Počítačová a internetová kriminalita v České republice

Doc. Ing. Vladimír Smejkal, CSc. *

Právní rozhledy 12/1999

I. Úvod a definice pojmu počítačová kriminalita

1. Počítače jako fenomén nového druhu kriminality

V okamžiku, kdy se počítače začaly měnit z počítacích, matematických strojů v původním slova smyslu v mnohoúčelově použitelná zařízení schopná převzít nejrůznější agendu a kdy spolu začaly komunikovat prostřednictvím sítí, staly se počítače, jejich programy a data v nich uložená jednak *cílem trestné činnosti*, ale současně se objevil také *počítač jako zločinný nástroj.* Vznikl tedy nový obor zločinnosti, *počítačová kriminalita.* Stojí za zmínku, že tento nový kriminální obor se rozvíjí stejně bouřlivě jako technický obor, s nímž souvisí. Dokonce tak bouřlivě, že už v roce 1990 byla na mezinárodním fóru zmíněna počítačová kriminalita jako jedna z nejnebezpečnějších forem kriminálních deliktů spolu s organizovaným zločinem a distribucí drog, což je mimochodem skoro to samé. [1][1] Možná to bude znít poněkud pateticky, ale využití počítačové techniky dává pachatelům trestné činnosti křídla. Otevírá jim netušený svět nových možností, jak páchat trestnou činnost.

2. Obor počítačová kriminalita a obory související

V souvislosti s kriminalitou a počítači byl použit výraz „*počítačová kriminalita*“. „Computer crime“ se jako všeobecně přijímaný a chápaný pojem objevuje v právní a kriminologické terminologii vyspělých zemí již v sedmdesátých letech - např. [10], [11], v letech osmdesátých již přímo masově. (V USA byl první počítačový trestný čin zaznamenán v roce 1958 [13] a od té doby roste počítačová kriminalita masově.) V naší literatuře se objevuje (s příznačným zpožděním odpovídajícím technologickému zpoždění) v letech osmdesátých, a to nejprve jako ojedinělé zprávy o jednotlivých odhalených trestných činech zejména v Kriminalistickém sborníku, později jako předmět základního výzkumu [12], [13] a prvních pokusů o systematické vymezení oboru [14]. Teprve koncem osmdesátých let a v letech devadesátých se objevuje několik pracovišť a odborníků, kteří se věnují systematicky teoretickým a/nebo praktickým aspektům počítačové kriminality u nás. Za zmínku stojí autoři, kteří začali systematicky budovat *obor počítačové kriminality* u nás, a to jak svým působením teoretickým (zejména literatura [15]), tak praktickým ([16], [17] apod.) a pedagogickým; patří mezi ně především T. Sokol, M. Vlček a autor tohoto textu [72], [74]. Jim sekundujícími pracovišti jsou Kriminalistický ústav Policie ČR [26] a Policejní akademie, často v součinnosti se Společností pro kriminalistiku [27], [28], [74].

Obdobný překotný rozvoj v souvislosti s novými informačními technologiemi naznal i obor blízký, v oblasti deliktů se s počítačovou kriminalitou částečně překrývající, a to *autorské právo*, reprezentované dříve především K. Knapem a M. Opltovou [18], [19], nyní okruhy autorů Kříž a

kol. [20], Boháček - Loebl [21], [22] a nejvýrazněji I. Telecem [23], [24], zejména pak jeho brilantním komentářem k autorskému zákonu [25].

Třetí oborovou „množinou“, která se dosti značným způsobem překrývá s problematikou počítačové kriminality (a počítačového práva) je *ochrana osobních dat* (zejména v informačních systémech), která rovněž nabývá v posledních letech v České republice na významu (opět kopírováním zahraniční křivky zájmu). Zde působí kromě výše uvedených autorů [15], [71], [74] především P. Mates [29], [30], [31], [62], [71].

Pro potřeby tohoto příspěvku se dále budu věnovat především problematice vlastní počítačové kriminality, přičemž budou diskutovány i ty aspekty, které se dotýkají autorskoprávní problematiky a ochrany osobních dat v informačních systémech, a to především z hlediska jejich trestněprávní aplikace.

3. Vymezení obsahu počítačové kriminality

Označení „*počítačová kriminalita*“ má obdobný charakter jako pojmy „násilná kriminalita“, „kriminalita mladistvých“ apod. Takovýmito názvy jsou označovány skupiny trestných činů, mající určitý společný faktor, jako např. způsob provedení, osobu pachatele (alespoň druhově) apod. Ve své podstatě přitom může jít o velmi různorodou směsici trestných činů, spojených oním společným faktorem, mnohdy zjištěným původně jako statistická veličina. Přitom ale - na rozdíl od jiných kategorií trestné činnosti - dlouho neexistovala jasná shoda v tom, co počítačovou kriminalitou je.

Diskuse, která proběhla u nás v devadesátých letech především v [15], [27], [74] se přiklonila k názoru poprvé publikovanému kolektivem Smejkal, Sokol, Vlček v [15], že pod pojmem „počítačová kriminalita“ je třeba chápat *páchání trestné činnosti, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení včetně dat*, nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď:

a) jako *předmět* této trestné činnosti, ovšem s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité,
b) nebo jako *nástroj* trestné činnosti.[2]

Počítač může být předmětem trestného činu; současně je ale také ke spáchání celé řady trestných činů ideálním prostředkem. Počítač nemusí být pouze předmětem manipulace typické pro majetkové útoky vůči jiným věcem. Počítač má i svůj vnitřní obsah, který může být samostatným předmětem útoku. Jeho obsah - data a software, může být např. pozměněn, a to jako cíl určité činnosti, nebo jako pouhý prostředek k dosažení nějakého jiného cíle. Jde tedy o problematiku mnohem složitější.

Pokud se více zaměříme na vlastní obsah počítačů a počítačových sítí, můžeme zde ze systémového a metodologického hlediska právních a kriminologických disciplín hovořit dokonce o vzniku *„informatického práva“* a *„informatické kriminality“* (možná také „informační kriminality“), která by mohla zahrnovat trestněprávní, autorskoprávní a občanskoprávní (osobnostní) aspekty. První dílčí pokus o syntézu byl učiněn v díle [15] a znovu detailněji v [75].

Překotný rozvoj výše nastíněných oborů si vyžádá nepochybně řadu dalších, navazujících a zpřesňujících publikací.

Soubor všech možných jednání souvisejících s počítači a kvalifikovatelných jako trestné činy lze alespoň pracovně rozdělit do těchto subkategorií:

1) *Trestné činy ve vztahu k počítači, jeho příslušenstvím a jiným nosičům informací jako věcem movitým.* Logicky by sem patřily i trestné činy ve vztahu k programu jako autorskému dílu - neboli útoky na nehmotný majetek, avšak právě pro specifika majetku nehmotného jej zařadíme do druhé skupiny - majetková kriminalita v klasickém významu.

2) *Trestné činy ve vztahu k software, k datům, resp. uloženým informacím.* Počítač jako cíl útoku, předmět trestného činu - informační kriminalita v souladu s předchozími definicemi.

3) *Trestné činy, při nichž je počítač prostředkem k jejich páchání.* (Počítač je zde použit jako nástroj zločince, hmotná schránka ani její obsah nejsou cílem útoku, což ovšem zcela nevylučuje souběh s jednáními podle bodu 2) - hospodářská kriminalita (obvykle podvody, defraudace apod.).

Z hlediska obecné teorie trestního práva můžeme definovat následující skupiny znaků jednotlivých skutkových podstat:

1. objekt trestného činu - za objekt trestného činu jsou považovány předměty ochrany trestním zákonem;

2. předmět útoku - tím může být člověk, věc, ale i nehmotný majetek (právo, informace apod.); porušení předmětu útoku je účinkem trestného činu;

3. objektivní stránka trestného činu - zahrnuje především tzv. obligatorní znaky, kterými jsou: jednání, následek a příčinný vztah mezi nimi (kauzální průběh);

4. subjektivní stránka trestného činu - zahrnuje znaky týkající se psychiky pachatele (zavinění, pohnutka apod.).

Jak bychom mohli definovat z těchto hledisek hlavní skutkové podstaty přicházející v úvahu v souvislosti s počítači je uvedeno *v tabulce 1*.

Skutková podstata	**Druh trestného činu**	**Objekt trestného činu**	**Předmět útoku**	**Účinek trestného činu**	**Příklad trestného činu**
§ 257a	majetkový	ochrana dat uložených na nosiči informací a ochrana počítače;	nosič informace i informace na něm	změna informace nacházející se na nosiči informací	zásah do databáze klientech banky; zničení obsahu

		tím se zprostředkovaně chrání další zájmy a vztahy - projevy osobní povahy, obchodní tajemství, autorská díla apod.	uložená		pevného disku počítače jeho vymazán m; zkopírová í seznamu zákazník a předání konkuren
§ 152	hospodářský	ochrana autorských práv nebo práv autorským příbuzných	autorské dílo	neoprávněné nakládání s dílem (užívání autorského díla bez souhlasu autora; zásah do cizího autorského díla)	neoprávné užívání počítačového programu okopírová í nebo zásah do cizích WWW stránek n Internetu
§ 178	proti pořádku ve věcech veřejných	právo na ochranu před neoprávněným nakládáním s osobními údaji (zveřejněním, jiným zneužitím)	osobní údaj	prozrazení osobních údajů jiné osobě nebo umožnění jiným osobám, aby se s nimi seznámily	vyzrazení údajů o zdravotní stavu urč osoby (např. pohlavní choroba)
§ 250	majetkový	cizí majetek	věc, pohledávka nebo jiné právo nebo penězi	uvedení někoho v omyl, využití omylu	změna platebního příkazu předávan o bankou ke zúčtován do ČNB

§ 125	hospodářský	zájem na vedení řádné hospodářské a obchodní evidence a na pravdivosti zápisů v obchodním rejstříku	ocenitelná hodnota a výkaz, evidence, hlášení, údaje vkládané do počítače, program počítače	uvedení nepravdivých nebo zkreslených informací; zásah do technického nebo programového vybavení počítače	úprava účetních záznamů informačním systém podnikate

Z hlediska aplikace ustanovení zvláštní části trestního zákona představuje problematika počítačů v trestné činnosti nebo úžeji počítačová kriminalita velmi zajímavý a možná nejrozsáhlejší soubor problémů. Trestní zákon je také dosud jediným obecným právním předpisem, obsahujícím normu, která upravuje skutkovou podstatu jednání, která souvisí výhradně s počítačem (§ 257a).[3] Pro úplnost je třeba dodat, že trestní zákon obsahuje i několik ustanovení, jejichž skutková podstata může být také naplněna (a stále častěji naplněna je) jednáním souvisejícím s počítači (zejména § 152 - Porušování autorského práva v podobě neoprávněného užívání počítačových programů a § 178 - Neoprávněné nakládání s osobními údaji).

Podobně i jiné trestní zákony vyspělých zemí obsahují zvláštní ustanovení týkající se trestných činů souvisejících s počítači. Nejkomplikovanější je situace ve Spojených státech amerických, kde existují federální zákony i zákony jednotlivých států USA, přičemž „počítačové právo“ je postupně upravováno a rozvíjeno jak v trestněprávní, tak veřejnoprávní a soukromoprávní oblasti prostřednictvím řady na sebe navazujících zákonů. Viz např. zákon č. 18. U.S.C. Crimes and Criminals Procedure, Sec. 1029 „Fraud and related activity in connection with access devices, Sec. 1343 „Fraud with wire, radio or television“, a zejm. Sec. 1030 „Fraud and related activity in connection with computers“ [první právní úprava 1977 - Federal Systems Protection Act Bill, následovaná významným Federal Computer Systems Protection Act (tzv. Ribicoff) z roku 1979, zavádějícím pojmy „Computer Fraud“ a „Computer Abuse“, dále upraveno na základě Computer Fraud and Abuse Act, 1986-1994 atd.] - viz lit. [13], [35]. Uveďme si jako ilustrativní příklad stát Pensylvania - 18. Crimes and Offenses, ustanovení 3393. Nezákonné používání počítače: „*Osoba se dopustí trestného činu, jestliže (1) otevře, provede změny, zničí nebo poškodí jakýkoliv počítač, výpočetní systém, počítačovou síť, počítačový software, počítačový program nebo databázi nebo jejich jakoukoliv část, a to s úmyslem přerušit normální fungování organizace nebo vymyslet nebo provést jakékoliv schéma nebo za pomoci triku podvodně získat nebo oklamat nebo řídit majetek nebo služby, a to prostřednictvím falešných nebo klamných záminek, prohlášení nebo slibů; (2) záměrně, a bez oprávněných přístupů změní, zasáhne do provozu, poškodí nebo zničí jakýkoliv*

počítač, výpočetní systém, počítačovou síť, počítačový software, počítačový program nebo počítačovou databázi nebo jejich jakoukoliv část; nebo (3) záměrně nebo vědomě a bez oprávnění poskytne nebo zveřejní přístupové heslo, identifikační kód, osobní identifikační číslo nebo další důvěrné informace o počítači, výpočetním systému, počítačové síti nebo databázi.“ Srovnání této definice skutkové podstaty s českou právní úpravou (§ 257a) vypovídá o cestě, kterou naše kodifikace ještě musí urazit.

Podobnou cestou prošly všechny vyspělé země (např. SRN § 263a, 269, 270, 303 StGB [36], Švýcarsko § 143, 144, 147 StGB (CH) [37] apod.).

II. Historická doba počítačové kriminality

Tato část slouží k rozdělení jednotlivých druhů (projevů) počítačové kriminality podle skutkových podstat definovaných v našem trestním zákoně (č. 140/1961 Sb., ve znění pozdějších předpisů, dále jen TrZ). (Připomínám zásadu „nullum crimen, nulla poena sine lege“ - jen zákon stanoví, které jednání je trestným činem a jaký trest lze za jeho spáchání uložit.) Může se tedy stát, že některé skutkové podstaty nedostatečně pokrývají vyskytující se společensky nebezpečnou činnost, kterou je tedy nemožné (alespoň pod přesným vymezením objektivní stránky trestného činu - viz § 3 TrZ) sankcionovat. Tak, jak se vyvíjely počítačové a informační technologie, vznikla a dále se vyvíjela (a nyní přímo kvete) počítačová kriminalita. Stav techniky a jejího využívání limitoval i možnosti zločinců, což uvidíme z charakteristiky počátečního období počítačů a počítačových zločinů u nás.

1. Sabotáž

Pravděpodobně první čistě počítačový zločin se u nás odehrál v sedmdesátých letech, kdy nespokojený pracovník Úřadu důchodového zabezpečení poškozoval magnetem záznamy na magnetických páskách. Tento pracovník byl odsouzen podle neověřených informací za sabotáž. (Poznámka: údajně první počítačovou sabotáží bylo ničení textilních tkacích strojů řízených štítky v manufaktuře pana Josefa Jacquarda ve Francii v roce 1801 [39]).

Podobný případ se odehrál v letech 1985-87, kdy pracovníci výpočetního střediska poškozovali počítač sovětské výroby (nechvalně známý systém SMEP), aby dosáhli zrušení jeho instalování a výměnu za kvalitnější západní systém. Trestní stíhání (prováděné tehdejší StB) bylo zahájeno pro *sabotáž (§ 97 TrZ)*, aby bylo později dvakrát překvalifikováno na jiné trestné činy - jednou prokuraturou překvapivě na *porušování povinností v provozu socialistické organizace (§ 129-130 tehdejšího TrZ)* a podruhé soudem na *poškozování majetku v socialistickém vlastnictví (§ 136 - 137 tehdejšího TrZ)* - a konečně bylo zastaveno na základě stanovení skutečně vzniklé škody soudním znalcem vzhledem k amnestii. Princip ohodnocení škody totiž spočíval v tom, že počítač nebyl předán do reálného provozu (řízení válcovací pece), tudíž výpadky ve výrobě nevznikly a do výpočtu škody mohly být zahrnuty pouze položky jako „přeštípnutý drát“„izolovaný konec pojistky“ apod. a započteny práce na uvedení do původního stavu, tedy vysloveně haléřové či korunové položky. Samozřejmě, že trestní stíhání by mělo jiný výsledek, pokud by byla podána obžaloba pro sabotáž.

2. Dokladové delikty

Tak, jako se měnily údaje v běžných papírových dokladech, začali zločinci měnit podklady připravené ke zpracování do počítače. Teprve poté si uvědomili, že daleko jednodušší je měnit údaje přímo v počítači.

Typickým příkladem byl podvod spáchaný v zásilkové službě MAGNET, kdy pracovnice odebírala zboží na adresu své matky a do databáze odběratelů vždy uvedla, že zboží bylo zaplaceno.

Jiné způsoby těchto „dokladových" deliktů spočívaly v zasílání faktur na jiné velkoodběratele, manipulace s výplatami apod. Jednalo se o nejčastější odhalený počítačový zločin, jehož podstatou byly manipulace v mzdových účtárnách, MTZ, odbytech a na jiných pracovištích, kde pracovník měl možnost manipulovat s penězi (ať už v hotovosti nebo přes čísla účtů) či zbožím; jen v osmdesátých letech to bylo 14 případů trestního stíhání.

Právní kvalifikace v době předrevoluční se obvykle klonila k obávanému § 132 tehdejšího TrZ „*Rozkrádání majetku v socialistickém vlastnictví",* zatímco dnes jsou skutky tohoto typu obvykle kvalifikovány jako podvod (§ 250 TrZ) nebo zpronevěra (§ 248 TrZ). Na rozdíl od podvodu získá u zpronevěry pachatel faktickou moc nad věcí bez vyvolání nebo využití omylu - např. bankovní úředník, zaměstnanec pošty.

3. Neoprávněné užívání počítačů

Další masivní způsob páchání trestné činnosti související s počítači byl spjat s vysokou nedostupností počítačů a spočíval v provádění výpočtů na počítačích zaměstnavatele. Stupeň tohoto nelegálního užívání cizí věci (podle tehdejší kvalifikace *Neoprávněného užívání věci z majetku v socialistickém vlastnictví - § 133 tehdejšího TrZ*) byl různý: od tisku populárních obrázků na řádkové tiskárně, přes kondiciogramy a výpočty diplomových prací až po skutečné nelegální podnikání za účelem vlastního obohacování.

Jedním z prvních případů byl trestný čin spáchaný systémovým programátorem LPS VUT Brno, který na počítači zpracovával (dlouhodobě a opakovaně) pořadníky bytových družstev v Brně. Tento případ byl soudy různých stupňů posuzován různě, protože soud se pohyboval ve stavu důkazní nouze o skutečném rozsahu nelegálního počítání, což vyplývalo především z charakteru počítače SAAB jakožto školního počítače, kde nebyla vedena detailní evidence o spotřebovaném strojovém času.[4]

V této době se také objevuje *vysoká míra latence počítačových deliktů,* daná vztahem občanů k tzv. společnému, socialistickému vlastnictví, umocněná nehmotným charakterem počítačového času, kdy vlastně v podstatě vůbec nic hmatatelného ukradeno nebylo. Nutno říci, že toto pojetí přetrvává u některých reprezentantů orgánů činných v trestním řízení doposud. Zvláštní charakter počítačového času vedl v počátcích boje proti počítačové kriminalitě k nutnosti aplikovat na skutkové podstaty ustanovení trestního zákona, která vůbec se skutečným činem nesouvisela: klasickým zahraničním případem je odsouzení hackera za krádež elektrické energie, kterou spotřeboval neoprávněným užíváním počítače. Trestní postih plnohodnotné počítačové kriminality se datuje v českém právním řádu až od vložení ust. § 257a - viz dále.

4. Jiné delikty

O jiné počítačové nebo podobné trestné činnosti v době sálových počítačů prakticky nelze hovořit, protože komunikace byly v nepřetržitém kolapsu a ty, které fungovaly, byly přísně střeženy. Co nebylo povoleno, to bylo zakázáno nebo přinejmenším netolerováno a netrpěno. *Distanční trestná činnost* páchaná na dálku prostřednictvím telekomunikací byla zcela nerealizovatelná - snad s výjimkou zasílání výhružných či pomlouvajících dopisů.

III. Nová doba

Česká republika je jedním ze států, vzniklých v návaznosti na mohutné společensko-politické změny na počátku 90. let tohoto století ve střední a východní Evropě rozdělením bývalého Československa. Jedním z nejtypičtějších parametrů posledních několika let jsou především obrovské změny v oblasti hospodářství a ekonomiky. Ve světě nesrovnatelný proces privatizace, a to jak do srovnání relativní velikosti a rychlosti. Kupónová privatizace se přes všechny problémy stála světovým unikátem. Rychlost změn, zasahujících všechny společenské oblasti, je řádově vyšší než ve standardních ekonomikách. Značným problémem je pak udržet krok v těch částech, které jsou vždy v pozici reagující na společenský vývoj, resp. reagující na nedostatky vzniklé prázdnými místy v legislativě. (Nutno ovšem poznamenat, že dosti často používají pracovníci orgánů činných v trestním řízení argumentaci „špatná legislativa“ v případech, kdy se jim nechce pouštět do obtížného případu odehrávajícího se pro ně v neznámém prostředí moderních technologií, přičemž vidina získané „čárky“ je velmi nejistá.)

Obdobný akcelerující vývoj zaznamenal v ČR i vývoj kriminality, a to zejména hospodářské, ponejvíce podvody. Index nárůstu stíhaných osob v letech 1990 - 1995 činí cca 150 %, přičemž největší dynamiku nárůstu vykazuje hospodářská trestná činnost. Jsou to především majetková kriminalita v „klasické“ podobě (krádeže, zpronevěry a podvody), jednak její nové formy, vyplývající z politických a ekonomických změn (pojišťovací podvody; bankovní kriminalita - opět zejména podvody, pašování, krácení daní a podobných dávek; privatizační podvody). Současně se objevily české i mezinárodní zločinecké skupiny se všemi prvky organizovaného zločinu tak, jak jsme je doposud znali pouze z vyspělých zahraničních států (s aktivitami typu prostituce, drogy, praní špinavých peněz, vydírání, pašování apod.). I když absolutní čísla nepřevyšují svojí hodnotou údaje např. ze států západní Evropy, vnímá čs. veřejnost tyto údaje velmi citlivě - *viz tabulka č. 2*.

Kritérium	1	1	1	1	1	1	1	1
	9	9	9	9	9	9	9	9
	8	9	9	9	9	9	9	9
	9	0	1	2	3	4	5	6
Počet	6	5	6	6	8	8	1	1
stíhaných	5	5	3	6	2	5	0	0
osob celkem	9	3	1	5	5	9	8	9
v ČR	5	1	9	6	7	2	6	2
	7	7	4	5	5	9	8	0
							0	4
Počet	4	2	4	4	5	6	8	8
obžalovanýc	5	6	4	8	7	5	4	5

h osob celkem v ČR	8 2 3	3 4 1	1 1 4	5 5 6	9 1 7	1 3 9	0 6 6	3 4 7
Počet odsouzených osob celkem v ČR	5 7 7 4 3	1 8 8 7 1	2 7 9 6 4	3 1 0 3 2	3 5 1 5 7	5 1 9 3 1	5 4 9 5 7	5 7 9 7 4
Z toho podle § 125 stíháno/obža lováno odsouzeno	4 9 8 1	3 9 1 9	1 1 2 8	1 3 / 9 / 5	4 3 / 2 9 / 1 0	3 5 / 1 4 / 1 9	4 8 / 2 8 / 1 7	7 1 / 4 4 / 1 6
Z toho podle § 152 stíháno/obža lováno odsouzeno	0	0	0	3 8 2 / 3 0 6 / 2 3 6	1 5 4 / 1 2 5 / 1 2 5	1 6 6 / 1 2 5 / 1 3 2	1 8 1 / 1 5 8 / 1 2 1	1 5 9 / 1 2 5 / 8 2
Z toho podle § 178 stíháno/obža lováno odsouzeno	-	-	-	0	0	2 / 0 / 0	1 / 1 / 4	6 / 4 / 4
Z toho podle § 250 stíháno/obža lováno odsouzeno	-	-	-	3 4 6 6 / 2 2 5 3 / 1 0 1 6	4 8 7 3 / 3 0 9 6 / 1 3 3 5	5 1 0 4 / 3 4 5 8 / 2 0 7 3	7 3 3 8 / 5 8 4 2 / 2 8 2 7	7 5 2 9 / 6 1 1 2 / 3 5 0 0

Z toho podle § 250a stíháno/obža lováno odsouzeno	-	-	-	90/65/4	246/190/48	63/38/50	17/12/9	14/9/11
Z toho podle § 257a stíháno/obža lováno odsouzeno	-	-	-	0	1/1/0	4/4/0	4/2/0	6/6/1

Jelikož neexistuje speciální statistické sledování trestné činnosti s prvkem počítače, lze pouze při výskytu skutkových podstat podle § 257a usuzovat na opravdu počítačovou trestnou činnost, zatímco další dvě skupiny (§ 152, § 178, § 250 a § 250a), kde se počítače stále více vyskytují, jsou prakticky nerozkódovatelné. Přesto zde můžeme vysledovat řadu trendů, z nichž jeden není velmi povzbuzující: snižující se počet pachatelů skutečně odsouzených za spáchání trestného činu podle ust. § 257a (markantní pokles jednak absolutně, jednak relativně oproti počtu obviněných a obžalovaných). Naopak počet stíhaných i odsouzených osob, které nakládaly s osobními daty v rozporu se zákonem (§ 178), stále roste.

Teprve dva další technologické zlomy v oblasti počítačových systémů (společně s kontinuálně se vyvíjejícími prakticky všemi technologickými možnostmi počítačů) umožnily jejich masivní využívání a tudíž i neméně masivní trestnou činnost s počítači spojenou. *Nová doba počítačového zločinu se datuje dvěma zásadními momenty: 1. nástupem osobních počítačů, 2. vznikem počítačových sítí a vzdáleného přístupu k počítačům.* Počítač se z výjimečného a chráněného prostředí klimatizovaných sálů s úzkým okruhem obsluhy dostal k uživatelům a tedy i ke zločincům. Tím se změnily i kriminogenní podmínky, modus operandi, typy pachatelů a obětí a další základní charakteristiky trestné činnosti nějakým způsobem spojené s počítači.

Celkově můžeme říci, že na přelomu let 1991 - 1992 v rámci tehdejší hektické právní doby došlo k velmi žádoucímu zařazení nových skutkových podstat do trestního zákona, a to včetně skutkových podstat souvisejících s počítačovou kriminalitou. Jsou to ustanovení § 257a - Poškození a zneužití záznamu na nosiči informací a § 178 - Neoprávněné nakládání s osobními údaji (jakož i nepočítačový, nicméně v souvislosti s využitím počítače se vysoce vyskytující § 250a - nyní § 250c). Ukázalo se to velmi prorockým , protože od té doby se datují i největší podvody spáchané prostředky výpočetní techniky v českých bankách. U bankovní kriminality bych se rád zastavil podrobněji, protože vývoj v této oblasti je dosti typický.

1. Podvody a padělky

Nové technologie vytvořily živnou půdu pro podvodníky, kteří začali využívat počítačů pro „klasickou“ trestnou činnost, nyní ovšem snáze proveditelnou. Hlavní oblastí, která představuje těžiště hospodářské trestné činnosti v ČR, jsou podvody. Klasické podvody (§ 250 - *„Kdo ke škodě cizího majetku sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti,...“)* byly nyní zdokonaleny pomocí počítačů, případně se objevily zcela nové druhy podvodů.

Sjednocujícím kritériem takovýchto jednání je vždy více méně *využití něčího omylu ve svůj prospěch*. Psychologická stránka vztahu počítač - člověk byla již několikrát popsána (např. [13], [15], [33] apod.), a proto bych jenom shrnul. Na rozdíl od klasických manipulací s „papírovými“ doklady má manipulace s počítačovými daty pro pachatele několik výhod:

1. vymazání či přemazání údaje na magnetickém médiu je podstatně snazší a nezanechává prakticky žádné stopy,

2. člověk (kontrolor, zákazník apod.) z psychologického hlediska považuje výsledky z počítače za a priori správné a více jim (byť podvědomě) důvěřuje.

Tento druhý aspekt počítačové kriminality má za následek vysokou úspěšnost trestných činů páchaných za využití výpočetní techniky. Právě vysoká důvěryhodnost výstupů z počítače je základním předpokladem úspěšného podvodníka. A není nic jednoduššího, než si ji tímto způsobem vylepšit. (Kdo z nás bude přepočítávat delší sloupec čísel sečtený počítačem nebo jen obyčejnou kalkulačkou s páskou?) Tento princip bezmezné důvěry ostatně zvýhodňuje jakékoliv manipulace s počítači a vším, co s nimi souvisí.

Kromě toho se zde objevují další aspekty podmiňující úspěchy počítačových zločinců:

3. vysoká kvalifikace pachatelů tohoto druhu trestné činnosti [38];

4. obtížná kontrola toho, co se odehrává ve výpočetním systému [39];

5. lehkost provádění operací s počítačovými daty oproti reálnému životu [9]; ukrást někomu z kapsy peněženku je výrazně obtížnější, než napsat příkazový řádek na počítači - alespoň pro kvalifikovaného programátora.

Psychologickému profilu pachatelů počítačových zločinů by měla být v kriminologických výzkumech věnována pozornost; v České republice tomu zatím tak není. Jedinou „vlaštovkou“ zahrnující i problematiku tohoto typu je výzkum uskutečněný katedrou kriminalistiky Policejní akademie ČR [27].

1. 1 Padělky

V praxi zločinců se například velmi osvědčily grafické počítačové systémy pro elektronickou sazbu a grafickou úpravu publikací, tzv. Desk Top Publishing. S jejich pomocí zhotovovali

pachatelé v několika rozsáhlých sítích obchodníků s kradenými automobily falešné technické průkazy a jiné doklady. Byly použity i pro zhotovení falešných cenných papírů a jiných bankovních dokumentů.

Změnit data lze buď úpravou dokladů, ze kterých jsou data pořizována, dále jejich úpravou na médiu, na němž jsou uložena, rovněž přímo při výpočtu v počítači a konečně na výstupní sestavě. Z technického hlediska je nejobtížnější provést změnu na již vytištěné sestavě, pokud je ale sestava rovněž ukládána na magnetické medium, není nic jednoduššího. Pro méně kvalifikované pracovníky je nejčastější formou defraudace změnou vstupních dokladů (resp. pořízení jiných dat do počítače). Pracovník, který na počítači přímo zpracovává svoji agendu - ať už na osobním počítači nebo na terminálu k velkému počítači, může prakticky libovolně měnit data před zpracováním, při něm a po něm. Musí samozřejmě nějakým způsobem ale „ošetřit“ ostatní informační soustavu firmy, s níž je propojen logickými vazbami.

Nejnovější druhy padělků se rekrutují z padělaných karet: telefonních, kreditních (úvěrových), debetních (platebních) apod. [40], čemuž odpovídá i dosti nové ust. § 249b TrZ - Neoprávněné držení platební karty.[5] Zvýšená společenská nebezpečnost tohoto druhu trestné činnosti si vynutila zařazení speciální kvalifikace k § 249 TrZ.[6] Záměr zákonodárce reagovat na novou, silně se rozmáhající trestnou činnost a postihnout tak i jiné formy jednání ve vztahu k platební kartě je zřejmý, otázkou je, nakolik je zvolená formulace šťastná. Uvedené ustanovení postihuje pachatele, který si jakýmkoliv neoprávněným způsobem (krádež, podvod, ale zřejmě i nálezem, pokud si kartu i nadále ponechá, nebo formou podílnictví apod.) opatří platební kartu. Tím se tato norma stává speciální úpravou ve vztahu k obecným majetkovým trestným činům. Bude použita všude tam, kde nebude možno pachateli prokázat, že zmocnění se karty bylo přípravou ke spáchání jiného majetkového trestného činu, tedy např. že pachatel hodlal v budoucnu kartu použít k nákupu zboží.

Právní úpravu týkající se padělků platebních karet najdeme i v § 27 zákona č. 200/1990 Sb. ve znění pozdějších předpisů (přestupkového zákona, dále jen PřZ) - Přestupky na úseku financí a měny. [7]

V kontextu ust. § 249b TrZ a § 27 PřZ zde dochází k jisté dualitě, která může způsobit komplikace při posuzování konkrétního zneužití platební karty. Trestní zákon sankcionuje toho, kdo „si opatří“ platební kartu nebo její padělek, zatímco přestupkový zákon toho, kdo „zhotoví“ padělek. Potom zhotovitel padělku spáchal přestupek, ovšem za předpokladu, že věděl a vědět mohl, že zhotovuje padělek platební karty, naplnil by zřejmě i skutkovou podstatu pomoci podle § 10/1/c k § 249b TrZ a došlo by k faktické konzumpci přestupku. V případě, že by si padělek zhotovil sám pro sebe, jednalo by se nejprve o spáchání přestupku podle § 27 a následně, neboť by si padělek ponechal, naplnil by skutkovou podstatu § 249b (takže by pravděpodobně opět došlo ke konzumpci).

V souvislosti s platebními kartami je třeba uvést dvě poznámky:

1. podle literatury [42, str. 959] platební kartou není karta identifikační (pro vstup do objektu), členská (klubová), předplatní (telefonní) ani zákaznická (např. CCS); domnívám se, že pokud

předmět má funkci platební karty (použití karty CCS má za faktický důsledek provedení úhrady z účtu zákazníka), nelze je z ochrany podle tohoto ustanovení vyloučit;

2. současné platební karty již v mnoha případech obsahují magnetický kód nebo čip, umožňující výběr z peněžního automatu. Jsou tedy nosičem informace - přinejmenším osobního kódu, někdy i jiných informací (obvykle výše úvěru nebo limitu výběru). Pak ovšem by hrozila v trestním zákoně reálná konkurence dvou speciálních norem. V případě, že úmysl pachatele, který si neoprávněně opatřil magnetickou platební kartu, pokrýval i způsobení škody, minimálně odpovídající nákladům na zablokování výběrů z karty (což v případě karty platné i mimo území republiky nemusí být zanedbatelná částka) a vydání karty nové, ale i způsobení dalších výdajů (např. znemožněním využití slev z předložení karty vyplývajících), nepochybně se *zmocnil nosiče informací s úmyslem způsobit jinému škodu a tyto informace učinil pro majitele neupotřebitelnými.* V tom případě není podle mého názoru zcela jasné, zda by se jednalo o jednočinný souběh s ust. § 257a TrZ či nikoliv, neboť jej můžeme chápat jako druhý následek jednoho skutku (čímž by se mohlo jednat o jednočinný souběh nestejnorodý), ale stejně tak lze předpokládat, že ust. § 249b je speciálním ustanovením k § 257a.[8]

Analogii ochrany karet (zejména kreditních, debetních, ale i telefonních apod.) najdeme v právních předpisech všech vyspělých zemí, protože se staly samozřejmou součástí každodenního života; ještě více než počítače. Právní ochrana je řešena různě: např. 15. U.S.C. Commerce and Trade, Sec. 1644 „Fraudulent use of credit cards“, který zakazuje použití, pokus nebo spiknutí (podle naší terminologie spíše zorganizování zločinu) za účelem použití kreditních karet v transakcích vnitřního nebo zahraničního obchodu. Také zahrnuje transport karet, přijmutí nebo zatajení zboží a stvrzenek, jakož i opatření si peněz prostřednictvím karet. Toto ustanovení může být použito i při zasílání nebo výměně karet (zřejmě se myslí údajů o kartách) poštou nebo přes počítač. Podle [35] může být ochrana rozšířena na všechny typy kódů a čísel účtů použitých pro zboží a služby, např. počítačové uživatelské identifikace, hesla, čísla počítačových účtů, PINy, telefonní kreditní karty, kryptografické klíče apod. Podle názoru autora jde o značně extenzívní výklad, nicméně v rámci angloamerického common law není vyloučený, zejména vzhledem k relevantním ustanovením zákona č. 18. U.S.C. Crimes and Criminal Procedure.

Podle Model Penal Code (US), § 224.6 je trestným činem spojeným s kreditní kartou *zneužití karty*, čehož se dopustí ten, kdo užívá kreditní kartu pro účely získání zboží nebo služeb a je si vědom, že: 1. karta je odcizená nebo padělaná, nebo 2. karta byla odvolána nebo zrušena, nebo 3. z jakéhokoliv jiného důvodu je použití karty neoprávněné.

Podle zákona č. 18. U.S.C. Crimes and Criminal Procedure, Sec. 1029 „Fraud and related activity in connection with access devices“ jsou zakázány podvody a podobné aktivity umožňující napodobit přístupový prostředek jako je PIN, karta, číslo účtu a jiné druhy elektronické identifikace. (Sankce se pohybují od 10 000 USD a/nebo 10 let vězení pro uživatele těchto předmětů, přes 50 tis. USD nebo dvojnásobek škody a/nebo 15 let vězení pro výrobce a distributory, při opakovaném deliktu 100 tis. USD a/nebo až 20 let vězení. Jde o výrazně vyšší sankce oproti českému maximálnímu možnému odnětí svobody do 2 let nebo peněžitému trestu nebo propadnutí věci.)

Na rozdíl od našeho pojetí § 249b se právo USA vztahuje nejen na platební kartu nebo předmět schopný plnit její funkci (padělek), ale i na jednání směřující k zneužití: získání informací, jejich

poskytnutí jinému, výrobu a užívání zařízení umožňujících monitorovat nebo (HW, SW či jinak) modifikovat telekomunikační přístroje za účelem získání neautorizovaného přístupu k telekomunikačním službám apod.

1. 2 Bankovní počítačové podvody

Bankovní sektor ČR se zásadním způsobem vyvíjel od roku 1990 (zpočátku v podmínkách bývalého Československa). Z původních čtyř bank vzniklo postupně až na 50 bankovních ústavů a na čs. trh vstoupily první zahraniční banky. Tak, jak bylo zmíněno o vývoji celé společnosti, tak i bankovní systém prodělal a prodělává bouřlivý vývoj. Jevy, které řada bank v západní Evropě a USA poznávala v průběhu několika desítek let, proběhly a zřejmě řada z nich bude ještě probíhat, když ne v měsících, tak maximálně v letech. Rychlost změn, chybějící zkušenosti a nevyváženost trhu byla vedle zřejmě zjevných kriminálních činů příčinou krachu více než desítky menších českých bank.

V českém bankovním sektoru došlo v letech 1992 - 1999 celkem k devíti zveřejněným bankovním počítačovým zločinům [38], [41]. Všechny trestné činy spáchané pomocí počítače měly charakter *neoprávněné manipulace* s bankovními záznamy (účty, hlavní knihou, souborem převodních příkazů apod.) a byly kvalifikovány jako podvody podle ust. § 250 TrZ. Přestože ve všech případech se pachatelé dopustili současně trestného činu podle ust. § 257a, nebylo jim ve většině případů obvinění z tohoto trestného činu sděleno. Přitom souběh obou trestných činů je možný [15], [42].

Zdá-li se malé množství útoků, je zde nutno zdůraznit vysokou latenci tohoto druhu kriminality, potvrzovanou zahraničními zkušenostmi [41]. K oznámení nedochází příliš často, a to vzhledem ke skutečnosti, že některé banky řeší problém samy, resp. případ raději neřeší vůbec, nebo - a to tuším dosti často - delikt vůbec nezjistí. Utajování jsou motivována především snahou nezdiskreditovat pověst banky.

Situace od roku 1996 je tedy zatím relativně pozitivní, možná ovšem pouze zdánlivě. Podle informací dostupných autorovi byl každý rok oznámen orgánům činným v trestním řízení nejméně jeden trestný čin tohoto druhu: pokus o podvod za pomoci výpočetní techniky ve výši cca 70 mil. v UNION bance, dokonaný podvod provedený zásahem do informačního systému v bance CREDITANSTALT v objemu cca 1,5 mil. Kč, dokonaný podvod provedený zásahem do souboru převodních příkazů předávaných z První městské banky Praha do mezibankovního zúčtování v clearingu ČNB v objemu cca 20 mil. Kč, neoprávněný převod cca 15 mil. Kč v rámci úhrady faktur VZP. Zájem většiny odhalených pachatelů působících v bankovním sektoru se zaměřil spíše na úvěrové podvody, padělané dokumenty a nadhodnocené zástavy. Jiné případy zveřejněny nebyly; otázkou je, zda se nestaly, nebyly odhaleny nebo pouze byly utajeny vedením bank. (Podle zahraničních údajů je odhaleno velmi malé procento, dokonce až promile počítačových podvodů.)[9]

Jak je vidět, byla donedávna křivka bankovních počítačových „loupeží“ rostoucí - z čehož lze dovodit, že je možná rostoucí stále, ale pachatelé, ba dokonce samotná existence dokonaného trestného činu zůstávají neodhaleni. Svědčí to o skutečnosti, že banky stále více přecházejí na stále složitější počítačové zpracování,[10] i o tom, že tento způsob zpracování láká nepoctivce z řad bankovních zaměstnanců. Protože kromě bank existuje i řada dalších firem působících na finančním

trhu (pojišťovny, leasingové společnosti, obchodníci s cennými papíry apod.), ale obecně ještě více firem, kde jsou počítačově zpracovávány velké finanční převody nebo mnoho inkas (od energetických společností až po zásilkové služby), lze další nárůst této trestné činnosti v příštích letech dozajista očekávat. Na druhou stranu se věnují tyto instituce stále více obraně proti takovýmto útokům, takže je možné, že pachatelé dávají přednost „snazším“ cestám, jako jsou již zmíněné úvěrové podvody.

Domnívám se jednoznačně, že pro bankovní podvody - ať již počítačové nebo „ruční“ - je charakteristická vysoká *latence*, tj. skrytost. Napomáhají tomu charakteristicky prostředí: v obrovských objemech transakcí probíhajících nyní v českém bankovním světě se jednorázový „úlet“ snadněji schová, než tomu bylo dříve. Navíc klíčovou úlohu hrají znalosti pachatele o účtech, jejich stavu a operacích s nimi prováděných. Lze využít tzv. mrtvé účty, interní účty banky, úvěrové účty, vkladové účty a další. Stejně může být při velkém objemu transakcí úspěšná metoda „zdanění“ každé operace - např. odebíráním částky na 3. desetinném místě při úročení, zvýšením „poplatku“ při provádění příkazů, změnou kursu atd. Možností je mnoho.

Obrana proti tomuto skrytému okrádání spočívá především v zásadě „mít pořádek v bance a v jejím informačním systému“. Znamená to mít standardní pracovní postupy a dodržovat je, mít vnitřní kontrolní mechanismy, využívat interní a externí finanční audit, audit bankovních operací a bezpečnostní audit [43], [44].

1. 3 Letadla

Klasickým zástupcem tohoto „oboru“ je dnes již legendární případ počítačových finančních her. Již dříve známé „pyramidy“ neboli tzv. „letadla“ se pomocí počítačů znásobila do tisíců účastníků, protože inzeráty vábily slogany typu „Není třeba hledat následovníky, vše řízeno počítačem ...“ apod. Podstatou těchto her je přerozdělování finančních prostředků vložených „hráči“ do „hry“, a to částečně ve prospěch hráčů, částečně ve prospěch pořadatele. Nejedná se o žádnou formu podnikání ze strany hráčů, protože v tomto případě je jejich jedinou aktivitou přihláška a zaplacení vkladu, bez nutnosti shánět následovníky, „prodávat“ další přihlášky apod. Podle toho, v jakém pořadí jsou hráči zadáváni do programu počítače (přesně řečeno do databáze hráčů), je také určena priorita hráčů a tedy pravděpodobnost, že neskončí hru se ztrátou. Kolik bude vyhrávajících hráčů a jaké získají částky, je závislé na pravidlech konkrétní hry a na tom, zda pořadatel vůbec tato pravidla dodržel (většinou se tak nestalo a tím právě došlo k poškození hráčů).

V letech 1990-1991 se vynořilo v českých zemích několik desítek takových her, přičemž jejich organizátoři pocházeli většinou z Kyjova a okolí. Využívali prakticky stejného programového vybavení a velmi podobných pravidel, kdy koncovou výhru (okolo 150 tisíc Kč) získávalo průměrně 15-20 hráčů na prvních místech z cca 10 000 účastníků hry. Prakticky všichni organizátoři těchto her jsou nyní trestně stíháni pro podvod podle § 250 TrZ, kterého se měli dopustit tím, že v rozporu se zveřejněnými pravidly her předřadili na prvních 5-8 místech sebe, své příbuzné či známé, nemluvě o tom, že obvykle zde docházelo ještě k souběhu s další trestnou činností - krácením daně. Největší počet účastníků v jedné z těchto her činil přes dvacet tisíc lidí.

Na enormní výskyt těchto her reagoval zákonodárce vložením § 250a TrZ - Provozování nepoctivých her a sázek: „Kdo provozuje peněžní nebo jinou podobnou hru nebo sázku, jejíž

pravidla nezaručují rovné možnosti výhry všem účastníkům, bude potrestán odnětím svobody až na dvě léta nebo peněžitým trestem. Odnětím svobody na jeden rok až pět let bude pachatel potrestán, získá-li činem uvedeným v odstavci 1 značný prospěch.“, který právě uvedené jednání postihl. Pochopitelně nikoliv zpětně, takže pro skutky spáchané před touto novelou platí dřívější stanoviska Generálních prokuratur, federálního ministerstva financí a Správy pro vyšetřování Policie ČR, kdy trestnost vzniká pouze v případě, že pořadatel nedodržel před začátkem hry veřejně vyhlášená pravidla. Teprve od této novelizace k 1. 1. 1992 jde o jednoznačný trestný čin podle § 250a, kdy místo nutnosti zkoumat dodržení pravidel je třeba posuzovat, zda všichni hráči mají podle těchto pravidel stejné šance a předpoklady k výhře.[11] Jen na okraj poznamenávám, že podle mých informací se orgány činné v trestním řízení velmi obtížně vyrovnávají s třetí vlnou těchto „pyramid“, která se znovu začala šířit v letech 1998 - 1999 pod dokonalejším krytím různých „podnikatelských“ aktivit.

Bohužel musím také upozornit na zmatek v číslování, neboť novelou TrZ č. 253/1997 Sb. došlo k přečíslování § 250a na § 250c, což pravděpodobně ztíží práci s dotčeným ustanovením TrZ i s navazujícími informačními systémy, např. statistickými, a je pro mne dosti nepochopitelným zásahem do systematiky trestního zákona.

Zmínit se o tomto trestném činu v souvislosti s počítači je nutné především z věcného a procesního hlediska, neboť prakticky všichni organizátoři těchto letadel používali k organizování her počítače a v rámci těchto počítačů obvykle páchali další delikty zaměřené na zvýšení svého obohacení v podobě manipulací se záznamy v neprospěch „hráčů“ (§ 257a) nebo finančního úřadu (§ 125 - Zkreslování údajů o stavu hospodaření a jmění, donedávna ještě Zkreslování údajů hospodářské a obchodní evidence, § 148 - Zkrácení daně, poplatku a podobné povinné platby).

Právě geneze ust. § 125 ukazuje, jak se promítá technologický vývoj do ustanovení TrZ, ale současně jak zákonodárce tápe v momentech souvisejících s počítači. Stávající dikce ust. § 125[12] říká: „(1) Kdo nevede účetní knihy, zápisy nebo jiné doklady sloužící k přehledu o stavu hospodaření a majetku nebo k jejich kontrole, ač je k tomu podle zákona povinen, nebo kdo v takových účetních knihách, zápisech nebo jiných dokladech uvede nepravdivé nebo hrubě zkreslující údaje, nebo kdo takové účetní knihy, zápisy nebo jiné doklady zničí, poškodí, učiní neupotřebitelnými nebo zatají a ohrozí tak majetková práva jiného nebo včasné a řádné vyměření daně, bude potrestán odnětím svobody na šest měsíců až tři léta nebo zákazem činnosti nebo peněžitým trestem. (2) Stejně bude potrestán, kdo uvede nepravdivé nebo hrubě zkreslené údaje v podkladech sloužících pro zápis do obchodního rejstříku.“ Předchozí znění tohoto ustanovení se výslovně zabývalo počítači takto: „(1) Kdo v úmyslu zajistit sobě nebo jinému neoprávněné výhody uvede o závažných skutečnostech ve výkazu, hlášení, *vstupních údajích vkládaných do počítače* nebo v jiných podkladech sloužících ke kontrole hospodaření nepravdivé nebo hrubě zkreslené údaje, nebo kdo uvede nepravdivé údaje v podkladech pro zápis do obchodního rejstříku, bude potrestán odnětím svobody na šest měsíců až tři léta nebo zákazem činnosti nebo peněžitým trestem. (2) Stejně bude potrestán, kdo v úmyslu uvedeném v odstavci 1 a) *učiní zásah do technického nebo programového vybavení počítače,* nebo b) podklady uvedené v odstavci 1 zničí, poškodí, učiní neupotřebitelnými, zatají nebo nevede.“ Původní znění § 125 o hardware nebo software vůbec nehovořilo (a samozřejmě celkově bylo zaměřeno na způsob socialistického podnikání): „Narušování řízení, plánování a kontroly národního hospodářství: Odpovědný hospodářský pracovník, který v úmyslu zajistit státní, družstevní nebo jiné socialistické organizaci

nebo její složce neoprávněné výhody uvede ve výkazu nebo hlášení sloužících k řízení, plánování nebo kontrole národního hospodářství, anebo ke stanovení cen o závažných skutečnostech nepravdivé nebo hrubě zkreslené údaje, bude potrestán odnětím svobody až na dvě léta nebo nápravným opatřením nebo zákazem činnosti nebo peněžitým trestem.“

Není mi zcela jasné, proč byla opuštěna ta část skutkové podstaty, kde se původně hovořilo ve 2. odstavci § 125 o zásahu do technického nebo programového vybavení počítače; pravděpodobně pro překrývání se s ust. § 257a, kde je definován v odst. 1 písm. c) způsob útoku stejně. Zde je ale sankce limitována odnětím svobody pouze až na jeden rok, takže - nebude-li výkladem stávající dikce § 125 odst. 1 zahrnut i obsah informačních systémů v počítači podnikatele, dochází tím ke zmírnění sankcí v tomto společensky vysoce nebezpečném jednání.

2. Porušování autorských práv

Nelegální užívání počítačů - resp. jejich hardware - bylo rychle dohnáno stejně nelegálním užíváním programového vybavení - software. Jelikož do roku 1989 (a bohužel i po něm) stále přetrvávalo vševlastnické uvažování většiny spoluobčanů, nebyly tyto aspekty dlouho ve zřeteli zájmu orgánů činných v trestním řízení. Rovněž nelegální užívání počítačů jakožto takových se stalo ještě skrytějším, protože co kdo dělal na svém osobním počítači, se dalo sledovat dosti obtížně.

„Uvědomění si“ samotné existence nehmotných statků je spojeno až s pozdější porevoluční dobou, kdy se duševní vlastnictví objevuje jako nehmotný majetek v obchodním majetku společností, v daňových zákonech, v novelizovaných zákonech na ochranu duševního vlastnictví a jako předmět obchodních vztahů i soudních sporů [20], [23], [50]. Od té doby je stále větší pozornost věnována i ochraně průmyslových práv, autorských práv a práv jim podobných (mj. i v důsledku intenzívnějších mezinárodních hospodářských vztahů). Dva druhy duševního vlastnictví - oba spadající pod ochranu autorským zákonem[13] (dále také jen AutZ) - se staly masivním předmětem útoku pachatelů: *audiovizuální nahrávky a počítačové programy.*

Nelegální užívání software prošlo intenzívním nárůstem, kdy se hovořilo až o 80 % nelegálně užívaného programového vybavení. Současná situace není tak dramatická, ale podle odhadů (byť ze strany výrobců a distributorů software) je každý druhý počítačový program užíván v ČR nelegálně. Z jednotlivých způsobů neoprávněných zásahů do práva autorského tak, jak je uvádí Telec v [25], jsou nejčastější v souvislosti s programy počítačů:

- • osobování si autorství nebo spoluautorství cizího díla (nejčastěji v souvislosti s díly vtyvořenými ke splnění povinností vyplývajících z pracovního poměru nebo dodanými externím autorem);
- • neuvedení nebo nesprávné uvedení autora (časté jak u „klasických“ děl - fotografií, ale i u software);
- • změna díla bez svolení autora (zásah do díla je právě v oblasti software nejčastějším deliktem);
- • užití díla bez svolení autora (vztahuje se jak na užití u koncového uživatele, tak na distribuci díla, opět typické pro audiovizuální nahrávky a počítačové programy);
- • nezaplacení autorské odměny za užití díla.

V praxi jsou realizovány delikty například takto:

- • *Velmi častý je případ, kdy programátor užívá licenční programové vybavení patřící zaměstnavateli pro svoje soukromé podnikání.* (Proč by si pachatel pořizoval nákladné programové vybavení, když je může okopírovat ve firmě, kde pracuje, a doma používat - ať už pro zábavu, vzdělávání nebo výdělečnou činnost.)
- • Běžné jsou *zásahy do programů jinými osobami,* další přepracovávání těchto programů a následně jejich užívání (případně včetně distribuce dalším subjektům).
- • *Společensky velmi nebezpečné je jednání řady firem, kde bylo zcela vědomě zakoupeno programové vybavení pouze jedenkrát nebo vůbec a rozkopírováno na více počítačů a tam používáno k podnikání.*[14]
- • Kromě toho se vyskytují i případy výroby *padělků* softwarových produktů - významný byl tzv. karlovarský případ, kde byla odhalena „továrna“ na výrobu padělaných produktů firmy Microsoft v objemu desítek tisíc kusů.
- • Stále jsou časté *spory o autorská práva*, resp. především o nároky z nich uplatňované mezi programátory a jejich zaměstnavateli. Podle mnoha osobních zkušeností autora jde o spory prakticky průřezové celým právním řádem, protože většinou začínají jako pracovněprávní, pokračují jako občanskoprávní a mnohdy končí jako trestněprávní, jelikož obě strany se v důsledku těchto sporů dopouštějí postupně různých protiprávních jednání (poškozování pověsti zúčastněných, zadržování mezd, neoprávněné výpovědi, znepřístupnění dat zaměstnavatele atd.).

Podle názoru autora požívá většina počítačových programů ochrany podle autorského zákona [45]. (Nelze souhlasit se stanoviskem uveřejněným v [25, s. 57-58], že „legální podmínky pro autorskoprávní ochranu počítačových programů českým AutZ může v důsledku své povahy a povahy práva autorského splnit jen malé procento programů“.) Na druhou stranu nelze a priori předpokládat, že každý program požívá ochrany jakožto autorské dílo tak, jak je tomu v některých právních úpravách jiných zemí, kde je uzákoněna generální ochrana počítačových programů právem autorským. Není nicméně předmětem této práce, aby hodnotila de lege lata či dokonce de lege ferenda autorskoprávní ochranu počítačových programů.[15] Je zaměřena na informační a počítačovou kriminalitu, kde tzv. „softwarové pirátství“, jak se také nepříliš vhodně porušování autorských práv říká, představuje pouze jednu, nikoliv na prvním místě stojící oblast.

K teoretickým problémům AutZ v souvislosti s informatikou uvádím pouze některé z otázek, jejichž vyřešení je v souvislosti s počítačovými programy a jejich příslušenstvím žádoucí:

- • generální versus speciální ochrana počítačových programů podle AutZ;
- • samotná koncepce AutZ jako speciální právní úpravy versus začlenění autorskoprávní ochrany do ObčZ;
- • ochrana přípravné a doprovodné dokumentace k počítačovému programu;
- • charakter některých počítačových programů z hlediska § 2 odst. 1, příp. § 6 AutZ (jde o audiovizuální díla - počítačové hry, multimediální projekty apod.);
- • sjednocování ochrany autorských děl v rámci ES [51];
- • ochrana databází [52];

• práva k počítačovým programům vytvořeným ke splnění povinností vyplývajících z pracovního poměru a jejich vykonávání apod.

K pojmovým znakům počítačových programů jako autorských děl stále probíhá obsáhlá diskuse a v důsledku toho vzniká i bohatá literatura, z níž uvádím zejména [19], [21], [22], [25] atd. K novele autorského zákona č. 86/1996 Sb. zejména [25], dále kriticky [53] až [55] a zejména [76].

Z hlediska trestněprávních aspektů jsou významná především následující ustanovení AutZ ve vztahu k počítačovým programům: § 2, odst. 1 - Dílo; § 12 - Osobní a majetková práva; § 14, 15 - Užití díla; § 17 - Zaměstnanecká díla.

Jak vyplývá z výše uvedeného, autorskoprávní ochrana se vztahuje na osobní práva autorova i neoprávněné nakládání s dílem, přičemž u software je posuzování konkrétních případů nakládání s programy komplikováno ne zcela jednoznačnými ust. § 15 odst. 5 a 6 AutZ - viz kritické zhodnocení Telece [25], Smejkala [54], [55] a Vlčka [56]. V každém případě se i v rámci nakládání tímto způsobem s programem musí držet jeho oprávněný uživatel dobrých mravů, jak je velmi vhodně uvedeno v [25]. Dalším zdrojem problémů je výklad § 17 odst. 5 AutZ, kde se názory jednotlivých skupin expertů nejvíce odlišují [25] a [57] versus [54], [55], [56].

Trestní postih pro porušování autorského práva riskuje ten, kdo programy pirátsky šíří, ale i ten, kdo takové programy užívá. Programům jako autorským dílům poskytuje jednak ochranu autorský zákon jako takový - § 32, s případnou aplikací ust. ObčZ o náhradě škody, příp. právu na vydání předmětu bezdůvodného obohacení, a také trestní zákon ve svém ustanovení § 152 - Porušování autorského práva: *„Kdo s dílem, které je předmětem ochrany podle práva autorského*, nebo s výkonem výkonného umělce, zvukovým či obrazovým záznamem nebo rozhlasovým či televizním pořadem, které jsou předmětem práva příbuzného právu autorskému, neoprávněně nakládá způsobem, který přísluší autoru, výkonnému umělci, výrobci zvukového či obrazového záznamu, rozhlasové či televizní organizaci nebo jinému nositeli těchto práv, anebo kdo jinak tato práva porušuje, bude potrestán odnětím svobody až na dvě léta nebo peněžitým trestem nebo propadnutím věci.“

Podle tohoto ustanovení trestního zákona budou zřejmě stíhány jen nejzávažnější případy úmyslného porušování autorských práv jiného, u programů zejména při kopírování (rozmnožování) ve velkém na trh, pro další šíření, při provádění změn v programu, kterými má být přivlastněno autorství s možností s programem dále nakládat, při zahrnutí programu nebo jeho částí do programu cizího apod., tedy vše, co se týká autorství k dílu, nakládání s ním včetně jeho užití a možného zveřejnění, provádění změn bez souhlasu autora, šíření díla. Vzhledem k subjektivní stránce trestného činu (z hlediska úmyslu pachatele) musíme také předpokládat pachatelovu vědomost týkající se rozsahu jeho útoku na autorská práva poškozeného. Toto ustanovení nemá nedbalostní variantu, tudíž se lze dopustit porušování cizích autorských práv pouze úmyslně. Jedná se ovšem o trestněprávní normu s blanketní dispozicí (ignorantia iuris nocet - neznalost zákona neomlouvá), takže pachatel v případě právního omylu bude trestně odpovědný.

Sama formulace § 152 TrZ předpokládá, že nepůjde o ojedinělý útok na program, ale o případy, kdy jde o porušování s vážnějšími následky, kdy budou - buď samostatně, anebo paralelně s občanskoprávní ochranou - namístě prostředky trestněprávní. Je třeba vycházet ze zásad trestního

práva hmotného: základním principem je, že trestným činem je pro společnost nebezpečný čin, jehož znaky jsou uvedeny v trestním zákoně.[16] K trestnosti činu je třeba úmyslného zavinění, nestanoví-li tento zákon výslovně, že postačí zavinění z nedbalosti.[17] Pro posouzení nebezpečnosti trestného činu jsou zvažovány veškeré okolnosti, neboť stupeň nebezpečnosti činu pro společnost je určován zejména významem chráněného zájmu, který byl činem dotčen, způsobem provedení činu a jeho následky, okolnostmi, za kterých byl čin spáchán, osobou pachatele, mírou jeho zavinění a jeho pohnutkou.[18] A konečně si řekněme, že čin, jehož stupeň nebezpečnosti pro společnost je nepatrný, není trestným činem, i když jinak vykazuje znaky trestného činu.[19] Není tedy zřejmě trestným činem stíhatelným podle tohoto ustanovení případ, kdy si okopíruji Text602 ve verzi z roku 1994, abych doma na svém PC psal dopisy příbuzným. Na druhou stranu sama instalace počítačových programů (například ve velkém, tj. na mnoho počítačů v podnikatelském subjektu) již podle mého názoru zakládá skutkovou podstatu definovanou jako *„neoprávněně nakládá způsobem, který přísluší autoru nebo jinak tato práva porušuje“*, aniž by bylo třeba dokazovat, zda a v jakém rozsahu byly používány.[20]

Porušování autorského práva nespadá mezi zcela typická jednání zahrnovaná do počítačové kriminality, na druhou stranu je s ní úzce propojeno. Zda budeme porušování autorského práva zahrnovat do počítačové kriminality, to ovšem záleží na její definici a na tom, co vše jí chápeme : pokud to bude tzv. počítačové pirátství, pod nímž rozumíme právě útoky proti autorskému dílu v podobě nelegálního nakládání s programy (nelegální kopírování, šíření, plagiátorství programů) k získání prospěchu pro sebe nebo jiného, tj. s komerčním využitím, můžeme i útoky postihované § 152 TrZ považovat za součást počítačové kriminality.

K porušování autorských práv podle § 152 TrZ dochází většinou tímto možným způsobem:

1. provozem programu na více počítačích než bylo ve smlouvě dohodnuto (nebo zcela beze smlouvy),

2. zasahováním do programu, prováděním jeho změn a úprav nad rámec daný platným - a dosti benevolentním - zněním AutZ,

3. poskytnutím tohoto programu jiným osobám (nejčastěji okopírováním, ale také výrobou a prodejem plagiátů),

4. jako nový projev porušování autorských práv v počítačovém prostředí lze posuzovat zasahování do WWW - stránek hackery nebo jejich kopírování do jiných autorských děl.

Pro naplnění skutkové podstaty trestného činu podle § 152 TrZ tedy stačí, dojde-li k jednomu z výše uvedených skutků, přičemž - podle dikce § 152 - pro zahájení trestního stíhání není podstatné stanovení výše škody nebo neoprávněného majetkového prospěchu. Toto stanovení může být pouze dalším důkazem předloženým státním zástupcem soudu za účelem stanovení společenské nebezpečnosti tohoto trestného činu.

Toto programové pirátství je u nás (a obecně ve většině postkomunistických či z jiných důvodů rozvojových zemí) stále považováno za zcela normální způsob získání potřebného programu a je často bagatelizováno nejen veřejností, ale i některými orgány činnými v trestním řízení.[21]

Novela AutZ z roku 1996 zařadila do textu zákona nové ustanovení § 32a, které bylo také předmětem obsáhlé diskuse: „Stejné nároky jako při ohrožení nebo porušení autorských práv příslušejí autorovi vůči osobám, které vyrábějí, uvádějí do oběhu nebo využívají pro dosažení majetkového prospěchu pomůcky výlučně zamýšlené k odstranění, vyřazení z provozu nebo omezení funkčnosti technických zařízení nebo jiných prostředků, použitých k ochraně jeho díla před neoprávněným užitím.“ Ve své podstatě jde o technické nebo programové prostředky, umožňující používat chráněné programy; známou variantou jsou hardlocky (klíče zasouvané do některého z portů počítače) umožňující pracovat s dražšími programy jako AutoCAD nebo JURIX. Podle literatury [25], [60], [61] jde o nekalosoutěžní jednání s objektivní odpovědností toho, kdo pomůcky vyrábí, uvádí do oběhu nebo používá. Problém může nastat v okamžiku, kdy bude zkoumáno naplnění druhého podstatného znaku, tj. „výlučně zamýšlené“. Dovedu si představit zkomplikování situace, kdy bude program kromě dešifrování přístupu také hrát písničky nebo počítat kondiciogramy.

Závěrem k otázkám spojeným s trestnou činností spočívající v porušování autorských práv je třeba se zmínit o ochraně informačních systémů a počítačových databází autorskoprávním způsobem a tedy následně i podle ust. § 152 TrZ.

Otázka definice informačního systému (IS) není naprosto triviální. Přinejmenším můžeme chápat IS v širším a v užším pojetí. V užším pojetí jde o nějakou množinu dat a prostředky, které s těmito daty manipulují (tedy v podstatě databáze + program nebo kartotéka + ruce). V širším pojetí je IS sestaven z technických, programových, datových, personálních a dalších složek. IS můžeme chápat pouze jako černou skříňku, na jejímž vstupu a výstupu jsou informace, bez ohledu na to, jak je realizován vnitřek této černé skříňky. Tomuto pojetí odpovídá definice jako např. *„systém, jehož prvky mají funkce transformace informací“* [58], *„systém, v němž vazby mezi prvky se chápou jako informace (data), resp. směry jejich toků a jednotlivé prvky jako místa vzniku, sběru, předzpracování, přenosu, uchování, zpracování, distribuce či zániku informací (dat); jeho účelem je tvorba a prezentace informací“* [59]. Nebo se zaměříme i na obsah této skříňky: „*Informačním systémem se rozumí funkční celek zabezpečující cílevědomé a systematické shromažďování, zpracovávání, uchovávání a zpřístupňování informací. Každý informační systém zahrnuje informační základnu, technické a programové prostředky, technologie a procedury a pracovníky.“* (§ 4 zák. č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech) nebo návrh definice formulovaný v [15]: „*Informační systém zahrnuje informační dokumenty, informační pracovníky a informační procesy. Informační dokumenty jsou nosiče informací, na nichž jsou zaznamenány tématické obsahy těchto informací. Informační procesy jsou všechny činnosti, jimiž se manipuluje s informacemi a vztahy mezi nimi.“* Právní otázky spojené s IS např. v souvislosti s výkonem veřejné správy (mj. vzhledem k jejich významu z hlediska konstitutivních a deklarativních aktů [62]) představují dnes v ČR „balík“ nedořešených nebo nejasných problémů.[22]

Informační systém bude tedy obvykle sestávat z komponent, z nichž některé mohou podléhat ochraně podle AutZ, jiné nikoliv. Kromě software jsou druhým „nejžhavějším“ kandidátem na

ochranu podle AutZ (zatím ovšem nikoliv v ČR) databáze. Vyplývá to ze směrnice ES o právní ochraně databází ze dne 11. 3. 1996 [52], která zahrnuje databáze do ochrany autorským právem s podmínkou splnění jediného pojmového znaku - aby byla databáze vlastním duševním výtvorem autora (v důsledku výběru nebo uspořádání). Podle [25] bychom mohli pohlížet na databáze jako na díla souborná podle § 4 AutZ, jednalo by se o uspořádání děl splňujících pojmové znaky podle AutZ nebo tvůrčí uspořádání netvůrčích prvků. Výklad nebude jednoduchý a ani jednoznačný, protože klíčovou otázkou bude míra tvůrčího přínosu autorova, podobně jako tomu je u jiných autorských děl.[23] Podle autora tohoto textu je u počítačových databází možné rozlišovat *strukturu databáze* (formální návrh obsahu a jeho uspořádání, obvykle v nějakém programovacím databázovém jazyku) a vlastní *obsah databáze* (data). Potom bychom mohli posuzovat zvlášť ochranu návrhu databáze, jako autorské dílo typu počítačového programu, a zvlášť ochranu jejího obsahu. V zhledem k citované směrnici ES je třeba předpokládat, že v rámci harmonizace práva dojde k začlenění databází do výčtu děl uvedených v § 2 AutZ. Návrh nového znění AutZ, byť je ve velmi „syrové“ podobě, předpokládá ochranu databází, jsou-li původní v tom smyslu, že jsou autorovým vlastním duševním výtvorem [76]. Nyní lze databáze trestněprávně chránit pouze z hlediska jejich záznamu na nosiči informací (podle ust. § 257a), nebo je chápat jako know-how a chránit jako obchodní tajemství podle ust. § 149 TrZ - Nekalá soutěž [42, s. 612-622], kdy by se mohlo jednat o porušování obchodního tajemství (viz ust. § 17 ObchZ).

3. Počítačové viry a ustanovení § 257a TrZ

Počítačovým zločinem, o kterém se ve sdělovacích prostředcích asi nejčastěji mluví a píše - i když si málokdo uvědomuje, že jde o trestnou činnost - je *infikování počítačovým virem.* Nemine snad týden, abychom nebyli varováni před spouštěním počítače v určitý den, kdy nově objevený virus by mohl zničit naše data a programy. Většina těchto informací jsou sice pouhé novinářské „kachny“ nebo zveličené informace, neplatí to ale obecně a v poslední době jsme se mohli nejen setkat s velmi nebezpečnými viry a tzv. makroviry, ale dokonce s dopadením a trestním stíháním jejich autora.[24]

Delikt související s počítačovým virem má *dvě fáze:* nejprve někdo napíše program, tedy vytvoří takový virus. Dokud jej chová jako v inkubátoru ve svém počítači, nemůžeme hovořit o dokonaném trestném činu. Pouze v případě, že by se nám podařilo prokázat, že pachatel skutečně se připravoval takto vytvořený virus použít k nějakému útoku, mohli bychom hovořit o přípravě.[25] V okamžiku, kdy ovšem tímto virem infikuje jakýkoliv nosič informací patřící druhé osobě (počítač, disketu apod.), domnívám se že zde dochází k naplnění skutkové podstaty trestného činu podle § 257a TrZ - Poškození a zneužití záznamu na nosiči informací.

Podobně je naplněním skutkové podstaty tohoto trestného činu jakékoliv jiné jednání osoby, která zneužije přístupu k nosiči informací a zde se nacházející informace zneužije nebo poškodí - například při průniku. (Poškozování WWW stránek hackery může být poškozením autorského díla, tedy porušováním autorských práv podle ust. § 152 TrZ, nicméně zcela nepochybně půjde o poškození záznamu na nosiči informací podle § 257a TrZ.)

Ustanovení § 257a bylo do TrZ zařazeno novelizací v roce 1991 jako jeden z prvních „počítačových“ deliktů. Přitom jeho aplikace je širší než pouze na prostředky výpočetní techniky,

alespoň dle názoru autora de lege lata, protože (jako u jiných nových skutkových podstat) zde je naprostá absence jakékoliv judikatury. Cituji: „Kdo v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch získá přístup k nosiči informací a

a) takových informací neoprávněně užije,
b) informace zničí, poškodí nebo učiní neupotřebitelnými, nebo
c) učiní zásah do technického nebo programového vybavení počítače,

bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti nebo peněžitým trestem nebo propadnutím věci.“

Objektem trestného činu je nejen hmotný substrát (nosič informací nebo počítač), ale i nehmotný obsah informací. Tím se zprostředkovaně chrání další zájmy a vztahy - např. projevy osobní povahy, obchodní tajemství, soukromí osob, autorská díla, státní tajemství apod. [42].

Ustanovení § 257a TrZ popisuje v zásadě (i když toliko ve vztahu k informacím) plným způsobem, co nedovoleného lze s daty dělat: *„neoprávněně užít, zničit, poškodit nebo učinit neupotřebitelnými“*. Při pozornějším studiu ustanovení § 257a TrZ je zjevná jistá nevyváženost tohoto ustanovení, která jej ale nijak neznehodnocuje. Zatímco písm. a) odst. 1 postihuje specifický způsob útoku na informaci - neoprávněné užití, v písm. b) je poněkud kasuisticky popsáno to, co pokud jde o programové vybavení je v písm. c) popsáno jediným pojmem, totiž „učiní zásah“. Pojem *„učinit zásah“* lze považovat za ekvivalentní všem třem dříve uvedeným pojmům. Kromě popsaných zásahů existuje jednání, které není postihnuto tímto ustanovením a o jehož postižitelnosti vůbec se vedou diskuse, totiž průnikářství neboli hackerství.

V rámci rozboru speciální úpravy postihující neoprávněné manipulace s daty je třeba připomenout, že na některá jednání dopadají za určitých okolností i postihy podle některých jiných ustanovení TrZ; jde např. o vyzvědačství (§ 105 TrZ), ohrožení utajované skutečnosti (§ 106 a 107 TrZ), nekalá soutěž (§ 149 TrZ) a pod. Taková jednání lze ale postihnout v rámci jednočinného souběhu s trestným činem podle § 257a a jejich detailní rozbor by nesouvisel s počítačovou problematikou.

Aby mohl být spáchán jakýkoliv útok na data, je nutné, aby k těmto datům získal pachatel přístup. Přitom sledujeme okruh případů, kdy jednání vůči datům je vedeno úmyslem - a to zlým úmyslem, společností neaprobovaným. Zákonodárce tento předpoklad vyslovuje formulací, *„kdo v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch“*. V praxi si pachatel především získává přístup do počítače nebo počítačové sítě a poté teprve realizuje konkrétní záměr, totiž útok na program nebo informace, případně oboje.

Tento praktický aspekt nezohledňuje nejšťastněji ustanovení § 257a TrZ; jako společnou podmínku trestnosti uvádí získání přístupu k *„nosiči informací“* s tím, že poté pod bodem c) navazuje *„učiní zásah do technického nebo programového vybavení počítače“*. Tedy jinak řečeno, poté co získá přístup k nosiči informací, zaútočí na vybavení počítače. Rozborem pojmů „počítač“ a „nosič informací“ můžeme dojít až k závěru, že norma je prakticky nesrozumitelná. Asi vyloučíme možnost, že by pro naplnění skutkové podstaty postačovalo získat přístup k jakémukoliv nosiči informací a poté zasáhnout do programu jiného počítače, i když ustanovení samo spojitost těchto

dvou prvků neupravuje. Je ale zřejmé, že byl míněn nosič informací umístěný v napadeném počítači. Větší problém ale je, že pokud automaticky nepovažujeme počítač za nosič informací, pak k tomu, aby pachatel učinil zásah do technického nebo programového vybavení počítače nepotřebuje vůbec získávat přístup k nosiči informací. Dokonce v případě speciálních počítačů nemusí takový počítač žádný nosič informací mít (s výjimkou operační paměti, kde je uloženo programové vybavení, které ale, vycházeje z dikce § 257a, považuje zákonodárce za něco jiného než informace). Podle názoru autora lze i operační paměť považovat za nosič informací, protože obsahuje jednak program, jednak data (byť obsah tohoto nosiče mizí při vypnutí počítače. Pokud by se soudní výklad (nepravděpodobně) přiklonil k tomu, že operační paměť není nosičem informace, přesto není vše ztraceno, neboť písm. c) praví *„učinil zásah do technického nebo programového vybavení počítače“,* přičemž operační paměť bezesporu technickým vybavením počítače je.

V praxi tedy uvedené ustanovení obstojí jedině za předpokladu premisy, kterou zákonodárce zřejmě přijal za vlastní, že každý počítač je také nosič informací a získáním přístupu k počítači získává pachatel za stejných podmínek a se stejným úmyslem přístup k nosiči informací. I když ve většině případů tato podmínka skutečně bude splněna, bylo by zřejmě vhodné při nejbližší novelizaci uvedené vnitřní rozpory odstranit.

Pokud jde o jednotlivé formy, v případě informací je neoprávněné užití zcela zřejmá činnost, která nepotřebuje sama o sobě hlubšího rozboru. Je nesporné, že tohoto trestného činu se lze dopustit v jednočinném souběhu s již uváděnými trestnými činy. Zvláště je ale třeba upozornit na trestný čin podle § 178 TrZ - Neoprávněné nakládání s osobními údaji.

V této souvislosti se znovu vynořuje problém spočívající v nejasnosti pojmu „*nosič informací“*. Ustanovení § 178 postihuje neoprávněné sdělení údajů o jiném, aniž by odlišovalo způsob uložení těchto údajů; pojem „*nosič informací“* je vztahován pouze k jeho elektronické verzi. Tím může dojít k poněkud kuriózní situaci, kdy dva pachatelé spáchají naprosto stejný trestný čin, spočívající v neoprávněném sdělení osobních údajů shromážděných v souvislosti s výkonem státní správy. Rozdíl bude pouze v tom, že jeden z pachatelů tyto údaje získá z počítače, tedy toho, co je považováno za *nosič informací,* zatímco na pracovišti druhého se v důsledku nedostatečného pokroku stejné údaje zapisovaly do bloku nebo ukládaly na papírové doklady. Při užívaném výkladu pojmů bude v prvním případě pachatel obviněn z jednočinného souběhu trestných činů dle § 178 a 257a TrZ, zatímco v druhém případě by přicházela v úvahu toliko právní kvalifikace dle § 178 TrZ.

Vzniká i otázka, zdali lze podle ustanovení § 257a TrZ postihnout jako neoprávněné užití i užití informací, které shromáždil ten, kdo je později šířil a do jehož vlastnictví tyto informace patří. Zákon zde uvádí jako podmínku naplnění skutkové podstaty trestného činu dle § 257a pouze úmysl způsobit jinému škodu nebo újmu, sobě získat neoprávněný prospěch, dále získání přístupu (přitom se nerozlišuje zda oprávněného či nikoliv) k nosiči informací a neoprávněné užití těchto informací. Neoprávněnost nelze chápat než jako protiprávní jednání z hlediska celého právního systému, tedy jako porušení kteréhokoliv ustanovení platného právního předpisu. Z tohoto rozboru nevyplývá nic, co by tuto interpretaci vylučovalo. Ve prospěch takového výkladu by svědčilo i znění § 178 odst. 2 TrZ, postihující obdobné jednání ve vztahu k osobním údajům, získaným „*v souvislosti s výkonem svého povolání, zaměstnání nebo funkce“*. Proti hovoří pouze představa důsledné realizace takovéhoto výkladu. Zatímco ustanovení § 178 odst. 2 TrZ omezuje postih za zveřejnění na *osobní*

údaje, získané pouze v souvislosti s *výkonem svého povolání, zaměstnání nebo funkce,* ustanovení § 257a pro naplnění skutkové podstaty požaduje z hlediska zveřejněných informací toliko *neoprávněnost.* Zákon ani nerozlišuje to, zda jde o informaci pravdivou či nikoliv. To by tedy znamenalo, že v případě jakéhokoliv tvrzení, působícího někomu škodu a užitého neoprávněně, např. v rozporu s ustanovením § 12 ObčZ, § 17-20, 45-47 a 50 ObchZ aj. by bylo nutno zkoumat, zda údaje nebyly získány z nosiče informací. Tento zcela náhodný fakt, navíc výrazně ovlivnitelný a obtížně prokazatelný, by byl jediným kritériem pro posouzení toho, zda byl spáchán trestný čin či nikoli.

Zničit, poškodit nebo učinit neupotřebitelným nosič informací je podle názoru uvedeného v [15] činnost, která se obsahově kryje se zásahem do programového vybavení, a lze tedy obě ustanovení analyzovat současně. Pojmy *„zničení“* a *„poškození“* jsou notorietami, přičemž půjde o konkrétní posouzení, k čemu v daném případě došlo. I zde přichází v úvahu celá řada trestných činů v jednočinném souběhu. Záleží pouze na tom, jaká data jsou poškozena nebo zničena. Závažnější poškození dat v počítačích řídících činnosti, při nichž jsou ohroženy životy a zdraví lidí, dopravní systémy, letecký provoz, nemocnice by např. mohlo být kvalifikováno jako *obecné ohrožení* (§ 179-180 TrZ), možná i poškozování a ohrožování provozu obecně prospěšného zařízení (podle § 182 a 184 TrZ).

Ve vztahu k ničení informací je třeba si také položit otázku, kdo všechno může být pachatelem. Při stejném zadání jako v předchozím případě je i velmi podobná odpověď. Jistě si lze představit společníka, který zničí informace o obchodních aktivitách své obchodní společnosti proto, aby se zvýhodnil vůči svým společníkům, nebo spíše proto, aby zakryl machinace, kterých se jako jednatel společnosti dopustil ke škodě této společnosti a tedy i společníků.[26] Ještě markantnější je případ podnikatele, fyzické osoby, který se pokusí vyhnout důsledkům konkursu zničením informací na jejich nosiči, tedy jejich vymazáním. Z hlediska ustanovení § 257a je zde vše požadované. Úmysl směřující ke způsobení škody jinému - věřitelům - a zničení informací. Třeba podotknout, že v tomto případě zákon dokonce ani nepožaduje neoprávněnost zničení informací a pro naplnění skutkové podstaty tedy postačuje pouhý úmysl způsobit škodu nebo získat neoprávněný prospěch.

Zákon požaduje splnění ještě jedné, zdánlivě samozřejmé podmínky: totiž *„získání přístupu k nosiči informací“*. I toto ustanovení není formulačně nejšťastnější, neboť navozuje představu, že pachatel již v době získání přístupu k nosiči informací má úmysl způsobit škodu nebo získat neoprávněný prospěch, přesněji, že s tímto úmyslem již získává přístup k nosiči. Důsledné lpění na této podmínce by v praxi dosti omezovalo použití ustanovení § 257a, neboť prokazovat po několika letech pracovního poměru pracovníkovi, že již v době, kdy se o pracovní poměr ucházel, měl úmysl jednou svému zaměstnavateli odcizit informace nebo zavirovat počítač, by bylo velmi obtížné. Rozhodně šťastnější by byla formulace *„Kdo poté, co získal přístup k počítači (nosiči informací), v úmyslu... atd. “*.

V souvislosti s uvedeným zněním tohoto ustanovení by mohlo být namítnuto, že jedním ze znaků skutkové podstaty je právě *„získání přístupu k nosiči informací“,* přičemž vlastník žádný přístup nezískává, neboť počítač vlastní a přístup vyplývá z jeho vlastnického práva. Této úvaze zjevně nelze přisvědčit, neboť zákonodárce nerozlišuje způsoby získání přístupu k nosiči informací, takže vlastnictví je také jedním z nich. Není také řečeno, že by potenciální pachatel musel získat přístup k

nosiči informací, který již informace obsahuje, nebo aby tyto informace byly do počítače uloženy poté co přístup získal a případně jím samým.

Jelikož *tento delikt nezná nedbalostní kvalifikaci*, nelze stíhat zaměstnance, jenž vložil zavirovanou disketu do počítačového systému svého zaměstnavatele, čímž došlo k vymazání obsahu pevného disku, ale lze stíhat pouze ty osoby, u nichž by úmysl byl prokázán (viz § 3/3 TrZ), maximálně pak ve výjimečných případech s přihlédnutím k ust. § 4, který praví mj. „*Trestný čin je spáchán úmyslně, jestliže pachatel... b) věděl, že svým jednáním může takové porušení nebo ohrožení způsobit, a pro případ, že je způsobí, byl s tím srozuměn.*" Ovšem při mých zkušenostech s odkládáním trestních oznámení a zastavováním trestního stíhání v podstatně významnějších případech zůstane tato úvaha pouze na úrovni teoretických publikací. Skutková podstata tohoto trestného činu a s tím související záležitosti nejsou zcela triviální.

Tento trestný čin je obvykle v jednočinném souběhu s jinými trestnými činy, kdy skutek kvalifikovaný podle tohoto ustanovení je pouze skutkem pomocným pro jiný delikt, zakládající hlavní úmysl pachatele - obvykle majetkový prospěch.

Obdobou tohoto ustanovení je několikrát již citovaný zák. č. 18. U.S.C., Sec. 1030 „Fraud and related activity in connection with computers" - viz příloha č. 1. Při zavirování prostřednictvím telekomunikací může přicházet v úvahu také aplikace zákona v Sec. 2510 „Wire and Electronic Communications Interception and Interception of Oral Communications".

4. Zneužívání osobních dat občanů a počítačová špionáž

S tím, jak stále více údajů je uloženo na magnetických médiích, *roste zájem zločinců o obsah těchto nosičů informací.* Těžiště jejich zájmu představují dnes zejména dvě oblasti:

a) osobní data občanů;
b) hospodářsky využitelné údaje.

4.1 Osobní data občanů

Ochrana osobních dat občanů je typickým požadavkem na zvýšenou ochranu osobnosti akcentovaným porevoluční dobou v ČR [63], jednak vzhledem k zásadní změně v chápání vztahů občan - stát (dané např. Listinou základních práv a svobod), jednak k celosvětovému trendu ochrany těchto dat a s tím souvisejícím mezinárodním ujednáním [64]. V jednotlivých západoevropských státech se datuje *první generace zákonů* na ochranu osobních dat ze sedmdesátých let, přičemž v osmdesátých letech došlo v těchto státech k vydání informačních zákonů tzv. *druhé generace,* které ochranu osobních údajů dále zdokonalují. Vyspělé státy EU dnes v návaznosti na poslední *Směrnici Evropského parlamentu a Rady č. 95/46/ES ze dne 24. října 1995 o ochraně jednotlivců se zřetelem na zpracování osobních dat a o volném pohybu takových dat* pracují na dalším zdokonalení těchto zákonů, na tzv. *třetí generaci.*

Český *zákon č. 256/1992 Sb., o ochraně osobních dat v informačních systémech,* byl schválen Federálním shromážděním ČSFR dne 29. dubna 1992 s účinností dnem 1. 6. 1992. Tento zákon je prvním uceleným právním předpisem, který definoval některé informatické pojmy a stanovil

základní pravidla pro nakládání s tzv. osobními údaji. Vychází z principů a požadavků daných Listinou základních práv a svobod, reaguje na doporučení Rady Evropy a Evropských společenství a přispívá tak do komplexního systému právních předpisů chránících lidská práva, který je u nás postupně vytvářen. V době projednávání tohoto zákona přitom již byl spáchán jeden ze známých a rozsáhlejších deliktů tohoto typu u nás, a to poskytnutí osobních dat občanů bývalým FMV obchodním společnostem; ovšem vzhledem k tehdejší absenci hmotněprávní úpravy byl nestíhatelný.

Zákon vymezuje některé pojmy, a to prakticky poprvé v českém právním systému (např. *Informace, Informační systém, Provozování informačního systému, Zpracování informace, Likvidace informace atd.). Zákon upravuje ochranu osobních údajů, zejména povinnosti související s ochranou informací při provozování informačního systému, který nakládá s osobními údaji a odpovědnost provozovatele informačního systému a dalších fyzických a právnických osob.* V § 3 zákona je uvedeno: „*informace, které se vztahují k určité osobě, jsou osobními údaji“.* Musí se jednat o informace tuto osobu jednoznačně identifikující. Takovým údajem může být i pouhá adresa osoby, bude-li se nacházet v určitém vybraném souboru adres - např. odběratelů elektrické energie. Jakmile jsou zaznamenány jakékoliv další osobní údaje, není již vůbec o čem diskutovat a dikce zákona je naplněna bezezbytku.

Ustanovení v § 16 říká, že „Provozovat informační systém, který nakládá s informacemi, které vypovídají o osobnosti a soukromí dotčené osoby, jejím rasovém původu, národnosti, politických postojích a členství v politických stranách a hnutích, vztahu k náboženství, o její trestné činnosti, zdraví, sexuálním životě a majetkových poměrech, lze pouze, stanoví-li tak zvláštní zákon, nebo se souhlasem žijící dotčené osoby, pokud je možné, aby tento projev vůle učinila. Jestliže nelze podmínku souhlasu splnit, lze s informacemi nakládat jen za předpokladu, že bude zachována lidská důstojnost, osobní čest, dobrá pověst a chráněno dobré jméno dotčené osoby.“[27]

Přitom dosti rozšířeným omylem navíc je, že se musí jednat pouze o počítačové informační systémy a počítačové databáze. Informační systém může být realizován i jiným způsobem (spis, kartotéka...), a i v tomto případě spadá do působnosti zákona č. 256/1992 Sb.

Ustanovení § 17 uvádí mezi povinnostmi provozovatele mj.: provozovat informační systém v souladu s účelem, pro který je systém zřízen; získávat informace rozsahem tomuto účelu přiměřené, zejména vystříhat se shromažďování nadbytečných údajů; ověřovat, zda informace, s nimiž informační systém nakládá, jsou přesné, a podle potřeby je aktualizovat, označit náležitým způsobem v informačním systému nepřesné nebo neověřené informace, neuchovávat nepravdivé informace; zamezit sdružování informací a informačních systémů sloužících k rozdílným účelům, pokud zvláštní zákon nestanoví jinak; získávat informace pro informační systémy náležitým způsobem; získávat informace pod krytím jiným účelem nebo jinou činností lze pouze, pokud tak stanoví zvláštní zákon; zajistit ochranu informací i celého systému před náhodným nebo neoprávněným zničením, náhodným poškozením, jakož i před neoprávněným přístupem nebo zpracováním; poskytnout jednou do roka bezplatně, nebo za přiměřenou úplatu kdykoli, každé dotčené osobě na požádání zprávu o informacích o ní uchovávaných v informačním systému, pokud zvláštní zákon nestanoví jinak apod.

Podle § 20 „V případě porušení povinností provozovatele uvedených v § 17 vzniká oprávněné fyzické osobě vůči provozovateli nárok na: a) zdržení se takového jednání, odstranění závadného stavu, vydání bezdůvodného obohacení tomu subjektu, na jehož úkor bylo toto obohacení získáno, a poskytnutí zadostiučinění tomu, jehož porušení povinností poškodilo, na náklady provozovatele, b) likvidaci informace; c) doplnění informace, jedná-li se o informaci, která byla do informačního systému vložena se souhlasem dotčené osoby, nebo jestliže se jedná o zveřejněnou informaci, d) zaplacení přiměřené peněžní úhrady, jestliže bylo porušeno její právo na zachování lidské důstojnosti, osobní cti, dobré pověsti a na ochranu jejího jména, pokud není postižitelná stávajícími občanskoprávními a obchodněprávními instituty, e) zamezení přístupu k informacím v průběhu sporu, pokud orgán příslušný pro rozhodnutí sporu výjimečně nestanoví jinak; nárok se týká pouze sporem dotčených informací.“

Poskytnutí uvedených informačních systémů nebo dat z nich - ať už úplatně nebo bezplatně - třetí osobě je v rozporu s citovaným zákonem č. 256/1992 Sb. Pokud by k takovému jednání došlo po 1. 1. 1994, od kdy je účinná novela trestního zákona, a pokud by šlo o údaje získané při výkonu státní správy anebo údaje získané v souvislosti s výkonem povolání, zaměstnání nebo funkce, jejichž sdělením byla porušena právním předpisem stanovená mlčenlivost, lze je kvalifikovat jako trestný čin neoprávněného nakládání s osobními údaji podle § 178 TrZ.

Ustanovení § 178 - Neoprávněné nakládání s osobními údaji bylo nově zařazeno do TrZ v návaznosti na zákon č. 256/1992 Sb. ze dne 29. 4. 1992, o ochraně osobních údajů v informačních systémech, a zákonem č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů, novelizováno s účinností od 1. 11. 1998. Uvádí se v něm: „(1) Kdo, byť i z nedbalosti, neoprávněně sdělí nebo zpřístupní údaje o jiném shromážděné v souvislosti s výkonem veřejné správy, bude potrestán odnětím svobody až na tři léta nebo zákazem činnosti nebo peněžitým trestem. (2) Stejně bude potrestán, kdo údaje o jiném získané v souvislosti s výkonem svého povolání, zaměstnání nebo funkce , byť i z nedbalosti sdělí nebo zpřístupní, a tím poruší právním předpisem stanovenou povinnost mlčenlivosti. (3) Odnětím svobody na jeden rok až pět let nebo zákazem činnosti nebo peněžitým trestem bude pachatel potrestán, a) způsobí-li činem uvedeným v odstavci 1 nebo 2 vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se údaj týká, b) spáchá-li čin uvedený v odstavci 1 nebo 2 tiskem, filmem, rozhlasem, televizí nebo jiným obdobně účinným způsobem, nebo c) spáchá-li uvedený v odstavci 1 nebo 2 porušením povinností vyplývajících z jeho povolání, zaměstnání nebo funkce.“ Je třeba ocenit zařazení nedbalostní varianty do této skutkové podstaty, protože lehkomyslné zacházení s osobními údaji občanů je mimořádně rozšířeným zlozvykem v České republice.

Příkladem porušení tohoto zákona v posledních letech je odcizení údajů o telefonních účastnících (včetně tzv. tajných čísel) z evidence Telecomu. Zde porušil jednak Telecom povinnosti uložené písm. i) § 17 zák. č. 256/1992 Sb. „zajistit ochranu informací i celého systému před náhodným nebo neoprávněným zničením, náhodným poškozením, jakož i před neoprávněným přístupem nebo zpracováním“, jednak doposud neznámý pachatel spáchal trestný čin podle ust. § 178 TrZ.[28] Detailně byl tento případ rozebrán v [71]. Jiným příkladem byla situace, kdy zdravotnický personál poskytl seznam pacientek s diagnózou rakoviny distributorovi léčiv (za mizivého zájmu nejen orgánů činných v trestním řízení, ale i tehdejších představitelů Ministerstva zdravotnictví).

Nutno říci, že *útoky proti osobním datům občanů se množí,* a to jednak ze strany jiných osob, jednak i ze strany samotného státu, který nemá většinu svých evidencí upravenu v souladu s požadavky platných právních předpisů, zejména zákona č. 256/1992 Sb.

Na závěr této problematiky je třeba zmínit § 24 tohoto zákona, který předjímá zřízení Úřadu pro ochranu osobních dat občanů *„K provedení registrace a provádění dozoru nad provozem informačních systémů jsou příslušné orgány, zřízené zvláštními zákony.“* Na jeho zřízení kvalifikovaným způsobem čekáme sedm let.

Je zřejmé, že stávající právní úprava v ČR zákonem č. 256/1992 Sb. není zcela vyhovující, a to i kdyby byla naplněna ve všech svých ustanoveních. Velmi brzy po vydání zákona se stal terčem kritiky pro svoji bezzubost, především pro nepřesné definice a neaplikovatelná ustanovení. Pozitivně nutno hodnotit, že byl zákon na ochranu osobních dat v informačních systémech v roce 1992 přijat. Na druhou stranu vývoj informačních technologií i právní teorie v oblasti ochrany dat za více než deset let od roku 1981 tak pokročil, že již v době přijetí tohoto zákona jsme museli konstatovat jeho jistou zastaralost a nedokonalost.[29] Důsledkem je *řada definičních nepřesností*, jejichž výklad je obtížný, ne-li nemožný, a to zejména v tak základních pojmech, jako jsou „Informace“, „Informační systém“, „Provozování informačního systému“, „Zpracování informace“ apod. Podobně *nejsou řešeny procedurální otázky,* např. příslušnost soudu podle § 23, ale zejména vše, co se nachází v ust. § 24 a následujících, tedy v ustanoveních zajišťujících vlastní provádění tohoto zákona.

Tyto nedostatky by měl odstranit nový návrh *Zákona o ochraně osobních údajů a o působnosti Úřadu pro ochranu osobních údajů a o změně některých dalších zákonů,* který byl zpracován Úřadem pro státní informační systém (dále jen ÚSIS), a protože tento úřad (konečně) neváhal ke spolupráci vyzvat opravdu renomované odborníky, vše nasvědčuje tomu, že by se mohlo podařit zkvalitnit tuto významnou oblasti ochrany základních lidských práv u nás.

Navrhovaný nový zákon upravuje ochranu osobních údajů, práva a povinnosti vznikající při jejich zpracovávání, stanoví podmínky, za nichž se uskutečňuje předávání osobních údajů do jiných států a sankce za porušení povinností stanovených tímto zákonem nebo na jeho základě. Upravuje dále zřízení Úřadu pro ochranu osobních údajů a vymezení jeho pravomocí a působnost. Podstatné je, že se vztahuje na osobní údaje, které zpracovávají státní orgány, orgány územní samosprávy, jiné orgány veřejné moci, jakož i fyzické a právnické osoby, a na veškeré zpracovávání osobních údajů, ať se tak děje automatizovaně nebo jinými prostředky. Na rozdíl od zákona č. 256/1992 Sb. zavádí docela slušné sankce: přestupky sankcionované až do 50 tis. Kč a pokuty správcům a zpracovatelům až do výše 20 mil. Kč. Nad jeho dodržováním bude bdít Úřad pro ochranu osobních údajů, jehož struktura a pravomoci se více blíží NKÚ nežli orgánům činným v trestním řízení. Co bude asi největším problémem (a k jehož řešení přistupuji s hlubokou skepsí) je otázka personálního obsazení. V čele tohoto Úřadu by v každém případě měl stát renomovaný odborník - nezpochybnitelná a zcela nezávislá autorita.

Podobně jako u nás existují zákony na ochranu osobních dat občanů prakticky ve všech vyspělých státech - viz [65] až [67]. Např. ochranu osobních údajů ve Francii upravuje zákon č. 78-17 z 6. 1. 1978, kterým byl zřízen Celostátní výbor pro informatiku a svobody (CNIL), jako nezávislá instituce, jejímž posláním je dbát na dodržování výše uvedeného zákona, zajišťovat

informování občanů o jejich právech a povinnostech, provádět kontrolu zpracovaných informací vztahujících se k osobám. Tento zákon současně sankcionuje neoprávněné zacházení s osobními údaji. [65] Podobně ve Španělsku platí ústavní zákon č. 5/1992 ze dne 29. 10. 1992 o úpravě automatizovaného zpracování dat osobního charakteru. Tento zákon zakládá odborný orgán zvaný Úřad pro ochranu dat. Na rozdíl od francouzské úpravy tento zákon nevymezuje nové trestní přestupky, ani nedefinuje zvláštní trestní odpovědnosti to je svěřeno trestnímu zákonu. [66]

4.2 Počítačová špionáž

Stále více lidí si uvědomuje, že informace jsou cenným zbožím, za které je třeba platit a pomocí kterých lze získat i velké bohatství. Příkladem opět ze současnosti mohou být utajené obchodní informace - např. o strategických záměrech firmy nebo, což se ukázalo v souvislosti s kupónovou privatizací a následným rozjezdem kapitálového trhu, o vlastnických poměrech a poptávce/nabídce na trhu s cennými papíry. Je celosvětovým trendem, že politická špionáž se stále více mění na špionáž ekonomickou, a to i proti politickým spojencům. Podobně v hospodářské soutěži se získávání informací o konkurenci stává jednou z podmínek obchodních úspěchů.

Některá jednání uskutečněná v souvislosti s automatizovanými (i neautomatizovanými) informačními systémy (státními i soukromými) mohou být za určitých okolností postihnuta podle některých obecně použitelných ustanovení TrZ. Jde např. o *vyzvědačství* (§ 105 TrZ), *ohrožení utajované skutečnosti* (§ 106 - 107 TrZ), ale také *porušování předpisů o nakládání s kontrolovaným zbožím a technologiemi* (§ 124c nebo § 124f TrZ), *zkreslování údajů o stavu hospodaření a jmění* (§ 125 TrZ), *nekalou soutěž* (§ 149 TrZ), *porušování práv k ochranné známce, obchodnímu jménu a chráněnému označení původu* (§ 150 TrZ), *porušování průmyslových práv* (§ 151 TrZ) apod.

Podobné kvalifikace najdeme opět v řadě zemí, např. v již citovaném zák. č. 18. U.S.C., Chapter 37 - Espionage and Censorship, Sec. 793 - Gathering, transmitting or losing defense information.

Zde je třeba říci, že mi není znám případ, kdy by došlo u nás k trestnímu stíhání pro počítačově realizované výše uvedené delikty. Není to zřejmě ani tak proto, že by se nikdy nestaly, ale spíše proto, že jsou velmi těžko k odhalení a ještě obtížněji k dokázání.[30]

IV. Perspektiva počítačového zločinu a jeho odhalování a boj proti němu

Zmínil jsem se o dvou významných technologických přelomech v počítačové technice. Prvním byly osobní počítače. Druhým významným fenoménem počítačových technologií a tedy i počítačového zločinu je s*pojování počítačů lokálními i vzdálenými sítěmi,* z nichž jmenujme především *Internet.* Propojování počítačů, kdy se na jiném místě nacházela data a na jiném místě uživatel, který s nimi pracoval, tedy oddělení vlastnictví a přístupu k nim, resp. možnost vzdáleného přístupu k informačnímu systému bez nutnosti fyzické přítomnosti u počítače, se ukázalo nejen jako výrazný rozvojový prostředek pro zlepšování informačních systémů, ale i jako nový impuls pro páchání distanční trestné činnosti. Možnost anonymity při vzdáleném přístupu k počítači vytváří dobré předpoklady pro utajení pachatele i pro skrytí jeho kořisti.

Pro Internet jsou charakteristické nové možnosti, jak páchat klasické trestné činy, i nové druhy trestné činnosti doposud nepoznané.

Trestnou činnost spojenou s Internetem můžeme klasifikovat do dvou základních kategorií:

1) zpřístupňování informací, které mohou někomu způsobit újmu nebo založit spáchání trestného činu nebo naopak shromažďování informací o osobách za účelem jejich pozdějšího nelegálního využití - neboli informační trestná činnost;

2) páchání trestné činnosti v internetovém prostředí - neboli internetovská trestná činnost.

1. Informační trestná činnost

Internet má dvě hlavní informační možnosti: první je šíření informací, druhou shromažďování informací.

1. 1 Šíření informací

Povaha Internetu jakožto prostředku, jehož prostřednictvím lze veřejně šířit informace, je významná v oblasti trestněprávní, konkrétně tam, kde se jedná o trestné činy, u nichž je veřejnost jejich znakem (např. podněcování podle § 164, schvalování trestného činu podle § 165 a výtržnictví podle § 202 TrZ).[31] Přitom je trestný čin spáchán veřejně, je-li spáchán obsahem tiskoviny nebo rozšiřovaného spisu, filmem, rozhlasem, televizí nebo jiným obdobně účinným způsobem. Internet nepochybně lze považovat právě za *„jiný obdobně účinný způsob“*.[32]

Jelikož je třeba Internet pojímat jako nástroj ke komunikaci, případně některé jeho produkty jako hromadný sdělovací prostředek, poskytovatelé připojení nepochybně nemohou nést odpovědnost za to, že někdo vystupuje v určité diskusní skupině se závadnými texty. Nepochybně ale bude majitel WWW stránky odpovídat za nezávadnost jejího obsahu stejně, jako každý uživatel bude odpovídat za porušování platných právních norem tohoto státu (například rozesíláním textů propagujících hnutí směřující k potlačení práv a svobod občanů).[33] Pokusy o cenzuru Internetu (odpojováním uživatelů služby CompuServe, vytvářením programových filtrů v prohlížecích programech nebo vydáváním zákonů - např. v USA) se jeví jako dosti bezzubé. Cenzura je zásadně nepřípustná (a odporuje to i Listině základních práv a svobod svobod, čl. 17 odst. 3). I autoři cenzorských zákonů mají v USA značné problémy se zde obzvlášť široce chápanou svobodou osobnosti. Na druhou stranu nevidím důvody, proč by se k Internetu mělo přistupovat jinak: stíhat lze konkrétní osoby za spáchání konkrétního, prokázaného deliktu, a to bez ohledu na to, zda jej spáchaly na Václavském náměstí nebo na Internetu. Tedy za šíření poplašných zpráv, za propagování nesnášenlivosti, za schvalování zločinu, za ohrožování mravnosti, za šíření toxikománie atd. - vždy ale s naplněním subjektivní i objektivní stránky trestného činu (muselo skutečně dojít ke spáchání zločinu, a to konkrétní osobou, která si musela být vědoma možnosti, resp. mít v úmyslu jeho spáchání). Daleko problematičtější než doposud ale bude zjištění skutečného pachatele, zadokumentování jeho trestné činnosti, jeho obvinění, dovlečení před soud a případné odsouzení.

Některé činnosti jsou na Internetu, podobně jako v jiných médiích, zakázány či regulovány přímo ze zákona. Příkladem může být zákon č. 40/1995 Sb., o regulaci reklamy a o změně a doplnění zákona č. 468/1991 Sb., o provozování rozhlasového a televizního vysílání, ve znění pozdějších

předpisů.[34] V něm podle ust. § 2 platí: „Reklama zboží nebo služeb nebo jiných výkonů či hodnot, jejichž prodej nebo poskytování nebo šíření není dovoleno, je zakázána. Reklama nesmí obsahovat nepravdivé údaje, prvky, které by byly v rozporu s dobrými mravy, zejména prvky urážející národnostní nebo náboženské cítění, ohrožující obecně nepřijatelným způsobem mravnost nebo propagující násilí, prvky snižující lidskou důstojnost nebo využívající motiv strachu. Reklamy určené osobám do 15 let, nebo v nichž vystupují osoby mladší 15 let, pokud podporují chování ohrožující jejich zdraví, psychický nebo morální vývoj, se zakazují. Zakazuje se: a) reklama založená na podprahovém vnímání člověka, b) reklama skrytá.“[35]

Je samozřejmě jinou věcí, zdali do budoucna nevznikne na trhu zpřístupňovatelů Internetu situace, kdy pro tzv. lepší připojovatele bude nepřijatelné z obchodního hlediska, aby se prostřednictvím jejich služeb připojovali šiřitelé takto kontroverzních informací či programů. Jiná věc je, že stačí jeden méně seriózní či svobodomyslnější a výsledek je stejný.

Moderní svět poskytl fantastické informační možnosti a pochopitelně každá technologie je zneužitelná. S tím se budeme muset naučit žít, i když vůbec nerezignujeme na právní instrumenty, sloužící k postihu obecně pohoršujícího jednání. U nás je takovým instrumentem zejména ustanovení § 202 TrZ, postihující výtržnictví. Dle tohoto ustanovení může být postižen, *kdo se dopustí veřejně nebo na místě veřejnosti přístupném hrubé neslušnosti nebo výtržnosti.* Podobně bychom mohli aplikovat i jiná ustanovení trestního zákona, např. § 205 - Ohrožování mravnosti.[36] Problém trochu bude s aplikací pojmu *veřejně* na virtuální svět Internetu, ale při výše uvedené aplikaci zákona č. 81/1966 Sb., o periodickém tisku a o ostatních hromadných informačních prostředcích, ust. § 89 odst. 4 TrZ („Trestný čin je spáchán veřejně, jestliže je spáchán a) obsahem tiskoviny nebo rozšiřovaného spisu, filmem, rozhlasem, televizí nebo jiným obdobně účinným způsobem, nebo b) před více než dvěma osobami současně přítomnými“) by to zřejmě šlo.

V úvahu přicházejí podle povahy zveřejněného materiálu i jiné trestní postihy, ovšem pochopitelně pouze vzhledem k pachatelům, příp. majitelům serveru umístěného na našem území. Teoreticky přichází v úvahu i podání trestního oznámení do zahraničí, neboť skoro každý evropský stát má ve svém trestním zákoně ustanovení, chránící veřejné mravy, mravopočestnost apod.[37]

Současně je ale třeba říci, že z hlediska prezentace Internetu některými médii lze považovat zdůrazňování existence zrovna těchto druhů informací za démonizaci Internetu. A asi nelze pochybovat o tom, že jistý díl odpovědnosti ponese i ten, kdo se na Internet připojí. Minimálně sám sobě odpovídá za to, že se ke klávesnici počítače nedostanou nepovolané ruce, resp. že se tam nedostanou bez dozoru či vhodného upozornění. Zcela přitom pomíjím přímé zájemce o tyto programy či informace; ti si své najdou i bez Internetu.

S touto problematikou souvisí i otázka, zda zaslání mailu konkrétní osobě představuje *šíření zpráv* a zda mail podléhá či nepodléhá listovnímu tajemství podle § 239 - 240 TrZ. Podle § 239 odst. 1 - Porušování tajemství dopravovaných zpráv „Kdo úmyslně poruší tajemství a) uzavřeného listu nebo jiné písemnosti, zasílaných poštou nebo jiným dopravním zařízením,[38] nebo b) zprávy podávané telefonem, telegrafem nebo jiným takovým veřejným zařízením, bude potrestán odnětím svobody až na šest měsíců.“ Na otázku, zda je Internet „jiným takovým veřejným zařízením“, se v

komentáři[39] praví, že jím je např. dálnopis, telefax, postfax apod. Podle mého názoru *jde o veřejné zařízení*, neboť e-mail využívá mezi místem odesílatele a příjemce dvou veřejných subjektů (alespoň veřejných pro předplatitele resp. účastníky): serveru poskytovatele připojení a jednotné telefonní sítě, po které je přenos mailu realizován. Lze se proto domnívat, že i přenos zpráv elektronickou poštou (nebo obecně jakýmkoliv výběrovým způsobem, při němž lze jednoznačně definovat osobu, k níž má být zásilka doručena - např. bankovní interní komunikační sítí, komunikační sítí armády či vnitra mimo JTS[40] apod.), je prostředím pro naplnění skutkové podstaty trestného činu podle § 239.

Podle odst. 2 tohoto ustanovení „Pracovník poštovní nebo telekomunikační služby, který a) spáchá čin uvedený v odstavci 1, b) jinému úmyslně umožní spáchat takový čin, nebo c) pozmění nebo potlačí písemnost dopravovanou poštou nebo jiným dopravním zařízením anebo zprávu podanou telefonicky, telegraficky nebo jiným podobným způsobem, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti.“ Rovněž v tomto případě je zřejmě pracovník providera Internetu pracovníkem „telekomunikační služby“, protože jde o službu poskytovanou veřejnosti - předplatitelům.[41]

Poněkud jiná je situace v ust. § 240 TrZ „(1) Kdo v úmyslu způsobit jinému škodu nebo opatřit sobě nebo jinému neoprávněný prospěch a) prozradí tajemství, o němž se dozvěděl z písemnosti, telegramu nebo telefonního hovoru, které nebyly určeny jemu, nebo b) takového tajemství využije, bude potrestán odnětím svobody až na jeden rok. (2) Pracovník poštovní nebo telekomunikační služby, který a) spáchá čin uvedený v odstavci 1, nebo b) jinému úmyslně umožní spáchat takový čin, bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.“ Zde nepoužil zákonodárce z neznámých důvodů obecnější definici podobně jako v § 239 *„telegrafem nebo jiným takovým veřejným zařízením“,* ale „natvrdo“ zde uvedl pojem „telefonní hovor“. Naskýtá se otázka, zda digitální přenos prostřednictvím JTS lze považovat za hovor: mohou spolu hovořit pouze dvě osoby nebo i dva počítače, zda je ještě hovorem fax a už není mail, či jak tomu je? Tady vidíme značný rozpor, který nepomýšlí na očekávaný vývoj technických prostředků. Rovněž otázkou k diskusi je definování pojmu „písemnost“ z hlediska nových technologií. Je dopis napsaný v textovém editoru a posílaný jako příloha mailu písemností? Podle § 2 zákona o archivnictví[42] je písemností *„písemný, obrazový, zvukový a jiný záznam“,* což by rozšířenému elektronickému pojetí vyhovovalo. Naproti tomu řada právních norem pracuje s pojmem „písemnost“ jako s notorietou, kterou netřeba definovat, ale v komentářích prakticky všech autorů není uvažována jiná varianta nežli „písemnost na papíru“. (Našemu právnímu řádu by prospěla revize z hlediska moderních informačních technologií; mé opakované volání bohužel zůstává stále nevyslyšeno.)

Již dříve jsme upozorňovali [34] na nutnost nejen informaci získat, ale tuto informaci *prozradit* nebo *využít.* Nemusí se jednat o sdělení charakteru utajované skutečnosti,[43] neboť v tomto případě jde o tzv. tajemství (všech) dopravovaných zpráv. A opět musí jít o úmyslný trestný čin, tedy nemusíte mít obavu, že po nahodilém napojení se na cizí telefonický hovor a jeho prozrazení bude následovat trestní postih.[44]

Abych se mírně zastal zákonodárců: jednak technický pokrok je zde opravdu překotný, jednak po dlouhá léta nebyla tato ustanovení v zorném úhlu státu a jeho právníků, neboť sám stát byl

nejflagrantnějším porušovatelem těchto tajemství vůči tzv. nepohodlným osobám. Na druhou stranu i „historické“ judikáty lze aplikovat na nejmodernější komunikační prostředky. Jelikož podle informací, které byly zveřejněny, patří do běžné praxe zaměstnanců providerů, že čtou (obvykle z dlouhé chvíle, ale možná nejen proto) poštu svých uživatelů, jsou výše uvedená varování zřejmě vysoce na místě. (A samozřejmě vůbec nepřichází v úvahu vnucovat uživateli smlouvu, kterou by dával zájemce o službu připojení k Internetu souhlas provozovateli, aby mohl - z jakýchkoliv důvodů - kontrolovat obsah jeho mailové schránky.)

Lze tedy souhrnně říci, že podle názoru mého a mých spolupracovníků[45] se na mail vztahuje ochrana podle ust. § 239 TrZ, tzv. listovního tajemství, tedy těžko lze z napsání a odeslání mailu konkrétní osobě dovodit *rozšiřování* informací. Z toho vyplývá mj. skutečnost, že urážlivým mailem zaslaným urážené osobě - a nikomu jinému - nelze spáchat trestný čin pomluvy. K naplnění skutkové podstaty trestného činu podle § 206 - Pomluva[46] by mohlo dojít v případě, že by urážlivý mail byl zaslán jiným osobám. Přitom aplikace druhého odstavce § 206 není v případě Internetu nebo i pouhého e-mailu vyloučena.

1. 2 Shromažďování informací

O tom, že Internet představuje vhodné prostředí pro provoz informačních systémů, není pochyb. Kromě Internetu již máme různé intranety a extranety a řada organizací uvažuje o tom, že zjednoduší provoz vlastních komunikací využitím Internetu. Pokud někdo jeho prostřednictvím bude provozovat informační systém obsahující určité údaje o osobách, vztahují se na něj příslušné předpisy upravující jejich provozování,[47] zejména pak obecně platný zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech. Půjde tu jak o povinnosti stanovené pro provozování informačních systémů s tzv. citlivými údaji,[48] tak obecné povinnosti provozovatele, resp. zprostředkovatele, jeho zaměstnanců i dalších osob,[49] tak v neposlední řadě o možnosti obrany proti jejich porušování ze strany dotčených osob a dalších fyzických osob.[50]

V prostředí Internetu jsou běžně sbírána data od uživatelů, aniž by k tomu měl provozovatel informačního systému oprávnění, aniž by uživatelé věděli, jak bude s jejich daty naloženo, o splnění požadavků ad i) a l) § 17 zák. č. 256/1992 Sb. už vůbec nemluvě. Většinou si za tento protiprávní stav mohou samotní uživatelé, kteří v touze dostat se na určité stránky nebo získat určitou nabízenou službu bez rozmyslu sdělují neznámé (nebo přinejmenším neověřené) protistraně svoje osobní důvěrné údaje.

Podle mého názoru je sledování internetových informačních systémů obsahujících osobní údaje občanů jedním z mnoha úkolů stále ještě (v roce 1999) neexistujícího Úřadu pro ochranu osobních údajů v ČR. V každém případě získávání informací o osobách (osobních údajů) je jednak porušováním předpisů o ochraně osobních údajů v informačních systémech (zákon č. 256/1992 Sb., o ochraně osobních dat v informačních systémech, bohužel bez přímých sankcí), ale může ve vybraných případech založit i trestní odpovědnost podle § 178 TrZ - Neoprávněné nakládání s osobními údaji.

Upozorňuji ještě jednou na skutečnost, že novelou trestního zákona, provedenou v rámci vydání nového zákona o ochraně utajovaných skutečností,[51] byla do znění § 178 přidána i *nedbalostní varianta*; nemusí se tedy jednat jen o úmyslný trestný čin, čímž se riziko trestní odpovědnosti pro provozovatele, ale i uživatele informačních systémů obsahujících osobní údaje občanů výrazně zvyšuje.

1. 3 Internetovská trestná činnost

Počítačová trestná činnost, kterou jsme si v předcházejícím výkladu podrobně probrali, má podle současných poznatků na Internetu tyto nejčastější podoby:

• zásahy do cizích programů a databází (§ 257a - Poškození a zneužití záznamu na nosiči informací, § 152 - Porušování autorského práva); typickým zločincem je český hacker CzERT, který již naboural a pozměnil řadu WWW stránek - od Ministerstva obrany po soukromé firmy, ale vyskytly se i případy „vykradení“ určité databáze - např. mailových adres nebo telefonních čísel;
• porušování autorských práv kopírováním cizích autorských děl (distribuce programů, kopírování WWW stránek, umísťování cizích autorských děl na vlastní WWW stránky a na servery - např. fotografie, archivy písničkových textů); vše je porušováním autorského práva podle § 152 TrZ;
• neoprávněné užívání počítače či komunikačního zařízení, obvykle pod identifikací jiného, oprávněného uživatele (§ 249 - Neoprávněné užívání cizí věci);
• neoprávněné užívání a distribuce počítačových programů (§ 152 - Porušování autorského práva);
• neoprávněný přístup k datům, získávání utajovaných informací - počítačová špionáž (některá jednání mohou být za určitých okolností postihnuta podle některých obecně použitelných ustanovení TrZ - např. Ohrožení utajované skutečnosti podle § 106 nebo § 107);
• v případě touhy po obohacení se, nikoliv pouze informacemi, ale přímo fiskálně (pěněžně), pravděpodobně nejčastěji se bude jednat o skutkovou podstatu podle ust. § 250 TrZ - Podvod (podvodné transakce s podvodným zbožím, penězi či falešnými identifikacemi při nákupu a prodeji;
• začínají se objevovat i další trestné činy - například internetová „letadla“ neboli pyramidy, což jest trestným činem podle ust. § 250a TrZ, daňové podvody (např. s DPH) apod.;
• v loňském roce byl obviněn pachatel, který se na internetové nástěnce dopustil trestného činu podle § 260 TrZ, tj. Podpory a propagace hnutí směřujících k potlačení práv a svobod občanů (uveřejňováním rasistických textů);
• v roce 1999 došlo ke spáchání podvodů spočívajících v zadávání nepravdivých čísel nebo čísel cizích platebních karet při nákupu v internetovém knihkupectví.

2. Změna kvality počítačové kriminality

Z hlediska kriminalistických charakteristik počítačových prostředků jako nástrojů trestné činnosti musíme vnímat obrovskou propast, která se otvírá mezi lokálními výpočetními systémy a počítačovými sítěmi, kdy bychom mohli hovořit o době „před sítěmi“ a „po nich“, jako o přelomu v

oblasti možností a dopadů počítačové kriminality. Existence„sítí sítí“, reprezentovaných zejména Internetem potom přináší další zásadní zlom do kvality (a bohužel i kvantity) zločinů souvisejících s počítači. [2], [3]

Objevují se zde nejen nové technologie, ale nové skutkové podstaty trestných činů, nové druhy důkazů a velké množství nových právních problémů, s jakými se u příležitosti nástupu jiných nových technologií právní teorie i praxe doposud nesetkala [4], [5], [6], [7], [8] apod.

Proto o skutečně velkých počítačových zločinech, především podvodech hovoříme právě v prostředí počítačových sítí - zejména v bankách, které jsou technologicky nejvíce napřed.

Ještě složitější je situace v případě velkých vzdáleností nebo geografického rozmístění počítačové sítě na území různých států. Typickým příkladem takové sítě, přesně řečeno „sítě sítí“ je Internet, který umožňuje situaci, kdy bude oběť (bankovní server) na území jednoho státu, pachatelé z několika různých států provedou nezákonný převod peněz a uloží je - opět elektronicky - na území dalšího státu. Pochopitelně stopa vedoucí k pachatelům bude velmi obtížně zjistitelná a komplikovaná teritoriální příslušnost učiní (alespoň podle dosavadních zkušeností s mezinárodní spoluprací) vyšetřování a trestní stíhání takřka nerealizovatelné nebo přinejmenším na hranici možností.

I lokální počítačové systémy, omezené na jednu instituci, rostou se svojí složitostí nad všechny meze. Pracoval jsem na případu týkajícím se kapitálového trhu, kde se transakce odehrávají v reálném čase na třech mimořádně velkých počítačích vzájemně propojených, kde databáze má velikost několik gigabytů a kde ani systémový technik počítače vždy neví, co se v něm přesně odehrává.

Další otázkou, která signalizuje ztížení boje proti trestné činnosti páchané s využitím počítačů, je stále rostoucí využívání *šifrování.* Jelikož neexistuje legální možnost získání přístupového hesla nebo klíče šifry od obviněné osoby, můžeme se dostat do situace (s kterou se snaží již různými, doposud neúspěšnými legislativními pokusy vyrovnat např. vláda USA), kdy data zločinců budou pro orgány činné v trestním řízení nedostupná. [68]

Jako tomu je ve všech ostatních oblastech trestné činnosti, *zločinci mají vždy náskok před ostatními.* Mají motiv (touhu po zisku), prostředky a lidi (které si zaplatí většinou lépe než banka nebo stát). Mají výhodu volby času a způsobu. A nahrávají jim výše uvedené technologické faktory. Všeobecně se u odborníků objevuje jistá skepse ohledně trendů počítačové kriminality a limitů jejího odhalování a vyšetřování. Podle mého názoru je třeba daleko více sil přesunout do oblasti prevence, obrany počítačů a informačních systémů, neboť jedině tak lze účinně bojovat proti tomuto druhu trestné činnosti, patřícímu do stále sílícího objemu kriminality bílých límečků a organizovaného zločinu.

Příkladem naprosté nezbytnosti prevence a nikoliv následné represe je tzv. homebanking a zpřístupňování bank či provádění obchodů po Internetu. O těchto obchodech se stále mluví, ale jejich skutečné využívání je v evropském virtuálním prostoru velmi malé. Proč? Právě proto, že nejsou vyřešeny otázky bezpečnosti transakcí a jejich právní zajištění. K právní problematice Internetu odkazuji na články [4], [5], [68], [69]. Součástí otázek, které právní teorie i praxe bude

muset řešit, jsou závazkové vztahy uzavírané prostřednictvím počítačů a telekomunikací, na dálku. S tím souvisí i problematika autentizace, reprezentovaná zejména tzv. digitálními podpisy [70], která si již našla cestu do zákonodárství států EU.[73]

V. Závěr

Počítačová kriminalita je (z hlediska historie kriminalistiky) zcela novým oborem. Akcelerace společnosti v oblasti informačních technologií se totiž promítá do všech sfér lidské činnosti: od obchodu a služeb, přes umění či erotiku a pochopitelně i do nových forem trestné činnosti. Člověk je zároveň stále závislejší na bezchybném fungování informačních technologií a tudíž roste společenský požadavek na ochranu těchto technologií před zločinci. Tento požadavek je o to významnější, že počítačová kriminalita je stále více spojována s organizovaným zločinem [46] až [49].

Možná by stálo za úvahu při příští novele nebo při rekodifikaci trestního zákona zvážit zařazení nové okolnosti podmiňující použití vyšší trestní sazby. Zatím je přísněji kvalifikováno, pokud je trestný čin spáchán se zbraní nebo v organizované skupině, ale to, že čin byl spáchán s počítačem, nebezpečnost pachatelova jednání v očích trestního zákona nijak nezvyšuje. Přitom podle mého názoru prorůstání počítačů všemi oblastmi lidského života by se mělo odrazit i v připravované rekodifikaci trestního zákona podobně, jako se zde v poslední době objevují náměty na zařazení zvláštních skutkových podstat souvisejících s finanční a zejména bankovní kriminalitou. *„Jestliže se ale informace stává v dnešní společnosti ekvivalentem materiálních statků, musí nakládání s nimi podléhat přirozeným omezením, etickým normám i vytčení právních mezí, které jsou běžné z jiných oblastí lidského konání.“* [9]

Důsledkem výše uvedených trendů je také stále větší překrývání řady oborů. Zatímco zpočátku k tomu docházelo jen po linii oborů technických - např. počítače a komunikace, nyní je již propojování informačních, organizačních, společenských a dalších vazeb takové, že znalostní domény vyhrazené dříve pouze úzkým specialistům se začínají překrývat a propojovat. Typickým příkladem je obor, pracovně nazvaný v roce 1995 „počítačové právo“[15], který dnes musíme pojímat jako mezioborovou disciplínu, zahrnující jak vlastní informatiku, zejména v oblasti budování a využívání informačních, počítačových a komunikačních systémů, tak vybrané právní disciplíny, a to jednak soukromoprávního charakteru (občanské a obchodní právo, autorské právo atd.), jednak charakteru veřejnoprávního (trestní právo, ochrana osobních dat, finanční právo, některé procesní normy apod.). Odborníci působící v oblasti prevence a represe proti informatické a počítačové kriminalitě budou muset disponovat právě takovými mezioborovými znalostmi: od informatiky přes bezpečnost informačních systémů až po právní disciplíny.

V posledním období začínáme hovořit, právě v důsledku proběhnuvších technologických změn, o *právu informačních a komunikačních systémů*, přičemž tento - opět pracovně nazvaný - právní obor nachází své zdroje nejen ve výše uvedených soukromoprávních a veřejnoprávních disciplínách, ale v řadě speciálních právních norem, které začínají právo informačních a komunikačních systémů vytvářet. A navíc je třeba zdůraznit, že s připravovaným vstupem České republiky do Evropské unie je to i právo komunitární, které svými vybranými směrnicemi rovněž přispívá k budování tohoto nového právního odvětví. Jde především o směrnice ES o právní ochraně počítačových programů [51], o právní ochraně databází [52], o ochraně jednotlivců ve

vztahu ke zpracování osobních dat a o volném pohybu těchto dat [77] nebo ještě speciálnější právní normy, vztahující se k určitému sektoru [78], [79], [80] apod.

Z hlediska českého právního řádu nám počítače a především jejich nehmotné složky - programy (software) a data dělají značné problémy. A nejsou to jen data ryze počítačová, protože dnes se součástí počítačových produktů stávají i nejrůznější audiovizuální díla. Jen namátkou lze uvést problémy, které vyplývají z obtížného pojetí nových technologií stávajícími právními normami a především z absence soudní judikatury, přičemž jejich výklad může mít pro některé subjekty podobně fatální důsledky, jako výklad rozdílů mezi motorovou naftou a lehkými topnými oleji:

1. Je dosti zřejmé, že ochrana tak dynamického a specifického díla, jakým je počítačový program, prostřednictvím *autorského zákona* je pouze „nejlepším ze všech špatných řešení". Čím více dochází ke globalizaci softwarového průmyslu, prolínání programů, databází a jiných autorských děl (obvykle audiovizuálních) v jednom produktu a čím více se zvyšuje ekonomický význam těchto děl, tím větší problémy činí „narazit" tuto oblast na kontinentální principy autorskoprávní ochrany. Ani existující směrnice ES [51], ani připravovaný návrh nového autorského zákona u nás, nejsou se schopny vyrovnat s některými palčivými otázkami, zejména ve vztahu k počítačovým programům.[86]

2. Speciální právní normy, především daňové, neumějí včas nebo správně reagovat na nové skutečnosti, nebo věci poměrně známé vykládají nesprávně. Známým příkladem je několikatiletý spor mezi správci daně a plátci DPH - videopůjčovnami - o sazbě DPH za *půjčování videokazet*. Zatímco správci daně se vesměs dívají na kazety jako na věci movité (se sazbou 22%), podle skutečného obsahu právního vztahu mezi půjčovnou a jejím zákazníkem o krátkodobé získání práva užít určité autorské dílo, které je zaznamenané na hmotném nosiči - kazetě. Korektní výklad zákona v souvislosti s touto otázkou nebyl zatím žádným soudem podle mých informací proveden, i když měly být nějaké žaloby podány. (Je přitom zajímavé, že prakticky totožný případ z oblasti dovozu počítačových programů na magnetických médiích byl vyřešen samostatnou fakturací nosiče a programu, tj. práva užívat program, jak z hlediska cla, tak z hlediska DPH.)

3. Stále se zvyšující význam tzv. *volně šířitelných programů* (tzv. „open source" či „free software"), jejichž užívání není v souladu s platným autorským zákonem [82], může tak vytvořit značné právní problémy pro autory, distributory i koncové uživatele.

4. Do autorskoprávní oblasti s následnými trestněprávními dopady patří i probíhající boj mezi výrobci zvukových a zvukově-obrazových záznamů na digitálních nosičích (zejména CD a DVD), které mohou být bez ztráty kvality nahrávky prakticky neomezeně kopírovány, a producenty a uživateli těchto nelegálních kopií. K *nelegálnímu šíření audiovizuálních nahrávek* (ve formátu MP3) i software je ve zvýšené míře využívána síť Internet, která je díky svojí anonymitě a schopnosti zastírat pravý původ produktu k tomuto účelu více než vhodná.[52] S tím souvisí i snahy o šifrovou ochranu těchto děl a napadání této ochrany hackery. Problémy nám bude činit zejména rozpor mezi teriotoriálním principem autorského práva a globálním charakterem Internetu, jakož i problémy s vyšetřováním a dokazováním tohoto druhu trestné činnosti.

5. Možnosti *kryptografických prostředků k utajování elektronické komunikace* zneklidňují vlády celého světa - i ty demokratické. Je charakteristické, že nejmodernějšími prostředky pro utajenou

komunikaci disponují zločinecké organizace. Prakticky v každém více technologicky pokročilém státě se proto vlády snaží prosadit jistý druh „zákona o elektronické komunikaci“, který by vymezil pravomoci státu a jeho orgánů vzhledem k účastníkům komunikace. Kdy se tak stane i u nás, je pouze otázkou času. Zatím můžeme diskutovat o legalitě poskytování informací ze strany provozovatelů mobilních telefonů o místě, kde se telefonující osoba v určitý okamžik nacházela, a o seznamu čísel, na které volala.[53]

6. *Používání jmen internetovských domén* představujících jméno města či obce (zde bych uvedl pouze dva možné pohledy: je či není používání jména v rozporu s dobrými mravy; je nebo není možné vydat vyhlášku, kterou by město zakazovalo používání jména města bez souhlasu a zaplacení poplatku ke komerčním účelům - podle mého názoru by taková vyhláška mohla být shledána jako protiústavní) nebo registrované ochranné známky - v detailech viz např. [75].

7. Ani nově vznikající zákony neberou v úvahu existenci jiných, než klasicky papírových technologických postupů: příkladem může být např. vládní návrh *tiskového zákona* neboli *zákona o právech a povinnostech při vydávání periodického tisku a o změně některých dalších zákonů,* který vůbec nevzal na vědomí existenci elektronické komunikace. V návrhu se nachází mj. tato definice: „*periodickým tiskem jsou noviny, časopisy a jiné tiskoviny.“*. Je zřejmé, že žádný elektronický (dnes prakticky vždy internetovský) deník či časopis nemůže naplnit pojem „tiskovina“ a tudíž podle zákona nebude existovat, přesně řečeno nebudou se na něj vztahovat ani práva, ale ani povinnosti. Jak snadný bude útěk vydavatele do elektronické ilegality.

8. Velmi problémovou otázkou je *volba rozhodného práva* v prostředí moderních informačních technologií umožňujících dálkový přístup - především na Internetu. Zatímco podle našich názorů je rozhodující umístění serveru s poskytovanou službou [84], existují názory odlišné (judikátů okresních soudů v USA), podle nichž je rozhodující místo, kde se nachází příjemce služby. Důsledky tohoto rozhodnutí si lze představit pouze se značným zděšením. Přitom zde existuje analogická otázka, jakým právním řádem (právním řádem jakého státu) se řídí satelitní vysílání z družice „zavěšené“ nad zeměkoulí. Jedná se o právo státu, odkud je signál vysílán k satelitu, nebo mohou přicházet v úvahu všechna jednotlivá autorská práva všech zemí, kde je signál přijímán? Směrnice Rady 93/83 EHS z 27. 9. 1993 považuje za zemi, kde dochází k užití díla a tedy jejíž autorský zákon se musí aplikovat v souvislosti s tímto vysíláním, jen ten stát, kde dochází k vysílání signálu vzhůru vůči satelitu [85]. Otázkou zasluhující si detailní zkoumání je, zda tomu tak je u Internetu, jehož topografie a způsob činnosti je přece jen jiný.

Řadu dalších problémů, vyplývajících z fenoménu jakým je Internet, právní praxe musí teprve vyřešit: je to např. rozhlasové a televizní vysílání prostřednictvím Internetu, internetová telefonie, komunikace mezi občanem a veřejnou správou prostřednictvím dálkového přístupu, elektronický obchod včetně celních předpisů atd. [87] Je pravděpodobné, že součástí těchto očekávaných právních úprav budou i nové skutkové podstaty trestního práva hmotného, nové úpravy procesních předpisů, ale i nové správní delikty, které se mohou vyskytnout v oblasti informačních a komunikačních systémů.

Podle mého názoru nastal okamžik, kdy je třeba učinit revokaci či jakýsi „úklid“ platného právního řádu součástí budování informační společnosti. Pokud bylo nedávno řečeno, „*Je přirozené a žádoucí, aby napřed vznikla nová oblast lidských vztahů, v té se začaly projevovat problémy a*

teprve poté se někdo začal zajímat, zda není nutné tyto vztahy regulovat právem, jinak řečeno vymyslet nějaký nový zákon. Ve věci jde jen o cit vyčkat tak dlouho, až se určité vztahy stanou zaběhnutými, standardními či zobecnitelnými, a nečekat zase příliš dlouho, až tyto vztahy a případné konflikty z nich plynoucí přerostou do naprosto neřešitelných či obtížně řešitelných situací." [81], pak tato doba nastala.

Aktuálním příkladem jsou dva zákony, nyní projednávané v Poslanecké sněmovně Parlamentu ČR. Prvním je vládní návrh *zákona o ochraně osobních údajů a o změně některých zákonů* (sněmovní tisk č. 374). Na rozdíl od poněkud zastaralého zák. č. 256/1992 Sb., který vycházel z Konvence Rady Evropy na ochranu osob se zřetelem na automatické zpracování osobních údajů č. 108 z roku 1981, značně zastaralé a překonané, je základem navržené úpravy Směrnice Evropského parlamentu a Rady 95/46/EC o ochraně jednotlivců ve vztahu ke zpracování osobních údajů a o volném pohybu těchto údajů [77]. Zákon definuje nově a kvalifikovaněji základní pojmy, popisuje práva a povinnosti dotčených osob i zpracovatelů osobních dat a zakládá Úřad pro ochranu osobních údajů, který bude bdít nad dodržováním zákona. Úřad, jehož struktura a pravomoci se více blíží NKÚ nežli orgánům činným v trestním řízení, provádí dozor nad dodržováním povinností stanovených tímto zákonem při zpracování osobních údajů, vede evidenci oznámení o zpracování osobních údajů a registr povolených zpracování osobních údajů[54], zpracovává a veřejnosti zpřístupňuje výroční zprávu o své činnosti, projednává přestupky a jiné správní delikty a uděluje pokuty podle tohoto zákona, zajišťuje plnění požadavků vyplývajících z mezinárodních smluv, jimiž je Česká republika vázána, poskytuje konsultace v oblasti ochrany osobních údajů, spolupracuje s obdobnými úřady jiných států, vykonává další působnosti stanovené mu tímto zákonem nebo zvláštními zákony. Jde zde navrhováno i zpřesnění ust. § 178 odst. 1 a 2 zákona č. 140/1961 Sb., TrZ, ve znění pozdějších předpisů.

Druhým je pro změnu poslanecká iniciativa - návrh *zákona o elektronickém podpisu* (sněmovní tisk č. 415), který vznikl v důsledku stále se zvyšující důležitosti elektronického obchodování a elektronické komunikace obecně. Jedním z prioritních úkolů je uzákonit elektronický podpis (tedy autentizovat uživatele, který provádí jakoukoli transakci prostřednictvím telekomunikační sítě) a dát dokumentům v elektronické podobě stejnou právní váhu jako dokumentům klasickým. Účelem zákona o elektronickém podpisu je zrovnoprávnění elektronického podpisu a elektronické dokumentace s podpisy ručními a s dokumentací papírovou se samozřejmým požadavkem na jejich bezpečnost a důvěryhodnost. Součástí návrhu zákona jsou i definice správních deliktů v této oblasti.

Oba dva připravované zákony mají značný dopad i na oblast počítačové a informační kriminality. První z nich by měl vytvořit dokonalejší nástroj pro potírání nelegálního sběru, zpracování a poskytování osobních dat občanů. Druhý z nich si klade za cíl vytvořit nástroj pro bezpečnou dálkovou komunikaci, využitelnou jak ve veřejnoprávní, tak v soukromoprávní sféře. Tento zákon byl připravován v předstihu před příslušným komunitárním právním aktem Evropských společenství, ale vychází z dostupného návrhu ES [88] i z prací probíhajících v rámci Komise OSN pro mezinárodní obchodní právo (United Nations Commission on International Trade Law - UNCITRAL).

Z hlediska očekávaného dalšího vzájemného ovlivňování práva a moderních informačních technologií to je pouze prvním krokem. *Potřebujeme zevrubnou analýzu našeho právního řádu z hlediska těchto moderních technologií*; je totiž třeba nejen vytvořit zákony nové, ale provést

především revizi stávajících zákonů z hlediska přípustnosti duality papírové a elektronické formy, z hlediska procesních forem umožňujících elektronické (a dálkové) zpracování. Nynější legislativní situace je bohužel v tomto směru inertní. Podle technické vyspělosti předkladatele navrhovaný zákon buď „nepapírová“ média bere na vědomí, nebo ne. V právních normách se stále setkáváme s používáním pojmů, které nejsou zcela správné z hlediska právního, ale i věcného nebo - což je nejčastější - jsou používány bez hlubšího zamyšlení různé termíny, které nejsou ani homonymy ani synonymy a jejich použití má přitom zcela odlišné konkrétní dopady[55]. [83] Méně technologické závislosti a standardnější terminologie v našich právních předpisech zvýší právní jistotu všech subjektů, zvýší efektivnost orgánů činných v trestním řízení nebo správních orgánů a přispěje i ke zkvalitnění rozhodovací praxe soudů.

Moderní technologie dávají nejdříve křídla pachatelům trestné činnosti, komplikují život přece jen konzervativněji postupujícím orgánům v trestním řízení a teprve o hodně později se tyto technologie stávají vydatným pomocníkem v boji proti zločinu. Snahou všech zúčastněných odborníků by mělo být co největší zkrácení odstupu mezi „zloději“ a „četníky“ na poli informačních technologií.

VI. Literatura

[1] Pravděpodobné modely organizované kriminality. 8. Konference OSN, Havana, 27. 8. -7. 7. 1990. Vydal Institut pro kriminologii a sociální prevenci, Praha 1994

[2] Smejkal, V.: Filipika proti Internetu.CHIP, č. 1-2/1997

[3] Smejkal, V.: Pohled na Internet z jiné strany. Mezinárodní konference „Internet a telekomunikace v České republice“, Praha 22. -23. 4. 1997

[4] Telec, I. : Šíření děl a výkonů v telekomunikačních sítích, zvláště v Internetu. Právní rozhledy, č. 4/1997, s. 179-182

[5] Smejkal, V.: Právní aspekty Internetu a jeho bezpečnosti. Konference AFOI '97 „Internet a informační bezpečnost“, Praha 25. 2. 1997

[6] Novák, L.: Bezpečnost a Internet - management a technologie. Tamtéž.

[7] Dočkal, J.: Bezpečné klíče a platby v Internetu. Tamtéž.

[8] Burkert, H.: Internet und Recht. Seminář „Internet und Recht“, St. Gallen, Švýcarsko 19. 7. 1996

[9] Zlatuška, J.: Počítače, jejich užití či zneužití. Zpravodaj ÚVT MU, Brno, 1997

[10] Parker, D. B.: Crime by Computer. New York 1976

[11] Computer Crime. Sborník U. S. Department of Justice, Washington 1979

[12] Boček, O.: Trestné činy spáchané pomocí počítače, expertíza ÚSP ČSAV, 1988

[13] Vlček, M.: Počítače a kriminalita (trestněprávní a kriminologické aspekty), Academia, Praha 1989

[14] Smejkal, V., Vlček, M.: Trestná činnost a počítače. Právník, č. 8-9/1988, s. 721-729

[15] Smejkal, V. Sokol, T., Vlček, M.: Počítačové právo. Praha, C. H. Beck 1995, 220 str.

[16] Smejkal, V.: Jak postupovat při vyšetřování počítačové kriminality; Sborník Právní prostředky proti softwarovému pirátství v ČSFR, Praha, 19. 10. 1992, s. 20-27

[17] Smejkal, V.: Metodika domovních prohlídek s prvkem výpočetní techniky, Odborná sdělení Kriminalistického ústavu, č. 5/1994, s. 1-8

[18] Knap, K.: Autorský zákon a předpisy související. Komentář, 4. vydání, Linde, Praha 1993

[19] Knap, K., Opltová, M.: Ochrana programu počítače v právu československém a zahraničním, Právny obzor, č. 10/1981

[20] Knap, K., Opltová, M., Kříž J., Růžička, M.: Práva k nehmotným statkům. Codex, Praha 1994

[21] Boháček, M., Loebl, Z.: Právní ochrana software v novele čs. autorského zákona, Softwarové noviny, č. 3, 1990

[22] Loebl, Z.: Computer Law in Central and Eastern Europe and Czech Republic. In:European Computer Law. Information Technology Law Group/Europe. Transnational Publishers Inc., New York 1995

[23] Telec, I. : Tvůrčí práva duševního vlastnictví. MU - Doplněk, Brno 1994

[24] Telec, I. : Autorský zákon a předpisy související. C. H. Beck, Praha 1995

[25] Telec, I. : Autorský zákon - komentář. C. H. Beck, Praha 1997

[26] Jechoutek, J., Hlaváček, J.: Naše představy o koncepci pracoviště počítačové kriminality Kriminalistického ústavu Praha. Odborná sdělení Kriminalistického ústavu, Praha, č. 1-2, 1993, s. 10-14

[27] Kriminalistická problematika při odhalování, vyšetřování a prevenci počítačové kriminality. Sborník odborných sdělení ze semináře uskutečněného na PA ČR dne 23. 12. 1996. Katedra kriminalistiky PA ČR, Praha 1997

[28] Smejkal, V.: Systémový přístup k ochraně dat a výpočetní techniky, Sborník semináře SpK „Ochrana výpočetní techniky a dat, počítačová kriminalita“, Praha, 8. 11. a 13. 12. 1990, s. 59-64

[29] Mates, P.: K některým otázkám provozování informačních systémů, Právní rozhledy, č. 4/1994, s. 110 a násl.

[30] Mates, P.: K některým problémům právní úpravy vedení informačních systémů ve státní správě. Právní praxe v podnikání, č. 9/1995, s. 18

[31] Mates, P., Matoušová, M.: Evidence, informace, systémy - právní úprava. CODEX BOHEMIA, Praha 1997

[32] Maštalka, J.: Jak dále při ochraně osobních údajů v informačních systémech. Obchodní právo, č. 3/1994, s. 10

[33] Smejkal, V.: K problematice počítačové kriminality, Kriminalistický sborník, č. 6-7/1990, s. 266-270

[34] Smejkal, V., Sokol, T.: Počítačová kriminalita a její trestně právní aspekty, Právo a podnikání, 1/1993 s. 24-29

[35] Icove, D., Seger, K., Von Storch, W.: Computer Crime. A Crimefighter's Handbook. O'Reilly & Associates, Inc., Sebastopol, CA, USA 1995

[36] Raubenheimer, A.:Germany Law. In: European Computer Law. Information Technology Law Group/Europe. Transnational Publishers Inc., New York 1995

[37] Neff, E. F.: Switzerland Computer Law. In: European Computer Law. Information Technology Law Group/Europe. Transnational Publishers Inc., New York 1995

[38] Smejkal, V.: Bankovní loupeže a počítačová kriminalita v České republice, Seminář Kontrola informačních systémů a počítačová kriminalita (Českobritská-irská účetní asociace), Praha, 25. 5. 1995, s. 13-19

[39] International review of criminal policy - United Nations Manual on the prevention and control of computer-related crime, **http://www.ifs.univie.ac.at/~pr2gq1/rev4344.html#crime**

[40] Morris, R. N.: Secret Service develops examination techniques for cards. IACCI NEWS, vol. 126, 1. Q. 1993. Překlad S. Machálka, KÚ P-ČR

[41] Kunzl, J., Smejkal, V.: Bankovní počítačová kriminalita v České republice. Mezinárodní konference INSIG (International Seminar „Security in Banking“), Paříž, 27-30. 1. 1997

[42] Šámal, P., Púry, F., Rizman, S.: Trestní zákon - Komentář. 2. vydání, C. H. Beck, Praha 1995

[43] Sardi, A.: Vnitřní bankovní audit. HZ, Praha 1996

[44] Raffegeau, J., Dufils, P., de Ménonville, D.: Finanční audit. HZ, Praha 1996

[45] Zákon č. 35/1965 Sb., o dílech literárních, vědeckých a uměleckých (autorský zákon) v platném znění

[46] Scheinost, M.: Tři sondy k problematice organizovaného zločinu. IKSP, Praha 1995

[47] Kadeřabíková, D.: Hospodářská kriminalita ve finanční oblasti. IKSP, Praha 1995

[48] Cejp, M.: Druhy a formy činností organizovaného zločinu. IKSP, Praha 1996

[49] Budka, I. : Organizovaná kriminalita v ČR a v USA - kriminologické a právní aspekty. IKSP, Praha 1996

[50] Smejkal, V.: Duševní vlastnictví, nehmotný majetek a jejich význam v podnikání. Sborník prací FP VUT, Brno 1997

[51] Směrnice Evropské unie o právní ochraně počítačových programů ze dne 14 5. 1991. (Council Directive 91/250 on the legal protection of computer programs, O. J. L122/42)

[52] Směrnice Evropské unie o právní ochraně databází ze dne 11. 3. 1996. (Council Directive 96/9 on the legal protection of databases, O. J. L77/20)

[53] Smejkal, V., Sokol, T.: Bude novelizován autorský zákon? CHIP, č. 11/1995, s. 34-36

[54] Smejkal, V.: Novela Autorského zákona přináší určité rozpaky (I), Hospodářské noviny, 17. 4. 1996, s. 13; Plus i minus Autorského zákona (II), Hospodářské noviny, 7. 5. 1996, s. 11

[55] Smejkal, V.: Novela Autorského zákona - jen malý krůček pro lidstvo. Softwarové noviny, č. 9/1996, s. 106-110

[56] Vlček, M.: Poznámky nikoliv na okraj. Softwarové noviny, č. 9/1996, s. 112-113

[57] Knap, K. a kol.: Autorský zákon a předpisy související - komentář. 5. Podstatně přepracované a doplněné vydání. Linde, Praha 1996

[58] Doporučený výkladový slovník ASŘ, INORGA, Praha 1979

[59] Veselý, J.: Systémové nástroje řízení, IŘ, 1982, s. 302

[60] Hajn, P.: Program - paklíč. IHVS, č. 1, 1995, s. 59-67

[61] Sokol, T., Smejkal, V.: Paklíče na software. CHIP, č. 10/1995, s.58-59 a Konkrétní paklíče a hypotetický soudní spor. CHIP, č. 1/1996, s. 30-34

[62] Mates, P.: K povaze záznamů do informačních systémů ve veřejné správě. Právní rozhledy, č. 3/1997, s. 117-122

[63] Švestka, J., Knap, K. a kol.: Ochrana osobnosti. 3. přepracované a doplněné vydání. Linde, Praha 1996

[64] Úmluva na ochranu osob se zřetelem na automatizované zpracování osobních údajů, č. 108, Rada Evropy, Štrasburk, 28. 1. 1981

[65] De Bellefonds, X. L.: L'Informatique et le droit. Presses Universitaires de France, Paris, 1992

[66] kol.: Legislación de datos de carácter personal. Tecnos, Madrid 1966

[67] 56. Spolkový zákon z 18. října 1978 o ochraně osobních dat (DSG SRN), 1978/565 v platném znění

[68] Kodl, J, Smejkal, V., Sokol, T.: Šifry, státní zájmy a lidská práva. CHIP, č. 4/1995, s. 34-36 a Smíme šifrovat? CHIP, č. 5/1995, s. 30-32

[69] Smejkal, V., Sokol, T.: V zajetí Sítě (Fenomén Internetu I.), CHIP, č. 6/1996, s.44-45 a Po hlavě do brouzdaliště (Fenomén Internetu II.). CHIP č. 8/1996, s. 36-39

[70] Smejkal, V., Sokol, T.: Podpisy na papíru a digitální podpisy. CHIP, č. 12/1996

[71] Mates, P., Smejkal, V.: Ochrana osobních dat. CHIP, č. 1/1997, s. 26-27

[72] Smejkal, V.: Současný stav počítačové kriminality, jejího odhalování, vyšetřování a pravence proti ní. Habilitační práce. FI MU, Brno, 1997

[73] Zákon upravující rámcové podmínky pro informační a komunikační služby (zákon o informačních a komunikačních službách, něm. Informations- und Kommunikationsdienste-Gesetz-InKDg) ze dne 22. července 1997, Spolkový sněm SRN.

[74] Porada, V., Konrád, Z.: Metodika vyšetřování počítačové kriminality. Katedra kriminalistiky PA ČR, Praha, 1998

[75] Smejkal, V.: Internet@§ § § (Internet a paragrafy). GRADA, Praha 1999

[76] Smejkal, V.: Ach ten Internet... CHIP, 1999, č. 8, s. 36-39

[77] Směrnice č. 95/46/EC Evropského parlamentu a Rady o ochraně jednotlivců ve vztahu ke zpracování osobních dat a o volném pohybu těchto dat (Directive of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281)

[78] Směrnice č. 97/66/EC Evropského parlamentu a Rady o zpracování osobních dat a o ochraně soukromí v sektoru telekomunikací (Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ L 024)

[79] Doporučení Rady Evropy R (87)15 Výboru ministrů členských států o používání osobních dat v policejním sektoru z roku 1987

[80] Doporučení Rady Evropy č. 87/54/EEC o právní ochraně topografií polovodičových výrobků (Council Directive of 16 December 1986 on the legal protection of topographies of semiconductor products, OJ L 024)

[81] Smejkal, V., Sokol, T.: Trocha historie, trocha prognóz. CHIP, 4/1999, s. 52-56

[82] Smejkal, V., Vlček, M.: Freeware, shareware a free software. CHIP, 12/1999, v tisku.

[83] Mates, P., Smejkal, V.: Dokumenty budoucnosti. Data Security Magazin, II, 1998, č. 5, s. 34-37

[84] Mates, P., Smejkal, V.: Internet - síť sítí očima práva. Právní rádce, 2/1999, s. 45

[85] Směrnice Rady Evropy č. 93/83/EEC z 27. 9. 1993 pro koordinaci některých otázek týkajících se copyrightu a práv vztahujících se k copyrightu při satelitním vysílání a kabelovém přenosu (Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission, OJ L 248)

[86] Smejkal, V.: Ach ten Internet. CHIP, 8/1999, s. 36-39

[87] Rosenoer, J.: CyberLaw. The Law of the Internet. Springer Verlag 1997

[88] Návrh č. 98/0191 (COD) směrnice Evropského parlamentu a Rady o společném rámci pro elektronické podpisy ze dne 16. července 1999 (Directive 1999//EC of the European Parliament and of the Council of on a Community framework for electronic signatures)

---

* Autor je soudním znalcem, docentem Masarykovy university v Brně a působí rovněž na dalších vysokých školách v Praze, Brně a Olomouci.

1 Čísla v hranatých závorkách označují odkazy na literaturu uvedenou v kap. VI.

2 Viz také [33], [34].

3 I když se ojevují počítačová specifika také v jiných ustanoveních TrZ - např. v § 124c/2 a 124f/2, § 125 TrZ.

4 Autorovi není známo konečné řešení tohoto případu, podle neověřených informací byl pachatel odsouzen k podmíněnému trestu, který podléhal amnestii.

5 „Kdo si neoprávněně opatří nepřenosnou platební kartu jiného, identifikovatelnou podle jména nebo čísla, nebo předmět způsobilý plnit její funkci, bude potrestán odnětím svobody až na dvě léta, nebo peněžitým trestem nebo propadnutím věci.“

6 Nepříliš dlouho poté, co bylo ve snaze o zjednodušování TrZ a odstraňování speciálních skutkových podstat vypuštěno ustanovení § 209a - Neoprávněné užívání cizího motorového vozidla (zařazené v roce 1969, vypuštěné v roce 1990).

7 „Přestupku se dopustí ten, kdo neoprávněně zhotoví reprodukci nebo zaměnitelnou napodobeninu bankovky, mince, šeku, cenného papíru nebo platební karty znějící na tuzemskou nebo cizí měnu anebo neoprávněně zhotoví předmět úpravou napodobující bankovku, minci, šek, cenný papír nebo platební kartu.“

8 Což jinak vynikající komentář *Šámal, P., Púry F., Rizman, S.:* Trestní zákon - Komentář. 2. vydání, C. H. Beck, Praha 1995 neřeší.

9 Jednotliví autoři udávají poměr odhalených a oznámených případů ku nikdy nezjištěným od 1:1 000 až po šokujících 1: 20 000.

10 Se zvýšeným rizikem v podobě homebankingu nebo připojení na Internet.

11 Otřesy státního zřízení v Albánii v důsledku těchto pyramid jsou důkazem, že v méně vyspělých zemích mohou letadla představovat skutečnou hrozbu.

12 Po novele zákonem č. 253/1997 Sb. účinné od 1. 1. 1998.

13 Zákon č. 35/1965 Sb., autorský zákon, ve znění pozdějších předpisů.

14 Snad nejmarkantnějším případem, se kterým jsem se setkal, byl případ, kdy konstruktérská divize velkého a významného podniku měla na cca 10 počítačích neoprávněně nainstalován program pro projektování AutoCAD, v celkovém objemu pořizovacích cen přes jeden milión korun.

15 V tomto duchu odkazuji na publikace I. Telece a vlastní články, např. [53], [54], [55] a nově zejména [76].

16 § 3 odst. 1 TrZ.

17 § 3 odst. 2 TrZ.

18 § 3 odst. 4 TrZ.

19 § 3 odst. 3 TrZ.

20 S tímto, podle mého názoru mylným přístupem, se setkávám u vyšetřovatelů Policie ČR, kteří v tomto smyslu často podléhají argumentaci obhájců obviněných.

21 Podle mých informací došlo v několika posledních případech k zastavení trestního stíhání podle ust. § 172/1/c TrŘ, tedy protože nebylo prokázáno, že skutek spáchal obviněný, resp. nebyl původce nainstalovaných počítačových programů v určitých firmách zjištěn a vyšetřovatelé se nezajímali o případnou trestní odpovědnost osob odpovědných za provoz výpočetní techniky či za celou organizaci (statutárních zástupců), případně akceptovali argumentaci obhájců obviněných, že software byl sice nainstalován, ale nebyl používán.

22 Viz např. *Smejkal, V.:* Legislativa na rozcestí. CHIP, 1999, č. 7.

23 Viz také rozhodnutí NS Zm I 614/24 (č. 1945/25 Sb.) „ Adresáře požívají ochrany práva původského, nejsou-li jen mechanickou snůškou adres, nýbrž projevuje-li se v jejich uspořádání dle určitých zásad a hledisek duševní činnost redakční (systematika).“

24 Autor nebezpečného viru Melissa, jenž způsobil zahlcení mnoha mail serverů po celém světě, kterým má být David L. Smith z USA, byl zatčen FBI. Žaloba zní na čtyři trestné činy podle federálních zákonů.

25 Za předpokladu splnění podmínek podle § 7 TrZ.

26 Zde opět přichází v úvahu již zmíněný postih podle § 125 TrZ.

27 Jen jako poznámka na okraj: řada IS o osobách provozovaných státem, a to zejména MV ČR, nemá doposud zákonnou oporu ve smyslu tohoto ustanovení; snad nejmarkantnějším příkladem je Centrální registr obyvatelstva.

28 Autorovi se nepodařilo zjistit, zda nedošlo k trestnému činu vyzvídání nebo vyzrazení státního tajemství podle ust. § 105 a 106 TrZ, protože příslušný útvar MV nebyl schopen sdělit, zda některé údaje byly či nebyly předmětem státního tajemství.

29 *Smejkal, V., Sokol, T, Vlček, M.:* Počítačové právo. Praha, C. H. Beck 1993, s. 182 a násl.

30 Příkladem může být známá aféra týkající se II. vlny kupónové privatizace, kdy podle mých informací docházelo pravděpodobně k ovlivňování průběhu počítačového zpracování některých kol kupónové privatizace.

31 Obdobně to platí samozřejmě také např. pokud jde o přestupek proti veřejnému pořádku podle § 47 odst. 1 písm. c) zákona o přestupcích, jehož se dopouští ten, kdo vzbudí veřejné pohoršení.

32 Podle § 89 odst. 4 TrZ.

33 Viz ust. § 260 a 261 TrZ.

34 Na Internet se tento právní předpis nepochybně vztahuje, neboť podle § 1 odst. 2 „Komunikačními médii se pro účely tohoto zákona rozumí televize, rozhlas, nosiče audiovizuálních děl, periodický tisk a neperiodické publikace, dopravní prostředky, plakáty a letáky, jakož i další komunikační prostředky umožňující přenos informací.“

35 Podobně je to třeba stanovení hranice pro přístupnost audiovizuálního díla šířeného Internetem, a to podle ust. § 4 odst. 3 zákona č. 273/1993 Sb., o některých podmínkách výroby, šíření a archivování audiovizuálních děl, ve znění pozdějších předpisů.

36 „Kdo uvádí do oběhu, rozšiřuje, činí veřejně přístupnými... zobrazení nebo jiné předměty ohrožující mravnost, v nichž se projevuje neúcta k člověku nebo násilí, nebo která zobrazují sexuální styk s dítětem, se zvířetem nebo jiné sexuálně patologické praktiky, bude potrestán odnětím svobody...“

37 V případě z počátku roku 1999, kdy se jednalo o dětskou pornografii umístěnou na serveru kalifornského poskytovatele prostoru pro soukromé nástěnky XOOM pravděpodobně českým občanem, jde zcela zřejmě o případ, kdy obsah schránky porušuje zákon ve více zemích - v zemi, kde je server umístěn, i u nás, ale i jinde. V uvažovaném případě by mělo být pachateli, bude-li zjištěn, sděleno obvinění u nás, pro trestný čin, který je sice technicky realizován na území jiného státu, ale škodlivý následek nastává v ČR.

38 Jiným dopravním zařízením se rozumí např. kurýrní služba.

39 Viz *Šámal, P., Púry, F., Rizman, S.:* Trestní zákon - komentář. 2. vyd., C. H. Beck, Praha 1995, s. 852.

40 Jednotnou telekomunikační síť podle zákona o telekomunikacích č. 110/1964 Sb., ve znění pozdějších předpisů.

41 Viz také zákon č. 110/1964 Sb., o telekomunikacích, Oddíl VIII - Telekomunikační tajemství, § 20.

42 Zákon č. 97/1974 Sb., ve znění pozdějších předpisů.

43 Podle zákona č. 148/1998 Sb.

44 Viz také judikát Nejvyššího soudu ČSR - Kr II 172/22 (z roku 1922), který říká: „Protiprávním otevřením dopisu není míněno pouhé mechanické otevření dopisu, nýbrž další protiprávní použití jej od okamžiku, kdy osoba čtoucí dopis nabyla vědomostí, že dopis jí nenáleží. Jen vrácením dopisu adresátu nebo odesilateli bez jakéhokoliv vlastního použití jeho obsahu lze se uvarovati trestu. Delikt sám se skládá z protiprávního otevření dopisu a z úmyslného porušení listovního tajemství, kterážto poslednější náležitost časově následovati musí prvější, a kteroužto jedině zákon chce míti chráněnou."

45 Viz např. *Smejkal, V., Sokol, T.:* Poštovní tajemství v Internetu. CHIP, č. 4/1997, s. 30-34.

46 „Kdo o jiném sdělí nepravdivý údaj, který je způsobilý značnou měrou ohrozit jeho vážnost u spoluobčanů, zejména poškodit jej v zaměstnání, narušit jeho rodinné vztahy nebo způsobit mu jinou vážnou újmu, bude potrestán odnětím svobody až na jeden rok. (2) Odnětím svobody až na dvě léta nebo zákazem činnosti bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 tiskem. filmem, televizí nebo jiným obdobně účinným způsobem."

47 Např. zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů, § 38 a násl., § 21/2 a § 22 zákona České národní rady č. 280/1992 Sb., o resortních, oborových podnikových a dalších zdravotních pojišťovnách, ve znění pozdějších předpisů, § 24/1 zákona České národní rady č. 185/1991 Sb., o pojišťovnictví, ve znění pozdějších předpisů, § 38/2 zákona č. 42/1994 Sb., o penzijním připojištění se státním příspěvkem a o změnách některých zákonů souvisejících s jeho zavedením ve znění pozdějších předpisů apod.

48 Podle § 16 zákona č. 256/1992 Sb.

49 Podle § 18-22 zákona č. 256/1992 Sb.

50 Podle § 20 zákona č. 256/1992 Sb.

51 Zákon č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů.

52 Nemusí tomu být tak vždy, jak ukázal případ ze září 1999, kdy pachatel, který odcizil osobní údaje klientů České spořitelny a následně tuto spořitelnu vydíral, byl vypátrán a odhalen i díky informacím ze sítí Internet.

53 Viz LZPS, čl. 7, 10 a 13.

54 Každý, kdo hodlá zpracovávat osobní údaje bude povinen oznámit tuto skutečnost Úřadu pro ochranu osobních údajů, který oznámení buď zaregistruje nebo rozhodne, že se zpracování nepovoluje. Ti, kdo již v současné době osobní údaje zpracovávají, se budou muset zaregistrovat do šesti měsíců po nabytí účinnosti zákona.

55 Příkladem může být prakticky libovolné používání a zaměňování pojmů „dokument“, „listina“, „doklad“, „záznam“ apod.