Analýza současného stavu a trendů vývoje trestné činnosti na úseku informačních technologií a internetu včetně návrhu řešení

1. Úvod

Předkládanou analýzu vypracoval odbor bezpečnostní politiky ministerstva vnitra. Vycházel z podkladů od Policie ČR a dalších odborných útvarů ministerstva vnitra. Ministerstvo vnitra současně požádalo o zpracování analogické analýzy soudního znalce a konzultanta v oblasti výpočetní technika – ochrana dat a počítačová kriminalita, autorské a počítačové právo Vladimíra Smejkala. Z jeho práce ”Informační a počítačová kriminalita v České republice”, vypracované v roce 1999, je na několika místech textu citováno, přičemž citovaný text je označen kurzívou.

1.1 Vymezení trestné činnosti na úseku informačních technologií

Definice počítačové kriminality se mění s vývojem technologií a změnami možností výpočetní techniky jako takové. 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 jako předmět této trestné činnosti, ovšem s výjimkou* majetkové *trestné činnosti, nebo jako nástroj trestné činnosti*.

V poslední době se prosazuje spíše termín informační kriminalita*, zvláště pokud se chce zdůraznit, že trestný čin má vztah k software, k datům, resp. uloženým informacím,* nebo šířeji k informačním technologiím. Důvodem tohoto

posunu je prolínání výpočetní techniky s komunikačními technologiemi a nabalování dalších aktivit na dosud poměrně úzce vymezenou oblast výpočetní techniky. Tím dochází k vytváření kompaktnějšího systému, kdy se do informační kriminality zahrnuje oblast výpočetní techniky, komunikačních technologií a další technicky vyspělá odvětví jako například elektronické platební prostředky. Z tohoto důvodu je v této analýze také používáno pojmu informační kriminalita. V mezinárodním společenství jsou také často používány pojmy ”kyberzločin” (”Cyber-Crime”) nebo ”high-tech” zločin.

Z hlediska trestního práva již v minulých letech došlo k vymezení, kdy se jako počítačová respektive informační kriminalita nechápe taková trestná činnost, která je zaměřená na techniku jako objekt zájmu pachatele majetkového trestného činu (například krádež počítače). Pochopitelně může docházet a dochází k prolínání, kdy je výpočetní a jiná technika objektem zájmu ryze ”počítačového” trestného činu, ale současné poškození této techniky vede k souběhu s majetkovým trestným činem (např. v případě, kdy počítačový vir způsobí poškození hardwaru).

S bojem proti informační kriminalitě souvisí i takové činnosti bezpečnostních složek, které vedou k odhalení pachatele trestné činnosti, která informační kriminalitou není. Jedná se především o běžné trestné činy, jejichž pachatelé užívají výpočetní techniky jako nástroj spáchání trestného činu, který by mohli spáchat i jiným způsobem, ale v konkrétním případě jeho spáchání výpočetní techniku vyžaduje (např. když zločinci spolu komunikují o připravovaném trestném činu prostřednictvím počítačových sítí, nebo tehdy, je-li internet použit jako médium verbální kriminality). Součástí předkládané analýzy je proto i rozbor problémů spojených s činností policie při odhalování kriminality, jejíž pachatelé využívají informačních technologií jako prostředků komunikace nebo jako nástroje spáchání činu.

1.2 Předpoklady rozvoje kriminality v oblasti informačních technologií

Počítačová a související kriminalita se stává fenoménem konce dvacátého století a je možno předpokládat, že v 21. století bude následovat její další prudký rozvoj. Souvisí to především se značným rozšířením výpočetní techniky

v ekonomice, v prudkém růstu jejího užívání v domácnostech a zejména v rozvoji počítačových sítí a zvláště internetu. Počet uživatelů internetu v ČR v roce 2000 je některými odborníky odhadován až na 1,2 – 1,3 milionu, jiné údaje ale uvádějí jen čtvrtinu uvedeného čísla (292 tisíc, z toho 139 tisíc studentů). Podle výzkumu Sondy do českého internetu, bylo v průběhu března 2000 alespoň jednou na minimálně jednom ze 24 sledovaných předních českých serverů identifikováno 1 163 511 unikátních návštěvníků serverů. Podrobnější analýza tohoto zjištění vyloučila přístupy ze zahraničí a dospěla k závěru, že českých uživatelů internetu bylo na sledovaných webových stránkách zaznamenáno 973 650, což je přibližně 84 % celkového počtu. Zdá se tedy, že přibližně 10 % obyvatelstva ČR nějak užívá internet. Ve vyspělých státech je přirozeně tento počet výrazně vyšší. Počet uživatelů internetu v USA je odhadován na 59%, v Kanadě 56 %, Švédsku 53 %, Austrálii 48 %, Švýcarsku 45 %, Japonsku 33 %, Velké Británii 33 %, Německu 29 %, Francii 22 % a Polsku 11 % (údaj pro Polsko dobře koresponduje s uvedeným odhadem pro ČR), celkem 300 milionů uživatelů ve světě (v polovině roku 2000). V následujících letech je očekáván prudký růst ve světě (a pravděpodobně i u nás). Ve světě má vzrůst počet uživatelů internetu do roku 2005 na 1 miliardu. V České republice je do roku 2003 odhadován roční přírůstek minimálně na 30 %, a skutečnost může být i výrazně vyšší, stačí si připomenout, jakým způsobem v poslední době překonával všechny odhady skutečný růst počtu mobilních telefonů. V podnikové sféře je vzrůst počtu používaných počítačů ještě výraznější než v soukromé sféře. Podle výzkumu provedeného v závěru roku 1999 u 609 podniků s více než 25 zaměstnanci, využívá internet 91 % podniků. V roce 1997 bylo připojeno 43 % podniků a v r. 1995 jen 4 %!

1.3 Rozdělení kriminality v oblasti informačních technologií

1.3.1 Rozdělení používané v mezinárodních dokumentech

V návrhu mezinárodní dohody o kyberzločinu, který vypracovala Rada Evropy, jsou trestné činy rozděleny následovně:

1. zločiny proti důvěrnosti, integritě a dosažitelnosti počítačových dat a systémů, které se dále dělí na:

- nezákonný přístup,
- nezákonné odposlouchávání,
- narušování dat,
- narušování systémů,
- zneužití prostředků,

2. zločiny se vztahem k počítači, které jsou děleny na
   - počítačové padělání a
   - počítačový podvod,
3. zločiny se vztahem k obsahu počítače, což je především dětská pornografie,
4. zločiny se vztahem k autorským nebo obdobným právům.

V akčním plánu *e*Europe 2002, který předložila Evropská unie, jsou počítačové zločiny rozděleny na:

1. zločiny porušující soukromí (ilegální sbírání, uchovávání, modifikace, zveřejňování a šíření osobních dat),
2. zločiny se vztahem k obsahu počítače (pornografie, zvláště dětská, rasismus, vyzývání k násilí apod.),
3. ekonomické (neautorizovaný přístup a sabotáž, hackerství, šíření virů, počítačová špionáž, počítačové padělání a podvody apod.),
4. zločiny se vztahem k duševnímu vlastnictví (autorské právo apod.).

1.3.2 Rozdělení podle společenského významu chráněných zájmů a připravenosti státních orgánů bojovat s příslušným typem kriminality

Vezmeme-li v úvahu současné chápání společenského význam jednotlivých zákonem chráněných zájmů a aktuální připravenost státních orgánů na jejich chránění, lze stanovit následující rozdělení kriminality v oblasti informačních technologií.

1. V současné době je největší pozornost věnována problému porušování autorského práva. Uvádí se, že 50 – 80% softwaru v ČR je používáno ilegálně. Uváděná čísla je však třeba brát jen jako hrubé odhady, odvozené buď ze

sociologických výzkumů nebo z porovnání přibližného počtu užívaných počítačů (= odhad počtu prodaných kompletních počítačů dosud používaných + odhad počtu dodatečně zkompletovaných počítačů) s počtem prodaných licencí na software. Tyto odhady jsou s vysokou pravděpodobností navíc často ovlivněné obchodním, politickým nebo jiným zájmem svých autorů.

Vyšší údaje jsou uváděny u nekomerčního softwaru a u starších počítačů, nižší u komerčního softwaru a nově kupovaných počítačů (mnoho nových počítačů se např. prodává i s nainstalovaným operačním systémem). Podle údajů mezinárodní organizace BSA (Busines Software Alliance) bylo v roce 1999 v ČR 42 % komerčního softwaru ilegálního (pro rok 2000 je předběžně uváděna hodnota 39 %). Je poučné srovnat tento údaj s analogickými údaji pro Maďarsko (52 %), Polsko (60 %), s průměrem střední a východní Evropy (70 %) a průměrem západní Evropy v roce 1999 (34 %) (Velká Británie 26 %, Německo 27 %, Rakousko 36 %, Francie 39 %, ale Holandsko 44 %, Portugalsko 47 %, Irsko 51 %, Španělsko 53 % a Řecko 71 %) a v roce 1996 (53 %). ČR je v množství ilegálního komerčního softwaru na stejné úrovni, na které byl průměr států západní Evropy asi před 4 roky. Odhady množství ilegálního nekomerčního softwaru BSA do roku 1999 neuváděla. V předběžných číslech pro rok 2000 je však uvedena hodnota 81 % pro množství ilegálního ”zábavného” (”entertainment”) softwaru. I když tyto hodnoty nemohou být nikdy zcela přesné a jsou nepochybně ovlivněné různými obchodními a politickými zájmy, porušování autorského práva v České republice je zcela jistě značné a má negativní dopady na politickou i ekonomickou situaci ČR i její postavení ve světě. Na druhou stranu se podle údajů BSA zdá, že množství ilegálního komerčního softwaru v ČR je nejmenší ze zemí střední a východní Evropy a ČR je v tomto ohledu dokonce lepší než některé státy EU.

2. Na druhém místě je u nás zatím problém narušování informačních systémů tzv. hackingem, při němž dochází k průnikům do počítačových sítí a k neoprávněnému čtení, úpravě nebo destrukci dat. Jednotlivé případy jsou značně různorodé, mají různé motivy[1] (vzrušení, zábava, náprava, ale i pomsta a peněžní zisk) a způsobená škoda může být někdy zanedbatelná, jindy naopak značná. Do

[1] *Psychologickému profilu pachatelů počítačových zločinů by měla být v kriminologických výzkumech věnována větší pozornost, neboť může být důležitou částí informací o uskutečněných či chystaných zločinech.*

současnosti byla v ČR většina útoků škodlivá poměrně málo a většinou se jednalo jen o pozměnění webových stránek. Druh napadnutých subjektů je značně různorodý a obsahuje na jedné straně gymnázium v Uherském Hradišti či základní školu v Anežské ulici 10, na druhé straně profesionální počítačové firmy (časopis Chip, české zastoupení Sun Microsystems), ministerstva (vnitra) nebo politické strany (KSČM). Nejznámější český (a také slovenský) hacker (nebo spíše hackeři) je znám pod jménem CzERT. Jemu se již podařilo pozměnit stránky ministerstva zdravotnictví (úpravou na stránky ”Ministerstva smrti Čínské republiky”), Armády ČR (neslušné obrázky), Union banky (úpravou na Ruin banka) a nejnavštěvovanější (a také velmi profesionálně vedené a proto obtížně napadnutelné) stránky vyhledávače Seznam. Způsobená škoda závisí na způsobu využívání webových stránek. Minimální škodu způsobí hackerův útok škole, která na svých stránkách vystavuje pouze základní informace o sobě, a poškozené stránky může snadno nahradit. Značnou škodu naopak může způsobit poškození stránek komerční firmy, která prostřednictvím internetu přijímá objednávky svých výrobků, či ministerstva, které na svých stránkách podává obyvatelstvu důležité informace.

3. Specifickou a vysoce nebezpečnou kriminalitou je využívání informačních technologií k praní špinavých peněz a jiným formám finanční kriminality. Internet bude v blízké budoucnosti umožňovat rychlé provedení finančních operací v prakticky libovolném množství v průběhu velmi krátké doby. Zahraniční experti předpokládají, že zločinecké skupiny vybavené profesionálním vybavením a vysoce kvalifikovanými odborníky mohou takovýmto způsobem získat možnost účinnou formou eliminovat snahy států v boji proti organizovanému zločinu a praní špinavých peněz.

4. Dalším typem kriminality v oblasti informačních technologií je využívání internetu ke grafické a verbální kriminalitě – zveřejňování návodů k násilné trestné činnosti (návody na výrobu výbušnin, zbraní apod.), dále k páchání mravnostní kriminality (dětská pornografie) nebo verbální kriminality (extremismus, vyhrožování).

1.3.3 Podle kriminalisticko taktických hledisek

V současnosti je možno z kriminalistického hlediska provést základní dělení informační kriminality takto:

1. porušování autorského práva – počítačové pirátství (§ 152 tr. zák.),
2. poškození a zneužití záznamu na nosiči informací (§ 257a tr. zák.), a to jako
   - útok z vnějšku subjektu,
   - útok zevnitř subjektu,
   - útoky kombinované (z vnějšku i zevnitř),
3. ostatní počítačová, resp. ”informační” trestná činnost, tj. trestné činy, které výpočetní techniku využívají jako prostředek k páchání trestných činů, nikoliv jako přímý objekt zájmu pachatele, i když není vyloučeno, že objektem zájmu mohou být počítačová data.

1.4 Struktura boje s informační kriminalitou

Aby mohl být boj s informační kriminalitou úspěšný, je třeba vyřešit případné problémy především ve třech hlavních oblastech:

1. v oblasti legislativní,
2. v oblasti organizačně-personální a v
3. oblasti technické.

Zákony by měly zejména:

- zahrnout všechny formy příslušné kriminality,
- stanovit přiměřené postihy a
- být koordinovány na mezinárodní úrovni.

Informační kriminalitu mohou (vzhledem k její specifičnosti) řešit pouze trvale pracující nadrezortní týmy, složené z jednotlivců, kteří

- dané problematice velmi dobře rozumí,
- jsou přiměřeně technicky vybaveni,
- jsou schopni identifikovat (potenciální i aktuální) trestný čin a zajistit

odpovídající důkazy,

- jsou schopni identifikovat pachatele a zadržet ho či zprostředkovat jeho zadržení,
- jsou schopni spolupracovat s nestátní sférou i v rámci samotné státní sféry,
- jsou schopni spolupracovat se zahraničními partnery.

Technický aspekt informační kriminality zahrnuje především vlastnosti používaného softwaru, zvláště jeho odolnost proti zavirování, možnosti šifrovat a dešifrovat komunikaci, možnosti využívat anonymní interakce na internetu, možností monitorovat provoz v počítačové síti apod.

V dalším textu jsou v kapitole 2 popsány podrobněji převládající formy informační kriminality z hlediska platné české legislativy. Následující kapitola 3 obsahuje stručný popis organizačního zabezpečení boje proti informační kriminalitě v rámci ministerstva vnitra České republiky a kapitola 4 přehled nejdůležitějších mezinárodních aktivit v této oblasti.

2. Informační kriminalita

2.1 Porušování autorského práva – softwarové pirátství

Softwarovým pirátstvím jsou všechny útoky na právo autora a další práva k počítačovým programům uvedená v autorském zákoně.

Názory právníků na míru chráněných práv v různých počítačových programech však dosud nejsou jednotné. Podle některých *"požívá většina počítačových programů ochrany podle autorského zákona"*, podle jiných "*legální podmínky pro autorskoprávní ochranu počítačových programů českým AutZ může v důsledku své povahy a povahy práva autorského splnit jen malé procento programů".* K výkladu uplatnění autorského zákona na počítačové programy probíhá rozsáhlá odborná diskuse, kterou pravděpodobně neukončí ani nedávno schválený nový autorský zákon (jeho účinnost je stanovena ke dni 1. 12. 2000).

Počty stíhaných, obžalovaných a odsouzených osob podle § 152 tr. zák. dlouhodobě kolísají. Podle trestních statistik státních zastupitelství a soudů jsou následující:

§152	1992	1993	1994	1995	1996	1997	1998	1999	2000
stíháno	382	154	166	181	159	256	281	325	402
obžalováno	306	125	125	158	125	223	136	265	307
odsouzeno	236	125	132	121	82	132	62	148	176

K porušování autorských práv podle § 152 tr. zák. dochází většinou tímto možným způsobem:

- *užíváním programu na jednom počítači případně více počítačích než bylo ve smlouvě dohodnuto (nebo zcela beze smlouvy),*
- *zasahováním do programu, prováděním jeho změn a úprav nad rámec daný platným zněním AutZ,*
- *šířením tohoto programu jiným osobám (nejčastěji okopírováním, ale také výrobou a prodejem plagiátů).*

2.1.1 Neoprávněné užívání softwaru

Pro potřeby této analýzy je vhodné rozdělit neoprávněné užívání softwaru podle toho, zda program používá nějaký jedinec doma pro svou soukromou potřebu, či jde o užívání softwaru za účelem zisku. Každé neoprávněné užívání softwaru de facto přináší svému uživateli zisk – totiž částku, kterou by za daný software zaplatil, kdyby si ho řádně koupil. Autorský zákon jasně odlišuje oprávněné a neoprávněné užívání a Trestní zákon v § 152 nerozlišuje ”běžného pachatele” a ”domácího užívatele”, studenta či pedagoga. Je však vhodné rozlišovat případ, kdy nějaký jedinec – fyzická osoba – užívá software doma pro svou osobní potřebu, od případů ostatních, kdy program neoprávněně užívá právnická osoba nebo fyzická osoba v rámci své komerční činnosti. Všechny tyto ostatní případy je ještě možné rozdělit na případy, kdy se užíváním daného programu dosahuje dalšího zisku, a případy, kdy je jediným ziskem úspora kupní ceny (v případě nekomerčních subjektů jako škol, ministerstev apod.). V některých takových případech může paradoxně docílit zisku jak výrobce dotyčného softwaru tak ten, kdo program nelegálně užívá. Např. jestliže pedagogové na vysoké škole neoprávněně nainstalují nějaký software za účelem výuky, dělají tím příslušnému softwaru značnou reklamu, studenti se s ním naučí pracovat a oblíbí si ho, po odchodu z fakulty a nástupu do zaměstnání se snaží, aby podnik, do kterého nastoupili, zakoupil a užíval spíše software jim už známý než neznámý apod.

2.1.1.1 Neoprávněné užívání softwaru domácím uživatelem

Neoprávněné užívání počítačových programů pro soukromou (domácí) potřebu je nejrozšířenějším činem, který lze zařadit mezi čistě počítačovou (informační) kriminalitu.

Neoprávněně užívat počítačové programy se v ČR stalo po roce 1989 běžným zvykem a má řadu příčin. Negativním faktorem je již stav na základních školách, kde dochází k masivnímu porušování zákona žáky, kteří si mezi sebou počítačové programy běžně půjčují, vyměňují a prodávají. Tato situace zakládá negativní důsledky do blízké budoucnosti, protože ”vychovává” nejmladší generaci k porušování autorských práv, které se tak stává normální. Starší generace na druhou

stranu takové jednání často nepovažuje za nemorální, proti svým potomkům nezasahuje, nýbrž je v jejich činnosti ještě podporuje. K podobnému chování dochází i na středních a vysokých školách, a tak je nutno situaci řešit systémově za účasti různých subjektů státní správy i ze strany soukromého sektoru zejména výrobců a prodejců softwaru. Součástí takového systémového přístupu musí být úsilí o nárůst počítačové, informační gramotnosti (rozšíření výuky ve specializovaných předmětech, přednášky expertů na školách i dalších státech financových subjektech – např. v nemocnicích, úřadech, pracovištích Policie ČR), dále pozitivní stimulace k používání legálního softwaru (např. zakládáním klubů legálního softwaru při školách ekonomicky podporovaných jeho výrobci, podpora společností, které nabízejí legální softwarová řešení školám za zlomek ceny, než za který je nabízen komerčním subjektům), ale význam má i represivní složka – nelze například tolerovat otevřenou propagaci pirátského software.

Důležitým faktorem, který ovlivňuje množství nelegálního užívání počítačových programů v domácnostech, je příliš vysoká cena kvalitních počítačových programů vzhledem k reálným příjmům obyvatelstva. Vliv tohoto faktoru se zcela jistě bude postupně snižovat s růstem průměrných platů občanů ČR, přičemž ceny programů se dlouhodobě udržují přibližně na světové úrovni. V současné době však tuto skutečnost ovlivnit nelze a proto je třeba s vědomím z ní vyplývajících důsledků soustředit činnost resortu MV do oblastí, v nichž jsou problémy vlastní činností odstranitelné. Výše citovaná zpráva BSA o softwarovém pirátství však ukazuje zajímavou skutečnost, že některé středně či značně bohaté země (Španělsko, Irsko, Itálie, Holandsko, Kanada, Hong Kong např.) mají podíl ilegálního softwaru přibližně stejný nebo dokonce i výrazně vyšší než v ČR. Je zjevné, že vliv životní úrovně mohou snadno převážit vlivy jiné (místní zvyklosti, kulturní tradice, ale i podmínky vytvořené ostatními institucemi apod.).

2.1.1.2 Užívání nelegálního softwaru pro komerční účely

V komerční oblasti dochází k podobným problémům jako v oblasti domácích uživatelů. Základním rozdílem je především množství informačních technologií používaných jednotlivci pro komerční účely, specifika v jejich využití (zisk) i rozdílné možnosti exekutivy potírat v této oblasti nelegální jednání.

Obvyklým případem je jednání, kdy podnikatel z důvodu neochoty k investicím nebo nedostatku finančních prostředků buď získá nelegálně software a užívá ho, nebo, a to je nejčastější případ, zakoupí menší množství licencí, než pak ve skutečnosti užívá. Podle BSA se relativní množství nelegálního komerčního softwaru v ČR v posledních letech neustále zmenšuje. V roce 1994 to bylo 66 %, 1995 – 62 %, 1996 – 53 %, 1997 – 52 %, 1998 – 45 %, 1999 – 42 %, 2000 – 39 %.

Negativním faktorem je vztah k řešení problému ze strany subjektů, které přímo prodávají licence k užívání počítačových programů, případně i zajišťují servis. Tyto společnosti a jednotlivci stojí na prodejním žebříčku mezi autorem nebo vykonavatelem autorských práv na území ČR a konečným uživatelem. Stává se, že zákazník, užívající více licencí než zakoupil, požaduje na nelegální instalace servisní zásahy a je mu vyhověno. Prodejci a jejich servisní složky tak disponují s informacemi o nelegálním užívání počítačových programů, a přitom nejsou zásadním způsobem motivováni k odstranění tohoto problému (je třeba podotknout, že trestný čin porušování autorského práva podle § 152 tr. zákona není zařazen mezi trestné činy, jejichž neoznámení nebo nepřekažení by bylo samo o sobě trestným činem). S autorem ani jeho zástupcem ale nekomunikují. Důvody jsou především ekonomické, tyto společnosti nechtějí ztratit své zákazníky a jsou přesvědčeny, že zákazník dříve či později potřebné licence zakoupí právě u nich. K tomu však dochází minimálně, protože porušovatel zákona není dostatečně motivován, aby situaci řešil.

Ve spolupráci s policií prodejcům brání také ”etika” obchodování a především strach ze ztráty zákazníka, který by se dozvěděl o tom, že distributor nebo prodejce spolupracuje s policií. Řešením je proto zejména aktivní přímá spolupráce prodejců a autorů (jejich zástupců), směřující k minimalizaci takového jednání, která na základě výměny informací o porušování autorského práva umožní řešit situaci standardními zákonnými občansko právními prostředky či, v krajním případě, trestním oznámením. Takovouto spolupráci by mohla zajišťovat protipirátská organizace výrobců software (tak jako existují takto zaměřené organizace v oblasti video a audio produkce). V současné době u nás vyvíjí činnost pouze Business Software Alliance prostřednictvím svých členů, kteří jsou aktivní v ČR (společnosti Adobe Systems, Apple Computers, Autodesk, Bentley, Corel, Microsoft a Symantec; česká pobočka BSA byla zrušena v roce 1998), na tuto činnost v ČR však existují značně rozporné názory a zdá se, že je spíše kontraproduktivní. BSA je od roku 1988 mluvčím předních světových výrobců softwaru. Jménem svých členů se angažuje v mnoha

aktivitách s cílem hájit své komerční zájmy. Organizuje akce a vzdělávací programy proti softwarové kriminalitě ve více než 65 zemích na celém světě. Obdobná organizace, ve které by byly zastoupeny i domácí subjekty, kterých se problematiky týká (výrobci, prodejci, odborná média, státní orgány apod.), v současné době v ČR neexistuje, nic ovšem nebrání tomu, aby při jejím vzniku hrálo určitou iniciační roli i Ministerstvo vnitra ve spolupráci s Ministerstvem kultury a Ministerstvem průmyslu a obchodu.

Nepříznivému stavu při odhalování této trestné činnosti navíc nahrává skutečnost, že subjekty státní správy nemají jednoduché a efektivní možnosti k identifikaci takového jednání přímou kontrolou programového vybavení u komerčního subjektu s vazbou na jeho legální nabytí a oprávněné užívání. Pracovníci živnostenských úřadů mají oprávnění kontrolovat živnostenské provozy a v případě zjištění porušení autorských práv mají povinnost (na základě § 8 trestního řádu) oznámit státnímu zástupci nebo policejním orgánům skutečnosti nasvědčující tomu, že byl spáchán trestný čin. Pracovníci finančních úřadů mají sice při daňové kontrole možnost zjistit porušování autorských práv, s ohledem na povinnost mlčenlivosti (tak jak je konstruována v § 24 zákona o správě daní a poplatků) nemají ovšem možnost tuto trestnou činnost oznámit orgánům činným v trestním řízení. Žádoucí novelizace zákona o správě daní a poplatků, která by zahrnovala oznamovací povinnost finančních úřadů, je v současnosti řešena v rámci boje s organizovanou kriminalitou.

2.1.2 Výroba nelegálního softwaru

Výrobu nelegálního softwaru můžeme rozdělit na výrobu průmyslovou, kdy pachatel potřebuje zvláštní vybavení, odlišné od vybavení běžného uživatele, případně musí zadávat tovární výrobu, kde (zcela jistě alespoň implicitně) deklaruje svou osobu jako nositele nebo vykonavatele autorských práv, a výrobu domácí, k níž pachatel nepotřebuje žádné výrazně odlišné vybavení v porovnání s běžným počítačem, ale stačí mu tzv. vypalovací mechanika, jejíž cena včetně příslušného softwaru již klesla na úroveň ostatních běžných hardwarových doplňků (v současnosti – začátek roku 2001 – je možné koupit nejlevnější mechaniku již na cca 4000 Kč).

Nelegální software je také nyní již možné vyrobit tzv. klonováním disků, kdy se pomocí odpovídajících programů vyrábí přesná kopie obsahu disku i se všemi nainstalovanými programy na disk jiného počítače. Lze čekat problémy s registrací produktů nebo značek klonovaných disků.

2.1.2.1 Průmyslová výroba

Průmyslovou výrobou CD-ROM je míněna jejich komerční výroba na zvláštních výrobních zařízeních továrního typu. V ČR působí podle poznatků pracovníků ministerstva vnitra (oficiální evidence neexistuje) čtyři takoví výrobci: GZ Digital Media, a.s. v Loděnici (dříve Gramofonové závody Loděnice, a.s.), C. D. C. a.s. v Čelákovicích, Fermata, a.s. v Čelákovicích (obě se sídlem na stejné adrese v Čelákovicích) a EXIMPO, a.s. v Praze. Samotná výroba je již technicky zvládnuta natolik, že je možno datové nosiče vyrábět v horších podmínkách než tomu bylo před několika lety. To znamená, že výrobní linka může být umístěna i v relativně malém prostoru s menšími nároky na výrobní prostředí.

Všichni provozovatelé výrobních provozů řeší každodenně otázku autorských práv. V současném světě je velmi obtížné ověřit, zda zákazník je skutečně oprávněn zadat výrobu konkrétního nosiče obsahujícího počítačové programy nebo jiná data. V případech, kdy se jedná o známý produkt, je situace jednodušší, ale v ostatních případech spoléhají často odpovědní pracovníci jen na tvrzení zákazníka. Mnohdy se tak stává, že je i u renomovaného výrobce vyrobeno velké množství datových nosičů s pirátskými počítačovými programy. Takové případy jsou obvyklé při zadávání výroby ze zahraničí, kam směřuje i výsledný produkt.

Problematika ochrany autorských práv při průmyslové výrobě datových nosičů není ani v celé Evropě dostatečně zvládnuta. V České republice se již několik let vedou diskuse nad legislativním řešením povinnosti výrobce přiměřeným způsobem ověřit oprávněnost zadání výroby konkrétním subjektem. Právní úprava by měla jasně vymezovat povinnost zadavatele výroby poskytnout všechny nutné informace o produktu a povinnost výrobce přiměřeným způsobem ověřit legálnost zakázky a vést evidenci zadavatelů jednotlivých sérií.

Dalším problémem je neexistence jednoznačné povinnosti identifikace jednotlivých nosičů záznamů (CD-ROM, DVD-ROM apod.), která by umožňovala

okamžité rozpoznání výrobce každého konkrétního výrobku. V některých zemích právní řády takovouto povinnost stanoví, (např. Řecko, Itálie), v řadě zemí jsou nosiče digitálních záznamů označovány (např. tzv. SID kódem) zcela dobrovolně z důvodu udržení dobrého jména podniku.

Povinnost označovat rozmnoženiny autorských děl mimo jiné obchodním jménem a sídlem nebo jménem, příjmením a trvalým pobytem osoby, která rozmnoženinu vyrobila, a rokem, ve kterém byla tato publikace vydána, u nás ukládá zákon o neperiodických publikacích. Tato povinnost se ovšem týká pouze zvukových a jiných záznamů na jakýchkoliv nosičích (tedy i na CD), pokud jsou autorskými díly, výslovně se netýká rozmnoženin audiovizuálních děl (na ty se vztahuje zvláštní zákon, který ukládá povinnost distributorovi uvést na rozmnoženinu díla mimo jiné své obchodní jméno) a rozmnoženin počítačových programů. Kromě toho zákon za porušení identifikační povinnosti neukládá přímo výrobci neoznačené rozmnoženiny žádné sankce, takže tuto povinnost nedodržují ani výrobci rozmnoženin zvukových záznamů, a to proto, že sami zadavatelé výroby rozmnoženin takové označování odmítají. Problémem je také to, že náš právní řád neukládá povinnost označovat tato média jednoznačným identifikačním znakem, jako je tzv. SID kód spravovaný Mezinárodní federací fonografického průmyslu (jehož používání je proto dobrovolné), který splňuje technické podmínky pro mezinárodní identifikaci výrobku a je obtížně padělatelný. Takový kód používají v ČR zatím jen GZ Digital Media, a.s. (dříve Gramofonové závody Loděnice a.s.), ostatní výrobci se tomu dosud brání. Označení výrobků umožňuje identifikovat kdekoliv na světě výrobce i osobu, které objednala výrobu pirátských nosičů a zjistit případné další pachatele trestné činnosti. Lisovny, které odmítají identifikaci svých CD-ROM, tak nemalou měrou přispívají k trestné činnosti. Jako vhodné řešení se jeví stanovení takovéto povinnosti novelizací zákona o neperiodických publikacích.

Průmyslově vyráběný nelegální software v ČR je určen většinou na vývoz. Případy pirátských datových nosičů CD-ROM pro domácí černý trh jsou spíše výjimečné, protože je vzhledem k obvyklým objemům výroby pohybujícím se řádově v desítkách tisíc kusů jednodušší vystopovat pachatele.

Ze zemí EU jsou však signalizovány aktivity našich občanů i cizích státních příslušníků k zadávání výroby pirátských nosičů v ČR a jejich vývozu do zahraničí, k těm patří například i zakázky na produkci CD-ROM s pornografickým obsahem.

2.1.2.2 Domácí výroba

V České republice je velmi specifická situace z hlediska původu nelegální produkce CD-ROM. Zatímco v zemích západní Evropy jsou pirátské nosiče vyráběny převážně průmyslově, či dováženy ze zahraničí, u nás se tak děje jen v omezeném měřítku. Lze ovšem odhadnout, že v dohledné době se situace ve vyspělých zemích spíše bude zhoršovat. Zapisovatelná (CD-RW) mechanika je stále dostupnější – 45 % nově prodaných počítačů v USA v únoru 2000 mělo tuto mechaniku zabudovánu. O tyto mechaniky je nebývalý zájem. Jedním z důvodů, proč v poslední době společnost Hewlett-Packard postoupila z třetího na první místo v maloobchodním prodeji osobních počítačů, je pravděpodobně právě její strategie, že zapisovatelnou mechaniku do svých počítačů dává automaticky. V blízké budoucnosti lze očekávat rychlý růst rozšíření mechanik typu DVD-ROM, vyjímatelných disků apod.

Vlivem tradice univerzálních dovedností našich občanů dochází již několik let k pokrývání poptávky po nelegálních počítačových programech produkcí CD-ROM, převážně vytvářených v domácích podmínkách. Celková poptávka tak není uspokojována masivní průmyslovou výrobou a dovozem, ale činností velkého počtu jednotlivců. V zemích EU navíc dochází při výrobě, dovozu a prodeji nelegálních počítačových programů k aktivitám organizovaného zločinu, které nebyly na našem území zatím zjištěny. Důvodem je právě značné množství aktivních jedinců s minimálními náklady na ”výrobu a distribuci”. K šíření nelegálního softwaru dochází často v uzavřeném kruhu známých osob, stále častěji jsou ale nabízeny především na internetu rozsáhlé seznamy pirátských CD.

Jednotlivce, vyrábějící CD-ROM popsaným způsobem, lze relativně snadno identifikovat a proto se stále více daří tuto činnost omezovat. Situace však není jednoduchá, protože náklady na takovou výrobu a distribuci pirátského softwaru jsou minimální a čisté zisky značné. To motivuje stále ještě řadu osob, aby takovou trestnou činnost prováděly. Vzhledem k zahraničním zkušenostem je nicméně možno konstatovat, že počet trestných činů porušování autorského práva touto formou bude klesat. V současné době je oproti předcházejícím letům patrný trend ve směru k ukládání přísnějších trestů za tuto nezákonnou činnost, pokud je v trestním řízení prokázána.

Současný stav, charakterizovaný vysokou mírou domácí ilegální výroby softwaru, lze částečně změnit jen dlouhodobým systematickým úsilím o systémové změny. Nelze očekávat, že by bylo možno dosáhnout výraznější změny pouze represivní činností státních orgánů. Ilegální domácí výroba totiž jen určitým způsobem reflektuje uvolňování tlaku, který vytvářejí faktické tržní síly: o software má obyvatelstvo zájem, ale je pro ně zpravidla příliš drahý a proto podstupují obtíže při ilegálním vypalování CD. Pokud by byl software výrazně levnější, ilegální vypalování disků by nepochybně výrazně pokleslo. Velké softwarové firmy, které zvolily strategii vysokých cen, nemohou proto očekávat, že se jim (a státu – pokud to ovšem není totalitní policejní stát) podaří ilegální domácí vypalování radikálně potlačit. Vysoké ceny spolu s důrazem na represi a trestněprávní postih navíc přispěly k tomu, že image velkých zahraničních softwarových firem na veřejnosti není v současné době příliš příznivý, a že převažuje názor, že ”okrást zloděje” není nic špatného. Většího úspěchu (i zisku) by třeba bylo možné dosáhnout strategií nižších cen a vyššího počtu prodaných licencí. Obchod je také někdy třeba chápat (stejně jako politiku) jako umění možného. Typického jedince, který doma pálí CD-ROM (nebo slivovici) nelze vyměnit za jiného, a ovlivnit ho lze mnohem více cenou výrobku o který usiluje než represí či výchovou. Analogický (do značné míry marný) boj, jehož odvrácenou stránku reprezentovaly např. výzvy k oznámení ilegálního softwaru na stránce www.zatepla.cz (jež se nedávno transformovaly do podoby výzev k vyplnění formuláře v rubrice ”Dejte nám vědět!” na českých stránkách BSA) vedou v současné době velká nahrávací studia proti projektům typu Napster apod. (viz též dále kap. 2.5). Čím dříve dojde ke změně celkového přístupu, tím lépe. První vlaštovkou se zdá být chování německého koncernu Bertelsmann (jehož součástí je nahrávací studio BMG), který ještě před soudním verdiktem nad firmou Napster, s Napster navázal obchodní spojení, se zjevným cílem zlegalizovat získávání hudebních nahrávek z internetu, a místo aby s tímto způsobem získávání hudby bojoval, bude se na něm snažit vydělat.

2.1.2.3 Kopírovací služby

V první polovině devadesátých let vedle rozvoje prodeje zapisovatelných mechanik CD-ROM došlo k růstu nabídek na kopírování dat jako komerční servisní služby. Zákon tak byl často ignorován nebo vědomě porušován.

Kopírovány byly a jsou většinou pirátské nosiče, či je vytvářeno množství ”záložních” kopií originálních nosičů, které jsou pak v rozporu s licenčním ujednáním dávány za úplatu či bezplatně k dispozici dalším osobám. Proti samotnému vytvoření skutečně záložní kopie z řádně nabytého nosiče nelze mít námitek.

Argumentem poskytovatelů těchto služeb obvykle bývá (podobně jako při průmyslové výrobě), že za dodržování zákona je odpovědný zákazník. Avšak zákony platí pro všechny, a proto i provozovatelé kopírovacích služeb jsou povinni je respektovat. K zlepšení situace by nepochybně přispělo zavedení zákonné povinnosti ověření práva k vytváření většího množství kopií od originálního nosiče.

Kopírovací služby stojí v současnosti již mimo masivní zájem zákazníků především proto, že ceny technického vybavení i prázdných medií podstatně klesly, a tak již není pro běžného uživatele ani pro komerční subjekt problém vytvořit si záložní kopii.

2.1.3 Šíření nelegálního softwaru

Prodej a nabídka nelegálně získaných či nelegálně šířených počítačových programů se řídí podobnými pravidly jako u běžného zboží. Zásadním rozdílem je úmyslné porušování zákona ze strany osob provádějících tuto činnost. Tomu odpovídá i specifický způsob komunikace se zákazníkem a vnější projevy takových aktivit.

2.1.3.1 Základní způsoby šíření ilegálního softwaru

Základní způsoby šíření pirátského softwaru v ČR jsou dány především zdrojem pirátských programů. Vzhledem k tomu, že je u nás mnoho jednotlivců, kteří vytvářejí

nelegální kopie v domácích podmínkách, odpovídá tomu i nadstavba této činnosti, kterou je nabídka a prodej vlastní produkce. Před razantním rozvojem internetu to byla především inzerce v celostátních a lokálních inzertních mediích (Annonce, Inzertspoj atd.). V současnosti tato forma ještě přetrvává, ale je patrný přesun na internet, protože na jednoduše vytvořenou stránku na zahraničním serveru je umožněn přístup každému, kdo o to má zájem, a autor nabídky zde může umístit značné množství informací, které jinak dodával zákazníkům komplikovaně a se značnými náklady písemnou formou nebo na disketě. Další výhodou je velmi jednoduchá komunikace pomocí anonymních poštovních služeb na internetu.

V současné době se stává internet dominantním prostorem výměny informací o programech i vlastních programů. Programy jsou umístěny na zahraniční anonymní FTP server (mimo dosah české legislativy) a za poplatek je poskytováno heslo a přístup. Jednotlivec si takový program pouze stáhne. Odpadá tak dodávka prostřednictvím pošty, což odhalení takového jednání ještě více znesnadňuje. K opravdovému rozmachu takové služby ale dojde po zlevnění telekomunikačním poplatků a zkvalitnění připojení.

Již několik let se na různých místech (adresách) internetu vyskytují tzv. sklady. Jsou to vybrané adresáře na jinak nenápadných počítačích s kvalitním připojením do internetu, které mají snadný přístup, téměř neomezenou velikost ukládaných souborů a minimální kontrolu správce. Vyhledávají a užívají je osoby, které zde shromažďují nelegální software s cílem umožnit jeho volné kopírování každému, kdo získá adresu tohoto ”skladu” na internetu a oprávnění k přístupu (pokud není volné pro každého). Cílem tohoto jednání není zisk ani jiný osobní prospěch, ale například snaha o volnou dostupnost jinak drahých programů jako projev svérázné životní filozofie. Jediným řešením je vyhledávání a identifikace takových míst a následná snaha o ukončení popsané aktivity. Takové servery jsou subvencovány reklamou na pornografické stránky a internetová kasina. Z těchto serverů by za určitých okolností mělo být možné získat informace o internetových adresách, ze kterých byly konkrétní soubory zaslány a kam byly odeslány kopie. Po jejich zjištění je proto možné identifikovat konkrétní osoby, které neoprávněně a v rozporu ze zákonem šířily počítačové programy, i ty, kdo je zkopírovaly pro další neoprávněná užívání. Takové servery jsou ale umístěny v zahraničí, kam česká legislativa nesahá a vzhledem k množství takových stránek na internetu je spolupráce s ostatními složkami velice

složitá, až téměř nerealizovatelná. Každý den totiž mnoho nových stránek přibývá a monitorovat jejich činnost je tak nemožné.

V komunikaci mezi značným množstvím uživatelů internetu je častým tématem vzájemná ”pomoc” při řešení problémů s nelegálním softwarem jeho umístěním na konkrétní internetové adrese nebo získáním tzv. cracku (program k umožnění plně funkčního užívání časově omezeného nebo jinak chráněného aplikačního programu nebo hry).). Kromě tzv. cracků je na internetu zveřejňováno ještě veliké množství sériových čísel k veliké spoustě programů, po jejichž zadání se program stává plně funkční.

Vzhledem k nadnárodnímu charakteru internetu je situace v této oblasti (a nejenom v ní) jen málo odlišná od situace v jiných zemích a rovněž ani není odděleně řešitelná. Je zjevné, že výraznější zlepšení je možné dosáhnout jen postupem, koordinovaným na mezinárodní úrovni a vycházejícím z mezinárodních úmluv. Přehled nejdůležitějších aktivit Evropské unie a Spojených států je podán v kapitole 6.

2.1.3.2 Neoprávněná instalace počítačových programů do nové výpočetní techniky

Softwarové společnosti umožňují prodej licencí (oprávnění) k užívání počítačových programů řadou různých způsobů. Jedním z nich je i uzavírání dohod s výrobci počítačů a různých hardwarových komponent o tzv. OEM softwaru. Smlouva obvykle stanovuje, že konkrétní výrobce počítačů nebo jejich dílů bude přidávat k této technice počítačový program za cenu, která je nižší než při jeho běžném prodeji. OEM software se v podstatě dělí do dvou kategorií:

1. Normální plná verze SW přibalovaná k novým počítačům. Od normálního krabicového SW většinou liší právě pouze tím, že není dodáván v krabici a prodává se za nižší cenu. Jinak je funkčně a vybavením úplně stejný (např. Windows, MS Office, některé antivirové programy apod.).
2. Omezená verze SW dodávaná zdarma s nějakým HW (např. hry bez manuálů, tzv. light verze kreslících programů dodávané s některými scannery či digitálními fotoaparáty apod.).

Cílem této aktivity je ze strany autorů softwaru jeho lepší šíření mezi uživateli výpočetní techniky s tím, že spokojený zákazník přijme kvalitní produkt a zakoupí si i další verze za plnou cenu. Pro výrobce výpočetní techniky je přínosem jakási ”přidaná hodnota”, která zatraktivní produkt na trhu a přinese vyšší prodej. Zákazník/uživatel pak získá kromě technického výrobku i hodnotný počítačový program, kterým je často operační systém. Dá se říci, že filozofie OEM produktů je všestranně pozitivní. Často dochází k porušování autorských práv prodejci umísťováním OEM programů bez souhlasu autora. Vzhledem k popsaným výhodám pro výrobce výpočetní techniky, spočívajícím především v atraktivitě zboží na trhu, dochází k neoprávněnému umisťování softwaru do počítačů výrobcem a následnému uveřejňování takové nabídky s cílem získání zákazníků. Na trhu jsou takové počítače jasně zvýhodněny svou cenou, protože umístění programů bez smlouvy znamená, že zákazník tyto programy získá levněji nebo dokonce naprosto zadarmo, a tak srovnatelná výpočetní technika od dvou výrobců, z nichž jeden dodržuje zákon a druhý nikoliv, se může svou cenou lišit o tisíce korun.

Policie ČR je jen v minimu případů schopna takové nelegální aktivity sama odhalit. Důvody spočívají především v nulové indikaci takového chování jako trestného činu ze strany kupujícího. Legálně a nelegálně nabízené instalované OEM programů se od sebe nijak neliší. Stav na trhu musí sledovat především sami autoři a vykonavatelé autorských práv, kteří mají jediní schopnost odlišit subjekt, se kterým byla uzavřena smlouva, od takového, který šíří OEM software bez ní.

Dalším problematickým rysem je skutečnost, že takového jednání se obvykle dopouštějí především malí výrobci okresní úrovně, kteří svou nabídku s informací o instalovaných programech šíří jen ve velmi omezeném prostoru. Autor tak sám mnohdy nezíská potřebnou informaci a obtížně reaguje na takové jednání. Řešením je zlepšení spolupráce autora s distributory a prodejci softwaru, kteří mají rozsáhlé sítě obchodních zástupců schopných registrovat podobné aktivity a informovat o nich.

2.1.3.3 Ostatní způsoby šíření ilegálního softwaru

V předchozích dvou bodech byly popsány nejčastější způsoby neoprávněného šíření počítačových programů. Pochopitelně existují další.

Vyskytují se půjčovny softwaru nebo výpočetní techniky včetně počítačových programů. Tyto aktivity obvykle bývají porušením autorského práva, protože v autorském zákoně je výslovně uvedeno, že v případě půjčování, pronájmu apod. musí být uzavřena smlouva mezi autorem a subjektem, nabízejícím takovou službu. Absolutní většina takových podnikatelů to však nerespektuje, což přináší riziko trestního oznámení autora pro porušování autorského práva dle § 152 trestního zákona. Přitom většina softwarových společností je připravena takové aktivity povolit na smluvním základě.[2] Důvod, proč provozovatelé půjčoven softwaru nebo výpočetní techniky nemají zájem o smlouvu, je finanční. Cena služby by se totiž zvýšila o částku, kterou si vymíní autor, a to by v počátečním stadiu mohlo mít negativní vliv na pozici provozovatele takové činnosti mezi ostatními, případně by to snížilo dlouhodobé kalkulace zisku.

Z hlediska konstrukce práva v ČR je aktivita při sledování porušování autorských práv především věcí autorskou. Policie ČR sama musí provádět aktivní odhalování podnikatelských subjektů v oblasti půjčování počítačových programů nebo pronájmu výpočetní techniky, řešení tohoto problému jen represivní cestou však dosáhnout nelze. V případě, že porušení zákona bylo oznámeno orgánům činným v trestním řízení, je možno vzhledem k charakteru trestného činu očekávat relativně rychlé a bezproblémové řešení. Ze státních orgánů nutno počítat také s podílem živnostenských a finančních úřadů.

2.1.4 Trendy

V blízké budoucnosti (několik let) očekávají odborníci prohloubení současných změn ve formě distribuce a prodeje počítačových programů jako základního způsobu porušování autorského práva, zahrnutého do problematiky informační kriminality. U absolutní většiny počítačových programů bude docházet k přímému prodeji, kdy zákazník po elektronické platbě zkopíruje software na počítač, pro který je určen. Tak bude posílena pozice autora nebo softwarové společnosti při komunikaci s uživatelem, protože každý oprávněný uživatel bude uložen v seznamu, který bude sloužit pro kontrolu v případech porušování autorského práva. Dosavadní

[2] To však neplatí o počítačových hrách, kdy dosud byla stanoviska autorů negativní.

neexistence nebo značná chybovost těchto seznamů u současných autorských subjektů je jedním z problematických faktorů softwarového pirátství. Stát oprávněně očekává od autora, že si v rámci účetnictví vede přesnou dokumentaci o prodaných licencích opravňujících k užívání počítačových programů. Je třeba upozorňovat na přímou vazbu mezi kvalitním vedením podobného přehledu a odlišením oprávněných a neoprávněných uživatelů.

Samotné autorské právo bude stále více napadáno, protože jednoduchost takového činu, zvláště při rychlém a levném nebo bezplatném připojení k internetu, umožňuje každému získat v podstatě jakýkoliv dostupný program. V současné době se prudce šíří programy, které vyhledání a stažení požadovaných dat velmi usnadňují. Tak např. v oblasti hudby kódované ve formátu MP3 došlo k značnému rozšíření projektu Napster. Po nainstalování malého programu se počítač každého uživatele změní v server, který sdílí svůj adresář se skladbami ve formátu MP3 s ostatními uživateli. Po zadání jména zpěváka nebo skupiny jsou automaticky prohledány archivy všech přihlášených uživatelů, přičemž udávaná úspěšnost je téměř stoprocentní. Na univerzitních serverech v USA tvořil přenos dat tímto způsobem až 80 % zatížení, než byl zablokován přístup na centrální stránku projektu. Od prosince roku 1999 se však začaly šířit aplikace Napigator, Wrapster, Gnutella, jež centrální stránku vynechávají a umožňují stahování přímo mezi uživateli. Tento typ spojení dvou počítačů (peer-to-peer) je velmi obtížně identifikovatelný. Tvůrci některých těchto programů se navíc brání případnému postihu tím, že ve stanovách k programům uvádějí, že program je určen výhradně pro použití s legálně zakoupenými daty, a že tedy jen uživatel je odpovědný za porušení zákona. Tato situace vyžaduje změny v uplatňování a vynucování autorského práva. Samotné autorské subjekty již dnes musí řešit způsoby, jak se vyrovnat s tímto nebezpečím. Jednoduché řešení není. Je možno odhadnout, že řada programů, především z kategorie těch, které jsou nutné pro základní funkčnost výpočetní techniky a jednoduchou práci, bude volně dostupných. Základní filozofií společností nebude účtovat za samotné programové vybavení, ale spíše za služby, které budou spojeny s jeho používáním (školení, servis, atp.).

Problémy bude určitě dlouho činit zejména rozpor mezi teritoriálním principem autorského práva a globálním charakterem internetu, řešitelný nejspíše pouze nějakou mezinárodní úmluvou, podobně jako je tomu u moře nebo kosmického prostoru. Je rovněž zřejmé, že kriminalitu, která souvisí s porušováním autorského

práva prostřednictvím internetu, nelze potírat dostatečně účinně bez boje i s dalšími formami ”internetové” kriminality. Na tuto situaci již zareagovala Rada Evropy a koncem dubna 2000 zveřejnila k diskusi první verzi návrhu mezinárodní dohody o zločinu v kyberprostoru. Tento návrh i další analogické mezinárodní aktivity jsou popsány v kapitole 4.

Z bezpečnostního hlediska je nutno konstatovat, že snižování objemu softwarového pirátství narazí v nebližších letech na hranici (cca 20 %), pod kterou pravděpodobně neklesne. Po snížení volné nabídky nelegálních počítačových programů je možno očekávat aktivity organizovaných skupin, které budou nabízet pirátský software, a v dalších letech pak kvalifikovanější trestnou činnost, spočívající v komplexním plagiátorství nejen CD-ROM jako nyní, ale i doprovodných materiálů a obalů. Další kapitolou je plagiátorství ochranných prvků, které bude stále kvalitnější. Tak bude stále složitější rozpoznat legální a nelegální programy i pro kvalifikovaného znalce.

Softwarovému pirátství lze v zásadě čelit dvěma na sebe navazujícími způsoby. První je ochrana pomocí nástrojů práva civilního, druhou pak pomocí nástrojů práva trestního. V rozvinutých ekonomikách je vždy prvotní použití nástrojů práva civilního. Prostředky práva trestního nastupují až ”ultima ratio”. V podmínkách ČR je z důvodu nedostatečné efektivnosti civilního soudnictví upřednostňováno použití prostředků trestněprávních před prostředky civilněprávními. Přitom z hlediska efektivnosti boje proti poškozování soukromovlastnických práv je velmi důležitá návaznost ochrany trestněprávní na účinnou ochranu civilněprávní. Ve vyspělých zemích je absolutní většina těchto problémů řešena na civilněprávní úrovni žalobou, případně náhradou škody a výlučně trestněprávní cesta je použita jen v krajním případě.

Činnost tzv. ”pirátů” je natolik ekonomicky zajímavá (téměř nulové investice do vytvoření autorského díla), že prosté potrestání jedinců, kterým je prokázáno úmyslné porušení zákona, způsobem presumovaným jednotlivými souvisejícími skutkovými podstatami trestných činů, jak je uvádí trestní zákon, stěží odradí další pachatele od této činnosti. Vzniklé škody, pokud je vůbec lze objektivně vyčíslit, se pak podaří na delikventech vymoci jen v mizivém procentu případů.

2.2 Poškození a zneužití záznamu na nosiči informací

Zatímco softwarové pirátství je trestným činem snadno odhalitelným, trestný čin poškození a zneužití záznamu na nosiči informací dle ustanovení § 257a trestního zákona je obvykle útokem komplikovaným a obtížně objasnitelným. To je také zjevné z počtů stíhaných, obžalovaných a odsouzených osob podle § 257a trestního zákona, získaných z trestních statistik státních zastupitelství a soudů:

§257a	1993	1994	1995	1996	1997	1998	1999	2000
stíháno	1	4	4	6	14	14	11	18
obžalováno	1	4	2	6	14	6	7	15
odsouzeno	0	0	0	1	1	0	2	0

V § 257a trestního zákona se hovoří o nosiči informací a záznamu či informaci na něm. Jako nosič informací je chápáno jakékoliv datové médium určené pro informační techniku. Zmíněný § 257a trestního zákona je jediným ustanovením, které je určeno pro informační technologie jako takové a postihuje vysoce kvalifikovanou trestnou činnost. Trestnou činnost tohoto typu je možno rozdělit na dvě mezní formy. Útok z vnějšku a zevnitř subjektu, který je cílem útoku. Jak pachatelé, tak způsoby spáchání trestného činu se v obou formách podstatně liší, stejně jako způsob objasňování trestného činu. Útoky z vnějšku vyžadují podstatně větší kvalifikaci orgánů činných v trestním řízení i odborných znalců. Skutečný útok samozřejmě může být i kombinovaný, vedený současně z vnějšku i zevnitř subjektu.

Již ze znění § 257a trestního zákona je zřejmé, že zákon vlastně zabírá tři formy trestné činnosti jakým jsou:

1. neoprávněné užití informací,
2. zničení, poškození nebo učinění informací neupotřebitelnými a
3. zásah do technického nebo programového vybavení počítače,

které je nutno vidět v souvislosti s předchozím rozdělením na vnější a vnitřní útok a tak také budou dále popsány.

2.2.1 Útok z vnějšku subjektu

Touto formou útoku je myšlen tzv. ”hacking” čímž se rozumí ”násilné” tj. neoprávněné získání přístupu k datům. Touto činností se rozumí ”proražení” ochrany počítače pachatelem, který není u počítače fyzicky přítomen, a který se obvykle nachází ve značné vzdálenosti od cíle útoku. Podmínkou tedy je, že výpočetní technika umožňuje připojení z jiného počítače, obvykle po pevné, telefonní nebo jiné lince (např. mikrovlnné spoje). V současnosti může jít i o plnohodnotné přenosné počítače nebo počítače typu PALM nebo IPAQ Pocket apod., spojení může být uskutečněno také pomocí mobilního telefonu.

Tato forma trestné činnosti se začala rozvíjet, až když bylo možné připojení k počítači datovou komunikací. V ČR byla trestná činnost tohoto druhu před rokem 1989 téměř neznámá, protože podmínky pro její spáchání byly minimalizovány stavem používaných technologií. Po tomto roce se začaly odpovídající podmínky vytvářet a již od roku 1995 se na našem území začali vyskytovat jednotlivci a skupiny hackerů, provádějící různou trestnou činnost tohoto druhu. Nejobvyklejším útokem se stalo pozměňování webových stránek různých subjektů nebo jejich nahrazování vlastními stránkami, v budoucnosti lze čekat navíc také snahu o získání nějakého finančního profitu. Nejznámější odhalený případ z poslední doby (září 1999) je odcizení databáze osobních dat z České spořitelny. Jedenadvacetiletý J. V. se snažil odcizená data prodat, choval se však značně diletantsky a byl proto brzy odhalen. Policie ani justice u nás ani v sousedních postkomunistických zemích nemají ještě dostatečné zkušenosti s tímto druhem trestné činnosti. Nejdále jsou v této oblasti země počítačově nejrozvinutější, a z nich zvláště USA. Nejnovější případ z března 2001 je odsouzení sedmnáctiletého hackera Dennise Morana, nazývaného Coolio k devíti měsícům odnětí svobody a zaplacení 5 000 $ svým obětem.

Tyto trestné činy jsou obvykle prováděny tak, že pachatel nebo pachatelé se nepřipojují k objektu útoku (počítači) přímo, ale přes jeden i více internetových serverů v různých částech světa. Cílem je podstatné snížení možnosti identifikace skutečného umístění počítače, který užívá pachatel k trestné činnosti. Užívání více internetových serverů se dosahuje prostřednictvím tzv. Trojan horses (trojští koně), programů, které se tváří jako zcela nevinný software a jejichž prostřednictvím si

jednotlivci v systému vytvoří tzv. backdoors (”zadní vrátka”), což obvykle znamená spáchání trestného činu podle ustanovení § 257a odstavec 1 písmeno c), protože pachatel získá neoprávněný přístup k internetovému počítači a změní jeho nastavení tak, aby ho mohl kdykoliv později použít. Po spáchání trestného činu na cílovém počítači je často možno zjistit pouze internetovou adresu předchozího počítače, k němuž byl pachatel připojen (a do kterého učinil popsaný zásah). Vytváření ”zadních vrátek” v počítačích ve světové síti je u pachatelů této trestné činnosti běžné, a každá taková osoba jich má připravenu celou řadu pro různé aktivity. Na internetu existuje celá řada běžně dostupného softwaru společně s popsanými postupy. Takové činnosti se tak dopouští stále více a více jednotlivců. V několika případech jde o amatérské průniky do systémů, které lze snadno odhalit. Existují však případy, kde k narušení došlo a pachatel nebyl vůbec odhalen (někdy však není odhalen ani samotný průnik, natož osoba za něj odpovědná). Ve všech případech jsou ale do určité míry vinni i správci počítačových systémů, neboť dostatečně nezabezpečili svěřený majetek.

Samotný útok na cílový počítač se v principu neliší od vytváření backdoors, s tím rozdílem, že jako ”přestupní stanice” se s předstihem připravují počítače s nízkou úrovní ochrany a tím i jednoduchou možností úpravy pro potřeby pachatele. Cíl útoku může mít i nemusí vysoký stupeň ochrany. Důvody útoku jsou:

1. neoprávněné získání a užití informací – kopírování dat (§ 257a odst. 1/a),
2. zničení, poškození nebo učinění informací neupotřebitelnými – destrukce, poškození nebo upravení dat (§ 257a odst. 1/b) a (jak již vyplývá z výše uvedeného)
3. zásah do technického nebo programového vybavení počítače (§ 257a odst. 1/c).

2.2.1.1 Neoprávněné užití informací

Neoprávněné získání dat (kopírováním) a jejich následné užití lze považovat za jeden z nejnebezpečnějších útoků na jakákoliv data. Samotné nebezpečí je v tom, že se kvalifikovanému pachateli podaří spáchat tento čin beze stop a bez odhalení správcem dat, což přináší zásadní bezpečnostní riziko pro rozsáhlé databáze různých subjektů. Tuto formu trestné činnosti mohou využívat i cizí zpravodajské

služby, protože přináší nejmenší riziko odhalení jejich činnosti. Zároveň již jsou v ČR poznatky o útocích na data klientských databází různých subjektů podnikatelské sféry jako nástroji konkurenčního boje. Stejně může docházet ke kopírování bezpečnostních, vědeckovýzkumných a podobně citlivých, např. osobních dat. V takových případech je ale zpravidla nutná spolupráce s jednotlivcem, který je zaměstnán uvnitř firmy, viz 3.3.

Takto spáchaný trestný čin se samozřejmě nemusí vyznačovat pouze kopírováním dostupných dat jako celku, ale i konkrétních fragmentů.

V současnosti dochází k zvyšování počtu útoků tohoto druhu.

2.2.1.2 Zničení, poškození nebo učinění informací neupotřebitelnými

Nepřátelskou manipulaci s daty, jejíž extrémním případem je jejich destrukce, lze považovat za primitivní formu trestného činu, protože její následky lze snadno zjistit. Příkladem jsou změny webových stránek, ke kterým čas od času dochází. Pohnutkou pachatele je nejčastěji ukázka vlastních schopností, případně záměrné poškozování firmy či osoby, které webové stránky vlastní, vytvářejí nebo spravují.

Na celém světě existuje rozptýlené a centrálně neorganizované společenství hackerů, které se vyvinulo v USA. Tito lidé uznávají svéráznou filozofii zásad pro svojí činnost na internetu. Jednou z nich je zásada, že útok by neměl zanechat nevratné následky, tedy správce webových stránek má být po útoku schopen je obnovit. Útok nemá způsobit finanční či jinou přímou škodu. Motivem je cítit vzrušení, bavit se, přijmout výzvu k soutěži, napravení chyby v programu či v chování správce sítě. Volnost společenství však přináší značnou pestrost chování těchto osob, které spočívá v relativně volném výkladu výše uvedených pravidel. I v ČR existují skupiny osob, které se při své činnosti řídí těmito pravidly, ale z podstaty jejich činnosti, která je protiprávní, často plynou vážné finanční škody. Proto všechny vyspělé země celého světa posuzují i takové útoky jako trestnou činnost.

Ze skupin ”rekreačních” hackerů se často vydělují jedinci (”institučí” hackeři), kteří jsou ochotni za úplatu od někoho, kdo je motivován ekonomicky nebo politicky (ekonomická konkurence, tajné služby) provést kopii, změnu či destrukci dat

v počítači připojeném do internetu, případně až totální vymazání počítače, a tím způsobit velmi vážné škody. Takové případy jsou již známy i u nás. Vyspělé země nebezpečí takových útoků nepodceňují a snaží se podnikat odpovídající protiopatření. Ve Spojených státech byla např. již vypracována a zveřejněna první verze Národního plánu pro ochranu informačních systémů (Plán). V prosinci roku 2000 začalo jeho zavádění a počítá se s tím, že bude plně funkční v květnu roku 2003. Jeho vypracování uložil president Clinton směrnicí č. 63 v květnu r. 1998. Je to první pokus (v USA i na mezinárodní úrovni) navrhnout způsob ochrany státního ”kyberprostoru”. Plán je 200 stránkový dokument dostupný veřejnosti na internetu. Obsahuje 5 kapitol a 4 dodatky. V kapitole 1 jsou stanoveny základní druhy hrozeb kritickým infrastrukturám. Kapitola 2 diskutuje základní otázky a možné rozporné body mezi ochranou soukromí a občanských práv na jedné a straně a způsoby navrhovanými v Plánu. Kapitola 3 popisuje cíle a základní přístup Plánu k ochraně vybraných infrastruktur. Nejrozsáhlejší 4. kapitola popisuje vlastní plán ochrany kritických infrastruktur federální vlády USA, 5 kapitola se věnuje analogické problematice na úrovni státních a lokálních vlád a v soukromém sektoru. V Dodatku A jsou uvedeny odpovědné osoby včetně kontaktních adres a telefonů, v Dodatku B jsou podrobně rozepsány nároky na rozpočet, Dodatek C se týká výzkumu a vývoje v oblasti ochrany kritických infrastruktur a posléze Dodatek D podává přehled a definice odborných termínů. V únoru roku 2001 byla zveřejněna rovněž velmi obsáhlá (209 stran) Zpráva presidenta Spojených států o stavu aktivit ochrany kritických federálních infrastruktur. Vypracování takovéhoto plánu a podávání analogických každoročních zpráv je nanejvýš nutné i v České republice.

2.2.1.3 Zásah do technického nebo programového vybavení počítače

Za zásah do technického či programového vybavení počítače lze na prvním místě označit tvorbu již zmíněných backdoors, která nemusí být jen jednoúčelová, ale může umožňovat řadu dalších aktivit. Například dochází k zneužívání možností konkrétního počítače, který má přímé a bezplatné napojení na jinak placenou službu.

Pachatel tak vlastně získává neoprávněný přístup ke škodě plátce služby, která může být i značně vysoká, pokud je platba vázána na objem dat nebo čas.

Na základě podobného zásahu lze také manipulovat s dalšími daty a účty na počítači ke splnění různých záměrů pachatele. Aktivity internetových hackerů jsou tím silnější, čím více mohou ukázat své úspěchy na veřejnosti a těšit se i mediální podpoře. Úspěšnost útoků je dána kvalitou bezpečnostních opatření na počítačích připojených k internetu, které jsou závislé jednak na schopnostech správce počítače nebo připojení a jednak na kvalitě použitého softwaru. Existují i útoky, jejichž autor je zdůvodňuje jako upozornění správci na jeho špatnou práci.

Protože převážná většina počítačů sloužících jako internetové servery pracuje na operačním systému linuxového typu, je funkce správce takového počítače určena pouze pro kvalifikovaného jedince, který je schopen sledovat nové informace o bezpečnostních problémech a v případě nutnosti je okamžitě zavést do vlastní činnosti. Protože však nemohou být všichni špičkovými odborníky, lze očekávat, že průměrná bezpečnost na internetu se bude zvyšovat jen velmi pomalu. To způsobuje stálé nebezpečí útoku jako trestného činu podle ustanovení § 257a trestního zákona.

Jednou z cest k systémovému řešení je zřízení skupiny typu CERT[3] jako nevládního sdružení kvalifikovaných odborníků informujících ostatní profesionály o bezpečnostních problémech a reagujících na probíhající útoky. Založení takové skupiny i u nás se v současnosti jeví jako velmi potřebné a již probíhající aktivity k tomu směřují.

2.2.2 Útok zevnitř subjektu

V některých aspektech se útok zevnitř systému může podobat útoku z venku, ale jinak se ve většině ohledů jedná o zcela jinou formu trestného činu.

První odlišností je osoba pachatele. Téměř vždy se jedná o současného nebo bývalého zaměstnance subjektu, který je cílem útoku nebo o osobu, která pro takový subjekt vykonává nebo vykonávala nějakou činnost. Pachatel vychází ze znalosti vnitřního systému, což ho podstatně odlišuje od mimo stojícího útočníka, který

[3] Central Emergency Response Team – koordinační centrum, založené v prosinci roku 1998 v Carnegie Mellon universitě poté, co určitý typ viru ochromil přibližně 10 % počítačů připojených na internet. Projekt je podporovaný federální vládou USA. V současnosti působí asi 70 takových skupin v různých zemích včetně většiny evropských.

disponuje jen těmi informacemi, které sám při testování systému zvnějšku nebo při samotném útoku zjistí. Pozice pachatele stojícího uvnitř subjektu je podstatně jednodušší. Obvykle navíc disponuje ze své zaměstnanecké pozice i určitou úrovní oprávnění přístupu k výpočetní technice nebo k informačnímu systému. Těchto znalostí a oprávnění pak zneužívá k samotnému trestnému činu.

Pachateli uvnitř subjektu mnohdy nahrává i úroveň vnitřní informační bezpečnosti. Mnoho subjektů ve sféře podnikání není schopno posoudit objem bezpečnostních opatření nutných k zabezpečení firemních dat a manipulace s nimi. Obvykle za dostatečnou ochranu považují ochranu softwarovou, čili programové vybavení, sloužící jako bezpečnostní filtr pro vstup do výpočetní techniky ze sítě internet a vnitřní auditní systémy nebo podobné programové vybavení. To vede k podcenění dalších forem útoků na data, kdy pachatel získává neoprávněný přístup svou fyzickou činností a nikoliv prací s výpočetní technikou. Jako příklad je možno uvést odcizení pevného disku, obsahujícího citlivá data, z počítače, odstaveného z technologických důvodů, který je jako server umístěn bez jakéhokoliv zabezpečení ve volně dostupném prostoru. Kromě ochrany softwarové je proto třeba zabezpečit ochranu dat i z hlediska stavebního a personálního.

V posledních letech bylo zaznamenáno celé spektrum útoků na data zevnitř systému ponejvíce motivovaných finančním prospěchem pachatele. Z toho plyne i skutečnost, že častým objektem zájmu pachatelů jsou společnosti, pracující s velkými finančními prostředky, jakými jsou finanční ústavy. Zaměstnanci těchto subjektů jsou vystaveni značnému pokušení poměrně jednoduchým způsobem získat značný finanční prospěch. Relativní jednoduchost takového činu spočívá ve znalosti systému a vlastnění přístupových práv ve spojitosti s vědomostmi o bezpečnostních nedostatcích. Navíc značné množství výpočetní techniky a její propojení do sítě umožňuje provést útok na majetek použitím několika stisků klávesnice jednoho z mnoha počítačů.

V první řadě zde selhává personální faktor. Ve všech případech minulých let v ČR nedošlo ke kvalifikovanému napadení vnitřního systému banky z vnějšku, ale ke zneužití znalostí ze strany zaměstnance. K tomu se přidávají další faktory obvykle též spočívající v personální rovině, kdy zaměstnanci zodpovědní za bezpečnost a výpočetní techniku nesplnili své povinnosti nebo podcenili hrozící nebezpečí. V řadě případů je spáchání trestného činu skutečně jednoduché, daný konkrétní způsob ale nelze použít jinde, protože jsou podmínky pro konkrétní trestný čin velmi specifické.

Často se jedná o zneužití určitých zvláštností na jediném pracovišti, či narušení systému ochrany dat činností určitého pracovníka nebo pracoviště. *V českém bankovním sektoru došlo v letech 1992 – 1999 celkem k jedenácti zveřejněným nebo známým bankovním počítačovým zločinům ... . Všechny spáchané trestné činy 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 ... . Podle zahraničních údajů je těchto typů podvodů odhaleno velmi malé procento, dokonce až promile*. ... *Jednotliví autoři udávají poměr odhalených a oznámených případů ku nikdy nezjištěným od 1 : 1 000 až po šokujících 1 : 20 000. ... 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.* Nedostatky informačních systémů bank a dalších finančních institucí je třeba hodnotit přísněji než u ostatních institucí, neboť nepracují s vlastními, ale svěřenými prostředky, a také proto, že je vyšší riziko, že následky úspěšných trestných činů neponese jen sama banka, ale především (přímo nebo nepřímo) všichni daňoví poplatníci případně jen klienti banky.

Na druhém místě stojí nedodržování bezpečnostních standardů či chybějící bezpečnostní projekt nebo kontrola jeho dodržování. Některé trestné činy je pak možné spáchat velmi jednoduchým způsobem, který ve svém důsledku téměř znemožní odhalení pachatele. Je velmi problematické vyšetřit útok na data, pokud přístup k terminálu vnitřního systému není kontrolován, pohyb zaměstnanců je naprosto volný včetně příchodů a odchodů ze zaměstnání a přístupové oprávnění zná více osob. V takovém případě se sice jedná o trestný čin podle ustanovení § 257a trestního zákona, ale v souběhu s dalšími trestnými činy majetkové povahy. I když je pachatelem konkrétní osoba, spáchání trestného činu bylo umožněno vnitřním systémem napadeného subjektu.

Někdy je naopak přeceňován stav vnitřní bezpečnosti a zaměstnanci jsou vlivem bezpečnostních opatření pod trvalým tlakem. Navzdory tomu pak dojde k trestnému činu např. tím, že si pachatel odnese data na přenosném médiu.

Problém útoků zevnitř systému je řešitelný lépe než útok z vnějšku. Bezpečnost dat je plně v kompetenci daného subjektu a při správných organizačních a technických bezpečnostních opatřeních je možno rizika minimalizovat. Důležité je např., aby nebyla spojena funkce správce počítačové sítě a osoby, která je odpovědná za její bezpečnost. Žádný systém však nemůže mít bezpečnost na 100 %. Tomuto stavu se lze jen přiblížit.

2.2.3 Kombinovaný útok

Kromě výše popsaných mezních možností existují přirozeně i případy kombinované. Ty můžeme dále rozdělit na úmyslné a neúmyslné.

2.2.3.1 Úmyslné útoky

Zde dochází k selhání zaměstnance či jakékoliv osoby, která má přístup k internímu zabezpečení. Ke konkrétnímu průniku se neodhodlá sama, ale získané informace a poznatky umožňující překonat zabezpečení předá třetí straně, která jich využije k průniku do systému.

2.2.3.2 Neúmyslné jednání umožňující útok

Na internetu jsou volně dostupné nejrůznější modifikace ”backdoors”, které si uživatel na svém systému nevědomky nainstaluje – především z neznalosti. Takové soubory jsou mu buď přímo zaslány s fiktivní adresou nebo je mu poskytnut odkaz a informace, že je instalace takového programového vybavení nutná pro lepší funkci jeho systému. Po nainstalování program umožní osobě mimo firmu mít kontrolu nad počítačem uvnitř celého systému, z kterého se lze mnohem snadněji dostat k citlivým datům. Počítačové viry jsou do velké míry destruktivní programy, které mohou samy mazat nebo pozměňovat programové vybavení na celých systémech nebo vyřazovat servery z provozu. Ve většině firem je nainstalována nějaká antivirová ochrana a firewall, ale i tak může dojít k tomu, že se přes tato opatření dostanou zprávy

s nebezpečným souborem. I zde je hlavní příčinou počítačová negramotnost osob, které bez sebemenších pochybností takové soubory otevírají (například vir ILOVEYOU).

2.2.4 Shrnutí

Útoky na data jakýmkoliv způsobem budou v ČR velmi pravděpodobně dále narůstat tak, jak narůstají od roku 1990. Stejně tak roste jejich nebezpečnost a způsobené škody. Jejich omezení však je dosažitelným cílem.

Úloha Policie ČR odpovídá postavení bezpečnostní složky, jejímž základním úkolem je ochrana občanů a jejich majetku. Bohužel o řadě útoků se Policie ČR nedozvídá, nebo je zjišťuje se značným časovým odstupem. Důvodem tohoto stavu je pravděpodobně nedůvěra v účinnou aktivitu Policie ČR a v případě řady subjektů i obava před zveřejněním útoku a způsobených škod. Především v bankovním sektoru dochází k oznámení trestného činu teprve tehdy, když škoda překročí únosnou hranici, která je různá pro různé banky a pro stav, v jakém se aktuálně nacházejí.

Podle posledních zjištěných informací dochází v ČR k oslabení počtu útoků po internetu a k poklesu zájmu pachatelů o medializaci. Nebezpečnost útoků zároveň stoupá a přibývá pachatelů, zneužívajících svých znalostí za úplatu.

2.3 Další typy trestné činnosti související s informační kriminalitou

Stejnou měrou, jakou získávají informační technologie postavení ve společnosti, se stávají součástí trestné činnosti. Pomocí informačních technologií je již dnes možno spáchat řadu trestných činů, nevyžadujících přítomnost pachatele na místě spáchání trestného činu. To se bude dále prohlubovat s dalším pronikáním informačních a jiných vyspělých technologií do běžného života.

K některým trestným činům, které nelze označit za přímou informační kriminalitu, pachatelé mnohdy informační technologie potřebují, nebo by se bez nich konkrétní trestný čin spáchat nedal. Tím se rozšiřuje problematika informační kriminality i do jiných oblastí.

Policisté, odhalující a objasňující různou trestnou činnost, jsou stále více konfrontováni s nutností pokročilejších znalostí informačních technologií, a vyžadují proto pomoc odborníků při specifických činnostech. To dnes i v budoucnu změní obvyklé způsoby práce policie stejně, jak se mění způsoby páchání trestné činnosti.

Cílem této analýzy není posuzovat paragrafy trestního zákona jeden po druhém a zkoumat, zda se ten který trestný čin dá či nedá spáchat pomocí informačních technologií. Bude věnována pozornost jen některým aspektům trestné činnosti a vybraným trestným činům, kde se ve spojení s informačními technologiemi změnily způsoby chování pachatelů.

Pro mnoho trestných činů je důležitý internet jako masové informační médium a elektronická pošta pro komunikaci mezi pachatelem a poškozeným, případně přímo mezi spolupachateli. Internetová komunikace především usnadňuje výměnu informací pomocí emailů, což je elektronické zasílání správ na adresy konkrétních osob. Vzhledem k masovosti internetu lze téměř za stejných nákladů rozeslat i tisíce až miliony emailů. Bez ohledu na obsah se pak jedná o tzv. spamming, který v české legislativě bude pravděpodobně zakázán jen tehdy, pokud se bude jednat o nevyžádanou reklamu (viz návrh zákona o reklamě). Dále zde existuji tzv. chaty, kdy probíhá komunikace v reálném čase. Dalším efektivním způsobem jsou tzv. konference – je založena určitá emailová adresu, na kterou členové pošlou svůj dotaz nebo jiné sdělení a ten je následně rozeslán i ostatním, jedná se tedy o hromadnější formu zasílání. To umožňuje rychlou komunikaci pachatelů trestné činnosti.

V několika posledních letech dochází k rozšiřování šifrování za užití asymetrického klíče. Technologie je již zvládnuta natolik, že ji může zvládnout běžný uživatel. Délka klíčů a jejich kvalita je taková, že dešifrování hrubou metodou (zkoušení různých kombinací) je odhadováno na cca 10 let. To je doba, která překračuje užitečnost takové aktivity. Problémem je, pokud dochází k šifrování komunikace mezi pachateli trestného činu, jako například zasílání informací o dodávkách drog. Bezpečnostní složky se dostávají do situace, kdy je stále obtížnější zjistit obsah dopravovaných zpráv i přes zákonné povolení. *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. K problematice šifrování je ze zahraničí možno získat značné množství materiálů, je třeba ovšem počítat s tím, že ty nejdůležitější informace zveřejňovány nejsou.

Internet je ideální prostředí pro nabídku jakéhokoliv zboží nebo služby. V kapitole věnované softwarovému pirátství je uveden jeden příklad. To samé ale platí i pro řadu dalších trestných činů jako je šíření poplašné zprávy, pomluva, neoprávněné nakládání s osobnímu údaji a třeba i ohrožování mravnosti. Všeobecně platí, že internet nemá samoregulační mechanismy, které by nedovolily spáchání některých trestných činů. Na internetu jde ve své podstatě pouze o práci s daty, a proto např. stačí jen záměrně zkreslit název souboru či jiný identifikátor, a nikdo není schopen ani při důkladném monitorování zjistit podezřelou činnost. To nejvíce platí o fotografiích a filmových sekvencích dětské pornografie, která je mediálně nejvděčnějším a nejlepším příkladem šíření informace, které je trestným činem (zde ohrožování mravnosti).

Vedle běžných politických stran, sdružení a hnutí se na internetu prezentují i taková uskupení, jejichž činnost je v konfliktu ze zákonem. Běžná anonymita na této síti dává aktivistům takových skupin zdání nepolapitelnosti a zároveň i obrovský prostor pro zveřejnění svých materiálů, které mnohdy směřují k podpoře a propagaci zakázaných hnutí (§ 259 tr. zák.) nebo trestnému činu hanobení národa, rasy a přesvědčení (§198 a § 198a tr. zák.).

Volné šíření informací přináší každému, kdo je dostatečně schopný, má patřičné vybavení a jazykové znalosti, možnost zjištění v podstatě každé dostupné informace o čemkoliv.

Internet je často chápán jako místo s obrovským výskytem kriminality a dalších negativních věcí. Je nutno říci, že internet je přesně takový, jací jsou lidé, kteří ho užívají. Míra kriminality na internetu se podle všeho ještě zvyšuje díky anonymitě, které toto médium skýtá.

V současnosti se jako jedna z cest k řešení internetové kriminality jeví legislativní vyjádření povinnosti přiměřených aktivit subjektů, poskytujících služby na internetu tak, aby vlastními silami kontrolovaly dodržování zákona a ve spolupráci s Policií ČR řešily případy jeho porušování. I pokud by nebylo toto diskutabilní řešení zvoleno, nezbytně třeba je vůči protizákonnému jednání na internetu začít využívat

ustanovení § 202 tr. zák., 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 o ohrožování mravnosti.

2.3.1 Komunikace

V poslední době dochází ke stále většímu propojování počítačové techniky a komunikačních technologií (proto i termín informační kriminalita). Zdá se, že to nebude dlouho trvat a dojde k jejich naprostému splynutí. Proto dochází k trestné činnosti, která již má znaky této budoucnosti. Poskytovatelé mobilní telefonie v ČR i ve světě dělají vše pro to, aby mobilní telefon byl jakýmsi terminálem množství služeb, které v současnosti jsou dostupné cestou výpočetní techniky. Na displeji mobilního telefonu si dnes již mnohý uživatel zobrazí řadu informací. Lze např. posílat krátké textové zprávy. Trestná činnost se děje v případech, kdy jsou zasílány (především prostřednictvím internetových rozhraní, kde je poslání SMS zprávy zcela anonymní záležitostí) zprávy, obsahující výhružky (s rasistickým obsahem např., jak se stalo nedávno) a podvodné texty.

Možnosti Policie ČR řešit tuto kriminalitu velmi závisí na spolupráci všech zainteresovaných, zejména operátorů mobilního připojení.

S problematikou komunikace souvisí i otázka ochrany informací zasílaných pomocí elektronické pošty (e-mailu), tedy zda posílání e-mailu podléhá či nepodléhá ochraně obdobné jako ochrana listovního tajemství. Trestní zákon poskytuje ochranu jednak před porušením tajemství dopravovaných zpráv (§ 239 tr. zákona), jednak před jejich dalším zneužitím (§ 240). Zatímco před porušením jsou chráněna ”tajemství uzavřeného listu nebo jiné písemnosti, zasílaných poštou nebo jiným dopravním zařízením, a dále zprávy podávané telefonem, telegrafem nebo jiným takovým veřejným zařízením” (za ”jiné takové veřejné zařízení” je nepochybně třeba považovat také internet – to znamená že ochrana je poskytována také obsahu e-mailových zpráv), před dalším zneužitím (kdy hrozí přísnější trestní postih) je ale chráněno pouze tajemství, o němž se někdo dozví z písemnosti, telegramu nebo telefonního hovoru, ale nikoliv už z internetu. Jinými slovy, pokud si někdo přečte cizí

e-mail, je stejně trestně odpovědný jako ten, kdo neoprávněně otevře cizí doporučený dopis, zatímco pokud někdo způsobí jinému škodu nebo získá majetkový prospěch tím, že někomu prozradí nebo sám využije informaci získanou porušením např. listovního tajemství, bude přísněji postižitelný, než ten, kdo zneužije informaci získanou přečtením něčího e-mailu. Tato právní úprava je zjevně překonaná, neboť není důvod diferencovat ochranu zasílaných informací podle prostředku jejich dopravy či přenosu. Bylo by vhodné novelizací ustanovení § 240 tr. zákona uvedený nedostatek odstranit.

2.3.2 Elektronické platební prostředky a zneužívání elektronického podpisu

Historie elektronických platebních prostředků je krátká a dynamická. Téměř každý se již setkal s platební kartou nebo nějaký její druh vlastní. Protože se zde jedná o platební prostředky, staly se samozřejmě tyto karty objektem zájmu pachatelů trestné činnosti.

Bezpečnost jejich užívání k placení po internetu je značně široké téma, které má velké množství problematických stránek od organizačních po aplikační. Obecně vzato se elektronické platební prostředky staly současným standardem při placení po internetu a objem jejich užívání generuje trestnou činnost, zaměřenou především na zjišťování údajů z těchto karet a jejich zneužívání. Na rozdíl od používání karet při skutečném nakupování, zde stačí zadat číslo kreditní karty a datum expirace, žádné další ověření není nutné. Základním bezpečnostním prvkem při placení po internetu je zabezpečená komunikace mezi vlastníkem karty (jeho počítačem) a počítačem (serverem) internetového obchodníka. Bohužel je nutno konstatovat, že řada elektronických obchodů v ČR tuto oblast neřeší a vystavuje tím zákazníka prozrazení údajů o platební kartě a tím možnosti jejich zneužití pachatelem trestného činu.

Používání moderních telekomunikačních prostředků, jakými jsou elektronická pošta, elektronická výměna dat (EDI), ale i telefaxy a jiné prostředky umožňující dálkový přístup za účelem provádění obchodních transakcí se rapidním tempem zvyšuje a lze očekávat, že se bude dále rozvíjet s tím, jak se informační dálnice a

internet stanou dostupnějšími. Komunikace sdělující závažné informace právní povahy formou netištěných zpráv však může narazit na překážky v právní oblasti, které by zabraňovaly jejich používání či by mohly vyvolat námitky ohledně jejich důkazní hodnoty. Proto byl připraven zákon o elektronickém podpisu, který byl chválen Parlamentem České republiky a posléze nabyl účinnosti 1. října 2000.

Klíčová myšlenka zákona, že informaci nelze upřít právní důsledky, platnost nebo vykonatelnost jen proto, že má formu datové zprávy, je jistým převratem v doposud omezeném chápání písemností a dokumentace jakožto informací výlučně spjatých s papírovým nosičem. Základním principem je zrovnoprávnění datových zpráv s běžnou ”papírovou” formou komunikace, tj. že nesmí existovat rozpor v zacházení mezi datovými zprávami a dokumenty na papíře. Zákon se zabývá základními pojmy používanými v obchodování, jako jsou ”dokument”, ”podpis”, ”vypracování smluv a jejich platnost”, ”uznání datových zpráv stranami”, ”potvrzení příjmu” apod. Začlenění zákona o elektronickém obchodě do českého právního systému vytvořilo legislativní podmínky pro skutečný rozvoj elektronického obchodování. Elektronický podpis může (s ohledem na technologické principy) znamenat mnohem větší míru právní jistoty než klasická komunikace, o to nebezpečnější je jeho případné zneužití. Zneužívaní elektronického podpisu je také identifikováno jako jedno z možných nebezpečí, které přinášejí moderní informační technologie.

2.3.3 Jména domén v internetu

Aby bylo možné jednoznačně identifikovat a adresovat každý z mnoha miliónů počítačů připojených k internetu, bylo třeba přidělit jednotlivým serverům určité adresy a tyto adresy hierarchicky uspořádat do tzv. domén (Domain Name Systém – DNS). Domény nejvyšší úrovně jsou tzv. generické a označeny známými koncovkami COM (komerční), ORG (organizace), GOV (vládní), MIL (vojenské), EDU (vzdělávací). Ostatní země mají každá přidělenu doménu nejvyšší úrovně (ne generickou) na základě názvu státu (CZ – Česká republika např.). Domény druhé úrovně (např. MVCR nebo SEZNAM) určují rozdělení serverů na daném území. Způsob, jakým jsou na území každého státu přidělována jména právě těchto domén druhé úrovně, má velkou důležitost pro využívání internetu v dané zemi.

V současnosti se v ČR vede nejvíce sporů o pravidla přidělování jmen domén (kdo má ”právo” na doménu PRAHA nebo SKODA např.) a o roli organizace, která národní doménu spravuje (v ČR je to dosud zájmové sdružení právnických osob CZ.NIC, vedené v Registru ekonomických subjektů s činnostmi 700 – soukromé neziskové instituce poskytující služby převážně domácnostem a 15 000 – neziskové instituce sloužící domácnostem, což se zdá být poněkud v rozporu se skutečností, CZ.NIC má naprostý monopol na činnost s celostátním významem, jež má postupně stále větší hospodářský dopad, a dále s tím, že za svoji činnost (přidělování a udržování domén v počtu přibližně 40 000) vybírá poplatky, jejichž výši lze odhadnout na 40 – 50 miliónů Kč ročně. Protože česká legislativa nestanovuje žádná pravidla pro registraci doménového jména, funguje jejich přidělování systémem ”kdo dřív přijde”. Tato situace s sebou přináší řadu konfliktních situací – není totiž stanoven právní režim domény. Např. ve Spojených státech takovou aktivitu řeší Anticybersquatting Consumer Protection Act (Zákon na ochranu spotřebitele před zabíráním domén). Bylo by v této souvislosti vhodné legislativně upravit právní režim doménových jmen.

3. Organizační zabezpečení boje proti informační kriminalitě v rámci ministerstva vnitra České republiky

Řešení problematiky nejefektivnějšího postupu proti trestné činnosti související s informačními technologiemi znamená stanovit optimální kompromis mezi ”distribuovaným” přístupem, kdy je všechno prováděno separátně všemi zainteresovanými subjekty, a ”centralizovaným” přístupem, kdy je na boj s internetovou kriminalitou zřízeno jedno centrální pracoviště. Nevýhoda ”distribuovaného” přístupu je nízká koordinace aktivit a nemožnost soustředit prostředky i lidi do jednoho pracoviště. Nevýhoda ”centralizovaného” přístupu je ztráta zdravého konkurenčního prostředí a obtížné stanovení skutečné úrovně práce jediného centrálního pracoviště. Zdá se, že nejvhodnější bude kombinace obou přístupů, kdy by v jednom nebo lépe několika málo centrálních pracovištích působili specialisté a metodici, a jednotlivé policejní útvary v krajích a další útvary s celostátní působností by měly podle své specializace pro informační kriminalitu stanoveny určité jednotlivce nebo skupiny. Systém boje proti počítačové kriminalitě se v rámci Policie ČR vyvíjí, je především nutné vyladit základní postupy a systém odborného řízení. Vzhledem k úrovni platů v resortu MV je velmi obtížné získat pro takovou práci špičkové specialisty, bez nichž kvalita a tím i efektivita práce nemůže být příliš vysoká. Odborníci působící v oblasti prevence a represe proti informační kriminalitě musí disponovat mezioborovými znalostmi: od informatiky přes bezpečnost informačních systémů až po právní disciplíny.

U Ředitelství služby kriminální policie Policejního prezidia (od 15. 1. 2001 kriminální úřad Policejního prezidia) bylo v polovině roku 1999 vytvořeno pracoviště boje proti počítačové kriminalitě (Skupina informační kriminality), jako orgán metodického řízení kriminální policie, které má za úkol položit kvalitní základy činnosti policie ve dvou základních oblastech:

1. Odhalování a objasňování trestné činnosti na úseku:
    a) ochrany duševního vlastnictví spojeného s informačními technologiemi,
    b) ochrany dat,

c) elektronického obchodu, elektronických platebních prostředků a kryptografické komunikace.

2. Vyhledávání a dokumentování trestné činnosti na internetu.

V obou těchto oblastech se zaměřuje na:

- sledování nových trendů, informování a upozorňování na bezpečnostní rizika,
- mezinárodní spolupráci pro zařazení ČR do evropského a světového systému boje proti trestné činnosti v rámci informačních technologií,
- vytvoření podmínek pro boj Policie ČR s uvedenými formami trestné činnosti.

Hlavními úkoly jejích pracovníků je:

- odhalovat, objasňovat a dokumentovat trestné činy operativně pátrací činností nebo konáním trestního řízení,
- koordinovat činnost útvarů služby kriminální policie s územně vymezenou působností a poskytovat jim osobní a metodickou pomoc,
- podílet se na profesní přípravě pracovníků služby kriminální policie na jednotlivých krajských a okresních úrovních a také u speciálních útvarů Policie ČR,
- spolupracovat s resortními i mimoresortními subjekty, působícími na vymezených úsecích trestné činnosti,
- analyzovat příčiny a podmínky páchání vymezené trestné činnosti a předkládat návrhy na jejich omezování.

Jakmile budou nižší útvary služby kriminální policie dostatečně připraveny na odhalování trestných činů v rámci počítačové kriminality, pracoviště u kriminálního úřadu Policejního prezidia si ponechá pouze metodické, koordinační a některé řídící pravomoci, především v oblasti závažné a mezinárodní trestné činnosti.

Otázkou je míra podílu specializovaných složek policie na stíhání informační kriminality. V rámci uvažované koncepce soustředění složek policie podílejících se na boji s trestnou činností do jednoho kriminálního úřadu zůstane pochopitelně zachován systém specializovaných jednotek zaměřených na konkrétní složitou oblast trestné činnosti (závažná hospodářská a finanční kriminalita, organizovaný zločin, drogová problematika). Informační kriminalita bude s dalším rozvojem moderních technologií stále více využívána i pachateli těchto zvláště sledovaných trestných činností. Nezbytné tedy bude postupné budování kapacit pro boj s informační trestnou činností i v rámci těchto speciálních jednotek. V současné době se má do

konce roku 2001 zřídit internetové pracoviště při PČR útvaru pro odhalování organizovaného zločinu služby kriminální policie. Tato služba PČR nyní provádí monitoring internetu, zejména v oblasti obchodu s lidmi a dětské pornografie.

V rámci resortu se počítačovou kriminalitou rovněž zabývají pracoviště na Kriminalistickém ústavu Praha (KÚP) a Policejní akademie České republiky (PA).

Lze říci, že problematika informační kriminality byla řešena, z pohledu předpokládaného zajišťování důkazních hodnot expertizním zkoumáním, jako první právě v KÚP, kde od konce roku 1990 probíhaly intenzivní přípravy na vytvoření specializovaného pracoviště počítačových expertiz. Toto pracoviště zakrátko zahájilo svoji práci a v roce 1993 bylo začleněno do organizační struktury KUP jako oddělení počítačové kriminality, později oddělení počítačové expertizy a od té doby podává znalecké posudky a odborná vyjádření v oboru kriminalistika, odvětví kriminalistická počítačová expertiza. Pro toto odvětví je od roku 1993 KÚP zapsán v příslušném Seznamu znalců vedeným Ministerstvem spravedlnosti.

Po linii kriminalistickotechnické a expertizní činnosti PČR doznala za krátkou dobu počítačová expertiza dynamický rozvoj. Už v roce 1996 byla zahájena výstavba expertizních pracovišť i na všech pracovištích kriminalisticko technické expertízy kriminální policie Správ krajů a hl. m. Prahy. Po nezbytném materiálovém a personálním zajištění a vyškolení expertů je toto expertizní odvětví zastoupeno od roku 1998 na všech krajských pracovištích. Taková dynamika rozvoje expertizního zkoumání v daném oboru byla dána nárůstem požadavků na zkoumání, zejména z řad vyšetřovatelů, který korespondoval se stoupajícím zneužíváním pro trestnou činnost nesmírně dynamicky se rozvíjejících samotných informačních technologií.

Snahy o dosažení maximální kvality expertizního zkoumání se projevily i na poli mezinárodních aktivit oddělení počítačové expertizy KÚP. První mezinárodní kontakty vznikaly už od roku 1994 směrem k Interpolu v Lyonu. Další kontakty však bylo potřebné hledat jinde, protože na úrovni Interpolu se neřešily konkrétní problémy expertizního (forenzního) zkoumání. Pro rozvoj mezinárodní spolupráce KUP bylo, z odborného hlediska, nejdůležitější událostí vznik ENFSI (Evropská síť forenzních vědeckých ústavů) v roce 1995 a přijetí KÚP do této organizace v roce 1998.

Dosavadním vyvrcholením práce expertů počítačové expertizy byla skutečnost, že KÚP byla dána důvěra ENFSI k zorganizování ustanovujícího setkání

pracovní skupiny předních evropských forenzních expertů v oboru informační kriminality. Setkání se uskutečnilo v září 1998 v Praze.

Policejní akademie ČR v rámci výzkumné činnosti řeší přibližně od roku 1996 "Kriminalistickou problematiku při odhalování, vyšetřování a prevenci počítačové kriminality". V rámci této práce vydává PA odborné sborníky a zpracovává studie dotýkající se problematiky informační kriminality.

V současné době se kriminální policie i útvary, které tento typ kriminality analyzují potýkají s řadou potíží, spojených s relativní novostí tohoto typu kriminality. Tak např. v Evidenčně statistickém systému kriminality (ESSK) není na vstupních formulářích do systému zavedena obecná položka ”použití počítače”, obdobná položce 07 formuláře trestného činu ”použití zbraně”, ale trestná činnost spáchaná pomocí výpočetní techniky se eviduje výhradně prostřednictvím hlediska hospodářské trestné činnosti (položka č. 16 a 17), včetně trestného činu poškození a zneužití záznamu na nosiči informací (§257a), který trestní zákon řadí mezi trestné činy proti majetku. Bylo by proto vhodné příslušný číselník odpovídajícím způsobem upravit.

4. Důležité mezinárodní aktivity v boji proti počítačové kriminalitě

4.1 Návrh mezinárodní dohody o ”kyberzločinu” vypracovaný Radou Evropy

Rada Evropy začala projevovat zájem o řešení problematiky hackerství a další počítačové kriminality již koncem osmdesátých let. V roce 1989 publikovala studii, obsahující zprávu o počítačové kriminalitě, a doporučení pro úpravy a vytváření nových zákonů jednotlivých států, které by měly kriminalizovat určité činy, spáchané prostřednictvím počítačových sítí (viz Doporučení RE č. 9 z r. 89). Následovala další studie, publikovaná v roce 1995, která obsahovala principy, týkající se trestněprávního postupu souvisejícího s informačními technologiemi (viz Doporučení RE č. 13 z r. 95). V roce 1997 byla ustavena Komise expertů na zločin v kyberprostoru (Commitee of Experts on Crime in Cyber-Space – PC-CY), aby začala práci na návrhu mezinárodní dohody, která by usnadnila mezinárodní spolupráci při zjišťování a pronásledování počítačových zločinů. Koncem roku 2000 byla zveřejněna pravděpodobně již téměř definitivní, 25. verze textu. Během roku 2001 komise zapracuje připomínky, finalizuje text a vypracuje vysvětlující memorandum, což je autoritativní vysvětlení textu Dohody (jeho návrh byl již zveřejněn v únoru 2001). Pak předá text k dalšímu zpracování Evropskému výboru pro problémy zločinu (European Commitee on Crime Problems – CDPC), a ten Radě ministrů. Podle současných plánů by Dohoda měla být připravena k podpisu (všemi 41 členy Rady Evropy a dalšími státy, které se zúčastnily vyjednávání nebo k podpisu budou pozvány) před koncem roku 2001.

Dohoda je prvním mezinárodněprávním instrumentem, určeným speciálně pro řešení problémů spojených s mezinárodním charakterem počítačového zločinu. Dohoda zejména požaduje, aby signatářské země kriminalizovaly určitá jednání, které je možné zařadit do oblasti počítačového zločinu, a dále požaduje, aby tyto země přijaly procesní normy, umožňující tuto trestnou činnost postihovat. Tím poskytuje pevnou základnu mezinárodní trestněprávní spolupráci v boji se zločinem,

spáchaným prostřednictvím informačních systémů. Dohoda sama nebude obsahovat detailní vzory jednotlivých národních legislativ a procesních norem, ale bude své požadavky formulovat poměrně obecně.

Skutky, spadající do počítačového zločinu, jsou rozděleny následovně:

1. zločiny proti důvěrnosti, integritě a dosažitelnosti počítačových dat a systémů, které se dále dělí na:
    - nezákonný přístup,
    - nezákonné odposlouchávání,
    - narušování dat,
    - narušování systémů,
    - zneužití prostředků,
2. zločiny se vztahem k počítači, které jsou děleny na
    - počítačové padělání a
    - počítačový podvod,
3. zločiny se vztahem k obsahu počítače, což je především dětská pornografie,
4. zločiny se vztahem k autorským nebo obdobným právům.

Kriminalizován je také návod a napomáhání k výše uvedeným typům zločinů, řešena je také otázka deliktní odpovědnosti právnických osob.

V oblasti procesních norem jsou pojednána obecná opatření pro všechny typy zločinů, dále zvláště opatření pro vyhledávání a zajišťování dat, uložených v počítačích nebo přijímaných v reálném čase (v průběhu vlastní komunikace).

V oblasti mezinárodní spolupráce jsou zpracovány principy a konkrétní způsob vzájemné pomoci jednotlivých států při vyšetřování počítačové kriminality, včetně takových otázek, jako vydávání osob, způsob předávání zajištěných dat i způsobů předávání požadavků.

4.2 *e*Europe 2002

V oblasti počítačové kriminality je v posledních 3 – 4 letech zvláště aktivní také

Evropská unie. Význačným činem je akční plán *e*Europe 2002 (dále jen Plán), který byl přijat v červnu r. 2000 a který má být splněn do roku 2002. Všechny zainteresované strany byly vyzvány, aby k Plánu, který je zveřejněn na internetu, zasílaly připomínky.

Plán v kapitole 1. zdůrazňuje velkou důležitost bezpečnosti počítačových sítí a boje proti kyberzločinu. Jeho cílem je zvýšit bezpečnost informačních infrastruktur a zajistit, aby orgány činné v trestním řízení měly veškeré přiměřené prostředky k činnosti. Zároveň požaduje plné respektování základních práv člověka.

Kapitola 2. je věnována bezpečnosti informačních infrastruktur. Je zde zmíněna m.j. potřeba používání šifrování pomocí veřejného klíče, využívání kvalitních antivirových programů i firewallů, identifikačních prostředků karetních či biometrických, elektronických podpisů apod.

V kapitole 3 jsou počítačové zločiny rozděleny na:

1. zločiny porušující soukromí (ilegální sbírání, uchovávání, modifikace, zveřejňování a šíření osobních dat),
2. zločiny se vztahem k obsahu počítače (pornografie, zvláště dětská, rasismus, vyzývání k násilí apod.),
3. ekonomické (neautorizovaný přístup a sabotáž, hackerství, šíření virů, počítačové špionáž, počítačové padělání a podvody apod.),
4. zločiny se vztahem k duševnímu vlastnictví (autorské právo apod.).

Kapitola 4. pojednává o problematice zákonů, kapitola 5. o problematice procesních norem, a to velmi podrobně. Jsou uvedeny otázky monitoringu komunikace, zajištění dopravovaných dat, anonymního přístupu a užití zdrojů, praktické spolupráce na mezinárodní úrovni, jurisdikce a hodnoty počítačových dat v důkazním řízení. Kapitola 6. rozebírá (rovněž velmi podrobně) otázky nelegislativních opatření jako je činnost specializovaných jednotek na národní úrovni, speciálního výcviku, zlepšené informace a společná pravidla pro komunikační protokoly. Je zmíněna možná spolupráce na úrovni EU i spolupráce s nestátní sférou. V závěrečné 7. kapitole je problematika shrnuta a jsou zde předneseny návrhy v legislativní i nelegislativní oblasti.

4.3 Deset principů a desetibodový akční plán skupiny G8

Ministři spravedlnosti a vnitra zemí skupiny G8 přijali v prosinci roku 1997 deset principů a desetibodový akční plán, který byl následně podepsán na Birminghamském summitu skupiny G8 v květnu 1998.

Deset principů shrnuje cíle zúčastněných států v boji s ”high-tech” zločinem (pojem ”high-tech” zločinu se obsahově prakticky kryje s pojmem ”kyberzločinu” či s pojmem zločinu v ”kyberprostoru” i s námi používanými pojmy počítačové, informační a komunikační kriminality). Jedná se o tyto základní postuláty:

1. Nesmí existovat bezpečné útočiště pro ty, kteří zneužívají informační technologie.
2. Vyšetřování a trestní řízení v oblasti mezinárodního ”high-tech” zločinu musí být koordinováno mezi všemi zúčastněnými státy bez ohledu na to, kde se škoda stala.
3. Orgány prosazující zákonnost musí být dostatečně vyškoleny a vybaveny pro potírání ”high-tech” zločinu.
4. Právní systémy musí chránit důvěrnost, integritu a dosažitelnost dat a systémů před neoprávněným narušením a zajistit, aby jejich vážné zneužití bylo trestáno.
5. Právní systémy by měly zajistit zachování elektronických dat a rychlý přístup k nim, což je jedním ze základních předpokladů pro úspěšné vyšetření této trestné činnosti.
6. Vzájemná spolupráce vlád musí zajistit včasný sběr a výměnu důkazů v případech zahrnujících ”high-tech” zločin.
7. Přeshraniční přístup právo prosazujících orgánů k veřejně dostupným informacím (z tzv. otevřených zdrojů) nesmí být podmíněn povolením od státu, na jehož území jsou data fyzicky umístěna.
8. Pro vyhledávání a ověřování elektronických dat při kriminálním vyšetřování a trestním řízení musí být vyvinuty a používány příslušné forenzní standardy.
9. Informační a komunikační systémy by měly být pokud možno navrženy tak, aby přispívaly k obraně proti zneužití sítí, k detekci takového zneužití a měly by usnadnit vystopování zločinců a sběr důkazů.

10. Veškeré aktivity v této oblasti by měly být koordinovány s činností ostatních relevantních mezinárodních fór, aby se zabránilo zdvojování těchto aktivit.

Tyto obecné a do jisté míry proklamativní principy jsou konkretizovány v Akčním plánu pro potírání ”high-tech” zločinu. Příslušné orgány mají za úkol:

1. Využít vybudovanou síť odborného personálu, aby byla zajištěna včasná a efektivní odpověď na nadnárodní případy informační kriminality a ustanovit styčná místa, která budou dosažitelná 24 hodin denně.
2. Přijmout odpovídající opatření k zajištění dostatečných kapacit orgánů prosazujících zákonnost (náležitě odborně a materiálně vybavených), tyto orgány musí být připraveny postihovat ”high-tech” zločin a vzájemně spolupracovat s příslušnými orgány jiných států.
3. Provést revizi právních systémů tak, aby bylo dostatečně kriminalizováno zneužití telekomunikačních a počítačových systémů, a dále podporovat odhalování ”high-tech” zločinu.
4. Při vyjednávání dohod a ujednání o vzájemné pomoci brát v úvahu otázky spojené s ”high-tech” zločinem.
5. Pokračovat ve zkoumání a rozvíjení prakticky proveditelných řešení, které se týkají zachování důkazů před vydáním soudního rozhodnutí, přeshraničních prohlídek a prohledávání dat v počítačích v těch případech, kdy není známo umístění těchto dat.
6. Vyvinout urychlené postupy pro získání provozních dat ze všech komunikačních prostředků v řetězci komunikace, studovat způsoby urychleného mezinárodního předávání těchto dat.
7. Spolupracovat s průmyslovými odvětvími tak, aby bylo zajištěno, že nové technologie usnadní boj s ”high-tech” zločinem (umožní zachování a sběr důležitých důkazů).
8. Vytvořit mechanismy pro zajištění bezprostředního přijetí požadavků vzájemné pomoci v naléhavých a důležitých případech a včasných odpovědí na ně pomocí rychlých a dostatečně spolehlivých prostředků komunikace (i prostřednictvím hlasu, faxu nebo e-mailu, spolu s případným dodatečným písemným potvrzením).
9. Podpořit organizace, zabývající se tvorbou mezinárodně uznávaných

standardů v oblasti telekomunikačních a informačních technologií, aby trvale poskytovaly veřejnému i privátnímu sektoru standardy technologií bezpečné telekomunikace a zpracování dat.

10. Vyvinout a použít kompatibilní forenzní standardy pro vyhledávání a ověřování elektronických dat při kriminálním vyšetřování a trestním řízení.

Skupině G8 se již podařilo splnit jeden z nejdůležitějších bodů, bod 1. Ke konci roku 2000 se již asi 20 zemí podílelo na síti kontaktních míst dosažitelných nepřetržitě 24 hodin denně a 7 dní v týdnu. Je žádoucí, aby byl počet těchto zemí co nejvíce rozšířen. Bylo by vhodné, aby se také Česká republika vážně zabývala myšlenkou konstituování obdobného styčného místa.

Obsah