2007 ACTA UNIVERSITATIS CAROLINAE – IURIDICA 2 PAG. 167–172

POČÍTAČOVÁ KRIMINALITA V OSNOVĚ TRESTNÍHO ZÁKONÍKU

TOMÁŠ MINÁRIK

student 5. ročníku Právnické fakulty UK v Praze

Ve svém příspěvku bych chtěl pojednat o souladu osnovy trestního zákoníku (dále jen „NTZ") s mezinárodními závazky ČR a s akty evropského práva, jako i o její obecné dostatečnosti, z hlediska počítačové kriminality.

Za nejvýznamnější dokumenty evropského a mezinárodního práva v oblasti počítačové kriminality považuji tyto dva:

- Úmluvu Rady Evropy o počítačové kriminalitě[1] (Convention on Cybercrime, ETS No. 185), Budapešť, 23. 11. 2001, kterou ČR podepsala 9. 2. 2005 a k jejíž ratifikaci zdá se směřuje (dále jen „Úmluva"), a
- Rámcové rozhodnutí Rady 2005/222/JHA ze dne 24. února 2005 o útocích proti informačním systémům, které přebírá některé skutkové podstaty z Úmluvy a které mělo být implementováno do 16. 3. 2007 (dále jen „Rámcové rozhodnutí").

Počítačové kriminality se částečně týká i Rámcové rozhodnutí Rady ze dne 28. května 2001 o potírání podvodů a padělání bezhotovostních platebních prostředků (2001/413/JHA).

Počítačovou kriminalitou označujeme trestnou činnost, při níž je počítač nebo [počítačová] síť nástrojem, předmětem útoku nebo (v přeneseném slova smyslu, považujeme-li kyberprostor za prostor) místem spáchání trestného činu. Termín se obvykle používá v širším smyslu a zahrnuje se do něj veškerá kriminalita v oblasti IT (informačních technologií).

Členíme ji podle kritéria, zda jsou IT podstatným znakem trestného činu nebo znakem nahodilým. Do první skupiny tak řadíme tzv. „nové" formy počítačové kriminality: neoprávněný přístup, zásah do dat, zásah do systému, některá k nim přípravná jednání a některé formy protiprávního „odposlouchávání". Do druhé skupiny pak spadají formy „tradiční", např. podvod, pomluva nebo šíření poplašné zprávy. Na pomezí obou skupin stojí dětská pornografie a porušování různých druhů práva duševního vlastnictví.

Členění je výhodné pro zákonodárce: zatímco u „tradičních" forem již patřičné skutkové podstaty existují a stačí je jen přizpůsobit společenskému vývoji, u „nových"

[1] http://conventions.coe.int.

forem je obvykle třeba vytvořit skutkové podstaty nové, s novými znaky. V příspěvku se soustředím na formy „nové", upravené především v § 204–206 Osnovy.[2]

K těmto ustanovením mám několik výhrad.

U § **204 odst. 1** by se dalo uvažovat o výslovném **doplnění** formy neoprávněného přístupu o **překročení oprávněného přístupu**, což je obsaženo v americkém kodexu, ale například i v § 300/C kodexu maďarského[3]. I současné znění je ale vyhovující a souladné s čl. 2 Úmluvy a čl. 2 Rámcového rozhodnutí.

§ **204 odst. 2** obsahuje dle mého názoru **nadbytečnou podmínku** „získá přístup k počítačovému systému nebo k nosiči informací". Judikatura a teorie sice vykládají podmínku „získá přístup" v tom smyslu, že se nemusí jednat o přístup neoprávněný ani bezprostřední, přesto však může být na překážku trestnosti některých činů; uvažme případ, kdy tvůrce malwaru (např. viru sloužícího k poškození dat) vypouští svůj výtvor do světa a umístí infikovaný soubor pomocí svého počítače na server. Pak svůj počítač vypne a už jen čeká, jak si důvěřiví návštěvníci serveru infikovaný soubor stahují a vir šíří. Pachatel sice „získal přístup", ale ne k těm počítačům, na kterých data poškodil, jak je třeba dle mého názoru systematicky vykládat § 204 odst. 2 písm. b).

Tato podmínka se nevyskytuje ani v Úmluvě, ani v Rámcovém rozhodnutí, ani v právních úpravách[4] Rakouska (§ 126a odst. 1 rakouského StGB), Německa (§ 303a odst. 1 německého StGB), Maďarska (§ 300/C odst. 2 maďarského trestního zákoníku), Estonska (§ 206 estonského trestního zákoníku) ani v Modelovém zákoně o počítačové kriminalitě pro země Commonwealthu (Článek 6)[5]. Podle mého názoru se jedná o neblahý pozůstatek dosavadní právní úpravy v § 257a odst. 1 TZ a doporučoval bych ji zcela vypustit, protože podle mých závěrů **porušuje podmínky** Úmluvy (čl. 4–5) a Rámcového rozhodnutí (čl. 3–4).

§ **204 odst. 2 písm. a)** se podle mého názoru dubluje s § 158 odst. 1, co se týče ochrany soukromých tajemství a informací, a s § 248 odst. 1, co se týče ochrany autorských práv. Jde o převzetí dosavadní úpravy v § 257a odst. 1 písm. a) TZ, z čehož asi pramení i užití podmínky „získá přístup" v návětí. Ve srovnání se zahraničními úpravami a Úmluvou se jedná o **zcela ojedinělou** skutkovou podstatu. Rozsah a neurčitost pojmu „neoprávněně užije" je znepokojivý.[6] Zvážil bych, zda písm. a) **vypustit**, čímž by z názvu § 204 mohlo být vypuštěno „zneužití".

Vůbec celý název § 204 je zavádějící. Kromě zásahu do dat v odst. 2 písm. b) (čl. 4 Úmluvy) přece obsahuje i úpravu zásahu do systému v odst. 2 písm. d) (čl. 5 Úmluvy), což nelze nazvat souhrnně „poškození záznamu". Lze mít výhrady i k umísťování několika nesourodých skutkových podstat do jediného paragrafu, ba i jediného odstavce, a k „pyramidové" struktuře § 204: kvalifikované skutkové podstaty (odst. 3–5)

---

[2] Číslování paragrafů a jejich znění uvádím podle *Šámal, P.*: Osnova trestního zákoníku 2004–2006. Vydání první. Praha: C. H. Beck, 2006.

[3] http://www.cybercrimelaw.net/laws/countries/hungary.html, 27. 4. 2007.

[4] http://www.cybercrimelaw.net/laws/survey.html, 27. 4. 2007.

[5] http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf, 27.4.2007.

[6] Výklad pojmu „zneužití informací" v § 257a odst. 1 TZ viz in: *Šámal, P., Púry, F., Rizman, S.*: Trestní zákon. Komentář. II. díl. 6., doplněné a přepracované vydání, Praha: C. H. Beck, 2004, strana 1587.

se vztahují rovnocenně na odst. 1 i odst. 2, přestože závažnost činů podle odstavců 1–2 je jasně rozlišena i základní trestní sazbou.

První varianta § 205 odst. 1 NTZ vyvolala při projednávání ve Sněmovně nevoli ze strany odborníků v oboru IT, kteří se obávali kriminalizace výzkumu v oblasti počítačové bezpečnosti.[7] Slůvko „neoprávněně" je podle jejich názoru dostatečně nechránilo před trestní represí. Přitom NTZ výslovně upravuje novou okolnost vylučující protiprávnost, a to **přípustné riziko**, v § 31 odst. 1. Výkon společensky prospěšné činnosti, a tou bezpochyby tento výzkum je, v souladu s dosaženým stavem poznání vylučuje protiprávnost.

Tato varianta je přesto zbytečně přísná; podívejme se na čl. 6 Úmluvy. Ten vyžaduje kromě **objektivního primárního** určení zařízení[8] k páchání činů podle čl. 2 – čl. 5 také **úmysl** spáchat nebo umožnit spáchání uvedených činů (dále jen „druhý úmysl"). Není nic jednoduššího, než co nejpřesněji převzít článek 6 a vytvořit tak tento § 205 odst. 1 (odlišnosti od první varianty jsou vyznačeny tučně):

(1) Kdo neoprávněně vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává

a) zařízení nebo jeho součást, ~~**postup**~~, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, **primárně vytvořený nebo přizpůsobený k [alternativa: „jehož prvotním účelem je"]** spáchání trestného činu neoprávněného přístupu k počítačovému systému a poškození a zneužití záznamu v počítačovém systému a na nosiči informací podle § 204 nebo trestného činu porušování tajemství dopravovaných zpráv podle § 157 odst. 1 písm. b), c),

b) počítačové heslo, přístupový kód, ~~**postup**~~ nebo podobná data, pomocí nichž lze získat přístup k počítačovému systému nebo jeho části, **v úmyslu [lépe „s cílem" nebo „v přímém úmyslu"], aby jich bylo užito ke spáchání trestného činu neoprávněného přístupu k počítačovému systému a poškození a zneužití záznamu v počítačovém systému a na nosiči informací podle § 204 nebo trestného činu porušování tajemství dopravovaných zpráv podle § 157 odst. 1 písm. b), c),** bude potrestán odnětím svobody až na jeden rok, propadnutím věci nebo zákazem činnosti.

Doplněním skutkové podstaty o slovo „primárně" (nebo vhodný český ekvivalent) a podmínku druhého úmyslu by byla jasněji vyloučena trestnost jednání v souladu s právem. Druhý úmysl by navíc měl mít omezenější formu **úmyslu přímého**, jak žádá Vysvětlující zpráva k Úmluvě.[9]

Do písmen a) i b) bylo propašováno slovíčko **„postup"**, které v čl. 6 Úmluvy vůbec nefiguruje a které staví obsah zejména písmene b) na hlavu. Jde o značně abstraktní pojem. Možná jím chtěl tvůrce ustanovení řešit situace známé jako Zero-Day Attack.[10] Ty obvykle začínají tak, že někdo objeví slabinu (vulnerability) programu nebo systému. Následně slabinu uveřejní, přičemž obrana (tzv. záplata) ještě neexistuje. Toho

[7] *Šámal, P.*: Osnova trestního zákoníku 2004–2006. Vydání první. Praha: C. H. Beck, 2006, strana 223.
[8] Vysvětlující zpráva k Úmluvě, odstavec 73., z http://conventions.coe.int/Treaty/en/Reports/Html/185.htm, 10. 5. 2007.
[9] Vysvětlující zpráva k Úmluvě, odstavec 76., z http://conventions.coe.int/Treaty/en/Reports/Html/185.htm, 10. 5. 2007.
[10] http://en.wikipedia.org/wiki/Zero-Day_Attack, 12. 5. 2007.

využijí script kiddies, ale i jiní hackeři/crackeři, kteří začnou slabinu masově využívat k různým nekalým účelům.

Přesto si myslím, že slovo „postup" je zbytečně široké. Netrestáme přece samotné uveřejňování postupů k výrobě lidské bomby ani postupů k ilegální výrobě drog a nejsem si jist, zda je zvolené řešení optimální. Řešení by mohlo spočívat v lepší specifikaci onoho nežádoucího „postupu".

Inspirací pro náš § 205 NTZ by mohl být i navrhovaný **§ 202c německého StGB**:

§ 202c

Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passworte oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) § 149 Abs. 2 und 3 gilt entsprechend.

Je třeba vzít v potaz, že tento paragraf odkazuje pouze na sniffing, tj. na méně forem kriminality než § 205 NTZ. Na tento paragraf se ale chytře váží i doplněné §§ 303a (odst. 3) a 303b (odst. 5) StGB, takže ve výsledku je jeho působnost kompletní. Podmínka druhého úmyslu je formulována jako „**Kdo připravuje** trestný čin podle § 202a nebo § 202b...". Podmínka objektivního primárního určení podle čl. 6 Úmluvy je podle mě velmi elegantně formulována slovy „počítačové programy, **jejichž účelem** je spáchání takového činu".

Přijetí **druhé varianty** § 205 odst. 1 bych považoval za mírně řečeno nevhodné. Tato varianta je důkazem toho, jak lze drobným pozměňovacím návrhem zpřetrhat jemné předivo uceleného kodexu, v němž existují skryté vazby mezi ustanoveními. Prostředky uvedené v písmenech a) a b) by se omezily na prostředky umožňující neoprávněný přístup; tak by zůstal beztrestným vývoj prostředků umožňujících počítačový podvod ve smyslu čl. 3 Rámcového rozhodnutí Rady 2001/413/JHA a § 204 odst. 2 písm. c) NTZ, což podle mě vyvolává **rozpor s čl. 4 in fine** Rámcového rozhodnutí Rady 2001/413/JHA; beztrestný by byl vývoj prostředků umožňujících protiprávní odposlechy, zásah do dat a do systému [čl. 3 – čl. 5 Úmluvy, § 157 odst. 1 písm. b) a c), § 204 odst. 2 písm. a), b), d) NTZ], takže by byla beztrestná například výroba počítačových virů a soulad s Úmluvou by byl možný pouze s nejzazší povolenou výhradou.

Nedbalostní forma protiprávního zásahu do dat nebo do systému v **§ 206 NTZ** není v rozporu se závazky ČR; žádný z nich ČR ani k trestání takových jednání nezavazuje. Omezení trestnosti na případy „z nedbalosti porušením povinnosti..." a způsobivší značnou škodu je podle mého názoru vyhovující a nemělo by způsobovat přehnanou kriminalizaci.

Úpravu porušování tajemství dopravovaných zpráv a dokumentů uchovávaných v soukromí (**§§ 157–158 NTZ**) s ohledem na počítačovou kriminalitu považuji za velmi dobrou a **souladnou** s Úmluvou. Její článek 3 se podle mého názoru celý vešel do § 157 odst. 1 písm. c) NTZ, čímž nechci zpochybňovat užitečnost písm. b) tohoto ustanovení.

Na závěr si dovolím drobnou odbočku do práva evropského.

Rámcová rozhodnutí jsou akty sekundárního unijního práva. Jsou přijímána na základě čl. 34 písm. c) Smlouvy o Evropské Unii (dále jen „SEU") jednomyslně Radou EU, takže spadají do třetího pilíře EU. Stejně jako směrnice jsou závazná co do výsledku, jehož má být dosaženo, ale na rozdíl od směrnic jim nelze přiznat přímý účinek.[11] Jsou (nebo až do vynesení rozsudku v případě C-176/03 byla) základním nástrojem harmonizace skutkových podstat některých trestných činů.

Evropský soudní dvůr 13. září 2005 na základě žaloby Komise podle čl. 35 SEU zrušil rozsudkem v případě C-176/03 Rámcové rozhodnutí Rady 2003/80/JHA ze dne 27. ledna 2003 o trestněprávní ochraně životního prostředí. Hlavní výhrada směřovala proti právnímu základu napadeného rozhodnutí. Podle Komise (a ESD) nespočíval ve třetím, nýbrž v prvním pilíři, takže harmonizace mělo být dosaženo aktem komunitárním (např. směrnice), nikoli unijním (např. rámcové rozhodnutí). Společenství nemá sice obecnou pravomoc v oblasti trestního práva, ale může na základě Smlouvy o založení ES (dále jen „SES"), např. čl. 175, uložit členským státům povinnost stanovit trestní sankce nezbytné pro zajištění účinnosti předpisů Společenství.[12]

V návaznosti na to vydala 24. 11. 2005 Komise sdělení COM (2005) 583, v němž uvedla, že důsledky rozsudku v případě C-176/03 se vztahují i na několik již vydaných aktů; mezi ty podle ní patří i dvě Rámcová rozhodnutí Rady 2005/222/JHA ze dne 24. února 2005 o útocích proti informačním systémům, 2001/413/JHA ze dne 28. května 2001 o potírání podvodů a padělání bezhotovostních platebních prostředků a připravovaná směrnice IPRED-2. Komise připravované předpisy přepracovala (IPRED-2) a ty již schválené navrhla buď bez přepracování přijmout na novém právním základě, nebo je předtím znovu vyjednat.[13] Navrhuje dále přenést pravomoci k vydávání trestních předpisů pomocí čl. 42 v kombinaci s čl. 29 SEU (tzv. passerelle) na Společenství.

K tomu se ale staví skepticky jak Rada, tak většina členských států EU. Logicky by to znamenalo jejich oslabení v oblasti trestního zákonodárství (u směrnic nemají členské státy právo veta). Renegociace nebo dokonce zrušení již přijatých aktů se také nezdá jako schůdné řešení a zdá se, že i Komise raději vyčká vydání rozsudku ESD v případě C-440/05.[14]

---

[11] *Tomášek, M.*: Jsou rámcová rozhodnutí klíčovým nástrojem europeizace trestního práva? In: Trestněprávní revue, 3/2006, strana 84.

[12] *Pítrová, L.*: Komunitarizace bez Ústavy?, z http://www.psp.cz/kps/pi/PRACE/pi-5-264.pdf, 7. 5. 2007, strana 3.

[13] *Pítrová, L.*: Komunitarizace bez Ústavy?, z http://www.psp.cz/kps/pi/PRACE/pi-5-264.pdf, 7. 5. 2007, strana 5.

[14] Letter from Mr Gerry Sutcliffe MP, Parliamentary Under Secretary of State, Home Office, to Lord Grenfell, Chairman of the European Union Committee, http://www.publications.parliament.uk/pa/ld200506/ldselect/ldeucom/227/6062802.htm, 10. 5. 2007, otázka 2.

Samotný rozsudek v případě C-176/03, vydaný jen několik měsíců po neúspěšných referendech o Smlouvě o ústavě pro Evropu, je odborníky vesměs považován za „aktivistický" a jeho výklad ve sdělení Komise COM (2005) 583 „extenzivní".[15]

Zmíněná rámcová rozhodnutí tedy zůstávají v platnosti. **Lhůta k implementaci** Rámcového rozhodnutí Rady 2005/222/JHA vypršela 16. 3. 2007 a uvidíme, jak se projeví dosavadní beztrestnost protiprávního přístupu k informačním systémům v ČR v hodnotící zprávě Komise, potažmo v hodnocení Rady (viz čl. 12 Rámcového rozhodnutí).

COMPUTER CRIME IN THE DRAFT OF THE PENAL CODE

Summary

This article deals chiefly with §§ 204–206 of the proposed (2007) Czech Penal Code, which are meant to implement Articles 2–6 of Convention on Cybercrime (Budapest 2001) and Articles 2–4 of Council Framework Decision (2005/222/JHA) on attacks against information systems, into Czech substantive criminal law. The article is critical of the Proposition due to its inconsistency with both of these documents.

Key words: computer, cybercrime, proposed penal code, unauthorised access, data interference, system interference, misuse of device, framework decision

Klíčová slova: počítač, počítačová kriminalita, osnova trestního zákoníku, neoprávněný přístup, zásah do dat, zásah do systému, zneužití zařízení, rámcové rozhodnutí

[15] *Pítrová, L.*: Komunitarizace bez Ústavy?, z http://www.psp.cz/kps/pi/PRACE/pi-5-264.pdf, 7. 5. 2007, strana 2.