgány činné v trestním řízení, data

Thesis title

Substantiation of Electronic Evidence

Abstract

Thesis deals with the substantiation of electronic evidence within the framework of criminal procedure. The importance of the issue of obtaining such a category of evidence further intensifies as the technology continues to develop. The various types of crime perpetrators simultaneously leave behind digital traces with regard to almost all cases. Therefore, the author focuses on the issue, whether is it possible to obtain such an evidence effectively. The author concurrently takes into account the question of whether the process of obtaining electronic evidence meet certain threshold of protection of the fundamental rights and freedoms of an individual. Hence, the author analyses the characteristic of the individual relevant procedures. The issue of *data retention*, in other words the areal data collection and preservation in the light of recent case law as well as the possible adjustments to current legislation is subject to scrutiny. Attention is drawn, inter alia, to the novel procedure which enables preventive preservation of data important for the criminal proceedings. Furthermore, the author takes into account the issue of obtaining the content of the communication by means of electronic mail. Moreover, thesis deals with the partial problems of the provisions with regard to the obtaining of electronic evidence, e.g. unsuitable limitation conditions of surveillance of persons and items, during which shall any audio, visual or other records be made.

Thesis further outlines the issue of how to obtain relevant data from the social media. In this context, the voluntary channel of cooperation has come along as a response to the current inefficient legislation. Thus, the author has chosen to discuss the European Union proposal, as well as the initiation of the mutual agreement between the European Union and the USA. These constitute a reaction to the new US law, i.e. CLOUD Act, which established the obligation of social media to provide for the user data to federal authorities regardless of the location of such data. In the last part of the thesis, the author deals with the proposed principles and their contribution.

Keywords

Electronic evidence, law enforcement authorities, data