Bezpečnostní technologie, systémy a management
11. – 12. září 2013, Univerzita Tomáše Bati ve Zlíně

Digitální svět a dokazování obsahu elektronických dokumentů

Prof. JUDr. Ing. Viktor PORADA, DrSc. dr. h. c. mult., Doc. JUDr. Eduard BRUNA, Ph.D.
Vysoká škola Karlovy Vary, T. G. Masaryka 3, 360 01 Karlovy Vary
viktorporada@vskv.cz, eduardbruna@vskv.cz

Abstrakt: Příspěvek pojednává o problémech s poznáním a prokázáním, resp. dokázáním dějů, které v digitálním světě probíhají. Tato otázka zajímá jak teoretiky – filosofy a matematiky, tak praktiky – konstruktéry a návrháře. Ale možná ještě významnější se dnes stává pro kriminalisty při forenzní analýze počítačových systémů a sítí, jakož i digitálních nosičů dat z hlediska dokazování jejich obsahu. Nejčastější formou forenzního zkoumání elektronických dokumentů nacházejících se v prostředcích ICT jsou digitální dokumenty ve statické formě, které byly opatřeny nebo zajištěny orgány činnými v trestním řízení. Pokud nebyly již při svém vytvoření doplněny nástroji pro zajištění věrohodnosti původu dokumentu, neporušitelnosti jeho obsahu a zakotvení existence dokumentu v čase, je obtížné až nemožné prokázat nebo vyvrátit tvrzení, které se k takovým dokumentům vztahují.

Klíčová slova: digitální svět; kyberprostor; forenzní analýza; elektronické dokumenty; dokazování;

1 Digitální svět

Druhá polovina minulého století a zejména pak počátek století tohoto jsou svědky, jak se stále více našich aktivit odehrává v tzv. virtuálním prostředí, na Internetu. Někdy vědomě, někdy nevědomě. Ale není to pouze svět Internetu, který vytváří kyberprostor, a není to jen kyberprostor, který tvoří digitální svět okolo nás. A už vůbec to není (pouze) informační společnost, jakkoliv jde o termín, především politiky značně užívaný.

Digitální svět je tvořen jedničkami a nulami, tedy nejjednodušším zobrazením informace, nacházejících se na různých nosičích a v různých systémech.

Tento svět se dnes nachází všude okolo nás – a v případě např. lékařských přístrojů i v nás (kardiostimulátor[1]). Někdy se jedná o autonomní systémy (elektronika v automobilu) pracující prakticky bez interakce s člověkem, někdy o informační systémy v klasickém slova smyslu, sloužící pro sběr, zpracování, ukládání, vyhledávání a šíření informací, jehož prvky jsou informační a komunikační technologie, data a lidé. Cílem informačního systému je efektivní podpora informačních a rozhodovacích procesů.[2] V momentě, kdy jsou jednotlivé prvky informačních systémů nebo informační systémy jako takové propojovány prostřednictvím Internetu (obecně ale jakýmkoliv způsobem), můžeme hovořit o kyberprostoru.

Internet se nevnímá jako podmnožina kyberprostoru ani naopak, spíše jsou pojímány jako dvě množiny, které se částečně překrývají; „Internet“ se tu vztahuje především k obecnějším a techničtějším aspektům, „kyberprostor“ či „virtuální prostor“ je – mimo parafráze, kde se ponechává výraz užitý příslušným

[1] Viz např. TEJKL, J. *Mikrosenzory a mikrosystémy v medicíně*. Kardiostimulátory. Zdroj: jaromir.tejkl.sweb.cz/kardiostim/clanek.pdf.

[2] MATES, V., SMEJKAL, V. *E-government v České republice. Právní a technologické aspekty*. 2. vydání. Praha: Leges, 2012, s. 21.

autorem – interpretačním pojmem užívaným tam, kde není předmětem zájmu síť propojených počítačů (typ média), nýbrž síť sociálních vztahů a vztahů k samotnému Internetu, přesněji řečeno jeho specifickým částem.[3]

Ve všech těchto součástech, tvořících digitální svět, dochází ke vzniku, zpracování, sdělování a příjmu informací. Vzhledem ke složitosti tohoto typu světa a rychlosti procesů, v něm probíhajícím, je otázkou, zda vůbec a nakolik je tento svět poznatelný a zda můžeme získané poznatky interpretovat.

2 Poznání v digitálním světě

Říká se, že poznání znamená proces nabývání znalostí o reálném světě (poznávání), jehož výsledkem je snížení entropie, tedy získání nějakého poznatku. Poznání není emotivní či subjektivní, ale objektivní, jako výsledek spolehlivého, důvěryhodného a ověřitelného poznávacího procesu. Rozporuplnost toho konstatování, viz .např. [4]

Jinou otázkou ovšem je, zda a jak je schopen člověk o svých poznatcích vypovídat, tj. zda objektivní fakta nebudou zatížena osobním vnitropsychickým kognitivním modelem referujícího (a následně stejným modelem, či můžeme říci osobností) příjemce sdělení. Při komunikaci lidé totiž jednají a reagují subjektivně – na základě současné situace a také na základě své minulosti, dřívějších zkušeností, postojů, kulturních návyků a spousty s tím spojených činitelů. Z toho vyplývá, že akce a reakce při komunikaci jsou určovány nejen tím, co bylo řečeno, ale i způsobem, jak si zúčastněná osoba vykládá to, co bylo řečeno. Díky tomu si dva lidé naslouchající témuž sdělení mohou často vyložit jeho význam velmi odlišně. Ačkoli slova a gesta jsou stejná, každý z nich si je vykládá odlišně z prostého důvodu, že každý člověk je jiný a má i jiné zkušenosti.[5]

Informace je poznatek týkající se jakýchkoliv objektů, např. fakt, událostí, věcí, procesů nebo myšlenek, včetně pojmů, který má v daném kontextu specifický význam.[6] V případě mezilidské komunikace je ovlivněna výše uvedeným osobními faktory a vlivy. V případě strojové komunikace prostřednictvím kanálu, spojujícího zdroj a přijímač informací může mít na kvalitu informace vliv rušení (šum, jako rušivý signál, který v průběhu komunikace mění a poškozuje přenášenou zprávu), ale nenastává zde interpretační problém – přijatá nula bude stále nulou a jednička jedničkou.

Stále větší problém nám činí vzrůstající složitost informačních systémů a sítí. Běžící informační systém, kde probíhá mnoho paralelních procesů, komunikujících mezi sebou a s uživateli, jejichž stav je v každý okamžik variabilní a mnohdy neopakovatelný, klade velké překážky a možná i činí nemožným beze zbytku poznat vnitřní svět počítačových systémů.

Zatímco jejich tvůrci mají možnost modelování a trasování krok po kroku, přičemž řízenými experimenty mohou získávat informace o tom, co se v systému do značné míry odehrává, v případě zjišťování toho, co se odehrálo ante tempora, především pro účely soudních a správních řízení, především pak pro účely trestního řízení je situace velmi složitá.

3 Zkoumání digitálních stop

3.1 Definice a vlastnosti digitálních stop

Každé technologické zařízení, které získává, zpracovává, předává nebo uchovává data, zanechává záznamy (odrazy) o své činnosti. Tyto záznamy z kriminalistického

[3] ZBÍRAL, D. *Náboženství a internet.* Zdroj: www.david-zbiral.cz/nabinternet.pdf.

[4] ZOUBEK, V. *Právověda a státověda. Úvod do právního a státovědního myšlení*. 1. vydání. Plzeň : Aleš Čeněk, 2010. 700 s. ISBN 978-80-7380-239-4. ZOUBEK, V. *Lidská práva - globalizace - bezpečnost.* 2. upravené vydání. Plzeň : Aleš Čeněk, 2008. 461 s. ISBN 978-80-7380-103-8. ZOUBEK, V. Dolgosročnyje globaĺnyje problemy bezopasnosti. In: *Formirovanije tolerantního soznanija v obščestve: materiály VII. meždunarodnogo antiterroristističeskogo foruma.* Ids. I. I. Bondarenko i A. I. Dičenko. Kijev : Kijevskaja pravda, 2011, s. 139-145. ISBN 978-966-7270-65-0.

[5] DEVITO, J. A. *Základy mezilidské komunikace*. 1. vyd., Praha: Grada Publishing, 2001, s. 21.

[6] ČSN ISO/IEC 2382-1, s. 7.

hlediska jsou stopami. V oblasti IS/IT jsou tedy především digitální stopy, které lze definovat podle SWGDE (Scientific Working Group on Digital Evidence) jako jakékoliv informace s vypovídající hodnotou, uložené nebo přenášené v digitální podobě.[7]

Z hlediska trestního či správního řízení je ale pro nás možná užitečnější užší definice International Organization of Computer Evidence (IOCE), která definovala původně digitální stopu jako jakoukoliv informaci, uloženou nebo přenášenou v binární formě, která může být předložena soudu jako věcný důkaz. V této definici je kladen důraz na předkládání důkazů soudu a právě předložitelnost důkazu soudu je hlavním kritériem úspěšnosti kriminalistické počítačové analýzy (na rozdíl od tzv. znalecké analýzy prováděné za účelem soukromoprávním).

Lze také říci, že digitální stopa je fyzikální interpretací (záznamem) nehmotné informace, zakódované do digitálního formátu.[8]

Digitální stopy se nacházejí v počítačových systémech a na nosičích dat,[9] případně kdekoliv v kyberprostoru. Jejich vlastnosti jsou ovšem takové, že příliš neusnadňují práci orgánů činných v trestním řízení, resp. jimi ustanovených znalců. Patří sem kromě dalších zde uvedených[10] také ty vlastnosti, které souvisejí s pomíjivým stavem informačního obsahu složitých počítačových systémů:

- nehmotnost digitálních stop,
- latentnost digitálních stop,
- manipulovatelnost s časem v počítačových systémech,
- velmi nízká životnost digitálních stop,
- způsob uchování záznamů,
- dynamika činnosti počítačových systémů,
- komplexnost prostředí,
- vysoký stupeň interní a externí interakce probíhajících procesů,
- velký geografický rozsah prostoru s digitálními stopami.

3.2 Statická a dynamická analýza digitálních stop

Jednou ze základních zásad při zajišťování digitálních stop je zachování jejich integrity a z toho vyplývající postup, který předpokládá pořízení identických binárních kopií originálních nosičů dat a jejich autentizace pomocí kontrolního součtu a provádění digitální forenzní analýzy na takto pořízených kopiích. Tento postup je charakteristický pro tzv. „klasickou“ digitální forenzní analýzu statických datových nosičů. V současné době je však v mnoha případech potřeba analyzovat obsah dynamických pamětí digitálních informačních a komunikačních technologií. V tomto případě nastává problém, protože pro pořízení kopie operační paměti nebo pro „živou“ analýzu informací a dat takové paměti je nutné spustit program, který tyto činnosti provádí. Spuštění programu však je možné pouze způsobem, že se tento program nahraje do operační paměti, tj. do paměti, kterou je potřeba kopírovat/analyzovat. Dochází tak ke změně předmětu zkoumání.

Pro tradiční digitální forenzní analýzu je charakteristické, že po zajištění dat pracuje s takovými daty, která jsou uložena na médiích s dlouhou dobou životnosti. To umožňuje detailní zkoumání, opakování jednotlivých SOP, verifikaci výsledků jinými metodami digitální forenzní analýzy nebo i dodatečné provedení analytických kroků i s odstupem několika let, např. pro účely dodatečných analýz, pro ověření/demonstraci správnosti analytických postupů před soudem apod.

Naproti tomu digitální forenzní analýza živých systémů (Live Forensics) se zabývá postupy získávání a analýzy digitálních stop ze systémů digitálních informačních a komunikačních technologií v případě, že tyto systémy nelze pro účely digitální forenzní analýzy vypnout nebo je nutné je pro získání

[7] RAK, R., PORADA, V. Charakteristiky a specifika digitálních stop. *Bezpečnostní teorie a praxe*, 2005, č. 1, s. 71 – 84, resp. PORADA, V., RAK, R. Digitální stopy v kriminalistice a forenzních vědách. *Soudní inženýrství*, XVII., 2006, č. 1, s. 3 – 21.

[8] PORADA, V. ŠEDIVÝ, P. Praktická využitelnost kriminalistických a forenzních aplikací v oblasti počítačové/kybernetické kriminality. *Karlovarská právní revue*, 2012, č. 3, s. 94 – 114.

[9] PORADA, V., STRAUS, J. *Kriminalistické stopy - Teorie, metodologie, praxe*. Plzeň: Aleš Čeněk, s.r.o. 2012, s. 282.

[10] PORADA, V., STRAUS, J. op. cit., s. 306 a násl.

určitých specifických informací ponechat zapnuté („živé“).

Hlavním problémem je extrémní dynamičnost prostředí digitálních stop. Organizace, provozující složité IS s mnoha uživateli, běžícími programy a procesy a rozprostírající se v lokálních i vzdálených umístěních (LAN, WAN) nikdy samy nedopustí „klasické ohledání místa trestného činu“ s vyloučením všech osob a činností po dobu ohledání a zajištění věcných důkazů, tedy včetně digitálních stop. Vyšetřování, expertiza musí být vedena v živém, produkčním prostředí, v krajním případě ze záložních nebo archivních médií. Produkční prostředí je ale extrémně dynamické, generuje obrovské množství transakcí, které mohou přepisovat, zneplatňovat či mazat skutečné, relevantní digitální stopy (důkazy). Pokud s aplikací pracuje větší množství uživatelů, pravděpodobnost zajištění relevantních důkazů s rostoucím časem prudce klesá. Naopak pachatel má dostatek času a prostoru aby stopy smazal nebo pozměnil. Situace je komplikována tím víc, má-li tato osoba dostatečné znalosti a oprávnění (administrátorské). Kritické aplikace musí být proto navrženy podle přísných bezpečnostních pravidel (oddělení pracovních rolí zaměstnanců, logování transakcí, archivace dat, průběžný monitoring apod.). Pokud tyto pravidla při vývoji nebo v provozu nejsou dodržována, hledání pachatele je velmi komplikovanou záležitostí s vysokou mírou nejistoty výsledku a velkou investicí do zdrojů vyšetřování.[11]

Digitální forenzní analýza běžících počítačových systémů se proto musí vypořádat s několika problémy:

- v živých systémech dochází k neustálým změnám dat, zkoumaný systém pracuje, neustále zpracovává data, tato se neustále přesouvají z pevného disku do operační paměti a procesoru počítače a nazpět. Jakákoliv analýza, zjištění nebo kopie dat tedy odpovídá pouze stavu systému v době, kdy analýza, zjištění nebo kopie dat byly provedeny;
- jakýkoliv forenzní programový nástroj, který je k digitální forenzní analýze živých systémů použit, se stává součástí takového systému, a tím provede v tomto systému změny. Nejedná se pouze o změnu v operační paměti, kde takový forenzní nástroj pracuje, ale dochází i ke změnám na pevných discích, byť forenzní nástroje tohoto druhu jsou postaveny tak, aby na originální datové nosiče zkoumaného systému v žádném případě nezapisovaly. Změny v datech na originálních pevných discích zkoumaného systému jsou způsobeny principem práce operačního systému zkoumaného počítače, protože (až na výjimky) všechny operační systémy běžně využívají pevný disk k tzv. odkládání částí momentálně nepoužívané operační paměti na disk (tzv. swapování), a tím se může „obraz“ forenzního nástroje, který primárně běží pouze v operační paměti, dostat i na pevný disk. Při takovémto druhu forenzní analýzy je třeba se s touto skutečností vyrovnat a takové změny identifikovat, zdůvodnit a zhodnotit jejich vliv na originální data;
- forenzní nástroje pro digitální analýzu živých systémů musí pro svoji práci použít alespoň minimální sadu funkcí běžícího originálního operačního systému. Riziko, že takový systém je modifikován nedefinovatelným způsobem je vždy potřebné zvažovat a výsledky získané tímto způsobem vždy kriticky přehodnocovat.[12]

Zde se zřejmě dostaneme do situace, kdy budeme muset kombinovat monitorování (sledování) běžícího systému resp. některého z jeho uživatelů a zaznamenávání statických stavů systému, byť ve velice krátce po sobě jsoucích okamžicích.

Zajímavou otázkou je, zda monitorování chování určitého uživatele „uvnitř“ počítavého

[11] Porada, Rak., op. cit.

[12] PORADA, V. ŠEDIVÝ, P. Praktická využitelnost kriminalistických a forenzních aplikací v oblasti počítačové/kybernetické kriminality. *Karlovarská právní revue*, 2012, č. 3, s. 94 – 114.

systému je podřaditelné pod některý druh činnosti, kterou umožňuje platné znění trestního řádu, jako je odposlech a záznam telekomunikačního provozu podle § 88 nebo zjištění údajů o telekomunikačním provozu podle § 88a trestního řádu.[13] Zřejmě nikoliv, protože dané činnosti předpokládají sledování přenosu dat mezi uživatelem a příjemcem, přičemž pracuje-li trestní řád s pojmem „telekomunikační provoz“, pak s přihlédnutím k dikci § 97 zákona o elektronických komunikacích[14] se tím rozumí odposlech a záznam zpráv přenášených veřejnou komunikační sítí nebo pomocí veřejně dostupné služby elektronických komunikací.
Sledování provozu v počítačových sítích naproti tomu může být podřazeno pod tuto činnost, a to vzhledem k obecné definici služby elektronických komunikací dle § 2 písm. n) zákona o elektronických komunikacích.[15] Problémem ovšem je komplexnost a obtížná přiřaditelnost přenášených informací k určitému objektu či subjektu. Těžko předem určit, zda ta která činnost systému, která je zaznamenána v rámci síťového provozu, je činností iniciovanou uživatelem nebo automatickou činností systému. Navíc v procesu zaznamenávání síťového provozu se nejedná o jeho analýzu, která jediná může věrohodně určit zdroje, které iniciovaly zaznamenaný provoz.[16]

Trestní řád dále umožňuje sledování osob a věcí, jež je v ust. § 158d definováno jako získávání poznatků o osobách a věcech prováděné utajovaným způsobem technickými nebo jinými prostředky, přičemž sledování, při kterém mají být pořizovány zvukové, obrazové nebo jiné záznamy, lze uskutečnit pouze na základě písemného povolení státního zástupce. Otázkou ovšem je míra součinnosti provozovatele systému, která podle cit. ust. zákona není zřejmě vynutitelná.

Z hlediska kriminalistické počítačové analýzy je pro nás klíčové, abychom mohli konformně správným a přísně legálním způsobem najít, zadokumentovat a provést důkazy, zjištěné z digitálních stop.

Musíme ovšem počítat s tím, že takto nemusíme získat všechny informace, které mohou být skryté nebo nekopírovatelné. Jejich průkazní hodnota je proto slabší.[17]

3.3 Forenzní zkoumání elektronických dokumentů

Jak již bylo naznačeno výše, existuje řada aspektů, které nám dokazování v souvislosti s elektronickými dokumenty mimořádně znesnadňuje:

- čas,
- čitelnost dat,
- identifikace a autentizace,
- průkaznost důkazů.

3.3.1 Čas

Je známo, že nastavení času na počítači lze kdykoli změnit. Pouze takový počítač, který by byl připojen na časový normál či jiný zdroj jednotného času a toto nastavení by nebylo možno modifikovat či vypnout, je nezpochybnitelným zdrojem o době určitého úkonu. U obyčejných počítačů musíme mít štěstí, abychom z více provázaných údajů mohli spolehlivě prokázat, kdy se v počítači co odehrálo, a to jak v případě, kdy pachatel s faktorem času počítal a nastavil jej určitým způsobem, tak v situaci,

[13] Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.
[14] Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů
(zákon o elektronických komunikacích), ve znění pozdějších předpisů.
[15] Poněkud klopotná definice zní takto: službou elektronických komunikací se rozumí služba obvykle poskytovaná za úplatu, která spočívá zcela nebo převážně v přenosu signálů po sítích elektronických komunikací, včetně telekomunikačních služeb a přenosových služeb v sítích používaných pro rozhlasové a televizní vysílání a v sítích kabelové televize, s výjimkou služeb, které nabízejí obsah prostřednictvím sítí a služeb elektronických komunikací nebo vykonávají redakční dohled nad obsahem přenášeným sítěmi a poskytovaným službami elektronických komunikací; nezahrnuje služby informační společnosti, které nespočívají zcela nebo převážně v přenosu signálů po sítích elektronických komunikací.
[16] Porada, V. Šedivý, P. op. cit.
[17] SMEJKAL, V. Současné možnosti boje proti počítačové kriminalitě. *Data Security Management*, XV., 2011, č. 4, s. 18 – 23.

kdy podezřelý či obviněný zpochybňuje časové údaje zjištěné v průběhu vyšetřování.[18]
Další vlastní, související s časem, je extrémní dynamičnost prostředí digitálních stop. Organizace, provozující složité IS s mnoha uživateli, běžícími programy a procesy a rozprostírající se v lokálních i vzdálených umístěních (LAN, WAN) nikdy samy nedopustí „klasické ohledání místa trestného činu“ s vyloučením všech osob a činností po dobu ohledání a zajištění věcných důkazů, tedy včetně digitálních stop. Vyšetřování, expertiza musí být vedena v živém, produkčním prostředí, v krajním případě ze záložních nebo archivních médií. Produkční prostředí je ale extrémně dynamické, generuje obrovské množství transakcí, které mohou přepisovat, zneplatňovat či mazat skutečné, relevantní digitální stopy (důkazy). Pokud s aplikací pracuje větší množství uživatelů, pravděpodobnost zajištění relevantních důkazů s rostoucím časem prudce klesá. Naopak pachatel má dostatek času a prostoru aby stopy smazal nebo pozměnil. Situace je komplikována tím víc, má-li tato osoba dostatečné znalosti a oprávnění (administrátorské). Kritické aplikace musí být proto navrženy podle přísných bezpečnostních pravidel (oddělení pracovních rolí zaměstnanců, logování transakcí, archivace dat, průběžný monitoring apod.). Pokud tyto pravidla při vývoji nebo v provozu nejsou dodržována, hledání pachatele je velmi komplikovanou záležitostí s vysokou mírou nejistoty výsledku a velkou investicí do zdrojů vyšetřování.[19]

3.3.2 Čitelnost dat

Zde budeme řešit dva základní problémy:
a) čitelnost formátu, v němž jsou dokumenty vytvořeny a uloženy; může se jednat o natolik zastaralý nebo ojedinělý datový formát, že nebudeme mít k dispozici nástroj pro jeho analýzu a zjištění obsahu,
b) čitelnost nosiče dat v důsledku stáří, poškození, fyzikálních vlivů atd.,
c) úmyslné znečitelnění obsahu pro nepovolané osoby.

Druhý případ je možný, ale nejproblematičtější a zřejmě nejpravděpodobnější u pachatelů z řad „bílých límečků“ je třetí, neboť je snadno realizovatelný prostřednictvím hesel, šifer, ukrytím (zneviditelněním) souboru apod.
Pokud podezřelý neprozradí heslo či klíč a ochranu se nepodaří prolomit, neexistuje zákonný nástroj, jak si tento přístup vynutit. Při použití dostatečně sofistikovaného postupu či nástroje mohou být data znepřístupněna navždy.[20]

3.3.3 Identifikace a autentizace

Klíčovým problémem dokazování prostřednictvím elektronických dokumentů je přiřazení dokumentu, resp. jeho obsahu konkrétní osobě. Pokud není dokument opatřen elektronickým podpisem, pokud možno tzv. zaručeným elektronickým podpisem,[21] prakticky není možné prokázat, kdo je skutečným autorem dokumentu nebo kdo jej nějak modifikoval. Vyplývá to z možnosti jakýchkoliv změn digitálně zaznamenaných dat, přičemž použití nějakého logu, znamenávající činnosti v počítačovém systému se obvykle omezuje pouze na přihlášení/odhlášení, v lepším případě na to, že určitá osoba v jistý okamžik nějak s dokumentem nakládala.
Ale ani to nemusí být dostatečné – viz výše uvedená zmínka o možnosti ovlivňování času počítačového systému. Opět pouze existence časového razítka[22] představuje důkaz jednoznačný, který může být nahrazen pouze soustavou dalších důkazů, vztahujících se k procesům, probíhajícím v počítačovém systému.
Značným omylem současnosti je dokazování prostřednictvím tzv. metadat dokumentu, obsahující údaje, kdo dokument vytvořil, kdy

[18] Smejkal, V. op. cit.
[19] Porada, Rak., op. cit.

[20] Smejkal, V. *Problémy při stíhání počítačové kriminality*. Data Security Management, XIV., 2010, č. 1, s. 14 – 18.
[21] Viz např. Smejkal, V. *Elektronický podpis*. Právní rádce, XII., 2004, č. 12, s. 9 – 14 a Smejkal, V. *Elektronický podpis v Slovenské republice*. Data Security Management, XI., 2007, č. 2, s. 16 – 20.
[22] Podrobně viz zejm. Mates, V., Smejkal, V. *E-government v České republice. Právní a technologické aspekty.* 2. podstatně přepracované a rozšířené vydání. Praha: Leges 2012, 456 str., ISBN: 978-80-87576-36-6

se tak stalo, kolik času bylo spotřebováno na práci s ním, kdy byl naposledy vytištěn atd. Při běžné práci, kdy se nikdo nesnaží „škodit“ a s daty záměrně manipulovat, jsou metadata užitečná, protože běžné programy je při správném nastavení vyplňují podle skutečnosti. Nicméně stále je nutné mít na paměti, že je v případě nutnosti lze snadno změnit. Pokud je zveřejněn formát dokumentu, nebo v případě, že jej podrobíme vlastnímu zkoumání, můžeme snadno dostupnými nástroji změnit obsah těchto metadat podle potřeby. Například dokumenty vytvořené ve většinových formátech MS Office lze otevřít v libovolném textovém editoru či jiném nástroji, pomocí vyhledávání najít text, který chceme změnit a upravit jej dle vlastního uvážení. Jakékoliv znalecké zkoumání tohoto dokumentu nedokáže původní informace získat, ba dokonce ani odhalit, že byly změněny a musí se spokojit s podvrženými údaji.

Jistou naději pro OČTŘ, resp. znalce může přestavovat jedna z vlastností digitálních dokumentů, kterou si ne mnoho lidí uvědomuje: kopie digitálního dokumentu se může nacházet nejen kdekoliv na počítačovém systému či informačním systému, ale v podstatě kdekoliv v kyberprostoru. Nikdy nemůžeme vědět a nikdy to nezjistíme, zda někdo někam určitý dokument neuložil, neposlal, vědomě či nevědomě. Nevíme, zda nezůstal uložen v nějaké mezipaměti, v mailové či datové schránce. Toto je nové riziko a nová naděje pro vyšetřovatele.

3.3.4 Průkaznost důkazů

Existuje několik zásad, jež jsou nezávislé na použitých technologiích, ale které jsou důležitým předpokladem pro to, aby znalecký posudek mohl být použit v rámci soudního nebo správního řízení: [23]

- Integrita – vše, co bylo prováděno, veškeré způsoby práce se vstupními informacemi musí být prováděno způsobem, ze kterého je jednoznačně jasné, že nemohlo dojít k úmyslné nebo neúmyslné manipulaci nebo změně dat, včetně zadokumentování kdo, kdy, kde, jak a proč s nimi co dělal apod.
- Opakovatelnost/přezkoumatelnost – použití takových způsobů práce a jejich dokumentace tak, aby metody mohly být opakovaně provedeny stejným způsobem, čímž by se ověřilo, zda se dospěje ke stejným závěrům, nebo aby mohla být správnost závěrů ověřena pomocí jiných metod (pokud existují). Nepřezkoumatelnost je často způsobena snahou, neuvádět do posudku všechny detaily, nezatěžovat příslušný orgán stovkami až tisíci stran příloh apod.; toto lze zcela jistě vyřešit přílohou na CD/DVD.
- Objektivnost – znalec by měl přistupovat ke zkoumání objektivně, bez předchozího ovlivnění (zadavatelem posudku nebo tzv. veřejným míněním, sdělovacími prostředky apod.) nebo vytváření hypotéz, pro které se bude pouze snažit najít potvrzující důkazy (a současně přehlížet nebo vědomě či nevědomě potlačovat důkazy proti původní hypotéze).

4 Závěry

Ačkoliv by se mohlo zdát, že v úvodu toho textu najdeme povzdech či dokonce rezignaci nad složitostí digitálního světa, přesto můžeme dospět k podmíněně optimistickému závěru.

Spočívá v tom, že tak jako v dřívějších etapách lidstva se zdály být některé problémy, dané s poznatelností světa limitující další možnosti lidské společnosti, ukázalo se prakticky ve všech případech, že tomu tak není.

Zkoumání nitra hmoty na straně jedné – viz např. experiment prováděný ve švýcarském urychlovači částic LHC (Large Hadron Collider neboli Velký hadronový urychlovač)[24] či naopak v kosmickém prostoru – viz např. sonda Voyager 2 mohou být zdrojem optimismu, že se nám podaří zkoumat i chování složitých a vysoce dynamických počítačových systémů. Poznání dějů, které se zde odehrávají obecně, je přitom snazší, nežli

[23] Viz např. Svetlík, M. *Digitální forenzní analýza a bezpečnost informací.* Data Security Management, XIV., 2010, č. 1, s. 20 – 23.

[24] http://lhc.web.cern.ch/lhc/

konkrétní přiřazení určitých procesů určitým subjektům.

Digitální technologie pronikly do běžného života společnosti takovým způsobem, že pro orgány činné v trestním řízení, ale obecně pro každého, kdo bude zkoumat chování složitého počítačového systému, se tyto musí stát z jedné strany nedílným a zásadním nástrojem práce, z druhé strany kladou tyto technologie, díky jejich složitosti a dynamice vývoje, vysoké nároky na odpovídající vědomosti a speciální postupy identifikace, vyhledávání, zajišťování, dále pak na analýzu, interpretaci a prezentaci digitálních stop.

Současná úroveň rozvoje a existence informačních a komunikačních technologií jednoznačně vyžaduje vytvoření specializovaných a kvalifikovaných týmů sestávajících nejen ze specialistů na digitální techniku, ale i na odborníky v oblastech lidské činnosti, která digitální technologie specificky využívá. Jedná se tedy o reálnou potřebu vzniku multioborových vyšetřovacích týmů.

Konkrétním příkladem může být potenciální snaha pachatele nebo pachatelů zaútočit pomocí informačních a komunikačních technologií na některý z prvků klíčové infrastruktury státu nebo na řídicí a informační systém některé z předních nemocnic nebo významného průmyslového podniku. V takto závažných nebo složitých případech nebude postačovat v praxi používaná metoda určité „off-line“ spolupráce. I když se zdají být použité příklady zatím na první pohled nereálné, světová zkušenost potvrzuje opak a není nic lepšího, než být připraven jak organizačně, procesně, odborně ale i právně. Lze se důvodně domnívat, že takové situace, kdy by bylo potřebné sestavit specializovaný multioborový vyšetřovací tým již v minulosti nastaly, jen se o nich neví, nebo nebyly jako takové klasifikovány. Je potřeba se připravit na nepříznivé situace, které mohou nastat už v blízké době.[25]

Na otázku, zda otázkou, zda je digitální svět poznatelný, lze zřejmě odpovědět kladně. Složitější je, zda budeme schopni získat digitální stopy v souladu s právním řádem, a ještě více, zda budeme schopni získané poznatky interpretovat a tuto intepretaci obhájit. Některé případy, které se vyskytly v poslední době, ukazují, že existuje nebezpečí jednostranné interpretace, kdy jsou fakta vybírána či uvažována selektivně či dokonce tak, aby doplnila předem vytvořenou hypotézu. Důvodem nemusí být jen záměr či ovlivnění ze strany jiné osoby, ale „pouze“ strach ze složitosti a omezené poznatelnosti dané právní či trestní věci. Zde tedy existuje velký prostor pro výzkumnou a pedagogickou činnost v oblasti tak obecné, jakou je gnoseologie, ale i tak konkrétní, jako jsou forenzní metody v digitálním světě.

Z výše uvedených poznatků a argumentů lze vyvodit dva následující klíčové závěry, které významným způsobem ovlivňují nejenom kriminalistické úspěchy při vyšetřování a odhalování počítačové nebo kybernetické trestné činnosti, ale potenciálně i při odhalování většiny nebo alespoň značné části ostatní trestné činnosti, nezávisle na jejím druhu:

I. Spolupráce orgánů činných v trestním řízení (OČTŘ) se specialisty v oboru informačních a komunikačních technologií je již nedostatečná na té úrovni, na jaké je využívána v současné době, tj. zadáváním zpracování znaleckých posudků nebo v lepším případě ad-hoc dílčími konzultacemi. Digitální technologie pronikly do běžného života společnosti takovým způsobem, že pro OČTŘ se tyto musí stát z jedné strany nedílným a zásadním nástrojem práce, z druhé strany kladou tyto technologie, díky jejich složitosti a dynamice vývoje, vysoké nároky na odpovídající vědomosti a speciální postupy identifikace, vyhledávání, zajišťování, dále pak na analýzu, interpretaci a prezentaci digitálních stop. Bez špičkových specialistů nebude odvedená práce na odpovídající nebo alespoň akceptovatelné úrovni. Současná úroveň rozvoje a existence informačních a komunikačních technologií jednoznačně vyžaduje po OČTŘ vytvoření co největšího počtu specializovaných a kvalifikovaných týmů a pro specializované činnosti kontinuální a těsnou spolupráci s experty v oboru digitálních technologií.

[25] PORADA, V. ŠEDIVÝ, P. Praktická využitelnost kriminalistických a forenzních aplikací v oblasti počítačové/kybernetické kriminality. *Karlovarská právní revue,* 2012, č. 3, s. 94 – 114.

II. Uplatnění informačních a komunikačních digitálních technologií ve všech oblastech lidské činnosti a jejich přímé či nepřímé využití prakticky celou populací přináší požadavek, který vyžaduje v určitých případech trestné činnosti nutnost rozšířit vyšetřovací týmy nejenom o specialisty na tuto digitální techniku, ale i na odborníky v oblastech lidské činnosti, která digitální technologie specificky využívá. Jedná se tedy o reálnou potřebu vzniku multioborových vyšetřovacích týmů. Konkrétním příkladem může být potenciální snaha pachatele nebo pachatelů zaútočit pomocí informačních a komunikačních technologií na některý z prvků klíčové infrastruktury státu nebo na řídicí a informační systém některé z předních nemocnic nebo významného průmyslového podniku. V takto závažných nebo složitých případech nebude postačovat v praxi používaná metoda určité „off-line" spolupráce. I když se zdají být použité příklady zatím na první pohled nereálné, světová zkušenost potvrzuje opak a není nic lepšího, než být připraven jak organizačně, procesně, odborně ale i právně. Lze se důvodně domnívat, že takové situace, kdy by bylo potřebné sestavit specializovaný multioborový vyšetřovací tým již v minulosti nastaly, jen se o nich neví, nebo nebyly jako takové klasifikovány. Je potřeba se připravit na nepříznivé situace, které mohou nastat už v blízké době.[26]

Významným pomocníkem se může stát rozhodovací praxe soudů, která ukáže, jak je možné se vypořádat se zdánlivě obtížně uchopitelnými, nehmotnými důkazy s využitím znaleckých posudků. Hodnocení důkazu znaleckým posudkem spočívá v posouzení, zda závěry posudku jsou náležitě odůvodněny, zda jsou podloženy obsahem nálezu, zda bylo přihlédnuto ke všem skutečnostem, s nimiž se bylo třeba vypořádat, zda závěry posudku nejsou v rozporu s výsledky ostatních důkazů a zda odůvodnění znaleckého posudku odpovídá pravidlům logického myšlení. Důkaz znaleckým posudkem tedy soud hodnotí jako každý jiný důkaz, nemůže však přezkoumávat věcnou správnost odborných závěrů. Závěry znaleckého posudku nelze bez dalšího přebírat, ale je třeba v případě potřeby je ověřovat i jinými důkazy, a to zejména tehdy, jestliže mohou být pochybnosti o správnosti závěrů znaleckého posudku. Tak tomu je např., připouští-li znalecký posudek možnost zpřesnění jím uváděných údajů, avšak k tomuto zpřesnění znalec nepřikročí, nebo postupuje-li znalec ve znaleckém posudku podle určitého předpisu, ale v dílčím závěru se od něho bez bližšího zdůvodnění odchýlí.[27]

Nutnost interpretace digitálních stop do vnímatelné podoby a enormní složitost digitálních technologií obecně jednoznačně vede k novému modelu integrované kriminalisticko-expertizní práce, k vytvoření (reálnému nebo virtuálnímu) integrovaných vyšetřovacích týmů, ve kterých je nezbytné odborně, procesně, právně i organizačně zajistit těsnou spolupráci kriminalistů a digitálních expertů. Taková potřeba se stává realitou, se kterou je potřeba se vypořádat.

[26] Porada, V. Šedivý, P. Praktická využitelnost kriminalistických a forenzních aplikací v oblasti počítačové/kybernetické kriminality. Karlovarská právní revue, 2012, č. 3, s. 94 – 114.

[27] Rozsudky Nejvyššího soudu ČR ze dne 25. dubna 2002, sp. zn. 25 Cdo 583/2001 a ze dne 16. února 1995, sp. zn. Cdon 24/94. Cit. dle Smejkal, V. *Limity a možnosti kriminalistické počítačové analýzy.* In: *Identifikace potřeb právní praxe jako teoretický základ pro rozvoj kriminalistických a právních specializací.* Sborník vědeckých prací. Karlovy Vary: Vysoká škola Karlovy Vary, 2011, s. 102 – 114. ISBN 9788087236093.