JUDr. Jan Kolouch

Trestněprávní ochrana před kybernetickou trestnou činností v ČR a SR

Cílem článku je provést komparaci české a slovenské právní úpravy, zejména hmotně právních ustanovení týkajících se kybernetické trestné činnosti[1]. Záměrně jsem si vybral Slovenskou republiku, důvodů k mému výběru bylo několik. V současnosti dochází v rámci Evropské unie k implementaci právních norem schopných efektivně ochránit společnost před kybernetickou trestnou činností a zároveň postihnout pachatele této trestné činnosti. K „účinnému“ trestněprávnímu postihu kybernetické trestné činnosti dochází v současné době pouze na území USA[2], a to jen díky obrovské odlišnosti jejich právního systému jako takového. Slovenská republika, stejně jako Česká republika podepsala ve stejném období Úmluvu o kyberkriminalitě[3], avšak na rozdíl od České republiky ji již ratifikovala[4] a tento akt by se měl odrazit i v trestním

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

2 Kde například došlo, jak již bylo uvedeno, i k trestně právnímu postihu spammera.

3 Blíže viz Úmluva Rady Evropy o kyberkriminalitě. Úplné znění Úmluvy v anglickém jazyce je možné nalézt na World Wide Web: <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm> [cit. 8.3.2008].

4 [cit. 28.3.2008]. Dostupné na World Wide Web:

<http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>

právu.[5] Mimo jiné i proto se domnívám, že je právní úprava Slovenské republiky velmi vhodná k provedení komparace.

Článek je rozdělen do dvou hlavních částí. V první z nich dochází k popisu slovenské trestněprávní úpravy kybernetické trestné činnosti a k její komparaci s trestněprávní úpravou České republiky de lege lata. Druhá část článku se pak věnuje české právní úpravě kybernetické trestné činnosti de lege ferenda (v rámci ní by mělo dojít k implementaci některých ustanovení z Úmluvy o kyberkriminalitě do českého právního systému).

PRÁVNÍ ÚPRAVA KYBERNETICKÉ TRESTNÉ ČINNOSTI V SR

Na Slovensku došlo v roce 2005 ke kompletní rekodifikaci trestních zákonů. Rekodifikace trestního práva vycházela z nutnosti změn trestních zákonů s přihlédnutím ke společenským, politickým a ekonomickým změnám, které nastaly po roce 1989. V rámci slovenského trestního práva bylo třeba reflektovat změny související se vstupem Slovenska do EU. Výsledkem této činnosti bylo schválení zákona č. 300/2005 Z.z., trestný zákon a zákona č. 301/2005 Z.z., trestný poriadok.

Schválené zákony především zabezpečují ochranu základních lidských práv a svobod, jakožto i dalších práv, které jsou zakotveny v Listině základních práv a svodod (úst. zák. č. 23/1991 Sb.) a Ústavě Slovenské republiky (č. 460/1992 Z.z.) prostřednictvím trestního práva, kde trestní právo plní subsidiární funkci.

a) Vymezení pojmu trestný čin

Jednou z největších změn je právě nové pojetí trestného činu v rekodifikovaném slovenském trestním zákoně. Trestný čin nově vychází ze zcela formálního pojetí, kde odpadá materiální korektiv. Právě ten byl často kritizován, že dochází k jeho využívání

5 Například Velká Británie uvedenou úmluvu také zatím neratifikovala.

jak ve prospěch, tak neprospěch pachatele. Formální pojetí trestného činu by pak mělo lépe zaručit ústavně garantovanou zásadu rovnosti před zákonem.

„Formálne chápanie trestného činu umožní súčasne orgánom činným v trestnom konaní sústrediť sa na základné otázky trestného konania a to zistenie trestného činu a jeho páchateľa.[6]*“*

Pro to, aby byl čin posuzován jako trestný, musejí být současně splněny dvě podmínky:

1.Musí jít o protiprávní čin,

2.jeho znaky musejí být uvedeny v trestním zákoně, pokud tento zákon nestanoví jinak (§ 8 zák. č. 300/2005 Z.z.).

Určitý korektiv společenské závažnosti (nebezpečnosti) se však z trestního zákona nevytratil. Jednak je závažnost dána tím, že zákonodárce označil určité činy za trestné činy a dále je v zákoně uvedena možnost, že i při naplnění znaků skutkové podstaty ***nejde o trestný čin, pokud je jeho závažnost nepatrná a u mladistvého malá, pokud jde o přečin***.[7] Je tedy otázkou, zda se jedná o čistě formální pojetí, neboť pojem **závažnost** (§ 10 odst. 2 zák. č. 300/2005 Z.z.) do jisté míry nahrazuje pojem „stupeň nebezpečnosti činu pro společnost“. V rámci trestního řádu jsou pak zakotveny i další možnosti odklonů (např.: dohoda o upuštění od potrestání § 232 odst. 3 zák. č. 301/2005 Z.z., nebo podmíněné upuštění od potrestání).

Ve slovenském trestním právu se opět zavádí tzv. **bipartice** tzn., že pojem trestný čin zahrnuje dvě kategorie protiprávních jednání, a to **přečiny** a **zločiny.**

Dle ustanovení **§ 10** je **přečinem:**

a)trestný čin spáchaný z nedbanlivosti alebo

6[cit. 6.8.2005]. Dostupné na World Wide Web:

<http://www.nrsr.sk/appbin/Tmp/D%F4vodov%E1%20spr%E1va-NR%20SR-febr.2005.rtf>

7§ 95 odst. 2 zák. č. 300/2005 Z.z., trestný zákon

b)úmyselný trestný čin, za ktorý tento zákon v osobitnej časti ustanovuje trest odňatia slobody s hornou hranicou trestnej sadzby neprevyšujúcou päť rokov.

(2) Nejde o prečin, ak vzhľadom na spôsob vykonania činu a jeho následky, okolnosti, za ktorých bol čin spáchaný, mieru zavinenia a pohnútku páchateľa je jeho závažnosť nepatrná.[8]

Zločin je v ustanovení § 11 vymezen takto:

(1) Zločin je úmyselný trestný čin, za ktorý tento zákon v osobitnej časti ustanovuje trest odňatia slobody s hornou hranicou trestnej sadzby prevyšujúcou päť rokov.

(2) O zločin ide aj vtedy, ak v prísnejšej skutkovej podstate prečinu spáchaného úmyselne je ustanovená horná hranica trestnej sadzby prevyšujúca päť rokov.

(3) Zločin, za ktorý tento zákon ustanovuje trest odňatia slobody s dolnou hranicou trestnej sadzby najmenej osem rokov, sa považuje za obzvlášť závažný.[9]

Záměrem zákonodárce bylo zřejmě přesněji vyjádřit společenskou závažnost a škodlivost, jakož i provést diferenciaci závažnějších forem trestné činnosti od méně závažných forem trestné činnosti. Dalším důvodem je i zrychlení trestního řízení a možnost využití zmíněných odklonů v případě přečinů. Ustanovením § 10 odst. 2 zák. č. 300/2005 Z.z. je sledována možnost vyloučení soudního projednávání „bagatelních“ přečinů.

b)Hmotně právní úprava kybernetické trestné činnosti

Další viditelnou změnou v rámci slovenského trestního zákona je přeměna struktury zvláštní části tohoto zákona, která má lépe odrážet hierarchii zájmů chráněných trestním zákonem.

8§ 10 zák. č. 300/2005 Z.z., trestný zákon

9§ 11 zák. č. 300/2005 Z.z., trestný zákon

V této části článku uvedu jednotlivá ustanovení slovenského trestního zákona, která se zabývají kybernetickou trestnou činností. Vzhledem k rekodifikaci obsahuje zák. č. 300/2005 Z.z. některá nová ustanovení, která jsou více zaměřena na trestnou činnost páchanou prostřednictvím informačních a komunikačních technologií. U srovnatelných ustanovení se pokusím vystihnout odlišnosti od české právní úpravy.

c)Porušování práva autorského

V slovenském trestním zákoně je ochrana autorského práva upravena v ustanovení **§ 283** zák. č. 300/2005 Z.z. (Hl. V., oddíl 4 – trestné činy proti průmyslovým právům a proti autorskému právu). Ochrana práva autorského je de facto totožná jako v českém trestním právu, s tou výjimkou, že slovenská právní úprava obsahuje tři kvalifikované skutkové podstaty:

(2) Odňatím slobody na šesť mesiacov až tri roky rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a)a spôsobí ním väčšiu škodu,
b)závažnejším spôsobom konania,
c)z osobitného motívu, alebo
d)prostredníctvom počítačového systému
(3) Odňatím slobody na jeden rok až päť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 a spôsobí ním značnú škodu.
(4) Odňatím slobody na tri roky až osem rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1
a)a spôsobí ním škodu veľkého rozsahu, alebo
b)ako člen nebezpečného zoskupenia.

Jiná skutečnost uvedená v ustanovení **§ 283 odst. 2 písm. d)** reaguje na masivní nárůst softwarového pirátství a na způsob jeho páchání prostřednictvím počítačů a počítačových sítí.

d)Poškození a zneužití záznamu na nosiči informací

Poškození a zneužití záznamu na nosiči informací je obsaženo v ustanovení **§ 247** zák. č. 300/2005 Z.z. (Hl. IV. - trestné činy proti majetku). Zásadní změna oproti české právní úpravě nastala v rámci základní skutkové podstaty, kde byl vložen nový druh jednání:

d)***vkladaním, prenášaním, poškodením, vymazaním, znížením kvality, pozmenením alebo potlačením počítačových dát marí funkčnosť počítačového systému alebo***

vytvára neautentické dáta s úmyslom, aby sa považovali za autentické alebo aby sa s nimi takto na právne účely nakladalo,
potrestá sa odňatím slobody na šesť mesiacov až tri roky.

Dále došlo k vložení základní skutkové podstaty, která nově postihuje nelegální sledování přenosu dat (tzv. sniffing) a činnost crackerů. Otázkou je, zda je vhodné trestněprávně postihovat pouhé obstarání si programu umožňujícího prolamovat hesla (crackeru či keygenu) či přístupového kódu k počítačovému systému. Na druhou stranu je pochopitelná snaha slovenského zákonodárce po postihnutí stále častějších průniků do počítačových systémů.

(2) Rovnako ako v odseku 1 sa potrestá, kto na účel spáchania činu uvedeného v odseku 1
a)***neoprávnene sleduje*** *prostredníctvom technických prostriedkov* ***neverejný prenos počítačových dát do počítačového systému, z neho alebo v rámci počítačového systému****, alebo*
b)***zaobstará alebo sprístupní počítačový program a iné zariadenia alebo počítačové heslo, prístupový kód alebo podobné údaje umožňujúce prístup do celého počítačového systému alebo do jeho časti****.*

Domnívám se, že vhodnější by asi bylo formulovat část tohoto ustanovení [odst. 2 písm. b)] například takto:

„kdo neoprávněně pronikne do počítačového systému či jeho součásti za použití programu, jiného zařízení či jiným způsobem“. Takováto formulace by postihovala i neoprávněné průniky, jejichž cílem není poškodit či jinak zneužít data.

e)<u>Ochrana přepravovaných zpráv</u>

Nově je v ustanovení **§ 198** zák. č. 300/2005 Z.z. zakotvena ochrana proti sniffingu.

„Kto v rozpore so všeobecne záväzným právnym predpisom ***vyrobí****, sebe alebo inému* ***zadováži*** *alebo* ***prechováva*** *zariadenie spôsobilé na odpočúvanie informácií prenášaných prostredníctvom elektronickej komunikačnej služby, potrestá sa odňatím slobody až na tri roky.“*

Bohužel není tímto ustanovením postihován nelegální odposlech, ale pouze vlastnění, obstarání nebo přechování prostředku způsobilého provádět nelegální odposlech.

Vlastní **ochrana** přepravovaných zpráv, mezi které je možné zařadit i **přenos informací přenášených prostřednictvím elektronické komunikační služby**[10], je poskytována ustanoveními **§ 196 a 197** zák. č. 300/2005 Z.z. - Porušování tajemství dopravovaných zpráv. Ustanovení § 196 zároveň chrání i bezdrátový přenos[11] mezi počítačem a jiným zařízením.

§ 196

(1)Kto úmyselne poruší
a)listové tajomstvo vyzvedaním alebo otvorením uzavretého listu alebo inej písomnosti prepravovanej poštovým podnikom alebo iným obvyklým spôsobom,
b)***tajomstvo informácie prenášanej prostredníctvom elektronickej komunikačnej služby**, alebo*
c)***tajomstvo neverejného prenosu počítačových dát do počítačového systému**, z neho alebo v jeho rámci, **vrátane elektromagnetického vyžarovania z počítačového systému, prenášajúceho takéto počítačové dáta**,*
potrestá sa odňatím slobody až na tri roky.

Na závěr hmotně právní úpravy lze konstatovat, že zákonodárci slovenské republiky se snažili reagovat na nové formy trestné činnosti páchané prostřednictvím informačních a komunikačních technologií. Uvedené změny jsou značně pokročilé, avšak ne zcela reagují na již zmíněnou Úmluvu o kyberkriminalitě, kterou Slovensko ratifikovalo.

f)Procesně právní úprava

V rámci procesně právní úpravy chci pouze upozornit na ustanovení týkající se odposlechu a záznamu telekomunikačního provozu § 115 a 116 zák. č. 301/2005 Z.z. Tato ustanovení jsou prakticky totožná s ustanovením § 88 a 88a tr. řádu a užije se jich obdobně jako v České republice k odhalování a objasňování softwarové a internetové trestné činnosti. Jedinou výjimkou je, že v rámci § 116 (záznam telekomunikačního provozu) je konkrétně uvedeno:

10Mezi tyto služby je možné zařadit i přenos dat například v rámci telefonování po internetu.

11V současnosti jde nejběžněji o velmi rozšířený přenos pomocí wi-fi, bluetooth, aj.

(4) Ustanovenia odsekov 1 až 3 sa primerane vzťahujú na obsahové údaje alebo prevádzkové údaje ***prenášané prostredníctvom počítačového systému****.*

Zákon tedy otevřeně deklaruje, že je možné užít tento zajišťovací úkon k zajištění informací přenášených prostřednictvím informačních a komunikačních sítí.

PRÁVNÍ ÚPRAVA KYBERNETICKÉ TRESTNÉ ČINNOSTI V ČR – DE LEGE FERENDA

V úvodu článku jsem si za jeden z cílů vytýčil popsat a analyzovat připravovanou trestněprávní úpravu týkající se ochrany před kybernetickou trestnou činností, včetně posouzení, do jaké míry bude tuzemská trestněprávní úprava odpovídat závazkům, které pro Českou republiku vyplývají z ratifikovaných a vyhlášených mezinárodních smluv v této oblasti. Na základě provedené analýzy pak na tento cíl bezprostředně navazuje snaha o **posouzení vhodnosti nově navrhované trestněprávní úpravy** v boji s touto trestnou činností.

g)Rekodifikace trestního práva

V současnosti je rekodifikace českého trestního práva ve dvou fázích. Návrh trestního zákoníku vypracovaný ministerstvem spravedlnosti je v současné době předložen Poslanecké sněmovně Parlamentu ČR a byly do něj promítnuty i některé připomínky ze strany veřejnosti.[12] Trestní řád existuje pouze ve formě věcného záměru a jako takový byl předložen odborné veřejnosti.[13] Je předpokládáno, že trestní zákoník by teoreticky mohl vstoupit v účinnost v letech 2009-2010 a trestní řád v roce 2011.

12Blíže World Wide Web: <http://portal.justice.cz/ms/ms.aspx?j=33&o=23&k=381&d=160504> [cit. 27.3.2008].

13Blíže World Wide Web: <http://portal.justice.cz/ms/ms.aspx?j=33&o=23&k=381&d=168724> [cit. 27.3.2008].

Trestný čin, stejně jako tomu je na Slovensku, má být pojat čistě formálně (na rozdíl od současného formálně materiálního pojetí).

h)Porušování práva autorského

V rámci ochrany práva autorského a práv souvisejících s právem autorským a práv k databázi nedošlo v nově připravovaném trestním zákoníku k výraznějším změnám. Ochrana těchto práv je upravena ustanovením § 268 **(Hl. VI - trestné činy hospodářské, díl 4 - Trestné činy proti průmyslovým právům a proti autorskému právu). Bohužel *nedošlo k zdůraznění ochrany před touto trestnou činností páchanou prostřednictvím informačních a komunikačních technologií*, tak jak tomu je například ve slovenském trestním zákoně v § 283 odst. 2 písm. d).**

Domnívám se, že by bylo vhodné doplnit příslušné ustanovení připravovaného trestního zákona o *kvalifikační okolnost*, kdy je čin spáchán prostřednictvím informačních a komunikačních technologií**, neboť právě jejich prostřednictvím dochází v současnosti k nejzávažnějším a nejmasivnějším zásahům do práva autorského.**

Jako přínosné lze hodnotit vložení nových okolností podmiňujících použití vyšší trestní sazby do kvalifikovaných skutkových podstat. Zákonodárce tak reagoval na opatření přijatá směrnicí Evropského parlamentu a Rady, týkající se trestních opatření k prosazování práv duševního vlastnictví (2005/0127/COD).

i)Trestné činy související se zásahem do počítače a jeho systému

V rámci připravovaného trestního zákoníku došlo nově k širší úpravě trestných činů, které souvisí se zásahem do počítače a jeho systému, v rámci hl. V. – trestné činy proti majetku. Skutkové podstaty trestných činů neoprávněného přístupu k počítačovému systému a nosiči informací (§ 228) a opatření a přechovávání

přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 229) byly do návrhu zákona vloženy na základě Úmluvy kyberkriminalitě, která stanoví kriminalizaci nezákonného získání přístupu k počítačovému systému, nezákonného odposlechu počítačového systému technickými prostředky, neoprávněného poškození, vymazání, snížení kvality, pozměnění nebo potlačení počítačových dat, která jako širší pojem zahrnují i počítačové informace, omezování funkčnosti počítačového systému pomocí manipulace s počítačovými daty, počítačového padělání, dále výrobu, prodej, opatření za účelem použití, držení, dovoz, distribuci a zpřístupňování zařízení, která jsou vytvořena nebo uzpůsobena k páchání trestných činů uvedených pod články 2 až 6 Úmluvy o kyberkriminalitě. V souvislosti s tím návrh trestního zákona na základě požadavků z praxe upravuje i trestný čin poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti podle § 230.[14]

Ochrana před hackingem a úmyslným poškozováním dat na nosiči informací

(1)*Kdo* ***překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části****, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.*

(2) Ustanovení § 228 odst. 1, týkající se neoprávněného přístupu k počítačovému systému a nosiči informací[15], nově **zavádí** až doposud neřešenou **ochranu před pouhým vniknutím do počítačového systému nebo jeho části**.

14Blíže důvodová zpráva k připravovanému trestnímu zákonu, dostupná na World Wide Web: <http://portal.justice.cz/ms/ms.aspx?j=33&o=23&k=381&d=160504> [cit. 27.3.2008].

15**Neoprávněný přístup k počítačovému systému a nosiči informací.**

(3) Dochází tedy k zavedení ochrany před crackerskými a zejména hackerskými aktivitami, neboť cílem hackerů je ve většině případů pouhé překonání ochrany systému a prokázání svých schopností. V současnosti je pachatele průniku možné postihnout pouze v případě, že nějakým způsobem zasáhne do dat a informací (viz ustanovení § 257a tr. zákona). Zákonodárce tak do trestního zákoníku implementuje čl. 2 Úmluvy o kyberkriminalitě neboť stanoví, že **trestné je překonání opatření, a tím získání přístupu k počítačovému systému nebo jeho části.**

(4)*Kdo **získá přístup k počítačovému systému nebo k nosiči informací** a*

a)***neoprávněně užije data** uložená v počítačovém systému nebo na nosiči informací,*

b)***data** uložená v počítačovém systému nebo na nosiči informací **neoprávněně vymaže** nebo jinak **zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými**,*

c)***padělá nebo pozmění data** uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo*

d)***neoprávněně vloží data** do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat,*

bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

Jednání uvedená v odstavci 2 postihují ostatní nové formy trestné činnosti páchané prostřednictvím informačních a komunikačních technologií, které reagují na podpis úmluvy o kyberkriminalitě. Jedná se o implementaci **článků 2, 4, 5** uvedené úmluvy, které řeší **nezákonný přístup** (nedovolené získání přístupu k systému), **narušování dat** (poškozování dat), **narušování systémů** (narušování běhu informačních systémů včetně jejich poškozování, či ničení), **zneužití prostředků**

(míněno je zde užití technických prostředků – informačních a komunikačních technologií, včetně programů určených, ke spáchání výše uvedených činů a jejich držení). Český zákonodárce vložil do připravovaného zákona i ochranu před jednáním, které spočívá v **neoprávněném vkládání dat do systému** (jde o ochranu počítačových systémů před útoky virů, logických bomb, aj.)

Z kvalifikované skutkové podstaty je vhodné zmínit tři okolnosti podmiňující použití vyšší trestní sazby [jedná se o jiné skutečnosti dle ustanovení § 6 písm. b) tr. zákona]:

(5)*„v **úmyslu neoprávněně omezit funkčnost počítačového systému** nebo jiného technického zařízení pro zpracování dat“.*[odst. 3 písm. b)]

(6)*„**způsobí-li** takovým činem vážnou poruchu **v činnosti orgánu státní správy, územní samosprávy, soudu nebo jiného orgánu veřejné moci**,* [odst. 4 písm. c)]

(7)*způsobí-li takovým **činem vážnou poruchu v činnosti právnické nebo fyzické osoby, která je podnikatelem**.“* [odst. 4 písm. e)]

<u>Ochrana před sniffingem a crackingem</u>

Český zákonodárce dle mého názoru formuloval precizněji ochranu před nelegálním sledováním přenosu dat (viz sniffing). Oproti slovenské právní úpravě je také lépe formulována podstata držení programu či zařízení (crackeru, keygenu, aj.) schopného prolamovat hesla. Takovéto zařízení je velmi precizně charakterizováno v ustanovení § 229 trestního zákoníku jako:

a)***zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému** nebo k jeho části, nebo*

b)***počítačové heslo, přístupový kód, data, postup*** *nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup do počítačového systému nebo jeho části,*

Vyrobení, uvedení do oběhu, dovezení, vyvezení, provezení, nabízení, zprostředkování, prodej nebo **jiné zpřístupnění, opatření nebo přechovávání** takového prostředku, by bylo trestné pouze v tom případě, kdyby došlo k uvedenému jednání **s úmyslem spáchat trestný čin** dle ustanovení § 180 odst. 1 písm. b), c) – ***porušení tajemství dopravovaných zpráv*** a § 228 odst. 1, 2 – ***neoprávněného přístupu k počítačovému systému a nosiči informací*** trestního zákoníku. Ustanovení § 229 dochází k naplnění **článků 3 a 6** Úmluvy o kyberkriminalitě, který chrání právě před výše uvedeným jednáním.

Pozitivně lze vnímat, že se zákonodárce nesnaží trestat pouhé držení takového prostředku bez úmyslu užít ho ke spáchání trestného činu, na rozdíl od slovenské právní úpravy. Domnívám se, že trestání pouhého držení takovéhoto prostředku bez úmyslu jeho užití k trestnému činu by vedlo ke zbytečné kriminalizaci.

(8) Vlastní ochrana přepravovaných elektronických zpráv má být poskytnuta navrhovaným ustanovením § 180 odst. 1 písm. b), c) trestního zákoníku, podle kterého by bylo možno postihnout porušení ***datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli, který zprávu přijímá, nebo neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková počítačová data.***

(9)Tímto ustanovením zároveň dochází k naplnění dalšího požadavku Úmluvy o kyberkriminalitě vztahujícího se k postižení **nezákonného odposlouchávání** (míněno je i nedovolené narušování elektronické komunikace).

(10)Ochrana před nedbalostním poškozováním dat

(11) Jako přínos lze bezesporu hodnotit i vložení ustanovení, které řeší **poškození záznamu v počítačovém systému** a na nosiči informací a zásahu do vybavení počítače **z nedbalosti**. Trestní zákoník stanoví, že potrestán bude ten, kdo **z hrubé nedbalosti porušením povinnosti** vyplývající ze zaměstnání, povolání, postavení nebo funkce nebo uložené mu podle zákona, případně smluvně **zničí, poškodí, pozmění nebo učiní neupotřebitelnými data uložená v počítači nebo na nosiči informací**, nebo provede **zásah do technického či programového vybavení počítače a způsobí tak** na cizím majetku **značnou škodu.**

(12) Hrubou nedbalost je třeba vykládat dle ustanovení § 16 odst. 2 trestního zákoníku. Lze ji chápat jako vyšší stupeň intenzity nedbalosti, ať již vědomé či nevědomé, zejména na základě přístupu (postoje) pachatele k požadavku náležité opatrnosti, který svědčí o zjevné bezohlednosti pachatele k zájmům chráněným trestním zákoníkem.

(13) Pokud se jedná o další trestnou činnost, která by měla být postihována dle Úmluvy o kyberkriminalitě, nereaguje připravovaný zákon pouze na zločiny se vztahem k počítači, tj. **počítačové padělání** (padělání za použití počítače) a **počítačový podvod. Domnívám se, že tímto** nerespektováním Úmluvy o kyberkriminalitě a nezařazením počítačového padělání a počítačového podvodu do připravovaného trestního zákona, **nechává zákonodárce volné pole působnosti kybernetickým útočníkům, kteří se zabývají především phishingem a pharmingem**.

(14) Argumentace, že jejich jednání může být postihnuto dle přípravy (§ 20) k podvodu (§ 207), či za podvod samotný (při odčerpání hotovosti) je částečně chybná. Pokud dojde k finančnímu

obohacení pachatele je bezesporu možné ustanovení o trestném činu podvodu použít. Pokud bychom však řešili trestnost přípravy k tomuto trestnému činu, nebude činnost phishera trestná, neboť příprava bude trestná pouze za zvlášť závažný zločin, kterým podvod není. Pokud tedy phisher bude pouze získávat „citlivá data“ a nijak jich nevyužije, nebude trestný. Phisherovu činnost nebude možné postihnout ani podle ustanovení § 228 a 229, neboť získané informace budou zadávány samotnými uživateli na jeho vlastních internetových stránkách.

(15)Jako vhodné se jeví doplnit do zákona ustanovení, které by poskytovalo ochranu před zde uvedeným jednáním. Navrhované znění by mohlo například znít:

(16)*„Kdo neoprávněně za pomoci počítačového systému získá informace, jichž může být využito ke spáchání počítačového podvodu, bude potrestán…“*

(17) Otázka trestných činů souvisejících s obsahem počítače (zejména se jedná o držení, šíření a výrobu dětské pornografie) je již de lege lata dostatečně vyřešena v ustanoveních § 205 – 205b tr. zákona a jako taková jsou de facto přejata do připravovaného zákona.

De lege ferenda by bylo vhodné upravit celou problematiku počítačové trestné činnosti v samostatném oddíle zvláštní části trestního zákona, kde by byla specifikována i softwarová kriminalita, aby nedocházelo k nejednotnosti a roztříštěnosti legislativní úpravy a terminologie. Samostatná **pozornost by pak měla být věnována právě otázce tzv. softwarového pirátství**. To je v návrhu zákona, stejně jako v současnosti podřazeno pod ustanovení týkající se ochrany autorských práv. [16]

16Blíže KOLOUCH, J., SOUČEK, J. Několik poznámek k specifikům dokazování softwarové kriminality. In *Trestní právo,* 2007, roč. 12, č. 12, s. 12

Případné ustanovení řešící ochranu před softwarovým pirátstvím by mimo jiné mělo demonstrativně vyjmenovat ta jednání, která jsou natolik společensky nebezpečná, že je nutno jim zamezit pod hrozbou trestní sankce. Takovéto ustanovení by pak bylo vhodné strukturovat tak, aby rozlišovalo mezi méně závažnou činností (např. zálohování softwaru domácím uživatelem), a závažnějším trestním jednáním, které způsobuje buď ekonomickou škodu, nebo je páchané pravidelně za účelem dosažení zisku.

Domnívám se také, že by měla být věnována větší pozornost i otázce odborné přípravy a specializace orgánů činných v trestním řízení (tak jak tomu například je v ustanovení § 3 odst. 8 zák. č. 218/2003 Sb., zákon o soudnictví ve věcech mládeže), **neboť softwarová a internetová trestná činnost je progresivní a dynamicky se vyvíjející trestná činnost, k jejímuž zvládnutí je třeba odborníků.**