NĚKTERÉ PRÁVNÍ ASPEKTY FORENZNÍ ANALÝZY DIGITÁLNÍCH DAT

LILJANA SELINŠEK[1]
Právnická fakulta Univerzity v Mariboru, Slovinsko

1. ÚVOD

Není pochyb o tom, že žijeme v digitálním věku, kdy je stále více činností založeno na sofistikované počítačové technologii, jež téměř nepozorovatelně ovlivňuje náš každodenní život. Moderní technologie se používají v lékařství, ekonomii, vzdělávání, státních záležitostech, všech druzích dopravy apod. Moderní člověk při telefonování, cestování, komunikaci prostřednictvím elektronické pošty apod. zanechává zpravidla elektronickou stopu o těchto činnostech, která se v případě potřeby může stát rovněž důkazem v některých právních řízeních. Vedle svých pozitivních stránek, projevujících se zejména usnadněním každodenního života, však mají moderní technologie i svou stinnou stránku spočívající ve zneužití těchto technologií k různé trestné činnosti. S rozvojem počítačových technologií se bohužel staly propracovanější a lépe koordinované i techniky počítačové kriminality.

Tento vývoj klade stále vyšší nároky na obor, jenž byl založen pro účely vyhledávání důkazů v digitální podobě a jejich převádění do člověku srozumitelného jazyka: forenzní analýzu digitálních dat. Bylo by chybou spojovat forenzní analýzu digitálních dat pouze s trestnou činností páchanou prostřednictvím moderních technologií. Vzhledem k tomu, že stále více relevantních skutečností je v digitální podobě,[2] měly by se digitální důkazy stát stále relevantnějšími důkazními prostředky při všech druzích soudního řízení. Je třeba zdůraznit, že forenzní analýza digitálních dat a digitální důkazy jsou užitečné nejen při vyšetřování počítačové kriminality a jiných forem trestné činnosti, ale i při prokazování řady dalších skutečností, například vůle smluvních stran v občanskoprávních věcech.

Ve společnosti založené na moderních technologiích by se forenzní analýza digitálních dat měla nepochybně stát jednou z hlavních vyšetřovacích metod a digitální důkazy by měly být hlavními důkazními prostředky, v mnoha evropských zemích se

[1] Překlad: Mgr. Alžběta Soperová.

[2] Každoročně je po celém světě zasláno přes tři biliony elektronických zpráv. Více než 90 % dokumentů vytvořených v různých organizacích je v elektronické podobě, a méně než 30 % těchto dokumentů je vytištěno. Viz zpráva Cybex, 2007, str. 25.

však v obou případech jedná o poměrně neznámou a exotickou oblast vyšetřování trestných činů[3] a soudního řízení. Na jednu stranu je to pochopitelné, neboť forenzní analýza digitálních dat je novým vědním oborem a digitální důkazy se od klasických podstatně liší. Vzhledem k rychlému a obrovskému rozvoji technologií by však právo mělo co nejdříve přijmout metody forenzní analýzy digitálních dat a digitální důkazy jako realitu i ve státech, kde této oblasti není věnována pozornost. K tomu jsou nezbytné změny na úrovni legislativy, soudní praxe a vzdělávání stávajících a budoucích pracovníků. Avšak předtím, než bude možné podniknout jakékoli konkrétní kroky, je třeba zodpovědět základní teoretické otázky týkající se vztahu mezi forenzní analýzou digitálních dat a (trestním) právem. Tento článek se zaměřuje na některé z nich, jež zůstávají nedořešeny i v mnoha evropských zemích. V rámci níže uvedených témat se pokusíme nalézt odpovědi nebo upozornit na zvláštní témata, jimž je třeba věnovat pozornost:

- Co je forenzní analýza digitálních dat a je namístě ji upravit zákonem a případně jak?
- Kdo má provádět forenzní analýzu digitálních dat při vyšetřování trestní věci?
- Kdy by měl odborník na forenzní analýzu digitálních dat vstoupit do trestního řízení?
- Jak zajistit, aby byly výsledky forenzní analýzy digitálních dat použitelné u soudu?

2. CO JE FORENZNÍ ANALÝZA DIGITÁLNÍCH DAT A JE NAMÍSTĚ JI UPRAVIT ZÁKONEM A PŘÍPADNĚ JAK?

Forenzní analýza digitálních dat se liší od většiny tradičních forenzních disciplín. Od doby objevení technologie analýzy DNA neměla žádná metoda tak rozsáhlý potenciální účinek na konkrétní druhy vyšetřování a trestního stíhání jako forenzní analýza digitálních dat. Jedná se o vysoce technický obor, související s řadou vědních oborů a oblastí: informatikou (počítačovou vědou), matematikou, fyzikou, elektrotechnikou, strojírenstvím a systémovým inženýrstvím, právem apod. Vzhledem ke všem těmto technickým detailům a složitým procesům mají právníci často problémy používat, či dokonce jen porozumět procesům používaným při vyšetřování prostřednictvím forenzní analýzy digitálních dat.[4] Použití vědy a inženýrství při konkrétním vyšetřování představuje složitý proces vyžadující profesionální úsudek a často se proto uvádí, že forenzní analýza digitálních dat je někdy spíše uměním než vědou.[5]

Existuje řada definic forenzní analýzy digitálních dat (též počítačová forenzní analýza, digitální forenzní analýza, forenzní analýza IT, atd.). Jednu z nejvýstižnějších vypracovali Broucek a Turner, kteří popisují forenzní analýzu digitálních dat jako *pro-*

[3] Například slovinská policie řešila v letech 2001–2006 celkem 487 957 trestních případů. Z toho byly k prozkoumání počítačového vybavení použity metody forenzní analýzy digitálních dat v celkem 212 případech. Z toho vyplývá, že slovinská policie používá metody forenzní analýzy digitálních dat přibližně v 0,05 % vyšetřovaných případů.

[4] Viz Ieong, R.S.C. FORZA – Digital forensics investigation framework that incorporate legal issues. (FORZA – Rámec vyšetřování prostřednictvím forenzní analýzy digitálních dat zahrnující právní aspekty.) Digital Investigation, Elsevier 3S, 2006, str. 29, (k dispozici na stránce www.dfrws.org/2006/proceedings/4-Ieong.pdf, ke dni 21. 7. 2008).

[5] Ryan, D. J., Shpantzer, G. Legal Aspects of Digital Forensics (Právní aspekty forenzní analýzy digitálních dat.) (k dispozici na www.danjryan.com/Legal%20Issues.doc, ke dni: 21. 7. 2008), str. 2.

cesy či postupy zahrnující sledování, shromažďování, analýzu a předkládání digitálních důkazů jako součást „předběžného" a/nebo následného („post mortem") vyšetřování trestné činnosti nebo nezákonného či jiného protiprávního jednání páchaných prostřednictvím internetu, tj. on-line.[6] Forenzní analýza digitálních dat však může být samozřejmě užitečná i při vyšetřování jiné trestné činnosti, bez přístupu na internet, tedy off-line. Jednoznačná je rovněž definice forenzní analýzy digitálních dat jako *disciplíny kombinující prvky práva a informatiky za účelem shromažďování a analýzy dat z počítačových systémů, sítí, bezdrátových komunikačních prostředků a paměťových zařízení způsobem, který je přijatelný jako důkaz u soudu.*[7]

Pojem forenzní analýza digitálních dat je těsně spjat s digitálními důkazy.[8] Obdobně jako v případě forenzní analýzy digitálních dat existuje mnoho definic pojmu „digitální důkaz", nejčastěji se však používá definice, již v roce 1999 navrhla pracovní skupina SWGDE,[9] která popisuje digitální důkaz jako *jakoukoli informaci s průkazní hodnotou ve vztahu k dané události, uložená nebo přenášená v digitální podobě.* Tato definice je velmi přesná, neboť ji lze použít na jakoukoli digitální technologii (zahrnuje počítače, mobilní telefony, digitální kamery, data z elektronických bezpečnostních systémů a jakékoli jiné technologie, jež mohou být případně spojeny s počítačovou kriminalitou nebo mohou případně poskytnout digitální důkazy).

Podstatnou otázkou spojenou s právními aspekty forenzní analýzy digitálních dat však je, zda by právníci neměli nejen znát výše uvedené definice, ale i rozumět tomu, jak počítače fungují. Sheetz jasně uvádí, že při jakékoli diskusi o forenzní analýze digitálních dat je třeba pochopit, jak počítače zpracovávají informace a jak souvisejí s okolním světem.[10] S tímto názorem musíme souhlasit. Právníci používající digitální důkazy v jakémkoli právním řízení by měli znát základní principy fungování počítačů a jiných digitálních přístrojů a měli by být rovněž obeznámeni se základními zásadami forenzní analýzy digitálních dat a technickými vlastnostmi digitálních důkazů. Nejsou třeba podrobné technické znalosti, avšak k přijetí správného (správných) rozhodnutí v případech, kde jsou použity digitální důkazy, je základní povědomí v tomto směru nezbytné. Jedná se především o to, že řádné posouzení průkazní hodnoty digitálních důkazů může vycházet pouze z pochopení takových vlastností digitálních důkazů, jež je odlišují od těch klasických.

Podíváme-li se na druhy a povahu digitálních důkazů podrobněji, je třeba nejprve uvést, že existují dva základní druhy údajů shromažďovaných metodami forenzní analýzy digitálních dat: trvalá a proměnlivá data. Trvalá data jsou data uložená na lokálním pevném disku nebo jiném médiu a zůstávají zachována i po vypnutí počítače. Pro-

---

[6] Viz Broucek, V., Turner, P. Winning the battles, losing the war? Rethinking methodology for forensic computer research. (Vyhrajeme bitvy, prohrajeme válku? Přehodnocení metodiky forenzního počítačového výzkumu.) Journal in Computer Virology, 2006, č. 2, str. 4.

[7] Srov. www.us-cert.gov/reading_room/forensics.pdf.

[8] Obdobně jako jiné forenzní oblasti, i forenzní analýza digitálních dat se provádí především s cílem získat důkazy použitelné u soudu.

[9] SWGDE je zkratka pracovní skupiny Scientific Working Group on Digital Evidence, www.swgde.org.

[10] Viz Sheetz, M. Computer Forensics. An Essential Guide for Accountants, Lawyers and Managers. (Počítačová forenzní analýza. Základní příručka pro účetní, právníky a manažery.) New Jersey: John Wiley & Sons, 2007, str. 14.

měnlivá data jsou data ukládaná v paměti (RAM) nebo existující při přenosu.[11] Základní vlastností proměnlivých dat je, že budou při vypnutí počítače ztracena, takže vyšetřovatel musí znát spolehlivé způsoby jejich zachycení; právník si přitom musí být vědom faktu, že vyšetřovatel musí tuto skutečnost znát; jinak budou shromážděné důkazy s velkou pravděpodobností nespolehlivé. Aby zajistili, že svou prací poskytnou řádný základ pro soudní přezkum, musí odborníci na forenzní analýzu digitálních dat zohlednit základní zásady forenzní analýzy digitálních dat.[12] Jednou ze základních zásad je, že při vyhledávání prostřednictvím forenzní analýzy digitálních dat musí být použita kopie (nikdy originál) dotčeného digitálního média, která však musí být s originálem zcela totožná. Během vyhledávání musí být věnována zvláštní péče zachování důkazu. Ten nesmí být žádným způsobem pozměněn. Digitální důkazy lze především snadno duplikovat nebo modifikovat, často bez zanechání jakýchkoli stop, a mohou tak představovat zvláštní problémy co se týče odborné způsobilosti. Opominutí zmrazit důkaz před otevřením souborů (spolu se skutečností, že samotným otevřením se soubory změní) může rozhodující důkaz znehodnotit, čehož si musí být vyšetřovatelé a právníci pracující na daném případu vědomi. Přestože technické stránky forenzní analýzy digitálních dat a digitálních důkazů mohou být pro právníky poněkud imaginární či složité, musí znát povahu těchto důkazů, pokud je chtějí správně vyhodnotit.[13]

Pravdou je, že forenzní analýza digitálních dat může velmi pracná a únavná. Přestože údaje lze jen těžko zničit, je na druhé straně často obtížné je najít. Nalezení relevantního důkazu v obrovském množství dat může být problematické (zejména pokud jsou kódována, označena zavádějícím způsobem nebo ukryta mezi mnoha nevinnými soubory). Ještě větší problém vznikne v případě, kdy kontrola počítače není dostačující, neboť digitální důkazy jsou uloženy na různých serverech napojených na internet a mohou se tudíž nacházet v různých zemích (z nichž každá má vlastní právní řád). Odborníci na forenzní analýzu digitálních dat však mají k dispozici řadu softwarových nástrojů a pomůcek, jejichž prostřednictvím mohou analyzovat počítač nebo jiná digitální zařízení podezřelého. Nejznámějšími komerčními nástroji jsou EnCase od Guidance Software a Forensic Toolkit (FTK) od AccessData, nejznámějším open source forenzním nástrojem je však Sleuth Kit.[14]

---

[11] Podrobnější informace získáte např. na webovém serveru United States Computer Emergency Readiness Team (US-CERT), www.us-cert.gov.

[12] Tyto zásady jsou technické povahy a formulují je některé nejvýznamnější forenzní instituce. Velmi dobrou praktickou příručku týkající se elektronických důkazů získaných prostřednictvím počítače vypracovalo sdružení ACPO (Association of Chief Police Officers, www.acpo.police.uk). Je k dispozici na internetu na adrese: www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf.

[13] Více informací týkajících se povahy digitálních důkazů naleznete např. v publikaci Sheetz, M. Computer Forensics. An Essential Guide for Accountants, Lawyers and Managers. (Počítačová forenzní analýza. Základní příručka pro účetní, právníky a manažery.) New Jersey: John Wiley & Sons, 2007.

[14] Pomocí těchto nástrojů je možné obnovit smazaná data, zjistit kdy byly soubory změněny, vytvořeny či smazány, určit, jaká paměťová zařízení byla připojena ke konkrétnímu počítači, jaké aplikace byly nainstalovány (i pokud již byly odinstalovány), jaké internetové stránky uživatel navštívil apod. Není však možné obnovit data, pokud již bylo příslušné digitální médium (fyzicky) zničeno. Pokud bylo digitální médium bezpečně přepsáno, je obnova dat buď velmi obtížná, nebo nemožná. Další účinnou obranu představuje kryptografie (šifrování), která činí data nečitelnými a tudíž nepoužitelnými. Pokud je správně použito a šifrovací klíče jsou bezpečně uschovány, lze šifrování dat jen těžko prolomit. Více informací ohledně šíře forenzní analýzy digitálních dat naleznete v publikaci Casey (2004). Každopáně každý, kdo sleduje seriál Kriminálka v Las Vegas a podobné vědeckofantastické filmy ví, že z technického hlediska jsou forenzní nástroje a techniky účinné, nikoli však všemocné.

Právníci nepotřebují vědět, jak tyto forenzní nástroje fungují, musí jim však být zřejmé, zda jsou dostatečně spolehlivé k tomu, aby poskytly digitální důkazy, které budou natolik průkazné, že budou moci být použity jako základ pro soudní rozhodnutí.

Vrátíme-li se k původní otázce, zda by měla být forenzní analýza digitálních dat upravena zákonem (a pokud ano, jak), je třeba zdůraznit, že to není potřebné. Forenzní analýza digitálních dat je určitým druhem služby. Vzhledem k tomu, že se jedná o jednu z mála forenzních oblastí, jež jsou zajímavé i pro soukromý sektor,[15] kde hrají významnou úlohu pravidla hospodářské soutěže, jakékoli omezení této služby by mohlo být velice problematické. Otázka, zda by měla být forenzní analýza digitálních dat upravena zákonem, by však neměla být zaměňována s otázkou, zda je třeba zákonem regulovat digitální důkazy a zda by měly právní předpisy stanovit některá omezení ohledně toho, kdo může provádět vyšetřování prostřednictvím forenzní analýzy digitálních dat, resp. příslušnou odbornou činnost. Těmito dvěma otázkami se zabývají následující kapitoly.

3. KDO BY MĚL PROVÁDĚT VYŠETŘOVÁNÍ PROSTŘEDNICTVÍM FORENZNÍ ANALÝZY DIGITÁLNÍCH DAT?

Otázka, kdo by měl shromažďovat a analyzovat digitální důkazy, je nejpalčivější ve fázi přípravného řízení, tj. ve fázi, kdy je věc v rukou policie a/nebo státních zástupců. Menší země se v tomto ohledu potýkají s problémy spojenými s nedostatkem finančních zdrojů. Forenzní analýza digitálních dat je zpravidla velmi nákladná. Vedle výkonného hardwaru a softwaru vyžaduje stálé vzdělávání příslušných pracovníků, což rovněž vyžaduje nemalé náklady. Zatímco větší a bohatší země si mohou dovolit financovat ze státního rozpočtu neziskové instituce jako laboratoře zabývající se forenzní analýzou digitálních dat, menší země čelí finančním omezením a následně nedostatku vyškolených odborníků. Ve Slovinsku se například objevily úvahy o možnosti překonat tento problém zapojením soukromého sektoru ve fázi shromažďování digitálních důkazů v (přípravném) trestním řízení (jako druh operativní pomoci policii, resp. státnímu zástupci). Tato myšlenka sice dosud nezískala významnější podporu, musíme však souhlasit s panem Goranem Oparnicou ze společnosti INsig2,[16] který uvedl, že dříve či později si vláda bude muset zvolit mezi dvěma zly: buď vůbec nevyšetřovat, nebo zapojit do části vyšetřování soukromý sektor. Druhá možnost je patrně lepší, navzdory všem souvisejícím problémům. Před uvedením jakéhokoli takového systému do praxe je samozřejmě nutné stanovit příslušná pravidla, aby se zabránilo jeho zneužití.

---

[15] Metody forenzní analýzy digitálních dat jsou užitečné nejen při vyšetřování trestných činů a jiných sporů končících před soudem, ale jsou vhodné rovněž k řešení některých případů porušení bezpečnosti, ztráty dat nebo obdobných (nikoli nezbytně kriminálních) případů, k nimž dochází v obchodních společnostech i jiných institucích. Abychom byli přesní, v těchto případech nelze hovořit o „forenzní" analýze digitálních dat, neboť pojem *forenzní* znamená *příslušející fóru, soudní, rovněž veřejný*, obsahově se však jedná o totožnou věc.

[16] INsig2 d.o.o. je chorvatská společnost zabývající se mimo jiné vyšetřováním prostřednictvím forenzní analýzy digitálních dat Viz www.insig2.hr.

Druhá otázka spojená s problematikou „kdo" by měl tuto analýzu provádět souvisí s dilematem týkajícím se potřebné kvalifikace odborníků na forenzní analýzu digitálních dat. Respektive konkrétněji: potřebují nějaké zvláštní vzdělání? Nebo postačí, pokud budou mít v tomto oboru praktické zkušenosti? Měli by být držiteli nějakého zvláštního (státního nebo soukromého) osvědčení? a podobně. Tyto poměrně složité otázky jsou aktuální v mnoha evropských zemích a souvisejí s některými jinými nedořešenými dilematy v rámci právních aspektů forenzní analýzy digitálních dat. Lze konstatovat, že neexistuje žádná konečná a univerzální odpověď, pro další diskusi o této problematice jsou však významná některá zjištění z průzkumu společnosti Cybex.[17] Podle tohoto průzkumu se právníci i odborníci na forenzní analýzu digitálních dat shodují, že k vedení vyšetřování prostřednictvím forenzní analýzy digitálních dat jsou potřebné praktické zkušenosti a podmínkou, již musí odborník na počítačovou forenzní analýzu splňovat, je vysokoškolské vzdělání v oboru informatika, inženýrství nebo matematika. Forenzní odborníci navíc považují za nezbytné, aby dotčená osoba získala osvědčení o znalosti forenzní analýzy digitálních médií vydané veřejným orgánem. Vysokoškolsky vzdělaný odborník by měl dále mít alespoň dva roky praxe a ti, kdo nemají vysokoškolské vzdělání, by měli absolvovat pět let praxe v příslušném oboru. Pro všechny odborníky je rovněž povinné další odborné vzdělávání, aby byli schopni sledovat nejnovější vývoj. Zatímco forenzní odborníci považují za vhodné řešení osvědčení vydané veřejným orgánem, právníci se na druhé straně domnívají, že odborník na počítačovou forenzní analýzu by měl být příslušníkem policie a měl by být držitelem osvědčení o znalosti forenzní analýzy digitálních médií vydaného soukromou institucí.[18] Z těchto zjištění vyplývá, že panuje poměrně vysoká míra konsensu ohledně otázky potřebného vzdělání a kvalifikace odborníků na forenzní analýzu digitálních dat, respondenti se však neshodují ve věci systému certifikace těchto odborníků. V každém případě by bylo vhodné uplatňovat při řešení této problematiky globální přístup, neboť víceméně jednotná kritéria platná pro odborníky na forenzní analýzu digitálních dat na celém světě by příznivě ovlivnila další vývoj tohoto oboru.

4. KDY BY MĚL ODBORNÍK NA FORENZNÍ ANALÝZU DIGITÁLNÍCH DAT VSTOUPIT DO TRESTNÍHO ŘÍZENÍ?

V rámci tohoto tématu je třeba zdůraznit dvě věci. Zaprvé, jak již bylo uvedeno, forenzní analýza digitálních dat a digitální důkazy nesouvisí jen s počítačovou kriminalitou a jinými formami trestné činnosti páchané prostřednictvím moderních technologií. Naopak! Digitální důkazy získané prostřednictvím metod forenzní

[17] Španělská společnost Cybex provedla specializovaný výzkum na téma „Přípustnost elektronických důkazů u soudu. Boj proti počítačové kriminalitě". Výsledky tohoto projektu financovaného v rámci programu AGIS byly zveřejněny v roce 2007 a jsou k dispozici na adrese www.cybex.es/agis2005/elegir_idioma_pdf.htm. Do projektu se zapojilo 16 zemí: Německo, Rakousko, Belgie, Dánsko, Španělsko, Finsko, Francie, Řecko, Nizozemsko, Irsko, Itálie, Lucembursko, Portugalsko, Spojené království, Rumunsko a Švédsko.

[18] Viz zpráva Cybex, 2007, str. 41.

analýzy digitálních dat mohou být relevantní v řadě trestních věcí – a to i u těch, kde počítače ani digitální zařízení při trestném činu vůbec nefigurovaly. Philips a Kent uvádějí jako příklad nedávný trestní případ z Británie, kdy byl muž uškrcen na cestě domů ze své oblíbené místní nálevny a zdálo se, že neexistuje žádný zřejmý motiv. Z oblasti krku oběti byly získány stopy DNA a policie vyzvala její rodinné příslušníky a přátele, aby dobrovolně odevzdali vzorek své DNA a mohli tak být vyloučeni z okruhu podezřelých. Švagr zemřelého nejprve žádosti nevyhověl, pak však neochotně souhlasil, když zjistil, že se stal hlavním podezřelým. Analýza DNA nepřinesla žádné výsledky, neboť silný déšť v noci, kdy se stala vražda, smyl většinu stop a nebyl tudíž k dispozici dostatek materiálu ke zjištění shody. Během dalšího vyšetřování byl zabaven švagrův počítač. Přitom příslušné orgány postupovaly v souladu se standardními postupy uznávanými všemi soudy ve Spojeném království. Odborník na počítačovou forenzní analýzu prozkoumal švagrův počítač a zjistil, že den před vraždou zadal do internetového vyhledávače výraz „jak zabít člověka". Tento jednoduchý digitální důkaz se tak ukázal jako podstatný pro vyřešení trestného činu vraždy,[19] který rozhodně není druhem trestné činnosti páchané prostřednictvím moderních technologií. Odpověď na otázku „kdy" je tedy v každém případě „často". Digitální důkazy se vyskytují všude kolem nás a mají mnoho podob, takže lze jejich prostřednictvím prokázat různé okolnosti.

Zadruhé je však třeba zmínit ještě jiné stanovisko. Někteří odborníci upozorňují, že, zejména v případech méně závažné trestné činnosti by měla být forenzní analýza digitálních dat použita pouze tehdy, není-li k dispozici dostatek jiných, tedy klasických důkazů. Tento názor vychází z takzvané ekonomické analýzy práva, která uvádí, že nákladné metody prokazování skutečností by se měly použít pouze pokud není k dispozici levnější cesta k dosažení stejného výsledku.[20]

5. JAK ZAJISTIT, ABY BYLY VÝSLEDKY FORENZNÍ ANALÝZY DIGITÁLNÍCH ÚDAJŮ POUŽITELNÉ U SOUDU?

Existuje pouze jeden způsob, jak zajistit, aby výsledky forenzní analýzy digitálních dat byly použitelné u soudu – musí být shromážděny zákonným způsobem, tedy v souladu s platnými právními předpisy. Nestačí zajistit usvědčující digitální důkazy; musí se tak stát zákonnou cestou.[21] V řadě států však nejsou stanovena zvláštní

[19] Viz Philips, A., Kent, J. eDisclosure: Lawyers are Treading a Risky Path. (Digitální důkazy: právníci se vydávají rizikovou cestou.) publikováno na www.7safe.com/assets/pdfs/eDisclosure%20white%20paper.pdf (práce byla vypracována v únoru 2007) (ke dni: 18. 7. 2008), str. 1.

[20] Více informací o těchto aspektech naleznete v publikaci Moore, T. The Economics of Digital Forensics. (Ekonomie forenzní analýzy digitálních dat.) (k dispozici na www.weis2006.econinfosec.org/docs/14.pdf, ke dni 21. 7. 2008), str. 1–10.

[21] Například ve Slovinsku smí soud vycházet při svém rozhodování v konkrétní trestní věci pouze z důkazů, jež byly shromážděny podle příslušných ustanovení Ústavy a trestního řádu. Důkazy získané způsobem porušujícím lidská práva nebo v rozporu s trestním řádem jsou absolutně neplatné a musí být vyloučeny (analýzu nákladů a přínosů nelze v tomto případě použít). Zákonný způsob shromažďování důkazů je však v trestním řádu v mnoha případech upraven pouze obecně a často proto není zřejmé, zda jsou určité vyšetřovací techniky a opatření dovolené či nikoli. Vzhledem k nedostatečné praxi to platí zejména

pravidla týkající se shromažďování, uchovávání, ukládání a analýzy digitálních důkazů. V těchto zemích platí pro digitální důkazy obdobně stejné předpisy jako pro klasické důkazy, což může přinášet problémy. Digitální důkazy jsou zejména natolik odlišné od těch klasických, že nepochybně vyžadují zvláštní právní úpravu.[22] Je však třeba zdůraznit, že zákonodárci musí postupovat velmi obezřetně. Pokud by byly digitální důkazy zakotveny v legislativě chybně, došlo by k ještě horší situaci, než když nejsou předmětem žádné zvláštní úpravy.[23]

Zvláštní skupinu tvoří digitální důkazy získané od třetích osob, např. obětí, správců sítě, osob odpovědných za bezpečnost informačních technologií ve společnostech nebo soukromých forenzních institucí. Ve skutečnosti je soukromé shromažďování digitálních důkazů stále běžnější. To je na jednu stranu pochopitelné, neboť v řadě zemí si nejsou donucovací orgány jisté, kdy a jak by měly být metody forenzní analýzy digitálních dat použity. Ve Slovinsku není například shromažďování důkazů soukromými subjekty právně upraveno, což však neznamená, že je takový způsob získávání důkazů nezákonný. Trestní řád především obecně nezakazuje soukromým subjektům shromažďovat informace, které mají povahu důkazů, pokud takové shromažďování není v rozporu s trestním řádem, trestním zákonem a jinými právními předpisy. Je proto možné použít digitální důkazy shromážděné soukromými subjekty jako relevantní důkazní prostředek v soudním řízení, pouze však pokud byly získány zákonným způsobem.

Nakonec je třeba upozornit ještě na jednu věc. Přestože odborníci na forenzní analýzu digitálních dat (zpravidla) nejsou právníci, měli by být do určité míry obeznámeni se základními instituty trestního práva procesního. Pokud nebude digitálním důkazům ve fázi jejich shromažďování věnována řádná péče a pozornost, mohou se stát bezcennými. Jak již bylo uvedeno, digitální důkazy jsou velmi proměnlivé a lze je snadno a rychle změnit. Pokud k tomu dojde, ztratí předmětný důkaz průkazní hodnotu a stane se nepoužitelným. Nejen legislativa, ale i znalosti odborníků na forenzní analýzu digitálních dat jsou klíčové k tomu, aby výsledky vyšetřování prostřednictvím forenzní analýzy digitálních dat byly použitelné u soudu. Pokud nebudou digitální důkazy shromážděny v souladu s příslušným zákonem stanoveným postupem, bude forenzní analýza digitálních dat pouze plýtváním časem a penězi.

---

v oblasti digitálních důkazů. Forenzní analýza digitálních dat je mladý obor, který (dosud) není ve Slovinsku příliš znám ani obecně přijímán soudy, takže hranice mezi zákonným a nezákonným shromažďováním digitálních důkazů nejsou přesně stanoveny. Podrobnější informace viz Selinšek, L. Legal Collecting of Digital Evidence. (Zákonné shromažďování digitálních důkazů.) In: Zbornik Pravne fakultete Univerze v Mariboru. Maribor, 2007, 3. ročník, (dokument v anglickém jazyce), str. 226–227.

[22] Ze studie společnosti Cybex vyplývá, že žádná ze zemí zapojených do projektu nemá systematickou právní úpravu digitálních důkazů, a to ani v trestním, ani v občanském procesním právu. V některých státech platí samostatná ustanovení týkající se výhradně digitálních důkazů, jiné státy však nemají ani taková ustanovení, takže digitální důkazy podléhají stejnému režimu jako ostatní, tzv. klasické důkazy. Mnoho právníků z celé Evropy se domnívá, že stávající právní situace v jejich zemi není ideální a vyžaduje provedení změn tak, aby právo odpovídalo reálnému stavu technologií. Viz zpráva Cybex, 2007, str. 31–32.

[23] Jak vysvětluje Sheetz, digitální důkazy nejsou ve skutečnosti nic jiného než série elektronických impulsů uložených ve více či méně stabilní podobě. Tyto uložené impulzy tvoří důkaz (viz Sheetz, M. Computer Forensics. An Essential Guide for Accountants, Lawyers and Managers. (Počítačová forenzní analýza. Základní příručka pro účetní, právníky a manažery.) New Jersey: John Wiley & Sons, 2007, str. 14). Narozdíl od klasických důkazů tedy nemůžeme digitální důkaz vidět, nemůžeme si na něj sáhnout ani jej cítit – můžeme vidět pouze jeho transkripci ze strojového do člověku srozumitelného jazyka.

6. ZÁVĚR

Výše přednesené otázky jsou pouze částí rozsáhlejší problematiky a měly být zohledněny při formování základu konstruktivního vztahu mezi forenzní analýzou digitálních dat a (trestním) právem. Podstatné je, že moderní technologie by se neměly stát překážkou dalšího účinného fungování orgánů činných v trestním řízení; a naopak, trestní právo by nemělo bránit využívání moderních technologií v soudním řízení. Styčné body mezi forenzní analýzou digitálních dat a trestním právem mohou být správně vymezeny pouze na základě vzájemného porozumění. Odborníci na forenzní analýzu digitálních dat musí ovládat nejen základní zásady trestního práva procesního, ale rovněž pravidla zákonného shromažďování digitálních důkazů; naopak právníci (státní zástupci, soudci a rovněž obhájci) musí být obeznámeni se základními postupy shromažďování, uchovávání, ukládání a analýzy digitálních důkazů, a tedy základními principy forenzní analýzy digitálních dat. Tato vzájemná znalost je zárukou správného a řádného použití výsledků vyšetřování prostřednictvím forenzní analýzy digitálních dat v soudním řízení, které je nejen vítané, ale dříve i později bude rovněž naléhavě nutné – neboť žijeme v digitálním věku.

LITERATURA

1. Broucek, V., Turner, P. Winning the battles, losing the war? Rethinking methodology for forensic computer research. (Vyhrajeme bitvy, prohrajeme válku? Přehodnocení metodiky forenzního počítačového výzkumu.) Journal in Computer Virology, 2006, č. 2, str. 3–12.
2. Casey, E. Digital Evidence and Computer Crime. (Digitální důkazy a počítačová kriminalita.) Londýn: Elsevier Academic Press, 2004.
3. Zpráva z výzkumného projektu společnosti: The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime (Přípustnost elektronických důkazů u soudu: boj proti počítačové kriminalitě), Cybex, Španělsko, 2007.
4. Ieong, R. S. C. FORZA – Digital forensics investigation framework that incorporate legal issues. (FORZA – Rámec vyšetřování prostřednictvím forenzní analýzy digitálních dat zahrnující právní aspekty.) Digital Investigation, Elsevier 3S, 2006, str. 29–36 (k dispozici na stránce www.dfrws.org/ 2006/proceedings/4-Ieong.pdf , ke dni 21. 7. 2008).
5. Moore, T. The Economics of Digital Forensics. (Ekonomie forenzní analýzy digitálních dat.) (k dispozici na www.weis2006.econinfosec.org/docs/14.pdf, ke dni 21. 7. 2008).
6. Philips, A., Kent, J. eDisclosure: Lawyers are Treading a Risky Path. (Digitální důkazy: právníci se vydávají rizikovou cestou.) publikováno na www.7safe.com/assets/pdfs/eDisclosure%20white%20paper.pdf (práce byla vypracována v únoru 2007) (ke dni: 18. 7. 2008).
7. Ryan, D. J., Shpantzer, G. Legal Aspects of Digital Forensics. (Právní aspekty forenzní analýzy digitálních dat.) (k dispozici na www.danjryan.com/Legal%20Issues.doc, ke dni: 21. 7. 2008).
8. Selinšek, L. Legal Collecting of Digital Evidence. (Zákonné shromažďování digitálních důkazů.) In: Zbornik Pravne fakultete Univerze v Mariboru. Maribor, 2007, 3. ročník, str. 217–230 (dokument v anglickém jazyce).
9. Sheetz, M. Computer Forensics. An Essential Guide for Accountants, Lawyers and Managers. (Počítačová forenzní analýza. Základní příručka pro účetní, právníky a manažery.) New Jersey: John Wiley & Sons, 2007.

Summary

The article is dealing with some legal aspects of digital forensics from the viewpoint of the countries where digital forensics is not (yet) often used investigation method, and digital evidences are not everyday evidence means. The questions discussed in the article should be answered at the beginning of the establishment the proper and legally accepted relation between digital forensics and law (the stress is, however, on criminal law, because the author is working in this field). The main goal of the article is to open some questions and to offer some possible answers. However, it has to be stressed that there is no universal answers on the questions about relation between digital forensics and law. While digital forensics is based on the similar principles and rules all around the world, the law is pretty much specific for almost each country. Besides, different levels of technical and informational development of the countries have to be taken into consideration. Even if questions from the article are already solved in some countries, they have just opened in the other ones, so it can be stated these questions are going to be relevant for some time.

Keywords: digital forensics, digital evidence, digital forensic expert, digital forensic examination, criminal procedure law

Klíčová slova: digitální analýza forenzních dat, digitální důkaz, odborníci na forenzní alalýzu digitálních dat, trestní právo procesní