JUDr. Jan Kolouch

Zajišťovací úkony a důkazní prostředky využitelné v rámci boje s kybernetickou trestnou činností

Článek charakterizuje jednotlivé zajišťovací úkony a možnosti jejich využití v rámci vyšetřování kybernetické trestné činnosti[1]. Specifikovány jsou i některé důkazy a důkazní prostředky. Samostatná pozornost je věnována otázce využití znalce při vyšetřování softwarové a internetové trestné činnosti.

Klíčová slova: Trestný čin. Internet. Kybernetická trestná činnost. Kyberkriminalita. Zajišťovací úkon. Důkaz. Důkazní prostředek. Ohledání. Znalec.

ÚVOD

Kybernetická trestná činnost je jednou z nejdynamičtěji se rozvíjejících forem trestné činnosti poslední doby. Jsem toho názoru, že je třeba na tento negativní trend reagovat zejména odbornou přípravou orgánů činných v trestním řízení a dalších subjektů podílejících se na boji s touto trestnou činností. Cílem tohoto článku je specifikovat některé zajišťovací úkony, důkazní prostředky a důkazy ve vztahu k této trestné činnosti.

ZAJIŠŤOVACÍ ÚKONY

„Úkony směřující k zajištění osob a věcí pro účely trestního řízení jsou závažnými zásahy do práv a svobod občanů, zaručených Listinou základních práv a svobod (Hl. II odd. 1) a jsou přípustné jen tehdy, jsou-li pro jejich výkon dány zákonné podmínky, čl. 8, 12, 13 LZPS.“[2]

Obecně je možné rozdělit zajišťovací úkony na **úkony** sloužící **k zajištění osob** a **úkony** sloužící **k zajištění věcí (a informací)**. Vzhledem ke specifičnosti kybernetické trestné činnosti se zaměřím především na úkony sloužící k zajištění věcí a informací (zejména § 88a tr. řádu).

1 Domnívám se, že výstižně lze kybernetickou trestnou činnost definovat jako jednání namířené proti počítači, případně síti, nebo jako jednání, při němž je počítač použit jako nástroj pro spáchání trestného činu. Počítačová síť je pak prostředím, v němž se tato činnost odehrává.

2 NOVOTNÝ, F. a kol. *Praktikum Trestní právo procesní.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2006. s. 84

Za věc důležitou pro trestní řízení je nutno považovat:

1. Předměty, které lze považovat za věcné důkazy ve smyslu ustanovení § 112 odst. 1 tr. řádu,
2. listiny, které lze považovat za listinné důkazy ve smyslu ustanovení § 112 odst. 2 tr. řádu,
3. předměty, na něž by se mohl vztahovat trest propadnutí věci nebo jiné majetkové hodnoty (§ 55 a násl. tr. zákona) nebo ochranné opatření zabrání věci nebo jiné majetkové hodnoty (§ 73 a násl. tr. zákona).[3]

Vydání a odnětí věci

Vydání a odnětí věci důležité pro trestní řízení je vymezeno ustanoveními § 78 a 79 tr. řádu. Samotnému odnětí věci musí předcházet výzva k vydání věci dle ustanovení § 78 tr. řádu, kde je zakotvena **povinnost** každého **předložit věc** důležitou pro trestní řízení na výzvu orgánů činných v trestním řízení, **případně** tuto **věc vydat**. Držitel věci musí být poučen o následcích neuposlechnutí výzvy. Povinnost vydat věc se nevztahuje na věci (zejména listiny, ale i data), jejichž obsah se týká okolností, o kterých platí zákaz výslechu, ledaže došlo k zproštění povinnosti zachovat věc v tajnosti nebo k zproštění mlčenlivosti (§ 99 tr. řádu).

V rámci kybernetické trestné činnosti se v praxi bude nejčastěji jednat o zajišťování výpočetní techniky včetně některých periférií (externí paměťová a rozmnožovací zařízení), interní či externí harddisky, datová média, komunikační prostředky (zejména mobilní telefony, SIM karty), listinné seznamy odběratelů, seznamy kontaktů, připravované papírové obaly datových nosičů (booklety), grafická zařízení k výrobě obalů, spotřební datový a kancelářský materiál apod. V případě zjištění, že pachatel svou trestnou činností získal prostředky, které následně užil např. na vybavení svého bytu spotřební elektronikou, je možné v rámci prohlídky zajistit i takové předměty.

V případě asijských velkotržnic, burz nebo klasických prodejen, kam má veřejnost volný přístup, lze popsaným způsobem zajistit věci, které jsou určeny k prodeji, nejčastěji padělané datové nosiče se softwarem, hudbou či filmy. O vydání věci se sepíše protokol, u kterého je nutné detailně popsat věc, kterou osoba vydává, aby nemohla být zaměněna za

3 Blíže NOVOTNÝ, F. a kol. *Praktikum Trestní právo procesní.* Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2006. s. 98

jinou.[4] Také je to třeba z důvodu případného následného vydání či vrácení věci, neboť popis věci se musí přesně shodovat s popisem věci, jak bude uváděn v usnesení o vrácení věci.[5]

Pokud nebyla věc dobrovolně **vydána** osobou, která ji má u sebe, **může být** na příkaz předsedy senátu a **v přípravném řízení na příkaz státního zástupce či policejního orgánu odňata.**[6] Příkaz k odnětí věci je rozhodnutím *sui generis* a není proti němu přípustný opravný prostředek. K odnětí věci by měla být přibrána nezúčastněná osoba (tzv. *extraneus* – svědek úkonu). Přítomnost nezúčastněné osoby není obligatorní, ale je žádoucí. Od přítomnosti nezúčastněné osoby lze upustit jen ve výjimečných případech, kdy není možné její účast hned zajistit a pro naléhavost věci nelze úkon odložit.[7]

O odnětí věci je třeba sepsat protokol (§ 55 tr. řádu) obsahující mimo obecných náležitostí i popis vydané nebo odňaté věci, tak aby ji nebylo možné zaměnit za jinou. Protokol také obsahuje údaj o tom, že bylo vydáno písemné potvrzení o převzetí věci. Osobě, která věc vydala, nebo jíž byla věc odňata, vydá orgán provádějící tento úkon písemné potvrzení o převzetí věci, nebo opis protokolu a to i v případě, že jej osoba nevyžaduje.

Prohlídka jiných prostor a pozemků

Prohlídku jiných prostor a pozemků lze vykonat, pokud jsou splněny zákonné důvody a podmínky pro její provedení. Prohlídku je možné vykonat, pokud je důvodné podezření, že v prostorech nesloužících k bydlení (jiných prostorech) a pozemku, které však nejsou veřejně přístupné, se nachází osoba nebo věc důležitá pro trestní řízení. V oblasti kybernetické trestné činnosti bude institut prohlídky jiných prostor a pozemků využíván převážně k zajištění věcných důkazů zpravidla tam, kde tato trestná činnost probíhá v podnikatelském prostředí. Zpravidla neoprávněná výroba, rozšiřování popř. jiné užití softwaru bývá prováděna fyzickými osobami, které jsou buď u podnikatelského subjektu zaměstnány, nebo jsou samy takovým podnikatelským subjektem. Ve většině případů je tato činnost prováděna v prostorách, které neslouží k bydlení, jako jsou živnostenské provozovny, sídla či provozovny obchodních kapitálových společností popř. jiných právnických osob, prodejny a servisy výpočetní techniky, asijské velkotržnice, stálé či příležitostné burzy apod. Odhalování této trestné činnosti s ohledem na náročnost a komplikovanost probíhá delší čas.

4 Nejčastěji nastává tento problém u datových médií typu CD a DVD
5 Srov. ust. § 80 a § 81 trestního řádu.
6 Policejní orgán potřebuje k odnětí věci předchozí souhlas státního zástupce, vyjma případu, kdy nebylo možné předchozího souhlasu dosáhnout a věc nesnese odkladu.
7 NOVOTNÝ, F. a kol. *Praktikum Trestní právo procesní.* Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2006. s. 100

Z praxe je možné uvést případ, kdy trestná činnost spočívající v nelegálním kopírování softwaru, byla prováděna z části v místě bydliště obviněného, z části v nebytovém prostoru, který sloužil jako sklad. V takovémto případě je nezbytně nutné specifikovat, na jakou část bydliště se bude vztahovat příkaz k prohlídce jiných prostor, a na jakou příkaz k domovní prohlídce.[8]

Nařídit uvedenou **prohlídku je oprávněn** předseda senátu, **v přípravném řízení státní zástupce nebo policejní orgán.** Policejní orgán k tomuto úkonu potřebuje předchozí souhlas státního zástupce. Bez příkazu nebo souhlasu může policejní orgán vykonat prohlídku, pokud příkazu nebo souhlasu nelze předem dosáhnou a věc nesnese odkladu, případně pokud uživatel těchto prostor písemně prohlásí, že s prohlídkou souhlasí a takové prohlášení předá policejnímu orgánu. Příkaz má opět formu *sui generis* a není proti němu přípustný opravný prostředek. Musí být písemný a odůvodněný.[9]

V případě zajišťování výpočetní techniky a paměťových datových médií je třeba přesný popis věci s nutnou technickou erudicí, nezřídka za přítomnosti počítačového experta (znalce). Policejní orgán by se měl vyvarovat povrchního označení výpočetní techniky konfigurací, kterou mu naznačí osoba u úkonu přítomná. Bez účasti znalce na místě je značně složité hodnověrně ověřit základní konfiguraci počítače, existuje tu možnost následného nařčení policisty z manipulace s důkazy nebo poškození zajištěné věci. Je vhodné také uvést výrobní číslo plechové vnější konstrukce počítače (tzv. case), pokud bude nalezeno (nejčastěji u vstupně/výstupních portů).

Po zaevidování počítače je nutné přijmout takové opatření, aby přístup k datům počítače v budoucnu mohl mít jako první znalec. K tomu jsou užívány metody zaslepení vstupně - výstupních zařízení včetně elektrického konektoru papírovými pásy, které po přilepení označí svým podpisem policejní orgán i osoba na úkonu účastná. Někdy je vhodné počítač vložit přímo do igelitového pytle nebo papírového boxu s protinárazovou výstelkou[10], a ten zajistit naznačeným způsobem. To platí i u zajišťovaných paměťových zařízení, u kterých je nutné označit minimálně typ, lépe výrobní číslo zařízení.[11] Datové nosiče (v poslední době jde nejčastěji o kompaktní disky typu CD a DVD) je vhodné přímo na místě označit číselnou řadou, která je vodítkem pro následné znalecké zkoumání a kontrolou, že po

8 KOLOUCH, J., SOUČEK, J. Několik poznámek k specifikům dokazování softwarové kriminality. In *Trestně procesní činnost policejních orgánů (aktuální problémy).* Praha: Policejní akademie České republiky v Praze, 2007, s. 62

9 NOVOTNÝ, F. a kol. *Praktikum Trestní právo procesní.* Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2006. s. 104-105

10 Použití molitanu, vzduchované igelitové fólie nebo papírových vložek.

11 Zejména pevné disky počítačů, paměťové karty, jiná externí přenosná zařízení na bázi pevného disku aj.

provedení prohlídky nebyly jiné datové nosiče do zajištěných přidávány nebo s nimi zaměněny.

Specifikum prohlídky jiných prostor a pozemků, stejně tak i domovní prohlídky v oblasti kybernetické trestné činnosti, spočívá v charakteru věcí, které hodlá policejní orgán získávat jako věcné důkazy. Jedná se zejména o věci informatického typu, programové vybavení, které bývá umístěno na pevných discích počítačů nebo na paměťových médiích. Jejich zajištění je takřka obligatorně nutné provádět za účasti znalce, neboť neodborné zacházení při zajišťování by mohlo způsobit ztrátu dat a zmaření účelu prohlídky. V případě aktivní účasti znalce z oboru informačních technologií na místě prohlídky je možné, a zpravidla i vhodné, zajistit důkazní materiál pomocí otisku dat na technologické zařízení znalce a vytvořit tak tzv. zrcadlovou kopii jakéhokoliv pevného disku (USB, HDD typu PATA, SATA I a II.). Problematickou však může být záloha diskového pole typu SCSI.

Zajišťování samotných pevných disků či celých počítačů se ne vždy jeví jako vhodné, neboť při zajištění pevného disku či celého počítače by případně mohla hrozit ekonomická a funkční destrukce mnohých společností. Mělo by docházet k naplnění základní zásady minimalizace a subsidiarity zásahů do základních lidských práv a svobod. Takovýto stav by rozhodně neměl být provedenou prohlídkou vytvořen, vždy však záleží na všech okolnostech konkrétního případu, neboť je třeba brát v úvahu i následné užití institutu zabrání věci nebo jiné majetkové hodnoty.[12]

Domovní prohlídka

Ve své podstatě je domovní prohlídka svým charakterem blízká popsané prohlídce jiných prostor a pozemků se základním rozdílem vyššího stupně zásahu ze strany orgánů činných v trestním řízení do základních lidských práv a svobod.[13] Stejně jako u prohlídky jiných prostor a pozemků, je možné ji vykonat, existuje-li důvodné podezření, že v bytě nebo jiné prostoře soužící k bydlení (trvalé či přechodné bydliště, ubytovny, vysokoškolské koleje, pronajaté místnosti určené k bydlení) nebo v prostorách k nim náležejících (např. garáž v domě, sklepní kóje, půda domu, kolna, aj.) se nachází osoba nebo věc důležitá pro trestní řízení.

Domovní prohlídku je oprávněn nařídit předseda senátu a v přípravném řízení

12 § 73 tr. zákona
13 KOLOUCH, J., SOUČEK, J. Několik poznámek k specifikům dokazování softwarové kriminality. In *Trestně procesní činnost policejních orgánů (aktuální problémy).* Praha: Policejní akademie České republiky v Praze, 2007, s. 64

na návrh státního zástupce soudce. Vlastní výkon domovní prohlídky provádí na příkaz předsedy senátu či soudce policejní orgán. Příkaz k domovní prohlídce je rozhodnutím sui generis. Příkaz musí být písemný a odůvodněný.

Typické odlišnosti u domovních prohlídek v oblasti kybernetické kriminality od domovních prohlídek u obecné kriminality spočívají například v tom, že pachatelé mohou mít výpočetní techniku, na které pracují, ukrytou i v jiných objektech, jež k obydlí náleží. Z praxe je možné uvést případ, kdy pachatel měl ve svém domě počítač se zcela legálním softwarovým vybavením a až při provádění prohlídky v souvisejících hospodářských staveních byla zjištěna místnost s počítačem a lisem určeným a užívaným k vytváření kopií softwaru a filmových disků.

U prováděných prohlídek v bytě, který pachatel obývá s dalšími osobami, bývá obtížné rozlišení věcí, které by měly být pro trestní řízení zajištěny a které ne. V praxi došlo při domovní prohlídce k tomu, že v jednom bytě bylo zajištěno více počítačů a datových médií, které byly umístěny v různých částech bytu. Po provedení znaleckého zkoumání vyšlo najevo, že trestné činnosti se dopouštěl jeden ze spolubydlících žijících ve společném bytě, přičemž ostatní spolubydlící užívali na svých počítačích legální software. K určení, která osoba vlastně trestný čin spáchala, výraznou měrou přispívá precizně sepsaný protokol o domovní prohlídce, kde je třeba popsat, v kterých místnostech byly věci zajištěny.

Zajištění jiné majetkové hodnoty a zajištění peněžních prostředků na účtu u banky

Trestní řád obsahuje stran zajištění věcí i speciální ustanovení, které popisují jiné majetkové hodnoty, zajištění peněžních prostředků na účtu u banky a zajištění zaknihovaných cenných papírů.[14]

Ve většině případů pachatelé zisky z tohoto druhu trestné činnosti použijí k okamžité spotřebě, nebo k nákupu spotřebního materiálu pro svoji další činnost, případně k nákupu výpočetní a jiné spotřební techniky. V tomto případě by bylo možné užít institutu zajištění jiné majetkové hodnoty, neboť takovýto materiál je výnosem z trestné činnosti. O zajištění jiné majetkové hodnoty **rozhoduje předseda senátu a v přípravném řízení státní zástupce nebo policejní orgán.** Policejní orgán potřebuje k takovému rozhodnutí předchozí souhlas státního zástupce, vyjma případů kdy věc nesnese odkladu. Uvedené rozhodnutí má formu

14 Srov. ustanovení § 79e a § 79a až 79c tr. řádu

usnesení a je proti němu přípustná stížnost.

Běžně se lze v praxi také setkat se situací, kdy pachatel výnosy z kybernetické trestné činnosti vkládá na účet banky. Pokud zjištěné skutečnosti nasvědčují tomu, že prostředky na účtu banky jsou výnosem z trestné činnosti, může **předseda senátu a v přípravném řízení státní zástupce nebo policejní orgán** rozhodnout o zajištění peněžních prostředků na účtu (případně prostředků na účat dodatečně došlých). Policejní orgán potřebuje k takovému rozhodnutí předchozí souhlas státního zástupce, vyjma případů kdy věc nesnese odkladu. Uvedené rozhodnutí má formu *usnesení* a je proti němu přípustná stížnost.

Mnohdy bývá problém určit, na jaký konkrétní účet pachatel výnosy z trestné činnosti ukládá, neboť mají pachatelé pro své potřeby založeno více bankovních účtů a pro zahlazení stop mezi nimi provádějí převody různých finančních částek, kdy jsou nelegální výnosy směšovány s běžnými příjmy pachatele. Tento problém vyvstává zejména v případě, kdy je pachatelem podnikatel - živnostník, které tyto příjmy může legalizovat fingováním své podnikatelské činnosti a zisků z ní.

Domnívám se, že díky novele trestního zákona je možné uplatnit na výnosy získané z kybernetické trestné činnosti ustanovení § 73 či 55 tr. zákona.

Záznam telekomunikačního provozu

Ustanovení § 88a tr. řádu je velmi významné při odhalování pachatele internetové trestné činnosti, neboť umožňuje zjistit **údaje o uskutečněném telekomunikačním provozu**. *„Jde o zásah do tajemnství zpráv podávaných telefonem nebo jiným podobným zařízením (čl. 13 LZPS). Telekomunikačním provozem je telefon, telefax, mobilní telefon, vysílačky i jiná telekomunikační zařízení včetně zasílání zpráv elektronickou poštou. E-mailovou zprávu po jejím vytištění prostřednictvím tiskárny je třeba považovat za věc důležitou pro trestní řízení, kterou lze vyžádat podle § 78 nebo odejmout podle § 79 tr. řádu. To lze považovat za správné, na rozdíl od názoru, podle něhož se na takovou zprávu vztahují ustanovení § 86 až §87c tr. řádu.“*[15]

K záznamu telekomunikačního provozu může dát příkaz předseda senátu a v přípravném řízení na návrh státního zástupce soudce, pokud se důvodně předpokládá, že budou zjištěny skutečnosti významné pro trestní řízení. Příkaz musí být vydán písemně a musí být odůvodněn. Záznam telekomunikačního provozu provádí Policie ČR. Bez příkazu je

15 CÍSAŘOVÁ, D., FENYK, J., GŘIVNA, T. a kol. *Trestní právo procesní.* 5. vyd. Praha : ASPI, 2008. s. 277

možné záznam provést pouze tehdy, pokud k poskytnutí údajů dá souhlas uživatel telekomunikačního zařízení.

Pro úplnost je třeba uvést dvě skutečnosti, které nemusí být zcela patrné ze znění vlastního ustanovení:

- Pokud má záznam telekomunikačního provozu sloužit jako důkaz, je třeba, aby byl doplněn o protokol, ve kterém je uvedeno: místo, čas, způsob a obsah provedeného záznamu, jakož i označení osoby, která takovýto záznam pořídila.[16]
- na rozdíl od ustanovení § 88 **neplatí v ustanovení § 88a** tr. řádu **omezení, že musí být vedeno trestní řízení pro trestný čin tam uvedený** - tedy § 88a tr. řádu lze aplikovat i na **trestné činy „lehčí" povahy**, než jsou zvlášť závažné trestné činy nebo trestné činy, jejichž stíhání je vázáno na vyhlášené mezinárodní smlouvy.

Vrácení věci

Jakmile není věci, která byla vydána nebo odňata pro potřeby trestního řízení již třeba, postupují orgány činné v trestním řízení dle ustanovení § 80 až 81a tr. řádu. Samotný akt fyzického vrácení věci se jeví problematickým u výpočetní techniky. Tuto techniku dostává policejní orgán po provedeném znaleckém zkoumání, přičemž její technický stav má zafixován v teoretické rovině ve znaleckém posudku. Znalec při své činnosti nezkoumá funkci zařízení, pokud mu to není v opatření uloženo. Policejní orgán většinou není schopen při předání věci uvést výpočetní techniku do provozu, aby přebírající osobu přesvědčil o stavu zařízení. Případné stížnosti osoby, že věci vydané pro trestní řízení byly, ať už při znaleckém zkoumání nebo jiné manipulaci s věcmi, poškozeny, by patrně musel řešit státní zástupce v rámci své dozorčí činnosti v rámci přípravného řízení. Tomu je nutné předejít zejména důsledným předáváním věcí s kontrolou jejich stavu při každé manipulaci s nimi a zvolením vhodných metod transportu a uložení věcí v depozitech.

Specifickým je případ, kdy oprávněná osoba ani po opakované výzvě věc nepřevezme. V takové situaci by mělo dojít k prodeji věci a získaná částka by měla být uložena v úschově soudu. V praxi se objevil případ, kdy bylo třeba vrátit datové nosiče s obsahem herního softwaru, u kterých nebylo možné vzhledem k absenci nositele autorských práv k softwaru určit, zda se jedná o originální či padělané disky. Osoba usnesení o vrácení věci prokazatelně obdržela, ale ani po opakované písemné výzvě věci fyzicky nepřevzala. Další postup v takové

16 Srov. CÍSAŘOVÁ, D., FENYK, J., GŘIVNA, T. a kol. *Trestní právo procesní.* 5. vyd. Praha : ASPI, 2008. s. 278

věci s ohledem na podstatu zajištěných věcí je u případů kybernetické trestné činnosti řešen nedostatečně. Zákonem stanovený postup, tedy prodej předmětných věcí a uložení získaných peněz do úschovy soudu, by v praxi přinesl řadu problémů a ve své podstatě by zcela nesmyslně zatížil osobu, která by takový úkon měla provést. Datové disky neurčitého původu a nezjistitelné kvality jsou prakticky nezpeněžitelné. Ze stejného důvodu také není možno ve smyslu ustanovení § 81 odst. 3 tr. řádu označit datové disky za věc bezcennou. Není tedy zcela zřejmý faktický postup u zákonem stanoveného teoretického řešení této situace. Jen pro doplnění lze uvést, že v naznačeném případě byla záležitost vyřešena dlouhodobým umístěním datových disků do depozita státního zastupitelství, což rozhodně není z hlediska času a nápadu obdobné trestné činnosti ideálním řešením.[17]

DŮKAZNÍ PROSTŘEDKY A DŮKAZY

Jako **důkazní prostředek** je možné označit jako **zákonem upravený způsob získání informace** (skutečnosti, která má být zjištěna - srov. ustanovení § 89 odst. 1 tr. řádu).[18] *„Důkazním prostředkem je zdroj, z něhož orgán činný v trestním řízení důkazy čerpá (výpovědi osob, věci). Je to určitá forma, jejímž prostřednictvím orgán činný v trestním řízení nabývá potřebných poznatků.“*[19] Trestní řád obsahuje **demonstrativní výčet** důkazů:

(2) ***Za důkaz může sloužit vše, co může přispět k objasnění věci****, zejména výpovědi obviněného a svědků, znalecké posudky, věci a listiny důležité pro trestní řízení a ohledání. Každá ze stran může důkaz vyhledat, předložit nebo jeho provedení navrhnout. Skutečnost, že důkaz nevyhledal nebo nevyžádal orgán činný v trestním řízení, není důvodem k odmítnutí takového důkazu.*

Při odhalování, objasňování a vyšetřování kybernetické trestné činnosti je možné užít všechny dostupné prostředky dokazování, které trestní řád při respektování základních zásad trestního řízení nabízí. V této kapitole popíši jen některé důkazy a důkazní prostředky, které slouží k odhalování a objasňování kybernetické trestné činnosti.

Věcné a listinné důkazy

Dle ustanovení § 112 odst. 1 tr. řádu se za **věcné důkazy** považují ty **předměty**,

17 KOLOUCH, J., SOUČEK, J. Několik poznámek k specifikům dokazování softwarové kriminality. In *Trestní právo*, 2007, roč. 12, č. 12, s. 11
18 NOVOTNÝ, F. a kol. *Praktikum Trestní právo procesní.* Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2006. s. 123
19 CÍSAŘOVÁ, D., FENYK, J., GŘIVNA, T. a kol. *Trestní právo procesní.* 5. vyd. Praha : ASPI, 2008. s. 284

kterými nebo na kterých byl trestný čin spáchán, jakož i **jiné předměty prokazující či vyvracející dokazovanou skutečnost**. Tyto předměty mohou být prostředkem k odhalení a objasnění trestného činu, jeho pachatele a případných stop. U kybernetické trestné činnosti budou nejčastěji **věcným důkazem paměťová média** (ve všech svých formách) obsahující určitá data a informace. Domnívám se, že dle výše uvedené charakteristiky **je možné** tyto **data a informace považovat za věcný důkaz**, i když nemohou existovat bez paměťového média. Jako příklad je možné uvést případ, kdy byla data před provedením domovní prohlídky odeslána na webhostingový server http://www.banan.cz/ a z počítače, na kterém se nacházela, byla zcela vymazána. Díky znaleckému zkoumání se podařilo část dat obnovit a dále získat přístup k datům uloženým na webhostingovém serveru. Data nebyla poškozena a prokázala vlastnění a šíření dětské pornografie pachatelem.

Za **listinný důkaz** dle ustanovení § 112 odst. 2 tr. řádu, je pak možné považovat ty **listiny, které svým obsahem** potvrzují či vyvracejí dokazovanou skutečnost. Typickým **listinným důkazem** u kybernetické trestné činnosti jsou **data či informace po jejich vytištění na tiskárně.**

Ohledání

Při ohledání se policejní orgán řídí obecnou kriminalistickou metodikou ohledávání s přihlédnutím k některým zvláštnostem kybernetické trestné činnosti. Vždy je nutné **přesně zadokumentovat** stav místa, např. obydlí, kde se ohledání koná.[20] Vedle protokolu, který musí být obligatorně sepsán o každém úkonu trestního řízení (§ 55 tr. řádu), nestanoví-li tr. řád něco jiného, je vhodné pořídit též obrazovou dokumentaci (fotodokumentaci), popř. **video dokumentaci** a přesně zachytit **umístění výpočetní techniky** v místnosti (zejména při ohledání v provozovnách a kancelářích právnických osob), její **přesné zapojení**, včetně popisu jednotlivých druhů kabeláže. Z těchto záznamů je potom možné zrekonstruovat, zda byl počítač v době prohlídky zapojen do počítačové sítě a jakou metodou[21], zda byl připojen k modemu s přístupem na Internet, případně zda bylo k počítači připojeno některé speciální periferní zařízení. Veškerá tato činnost směřuje k určení koncového uživatele počítače. Dle ustanovení § 113 odst. 1. tr. řádu se má k ohledání zpravidla přibírat znalec. V jednodušších případech však účast znalce není nutná, postačuje účast zvlášť vyškoleného kriminalistického technika či policisty specialisty, který však musí mít znalost počítačové terminologie a výpočetní techniky, včetně znalosti počítačových sítí. Policejní orgán také musí při ohledání

20 viz stať o domovní prohlídce resp. prohlídce jiných prostor a pozemků.
21 kabelové propojení, bezdrátové wi-fi sítě popř. technologie Bluetooth

uvažovat možnosti, že v rámci prohlídky dojde k ohledání velkého množství počítačů a paměťových médií, které bude nutné v protokole o ohledání přesně označit s využitím číselných řad včetně detailní lokalizace místa, kde se tyto předměty nalézaly.

Ohledání věci provádí policejní orgán zejména v souvislosti se zajištěním tzv. kontrolních nákupů. Jedná se o ohledání předmětů, které byly soukromými organizacemi (např. IFPI, BSA, aj.) zabývajícími se odhalováním a dokumentací případů porušování autorského práva v oblasti softwaru, získány od pachatele této trestné činnosti, a to zpravidla za úplatu. Ze způsobů předání paměťových médií s nelegálním softwarovým obsahem bývá nejčastější osobní předání, kdy pachatel na osobní schůzce prodá zájemci předem dohodnutý software, nebo korespondenční doručení, při kterém zájemce zasílá finanční částku pachateli buď bankovním převodem na účet, který je uvedený na poštovní poukázce, nebo formou poštovní dobírky. Kontrolní nákup je poté předáván jako příloha trestního oznámení policejnímu orgánu, a to ve stavu, v jakém byl od pachatele získán. Pro potřeby vyšetřování jsou často z takto získaných paměťových médií snímány převážně daktyloskopické stopy.

Ohledání věci lze dále využít i při prováděných prohlídkách v případě, že není předpoklad zajištění výpočetní techniky a je třeba zadokumentovat softwarové vybavení, které je na počítači nainstalováno. Po přesném popisu předmětného počítače, v rámci kterého je uvedena detailní hardwarová konfigurace včetně registračních údajů operačního systému, je např. pomocí screenshotu, případně fotograficky, snímán stav registračních údajů, který je zaznamenán do protokolu. Tímto způsobem je možné pro účely trestního řízení zaznamenat software, jenž je na počítači nainstalován, jeho verze, licenční čísla, uživatele programů apod. Je nutné dodat, že tento způsob popisu výpočetní techniky lze užít jen jako krajní prostředek.

V praxi nečastěji dochází k ohledání počítače při již popsaných prohlídkách, a vyvstává tak nutnost zajištění celého počítače jako **věci důležité pro trestní řízení** s následným předáním znalci ke zkoumání. Tím se policejní orgán vyhne případnému nařčení z manipulace s důkazy. Praktické užití ohledání věci je možné demonstrovat na případu z praxe, kdy byl dokumentován stav počítače u zákazníků, kteří si jej zakoupili v malém počítačovém obchodě. Zde jim servisní technik nainstaloval na zakoupený počítač operační systém a kancelářské aplikační programy, které však byly nelegální. Zajištění počítače koncovým uživatelům by bylo nevhodné, protože dle mého názoru pro účely trestního řízení plně dostačovalo k dokumentaci rozsahu trestné činnosti servisního technika, právě ohledání věci výše popsaným způsobem. Koncoví uživatelé byli upozorněni na nainstalovaný nelegální

software a byli poučeni o případných následcích jeho dalšího využívání.[22]

Znalecký posudek

Podle ustanovení § 105 odst. 1 tr. řádu rozhodne orgán činný v trestním řízení o přibrání znalce, je-li k objasnění skutečností důležitých pro trestní řízení třeba odborných znalostí. Zároveň toto ustanovení umožňuje využít v jednoduchých případech odborné vyjádření příslušného orgánu. U případů kybernetické trestné činnosti je de facto nemožné zajistit řádně důkazy bez přibrání znalce (nejčastěji z oboru kybernetika - výpočetní technika).

Ve složitějších případech je vhodné zvážit jeho **účast při prováděných prohlídkách**, neboť soudní znalec je schopen přímo na místě konzultovat nebo řešit technické problémy, které mohou s prohlídkou vzniknout. Typickým příkladem je pořizování identických otisků dat a jejich zálohování, není-li možné výpočetní techniku zajistit i s jejím datovým obsahem, zjištění rozsahu a způsobu propojení počítačů do sítě, zajištění zálohy velkého objemu dat apod.

V praxi běžně nastávají již zmíněné případy, kdy by díky zajištění desítek počítačů v rámci prohlídky mohlo dojít k rozsáhlým ekonomickým ztrátám podnikatelského subjektu, ať již spočívající v nutnosti nákupu nových počítačů a příslušného softwaru, nebo proplácení nucené dovolené zaměstnancům. Takovýto úkon by byl jistě podnětem pro podání žaloby soukromého subjektu na stát a zřejmě by muselo dojít k náhradě vzniklé škody. Proto je třeba v takových případech, pokud to dovolí technické možnosti, využít znalce k zadokumentování stavu výpočetní techniky včetně firemních serverů přímo na místě a zálohování identických obrazů dat na velkokapacitní paměťová zařízení, která umožní zpracování následného znaleckého posudku bez nutnosti faktické přítomnosti zkoumané výpočetní techniky.

Hlavní část využití znalce v rámci trestního řízení je jeho vlastní znalecká činnost, která se následně odrazí ve zpracovaném znaleckém posudku. V něm znalec odpovídá na otázky, které mu zadavatel (zpravidla policejní orgán) položil, přičemž mu nepřísluší hodnotit důkazy a také neřeší právní otázky. Znalecký posudek je zpracován zpravidla písemně, nicméně v oblasti kybernetické trestné činnosti se nelze vyhnout elektronické podobě (k posudku jsou běžně připojena vybraná zajištěná data v elektronické podobě na datových médiích). Jedná se zejména o případy zajištění elektronické pošty nebo obrazových a video dokumentů, jejichž vytištění na papír by mohlo způsobit značnou nepřehlednost a výrazně

22 Srov. PLECITÝ, David. *Prostředky dokazování softwarové kriminality*: bakalářská práce. Praha, 2006. 40 s. Policejní akademie ČR. Vedoucí práce JUDr. Jan Kolouch.

zvětšit rozsah znaleckého posudku v listinné podobě. Bohužel v praxi není nijak neobvyklé, že policejní orgán žádá po znalci vytištění veškerých dokumentů, neboť nemá technické vybavení na přehrání uvedených datových médií.

Obecně by měl policejní orgán od znalce vyžadovat minimálně následujících 5 úkonů:

- **Vytvořte kopii disku z počítače,**
- **zkopírujte uživatelská data z počítače,**
- **obnovte všechna smazaná data z disku počítače,**
- **zkopírujte všechna data z dalších paměťových zařízení (např. i z mobilního telefonu, SIM karty, aj.), včetně provedení obnovy dat z nich smazaných,**
- **ze záznamů uložených v počítači ověřte komunikaci uživatele.**

Dále by měly otázky směřovat na zjištění softwarového vybavení počítače, na zjištění, kdo je nositelem autorských práv ke konkrétnímu softwarovému produktu, kdy byl tento produkt do počítače nainstalován a zejména jaká je hodnota softwarového produktu. V mnohých případech není možné zjistit cenu produktu a znalec je tak prakticky jedinou objektivní osobou, která je schopna určit, jaká je hodnota (případně původ) jednotlivých programů, které pachatel neoprávněně užíval či rozšiřoval.

Toto zjištění má zásadní vliv na trestněprávní kvalifikaci skutku, zejména, zda pachatel svým jednáním nenaplnil i znaky kvalifikované skutkové podstaty trestného činu ustanovení § 152 odst. 2 tr. zákona.

Pro celkové pochopení činnosti znalce při znaleckém zkoumání uvádím nejčastější formulace otázek, které bývají znalci z oboru kybernetika - výpočetní technika pokládány. Závěry znaleckého posudku v oblasti kybernetické trestné činnosti jsou často rozhodujícím kriteriem pro zahájení trestního stíhání dle ustanovení § 160 odst. 1 tr. řádu.[23]

Otázky, které jsou nejčastěji kladeny znalci v souvislosti s vyšetřováním kybernetické trestné činnosti:

- **Proveďte základní popis a výpis hardwarové konfigurace zkoumaného počítače.**

Znalec popíše zkoumaný počítač tak, aby nemohl být zaměněn s jiným, určí jeho základní konfiguraci. Z vyjádření lze určit, zda má počítač vypalovací mechaniky, zda je

23 Blíže: PLECITÝ, David. *Prostředky dokazování softwarové kriminality*: bakalářská práce. Praha, 2006. 40 s. Policejní akademie ČR. Vedoucí práce JUDr. Jan Kolouch.

možné jej připojit k Internetu, zda a jaká periferní zařízení jsou užívána. Je také zjištěn systémový čas počítače, který stanovuje např. dobu spuštění či modifikace jednotlivých souborů.

- **Proveďte výpis veškerého nainstalovaného aplikačního programového vybavení z pevných disků zkoumaného počítače a rozlište, zda se jedná o software komerční nebo volně šiřitelný.**

Znalec zjistí, jaké konkrétní programy a jejich funkční či nefunkční části jsou na počítači nainstalovány či umístěny a určí, zda je k jejich užívání třeba licence a jaké.

- **U komerčního software, nainstalovaného na pevných discích zkoumaného počítače uveďte datum, kdy byl software nainstalován a nositele autorských práv k softwaru.**

U programu, k jehož užívání je třeba licence, je zkoumáno, kdy byl do počítače nainstalován, zda byl spouštěn a jak dlouho byl užíván. Tato zjištění mají vliv na trestněprávní kvalifikaci jednání pachatele a jsou určující při stanovování stupně společenské nebezpečnosti. Dále jsou určeny subjekty, které jsou nositeli práv k programu jako autorskému dílu. V praxi jsou možné případy, kdy nositel práv k programu je odlišný od jeho výrobce nebo prodejce. V souvislosti s tím se zjišťuje i hodnota programu a počet licencí, jejichž legalitu užívání by měl pachatel v následném řízení prokázat.

- **Při zkoumání zjistěte, zda se na pevných discích počítače nenachází soubor, ve kterém by byla uložena data klientů obviněného, jejich kontakty a další agenda, kterou mohl obviněný při své činnosti vést (databáze, účetní doklady, tabulky apod.).**

Uvedené informace mohou pomoci objasnit a prokázat rozsah pachatelovy trestné činnosti a dobu, po kterou jí páchá. Napomáhají ke zjištění dalších subjektů podílejících se na trestné činnosti, případně určení finančních prostředků, které svojí nelegální činností získal.

- **Proveďte výpis obsahu zajištěných nosičů (CD či DVD) označených číselnou řadou přičemž ke každému CD či DVD uveďte, zda je lisované či vypalované, zda se jedná o padělky či originály a proč. Dále rozlište, co je obsahem každého konkrétního datového nosiče.**

- **Proveďte u počítače zálohu e-mailové pošty.**

Výpisem elektronické pošty je možné zadokumentovat komunikaci pachatele např.

s odběrateli nelegálního softwaru či dalšími osobami podílejícími se na páchání softwarové a internetové trestné činnosti. Dále lze užít ustanovení § 88a tr. řádu a identifikovat dle e-mailové pošty případné spolupachatele. Tento úkon však lze aplikovat pouze tehdy, pokud pachatel užíval emailového klienta (např. Eudora, MS Outlook, Outlook Express, Mozilla Thunderbird apod.). Pokud pachatel vedl korespondenci přímo přes webové rozhraní, tento úkon nelze provést.

- **Uveďte další skutečnosti mající vztah k vyšetřovanému případu, pokud je považujete za potřebné v posudku uvést.**

V této části může znalec zmínit zjištěné skutečnosti, které zadavatel v opatření o přibrání znalce buď opomněl dotázat, nebo jejichž zjištění nemohl předpokládat. Domnívám se, že tato otázka by měla být v opatření uvedena obligatorně.[24]

ZÁVĚR

Jak již bylo uvedeno, není možné připustit, aby se virtuální prostor stal bezpečným prostředím pro pachatele, kde by mohli páchat de facto beztrestně jakoukoliv trestnou činnost. Jsem toho názoru, že je třeba efektivně zvyšovat vzdělanost orgánů činných v trestním řízení a dalších osob přicházejících do styku s touto trestnou činností, neboť existuje pouze jeden výchozí bod pro boj proti kybernetické trestné činnosti, a tím je kybernetická trestná činnost sama.

Hlavním cílem předložený článku bylo seznámit odbornou veřejnost s postupy, které mohou orgány činné v trestním řízení využít při odhalování, prověřování a vyšetřování internetové trestné činnosti.

Domnívám se, že by si zejména policejní orgán měl být vědom možností, které jsou mu poskytnuty trestním řádem a zákonem o Policii ČR, při odhalování a vyšetřování této značně specifické trestné činnosti. Jsem toho názoru, že de lege ferenda by měla být větší pozornost věnována i otázce odborné přípravy a specializace orgánů činných v trestním řízení, neboť se jedná o dynamicky se vyvíjející a stále progresivnější druh trestné činnosti, k jehož zvládnutí je třeba odborníků.

Nelze opomenout i tu skutečnost, že se bojem s protiprávními aktivitami v rámci internetu, ve světě i u nás, zabývají různé soukromé organizace. Domnívám se, že pokud

24 Při tvorbě této části bylo využito konzultací se soudním znalcem z oboru Kybernetika-výpočetní technika: Ing. Jiřím Bergerem, MBA

chceme účinně bojovat s a internetovou trestnou činností, mělo by v budoucnosti dojít k propojení soukromých organizací (zejména IT odborníků) s orgány činnými v trestním řízení, aby tak vznikly týmy schopné včas a adekvátně reagovat na stále sofistikovanější formy internetové trestné činnosti. Nezastupitelnou složkou pak je preventivní působení ze strany všech zainteresovaných subjektů.

Použitá literatura:

1. CASEY, E. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Second Edition.* London: Academic Press, 2004. 677 s. ISBN 0-12-163104-4
2. CÍSAŘOVÁ, D., FENYK, J., GŘIVNA, T. a kol. *Trestní právo procesní.* 5. vyd. Praha: ASPI, 2008. 824 s. ISBN 978-80-7357-348-5
3. DOSTÁLEK, L., KABELOVÁ, A. *Velký průvodce protokoly TCP/IP a systémem DNS*. 3. vyd. Praha: Computer Press, 2002. 552 s. ISBN 80-7226-675-6
4. JIROVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, a. s., 2007. 284 s. ISBN 978-80-247-1561-2
5. NOVOTNÝ, F., RŮŽIČKA, M. a kol. *Trestní kodexy: trestní zákon, trestní řád a související předpisy: (komentář)*. 2. vyd. Praha: Eurounion s.r.o., 2002. 1640 s. ISBN 80-7317-009-4
6. NOVOTNÝ, F. a kol. Praktikum Trestní právo procesní. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2006. 294 s. ISBN80-86898-74-1
7. PIKNA, B. *Výběr dokumentů ke studiu evropského práva s úvodním výkladem – oblasti justice a vnitřních věcí.* Praha: Policejní akademie ČR, 2003, 252 s. ISBN 80-7251-112-2
8. POLČÁK, R. *Právo na internetu.Spam a odpovědnost ISP*. 1. vyd. Brno: Computer Press, 2007. 150 s. ISBN 978-80-251-1777-4
9. PROSISE, Ch., MANDIVA, K. *Incident response & computer forensic, second edition.* Emeryville: McGraw-Hill Companies, 2003. 507s. ISBN 0-07-222696-X
10. SMEJKAL, V. a kol. *Právo informačních a telekomunikačních systémů.* 1. vyd. Praha: C. H. Beck, 2001. 542 s. ISBN 80-7179-552- 6

11. SMEJKAL, V. *Internet a §§§. 2. aktualizované a rozšířené vydání*. Praha: Grada Publishing, 2001. 283 s. ISBN 80-247-0058-1