ZÁVAZKY K OCHRANĚ KYBERPROSTORU VYPLÝVAJÍCÍ Z EVROPSKÉHO A MEZINÁRODNÍHO PRÁVA

TOMÁŠ GŘIVNA
Katedra trestního práva Právnické fakulty Univerzity Karlovy v Praze

1. ÚVODEM

V zahraniční literatuře se často používá ve spojení s internetem termín „cyberspace". Patrně nejpopulárnější encyklopedie s otevřeným obsahem – Wikipedia k tomuto termínu uvádí zevrubné pojednání.[1] Do českého jazyka se termín „cyberspace" buď nepředkládá nebo je překládán jako „kybernetický prostor" či zkráceně „kyberprostor".[2] Aniž bych měl v úmyslu uvádět desítky definic pojmu kyberprostoru, bude přeci jen nezbytné určitou charakteristiku podat, alespoň pro účely příspěvku.[3]

Kybernetický prostor nemá hmotnou podstatu, je imaginární. Jeho vznik a další existence je však závislá na světě reálném. Vznik kyberprostoru byl esenciálně spjat s určitou úrovní technologické vyspělosti společnosti, s rozvojem informačních a telekomunikačních technologií. Připojením na komunikační a informační služby vytváří jednotliví uživatelé určitý druh společného prostoru, který lze nazvat „kyberprostorem". V současnosti je kybeprostor převážně spojován či dokonce ztotožňován s internetem, jehož mohutný rozvoj nastává v 90. letech minulého století. Překročení jedné miliardy uživatelů internetu v roce 2006 jsou dokladem toho, že se kyberprostor „rozpíná". Internet nejen usnadňuje každodenní život, ale v jistém smyslu umožňuje uniknout z reálného světa do toho virtuálního.

Kyberprostor se vyznačuje řadou specifik. Především, pro kyberprostor neexistují státní hranice. Zatímco je v právě uvedeném významu prostorově neomezený, národní právní normy platí v zásadě jen na území pod jurisdikcí příslušného státu. Vytvoře-

[1] Srov. http://en.wikipedia.org/wiki/Cyberspace (naposledy navštíveno 8. 6. 2008).

[2] Srov. českou verzi slovníku Wikipedia: http://cs.wikipedia.org/wiki/Kyberprostor (naposledy navštíveno 8. 6. 2008).

[3] Pojem „kyberprostor" byl poprvé použit v kyberpunkové povídce „Burning Chrome" Williama Gibsona v roce 1982, o něco později ji popsal ve své knize „Neuromancer". Do obecného vědeckého povědomí, jako popisný termín pro realitu počítačových a telekomunikačních sítí, se dostal později od Johna Barlowa, zakladatele Electronic Frontier Foundation. Blíže k pojmu „cyberspace" srov. Jirovský, V. Kybernetická kriminalita. Praha: Grada Publishing, a. s., 2007, s. 15 an.; Yar, M. Cybercrime and Society. Sage Publications, London, 2006, s. 11, 155; Sieber, U. International Cooperation Against Terrorist Use of the Internet. In Cybercrime. The International Review of Penal Law. No. 77, 2006, s. 396; Schell, B. H., Martin, C. Cybercrime: A Reference Handbook. ABC-Clio, USA, 2004, s. 225; Chatterjee, B. B. Last of the rainmacs. In Wall D. (ed.). Crime and the Internet. Oxon, 2001 s. 81 an.; Williams, M. Virtually Criminal. Crime, deviance and regulation online. Oxon, 2006, s. 48.

ním kybernetického prostoru vznikl jako nechtěný produkt určitý prostor pro společensky nebezpečné aktivity nového typu, nazvěme je kybernetickými útoky. Útoky v kyberprostoru jsou velmi efektivní. Umožňují z jednoho místa zasáhnout chráněné zájmy na mnoha jiných místech ve velmi krátkém čase, v podstatě se zanedbatelnými finančními náklady a s minimálním nebezpečím okamžitého odhalení. Z toho rozporu plyne nezanedbatelná výhoda pro útočníka.

Na útoky v kyberprostoru je třeba adekvátně reagovat. O to se snaží většina vyspělých států. Jejich úsilí je však více či méně omezeno státními hranicemi. Jediným efektivním způsobem, kterým lze konflikt omezené jurisdikce a neomezeného kyberprostoru alespoň částečně překonat, je koordinovaný postup více (či ideálně většiny) států, jehož cílem je některá jednání v kybernetickém prostoru reglementovat a ty nejnebezpečnější z nich eliminovat. Při rozmanitosti národních právních úprav a partikulárních zájmů jednotlivých států a z toho plynoucí odlišný názor na postih toho či onoho jednání v kyberprostoru vede k tomu, že sice v obecné rovině panuje jednoznačná shoda část z nich regulovat, část z nich dokonce i postihovat, na druhou stranu se jen obtížně vymezují konkrétní jednání, jež by harmonizovanou reglementaci zasluhovala. Příkladem napětí regulovat či neregulovat je postih rasistických textů a projevů na internetu. Zde se zcela zřetelně projevuje odlišný přístup některých států. Zatímco některé státy zejména ty, jejichž obyvatele na vlastní kůži pocítily hrůznost nacismu, se hlásí k postihu takových projevů, jiné státy jsou z obavy před omezením svobody projevu k razantnějšímu postihu rezervovanější (např. USA).[4] Jednoznačně se to potvrdilo při podpisu Dodatkového protokolu k Úmluvě o počítačové kriminalitě, týkající se postihu rasistické a xenofobní povahy prostřednictvím počítačového systému.[5] Jiným příkladem může být postih dětské pornografie. V obecné rovině jsou všechny státy proti šíření dětské pornografie na internetu.[6] Rozdílné názory jsou však v otázce, kdy se jedná ještě o dítě z hlediska věku, zdali má být trestné i držení dětské pornografie pro vlastní potřebu, zdali má být trestné i zobrazení osoby, která se jeví býti dítětem nebo dokonce pouhé realistické vyobrazení dítěte vytvořené počítačem. Tak jako v jiných oblastech, i v oblasti kybernetických hrozeb jsou závazné mezinárodní právní nástroje výsledkem konsensu, tedy představují pouze jakési minimum, na kterém se shodla většina států. Obdobně je tomu i pokud jde o právo ES/EU. Cílem příspěvku je proto podat určitý, byť jistě nikoliv vyčerpávající, přehled mezinárodních úmluv a norem práva ES/EU, jež zavazují členské státy k regulaci některých jednání v kybernetickém prostoru.

Jsem si vědom, že žádný kyberprostor nebyl právně vymezen, ani to není možné, přesto jej pro účely toho příspěvku používám jako určitou abstrakci, neboť podle mého názoru poměrně dobře zastřešuje různorodost problematiky, o níž je pojednáno. Nejedná se totiž jen o oblast trestního práva, tedy zejména otázku, jaké jednání v kyberprostru

---

[4] V podrobnostech srov. např. Herczeg, J. Dodatkový protokol k Úmluvě o počítačové kriminalitě týkající se kriminalizace činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů. In: Gřivna, T., Polčák, R. (eds). Kyberkriminalita a právo. Praha: Auditorium, 2008.

[5] Úmluva Rady Evropy č. 189 ze dne 28. 1. 2003, vstoupila v platnost 1. 3. 2006, dodatek podepsalo 33 států, ratifikovalo však jen 13 z nich. Mezi signatáři chybí USA, ale např. i Česká republika nebo Slovensko.

[6] Srov. např. Poremská, M. Trestní postih šíření dětské pornografie. In: Gřivna, T., Polčák, R. (eds). Kyberkriminalita a právo. Praha: Auditorium, 2008. nebo tamtéž Gřivna, T. K ustanovením Úmluvy o počítačové kriminalitě.

má být trestným činem, a problematiku mezinárodní justiční spolupráce ve věcech trestních, ale spadají sem i otázky, jež bychom spíše zařadily do práva obchodního a občanského nebo správního.

V současné době se projevuje na mezinárodní úrovni či úrovni práva ES/EU snaha harmonizovat regulaci zejména následujících aktivit v kyberprostoru:

1. zvláště společensky nebezpečných a závadových jednání jako jsou útoky proti počítačovým systémům a počítačovým datům (např. neoprávněný přístup k počítačovému sytému, neoprávněné zachycení informací, zásah do počítačového systému nebo dat, zneužití zařízení), šíření závadného obsahu (např. dětská pornografie, rasistické a xenofóbní projevy), porušování autorského práva,
2. některé druhy podnikání prostřednictvím elektronické komunikační sítě a některé aspekty služeb informační společnosti,
3. zpracování osobních údajů a ochrana soukromí.

2. ORGANIZACE SPOJENÝCH NÁRODŮ[7] (OSN)

Pokud jde o Organizaci spojených národů, pak lze v oblasti ochrany kyberprostoru připomenout:

1. Rezoluci o **boji se zneužíváním informačních technologií** z 22. 1. 2001 (A/RES/55/63), která vyzývá státy, aby zaručily, že se nestanou bezpečnými ráji pro pachatele, kteří zneužili informační technologie. Mezi výzvami nalezneme mimo jiné apel, aby právní systémy členských států chránily *důvěrnost, integritu a dostupnost počítačových dat a systémů před neoprávněným zneužitím a zaručily, že takové zneužití bude trestáno.*
2. Rezoluci 56/261, kterou se vyhlašuje **plán činnosti pro implementaci Vídeňské deklarace o zločinu a trestní spravedlnosti: Výzvy 21. století**. Rezoluce v části věnované boji proti technologicky vyspělé (high-technology) a s počítačem související (computer-related) kriminalitě (XI. část) vedle dalšího stanoví, že státy budou usilovat na národní úrovni, aby zneužití informačních technologií bylo kriminalizováno včetně revize stávajících trestných činů za účelem posouzení, zda jsou aplikovatelné i na jednání, ve kterých byly použity počítačový systém, telekomunikační média a sítě.

Rezoluce Hospodářské a sociální Rady OSN týkající se **mezinárodní spolupráce v oblasti prevence, vyšetřování, stíhání a trestání hospodářských podvodů a trestných činů souvisejících s identitou osob** přijatá 26. 7. 2007 podněcuje členské státy, aby novelizovaly právní předpisy, především s ohledem na trestné činy nedovoleného získání, kopírování, padělání a zneužití dokumentů, které identifikují osoby, a osobních údajů. Ještě dříve, v roce 1990 vydalo OSN **pravidla regulace počítačem zpracovaných souborů osobních údajů** (14. 12. 1990).

Na půdě OSN nevznikla doposud mezinárodní úmluva, která by se specificky dotýkala kybernetického prostoru. Jelikož je někdy kybernetický prostor využíván jen jako

[7] United Nations (UN)

jeden z prostředků přenosu informací, dopadají na něj i některé úmluvy, které nemají s kyberprostorem jinak nic společného, např. Úmluva o právech dítěte z 20. 11. 1989 v čl. 37 zavazuje členské státy, aby přijaly opatření, která zabrání mimo jiné i svádění dětí k jakékoliv nezákonné sexuální činnosti, k čemuž je bezesporu využíván i internet.

3. RADA EVROPY[8]

1. Zatímco iniciativa OSN je v oblasti ochrany kyberprostoru téměř zanedbatelná, Rada Evropy přijala velmi silný nástroj k ochraně kyberprostoru před nejzávažnějšími činy kriminální povahy. Jedinečným právně závazným nástrojem komplexní povahy je **Úmluva o kybernetické kriminalitě**[9] (dále jen „Úmluva"). Přijetí Úmluvy předcházelo doporučení Rady Evropy č. R (89) 9 z 13. 9. 1989, které se týká trestných činů souvisejících s počítači.

Úmluva byla přijata po čtyřleté práci expertů Rady Evropy, USA, Kanady, Japonska a dalších dne 8. listopadu 2001. Otevřena k podpisu byla v Budapešti dne 23. listopadu 2001. V platnost vstoupila dne 1. července 2004. Ke dni 9. listopadu 2008 Úmluvu podepsalo 45 států, z nichž jí však ratifikovalo jen 23 států, tedy zhruba pouhých 50 %. Z nečlenských států Rady Evropy Úmluvu podepsaly a zároveň ratifikovaly jen USA. Česká republika podepsala Úmluvu dne 9. 2. 2005. K její ratifikaci prozatím nedošlo, na rozdíl od našeho východního souseda, Slovenské republiky, která Úmluvu podepsala dne 4. 2. 2005, ratifikovala 8. 1. 2008 a pro níž vstoupila v platnost dnem 1. 5. 2008.

K Úmluvě byl přijat dodatkový protokol, který se týká kriminalizace činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačového systému[10]. Otevřen byl k podpisu 28. 1. 2003, vstoupil v platnost 1. 3. 2005, podepsalo jej 33 států, z toho ratifikovalo jen 13. Česká republika, stejně jako např. Slovensko nebo USA, není signatářem dodatkového protokolu.

Úmluva, čítající 48 článků, se vedle preambule člení do 4 kapitol. Kapitola I. (používání pojmů) definuje pojmy „počítačový systém", „počítačová data", „poskytovatel služeb", „provozní data". Kapitola II. (opatření přijímaná na národní úrovni) upravuje závazky států v oblasti trestního práva hmotného (oddíl 1) i procesního (oddíl 2) včetně ustanovení o působnosti vnitrostátních norem (oddíl 3). Závazky na poli mezinárodní spolupráce jsou náplní kapitoly III. Závěrečná ustanovení nalezneme v kapitole IV.

Úmluva obsahuje znaky 9 trestných činů, které dělí do 4 kategorií. **Úmluva stanoví znaky těchto trestných činů**:

1. Trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů
   a. Neoprávněný přístup (čl. 2)
   b. Neoprávněné zachycení informací (čl. 3)

---

[8] Cancel of Europe (CoE)

[9] Podrobnější výklad k Úmluvě viz Gřivna, T. K ustanovením Úmluvy o počítačové kriminalitě. In: Gřivna, T., Polčák, R. (eds) Kyberkriminalita a právo. Praha: Auditorium, 2008.

[10] V podrobnostech srov. Herczeg, J. Dodatkový protokol k Úmluvě o počítačové kriminalitě týkající se kriminalizace činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů. In: Gřivna, T., Polčák, R. (eds). Kyberkriminalita a právo. Praha: Auditorium, 2008.

c. **Zásah do dat (čl. 4)**
d. **Zásah do systému (čl. 5)**
e. **Zneužití zařízení (čl. 6)**

2. Trestné činy související s počítači
   a. **Falšování údajů související s počítači (čl. 7)**
   b. **Podvod související s počítači (čl. 8)**
3. Trestné činy související s obsahem
   a. **Trestné činy související s dětskou pornografií (čl. 9)**
4. Trestné činy související s porušením autorského práva a práv příbuzných autorskému právu
   a. **Trestné činy související s porušením autorského práva a práv příbuzných autorskému právu (čl. 10)**

Vytvoření nových či modifikace stávajících znaků trestných činů, které postihují nebezpečné jevy v kyberprostoru je pouze prvním krokem k jejich efektivnímu postihu. Nové způsoby zneužívání kybernetického prostoru vyžadují i vytvoření nových, popř. úpravu stávajících (tradičních) procesních institutů, které umožní odhalit pachatele a zajistit důkazy, jež mohou vést k jeho usvědčení. Je totiž nutné si uvědomit, že v prostředí, které vznikne propojením mnoha sítí, je nesnadné identifikovat pachatele, zjistit rozsah a následky trestného činu. K tomu přistupuje fakt, že elektronická data jsou charakteristická svojí nestálostí – mohou být v okamžiku změněna nebo i zničena. Z této charakteristiky vyplývá i potřeba, aby odhalení pachatele a zajištění důkazů probíhalo velmi rychle a v utajení. V souvislosti s potřebou zajistit elektronická data se při přípravě Úmluvy široce diskutovalo, zda by neměla být uložena poskytovatelům služeb povinnost po určitou dobu shromažďovat a uchovávat data. Nakonec žádné obdobné ustanovení v Úmluvě nenajdeme, neboť konsensu nebylo dosaženo.

Elektronická data se dají rozdělit do několika skupin. Podle toho, jaké informace obsahují, je lze rozdělit zpravidla na **data provozní**, **data obsahová** a **data o odběratelích**. Úmluva definuje provozní data (jakákoli počítačová data související s přenosem dat prostřednictvím počítačového systému, generovaná počítačovým systémem, který tvořil součást komunikačního řetězce, jež vyjadřují původ, cíl, trasu, dobu, objem, dobu trvání přenosu dat nebo druh použité služby). Nezajímá nás tedy obsah komunikace, ale jak komunikace probíhá. Obsahová data definována nejsou. Lze je jistě vymezit negativně, jako data, která nejsou provozního charakteru. To samo o sobě k jejich definici nestačí, neboť jiná než provozní data zahrnují též např. data o odběratelích. Z označení „obsahová data" plyne, že nás zajímá, co je sdělováno (význam a účel sdělení, zprávy či informace předávané komunikací), tedy obsah komunikace. Informace o odběrateli zahrnují různé druhy informací o využívání služby a o uživateli této služby, pokud se nejedná o data provozní nebo obsahová. Jejich prostřednictvím lze zjistit: typ využívané komunikační služby, technické prostředky používané pro tuto službu a dobu trvání služby; totožnost uživatele, jeho poštovní nebo geografickou adresu, telefonní a jiné přístupové číslo a informace o fakturaci a platbách; jakékoli jiné informace o místu instalace komunikačního zařízení (srov. čl. 18 odst. 3). Rozlišení dat provozních, obsahových a o odběratelích má význam pro určení míry zásahu do soukromí osob, čemuž by měly odpovídat záruky proti případnému zneužití.

Dalším dělením počítačových dat podle okamžiku jejich výskytu může být klasifikace na **data uložená**, **data v procesu komunikace**, a **data, jež mají být teprve komunikována**.

Úmluva zavazuje státy k přijetí opatření, jež umožní efektivní využití počítačových dat k odhalení a usvědčení pachatele. Za tím účelem stanoví následující **procesní opatření**:

1. bezodkladné uchování uložených počítačových dat (čl. 16),
2. bezodkladné uchování a částečné poskytnutí (zpřístupnění) provozních dat (čl. 17),
3. příkaz k vydání (čl. 18),
4. prohlídka a zajištění uložených počítačových dat (čl. 19),
5. shromažďování provozních dat v reálném čase (čl. 20),
6. zachycení dat o obsahu (čl. 21).

Kapitola třetí Úmluvy obsahuje obecná a konkrétní ustanovení mezinárodní spolupráce, která je koncipována jako **doplňková ke stávajícím nástrojům** (mezinárodním dohodám o mezinárodní spolupráci v trestních věcech, ujednáním dohodnutých na základě jednotných nebo recipročních právních předpisů a vnitrostátních zákonů). Není tedy ambicí Úmluvy nahrazovat nebo stanovit nově a odlišně zásady spolupráce podle stávajících nástrojů.[11] Několik odlišných režimů, které by koexistovaly vedle sebe by mohlo způsobit zmatek a přinést pochybnosti o tom, která ustanovení aplikovat, zda této Úmluvy nebo jiná. Pouze s ohledem na mechanismy obzvláště nezbytné pro rychlou a účinnou spolupráci v oblasti trestné činnosti související s počítači stanoví Úmluva určité požadavky, například podle článků 29–35 se od každé strany požaduje vytvoření právního základu k umožnění v nich specifikovaných forem spolupráce, jestliže tak již nečiní její současné úmluvy, ujednání nebo zákony týkající se vzájemné pomoci.

Závěrem k Úmluvě lze konstatovat, že jde o výrazný počin v harmonizaci skutkových podstat trestných činů i v procesních opatřeních. Nelze však pominout celou řadu ustanovení Úmluvy, která závazky z nich plynoucí do značné míry relativizuje. Děje se tak nejen možností učinit výhradu k aplikaci některých článků, ale též cestou připuštění tzv. dodatečných podmínek při kriminalizace některých činů. Právní řád České republiky není v současné době v souladu se závazky, které vyplývají z Úmluvy. Nový trestní zákoník, který byl předložen Parlamentu České republiky ke schválení může alespoň částečně tento deficit napravit, pokud jde o závazky ke kriminalizaci některých typů jednání. Přesto zůstává harmonizovat celou řadu zejména procesních ustanovení ještě před tím, než bude Česká republika připravena k ratifikaci Úmluvy.

2. Již dříve (dne 28. 1. 1981) byla otevřena k podpisu **Úmluva o ochraně jednotlivců s ohledem na automatizované zpracování osobních údajů**.[12] K Úmluvě byl přijat dodatkový protokol, který byl otevřen k podpisu 8. 11. 2001.[13] Úmluva zavazu-

[11] Např. podle Evropské úmluvy o vzájemné pomoci v trestních věcech (ETS č. 30) a Protokolu k ní (ETS č. 99) či podle dvoustranných smluv.

[12] Úmluvu podepsalo 44 států a 40 z nich ji i ratifikovalo (údaj k 9. 11. 2008). Pro ČR vstoupila v účinnost 1. 11. 2001.

[13] Dodatkový protokol podepsalo 35 států, ratifikovalo 21 (údaj k 9. 11. 2008). Pro ČR vstoupil v účinnost 1. 7. 2004.

je členské státy k přijetí stanovených principů ochrany osobních údajů (kvalita údajů, speciální kategorie údajů, zabezpečení dat, záruky pro subjekt údajů). Dodatkový protokol prohloubil ochranu osobních údajů zejména při jejich přeshraničním poskytování. Ačkoliv automatizované zpracování dat nemusí být prováděno počítačovým systémem nebo s využitím počítačových sítí jako je internet, je zřejmé, že v současné době tomu tak je.

3. Závazky k postihu některých forem závadného obsahu v kyberprostoru obsahuje i **Úmluva o prevenci terorismu** (16. 5. 2005)[14], která v čl. 5 stanoví členským státům povinnost kriminalizovat veřejné (tedy i prostřednictvím např. internetu) podněcování k teroristickému činu. **Úmluva o ochraně dětí před sexuálním vykořisťováním a zneužíváním** (dosud není v platnosti, ČR není signatářem úmluvy) ze dne 25. 10. 2007 zavazuje mimo jiné k postihu nejen výroby, nabízení, distribuce dětské pornografie, ale též její získání, držení či vědomého získání přístupu k dětské pornografii prostřednictvím informačních a telekomunikačních technologií (srov. čl. 20).

4. Postih neautorizovaného přístupu k chráněným službám má být zajištěn v členských státech Rady Evropy podle **Úmluvy o právní ochraně služeb založených na (nebo zahrnujících) podmíněném přístupu** (24. 1. 2001).[15]

4. ORGANIZACE PRO HOSPODÁŘSKOU SPOLUPRÁCI A ROZVOJ (OECD)[16] A OSTATNÍ ORGANIZACE

Již v roce 1986 přijala OECD doporučení zabývající se manipulací s počítačovými systémy, padělání pomocí počítače, zasahování do počítačového systému a počítačových dat, porušování autorského práva, neoprávněným přístupem k počítačovému nebo telekomunikačnímu systému. Otázce budoucnosti internetu bylo věnováno také poslední zasedání na úrovni ministrů (Soul, 17.–18. 6. 2008),[17] kde byla přijata i deklarace[18] a formulovány základní politiky této problematiky.[19] V současnosti se pozornost upíná k takovým nežádoucím jevům jako je spaming,[20] krádež identity[21] a šíření malwaru.[22] Žádná mezinárodní úmluva však přijata nebyla.

OECD není jedinou organizací, která věnuje pozornost nežádoucím jevům v kyberprostoru, i G8 na zasedání ministrů spravedlnosti a vnitra v roce 1997 (9.–10. 12. 1997) přijala akční plán a 10 principů boje s high-tech trestnou činností. O právně závazné dokumenty se ani v jednom případě nejedná.

---

[14] Úmluva vstoupila v platnost 1. 6. 2007, podepsalo ji 43 států, z nichž ji ratifikovalo 15. ČR není signatářem Úmluvy.

[15] Úmluva vstoupila v platnost 1. 7. 2003, Úmluvu podepsalo 11 států, z nichž ji ratifikovalo 8. ČR není signatářem Úmluvy.

[16] Organisation for Economic Co-operation and Development.

[17] Blíže viz http://www.oecd.org/site/0,3407,en_21571361_38415463_1_1_1_1_1,00.html.

[18] http://www.oecd.org/dataoecd/49/28/40839436.pdf.

[19] http://www.oecd.org/dataoecd/1/29/40821707.pdf.

[20] OECD má speciální webovou stránku věnovanou problematice spamu: http://www.oecd-antispam.org/.

[21] Viz zpráva připravená jako podklad pro schůzi na úrovni ministrů http://www.oecd.org/dataoecd/35/24/40644196.pdf.

[22] http://www.oecd.org/dataoecd/53/34/40724457.pdf.

5. PRÁVO EU/ES

Jestliže mezinárodní smlouvy zasahují poměrně úzkou výseč aktivit odehrávajících se v kyberprostoru, pak naopak snaha o značnou míru regulace je patrná v oblasti práva **ES/EU**.

Vedle bezpočtu právně nezávazných dokumentů lze z mnoha směrnic a rámcových rozhodnutí uvést především tyto:

1. Rámcové rozhodnutí Rady 2005/222/SV ze dne 24. 2. 2005 o útocích proti informačním systémům.
2. Rámcové rozhodnutí 2004/68/SVV ze dne 22. 12. 2003 o boji proti pohlavnímu vykořisťování dětí a dětské pornografii.
3. Rámcové rozhodnutí Rady 2002/475/JHA ze dne 13. 6. 2002 o boji proti terorismu (bez specifických ustanovení o kyberterorismu).
4. Rámcové rozhodnutí Rady 2000/375/JHA ze dne 29. 5. 2000 o boji proti dětské pornografii na internetu.
5. Směrnice 2006/24/EC ze dne 15. 3. 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES.
6. Směrnice 2002/58/EC ze dne 12. 7. 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací.
7. Směrnice 2000/31/EC ze dne 8. 6. 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu.
8. Směrnice EP a Rady 97/66/ES ze dne 15. 12. 1997 o zpracování osobních údajů a ochraně soukromí v telekomunikačním sektoru.
9. Směrnice EP a Rady 95/46/ES ze dne 24. 10. 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

1. **Rámcové rozhodnutí Rady 2005/222/SV ze dne 24. 2. 2005 o útocích proti informačním systémům** má za cíl sblížení trestněprávních předpisů v členských státech v oblasti útoků proti informačním systémům. Ukázalo se totiž, že významné mezery a rozdíly v právních předpisech členských států v této oblasti mohou ztěžovat boj proti organizované trestné činnosti, komplikovat účinnou policejní a soudní spolupráci v oblasti útoků proti informačním systémům (útoky proti takovým systémům jsou často přeshraničního rázu). Rámcové rozhodnutí výzývá k legislativním krokům proti trestné činnosti v oblasti špičkové techniky, včetně společných definic, které jsou důležité v zájmu zajištění jednotného přístupu v členských státech při používání rámcového rozhodnutí.

Trestnými činy by měly být:

a) **protiprávní přístup k informačním systémům**, tedy úmyslný, neoprávněný přístup k celému informačnímu systému nebo některé jeho části; pokud se nejedná o případ menšího významu, přičemž každý členský stát může rozhodnout, že protiprávní přístup bude trestný jen tehdy, pokud byl spáchán překonáním bezpečnostního opatření;
b) **protiprávní zásah do systému**, tedy úmyslné, neoprávněné, závažné narušení nebo přerušení fungování informačního systému vložením, přenosem, poškozením,

vymazáním, znehodnocením, pozměněním, potlačením nebo znepřístupněním počítačových dat, alespoň pokud se nejedná o případy menšího významu;

c) **protiprávní zásah do dat**, tedy úmyslné, neoprávněné vymazání, poškození, znehodnocení, pozměnění, potlačení nebo znepřístupnění počítačových dat v informačním systému, alespoň pokud se nejedná o případy menšího významu.

Rámcové rozhodnutí však výslovně uvádí, že je třeba zamezit přílišné kriminalizaci, zejména v případě menšího významu, jakož i zamezit kriminalizaci držitelů práv a oprávněných osob. Proto např. u protiprávního přístupu nemusí být pokus trestný, zatímco u ostatních činů se jeho trestnost vyžaduje. V oblasti sankcí je použita jednak obecná, obvyklá formulace, že sankce musí být účinné, přiměřené a odrazující, jednak u protiprávního zásahu do systému nebo do dat je uveden výslovný požadavek, aby horní hranice trestní sazby odnětí svobody činila nejméně 1 až 3 roky. Byl-li trestný čin spáchán v rámci zločinného spolčení, pak má činit tato horní hranice 2 až 5 let. Vyžaduje se též alespoň nepravá trestní odpovědnost právnických osob. K výměně informací mezi členskými státy má být využito sítě operativních kontaktních míst s nepřetržitým provozem.

Rámcové rozhodnutí mělo být provedeno do 16. 3. 2007. Do téhož termínu byly členské státy povinny sdělit Komisi a Generálnímu sekretariátu Rady znění předpisů, kterými ve svém vnitrostátním právu provádějí povinnosti, jež pro ně vyplývají z tohoto rámcového rozhodnutí. **Ve zprávě Komise ze dne 14. 7. 2008** (KOM(2008) 448 v konečném znění) se uvádí, že 20 států informovalo Komisi, 7 tak neučinilo ani v dodatečné lhůtě. Komise uvádí, že došlo k výraznému pokroku a úroveň provádění byla shledána poměrně dobrou. Pokud jde o splnění povinností Českou republikou, pak ve vztahu k provedení čl. 2 (protiprávní přístup k informačním systémům) má Komise vážné výhrady ohledně toho, zda je česká právní úprava v souladu s pojetím okolností, za nichž se nejedná o „případy menšího významu", tak jak jsou pojímány rámcovým rozhodnutím. Komise je toho názoru, že pojetí „případu menšího významu" musí odkazovat na případy, kdy došlo k protiprávnímu přístupu menší důležitosti nebo kdy porušení důvěrnosti informačního systému je menšího stupně. Odpovídající česká pravidla však odkazují na následné zneužití či poškození dat, což nelze považovat za soudržné s výše uvedeným chápáním. Naopak souladný je zákonný požadavek úmyslu způsobit škodu nebo ztrátu v případě čl. 3 (protiprávní zásah do systému) a obdobně tomu je u čl. 4 (protiprávní zásah do dat). Česká republika však dostatečně neinformovala Komisi o provedení čl. 8 a 9 (odpovědnost právnických osob a sankce jim ukládané). Komisi také chybělo sdělení, jak je v České republice využívána stávající síť operativních kontaktních míst s nepřetržitým provozem pro výměnu informací (čl. 11).

2. **Rámcové rozhodnutí 2004/68/SVV ze dne 22. 12. 2003 o boji proti pohlavnímu vykořisťování dětí a dětské pornografii** sice není omezeno na činy spáchané prostřednictvím počítačového systému. Pro takový případ však stanoví, že každý členský stát přijme opatření nezbytná k založení své příslušnosti pro trestné činy podle článku 3 (trestné činy týkající se dětské pornografie), případně podle článku 4 (účastenství a pokus), spáchané prostřednictvím počítačového systému, do kterého bylo vstoupeno z jeho území, bez ohledu na to, zda se počítačový systém samotný nachází na jeho území či nikoli.

3. **Rámcové rozhodnutí Rady 2000/375/JHA ze dne 29. 5. 2000 o boji proti dětské pornografii na internetu**, jak již samotný název napovídá, je zaměřena na boj proti dětské pornografii specificky v prostředí internetu. Neobsahuje znaky skutkových podstat trestných činů. Spíše se soustřeďuje na některá související opatření, která by vedla k odhalení pachatelů. Např. ukládá členským státům, aby podpořily uživatele internetu, aby přímo nebo nepřímo oznamovali donucovacím orgánům podezření o šíření dětského pornografického materiálu na internetu, pokud se s takovým materiálem setkají. Uživatelé internetu jsou informováni o způsobech, jak se spojit s donucovacími orgány nebo se subjekty, které mají výsadní vztahy s těmito orgány, aby těmto orgánům umožnili řádné plnění jejich úlohy předcházet dětské pornografii na internetu a bojovat proti ní. Členské státy zajistí, aby donucovací orgány, pokud obdrží informace o podezření z výroby, zpracování, držení a šíření dětského pornografického materiálu, jednaly rychle a aby donucovací orgány členských států spolupracovaly v rámci již existujících právních nástrojů a využívaly již existujících sítí kontaktních míst k výměně informací Dále členské státy zahájí konstruktivní dialog s průmyslovým odvětvím a posoudí při tom vhodná dobrovolná nebo právně závazná opatření, která by umožnila odstranění dětské pornografie na internetu.

4. **Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob** v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů vyžaduje, aby členské státy chránily práva a svobody fyzických osob v souvislosti se zpracováním osobních údajů, a zejména jejich právo na soukromí, aby byl zajištěn volný pohyb osobních údajů ve Společenství. **Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích)** převedla zásady stanovené ve směrnici 95/46/ES do zvláštních pravidel pro odvětví elektronických komunikací. Rovněž tak nahradila **Směrnici Evropského parlamentu a Rady 97/66/ES ze dne 15. 12. 1997 o zpracování osobních údajů a ochraně soukromí v telekomunikačním sektoru.** Články 5, 6 a 9 směrnice 2002/58/ES stanoví pravidla zpracovávání provozních a lokalizačních údajů vytvářených při používání služeb elektronických komunikací prováděné poskytovateli sítí a služeb. Jakmile již nejsou potřebné pro přenos sdělení, musí být takové údaje vymazány nebo anonymizovány, s výjimkou údajů potřebných pro účtování nebo stanovení plateb za propojení. V případě souhlasu lze určité údaje zpracovávat i pro marketingové účely a pro poskytování služeb s přidanou hodnotou. Ustanovení čl. 15 odst. 1 směrnice 2002/58/ES stanoví podmínky, za nichž mohou členské státy omezit rozsah práv a povinností uvedených v článku 5, článku 6, čl. 8 odst. 1, 2, 3 a 4 a článku 9 uvedené směrnice. Každé takové omezení musí být v demokratické společnosti nezbytné, přiměřené a úměrné pro určitý účel veřejného pořádku, tj. zajištění národní bezpečnosti, obrany, veřejné bezpečnosti nebo pro předcházení, vyšetřování, odhalování a stíhání trestných činů nebo neoprávněného použití elektronických komunikačních systémů. Několik členských států přijalo právní předpisy, které stanoví poskytovatelům služeb povinnost uchovávat údaje pro účely předcházení, vyšetřování, odhalování a stíhání trestných činů. Tyto vnitrostátní předpisy se značně liší. Právní a technické odlišnosti mezi vnitrostátními předpisy o uchovávání

údajů pro účely předcházení, vyšetřování, odhalování a stíhání trestných činů představují překážku na vnitřním trhu elektronických komunikací, protože poskytovatelé služeb čelí různým požadavkům ohledně provozních a lokalizačních údajů, které se mají uchovávat, a podmínek a lhůt uchovávání. Účelem **směrnice 2006/24/EC ze dne 15. 3. 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí** je harmonizovat předpisy členských států týkající se povinnosti poskytovatelů veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí, pokud jde o uchovávání některých údajů jimi vytvořených nebo zpracovaných, s cílem zajistit dostupnost těchto údajů pro účely vyšetřování, odhalování a stíhání závažných trestných činů, jak jsou vymezeny každým členským státem v jeho vnitrostátních právních předpisech. Směrnice se vztahuje na provozní a lokalizační údaje o právnických i fyzických osobách a na související údaje, které jsou nezbytné k identifikaci účastníka nebo registrovaného uživatele. Nevztahuje se na obsah elektronických sdělení ani na informace vyžadované při použití sítě elektronických komunikací. Data jsou ve směrnici rozdělena do několika kategorií, přičemž členské státy zajistí, aby se tyto údaje uchovávaly po dobu nejméně šesti měsíců a nejvýše dvou let ode dne komunikace.

Všechny citované směrnice se tedy týkají nakládání s osobními údaji, problematice, která se označuje anglickým termínem „data retention". K tomu je možné blíže odkázat na zevrubné pojednání J. Hořáka.[23] Vedle toho upravuje Směrnice **o soukromí a elektronických komunikacích** také otázky jiné ochrany soukromí, např. uvedení a omezení identifikace volajícího a volaného (čl. 8), otázku nevyžádaných sdělení (čl. 13) apod.

5. Jediným dokumentem, který se zabývá odpovědností internetových poskytovatelů služeb (ISP), je **Směrnice 2000/31/EC ze dne 8. 6. 2000 o některých právních aspektech služeb informační společnosti**, zejména elektronického obchodu, na vnitřním trhu (Směrnice o elektronickém obchodu). Směrnice rozlišuje mezi prostým přenosem, ukládáním do vyrovnávací paměti a ukládáním informací. Podle toho je stanovena odpovědnost jednotlivých poskytovatelů za cizí obsah. K tomu lze odkázat na příspěvek J. Říhy v této publikaci. Vedle toho upravuje směrnice takové aktivity v kyberprostoru jako obchodní sdělení (čl. 6 až 8) a uzavírání smluv elektronickou cestou (čl. 9 až 11).

6. V posledních letech je i orgány ES/EU stále větší pozornost věnována **vytvoření obecné politiky boje proti počítačové kriminalitě**. Výsledkem této snahy je **Sdělení Komise** Evropskému Parlamentu, Radě, Hospodářskému a sociálnímu výboru a Výboru regionů k obecné politice v boji proti počítačové kriminalitě **ze dne 22. 5. 2007** (KOM (2007) 267).

Komise si je vědoma, že žádná efektivní trestní represe nemůže být funkční bez efektivní prevence. Ve sdělení se konstatuje, že nejsou k dispozici data a statistiky o kybernetických trestných činech. Navíc jsou tyto činy zřídka hlášeny příslušným orgánům, např. i proto, že společnosti, které se staly obětí takových činů, se bojí nega-

[23] Hořák. J. Právo na soukromí versus bezpečnost ve sjednocené Evropě: zamyšlení nad problematikou „data retention". Acta Universitatis Carolinae – Iuridica, 2006, č. 1, str. 81–98.

tivního dopadu, jestliže bude známo, že jejich systém je zranitelný. Prozatím přijaté právní instrumenty se zabývají jen některými aspekty boje proti kybernetické kriminalitě. Je proto žádoucí vytvořit komplexní politiku v boji proti kybernetické kriminalitě. Komise označila těchto osm okruhů problémů:

1. Rostoucí zranitelnost společnosti, obchodu a občanů vůči rizikům počítačové kriminality.
2. Zvýšená četnost a důmyslnost trestných činů v oblasti počítačové kriminality.
3. Nedostatečná ucelená politika a právní předpisy na úrovni EU v boji proti počítačové kriminalitě.
4. Specifické obtíže v operativní spolupráci při prosazování právních předpisů v oblasti počítačové kriminality.
5. Potřeba vytyčit pravomoci a technické nástroje, k čemuž je zapotřebí odborná příprava a výzkum.
6. Nedostatek funkčních struktur pro spolupráci mezi důležitými zúčastněnými stranami ve veřejném a soukromém sektoru.
7. Nejasné rozdělení odpovědnosti a závazků.
8. Nedostatek všeobecného povědomí o rizicích plynoucích z počítačové kriminality.

Uvedeným okruhům problémů odpovídá i vytýčení cílů, zejména:

1. Zlepšit operativní přeshraniční činnost v oblasti prosazování právních předpisů zaměřené všeobecně proti počítačové kriminalitě, a zejména jejich závažným druhům. Zlepšit výměnu informací, odborných znalostí, osvědčených postupů apod.
2. Určit a vytvořit operativní nástroje pro spolupráci a společné vytýčení cílů mezi veřejným a soukromým sektorem.
3. Vytvořit politickou platformu a politické struktury pro vypracování důsledné politiky EU v boji proti počítačové kriminalitě, zefektivnit stávající právní a institucionální rámce.
4. Čelit rostoucí hrozbě plynoucí ze závažných forem počítačové kriminality, a to podporou dovedností, znalostí a technických nástrojů.
5. Zvýšit obecné povědomí o hrozbě počítačové kriminality, zejména mezi spotřebiteli a jinými zranitelnými skupinami potenciálních obětí.

Komise na základě vytýčených cílů formulovala **ve čtyřech variantách** možné strategické politiky (1. zachování statu quo; 2. vytvoření všeobecných právních předpisů; 3. vytvoření neformálních sítí pro boj proti počítačové kriminalitě a veřejně-soukromých sítí; 4. soudržný strategický přístup), které následně analyzovala a dospěla k závěru, že optimální bude varianta 4, tedy že by byl zřízen strategický rámec pro politiku boje proti počítačové kriminalitě na úrovni EU, přičemž obecným cílem by bylo lepší řízení konkrétních činností a optimalizace stávajících prostředků. Dalšími prvky této strategie by byly: lepší spolupráce při prosazování právních předpisů na úrovni EU, zavedení strategické struktury pro veřejně-soukromou spolupráci v boji s kybernetickou kriminalitou, podpora zřízení rámce pro celosvětovou mezinárodní spolupráci, cílená legislativní opatření dle potřeby. Uvedená varianta má jen velmi málo negativních dopadů nebo překážek. Nevýhodou je, že její přímé dopady jsou v krátkodobém horizontu spíše skromné. Tato varianta byla vybrána za výchozí, nevylučuje však ani prvky varianty 2 nebo 3.

Pokud se jedná o přijímání právních předpisů, **některé cílené právní předpisy** by však měly být zváženy už nyní. Konkrétně jde o situace, kdy je počítačová kriminalita páchána ve spojení s tzv. krádeží identity. Pod pojmem „krádež identity" se všeobecně rozumí používání osobních identifikačních informací, např. číslo kreditní karty, jako nástroj ke spáchání jiných trestných činů. Krádež identity jako taková není ve většině členských států považována za trestný čin. Je často snadnější dokázat trestný čin krádeže identity, než trestný čin, který má být následně pomocí „odcizených" údajů spáchán, takže by spolupráci v oblasti prosazování právních předpisů na úrovni EU prospělo, kdyby byla krádež identity zákonně považována za trestný čin ve všech členských státech. Obdobně se uvažuje o právních předpisech, zavazujících k postihu spamu.[24] I když určité kroky již učiněny byly. Viz např. Směrnice 2002/58/EC ze dne 12. 7. 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací, která zakazuje spam zavedením zásady, že marketing zaměřený na fyzické osoby musí být založen na jejich souhlasu.

6. ZÁVĚREM

Cílem příspěvku bylo poukázat na stále rostoucí počet norem v oblasti mezinárodního a evropského práva, jejichž záměrem je regulovat nebo dokonce eliminovat některé aktivity v kyberprostoru. Ukazuje se, že regulace na této úrovni je nezbytná. Bez potřebné harmonizace některých právních norem by s ohledem na různorodost národních úprav nebylo možné efektivně čelit nežádoucím či celospolečensky nebezpečným jevům v prostoru hranicemi neomezeném. První právně závazné nástroje v boji proti nežádoucím jevům v kyberprostoru (tzv. kybernetickým hrozbám) vznikají až koncem 20. a počátkem 21. století. Z mezinárodních úmluv je na prvním místě podle svého významu nezbytné zmínit Úmluvu Rady Evropy o kybernetické kriminalitě, která je svým rozsahem a komplexností ojedinělá. V právu ES/EU nalezneme také několik právních dokumentů věnovaných problematice regulace některých činností v kyberprostoru. Jedná se především o směrnice a rámcová rozhodnutí. Lze říci, že Evropská společenství se snaží o regulaci v daleko širším rozsahu, než je tomu u mezinárodních úmluv. To je pochopitelné s ohledem na potřebu zabezpečit cíle Společenství, které jsou vytyčeny především ve Smlouvě o založení Evropského společenství. Od řešení dílčích otázek se postupně přechází k vytvoření obecné politiky s cílem vypořádat se s úlohami, které stojí před informační společností, v podstatě ve třech úrovní: 1) zvláštní opatření pro bezpečnost sítí a informací, 2) regulační rámec pro elektronické komunikace, 3) boj proti počítačové kriminalitě. Jakkoli je patrná snaha o právní regulaci kyberprostoru, je celkem zřejmé, že v této oblasti více než v kterékoliv jiné se zřetelně projevu určitá kontradikce mezi dynamickým rozvojem informačních a telekomunikačních technologií na jedné straně a rigidními a dlouhotrvajícím procesem přijímání nových či novelizací již existujících norem.

[24] Sdělení Komise o boji proti spamu, spyware, malicious software KOM(2006)688 ze dne 15. 11. 2006.

DIE VERPFLICHTUNGEN ZUM SCHUTZ DES KYBERRAUMS, DIE AUS DEM INTERNATIONAL- UND EUROPÄISCHEN RECHT HERVORGEHEN

Zusammenfassung

Der Autor weist in seinem Artikel auf die ständig steigende Anzahl der Normen im Gebiet des international- und europäischen Rechts hin, deren Vornehmen die Regulierung oder sogar Elimination von einigen Aktivitäten im Kyberraum ist. Er widmet sich den Normen der Organisation der Vereinigten Nationen, des Europarats, OECD und dem Recht der EU/EG. In den Einzelheiten widmet er sich vor allem dem Abkommen über Computerkriminalität, der Rahmenentscheidung über die Angriffe gegen Informationssystem und der Richtlinie über elektronisches Geschäft. Der Autor betont, dass sich die Europäische Gemeinschaft über die Regulation im breiten Umfang bemühen, als es in Internationalabkommen ist, was begreiflich im Hinblick auf den Bedarf die Ziele gewährleisten ist, die vornehmlich in dem Vertrag über Gründung der Europäischen Gemeinschaft festgesetzt sind.

Schlagwörter: der Kyberraum, die Kyberkriminalität, das Abkommen über Computerkriminalität, die Rahmenentscheidung über die Angriffe gegen Informationssystem, die Richtlinie über elektronisches Geschäft, die Verantwortung für fremden Inhalt

Klíčová slova: kyberprostor, kybernetická kriminalita, Úmluva o kybernetické kriminalitě, rámcové rozhodnutí o útocích proti informačním systémům, směrnice o elektronické komunikaci, odpovědnost za cizí obsah