PŘÍSTUP ORGÁNŮ ČINNÝCH V TRESTNÍM ŘÍZENÍ K DATŮM ULOŽENÝM V CLOUDU[*]

KATEŘINA HLAVÁČOVÁ[**], OLIVER CHORVÁT[***]

ABSTRAKT

Cloud computing využívá datová centra umístěná po celém světě a data uložená v těchto úložištích mohou migrovat mezi různými státy každou sekundu. Existence cloud computingu tedy minimalizuje existenci hranic a způsob, jakým jsou data uložena, klade vyšší nároky zejména na orgány činné v trestním řízení. Orgán činný v trestním řízení musí správně kvalifikovat odpovídající zajišťovací institut a poté zajistit příslušné povolení podle trestního řádu. Příspěvek se tudíž zaměří na analýzu použitelných zajišťovacích úkonů podle trestního řádu pro zajištění dat uložených v cloudu. Dalším aspektem nutným k posouzení je teritoriální omezení pravomoci orgánů činných v trestním řízení a možnost, že se datová centra nacházejí v jurisdikci jiných států.

KLÍČOVÁ SLOVA

cloud computing, důkaz, kyberkriminalita, zajišťovací úkony

ABSTRACT

Cloud computing uses data centers located around the world and the data stored in these repositories may migrate between different countries every second. Exis-

[*] Příspěvek byl odpřednášen dne 23. září 2016 na konferenci České právo a informační technologie 2016 v rámci sekce Elektronické důkazy. Příspěvek byl zpracován v rámci řešení projektu specifického výzkumu na téma „Vývojové tendence sankční politiky (MUNI/A/1347/2015)“.

[**] Pplk. Mgr. Kateřina Hlaváčová působí na Policejním prezidiu ČR a je doktorskou studentkou na Katedře trestního práva PrF MU. Kontaktní e-mail je 376181@mail.muni.cz.

[***] Mgr. et Mgr. Oliver Chorvát je advokátním koncipientem v advokátní kanceláři Weil, Gotshal & Manges v Praze. Kontaktní e-mail je oliver.chorvat@weil.com.

tence of cloud computing thus minimizes the existence of borders and the way the data is stored places higher demands especially on law enforcement authorities. The law enforcement authority must properly identify the corresponding seizure measure and then obtain the appropriate authorization under the Criminal Procedure Code. The paper therefore focuses on the analysis of the applicable seizure measures under the Criminal Procedure Code for seizure of data stored in the cloud. Another aspect that must be assessed is the territorial limitation of powers of law enforcement authorities and the possibility that data centers are located in the jurisdiction of other countries.

KEY WORDS

cloud computing, evidence, cybercrime, seizure measures

1. ÚVOD

S vývojem informačních a komunikačních technologií se mění způsob páchání trestné činnosti. Některé nově vyvinuté formy trestné činnosti jsou zcela páchány v kyberprostoru, zatímco tradiční formy trestné činnosti alespoň zanechávají elektronické stopy. Příkladem budiž výtržnictví na ulici natočeno mobilním zařízením či elektronická komunikace týkající se spáchané trestné činnosti v minulosti. U kybernetických trestných činů je vytěžení elektronických dat nezbytným předpokladem pro odsouzení pachatele, u ostatních trestných činů mohou elektronická data představovat významné ulehčení důkazní situace. Z kriminalistického hlediska mohou tedy elektronická data představovat významný zdroj důkazního materiálu. Orgány činné v trestním řízení, zejména orgány policejní, jsou povinny za účelem efektivity odhalování vyšetřování trestné činnosti modernizovat své postupy a zároveň aplikovat takové instituty trestního řádu, které zajistí adekvátní ochranu základním lidským právům a svobodám jednotlivců. Některá pro trestní řízení relevantní elektronická data mohou být uložená v cloudovém úložišti. Tato úložiště se těší vysoké oblibě nejen u podnikajících osob, ale také u běžných uživatelů internetu a lze do budoucna předpokládat jejich další rozšíření. Je nepochybné, že kriminalistické využití elektronických dat uložených v cloudovém úložišti je pro policejní praxi ne-

vyhnutelné. To klade zvýšené nároky zejména na zákonodárce, kteří by měli usilovat o modernizaci právního řádu schopného efektivního zajišťování elektronických dat, a rovněž na orgány činné v trestním řízení, jež musí analyzovat aktuální právní stav a najít způsob k zákonnému a procesně využitelnému získávání elektronických dat. Trestní zákoník účinný od počátku roku 2010 zareagoval na nové formy páchání trestné činnosti zavedením skutkových podstat tzv. kybernetických trestných činů[1]. Kriminalizace těchto jednání si však vyžaduje adekvátní procesněprávní instituty pro zajišťování elektronických dat schopné reagovat na přeshraniční a všudypřítomný charakter kyberprostoru.

2. CLOUD COMPUTING

Za široce uznávanou a do značné míry rozšířenou lze považovat definici popsanou v dokumentu amerického Národního institutu standardů technologie.[2] Podle tohoto dokumentu platí, že „*cloud computing je model umožňující všudepřítomný, pohodlný, na vyžádání dostupný síťový přístup ke sdílenému fondu konfigurovatelných výpočetních prostředků (např. sítě, servery, úložiště, aplikace a služby), které mohou být rychle opatřeny a uvolněny s minimálním úsilím na jejich správu anebo interakci ze strany poskytovatele služby.*“[3] Pozornost je přitom nutno věnovat zejména tomu, že se má jednat o jakýsi sdílený fond výpočetních prostředků, které daný cloud tvoří. Tímto se model cloud computingu, zejména v kontextu možnosti zajistit uložená data, zásadním způsobem liší od prostého hostingu. Pod pojmem hosting se obecně rozumí uložení dat v externím datovém úložišti, přičemž k takto uloženým datům je možné přistupovat po síti, tedy bez ohledu na lokalitu, odkud má k přístupu dojít.[4]

---

[1] Například § 230 a § 231 zákona č. 40/2009 Sb., trestního zákoníku.

[2] MELL, Peter a Timothy GRANCE. The NIST Definition of Cloud Computing. *Recommendations of the National Institute of Standards and Technology* [online]. 2011 [cit. 15. 10. 2016]. Dostupné z: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[3] Cloud computing is model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Z uvedeného je patrné, že pojem hosting je obecnější – vymezuje pouze obsah služby (externí úložiště dat), nikoliv ale už to, v rámci jaké technické architektury budou tato data uložena. Je možné, a v praxi celkem obvyklé, že tato data budou uložena právě v cloudu. Stejně tak je ovšem možné, a to zejména u menších poskytovatelů služeb, že model cloud computing využit nebude. V tom případě se tedy nebude jednat o žádný sdílený fond výpočetních prostředků, ale pouze o menší množství serverů a pevných disků, jež se budou zpravidla nacházet v jedné lokalitě. Z toho důvodu bude pak také možné mít jistotu, že pokud jsou požadovaná data uložená u daného poskytovatele služby, pak se budou fyzicky nacházet právě v dané lokalitě na příslušných pevných discích, které by případně mohly být orgány činnými v trestním řízení zajištěny.

To ovšem v případě cloud computingu neplatí, jelikož v rámci tohoto modelu často neexistuje pevný a trvalý vztah mezi daty a místem, resp. konkrétním pevným diskem, kde jsou uloženy. Naopak je obvyklé, že se data mezi úložišti svévolně[5] pohybují, nebo že u jednoho poskytovatele cloudové infrastruktury jsou uložena uživatelská data patřící uživatelům odlišných cloudových služeb.[6] To je přímým důsledkem modelu cloud computingu, jenž umožňuje sdílení výpočetních zdrojů, které mimo jiné podporuje efektivitu tohoto modelu. Nadto je rovněž běžné, že výpočetní zdroje tvořící daný cloud se často nachází fyzicky v odlišných lokalitách, což je dokonce žádoucí, zejména s ohledem na fyzickou bezpečnost a zálohování (např. ochrana před živelnými pohromami). Z těchto důvodů nutno konstatovat, že je krajně nepravděpodobné, aby bylo možno zajistit data uložená v cloudu tím způsobem, že by orgány činné v trestním řízení pří-

[4] Velice rozšířenou formou hostingu je tzv. webhosting, tedy hosting webových stránek. V tomto případě (zjednodušeně řečeno) dochází toliko přístupu k datům uloženým na jiném místě síti (webové stránky). Stejně tak je často nabízenou službou tzv. Filehosting, který umožňuje uživatelům uschovat data na serverech poskytovatele služby.

[5] Ve skutečnosti samozřejmě nejde o to, že by snad data cestovala z vlastní vůle, nýbrž jejich přesuny jsou způsobovány různými technickými procesy v rámci infrastruktury, tudíž se mohou zvenčí jevit jako nahodilé.

[6] Jako příklady služeb resp. platforem cloudové infrastruktury umožňující nasazení cloudových služeb provozovaných třetími stranami lze uvést Amazon Web Services nebo Google Cloud Platform.

slušnou výpočetní techniku (zejména pevné disky) zajistily prostřednictvím zajišťovacích úkonů směřujících k zajištění hmotné věci (§ 78 a násl. trestního řádu). Jelikož tedy tento způsob zajištění dat není aplikovatelný na data uložená v cloudu, ale pouze na data uložená v „prostém" hostingu, není tato varianta postupu dále diskutována.

Za zajímavost lze v této souvislosti považovat případ, který byl před jistou dobou hodně diskutován v médiích. V rámci trestního řízení policejní orgán zajistil při prohlídce jiných prostor (§ 83a trestního řádu) jistý počet pevných disků, přičemž se mělo jednat o úložiště, kde se nacházela data, jež byla pro trestní řízení důležitá.[7] Jádrem případu pak byla otázka, zda data uložená na těchto discích nacházejících se v prostorách provozovatele příslušného úložiště podléhají režimu dle § 85b trestního řádu (prostory, v nichž advokát vykonává advokacii). Při informování o tomto případu média neváhala používat pojem cloud.[8] Jak ovšem bylo objasněno výše, o cloud v pravém smyslu slova, resp. v souladu se zde citovanou definicí, se nejednalo. Pokud by se skutečně mělo jednat o cloud, bylo by zajištění dat prostřednictvím zajištění pevných disků prakticky nemožné (viz výše). Dané úložiště bylo naopak provozováno lokálně, tedy jako „prostý" hosting. Na druhou stranu ovšem nutno konstatovat, že byť není používání pojmu cloud v tomto případě v souladu s technickou definicí popsanou výše, nelze takovouto situaci kategoricky kritizovat, jelikož pojem cloud computing je i odbornou veřejností často používán tak, že není kladen důraz na jeho přesný, resp. původní technický význam. V populárně naučné literatuře se pak lze setkat s různými zjednodušeními, například že cloud computing znamená jednoduše ukládání dat na internetu, resp. že cloud je vlastně pouze metafora pro internet.[9]

---

[7] Pro bližší skutkové okolnosti případu viz usnesení Městského soudu v Praze č. j. Nt 615/2014 ze dne 9. 7. 2014.

[8] Případ vyvolal živou reakci, která byla uvedena titulky jako například: „Průlom: Policie může na data advokátů uložená v cloudu" (aktualne.cz), „Data uložená v cloudu jsou před policií chráněna méně než ta uložená fyzicky" (lupa.cz), „Data cloudu nejsou chráněna advokátním tajemstvím" (pravniprostor.cz).

[9] GRIFFITH, Eric. What Is Cloud Computing? *PC Magazine* [online]. 5. 5. 2016 [cit. 15. 10. 2016]. Dostupné z: http://www.pcmag.com/article2/0,2817,2372163,00.asp

3. OCHRANA SOUKROMÍ V PODOBĚ PRÁVA NA INFORMAČNÍ SEBEURČENÍ

Obecně je nutné každý úkon provedený orgánem veřejné moci posuzovat z toho hlediska, zdali je taková činnost schopná zasáhnout do práv právem chráněných zájmů jednotlivců či ne. V případě, že takový úkon, zákrok či zásah orgánů veřejné moci představuje zásah do práv a právem chráněných zájmů jednotlivců, je vždy nutné hledat v právním řádu České republiky pro takové jednání výslovné zákonné zmocnění.

Sledování a zajišťování elektronických dat uložených v cloudovém úložišti je nezbytné posuzovat v širším kontextu z hlediska práva na respekt k soukromému životu, jehož garanci lze dovozovat z čl. 7 odst. 1, čl. 10, 12 a 13 Listiny základních práv svobod, jakož i z čl. 8 Úmluvy o ochraně lidských práv a základních svobod. Jednou ze základních funkcí ochrany soukromí je zajistit prostor pro rozvoj a seberealizaci individuální osobnosti. Právo na ochranu soukromí proto v sobě zahrnuje rovněž garanci sebeurčení v podobě rozhodování jednotlivce o sobě samém. Řečeno jinými slovy, ochrana soukromí zaručuje rovněž právo jednotlivých osob podle svého rozhodnout o tom, zda a v jakém rozsahu budou skutečnosti a informace z jejich osobního soukromí zpřístupněny jiným osobám[10]. Tímto způsobem vymezené právo lze jednoduše označit jako právo na informační sebeurčení.[11] Evropský soud pro lidská práva dovodil jeho ochranu z práva na respektování soukromého a rodinného života podle čl. 8 Úmluvy o ochraně lidských práv a základních svobod.[12] Právo na ochranu soukromí má dvě dimenze, a to negativní a pozitivní. Problematika přístupu orgánů činných v trestním řízení do cloudového úložiště se dotýká zejména dimenze negativní, což znamená zákaz orgánů veřejné moci zasahovat do soukromí občanů, pokud takový zákaz není výslovně upraven v zákoně a není nezbytný v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, předcházení ne-

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

[11] Nález Ústavního soudu ČR ze dne 17. července 2007, sp. zn. IV. ÚS 23/05.

[12] Např. rozhodnutí Evropského soudu pro lidská práva ze dne 6. září 1978 ve věci stížnosti č. 5029/71 - Klass a další proti Německu.

pokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných.[13] Z ústavního pořádku ČR plyne, že k prolomení ochrany soukromí může dojít jen zcela výjimečně a jen je-li to nezbytné, a účelu sledovaného veřejným zájmem nelze dosáhnout jinak.[14] K tomu, aby tyto meze nezbytnosti nebyly překročeny, musí v právním řádu koexistovat se zákonným zmocněním zásahu do soukromí také systém adekvátních záruk a účinná kontrola jejich dodržování.[15] Navíc k tomu, aby elektronická data zajištěna policejním orgánem mohla sloužit jako důkaz v trestním řízení, je nutné, aby byla zajištěna v procesu dokazování procesně přípustným způsobem podle pravidel trestního řízení. Lze bezpochyby konstatovat, že sledování elektronických dat uchovávaných v soukromém cloudovém úložišti orgánem veřejné moci představuje závažné prolomení práva na soukromí uživatelů. Data jsou považována za uchovávaná v soukromí i za předpokladu, že je uživatel zpřístupnil třetí osobě – poskytovateli cloudu. Lze podotknout, že v USA není tento závěr zcela jednoznačný, a to díky takzvané „*third-party doctrine*“ stanovící, že data vědomě poskytnutá třetí osobě ztrácí ochranu v podobě práva na soukromí.[16]

Z nálezů Ústavního soudu týkajících se záznamu telekomunikačního provozu[17] lze analogicky dovodit, že hodná ochrany ve smyslu čl. 13 Listiny základních práva svobod jsou jednak data obsahová, a jednak data provozní, například datum vytvoření souborů, informace o přihlášení uživatele do cloudu, informace o platbách za cloudové služby apod.

Z výše uvedeného vyplývá, že k tomu, aby mohl policejní orgán legálně zajistit elektronická data uchovávaná v soukromí, která mají sloužit jako důkaz v trestním řízení, je nutné, aby užil institut, který je jednak obsažen

---

[13] KOWALCZUK, Izabela, Katarzyna SZYMIELEWICZ, Tomasz RYCHLICKI. The protection of privacy in Poland in the digital environment. *International Data Privacy Law*. 2011, (3), 161-171.

[14] Nález Ústavního soudu ze dne 29. února 2008, sp. zn. I. ÚS 3038/07, nález Ústavního soudu ze dne 13. února 2001, sp. zn. IV. ÚS 536/2000.

[15] Nález Ústavního soudu ČR ze dne 27. září 2007, sp. zn. II. ÚS 789/06.

[16] SERAFINO, Laurie Buchan. "I Know My Rights, So You Go'n Need Warrant for That": The Fourth Amendment, Riley's Impact, And Warrantless Searches of Third-Party Clouds. *Berkeley Journal of Criminal Law.* 2014, (19:2), 155-203.

[17] Nález Ústavního soudu ze dne 22. ledna 2011, sp. zn. II. ÚS 502/2000.

v trestním řádu a jednak poskytuje adekvátní záruky proti jeho zneužití, tedy zejména povolení státního zástupce či soudce.

4. POČÍTAČOVÝ SYSTÉM

Pojem „počítačový systém“ nalezneme v ustanoveních trestního zákoníku hned na několika místech[18]. Definici tohoto pojmu bychom však ve vnitrostátních právních předpisech hledali marně. Jedinou legální definici pojmu „počítačový systém“ obsahuje Úmluva o počítačové kriminalitě, jež je součástí právního řádu České republiky na základě čl. 10 Ústavy ČR. Úmluva o počítačové kriminalitě definuje počítačový systém jako „*jakékoli zařízení nebo skupinu propojených nebo přidružených zařízení, z nichž jedno nebo více provádí automatické zpracování dat podle programu.*“[19] Nezáleží na tom, zdali je či není systém připojen ke globální síti internet. Automatickým zpracováním dat je myšleno, že data jsou zpracovávána bez lidského přičinění pomocí počítačového programu. Pojem „počítačový systém“ v sobě zahrnuje nejen procesor, operační paměť či pevný disk, nýbrž rovněž tzv. přidružená zařízení, jakými jsou například tiskárna, monitor, čtečky biometrických údajů[20] apod., a je tudíž širším pojmem než pojem „počítač“.

Takto široce pojatá definice by mohla budit dojem, že součástí jednoho počítačového systému jsou rovněž i propojená zařízení, kterým je například i cloudové úložiště.[21] V takovém případě by byl přístup policejního orgánu k datům uloženým v cloudu prostřednictvím počítačového systému pachatele možný na základě jednoho institutu potřebného k jeho zajištění. Jinými slovy řečeno, zajistil-li by policejní orgán v rámci domovní prohlídky počítač pachatele, na kterém jsou ve webovém prohlížeči uloženy přístupové údaje do cloudového úložiště, mohl by policista zajistit data uložená v tomto úložišti již na základě povolení k domovní prohlídce.

---

[18] Například § 182, § 230 či § 231 zákona č. 40/2009 Sb., trestního zákoníku.

[19] Čl. 1 písm. a) Úmluvy o počítačové kriminalitě.

[20] Convention on Cybercrime, Explanatory Report, Article 1.

[21] Srov. POLČÁK, Radim, František PÚRY, Jakub HARAŠTA, Matěj MYŠKA, Václav STUPKA. *Elektronické důkazy v trestním řízení*. 1. vydání. Brno: Masarykova univerzita, 2015. Spisy Právnické fakulty Masarykovy univerzity. S. 105. ISBN 978-80-210-8073-7.

Podle našeho názoru by však takový výklad nebyl správný. Cloudové úložiště fungující na oddělených serverech samo o sobě tvoří další počítačový systém. Výklad, podle kterého je součástí jednoho počítačového systému další propojený počítačový systém, by vedl k nepřijatelným důsledkům. Argumentum *ad absurdum* by měl policista z jednoho legálně zajištěného počítačového systému pachatele přístup do všech dalších propojených počítačových systémů jednotlivců. Dovedeme-li to do extrémních důsledků, měl by policista přístup ke všem počítačům zapojeným do globální sítě internet. Ačkoliv Úmluva o počítačové kriminalitě hovoří výslovně o „*skupině propojených počítačů*“, je na místě v případě zásahu do práva na informační sebeurčení výklad co možná nejrestriktivnější. V neprospěch extenzivního výkladu pojmu „*počítačový systém*“ hovoří kontextuální výklad Úmluvy o počítačové kriminalitě. Přesněji řečeno ujednání čl. 19 týkající se prohlídky a zajištění uložených počítačových dat v odstavci 2 stanoví povinnost pro smluvní státy přijmout opatření, které zajistí, aby policejní orgán, jenž má přístup k jednomu počítačovému systému a je přesvědčen, že hledaná data jsou uložena v jiném počítačovém systému přístupném z původního počítačového systému, měl prostředky k urychlenému rozšíření prohlídky i k tomuto druhému systému. Je tedy zřejmé, že pokud by bylo úmyslem tvůrců Úmluvy o počítačové kriminalitě vykládat pojem počítačový systém tak extenzivním způsobem, jak bylo uvedeno shora, postrádalo by toto ujednání zcela smysl. Cloudové úložiště je tedy podle našeho názoru nutné pokládat za samostatný počítačový systém a přístup orgánů činných v trestním řízení k němu vyžaduje oddělený zajišťovací úkon.

5. DATA NACHÁZEJÍCÍ SE V POČÍTAČI

Některá cloudová úložiště nabízejí možnost přistupovat k souborům zde uloženým prostřednictvím složky v počítači, která se automaticky synchronizuje pomocí synchronizačního programu. Tento program umožňuje uživateli nastavit si správu ukládaných dat takovým způsobem, že se data při připojení k internetu automaticky stahují a ukládají do paměti datového nosiče uživatele a jsou zde uloženy do jejich trvalého odstranění.

V případě, že se kriminalistický technik na základě některého ze zajišťovacích úkonů (například § 78, § 79, § 82 trestního řádu) dostane k počítačovému systému důležitému pro trestní řízení, zpravidla pořídí tzv. bitovou kopii pevného disku. Bitová kopie je přesný otisk pevného disku, včetně systémové struktury, nevyužitého místa, nealokovaného místa i fragmentů vymazaných souborů, jež byly zčásti přepsány novými. Na bitové kopii tedy budou soubory z cloudového úložiště dostupné nikoliv pouze z webového rozhraní. Bylo-li tedy shora řečeno, že data uložená v cloudu nejsou součástí zajištěného počítačového systému, platí o těchto datech uložených zároveň na pevném disku přesný opak. K těmto datům poté je možné přistupovat již na základě opatření učiněného podle výše zmíněných zajišťovacích úkonů.

Lze si rovněž představit aplikaci výše popsaného právního závěru na data, jež se v okamžiku provádění zajišťovacího úkonu nachází v operační paměti (RAM). Z právního hlediska totiž není důvodu, proč by tato data měla podléhat odlišnému režimu pouze proto, že se fyzicky nachází na jiném komponentu daného počítačového systému. Z hlediska technického jsou ovšem jisté rozdíly patrné. Prvním je, že data v operační paměti zpravidla nebudou uložena tak „úhledně“, jako je tomu na pevném disku. V operační paměti může být například zrovna načtena pouze část daného souboru, či nemusí být vždy seznatelné, o který soubor se přesně jedná. Lze tedy konstatovat, že analýza obsahu operační paměti je úkol více náročný na expertízu pro kriminalistického technika než „pouhá“ analýza bitové kopie pevného disku.

Dalším podstatným rozdílem operační paměti oproti pevnému disku je, že se jedná o paměť tzv. volatilní, což znamená, že obsah této paměti se ztrácí v průběhu sekund po odpojení od elektrického proudu (vypnutí počítače). To znamená, že zajištění dat z operační paměti je nutno předem pečlivě naplánovat. Pokud by totiž kriminalistický technik postupoval obvyklým způsobem, tedy že počítač vypne a pevný disk připojí k zařízení na pořizování bitové kopie, v mezidobí by se obsah operační paměti nenávratně ztratil. Proto je nutno postupovat při pořizování kopie obsahu operační paměti tak, aby proběhlo co nejdříve po vypnutí příslušného počí-

tače. Za účelem prodloužení doby, po kterou lze data zajistit, než se ztratí, lze pak s úspěchem použít metodu schlazení paměťového modulu na velice nízkou teplotu.[22]

Pokud se ovšem podaří překonat výše nastíněné problémy a další značné praktické komplikace s tímto postupem spojené, může obsah operační paměti odkrýt něco více než bitová kopie pevného disku příslušného počítače. V operační paměti se totiž oproti pevnému disku může navíc nacházet například obsah souboru aktuálně prohlíženého na obrazovce, anebo šifrovací klíč k pevnému disku, pokud daný počítač využívá šifrování pevného disku. Z praktického hlediska však bude vždy nutné vyhodnotit účelnost takového postupu.

6. PŘÍSTUP „SVÉPOMOCÍ“

Jedna z nejčastějších situací, která se v policejní praxi může stát, je, že policista má přístup ke konkrétnímu počítačovému systému pachatele, jehož prostřednictvím se lze dostat přes hesla uložená ve webovém prohlížeči do cloudového úložiště. Svépomocí jsme tento přístup nazvali proto, že k jeho provedení není zapotřebí žádné součinnosti poskytovatele cloudových služeb. Jak jsme již nastínili shora, přístup orgánu činného v trestním řízení do cloudového úložiště pomocí webového rozhraní je přístupem do jiného odděleného počítačového systému, a nelze tudíž data zajistit na základě původního zajišťovacího institutu. Ukládaná data, jež nejsou veřejně přístupná, jsou uchovávána v soukromí jednotlivců a cloudové úložiště má charakter virtuálního soukromého prostoru. Je tedy na uvážení jednotlivce, v jakém rozsahu a za jakých okolností budou tato data zpřístupněna třetím osobám.

Dlužno podotknout, že trestní řád ne zcela úplně přiléhavě reaguje na tyto nové formy zajišťování důkazních prostředků. Proto je úkolem orgánů činných v trestním řízení využít takového institutu, který bude ospravedlňovat takový zásah a bude zaručovat záruky proti jeho zneužití. Zjišťování

[22] HALDERMAN, J. Alex et al. *Lest We Remember: Cold Boot Attacks on Encryption Keys* [online]. 2009 [cit. 15. 10. 2016]. Dostupné z: https://www.usenix.org/legacy/event/sec08/tech/full_papers/halderman/halderman_html

obsahu záznamů uchovávaných v soukromí za použití technických prostředků umožňuje se souhlasem soudce ustanovení o sledování osob a věcí podle § 158d odst. 3 trestního řádu. Ačkoliv se jedná o prostředek operativně pátrací činnosti, která je obecně považována za činnost utajenou a skrytou, je vzhledem k absenci jiného zajišťovacího institutu jeho užití zcela adekvátní. Samozřejmě musí být dán vztah mezi cloudovým úložištěm a podezřením ze spáchání určité trestné činnosti, což musí vyplývat z konkrétních indicií[23]. V této souvislosti nelze nepřipomenout rozhodnutí Ústavního soudu[24] týkající se zjišťování obsahu e-mailových schránek právě pomocí tzv. prostorového odposlechu. Z tohoto rozhodnutí lze analogicky dovodit jeho použitelnost na zajišťování obsahu cloudového úložiště. Institut prostorového odposlechu, jenž je podmíněn souhlasem soudce, je tudíž dostatečnou zákonnou licencí pro zásah do práva na informační sebeurčení. Jak jsme již uvedli, cloudové úložiště lze chápat jako soukromý virtuální prostor srovnatelný s každým jiným soukromým prostorem, ve kterém lze využít institutu sledování osob a věcí.

Mezi jednotlivými orgány činnými v trestním řízení se však názor na tuto problematiku značně liší. Mezi některými policisty a dokonce i státními zástupci stále panuje názor, že ke vstupu do cloudového úložiště postačí úkon k zajištění původního počítačového systému, například domovní prohlídka či odnětí věci. S ohledem na judikaturu Ústavního soudu[25] a výkladové stanovisko Nejvyššího státního zastupitelství[26] k zjišťování obsahu e-mailových schránek se však s tímto názorem nemůžeme ztotožnit. Ostatně podmínění vstupu do cloudového úložiště povolením soudce je zcela běžnou praxí i v ostatních právních řádech. Například v Austrálii, Kanadě či Dánsku je nutný tzv. příkaz k prohlídce (search warrant), a to pouze

[23] Nález Ústavního soudu ČR ze dne 27. ledna 2010, sp. zn. II. ÚS 2806/08.

[24] Usnesení Ústavního soudu ČR ze dne 3. října 2013, sp. zn. II. ÚS 3812/2012.

[25] Tamtéž.

[26] Stanovisko Nejvyššího státního zastupitelství poř. č. 1/2015 ke sjednocení výkladu zákonu a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek.

pokud je zde důvodné podezření, že se v cloudovém úložišti nacházejí informace důležité pro trestní řízení.[27]

7. VEŘEJNĚ PŘÍSTUPNÁ DATA

Jednou z často nabízených funkcí cloudového úložiště je sdílení jeho obsahu s ostatními uživateli. Povaha cloudového úložiště proto nemusí být vždy soukromá a vstup do něj nemusí narušovat právo na informační sebeurčení. Na tomto místě vyvstává otázka, jaká je hranice mezi veřejně přístupnými daty a daty uchovávanými v soukromí. Pojem „veřejně přístupná data" by měl být dle našeho názoru vykládán restriktivním způsobem, neboť pro uživatele to vždy představuje nižší míru ochrany. Domníváme se, že je-li cloudové úložiště přístupné určitému vymezenému okruhu osob, nehledě na jejich počet, jedná se o prostor soukromý. Analogicky lze úložiště přirovnat k profilu na sociální síti Facebook, který je přístupný pouze pro určitý okruh osob - tzv. přátel. Těchto osob může být klidně i tisíce, o jejich zařazení mezi „přátele" však rozhoduje vlastník profilu svým projevem vůle a je nutné tento prostor považovat za soukromý.[28] Obdobné teze lze vztáhnout na cloudová úložiště. Je-li sdílení jeho obsahu s určitou osobou závislé na projevu vůle uživatele, je nutné tento prostor považovat za soukromý a platí o něm výše uvedené. Má-li policista možnost dostat se k datům pachatele uloženým v cloudovém úložišti prostřednictvím profilu jiné osoby, která přístup poskytne dobrovolně, je přesto nutné opatřit si povolení podle § 158d odst. 3 trestního řádu.

Jsou-li však data přístupná neurčitému předem nedefinovanému okruhu osob, je možné zajistit data mající vztah k prověřované události ohledáním.[29] Ohledání je kriminalistická metoda, kterou se na základě bezprostředního pozorování zjišťuje a podchycuje materiální situace nebo stav objektů, majících vztah k prověřované události k získání důkazů dalších informací důležitých pro trestní řízení. Podstatou ohledání je to, že policista

[27] MAXWEL, Winston, Christopher WOLF. *A Global Reality: Governmental Access to Data in the Cloud* [online]. 2012 [cit. 15. 10. 2016].

[28] Srov. nález Ústavního soudu ČR ze dne 30. října 2014, sp. zn. III. ÚS 3844/13.

[29] § 113 zákona č. 141/1961 Sb., zákona trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.

bezprostředně svými smysly poznává skutečnosti, které mají důkazní nebo taktický charakter.[30] Prostřednictvím ohledání tedy lze zjistit a zkoumat veřejně přístupná data, jež mohou sloužit jako důkaz v trestním řízení. Mají-li mít výsledky ohledání důkazní charakter pro potřeby trestního řízení, musí být úkony při ohledání provedeny v souladu s trestním řádem. Zde je nejdůležitější neodkladnost ohledání, neboť data ve virtuálním prostředí podléhají velmi rychlým změnám, a samozřejmě dokumentace postupu a jeho výsledku.

Co se týká způsobu zajišťování obsahu cloudového úložiště, je možné vytvořit tzv. prostou kopii, tedy otisk vizuální podoby prostřednictvím funkce „print screen“. Obvyklejším a účinnějším způsobem zajištění však bude vytvoření kopie dat zde uložených. V této souvislosti se lze tázat, zdali není na místě využití § 158d odst. 2 trestního řádu, podle kterého lze pořídit záznam o sledované věci pouze na základě písemného povolení státního zástupce. I sledování lze stejně jako ohledání označit za pozorování za účelem objasnění skutečností důležitých pro trestní řízení. Sledování však je na rozdíl od ohledání operativně pátrací činností, jež se vyznačuje svým utajovaným charakterem.[31] Běžnou a základní funkcionalitou cloudového úložiště je „stáhnutí“ (tedy pořízení kopie) dat na vlastní pevný disk. Uživatel cloudu si tudíž musí být vědom toho, že veřejně přístupný obsah si může „stáhnout“ kdokoliv, a to i orgán činný v trestním řízení. Vytváření kopie dat ve veřejně přístupném cloudovém úložišti tedy není podle našeho názoru prováděno utajovaným způsobem, není proto nutné postupovat podle § 158d odst. 2 trestního řádu.

8. PŘÍSTUP PROSTŘEDNICTVÍM POSKYTOVATELE CLOUDOVÝCH SLUŽEB

Neméně častou situací v praxi orgánů činných v trestním řízení je, že tento orgán má vědomí o cloudovém úložišti pachatele, nemá však k němu pří-

[30] STRAUS, Jiří. *Kriminalistická taktika*. 2. rozš. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2008. ISBN 978-80-7380-095-6.

[31] ŠÁMAL, Pavel. *Trestní řád: komentář*. II, § 157-314, s. 7., dopl. přeprac. vyd. V Praze: C.H. Beck, 2013. Velké komentáře. ISBN 978-80-7400-465-0. S. 1985.

stup. V takovém případě je nutné žádat o součinnost poskytovatele cloudových služeb.

Hypoteticky je samozřejmě možné vyžádat si od poskytovatele cloudu přímo vydání dat podle § 79e trestního řádu. Je nutné však podotknout, že taková data musí být konkrétně specifikována a musí být odůvodněno, proč jsou konkrétně tato data důležitá pro trestní řízení, resp. jak byla určena nebo užita ke spáchání trestného činu. Při neznalosti konkrétního obsahu cloudového úložiště to však bude pro orgán činný v trestním řízení nesplnitelná podmínka. Pouze na okraj lze dodat, že orgány činné v trestním řízení se nemohou domáhat vydání dat z cloudového úložiště postupem podle § 8 odst. 1 trestního řádu, neboť toto ustanovení neobsahuje zákonnou úpravu umožňující prolomení ústavně zaručeného práva na informační sebeurčení. V takovém případě je na místě zajištění přístupu policejního orgánu do soukromého virtuálního prostoru opět na základě institutu prostorového odposlechu podle § 158d odst. 3 trestního řádu.

Aplikace správného zajišťovacího institutu však zde není tím největším problémem. Většina poskytovatelů cloudových služeb běžně využívaných uživateli v České republice jsou subjekty zahraniční (Dropbox, OneDrive, Google Drive) a policejní orgán je nucen zajistit data nacházející se na území jiného státu. K získání dat je tedy nutné využít cestu mezinárodní justiční spolupráce. V této souvislosti nelze nezmínit čl. 31 Úmluvy o počítačové kriminalitě umožňující zajištění dat na území jiného státu prostřednictvím žádosti o vzájemnou pomoc. Ve vnitrostátním právním řádu upravuje přeshraniční sledování § 62 zákona o mezinárodní justiční spolupráci ve věcech trestních. Zatímco fyzické přeshraniční sledování vyžaduje vzájemnou mezinárodní smlouvu, sledování prostřednictvím technických prostředků bez přítomnosti policejního orgánu na území jiného státu předchozí mezinárodní ujednání nevyžaduje.[32] Stát, který chce využít institutu prostorového odposlechu na území jiného státu, musí požádat druhý stát o jeho povolení. Nebude-li přeshraniční sledování povoleno prostřednictvím žádosti o právní pomoc, nelze data takto získaná užít jako důkaz v trestním řízení.

[32] Důvodová zpráva k zákonu č. 104/2013 Sb.

9. TERITORIALITA DAT

Dříve než může dojít k jakémukoliv zajišťování dat uložených v cloudu, musí být zodpovězena otázka, který stát, resp. jeho orgány činné v trestním řízení, má pravomoc daný úkon provést. Situace je zde o to zajímavější, že každý stát si odpověď na tuto otázku hledá sám.

Co se týče České republiky, jak je naznačeno výše, platí princip tzv. teritoriality dat, tedy že orgány činné v trestním řízení mají pravomoc data zajišťovat pouze na území České republiky, tedy zajišťovat pouze ta data, která se fyzicky nachází na úložišti na území České republiky. Podobná je situace v sousedním Německu a také v Japonsku, kde příkaz k prohlídce směřující k poskytovateli služeb umístěnému v dané zemi nemůže být rozšířen na servery umístěné v zahraničí, třebaže jsou požadovaná data dostupná prostřednictvím počítačových systémů daného poskytovatele. V takovéto situaci je nutno využít cestu mezinárodní justiční spolupráce.[33]

Z globálního hlediska se do značné míry tento přístup liší například od přístupu Spojených států amerických, kde obecně platí, že lze použít vnitrostátní mechanismy k vyžádání dat z jakéhokoliv cloudového serveru po světě, pokud je příslušný poskytovatel cloudových služeb subjektem amerického práva. Stejně tak australské orgány veřejné moci mohou vyžadovat po poskytovateli cloudových služeb data jak z domácích, tak ze zahraničních serverů. V Kanadě obecně subjekt, jež podléhá kanadské jurisdikci, musí vydat data, která má v držení nebo je může kontrolovat, a to i pokud je přístup k datům možný pouze prostřednictvím třetí osoby (například dceřiná společnost). Orgán veřejné moci může rovněž vydat tzv. production order, tedy příkaz k donucení poskytovatele cloudových služeb vydat konkrétní důkazní prostředek. Jestliže dánský poskytovatel cloudových služeb ukládá data na serverech umístěných v jiné zemi, orgány veřejné moci se mohou k těmto datům dostat prostřednictvím příkazu k prohlídce. Francouzské právo pak dokonce výslovně povoluje orgánům veřejné moci za splnění určitých předpokladů získávat všechny důležité informace pro trestní řízení z počítačových systémů, přičemž jediným omezením je to,

[33] MAXWEL, Winston, Christopher WOLF. *A Global Reality: Governmental Access to Data in the Cloud* [online]. 2012 [cit. 15. 10. 2016].

zda jsou příslušná data z počítačového systému, jenž je předmětem prohlídky, resp. zajištění, technicky dostupná.[34]

V této souvislosti nelze opomenout aktuální rozhodnutí ze Spojených států amerických, kde soud druhého stupně rozhodoval o tom, zda se společnost Microsoft zachovala protiprávně, když odmítla na příkaz orgánu veřejné moci vydat jistá data z cloudu, jenž provozuje.[35] Konkrétně se jednalo o obsah e-mailové komunikace, přičemž tato data se dle tvrzení společnosti Microsoft nacházela v datacentru, jež je provozováno její dceřinou společností na území Irska. Argumentace společnosti Microsoft obhajující, proč se společnost rozhodla data nevydat, pak stála zejména na tvrzení, že příslušný procesní instrument, jímž jí byla povinnost data vydat, nemá právní sílu mimo území Spojených států, tudíž na jeho základě nelze data z Irska vydat. Příslušný soud se pak s tímto argumentem ztotožnil, když konstatoval, že právní předpis, na základě něhož byl příkaz k vydání dat vydán, aplikaci mimo území Spojených států neumožňuje.

Byť nejsme toho názoru, že toto rozhodnutí lze považovat za dramatickou změnu přístupu Spojených států amerických k této otázce, to zejména z „procesních" důvodů, jež byly v rámci rozhodování řešeny, rozhodně dané rozhodnutí naznačuje krok směrem k aplikaci principu teritoriality dat. Pro státy, jež tento princip teritoriality aplikují, je ovšem zásadní otázkou, jež musí být při aplikaci tohoto principu zodpovězena, kde přesně se zajišťovaná data nachází. Stejně tak ale platí, že odpověď na tuto otázku často nezná ani poskytovatel příslušné cloudové služby, natožpak orgán veřejné moci. Nejen z tohoto důvodu je jedním z nejdiskutovanějších témat v souvislosti s daty uloženými v cloudu právě vhodnost aplikace principu teritoriality, případně možnost nahrazení tohoto principu principem odlišným.

Argumenty proti principu teritoriality přitom není obtížné najít. Jedním z argumentů je například právě to, že lokace dat pro uživatele nemá žádný zvláštní význam. Z praktického hlediska daného uživatele vůbec nemusí za-

[34] MAXWEL, Winston, Christopher WOLF. *A Global Reality: Governmental Access to Data in the Cloud* [online]. 2012 [cit. 15. 10. 2016].

[35] Rozhodnutí Odvolacího soudu Spojených států amerických druhého obvodu ze dne 14. 7. 2016, sp. zn. 14-2985.

jímat, kde přesně se data nachází. Podstatné je pouze to, že data jsou pomocí určitého rozhraní dostupná. Nadto uživatel lokaci dat často není schopen ovlivnit. Cloudové služby zpravidla neumožňují uživateli rozhodovat o tom, ve které zemi si přeje mít data uložena. To je opět dáno zejména povahou modelu cloud computingu, jehož technická architektura může často vyžadovat různé přesuny uživatelských dat mezi datovými centry z provozních důvodu, například kvůli zálohování. Ve složitějších případech pak nemusí být poloha dat určitelná vůbec, jelikož dílčí složky dat mohou být „roztroušeny" po více datových centrech.[36] Dalším velmi podstatným argumentem je skutečnost, že stát, na jehož území mohou být data lokalizována, nemusí mít žádný podstatný zájem na tom tato data chránit. Lze si představit hypotetickou situaci, kdy policejní orgán potřebuje zajistit data týkající se trestné činnosti spáchané na území České republiky českým pachatelem, jehož obětí je český občan, nicméně data této trestné činnosti jsou momentálně fyzicky uložena mimo území České republiky.

Za těchto okolností se může zdát, že v kontextu cloud computingu je lokace dat jednou z jejich nejméně podstatných a nejvíce nahodilých vlastností. Těžko lze pak obhajovat postoj, že právě lokace dat musí být určujícím kritériem při zjišťování právního režimu těchto dat, včetně určení toho, orgány kterého státu jsou oprávněny daná data případně zajistit.

Na druhou stranu se ale lze setkat s argumentací vycházející z mezinárodního práva, totiž že stát může svou svrchovanou státní moc uplatňovat skutečně pouze na svém území, přičemž výjimky z této zásady stanovuje mezinárodní právo taxativně. Za jisté „řešení" by zde bylo možno považovat odlišný výklad principu teritoriality. V pojetí, v jakém je aplikován českými orgány činnými v trestním řízení, je vykládán tak, že data lze zajišťovat pouze tam, kde se nachází, a nikoliv na dálku, z území jiného státu. Jinými slovy, není rozhodné, kde se nachází příslušný orgán, který zajištění provádí, ale to, kde se nachází předmět zajištění. Lze ale uvažovat tom, že by byl přijat závěr opačný, tedy že je rozhodné kde se nachází orgán prová-

[36] DASKAL, Jennifer. The Un-Teritoriality of Data. *The Yale Law Journal*. 2015, (125:326), s. 326-398.

dějící zajištění, a ne to, kde se nachází data. Dalo by se pak tvrdit, že stát vykonává svou státní moc pouze na svém území, a bylo by možno dovodit, že český orgán činný v trestním řízení nepřekračuje svou pravomoc pokud zajišťuje data nacházející se v zahraničí, pokud se on sám přitom nachází na území České republiky. Tato úvaha má ale svá úskalí, protože jejím důsledkem by bylo, že orgány veřejné moci každého státu by mohly zajišťovat data nacházející se kdekoliv na světě.

Další možností je pak použít jako určující kritérium pro stanovení pravomoci sídlo poskytovatele cloudové služby, od něhož mají data být zajištěna, přičemž jak bylo uvedeno výše, některé státy tento přístup uplatňují. Dle názoru autorů lze právě tento přístup považovat za nejvíce praktický a *de lege ferenda* vhodný pro aplikaci v prostředí České republiky. Uvedený přístup totiž nepřipisuje přílišný význam fyzické lokalitě dat (což není úplně optimální, jak je diskutováno výše), ale zároveň ani nepředstavuje neomezené rozšíření pravomoci orgánů činných v trestním řízení tak, že by tyto mohly bez dalšího zajišťovat jakákoliv data kdekoliv ve světě. Navíc je ve velké části případů při zajištění dat zapotřebí zajistit součinnost provozovatele cloudu, proto je praktické, když tuto součinnost bude vyžadovat domácí státní orgán daného subjektu. Tím by se předešlo nutnosti postupovat cestou mezinárodní spolupráce, což by celý proces urychlilo a zjednodušilo.

10. ZÁVĚR

Jak bylo předestřeno v úvodu, kriminalistické využití dat uložených v cloudovém úložišti je pro policejní praxi nevyhnutelné. Navzdory tomu ale nelze konstatovat, že by toto využití probíhalo hladce. Častou překážkou je právě rozmanitost v současné době se vyskytujících technologií a souvisejících služeb, které jsou v kontrastu se zavedenými instituty trestního řádu. Příspěvek se proto zabýval tím, jakým způsobem lze řešit zajištění dat z cloudových úložišť v situacích, které lze považovat za každodenní. Domníváme se, že právě aplikací právních úvah na jasně identifikované technické situace a problémy lze dospět k tomu, že za některých okolností jsou stávající instituty trestního řádu dostačující a bez větších problémů aplikovatelné. Rovněž jsme ale v příspěvku identifikovali jisté, ne úplně nestan-

dardní situace, ve kterých se zdá, že aplikace stávajících institutů představuje pro praxi problémy, anebo je přinejmenším nepraktická. Právě identifikaci těchto problematických momentů přitom považujeme za první krok k hledání budoucího vhodného řešení.

Jak bylo opakovaně konstatováno, jedno z nejvíce problematických míst aktuálně představuje právě systém mezinárodní spolupráce. To je dáno především objemem případů, při kterých by bylo zapotřebí mezinárodní spolupráci vyžadovat. Jelikož se většina poskytovatelů cloudových služeb nachází v zahraničí, přičemž navíc provozují úložiště nacházející se často rovnou ve vícero zemích, jsou případy zajištění dat z cloudu bez mezinárodního prvku raritní. Co se pak týče v závěru diskutované otázky principu teritoriality dat, navzdory předkládanému návrhu *de lege ferenda* jsme si vědomi, že identifikace jednoznačného řešení této otázky, jež by bylo globálně akceptováno, je s největší pravděpodobností hodně vzdálená. Najít správnou odpověď zde není jednoduché, jelikož v kolizi se potenciálně nachází zájmy států, jednotlivců a společnosti jako takové.

11. SEZNAM ZDROJŮ

11.1 MONOGRAFIE, ODBORNÉ ČLÁNKY, SBORNÍKY

[1] DASKAL, Jennifer. The Un-Teritoriality of Data. *The Yale Law Journal*. 2015, (125:326), s. 326-398.

[2] KOWALCZUK, Izabela, Katarzyna SZYMIELEWICZ, Tomasz RYCHLICKI. The protection of privacy in Poland in the digital environment. *International Data Privacy Law*. 2011, (3), s. 161-171.

[3] POLČÁK, Radim, František PÚRY, Jakub HARAŠTA, Matěj MYŠKA, Václav STUPKA. *Elektronické důkazy v trestním řízení*. 1. vydání. Brno: Masarykova univerzita, 2015. Spisy Právnické fakulty Masarykovy univerzity. S. 105. ISBN 978-80-210-8073-7. Dostupné také z: http://science.law.muni.cz/knihy/monografie/Polcak_Elektronicke_dukazy.pdf.

[4] SERAFINO, Laurie Buchan. "Know My Rights, So You Go'n Need A Warrant for That": The Fourth Amendment, Riley's Impact, And Warrantless Searches of Third-Party Clouds. *Berkeleky Journal of Criminal Law*. 2014, (19:2), s. 155-203.

[5] STRAUS, Jiří. *Kriminalistická taktika*. 2. rozš. vyd. Plzeň: Vydavatelství nakladatelství Aleš Čeněk, 2008. ISBN 978-80-7380-095-6.

[6] ŠÁMAL, Pavel. *Trestní řád: komentář*. II, § 157-314, s. 7., dopl. a přeprac. vyd. Praze: C.H. Beck, 2013. Velké komentáře. ISBN 978-80-7400-465-0. S. 1985.

11.2 ELEKTRONICKÉ ZDROJE

[7] *Explanatory Report to the Convention on Cybercrime* [online]. In: Budapest, 2001 [cit. 15. 10. 2016]. Dostupné z: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId = 09000016800cce5b

[8] GRIFFITH, Eric. What Is Cloud Computing? *PC Magazine* [online]. 5. 5. 2016 [cit. 15. 10. 2016]. Dostupné z: http://www.pcmag.com/article2/0,2817,2372163,00.asp

[9] HALDERMAN, J. Alex et al. *Lest We Remember: Cold Boot Attacks on Encryption Keys* [online]. 2009 [cit. 15. 10. 2016]. Dostupné z: https://www.usenix.org/legacy/event/sec08/tech/full_papers/halderman/halderman_html

[10] MAXWEL, Winston, Christopher WOLF. *A Global Reality: Governmental Access to Data in the Cloud* [online]. 2012 [cit. 15. 10. 2016]. Dostupné z: http://www.cil.cnrs.fr/CIL/IMG/pdf/Hogan_Lovells_White_Paper_Government_Access_to_Cloud_Data_Paper_1_.pdf

[11] MELL, Peter, Timothy GRANCE. The NIST Definition of Cloud Computing. *Recommendations of the National Institute of Standards and Technology* [online]. 2011 [cit. 15. 10. 2016]. Dostupné z: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

11.3 JUDIKATURA

[12] Nález Ústavního soudu ČR ze dne 22. března 2011, sp. zn. Pl. ÚS 24/10.

[13] Nález Ústavního soudu ČR ze dne 17. července 2007, sp. zn. IV. ÚS 23/05.

[14] Rozhodnutí Evropského soudu pro lidská práva ze dne 6. září 1978 ve věci stížnosti č. 5029/71 - Klass a další proti Německu.

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

[16] Nález Ústavního soudu ze dne 13. února 2001, sp. zn. IV. ÚS 536/2000.

[17] Nález Ústavního soudu ČR ze dne 27. září 2007, sp. zn. II. ÚS 789/06.

[18] Usnesení Ústavního soudu ČR ze dne 3. října 2013, sp. zn. II. ÚS 3812/2012.

[19] Nález Ústavního soudu ze dne 22. ledna 2011, sp. zn. II. ÚS 502/2000.

[20] Nález Ústavního soudu ČR ze dne 27. ledna 2010, sp. zn. II. ÚS 2806/08.

[21] Nález Ústavního soudu ČR ze dne 30. října 2014, sp. zn. III. ÚS 3844/13.

[22] Rozhodnutí Odvolacího soudu Spojených států amerických druhého obvodu ze dne 14. 7. 2016, sp. zn. 14-2985.

[23] Stanovisko Nejvyššího státního zastupitelství poř. č. 1/2015 ke sjednocení výkladu zákonu a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek.