ACTA
UNIVERSITATIS
CAROLINAE

IURIDICA 4/2008

ČESKÝ PRÁVNÍ ŘÁD A OCHRANA KYBERPROSTORU

(vybrané problémy)

UNIVERZITA KARLOVA V PRAZE
NAKLADATELSTVÍ KAROLINUM
2008

Vědecký redaktor: JUDr. Bc. Tomáš Gřivna, Ph.D.

Recenzovali: JUDr. Marie Vanduchová, CSc.
doc. Ing. Václav Jirovský, CSc.

Tato publikace vychází v rámci programu Bezpečnostní výzkum s názvem „Problematika kybernetických hrozeb z hlediska bezpečnostních zájmů České republiky" – VD2007010B01.

ISSN 0323-0619

OBSAH

URČENÍ ROZHODNÉHO PRÁVA PRO ODPOVĚDNOST VYPLÝVAJÍCÍ Z UŽITÍ DÍLA V KYBERPROSTORU

JIŘÍ ČERMÁK
Ústav práva autorského, práv průmyslových a práva soutěžního
Právnické fakulty Univerzity Karlovy v Praze
Baker & McKenzie, v.o.s., advokátní kancelář

1. OBECNĚ K PROBLEMATICE URČENÍ ROZHODNÉHO AUTORSKÉHO PRÁVA

1.1 PRINCIP TERITORIALITY

1.1.1 Bernská úmluva

Autorské právo má své kořeny v 18. století, v prostředí, kde hlavním autorským dílem byla kniha, obraz nebo divadelní hra. Postupem doby se okruh chráněných děl rozrůstal, nicméně stále bylo relativně velmi jednoduché určit, kde bylo dílo užito, například kde byla kniha vytisknuta či kde bylo divadelní představení (tj. divadelní hra) předvedeno publiku, případně kde došlo k neoprávněnému užití takového díla.

Na tomto poznatku byla postavena i Bernská úmluva[1], která na konci devatenáctého století mimo jiné zakotvila princip, podle kterého se, dle převažující interpretace, určí, jaký právní řád, tedy jaké rozhodné právo, je nutno aplikovat při posouzení konkrétního aktu užití díla, ať již jde o jeho rozmnožování, rozšiřování, veřejné vystavování či jiný způsob nakládání s ním. Bernská úmluva řeší tuto otázku tak, že požaduje aplikaci práva toho státu, na jehož území se uplatňuje ochrana (*lex loci protectionis*)[2]. Tento požadavek se též nazývá *princip teritoriality* a je v Bernské úmluvě vyjádřen na více místech, zejména v článku 5 odst. 2 RÚB a článku 6bis odst. 3 RÚB.

V tomto ohledu je zejména čl. 5 odst. 2 RÚB, který stanoví, že „*ustanovení této úmluvy řídí rozsah ochrany, jakož i právní prostředky vyhrazené autorovi k hájení jeho práv výlučně zákony státu, kde se uplatňuje nárok na ochranu*" do jisté míry zaváděPage_footer_7

[1] Bernská úmluva o ochraně literárních a uměleckých děl ze dne 9. 9. 1886, ve znění pařížské revize ze dne 24. 6. 1971 – pro ČR vyhl. MZV 133/1980 Sb., též často označována jako Revidovaná úmluva Bernská, ve zkratce „**RÚB**".

[2] Někteří autoři nevykládají příslušná ustanovení Bernské úmluvy jako kolizní normu a jsou toho názoru, že princip *lex loci protectionis* v ní vůbec zakotven není. I s tímto názorem lze souhlasit, neboť jak je uvedeno dále v článku, Bernská úmluva rozhodně není v tomto směru nijak jednoznačná a zdá se, že snaha vyložit ji tak, že princip *lex loci protectionis* skutečně zakotvuje, pravděpodobně není zcela v souladu s prvotním záměrem autorů této úmluvy. Nicméně i ti, kteří neuznávají, že Bernská úmluva se zabývá kolizní otázkou, připouštějí, že princip *lex loci protectionis* je vhodným vodítkem k určení, autorské právo jakého státu použít v případě neoprávněného zásahu do autorských práv.

jící, neboť může budit dojem, že je třeba vždy užít práva toho státu, kde probíhá soudní řízení (*lex fori*). Avšak převažující názor[3] se přiklání k výkladu tohoto ustanovení tak, že je třeba aplikovat právo státu, kde došlo ke (zne)užití díla, neboť v takovém státě hledá oprávněný subjekt ochranu, a to bez ohledu na to, zda se této ochrany, ať již z jakéhokoli důvodu, domáhá prostřednictvím soudu jiného státu.

Druhý přístup, který je řekněme více ekonomicky zaměřený, se kloní k tomu, že výše uvedené ustanovení je třeba vykládat tak, že umožňuje i aplikaci práva státu (či států), kde se projeví důsledek takového (zne)užití díla, tedy především právo státu, ve kterém vzniká z takového jednání škoda. Takový stát nemusí být totožný se státem, kde ke (zne)užití díla došlo. Vzhledem k možné distanční povaze určitých způsobů užití díla může, striktně vzato, k užití díla (např. jeho rozmnožením či zpřístupněním) dojít v jedné zemi, kdežto důsledek se projeví v zemi jiné (to platí typicky v případě dálkového přístupu k dílu).

Smluvními stranami Bernské úmluvy je ke dnešnímu dni 164 států světa, přičemž za nejvýznamnější rozšíření počtu signatářských států z „poslední doby" je třeba považovat přistoupení Spojených států amerických v roce 1989.

Tudíž princip teritoriality lze tak, jak je vyjádřen v Bernské úmluvě, považovat za vcelku univerzální vodítko k určení rozhodného práva pro mimosmluvní závazkové vztahy, které vznikají z porušení práva autorského.

1.1.2 Nařízení Řím II

Na úrovni komunitárního práva upravuje obdobnou otázku Nařízení Evropského Parlamentu a Rady (ES) č. 864/2007 ze dne 11. července 2007 o právu rozhodném pro mimosmluvní závazkové vztahy (dále je „**Nařízení**").

Nařízení s výjimkou ustanovení čl. 29 vstoupí v účinnost 1. ledna 2009 a podle českého ústavního pořádku má s ohledem na čl. 10 a čl. 10a Ústavy a čl. 249 SES přednost před zákonem i před starší a obecnější Bernskou úmluvou. Ze samotné povahy nařízení vyplývá, že jej není třeba provádět (transformovat) žádnou národní legislativní normou, je bez dalšího závazné a od 1. ledna 2009 bude platné a účinné bezprostředně ve všech členských státech, včetně České republiky. Je však třeba zdůraznit, že v návaznosti na čl. 1 a 2 Protokolu o přistoupení Dánska k Evropské unii není Dánsko Nařízením vázáno a dánské soudy se jím nebudou řídit[4].

Nařízení řeší otázku určení rozhodného práva pro odpovědnost z porušení autorského práva v článku 8 nazvaném „*porušení práv duševního vlastnictví*", který stanoví, že:

1. *Rozhodným právem pro mimosmluvní závazkové vztahy, které vznikají z porušení práva duševního vlastnictví, je právo* ***země, pro kterou je uplatňována ochrana těchto práv.***

---

[3] Např. Bainbridge, D. Intellectual Property. Pearson Education Limited, 2005; Świerczyński, M. Unification of the conflict rules concerning intellectual property right infringements. (http://www.ipr-helpdesk.org/newsletter/21/html/EN/IPRTDarticleN1094C.html, 28. 05. 2008); Kučera, Z. a kol. Mezinárodní právo soukromé. Doplněk Brno, 1996.

[4] Viz čl. 1 odst. 4 Nařízení.

2. *Rozhodným právem pro mimosmluvní závazkové vztahy, které vznikají z porušení jednotného práva duševního vlastnictví Společenství, je v otázkách neupravených příslušným aktem Společenství právo* ***země, ve které k tomuto porušení došlo.***
3. *Rozhodné právo určené podle tohoto článku nelze vyloučit dohodou podle článku 14.*

První odstavec stanovuje pro autorskoprávní delikty jakožto množinu porušení práv duševního vlastnictví stejný princip jako Bernská úmluva, a to stejně neurčitým způsobem. K jeho výkladu se vracíme níže.

Odstavec druhý nelze na autorské právo aplikovat, neboť Společenství jednotnou úpravu autorského práva (komunitární autorské právo) nezná. Ustanovení tohoto odstavce se tedy týká zejména komunitárních ochranných známek (ochranná známka Společenství) a komunitárních průmyslových vzorů (průmyslový vzor Společenství), které podléhají jednotné ochraně v rámci všech členských států na základě příslušných nařízení.

Ve třetím odstavci je stanoven zákaz stran (poškozeného a škůdce) si rozhodné právo určit vzájemnou dohodu podle čl. 14 Nařízení[5]. Nařízení tedy striktně požaduje, aby jediným kolizním určovatelem byl princip vyjádřený v čl. 8 odst. 1, respektive odst. 2.

K prvnímu odstavci čl. 8 Nařízení je třeba se vrátit v podrobnějším rozboru, neboť jak je na první pohled patrné, jeho znění připouští různé výklady.

Dle mého názoru je třeba čl. 8 odst. 1 Nařízení chápat tak, že přikazuje užití práva toho státu, kde bylo dílo neoprávněně užito (*lex loci protectionis*). K tomu mne vedou následující skutečnosti:

V prvé řadě Komise ve svém komentáři k čl. 8 Nařízení[6] výslovně uvádí, že princip teritoriality stanovený v tomto článku je třeba ve vztahu k autorskému právu vykládat (v souladu s čl. 5(2) RÚB) tak, že odkazuje na „právo státu, kde došlo k zásahu do práva", tedy kde bylo dílo neoprávněně užito.

Dále je třeba vzít v úvahu, že obecný princip k určení rozhodného práva, které Nařízení zavádí, stanoví, že rozhodným právem pro mimosmluvní závazkové vztahy má být právo země, kde vznikla škoda (*lex loci damni*), a to bez ohledu na to, ve které zemi došlo ke skutečnosti, jež vedla ke vzniku škody[7]. Tento obecný princip však neplatí pro odpovědnost vyplývající z porušení práv duševního vlastnictví. Komise ve svém zdůvodnění uvádí, že princip *lex loci damni* není ve vztahu k odpovědnosti z porušení autorských práv (a práv duševního vlastnictví obecně) vhodný a že je třeba se držet principu teritoriality (*lex loci protectionis*) zavedeného v Bernské úmluvě[8].

I z výše uvedeného lze vyvodit, že do jisté míry neurčité znění ustanovení článku 8 odst. 1 Nařízení nelze vykládat tak, že umožňuje aplikaci práva státu (či států), kde se projeví důsledek takového (zne)užití díla, tedy především právo státu, ve kterém vzniká z takového jednání škoda (*lex loci damni*). Zejména proto, že pokud by takový

[5] Vzhledem k tomu, že jde o mimosmluvní odpovědnost, čl. 14 hovoří o dohodě stran až po vzniku škody, což je třeba odlišit od dohody o rozhodném právu, která je učiněna předem, jak je tomu v případě smluvních závazkových vztahů.
[6] COM (2003) 427 final, str. 20.
[7] Článek 4 Nařízení.
[8] COM (2003) 427 final, str. 21.

důsledek zákonodárce zamýšlel, neměl by pak žádný důvod specificky a odlišně od této obecné zásady upravovat otázku odpovědnosti vyplývající z porušení práv duševního vlastnictví tak, jak je tomu v čl. 8 Nařízení.

Článek 8 nelze ani vkládat tak, že by mělo být aplikováno právo státu, ve kterém sídlí soud, jenž se sporem zabývá (*lex fori*), k čemuž jeho znění svádí. To vyplývá zejména ze samotné povahy Nařízení, jehož smyslem je zabránit nežádoucímu stavu, kdy by se rozhodné právo odvozovalo od státu, kde sídlí soud, u něhož je řízení vedeno. To je výslovně uvedeno v recitálu č. 6 Nařízení[9].

Zůstává tedy otázkou, proč nedošlo k výslovnému zakotvení *lex loci protectionis* do čl. 8 odst. 1 Nařízení způsobem, který by nepřipouštěl různé výklady. Nestalo se tak ani přesto, že byly během legislativního procesu podány návrhy, aby znění čl. 8 odst. 1 bylo jednoznačné a shodně s čl. 8 odst. 2 stanovilo, že rozhodným právem pro mimosmluvní závazkové vztahy, které vznikají z porušení práva duševního vlastnictví, je *právo země, ve které k tomuto porušení došlo* (namísto neurčitého *právo země, pro kterou je uplatňována ochrana těchto práv*). Osobně se domnívám, že současné neurčité znění je důsledkem střetu různých názorových směrů a vzájemných ústupků mezi mnoha zájmovými skupinami, neboť princip teritoriality rozhodně není jednomyslně přijímaný jako nejlepší a nejefektivnější metoda určování rozhodného práva. V určitých zájmových skupinách panuje obava, že v případě striktní aplikace principu teritoriality a posuzování autorskoprávních deliktů podle *lex loci protectionis* by mohlo dojít k nežádoucí situaci, kdy by bylo třeba aplikovat právo státu, které je buďto pro nositele práv (jako potenciálního žalobce) neznámé či neposkytuje dostatečnou ochranu. Snahou nositelů práv obecně je dosáhnout aplikace svého vlastního právního řádu, který tyto subjekty znají a který jim poskytuje pro ně dostatečnou míru ochrany.

To platí dvojnásobně zejména u deliktů, jejichž účinky mají „nadstátní" rozsah, což je především případ rozšiřování děl prostřednictvím internetu. Příčinou současného stavu je tedy podle mého názoru obava, že by princip zakotvený v čl. 8 odst. 1 bez jakýchkoli pochybností nutně vedl k aplikaci určitého konkrétního právního řádu, který by se mohl ukázat jako nevhodný či (a to častěji) nežádoucí v očích nositelů práv.

To je podpořeno i snahou většiny soudů pokud možno aplikovat své vlastní právo, které tyto soudy znají, a současně se zájmem nositelů práv žalovat u svého národního soudu. Pokud by byl princip teritoriality vykládán striktně tak, jak požaduje Komise ve svém odůvodnění, docházelo by velmi často k tomu, že by soud, který se sporem zabývá, byl nucen aplikovat cizí právo. A představa, že by zejména anglické soudy měly aplikovat cizí právo, je přijímána s výraznou nevolí.

Lze tedy shrnout, že potřeba umožnit výklad čl. 8 odst. 1 pružně a dle potřeb konkrétního subjektu a ponechat si tak „zadní vrátka" pro případ, že by se princip teritoriality (jak je vykládán výše) neosvědčil či nehodil, vedla, dle mého soudu, k současnému nepříliš šťastnému znění.

---

[9] Recitál č. 6 zní: *„Řádné fungování vnitřního trhu vyžaduje v zájmu zlepšení předvídatelnosti výsledku sporů, jistoty co do rozhodného práva a volného pohybu soudních rozhodnutí, aby kolizní normy platné v členských státech určovaly stejný právní řád bez ohledu na zemi soudu, který se sporem zabývá."*

1.1.3 Shrnutí

I přes nejednoznačné znění článku 5 odst. 2 Bernské úmluvy a 8 odst. 1 Nařízení převažuje názor, že obě tato ustanovení zakotvují pro odpovědnostní vztahy, které vznikají z porušení autorského práva, princip *lex loci protectionis* a že je tedy třeba aplikovat právo státu, kde došlo ke (zne)užití díla, neboť v takovém státě hledá oprávněný subjekt ochranu proti takovému jednání.

Jeho aplikace znamená, že pokud například státní příslušník země A užije autorské dílo státního příslušníka země B v zemi C, řídí se tento konkrétní akt užití díla (například vypalování CD s hudbou) autorským zákonem země C, nikoli zákony zemí A či B. Například: Čech v Bulharsku nelegálně vypaluje a distribuuje CD s hudbou Louise Armstronga. Takové jednání (tj. užití díla jeho rozmnožováním a rozšiřováním) je potřeba posoudit podle bulharských zákonů. Podmínkou pro nutnou aplikaci principu teritoriality je, aby daný stát přistoupil k Bernské úmluvě, respektive aby byl členem Evropské unie.

1.2 VOLBA ROZHODNÉHO PRÁVA

1.2.1 Volba práva pro mimosmluvní závazkové vztahy

Jak jsem již nastínil, Nařízení umožňuje v některých případech, aby si strany (tedy odpovědný a povinný z mimosmluvní odpovědnosti) dohodou zvolily právo, kterým se jejich odpovědnostní vztah bude řídit, *ex post*, tedy po události, která vedla ke vzniku odpovědnosti.

Tuto „zpětnou" volbu umožňuje článek 14 Nařízení, který stanoví, že *„strany si mohou zvolit právo, kterým se bude řídit jejich mimosmluvní závazkový vztah, a) dohodou, která byla uzavřena poté, co došlo ke skutečnosti, jež vedla ke vzniku škody, nebo b) dohodou, která byla svobodně sjednána před tím, než došlo ke skutečnosti, jež vedla ke vzniku škody, v případě, že všichni účastníci jednají v rámci své podnikatelské činnosti."*

Avšak tato možnost volby není dána pro mimosmluvní vztahy vyplývající z porušení práva duševního vlastnictví, neboť čl. 8 odst. 3 Nařízení tuto možnost výslovně zapovídá.

1.2.2 Volba práva pro smluvní závazkové vztahy

Pro úplnost považuji za vhodné uvést, že od rozhodného práva, kterým se řídí posouzení mimosmluvní odpovědnosti vyplývající z konkrétního aktu užití díla, je nutno odlišit právo, kterým se bude řídit dohoda stran týkající se nakládání s dílem či autorským právem k dílu – například smluvní převod autorského práva k dílu[10] nebo smluvní ujednání, kterým se uděluje oprávnění dílo užít (licence).

Právo, kterým se bude tento vztah řídit, se určuje podle norem mezinárodního práva soukromého toho státu, ve kterém probíhá soudní řízení. V České republice je touto normou zejména Římská úmluva, vyhlášená v pod č. 64/2006 Sb.m.s. („**Římská úmluva**") a zákon č. 97/1963 Sb. o mezinárodním právu soukromém a procesním („**ZMPS**"), ve znění pozdějších předpisů.

[10] Za předpokladu, že je takový převod možný – podle našich platných norem tak tomu není (viz § 11 odst. 4 a § 26 odst. 1 AutZ).

V těchto dvou normách, zejména v Římské úmluvě, jsou určeny základní principy pro určení rozhodného hmotného práva pro okruh smluvních závazkových vztahů.

Nejvýznamnější roli zde hraje čl. 3 Římské úmluvy a § 9 ZMPS, který hovoří o tzv. volbě práva. Ta umožňuje účastníkům smlouvy zvolit si konkrétní právo, kterým se mají řídit jejich vzájemné vztahy. Tento institut je znám většině právních řádů, a je proto velmi užívaný.

Lze tedy předpokládat, že právě volba práva bude převažujícím způsobem určení rozhodného práva pro autorskoprávní smlouvy. Tento institut však, jak bylo uvedeno, nelze uplatnit pro mimosmluvní odpovědnost vyplývající z porušení autorského práva.

1.3 PROBLEMATIKA URČENÍ AUTORA, BENEFICIANTA PŮVODNÍCH PRÁV

Souvisejícím problémem, na jehož řešení nepanuje všeobecná shoda, je stanovení právního řádu, podle kterého se určí, kdo je (byl) původní osobou oprávněnou k výkonu autorských práv – původní nositel práv (autor).

V zásadě lze uvažovat o dvou přístupech. První přístup se přiklání k tomu, že je třeba tuto osobu určit podle práva země původu díla (*princip originality*), kdežto podle jiného názoru je třeba postupovat podle práva země, kde bylo dílo (zne)užito (*lex loci protectionis*).

Zdá se, že převažuje názor – podle mého mínění zcela správný – že původního nositele práv je nutno určit podle práva země původu díla. Jiný výklad by podle mého názoru značně ohrožoval právní jistotu. Pokud bychom připustili, že podle *lex loci protectionis* je možné určit, že původním nositelem práv je někdo jiný, než jak stanoví práva země původu díla, došlo by k nežádoucímu stavu. Ten spočívá v tom, že původního nositele práv by bylo možné určit podle různých kritérií (v závislosti na tom, jaký právní řád by se v daném případě podle principu teritoriality určil jako *lex loci protectionis*), přičemž jednotlivé právní řády by mohly za takového původního nositele práv označit pokaždé jinou osobu. To by mělo negativní dopad zejména na právní jistotu třetích stran, neboť by mohlo dojít ke zpochybnění již dávno provedených smluvních převodů. (Podle zásady, že nikdo nemůže na jiného převést více práv, než sám má, by veškeré předchozí smluvní převody autorského práva nebo poskytnutá oprávnění k užití autorského práva (licence) byly neplatné.). Stejně tak by panovala pochybnost, kdo je oprávněn se domáhat ochrany autorského práva k dotčenému dílu.

Tato nejistota odpadá, pokud trváme na určení původního nositele podle práva země původu díla, neboť toto právo je pevně dáno. Je pak zaručeno, že tato osoba bude vždy jednoznačně určena.

Výjimkou, která je přímo uvedena v článku 14bis RÚB, jsou audiovizuální díla, u nichž se autorství posuzuje podle autorského práva státu, na jehož území se požaduje ochrana (tedy kde došlo k užití díla).

Pro úplnost je třeba upozornit na to, že od určení původního nositele práv je nutné odlišit další (odvozené) nositele práv či jinak oprávněné osoby k výkonu těchto práv. Jejich oprávnění vznikne na základě smluvních převodů těchto práv (v případech, kde je to možné), případně přímo na základě zákona, jak je tomu například u zaměstnaneckých děl podle § 58 českého autorského zákona.

1.4 PROBLEMATIKA OCHRANY OSOBNOSTNÍCH AUTORSKÝCH PRÁV (MORAL RIGHTS)

Vzhledem k odlišnému pojetí osobních autorských práv v kontinentálním (evropském) a anglo-americkém (copyright) právním systému, lze z řad zejména anglických odborníků příležitostně slyšet názory, že rozsah těchto práv a důsledky jejich porušení nelze posuzovat podle práva určeného na základě principu teritoriality (to jest *lex loci protectionis*), a tedy článek 8 odst. 1 Nařízení nelze pro tyto účely aplikovat. S tímto vnímáním Nařízení však podle mého názoru nelze souhlasit.

Článek 2 Nařízení stanoví, že „*škoda zahrnuje jakékoli následky civilního deliktu, bezdůvodného obohacení, jednatelství bez příkazu nebo předsmluvního jednání*". Nelze tedy škodu omezit pouze na škodu materiální, peněžitou. Újmu způsobenou neoprávněným zásahem do osobnostních autorských práv je proto třeba považovat za škodu ve smyslu Nařízení.

Nařízení dále v čl. 8 hovoří obecně o „porušení práv duševního vlastnictví", za která se považuje například autorské právo a práva související, zvláštní právo (*sui generis*) na ochranu databází a práva průmyslového vlastnictví. Pojem „autorské právo" (v anglickém jazyku „copyright") nelze zužovat pouze na majetková autorská práva, neboť osobnostní práva, která jsou garantována Bernskou úmluvou, jsou zakotvena např. i v britském Copyright, Designs and Patents Act 1988. Rozeznává je tudíž i anglické právo, které je jediným právním systémem v rámci EU, který je založen na anglosaském „copyright law" principu ochrany autorského práva.

Z výše uvedeného dle mého názoru jednoznačně vyplývá, že podle práva určeného na základě principu teritoriality zakotveného v čl. 8 odst. 1 Nařízení, je třeba stanovit i rozsah a povahu osobnostních autorských práv a důsledky jejich porušení.

1.5 ZÁVĚR

Z výše uvedeného vyplývá, že v případě mimosmluvní odpovědnosti vyplývající z porušení autorského práva (neoprávněného zásahu do autorského práva) je třeba aplikovat právo státu, kde došlo k takovému porušení, tedy ke (zne)užití díla. Tento princip je zakotven v čl. 5 odst. 2 Bernské úmluvy a čl. 8 Nařízení. Toto právo nemusí být identické s právem státu, kde sídlí soud, který se sporem týkajícím se nároků z neoprávněného užití díla zabývá.

V souvislosti s ochranou autorského práva je pak možné uvést, které konkrétní složky autorského práva se budou řídit právem země, kde došlo k užití díla. Jsou to:

1. určení, zda jde či nejde o autorské dílo a zda tedy požívá či nepožívá autorské ochrany;
2. určení, jaká práva má autor včetně nároků z porušení těchto práv (a to včetně rozsahu práv osobnostních a nároku z nich);
3. výjimky k těmto právům;
4. doba trvání těchto práv.

Ne zcela jasné zůstává, podle jakého práva je třeba určit autorství k dílu, to jest původního nositele práv, neboť tuto problematiku Bernská úmluva ani Nařízení výslov-

ně neupravují. Lze však shrnout, že za převažující názor je třeba považovat ten, který autorství posuzuje (až na výjimku u audiovizuálních děl) podle země původu díla.

2. PROBLEMATIKA URČENÍ ROZHODNÉHO AUTORSKÉHO PRÁVA V PROSTŘEDÍ INTERNETU

V první části tohoto příspěvku jsem se pokusil ve zkratce shrnout základní principy, podle kterých se v obecné rovině určí rozhodné právo pro odpovědnostní vztahy vyplývající z neoprávněného užití díla. V druhé části tohoto příspěvku bych se rád zaměřil přímo na otázku určení rozhodného práva v případech užití díla prostřednictvím internetu.

2.1 PROBLEMATIKA URČENÍ MÍSTA UŽITÍ DÍLA

Spolu s přenosem dat představující autorské dílo, případně s možností přistupovat k těmto datům dálkově, ať již prostřednictvím sítě internet nebo jinak, je spojen zásadní problém, a sice podle jakého právního řádu posuzovat takové jednání, když následky užití díla přesahují hranice jednoho státu.

Na úvod dvě přirovnání. Zpřístupnění autorského díla na konkrétní webové stránce, která je dostupná v podstatě z jakéhokoliv místa na světě, se dá s jistou nadsázkou a zjednodušením přirovnat k situaci, kdy divadelní představení probíhá na hranici dvou států, přičemž pódium divadla je v jednom státě a hlediště v druhém. Diváci tak sledují představení přes státní hranici. Nabízí se otázka, ve kterém z těchto dvou států k užití díla (v tomto případě živému provozování díla) vlastně došlo.

Na jednu stranu lze argumentovat tím, že k užití díla dochází pouze v tom státě, kde se „něco děje", kde dochází k aktivnímu nakládání s dílem osobou, jež jej provádí (hercem). Tedy kde se nachází jeviště.

Proti tomu je možné postavit tvrzení, že podstatné je až místo vnímání díla, neboť smyslem živého provozování díla je právě jeho zpřístupnění veřejnosti a teprve vnímáním příjemcem (divákem) je takové zpřístupňování dokonáno. V takovém případě bychom dospěli k názoru, že dílo je užito tam, kde se nachází hlediště.

V neposlední řadě je možné tuto situaci posoudit tak, že k užití díla v našem příkladě dochází jak na místě, kde fakticky dochází k nakládání s dílem (jeviště), tak i v místě, kde je takové dílo vnímáno (hlediště).

Modernější paralelou je případ satelitního vysílání. Při tomto vysílání je signál představující filmové dílo vyslán z určitého státu a pomocí družice je směrován zpět k zemi. Signál vyslaný ze satelitu většinou pokrývá území více než jednoho státu. S tím souvisí právní problém podle práva jakého státu je třeba takové užití díla (v tomto případě vysílání díla televizí) a jeho následky posoudit. Jde snad jen o právo státu, odkud je signál vysílán k satelitu, nebo snad mohou přicházet v úvahu všechna jednotlivá autorská práva všech zemí, v nichž je signál přijímán? Na rozdíl od prvního příkladu je tato oblast výslovně upravena zákonnou normou.

Směrnice Rady ES 93/83 z 27. 9. 1993 o satelitním vysílání považuje ve většině případů za zemi, kde dochází k užití díla a jejíž autorský zákon se tedy musí aplikovat v souvislosti s tímto vysíláním, pouze ten stát, odkud dochází k vysílání signálu vzhůru vůči satelitu. Toto pravidlo ale není absolutní a existují z něj výjimky, které mají zabránit tomu, aby jako rozhodné bylo určeno právo, které neposkytuje dostatečnou autorskoprávní ochranu. Shodně se směrnicí tuto otázku upravuje i český autorský zákon[11].

Zpřístupňování díla prostřednictvím internetu lze považovat za formu užití díla, která má shodné znaky s oběma výše uvedenými příklady.

Data představující autorská díla jsou fyzicky umístěna na serverech, které jsou připojeny k internetu a jsou tak vlastně přístupná každému a odkudkoliv.

Konečný uživatel, který sedí dejme tomu doma u svého počítače a „surfuje" po internetu, požádá prostřednictvím svého počítače server, na němž jsou příslušná data umístěna, aby mu je zaslal. Server tak učiní, požadovaná data odešle. Poté se spojení přeruší a server na klientský počítač koncového uživatele „zapomene". Data doručená uživateli se zobrazí na jeho monitoru a na přechodnou dobu se uloží u něj do paměti. Uživatel je též může natrvalo uložit (stáhnout) na své zařízení.

V tomto procesu dochází ke dvěma základním způsobům užití díla. Na jedné straně jde o sdělování díla veřejnosti (v podobě zpřístupnění díla na internetovém serveru), na druhé pak o rozmnožování díla (v podobě jeho stažení do počítače koncového uživatele).

2.2 ZPŘÍSTUPŇOVÁNÍ DÍLA (SDĚLOVÁNÍ DÍLA VEŘEJNOSTI) PROSTŘEDNICTVÍM INTERNETU

2.2.1 Určení rozhodného práva

Jak bylo uvedeno, zpřístupní-li kdokoli určitá díla prostřednictvím internetu, neučiní nic jiného, než že nahraje na disk serveru data, která dané dílo reprezentují.

---

[11] Viz § 21 autorského zákona:
(5) Vysílání díla pomocí družice se uskutečňuje na území toho členského státu Evropských společenství nebo jiné smluvní strany Dohody o Evropském hospodářském prostoru, kde jsou signály nesoucí zvuky nebo obrazy a zvuky nebo jejich vyjádření určené k příjmu veřejností uvedeny pod vedením vysílatele a na jeho odpovědnost na nepřerušený sdělovací řetěz směrem na družici a od ní zpět k zemi.
(6) Pokud se vysílání pomocí družice uskutečňuje na území takového státu, který neposkytuje úroveň ochrany autorského práva alespoň srovnatelnou s ochranou podle tohoto zákona, považuje se vysílání pomocí družice za uskutečněné na území toho členského státu Evropských společenství nebo jiné smluvní strany Dohody o Evropském hospodářském prostoru, kde
a) je umístěna stanice, ze které jsou signály nesoucí zvuky nebo obrazy a zvuky nebo jejich vyjádření určené k příjmu veřejností přenášeny na družici, nebo
b) je usazen vysílatel, jestliže nejsou dány skutečnosti uvedené v písmenu a).
Právo k vysílání pomocí družice lze uplatnit vůči osobě, která provozuje stanici podle písmene a), nebo vůči vysílateli podle písmene b).
(7) Pokud jsou signály nesoucí zvuky nebo obrazy a zvuky nebo jejich vyjádření určené k příjmu veřejností uvedeny na sdělovací řetěz směrem na družici a od ní zpět k zemi na území takového státu, který neposkytuje úroveň ochrany autorského práva alespoň srovnatelnou s ochranou podle tohoto zákona, a zároveň stanice, ze které je přenos uskutečňován, není na území jiného členského státu Evropských společenství, vysílání díla pomocí družice se považuje za uskutečněné na území takového členského státu Evropských společenství, kde má umístěny své řídící orgány vysílatel, na jehož podnět se vysílání uskutečňuje. Práva podle tohoto zákona lze pak uplatnit vůči takovému vysílateli.

Protože každý, kdo má k tomu potřebné technické vybavení, může takové dílo shlédnout, poslechnout si ho či jinak jej vnímat, anebo si vytvořit jeho trvalou rozmnoženinu tím, že si toto dílo stáhne a uloží na svůj disk, je nutno posuzovat zpřístupnění tohoto díla na internetu za akt užití díla.

Podle platného českého autorského zákona jde o „sdělování díla veřejnosti" podle § 18 odst. 1 a 2 zákona 121/200 Sb, ve znění pozdějších předpisů (autorský zákon), „**AutZ**". Zároveň dochází stejným jednáním v jednočinném souběhu i k rozmnožení tohoto díla podle § 13 AutZ.

Protože bylo dané dílo zpřístupněno uložením na disku konkrétního serveru umístěného v konkrétním státě, domnívám se, že v souladu s principem teritoriality, je možné tento akt užití (sdělování díla veřejnosti) posuzovat podle **práva státu, kde je tento server fyzicky umístěn**. K užití díla došlo nahráním dat na konkrétní webový server, prostřednictvím kterého je zpřístupněno veřejnosti způsobem, že kdokoli může mít k němu přístup na místě a v čase podle své vlastní volby. Webový server je vlastně „jevištěm" z našeho přirovnání k přeshraničnímu divadlu.

Osobně se však domnívám, že nelze ani vyloučit aplikaci práva těch zemí, **ze kterých je k takovému dílu umožněn přístup**. To ve svém důsledku znamená, že v případě internetu, jakožto celosvětové sítě (pokud není přístup určitým způsobem omezen), je přípustné za rozhodné právo považovat právo jakéhokoli státu světa. Celý svět se tak stává „hledištěm".

Jsem přesvědčen, že oba výše uvedené přístupy jsou v souladu s principem teritoriality, tak jak je stanoveno v čl. 5 odst. 2 Bernské úmluvy a shodně pak v čl. 8 odst. 1 Nařízení. Přesto je vhodné se nad nimi kriticky zamyslet.

2. 2. 2 Výhody a nedostatky popsaných způsobů určení rozhodného práva

Základním nedostatkem tohoto principu je problém s takzvanými „copyright havens[12]". Po vzoru daňových rájů by na servery umístěné v zemích s žádnou nebo jen minimální autorskou ochranou mohli piráti umístit autorskoprávně chráněná data a zpřístupnit je bez rizika právního postihu v podstatě komukoli na světě. Právě nedostatečná ochrana autorských práv v určitých jurisdikcích je hlavním argumentem odpůrců toho, aby se právní odpovědnost vyplývající ze zpřístupnění díla prostřednictvím internetu posuzovala výhradně podle práva státu, kde je fyzicky umístěn server s daty představující dílo.

K tomu přistupuje další argument, a sice že tuto metodu určení rozhodného práva lze použít pouze v těch případech, kdy je celé dílo zpřístupněno pouze na jednom serveru, to jest centralizovaným způsobem. Takový způsob zpřístupnění dat však není využíván v rámci peer to peer sítí typu BitTorrent[13] nebo sítí s distribuovaným ukládáním typu FreeNet[14]. V těchto systémech buď není prakticky možné určit, na jakém

[12] Nejde o oficiální právní pojem, nicméně je často používán. Jde o odvozeninu z anglického výrazu pro daňové ráje (tax haven – doslova „daňové útočiště").

[13] BitTorrent je peer-to-peer nástroj pro distribuci souborů. Při distribuci pomocí BitTorrentu jsou soubory rozděleny na menší bloky. Každý uživatel může požádat kteréhokoli jiného uživatele o chybějící blok, a zároveň poskytuje ostatním svoje již kompletně stáhnuté bloky (zdroj: Wikipedia.org).

[14] Soubory nejsou uloženy na konkrétním serveru, nýbrž do logického prostoru, tvořeného vyhrazeným místem na discích všech účastníků služby dohromady. Soubory nejsou identifikovány umístěním (např.

fyzickém serveru se data nacházejí, anebo se data představující dílo nacházejí v rozdrobené podobě na více místech (serverech) po celé síti[15], případně obojí. Vzhledem k těmto specifikům v zásadě nelze určit, kde se nachází server s daty, které dílo představují, a v důsledku toho není možné akt užití takového díla posuzovat podle práva státu, kde je takový server fyzicky umístěn.

Výše uvedené nedostatky se neprojeví v případě posouzení užití díla podle práva státu či států, ze kterých je k takovému dílu umožněn přístup. Nespornou nevýhodou takového způsobu stanovení rozhodného práva je však nejednoznačnost, jaké právo lze aplikovat, a z toho plynoucí právní nejistota. Pokud bychom připustili aplikaci práva všech států, odkud je možné na server přistoupit (což by fakticky představovalo možnost aplikace práva všech států světa, neboť internet je dosažitelný odkudkoli), mohlo by to vést k nežádoucímu jevu zvanému *forum shopping*.

Forum (nebo též *court*) *shopping* představuje nežádoucí jednání žalujícího, který na základě posouzení svých šancí podá žalobu v tom státě, jehož autorské právo mu dává nejlepší naději na úspěch ve věci. Soud pak aplikuje své vlastní hmotné právo (protože i z tohoto státu je dílo přístupné a tudíž i v tomto státu bylo dílo užito) a podle něj rozhodne.

Domnívám se, že přestože oba výše popsané přístupy k určení rozhodného práva, podle kterého se posoudí užití díla jeho zpřístupněním na internetu, mají své nesporné nedostatky, zájem na zaručení dostatečné míry autorskoprávní ochrany v kybeprostoru by měl převážit nad právní nejistotou a negativními důsledky *forum shopping*.

Uživatel, který se rozhodne zpřístupnit jakékoli autorské dílo prostřednictvím internetu, si musí být plně vědom celosvětového dosahu tohoto media, a proto je jistě srozuměn s tím, že jeho jednání může mít dopad i v zahraničí. Nelze pak ochranu proti takovému jednání striktně omezit jen na jeden právní řád. Teoreticky by měl takový uživatel počítat s tím, že jeho jednání může být posouzeno podle právní úpravy jakéhokoli státu, v němž je možné zpřístupněné dílo vnímat.

Praktické problémy s tím spojené pro osobu, která dílo zpřístupňuje, jsou menší v důsledku toho, že rozsah autorskoprávní ochrany se v oblasti zpřístupňování děl v jednotlivých státech v zásadě neliší. Proto by se nemělo stát, že zatímco domovské právo by takové její jednání povolovalo, právo jiné země by jej zakazovalo.

2.3 WEBCASTING

Webcastingem se rozumí tzv. „real time streaming" dat, tedy zpřístupňování určitého programu prostřednictvím sítě internet v reálném čase. Z pohledu posluchače je webcasting obdobou rozhlasového (případně i televizního) vysílání, neboť se

---

soubor xxx.mp3 na serveru s IP adresou 111.222.33.44, který má doménu www.music.com) jako u tradičního zpřístupňování souborů na Internetu prostřednictvím serverů, ale pouze názvem v adresovém prostoru celé sítě (např. hudba/xxx.mp3). Soubory se v síti kopírují a přesouvají automaticky podle toho, na kterém místě jsou data nejvíce požadována. Uživatel, který poskytne do sítě svá data, ztrácí kontrolu nad jejich umístěním.

[15] Teprve po pospojování všech jednotlivých částí dat (datových bloků) je možné dílo, které tato data představují, vnímat.

jedná o určitý „tok" zpravidla zvuků a obrazů, ve kterém příjemce nemůže sám přímo interaktivně volit sled prvků s tím, že pro všechny příjemce je v jednom okamžiku vždy program stejný. Tok dat (streaming) je technicky zabezpečen způsobem, že je nelze ukládat a pořizovat si tak rozmnoženinu díla, které je „vysíláno".[16] Webcasting tudíž svou povahou a způsobem konzumace vysílaného díla příjemcem v podstatě odpovídá klasickému televiznímu nebo rozhlasovému vysílání.

Webcasting je proto třeba ze své povahy odlišovat od zpřístupňování díla formou „vystavování" na webové stránce, tedy od „statického" zpřístupnění, tak jak je popsáno výše. Rozhodující zde není ani tak odlišný technický postup užití díla při webcastingu, ale důsledky pro uživatele (konzumenty díla).

Přestože lze na první pohled webcasting přirovnat spíše ke kabelovému televiznímu vysílání či vysílání „rozhlasu po drátě", než k tradičnímu zpřístupňování díla prostřednictvím webové stránky, kdy lze dílo „stáhnout" a uložit v počítači koncového uživatele, nemění to podle mého názoru nic na výše uvedeném. Dílo, které je v rámci webcastingu streamováno, je tak zpřístupňováno všem, kteří se k serveru, jenž datový rok zajišťuje, schopni připojit. Proto je dle mého názoru za rozhodné právo, podle kterého bude takový způsob užití díla posuzován, možné považovat právo všech zemí, ze kterých je webcasting díla dostupný.

2.4 STAHOVÁNÍ (ROZMNOŽOVÁNÍ) AUTORSKÝCH DĚL Z INTERNETU

Odlišným způsobem užití autorského díla od jeho zpřístupnění je stažení (rozmnožení) dat toto dílo představující z internetu. Stažením a následným uložením díla na disk dojde k vytvoření kopie (rozmnoženiny) díla, a to z vůle uživatele.

Určení rozhodného práva u tohoto způsobu užití díla je velmi důležité, neboť narozdíl od zpřístupňování díla prostřednictvím internetu, které, jak jsem již uvedl, snad bez výjimky a bez ohledu na rozhodné právo podléhá souhlasu autora či jiného nositele práv, v případě vytvoření rozmnoženiny koncovým uživatelem tomu tak vždy nemusí být. Panují významné rozdíly mezi tím, jak takové jednání posuzují autorskoprávní úpravy různých zemí. Některé jurisdikce stažení díla bez souhlasu autora pro osobní potřebu uživatele za určitých podmínek povolují, jiné nikoliv.

Například české právo považuje zhotovování rozmnoženiny čistě pro svou osobní potřebu za tzv. „volné užití díla", které nepodléhá souhlasu autora (§ 30 AutZ). Jde o značně širokou výjimku z práva autora rozhodovat o užití svého díla, z níž jsou vyjmuty pouze počítačové programy, elektronické databáze a užití architektonického díla stavbou (takové užití však není v prostředí internetu stejně možné). Přestože tento způsob volného užití podléhá určitým dalším omezením[17], je možné zobecnit, že podle českého práva většina případů stahování děl z internetu bez souhlasu autora není porušením autorského práva.

---

[16] Samozřejmě však existují programy, které ukládání streamovaných dat umožňují.

[17] Zejména musí vyhovět obecným ustanovením, která se vztahují k výjimkám a omezením autorského práva, jak je stanoveno v § 29AutZ.

Oproti tomu například anglické právo je v tomto ohledu velmi restriktivní a takto širokou výjimku z práv autora vůbec nezná.[18] Proto jednání spočívající ve stažení díla, které by podle českého práva vůbec nebylo zásahem do autorových práv, by pravděpodobně neoprávněným užitím díla podle práva anglického bylo. Z výše uvedených důvodů je tedy velmi významné, jaké právo bude rozhodné pro posouzení odpovědnosti vyplývající z takového užití díla.

Vzhledem k tomu, že rozmnoženina díla vznikne v místě, kde je umístěn počítač koncového uživatele, je podle mého názoru rozumné považovat **za rozhodné právo toho státu, kde se nalézá počítač koncového uživatele, v němž k rozmnožení díla dochází.**

Jsem přesvědčen, že tento způsob určení díla nejlépe odpovídá principu teritoriality stanoveném v čl. 5 odst. 2 RÚB a shodně čl. 8 odst. 1 Nařízení.

Výhodou této metody je i to, že každý koncový uživatel je sám schopen určit takové rozhodné právo a je pro něj přirozené, že se v naprosté většině případů uplatní právo státu, kde se nachází.

V případě dálkového přístupu k takovému počítači je však nejasné, zda je okruh rozhodného práva možné rozšířit i na právo státu, kde se nachází uživatel, který dílo rozmnožil.

Jak by například bylo posouzeno jednání, kdy uživatel fyzicky se nalézající v Anglii pomocí dálkové přístupu ukládá soubory stažené z internetu na svůj počítač fyzicky umístěný v České republice. Jde spíše o situaci hypotetickou, ale možnou, neboť možností, jak spravovat počítač na dálku je celá řada. Přestože k rozmnožení díla dojde v takovém případě pouze na počítači v Česku (kam jsou přímo stahována data z internetu), nelze zcela odmítnout názor, že je rozhodující i místo, kde uživatel, který dílo rozmnožil, byl přítomen, i když se samotná rozmnoženina nachází ve zcela jiném státě. Domnívám se, že ani takový přístup není v rozporu s právní úpravou zakotvenou v Bernské úmluvě a Nařízení.

3. ZÁVĚR

Odpovědnost z porušení autorských práv je třeba posuzovat podle práva státu, kde k aktu zneužití autorského díla došlo, a to v souladu s principem teritoriality stanoveném v čl. 5 odst. 2 RÚB a čl. 8 odst. 2 Nařízení.

Podle takto určeného práva je třeba posoudit, zda jde či nejde o chráněné autorské dílo, jaký je rozsah autorských práv, která se k němu váží, jaké jsou výjimky z těchto práv a jak dlouho ochrana díla trvá. Podle práva země původu autorského díla je třeba určit původního nositele práv (autora).

V případě zpřístupnění díla prostřednictvím internetu (sdělování díla veřejnosti) je podle mého názoru třeba za rozhodné považovat právo států, ze kterých je k takovému

[18] Viz Copyright, Designs and Patents Act 1988, Chapter III, Acts Permitted in Relation to Copyright Works.

dílu umožněn přístup, neboť ve všech těchto jurisdikcích dochází ke zpřístupnění díla. A to i v případě, že tímto způsobem bude možné za rozhodné považovat více právních řádů.

V případě stahování dat z internetu (rozmnožování díla) pak je rozhodné právo toho státu, kde je umístěn počítač koncového uživatele, ve kterém k rozmnožení díla dochází, případně kde se nachází koncový uživatel, který rozmnožení díla provedl.

LAW APPLICABLE TO NON-CONTRACTUAL OBLIGATIONS ARISING FROM USE OF COPYRIGHTED WORKS IN THE CYBERSPACE

Summary

The Article deals with applicability of the principle of territoriality, as introduced in the Berne Convention for the Protection of Literary and Artistic Works and new Regulation (EC) No 864/2007 on law applicable to non-contractual obligations (Rome II) to obligations arising from an infringement of copyright.

The recognized principle of lex loci protectionis, meaning the law of the country in which protection is claimed (on which e.g. the Bern Convention and Regulation Rome II are built), stipulates that the state shall apply its own law to an infringement of copyright infringement that is in force in its territory. This rule, also known as the "territoriality principle," requests that the courts apply the law of the country where the violation (copyright infringement) was committed. This solution confirms that the rights held in each country are independent.

The key issue, however, is how the principle of territoriality shall be applied to copyright infringements committed through the Internet.

An author of the article concludes that as a general rule, the principle of territoriality should be interpreted in a way that a copyright holder who complains that his work has been exploited without regard for his rights will be entitled to the protection given him by the copyright law in the country where the alleged infringement was committed.

In particular, in case of communication of copyrighted works to the public over the Internet, laws of all countries from which such disseminated work can be accessed may be applied in addition to the copyright laws of the jurisdiction where a server (on which the infringing content is stored) is located.

In case of downloading from the Internet, such act should be governed by copyright laws of a jurisdiction in which an end user (who initiates such download) or such end user's computer is located.

Key words: Internet, copyright, infringement, choice of law, governing law, conflict of laws, Regulation Rome II, Berne Convention, principle of territoriality, tort, liability

Klíčová slova: internet, autorské právo, neoprávněný zásah do práv, volba práva, rozhodné právo, určení rozhodného práva, nařízení Řím II, Bernská úmluva, princip teritoriality, delikt, odpovědnost

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

2008 ACTA UNIVERSITATIS CAROLINAE – IURIDICA 4 PAG. 35–49

EXTREMISMUS A HRANICE SVOBODY PROJEVU NA INTERNETU

JIŘÍ HERCZEG
Katedra trestního práva Právnické fakulty Univerzity Karlovy v Praze

1. ÚVOD

Ekonomická, sociální a kulturní globalizace spolu s krizí národního státu probouzí tendence, které odmítají demokracii, liberalismus i právní stát. Pod pojmem **extremismus** jsou zahrnovány aktivity se zpravidla ideologickou motivací, které vybočují ze zákonných norem, vyznačují se prvky netolerance a útočí proti demokratickým principům a společenskému uspořádání.[1] Extremismus je tak dítětem demokracie. Jistě ne jediným a určitě nechtěným, nicméně velmi skutečným.

Definice tohoto pojmu se liší podle toho, zda se pohybujeme v rovině sociologické, politologické, kriminologické či právní. Zřejmě nejobecnější definice extremismu říká, že extremismus je souhrnem určitých sociálně patologických jevů vytvářených více či méně organizovanými skupinami osob (extremistů).[2]

Pro potřeby policie je extremismus definován jako *verbální, grafické, fyzické a jiné aktivity spojené zpravidla s vyhraněným ideologickým nebo jiným kontextem, které vyvíjejí jednotlivci nebo skupiny osob s názory výrazně vybočujícími z všeobecně uznávaných společenských norem se zřetelnými prvky netolerance, zejména rasové, národnostní, náboženské nebo jiné obdobné nesnášenlivosti, a které útočí proti demokratickým principům, společenskému uspořádání, životu, zdraví, majetku nebo veřejnému pořádku.*[3]

Od extremismu je třeba odlišovat **kriminalitu s extremistickým podtextem,** kterou se rozumí protiprávní jednání páchané v souvislosti s extremismem, působením sekt nebo diváckým násilím, které naplňuje znaky skutkové podstaty trestného činu nebo přestupku.

Na definici a vymezení extremismu jsou mezi odbornou veřejností protichůdné názory, a to zejména z důvodu nejednoznačnosti jeho významu.[4] Často bývá složité ur-

[1] Informace o problematice extremismu na území ČR v roce 2002. Ministerstvo vnitra 2003.
[2] Marešová, A. a kol. Kriminologické a právní aspekty extremismu. Praha: IKSP, 1999, str. 114.
[3] Závazný pokyn policejního prezidenta ze dne 6. června 2002, č. 100/2002, kterým se upravuje činnost příslušníků Policie České republiky na úseku boje proti extremistické kriminalitě.
[4] Chmelík, J. Extremismus a jeho právní a sociologické aspekty. 1.vydání. Praha: Linde, 2001, str. 11.

čit, kdo je extremistou a kdo pouze radikálem, který se pohybuje ještě v rámci daného ústavního systému. Absence legálního vymezení tohoto pojmu je tak vnímána jako nedostatek platné právní úpravy, a proto například ústavněprávní výbor slovenského parlamentu navrhl v rámci připomínek k novému trestnímu zákonu zavést do trestního zákona legální definici pojmu *extremismus, extremista* a *extremistické skupina*.[5] Pojem extremismu je navrhován stejně jako ve výše uvedeném pokynu policejního prezidenta.[6]

Extremistou se rozumí osoba, která je vyznačuje zejména

a) odmítáním všeobecně závazných právních předpisů a vysokou mírou názorové, rasové nebo etnické nesnášenlivosti;

b) absencí hmotné pohnutky a motivací protiprávního jednání s prvky agresivity a brutality;

c) agresivním chováním projevujícím se fyzickými aktivitami v souvislosti s konáním společenských akcí, které směřují ke způsobení fyzické újmy osobám, škodám na majetku, nebo které jsou způsobilé narušit veřejný pořádek.

Extrémistickou skupinou se podle návrhu rozumí společenství nejméně tří osob, které splňují znaky extremisty a které se vyznačuje dělbou úkolů mezi jednotlivými členy skupiny, jejich plánováním a koordinovaností. Dle důvodové zprávy by následně bylo možno zavést extremismus a příslušnost k extremistické skupině jako pohnutku a znak kvalifikované skutkové podstaty zvyšující společenskou nebezpečnost, a tím i trestní sazbu u jednotlivých skutkových podstat.[7] Tento návrh nakonec nebyl přijat.

Extremismus obvykle používá tyto instrumenty: historický revizionismus, sociální demagogii, aktivismus, podporu verbálního až fyzického násilí vůči oponentům a vůči apriori definovaným sociálním skupinám a konspirativní teorii.

V politologické literatuře se obvykle rozlišuje extremismus pravicový a levicový, dále náboženský, ekologický a národnostní (regionalistický) extremismus. Poslední tři formy extremismu se v České republice vyskytují jen ojediněle nebo vůbec.[8] Novým fenoménem je **ekologický extremismus** *(enviromentalismus)*, který se projevuje v činnosti některých militantně orientovaných ekologických organizací a sdružení.

---

[5] Společná zpráva výborů Národní Rady SR k vládnímu návrhu trestního zákona ze dne 13. 1. 2005, tisk 656a.

[6] „Extrémizmom sa rozumejú verbálne, grafické, fyzické alebo iné aktivity spojené spravidla s vyhradeným ideologickým alebo iným kontextom, zväčša s absenciou hmotnej pohnútky, ktoré vyvíjajú jednotlivci alebo skupiny osôb s názormi výrazne vybočujúcimi zo všeobecne uznávaných spoločenských noriem so zreteľnými prvkami netolerancie, najmä rasovej, národnostnej, náboženskej alebo inej obdobnej neznášanlivosti, ktoré útočia proti demokratickým princípom, spoločenskému usporiadaniu, životu, zdraviu, majetku alebo verejnému poriadku".

[7] Z důvodové zprávy: *„Trestné činy spáchané členy extremistických skupin se vzhledem na vysoký stupeň organizovanosti, plánovitosti a častého používání zbraní svým charakterem a společenskou nebezpečností podobají trestným činů páchaným organizovanými zločineckými skupinami. Rozdíl oproti těmto skupinám však spočívá v motivu páchání skutků, kterým je v případě extremistických skupin ideologie rasizmu, nacizmu a xenofobie. Když tyto pojmy nejsou v trestním zákoně, vymožitelnost práva při spáchání trestného činu s extremistickým prvkem je minimální, když orgány činné v trestním řízení se odvolávají na to, že v trestním zákoně nejsou, a proto často takovému trestnému činu nepřipisují takovou důležitost. Současné znění trestního zákona však neumožňuje zohlednit vyšší společenskou nebezpečnost trestných činů páchaných příslušníky extrémistických skupin. Vzhledem k výše uvedeným nedostatkům současné právní úpravy navrhujeme doplnění trestního zákona o definici pojmů extremizmus, extremista a extremistická skupina."*

[8] Informace o problematice extremismu na území ČR v roce 2006. Ministerstvo vnitra 2007.

V rámci proklamovaného cíle – ochrana životních prostředí – tyto skupiny striktně odmítají např. využití atomové energie (což je cíl obecně pozitivní), nicméně volené prostředky jsou často neadekvátní a mohou působit na společnost destruktivně. Jde zejména o tzv. „procesní terorismus", mezi jehož metody lze zařadit i nepřímé využívání výpočetní a telekomunikační techniky pro přetěžování vytvořených demokratických mechanismů (soudy, správní orgány).

Pravicoví extremisté používající v prvé řadě nacionální, rasovou, etnickou zášť a sympatizují s historickým fašismem a nacismem. Základním myšlenkovým východiskem pravicového extremismu je *rasismus* projevující se jako přesvědčení o biologické výjimečnosti a nadřazenosti bílého etnika. Bílá rasa stojí podle stoupenců těchto myšlenek na vrcholu vývoje druhů a jejími vůdčími představiteli jsou árijci, jejichž předchůdci byli Germáni. Argumentem jsou rasově – antropologické teorie poloviny 19. století (Gobineau, Chamberlein), z nichž čerpali ideologové Třetí říše. Největším zločinem je pak míšení bílé rasy s ostatními. Rasisté hovoří o vypuknutí rasové svaté války či bílé revoluce, jako rozhodujícího zápasu bílé rasy o přežití. Odrazem přesvědčení o nerovnosti ras je otevřené pohrdání a nepřátelství vůči lidem jiné barvy pleti.

Levicové extremistické skupiny jsou motivované především záští sociální a třídní. Sympatizují s historickým komunismem nebo anarchismem. Například Spolkový úřad na ochranu Ústavy definoval levicové extremisty jako odpůrce státního a společenského upořádání v SRN, kteří v závislosti na ideologické orientaci – revolučně-marxistická nebo anarchistická – chtějí v Německu zavést socialisticko/komunistický režim nebo společnost (anarchii).[9] Příznivci levicového extremismu se pokoušejí o vytvoření společnosti, v níž by panovala naprostá rovnost. Realizace této představy předpokládá zrušení všech existujících států, likvidaci hierarchického uspořádání společnosti a odstranění jakékoli nerovnosti, včetně ekonomických rozdílů.[10]

2. ZNEUŽÍVÁNÍ INTERNETU

S rozmachem moderních komunikačních technologií je internet místem, kde dochází ve stále větší míře k šíření nenávistné propagandy.[11] Internet je používán jak pravicově, tak levicově zaměřenými extremistickými skupinami, ale i tzv. nebezpečnými sektami, k informačním a agitačním aktivitám, případně k náboru nových členů.

Možnost zveřejňovat programová prohlášení i aktuální informace prostřednictvím veřejné počítačové sítě skýtá následující výhody:

---

[9] Zpráva Spolkového úřadu pro ochranu ústavy (Bundesamt für Verfassungsschutz) za rok 2003.

[10] Chmelík, J. Symbolika extremistických hnutí. 1. vydání. Praha: Trevis, 2000, str. 9.

[11] **Internet** je celosvětová počítačová síť, která spojuje jednotlivé menší sítě pomocí sady protokolů IP. Název pochází z anglického slova *network* (síť), podle něhož tradičně názvy amerických počítačových sítí končily „-net", a mezinárodní (původně latinské) předpony **inter-** (mezi), vyjadřující, že internet propojil a vstřebal různé starší, dílčí, specializované, proprietární nebo lokální sítě. Internet slouží k přenášení informací a poskytování mnoha služeb, jako jsou elektronická pošta, chat, www stránky, sdílení souborů, on-line hraní her, vyhledávání, katalog a další. **World Wide Web** je informační systém pro práci s hypertextovými dokumenty, ve kterých jsou odkazy na internetovské zdroje uváděny pomocí adresy. http://www.wikipedia.cz.

– *globální dosah sítě umožňuje, že informace, které o sobě extremisté zveřejní, jsou celosvětově dostupné za zlomek nákladů nutných k šíření informací jiným způsobem,*
– *informace jsou v některých případech prezentovány mimo právní jurisdikci vlastní země,*
– *identifikace autora je velmi obtížná.*

Internet je médium, prostřednictvím kterého probíhá konkrétní emailová komunikace mezi příslušníky a stoupenci extremistických organizací. Veřejnou počítačovou sítí lze velmi rychle předat informace širokému okruhu adresátů. Na webových stránkách bývají umístěny letáky, pozvánky na srazy, demonstrace a koncerty takových organizací. Prostředí internetu je také vhodné pro tvorbu webových stránek, které prezentují ilegální extremistické organizace.

Rasistické a jiné nenávistné webové stránky, které jsou česky psané a veřejně přístupné, jsou nejčastěji umísťovány na servery internetových poskytovatelů v USA, kde je jiné právní prostředí, a propagace a další šíření rasových nebo jiných nenávistných projevů zde není trestné. V případě, že jde o stránku registrovanou na americkém serveru, USA žádosti o právní pomoc zpravidla odmítají, protože jejich první dodatek Ústavy (svoboda projevu) jim nedovolí donutit tvůrce této stránky, aby vydal jakékoli údaje. Tím je faktická dána nemožnost uskutečnit společné odhalování pachatelů takových činů s americkou stranou.[12]

Rovněž je třeba zmínit internetová diskusní fóra, která jsou často zneužívána k šíření rasistické a xenofobní propagandy. V této souvislosti je často diskutována odpovědnost

(i) poskytovatelů volného prostoru pro uložení elektronických dat (webhosting),
(ii) poskytovatelů internetového připojení a
(iii) *provozovatelů webových diskusních fór,* za obsah přenášených, sdílených nebo ukládaných informací.

Odpovědnost poskytovatele služby za obsah přenášených a ukládaných informací je upravena zákonem č. 480/2004 Sb., o některých službách informační společnosti.

A) **Přenos informací**: poskytovatel služby, jež spočívá v přenosu informací poskytnutých uživatelem prostřednictvím sítí elektronických komunikací nebo ve zprostředkování přístupu k sítím elektronických komunikací za účelem přenosu informací, odpovídá za obsah přenášených informací, jen pokud

a) přenos sám iniciuje,
b) zvolí uživatele přenášené informace, nebo
c) zvolí nebo změní obsah přenášené informace.

B) **Ukládání informací**: poskytovatel služby, jež spočívá v ukládání informací poskytnutých uživatelem, odpovídá za obsah informací uložených na žádost uživatele, jen

a) mohl-li vzhledem k předmětu své činnosti a okolnostem a povaze případu vědět, že obsah ukládaných informací nebo jednání uživatele jsou protiprávní, nebo

[12] V souvislosti se vzestupem veřejného publikování antisemitismu a revizionizmu na internetu je třeba zmínit česky psanou webovou stránku „Národně vzdělávací institut – NVI"), kde jsou publikovány rasistické, antisemitské, revizionistické a další nenávistné texty. Hostování webových stránek je umístěno na serveru bluehost.com v USA. V tomto případě se nejedná o organizaci, ale činnost několika jedinců, tedy malé virtuální skupiny, zaměřené na propagaci výše zmíněných názorů. Informace o problematice extremismu na území ČR v roce 2006. Ministerstvo vnitra 2007.

b) dozvěděl-li se prokazatelně o protiprávní povaze obsahu ukládaných informací nebo o protiprávním jednání uživatele a neprodleně neučinil veškeré kroky, které lze po něm požadovat, k odstranění nebo znepřístupnění takovýchto informací.

Tak v roce 2006 byli obviněni dva pachatelé pro trestné činy: hanobení národa, etnické skupiny, rasy a přesvědčení podle § 198 odst. 1 písm. a) TZ, podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod podle § 198a odst. 1 TZ, podpora a z propagace hnutí směřujících k potlačení práv a svobod člověka podle § 260 odst. 1, 2 písm. a) TZ a § 261a TZ, kterých se měli dopustit tím, že

- *nejméně od listopadu 2003 do prosince roku 2004 jako šéfredaktor a prozatímní šéfredaktor internetového časopisu „POSLEDNÍ GENERACE" zajišťovali organizačně i jako autoři textů jeho přípravu, výrobu a distribuci, respektive jeho umístění na výše uvedených světově veřejně přístupných webových stránkách, kdy písemný a obrazový záznam tohoto časopisu podporoval a propagoval hnutí směřující k potlačení práv a svobod člověka a hlásal národnostní, rasovou, náboženskou či třídní zášť nebo zášť vůči jiné skupině osob, respektive veřejně projevoval sympatie k těmto hnutím a zároveň veřejně hanobil národ, etnickou skupinu, rasu a přesvědčení a veřejně podněcoval k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod, respektive veřejně popíral, zpochybňoval, schvaloval nebo se snažil ospravedlnit nacistické genocidium nebo jiné zločiny nacistů proti lidskosti.*

Samostatným problémem je elektronická pošta (E-mail), která prostřednictvím tzv. anonymizérů umožňuje cílené zasílání zpráv bez možnosti zvenčí identifikovat odesílatele. Elektronická pošta, ve spojení s moderními volně dostupnými šifrovacími metodami, umožňuje extremistům činnost, kterou nemohou státní orgány monitorovat.

Policie zpravidla nebude mít doznání pachatele, že je autorem těchto stránek, a proto v takovém případě bude důkazním prostředkem nezbytným ke zjištění skutkového stavu a tím i osoby pachatele zpravidla znalecký posudek z oboru výpočetní techniky. Znalec by měl provést zkoumání zajištěných internetových stránek s cílem získat údaje směřující k identifikaci provozovatele stránek i k identifikaci osoby, která uvedené stránky zřídila a která sporný text na tyto stránky umístila.[13] Orgány činné v trestním řízení se přitom často dostávají do důkazní nouze jednak proto, že tyto stránky jsou znalci mnohdy předkládány v podobě tištěných kopií, kde jsou zcela ztracena důležitá megadata, a jednak proto, že digitální důkaz je stále ještě vnímán jako nespolehlivý důkazní prostředek.

3. INSTITUCIONÁLNÍ ZAJIŠTĚNÍ POSTIHU EXTREMISMU NA INTERNETU

A. **Policie České republiky.** Na plnění úkolů policie na úseku extremistické kriminality se podílejí

a) příslušníci policie v rozsahu stanoveném trestním řádem a zákonem o policii, a
b) policisté služby kriminální policie a vyšetřování, kteří jsou *pověřeni* vedoucím služebním funkcionářem k plnění úkolů na problematice extremistické kriminality a jsou *zařazeni* na

[13] Rozsudek Nejvyššího soudu ze dne 16. 1. 2001, sp. zn. 4 Tz 265/2000, ASPI.

1. odděleních obecné kriminality služby kriminální policie a vyšetřování Policie České republiky, okresních (obvodních) ředitelstvích a odborech obecné kriminality služby kriminální policie a vyšetřování Policie České republiky městských ředitelství v Plzni, Brně a Ostravě *(odborné pracoviště okresu)*,
2. odborech obecné kriminality služby kriminální policie a vyšetřování Policie České republiky správ krajů a odboru pro boj s organizovaným zločinem služby kriminální policie a vyšetřování Policie České republiky správy hl. m. Prahy *(odborné pracoviště kraje)*,
3. skupině odhalování extremistické kriminality odboru obecné kriminality úřadu služby kriminální policie a vyšetřování Policejního prezidia České republiky *(odborné pracoviště úřadu)*,
4. oddělení extremismu odboru extremismu a terorismu Policie České republiky útvaru pro odhalování organizovaného zločinu služby kriminální policie a vyšetřování *(oddělení extremismu útvaru)*.[14]

Počátkem roku 2006 se uskutečnila reorganizace Úřadu služby kriminální policie a vyšetřování Policejního prezidia ČR (ÚSKPV PP ČR). V rámci této reorganizace byla ke dni 1. února 2006 problematika pravicového a levicového extremismu, včetně metodiky, plně převedena do působnosti odboru terorismu a extremismu Útvaru pro odhalování organizovaného zločinu (ÚOOZ) služby kriminální policie a vyšetřování Policie ČR, který se do té doby zabýval jen závažnou trestnou činností s extremistickým podtextem mající organizovaný charakter, anebo mající mezinárodní prvek.

Skupina informační kriminality úřadu služby kriminální policie a vyšetřování Policejního prezidia České republiky, jako servisní pracoviště,

a) vyhledává informace na síti internet vztahující se obecně k extremismu, působení sekt a diváckému násilí,

b) prověřuje informace a zjišťuje všechny související operativní údaje,

c) sleduje otevřené zdroje z hlediska možnosti zjištění podezření z páchání extremistické kriminality.

Oddělení strategické analýzy Policie České republiky útvaru pro odhalování organizovaného zločinu služby kriminální policie a vyšetřování, jako servisní pracoviště, vyhledává informace na síti internet vztahujících se k organizované extremistické kriminalitě.

B. **Státní zastupitelství** počátkem 90. let nevěnovalo extremistické trestné činnosti zvláštní pozornost. Změna nastala až po rasistické vraždě Roma Tibora Daniela v Písku v roce 1994. Vláda České republiky zařadila ve „Zprávě o bezpečnostní situaci na území ČR" rasové konflikty mezi bezpečnostní rizika a Nejvyšší státní zastupitelství na to reagovalo **pokynem obecné povahy** ze dne 15. května 1995, *kterým upravilo podrobnosti postupu státních zastupitelství při postihu trestných činů motivovaných národnostní a rasovou nesnášenlivostí, popřípadě zaměřených na jiné občany pro jejich politické přesvědčení nebo náboženské vyznání.*

[14] Závazný pokyn policejního prezidenta ze dne 6. června 2002, č. 100/2002, kterým se upravuje činnost příslušníků Policie České republiky na úseku boje proti extremistické kriminalitě.

Tento pokyn byl zrušen **pokynem obecné povahy** nejvyšší státní zástupkyně č. 4/2006 ze dne 30. srpna 2006, *o postihu trestných činů motivovaných národnostní, rasovou, politickou a náboženskou nesnášenlivostí*. Státní zastupitelství postupují podle tohoto pokynu v trestním řízení jak o trestných činech spáchaných z národnostních, rasových a jiných nenávistných pohnutek, kde pohnutka spočívající v rasové, národnostní, náboženské a jiné nenávisti nebo nesnášenlivosti je znakem skutkové podstaty, tak i v trestním řízení o jiných trestných činech, kde tato zjištěná pohnutka znakem skutkové podstaty trestného činu není.[15]

Vedoucí státní zástupci nebo státní zástupci jimi pověření pravidelně vyhodnocují situační zprávy Policie České republiky, informace ze sdělovacích prostředků i jiné podněty za účelem zjištění, zda nejde o určené trestné činy. Státní zastupitelství evidují poznatky o výskytu určených trestných činů, jejich příčinách a poznatky o rozhodování orgánů činných v trestním řízení o těchto trestných činech.

Státní zástupce při výkonu dozoru ve věcech, v nichž je vedeno trestní stíhání pro určené trestné činy, dbá především na důsledné a urychlené provedení všech vyšetřovacích úkonů ke zjištění pohnutek pachatele. Při dohledu věnují státní zastupitelství zvýšenou pozornost věcem, v nichž je vedeno trestní řízení pro určené trestné činy a zjišťují, zda byla věc odpovídajícím způsobem právně posouzena a byly provedeny všechny úkony nezbytné k objasnění pohnutky jednání pachatele.

4. MEZINÁRODNÍ SPOLUPRÁCE – DODATKOVÝ PROTOKOL K ÚMLUVĚ O POČÍTAČOVÉ KRIMINALITĚ

Přestože technologický rozvoj sbližuje lidi na celém světě, rasová diskriminace, xenofobie a další formy intolerance ve společnosti nadále setrvávají. Počítačové systémy nabízejí na jedné straně nebývalé prostředky k usnadnění svobody projevu a komunikace, na straně druhé však vývoj mezinárodních komunikačních sítí jako je internet umožňuje určitým osobám snadno rozšiřovat rasistické a xenofobní myšlenky.[16] K tomu, aby byly takové osoby vypátrány a postiženy, je nezbytná mezinárodní spolupráce.[17]

S přesvědčením o nutnosti harmonizovat důležitá zákonná opatření, týkající se boje proti rasistické a xenofobní propagandě, proto členské státy Rady Evropy dne 28. 1. 2003 přijaly Dodatkový protokol k Úmluvě o počítačové kriminalitě, týkající se kriminali-

[15] Trestnými činy, kde pohnutka spočívající v rasové, národnostní, náboženské a jiné nenávisti nebo nesnášenlivosti je znakem skutkové podstaty, jsou dle pokynu č. 4/2006 trestné činy: násilí proti skupině obyvatelů a proti jednotlivci podle § 196 TZ, hanobení národa, rasy a přesvědčení podle § 198 TZ, podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod podle § 198a TZ, vraždy podle § 219 odst. 1, 2 písm. g) TZ, ublížení na zdraví podle § 221 odst. 1, 2 písm. b) a § 222 odst. 1, 2 písm. b) TZ, vydírání podle § 235 odst. 1, 2 písm. f) TZ, poškozování cizí věci podle § 257 odst. 1, 2 písm. b) TZ a podpora a propagace hnutí směřujících k potlačení práv a svobod člověka podle § 260, § 261 a § 261a TZ.

[16] *Kunz, K.-L. Kriminologie. 4. Auflage. Bern: Haupt Verlag, 2004.*

[17] Bourney, E., Rose, G. Racist Offences: How is the Law Working? In: Home Office Research Study 244. London: Home Office 2002, str. 96–110.

zace činů rasistické a xenofobní povahy, spáchané prostřednictvím počítačových systémů (dále jen „Protokol").[18] Samotná Úmluva o počítačové kriminalitě žádné skutkové podstaty týkající se rasismu a xenofobie neobsahuje. Bylo tak učiněno z důvodu, že se předpokládala účast USA na Úmluvě (ratifikovaly 29. 9. 2006). Legislativa USA je totiž značně liberálnější, co se týče svobody projevu a hrozilo by, že USA Úmluvu neratifikují. Pro zjednodušení situace byl proto navržen Dodatkový protokol k Úmluvě. Česká republika Dodatkový protokol dosud nepodepsala, nicméně jedná se o jeden z nejvýznamnějších legislativních počinů na poli boje proti rasismu a xenofobii z poslední doby, a proto se jím budu zabývat podrobněji.[19]

Účelem tohoto Protokolu je harmonizace trestního práva hmotného v boji proti rasismu a xenofobii na internetu a zlepšování mezinárodní spolupráce v této oblasti. Protokol se zabývá především těmito otázkami:

1. *definice skutkových podstat a rozsah kriminalizace činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových sítí;*
2. *opatření ke spolupráci v oblasti trestního práva hmotného, procesního a mezinárodního.*

Protokol znamená rozšíření rozsahu Úmluvy o počítačové kriminalitě tak, aby bylo možno účinně postihnout rasistickou a xenofobní propagandu šířenou prostřednictvím počítačových sítí. Tudíž kromě harmonizace skutkových podstat trestných činů má Protokol za cíl i zlepšení metod mezinárodní spolupráce. Smluvní státy se zavázaly přijmout taková legislativní a další opatření, která mohou být nezbytná k tomu, aby následující jednání bylo označeno podle národního práva za trestný čin, pokud k němu dojde prostřednictvím počítačového systému, úmyslně a neprávem:

1. *šíření rasistických a xenofobních materiálů,*
2. *rasisticky a xenofobně motivovaná pohrůžka,*
3. *rasisticky a xenofobně motivovaná urážka,*
4. *popření, hrubé snižování, schvalování nebo ospravedlnění genocidy nebo zločinů proti lidskosti,*
5. *návod a pomoc k jednáním 1) až 4).*

Ad 1. Šíření rasistických a xenofobních materiálů.

Tento článek nařizuje zúčastněným státům, aby kriminalizovaly distribuci nebo jiné zpřístupnění rasistických a xenofobních materiálů veřejnosti prostřednictvím počítačového systému.[20]

„Distribucí" je míněno aktivní rozšiřování rasistického nebo xenofobního materiálu, zatímco *„zpřístupněním"* se míní umístění rasistických a xenofobních materiálů na

[18] Dodatkový protokol (ETS No. 189) k Úmluvě Rady Evropy o počítačové kriminalitě ze dne 28. 1. 2003.

[19] Česká republika Úmluvu o počítačové kriminalitě podepsala dne 9. února 2005. Tuto Úmluvu však, vzhledem k probíhajícím pracím na rekodifikaci trestního práva hmotného, do současné doby neratifikovala.

[20] Počítač se obecně chápe jako funkční jednotka, která může provádět výpočty všech číselných aritmetických operací a logických operací bez lidského zásahu. Definice *„počítačového systému"* je uvedena v Úmluvě o počítačové kriminalitě, na kterou Protokol odkazuje. Počítačový systém tedy znamená jakékoli zařízení nebo skupinu propojených souvisejících zařízení, z nichž jedno či více, provádí dle programu automatické zpracování dat.

internetu „on line" pro použití ostatními. Zpřístupněním se rozumí i vytváření nebo kompilace odkazů v hypertextovém dokumentu, aby se zjednodušil přístup k takovému materiálu. K rozšiřování musí dojít *veřejně*, což vylučuje postih soukromé komunikace (ochrana korespondence dle čl. 8 Úmluvy o lidských právech a základních svobodách). Zda je šíření rasistického nebo xenofobního materiálu považováno za soukromou komunikaci nebo za rozšiřování na veřejnosti, musí být určeno na základě okolností konkrétního případu. Co hraje primárně roli, je úmysl odesilatele, že předmětnou zprávu obdrží pouze konkrétní, předem určený příjemce. Existence takového úmyslu (subjektivní stránky) může být stanovena na základě řady objektivních faktorů, jako jsou obsah této zprávy, použitá technologie, bezpečnostní opatření a kontext, ve kterém je zpráva odeslána. Když jsou takové zprávy poslány ve stejnou dobu více než jednomu příjemci, počet příjemců a povaha vztahu mezi odesilatelem a příjemci/příjemcem je faktorem, který určuje zda je možné takovou komunikaci považovat za soukromou. Výměna rasistického a xenofobního materiálu v chatovacích místnostech, zasílání podobných zpráv v diskusních skupinách a fórech, jsou příkladem zpřístupňování takového materiálu veřejnosti. V těchto případech je takový materiál přístupný individuálně neurčenému počtu osob. Dokonce i když přístup k materiálu by vyžadoval autorizaci pomocí hesla, je takový materiál přístupný veřejnosti, pokud by taková autorizace byla dána komukoli nebo kterékoli osobě, která splní určitá kritéria. K tomu, aby se určilo, zda zpřístupnění nebo distribuce byla veřejná nebo ne, měla by být vzata v úvahu i povaha vztahu mezi dotyčnými osobami.

Pro účely tohoto Protokolu *„rasistický a xenofobní materiál"* znamená jakýkoli písemný materiál, jakékoli obrazové nebo jiné znázornění myšlenek nebo teorií, které obhajují, propagují nebo podněcují nenávist, diskriminaci nebo násilí proti jednotlivci nebo skupině osob na základě rasy, barvy pleti, náboženství, národnostního, etnického nebo jiného původu. Jedná se o písemné materiály (např. texty, knihy, časopisy, prohlášení, zprávy, atd.), obrazové záznamy (např. obrázky, fotografie, výkresy, apod.) nebo kterékoli jiné zobrazení myšlenek nebo teorií rasistické a xenofobní povahy, v takové formě, že mohou být ukládány, zpracovávány a přenášeny prostřednictvím počítačového systému.[21]

Pojem *„násilí"* je míněn jako nezákonné použití síly, zatímco termín *„nenávist"* je míněn jako silný odpor nebo nepřátelství. Pojem *„diskriminace"*, používaný v Protokolu je míněn jako jiné neoprávněné zacházení s osobami nebo skupinami osob na základě určitých charakteristik. Zacházení je diskriminační, pokud nemá žádné objektivní a rozumné odůvodnění, tj. pokud nesleduje nějaký legitimní cíl nebo pokud neexistuje rozumný vztah proporcionality mezi použitými prostředky a cílem, jež má být zrealizován.[22] Nenávist, diskriminace nebo násilí musí být namířeny proti osobě nebo skupině osob z důvodu, že náleží ke skupině, odlišené podle rasy, barvy pleti, náboženství, národnostního, etnického nebo jiného původu.

[21] Niggli, M. A. Rassendiskriminierung und Internet. In: Internet – Recht und Strafrecht. Bern: Stämpli Verlag 2005, str. 258–274.

[22] Rozsudek Evropského soudu pro lidská práva ze dne 23. 5. 1985 ve věci Abdulaziz, Cabales a Balkandali.

„Původ" zde není míněn jako společenský původ. Je míněn zejména ve vztahu k osobám nebo skupinám osob, které pocházejí z osob, jež by mohly být identifikovány podle určitých charakteristik (jako jsou rasa nebo barva pleti). Takové osoby nebo skupiny osob mohou být kvůli svému původu předmětem nenávisti, diskriminace nebo násilí. Pojem *„národnostní původ"* má být chápán v širokém smyslu, tedy nejen s ohledem na národnost nebo etnický původ napadených osob, ale také na jejich státní příslušnost. Navíc, pojem „národnostní původ" se nemusí vztahovat pouze ke státům, které jsou jako takové mezinárodně uznávané, ale také k národnostním nebo etnickým menšinám nebo jiným skupinám osob s podobnými charakteristikami.

Smluvní státy si mohou vyhradit právo nevyvozovat trestní odpovědnost z výše uvedeného jednání, pokud tento materiál obhajuje, propaguje nebo podněcuje diskriminaci, která není spojena s nenávistí nebo násilím, za předpokladu, že jsou k dispozici jiné účinné právní prostředky (např. občanskoprávní či správní trestání). Smluvní státy si mohou rovněž vyhradit právo neaplikovat toto ustanovení na ty případy diskriminace, u kterých nemůže zajistit účinné právní prostředky, z důvodu zavedených principů v jeho národním právním systému, týkajících se svobody projevu.

Ad 2. Rasisticky a xenofobně motivované vyhrožování.

Přestože legislativa většiny států Rady Evropy zajišťuje kriminalizaci vyhrožování obecně, smluvní státy se dohodly, že je potřebné výslovně kriminalizovat vyhrožování z rasistických a xenofobních motivů. *„Vyhrožování"* znamená jednání, které u osob, proti kterým je výhrůžka namířena, vyvolává obavu, že budou poškozeni závažným trestným činem (např. pohrůžka usmrcením, ublížením na zdraví nebo způsobením majetkové škody). Pohrůžka musí uskutečněna prostřednictvím počítačového systému a musí být namířena proti

(i) ***jednotlivci*** *pro jeho rasu, barvu pleti, náboženství, národnostní, etnický nebo jiný původ,*

(ii) ***skupině osob****, která se odlišuje podle některé z těchto charakteristik.*

Ad 3. Rasisticky a xenofobně motivovaná urážka.

Podle tohoto ustanovení se smluvní státy zavazují trestat veřejnou urážku jednotlivce nebo skupiny osob spáchanou prostřednictvím počítačového systému pro jejich rasu, barvu pleti, náboženství, národnostní, etnický nebo jiný původ. Jde tedy o postih verbálních útoků proti jednotlivci nebo skupině osob z důvodu skutečné nebo domnělé náležitosti k určité skupině, odlišené podle specifických charakteristik.

Pojem *„urážka"* se týká jakýchkoliv urážlivých, pohrdavých nebo invektivních výrazů, které poškozují čest nebo důstojnost napadené osoby. Mělo by být jasné z výrazu samého, že urážka je přímo spojena s tím, že osoba náleží k určité vymezené skupině. Na rozdíl od případu výhrůžky, urážka vyjádření v soukromé komunikaci není tímto ustanovením pokryta.

Ad 4. Popření, hrubé snižování, schvalování nebo ospravedlnění genocidy nebo zločinů proti lidskosti.

V posledních deseti letech je možno v Evropě i u nás sledovat nárůst pravicového extremismu, zejména neonacismu. Neoddělitelnou součástí neonacistické propagandy

je snaha o rehabilitaci nacistické ideologie prostřednictvím výroků, které popírají nacistické zločiny.[23] Tzv. „osvětimskou lež" můžeme charakterizovat jako výroky, které bagatelizují, popírají, zlehčují či ospravedlňují nacistické pronásledování a genocidu Židů, Romů, a dalších skupin, které nacistický režim považoval za méněcenné. Vyjadřování takových myšlenek uráží památku obětí a jejich rodin. Snaha o rehabilitaci nacistické ideologie popíráním či zpochybňováním nacistických zločinů je neoddělitelnou součástí antisemitsky a rasisticky motivovaného politického názoru, který směřuje proti základním zásadám demokratického právního státu.[24] Skutečnosti, u kterých byla prokázána historická správnost, nesmějí být popírány, hrubě snižovány, schvalovány nebo ospravedlňovány za účelem podpory rasistických teorií a myšlenek.[25]

Smluvní státy se proto dohodly, že je důležité kriminalizovat projevy, které popírají, hrubě snižují, schvalují nebo ospravedlňují genocidu nebo zločiny proti lidskosti, jak jsou definovány mezinárodním právem a uznány jako takovými

- *rozhodnutím Mezinárodního vojenského tribunálu, ustanoveného dohodou, uzavřenou v Londýně dne 8. dubna 1945; nebo*
- *rozhodnutím jiného mezinárodního soudu, jejichž jurisdikce je smluvním státem uznána.*

K nejzávažnějším jednáním naplňujícím znaky genocida nebo zločinů proti lidskosti, došlo v průběhu období let 1940–1945. Od té však došlo k dalším případům genocidy a zločinům proti lidskosti, které byly silně motivovány teoriemi a myšlenkami rasistické a xenofobní povahy. Protokol proto neomezuje rozsah tohoto ustanovení pouze na zločiny spáchané nacistickým režimem v průběhu 2. světové války, které byly jako takové prokázány Norinberským tribunálem, ale také na genocidu a zločiny proti lidskosti, prokázané ostatními mezinárodními soudy, ustavenými od roku 1945 relevantními mezinárodními právními dokumenty.

Protokol tak umožňuje se odvolat na konečná a závazná rozhodnutí budoucích mezinárodních soudů, v rozsahu, v jakém je jurisdikce takového soudu je uznána státem, který podepsal tento Protokol. Distribuce nebo jiný způsob zpřístupnění takového materiálu veřejnosti prostřednictvím počítačového systému, který popírá, hrubě snižuje, schvaluje nebo ospravedlňuje genocidu nebo zločiny proti lidskosti má být proto postavena mimo zákon a prohlášena za trestný čin.

5. ZÁVĚR: TOLERANCE INTOLERANTNÍCH

Tolerance, snášenlivost, ochota připustit u druhých odlišné názory, jiné chování, či provokativní vzhled je považována za jednu ze základních hodnot demo-

---

[23] Lipstadt, D. E. Popírání holocaustu. Praha: Paseka, 2001, str. 45.

[24] Usnesení Spolkového ústavního soudu ze dne 13.dubna 1994 čj. 1 BvR 23/94, publikováno ve Sbírce rozhodnutí Spolkového ústavního soudu, svazek 1990, J. C. B. Mohr, Tubingen 1994, pod č. 12, str. 241 n., stejně rozsudek Spolkového soudního dvora ze dne 9. 6. 1992, 1 BvR 824/1990, in Neue Juristische Wochenschrift, 14/1993, str. 916.

[25] Srov. např. rozhodnutí Evropského soudu pro lidská práva ve věci Lehideux a Isorni proti Francii ze dne 23. září 1998 č. 24662/94, in Soudní judikatura-Přehled rozsudků Evropského soudního dvora č. 2/1999, str. 25, stejně rozhodnutí Evropského soudu pro lidská práva ve věci Witzsch proti Spolkové republice Německo ze dne 20. dubna 1999 č. 41448/98.

kracie. Extremistické postoje jsou způsobilé přejít v aktivity, které působí, ať již přímo nebo v dlouhodobém důsledku, destruktivně na stávající politicko – ekonomický systém. Je nepochybné, že demokratická společnost má právo se proti takovým rasistickým a xenofobním postojům bránit. Oprávněně se proto klade otázka, nakolik může demokracie tolerovat zneužívání politických práv (zejména práva na svobodu projevu), aniž by přitom zničila samu sebe. Problémem je, jak stanovit práh tolerance a zabránit tak nebezpečí, které vyplývá z toho, že budeme tolerovat i ty intolerantní.

V diskuzích o mezích svobody projevu v souvislosti s rasismem a intolerancí se mnozí inspirují příkladem Spojených států a vyslovují pochyby, zda verbální a grafické formy rasismu vůbec trestněprávně stíhat.[26] Poukazují na existenci neopominutelného rozdílu mezi myšlenkou a slovem, mezi slovem a skutkem. Jak řekl prokurátor Jackson na norimberském tribunálu: *„Nesoudíme vás za vaše zrůdné myšlenky, ale za vaše zrůdné činy"*.

A. **Americké pojetí svobody projevu**. Bez tolerance není demokracie. Chybí-li tolerance, demokracie se mění v tyranii těch, kteří mají v rukou moc. Tolerance však není totéž co indiference. Ten, kdo je k nějakému názoru tolerantní, nemusí k němu být ještě lhostejný. Řečeno spolu Voltairem, hluboce s vámi nesouhlasím, ale budu se bít, abyste svůj názor mohl projevit. Tento typ tolerance vychází z přesvědčení, že každé omezení svobody slova nás omezuje více než svoboda slova sama. Jak říká Bělohradský[27]: *„Demokracii ale neohrožuje svoboda všech říci nebezpečná slova, šířit nebezpečné texty a obrazy. Ohrožují ji naopak ti, kdo chtějí dnes zakázat nebezpečná slova a nebezpečné obrazy, aby zítra mohli zakázat slova a obrazy, které je obviňují a usvědčují"*. Zastánci neomezené svobody slova tak důvěřují v moc svodné diskuse i v boji proti rasismu a dalším nepřátelských ideologiím.

Tomuto pojetí se nejvíce blíží ochrana svobody projevu ve Spojených státech, i když ani zde není absolutní. Americká ústava šetří slovy. Nenajdeme v ní slova o Bohu a ani jednou slovo demokracie. Prostor svobody vymezuje výhradně negativně, říká, co vláda „nikdy nesmí udělat". Podle Prvního dodatku k Ústavě Kongres nevydá zákon omezující svobodu slova a tisku.

V judikatuře Nejvyššího soudu USA, kde se od 60. let prosazuje interpretační doktrína nazývaná *„preferred-position doctrine"*, podle níž politická a osobní práva garantovaná Prvním dodatkem mají preferované postavení, které zaručuje jejich nedotknutelnost a nezcizitelnost, a proto každý zákon, který je omezuje, je nutno presumovat jako neústavní, pokud nebude prokázán opak.[28]

Za tímto názorem stojí hluboce zakořeněné přesvědčení, že právě neomezený trh myšlenek nejlépe působí na hledání pravdy a dosažení obecného blaha. Teorii trhu

---

[26] Např. Boguszak vidí řešení v přijetí americké koncepce přímého a jasného nebezpečí. K postihu by tak nestačilo pouhé abstraktní nebezpečí ohrožení chráněných zájmů. Omezit by bylo možno jen takové projevy, které byly učiněny za okolností, kdy použití násilí nebo jiný bezprávný čin bezprostředně hrozí. In: Boguszak, J. K problematice svobody projevu v právu České republiky. Acta Universitatis Carolinae Iuridica, 1996, č. 1–2, str. 102.

[27] Bělohradský, V. Je u nás dost svobody. Právo, 29. 12. 2001, str. 7.

[28] Blahož, J. Ústavní koncepce a interpretace lidských a občanských práv: srovnávací pohled. Právník, 1998, č. 7, str. 591.

myšlenek poprvé vyjádřil soudce Holmes v rozhodnutí Whitney v. Kalifornie[29]: *„Dovolíme-li v diskusi odlišný názor, může se zdát, že tím považujeme slovo za nedůležité, nebo že nám na výsledku příliš nezáleží, nebo že pochybujeme o vlastní síle nebo o síle svých argumentů. Když ale lidé pochopili, že čas zatratil mnoho bojovných názorů, mohli dojít k tomu, že ještě víc než vlastním názorům věří, že nejvyššího dobra se dosáhne nejlépe svobodnou výměnou myšlenek. Nejlepším testem pravdy je její schopnost prosadit se v soutěži na trhu myšlenek.*"

Nejvyšší soud USA tak rozlišuje mezi pouhým hlásáním určitých myšlenek, byť propagujících násilí, a přímým podněcováním k násilí. Omezit svobodu slova je možno pouze v případě, kdy násilí nebo porušení práva bezprostředně hrozí *(clear-and-present-danger-test)*. Z výše uvedeného vyplývá, že řada projevů, které jsou v kontinentální Evropě stíhány jako extremistické, se v USA těší ochraně Prvního dodatku Ústavy. Proti řadě projevů, které jsou většinovou společností odmítány nebo jsou vůči ní dokonce nepřátelské, tak existuje pouze jedna zbraň – protiargument. S ohledem na zásadní význam svobody slova v judikatuře Nejvyššího soudu USA, jejímž nevyhnutelným důsledkem je i určitá tolerance k propagaci rasové či národnostní nesnášenlivosti, USA nikdy neratifikovaly Mezinárodní úmluvu o odstranění všech forem rasové diskriminace a k čl. 20 Mezinárodního paktu o občanských a politických právech učinily výhradu, že se nesmí dostat do konfliktu s ústavně zaručenými právy.[30]

B. **Evropská doktrína aktivní intolerance**. Druhým typem tolerance je vlastně intolerance, neboť určité názory, které považuje za škodlivé, v té či oné míře zakazuje. Každé přirovnání kulhá, nicméně druhé pojetí tolerance by se dalo s nadsázkou charakterizovat heslem Saint-Justa[31] *„žádnou svobodu nepřátelům svobody."* Tento myšlenkový směr nechápe toleranci jako pouhé neomezování, nezakazování či lhostejnost, ale jako postoj, při kterém se aktivně vystupuje proti projevům intolerance. Například důvodová zpráva k novele německého trestního zákona uvádí: *„Neonacistické aktivity jsou nesnesitelnou provokací demokratického právního státu, a proto vedle odvážného, ofenzivního politického vypořádání se s pravicovým extremismem, musí být nepoučitelní potíráni také prostředky trestního práva."*[32] Pokud společnost určité názory tolerovat nehodlá, má možnost je postavit mimo zákon. Smyslem tohoto řešení je zabránit dalšímu šíření intolerantních myšlenek a jejich praktické realizaci.

Evropský soud pro lidská práva vychází z toho, že tolerance a respekt k rovné důstojnosti všech lidských bytostí představují základy demokratické pluralitní společnosti. Proto Soud považuje za nebytné sankcionovat všechny formy projevů, jež rozšiřují, podněcují, podporují či ospravedlňují nenávist založenou na intoleranci. Každé

---

[29] Rozhodnutí Nejvyššího soudu USA ze dne 16. 5. 1927, 274 U.S.357 (1927), ve věci Whitney v. People of State of California, in http://laws.lp.findlaw.com/getcase/US/315/568.html.

[30] Hyde, J. H. Úvodní slovo. In: Sborník Svoboda projevu a tisk. Brno: Masarykova univerzita, 1995, str. 14.

[31] Saint-Juste byl popraven v roce 1794 spolu s Robespierem, jejich smrtí končí období revolučního teroru, masových vražd kněží, politických jinověrců, povinného podezřívání celých sociálních tříd, které Saint-Justovo heslo ospravedlňovalo. Osvětluje paradox boje za svobodu, který můžeme vyjádřit i takto: *„Proč sis nevzal červenobílou kokardu, symbol naší svobody? Nevzal jsem si červenobílou kokardu, abych zjistil, zda jsem opravdu svobodný"*. In: Bělohradský, V. Je u nás dost svobody. Právo, 29. 12. 2001, str. 7.

[32] Návrh novely trestního zákona poslaneckého klubu SPD, Deutscher Bundestag, 12. období, tisk 12/7960.

takové omezení musí zároveň odpovídat naléhavé společenské potřebě, být přiměřené sledovanému účelu a zakládat se na dostatečných a relevantních důvodech.[33] Je koncept tzv. **„demokracie schopné bránit se"** *(wehrhafte Demokratie, démocratie aapte se défendre, democracy capable of defending itself)*, kterou Soud opakovaně uznal ve svých rozhodnutích. Soud považuje její realizaci za *„legitimní cíl"*, jehož naplňování dovoluje v přiměřených mezích státům omezit práva zaručená v Úmluvě.[34]

Doktrína aktivní intolerance tak znamená, že ve jménu tolerance musíme požadovat i právo netolerovat intoleranci. Ústavní soud tuto doktrínu aktivní intolerance potvrdil v roce 1992, když judikoval, že

- *hnutí, která prokazatelně směřují k potlačení občanských práv nebo k hlásání vymezené záště, ať jsou jakkoli pojmenovaná a zdůvodňovaná jakýmikoli ideály či cíly, jsou hnutí, která demokratický stát, jeho bezpečnost a bezpečnost jeho občanů ohrožují; jejich zákonný zákaz je proto nezbytným opatřením k omezení svobody projevu a svobody sdružovací ve smyslu čl. 17 odst. 4 a čl. 20 odst. 3 Listiny základních práv a svobod;*
- *trestněprávní zákaz podpory a propagace určitých ideologií, které svou doktrínou i praktickým postupem vylučovaly a vylučují šířeních jiných ideologií, přispívá k zabezpečení plurality názorů, ideologií, politických a jiných hnutí a k reálné možnosti jejich šíření; toto omezení nechrání pouze lidská práva a svobody, nýbrž i demokratické základy státu.*[35]

Lidská práva jsou založena na univerzální identitě lidské bytosti, na rovnosti všech lidí v jejich důstojnosti a právech. Rasismus je útokem na lidskou důstojnost každého jednotlivce a ohrožuje soudržnost společnosti a její demokratické základy. Právo nebýt diskriminován z rasových důvodů a právo na ochranu před projevy rasové nenávisti tak patří k základním lidským právům.[36]

Rasismus je antidemokratický ze své podstaty, odpírá jiným základní práva a svobody. Projevy rasismu jsou zlem, jsou emoční přípravou budoucího násilí.[37] Rasistická ideologie byla vymyšlena, aby odůvodnila násilí. Rasistická pseudofilosofie a pseudověda poskytuje vysvětlení a důvod pro takové násilné činy, neboť považuje lidi s jinou barvou pleti, jiné národní či etnické příslušnosti za méněcenné, za podlidi. Každá rasistická propaganda je těhotná násilím. Nelze tedy čekat, až se tato hrozba násilím naplní, ale je třeba postihovat již verbální a grafické předpolí rasistických násilných trestných činů.

Absolutizování svobody projevu tváří v tvář projevům rasismu není cestou, kudy by se Česká republika měla ubírat. Česká republika se nemůže se vyvázat z celé sítě mezinárodních závazků namířených proti rasismu, aniž by se nevyčlenila z rodiny de-

---

[33] Např. rozhodnutí Evropského soudu pro lidská práva ze dne 27. 3. 1996 ve věci Goodwin v. Spojené království.

[34] Např. rozhodnutí Evropského soudu pro lidská práva ze dne 26. 9. 1995, ve věci Vogt proti Německu, ASPI.

[35] Nález Ústavního soudu ČSFR ze dne 4. 9. 1992, sp. zn. Pl. ÚS 5/92, Sb. nál. a usnesení ÚS ČSFR, 1992, str. 25.

[36] Repík, B. Svoboda projevu versus rasismus ve štrasburské judikatuře. Trestněprávní revue, 2004, č. 2, str. 49.

[37] Repík, B. Svoboda projevu versus rasismus ve štrasburské judikatuře. Trestněprávní revue, 2004, č. 2, str. 52.

mokratických evropských států. Americký model svobody projevu proto nemůže být vzorem pro Evropu, která má jinou historickou zkušenost a jiné právní tradice. Do 21. století vstoupila Evropa nerozdělená železnou oponou, plná úsilí o vytvoření tolerantního, multikulturního klimatu. Tatáž Evropa se však s sebou nutně nese i rezidua své vlastní minulosti. Právě evropský kontinent zplodil v minulém století dvě války. V důsledku druhé z nich přetrvává dnes v Evropě zvýšená citlivost daná historickou zkušeností na projekci některých negativních jevů ve společnosti. Právě díky svým bezprostředním historickým zkušenostem je Evropa svým způsobem více ostražitá a mnohem méně benevolentní ve vnímání podhoubí těchto jevů než např. USA.

EXTREMISMUS UND DIE GRENZE DER REDEFREIHEIT IM INTERNET

Zusammenfassung

In der Einführung beschäftigt sich der Autor mit der Definition des Extremismus und mit seinem Unterschied von der Kriminalität mit dem extremistischen Unterton. Weiter befasst er sich mit der Form des Internetmissbrauchs von Extremisten, mit der Verantwortung der Raumanbieter für Elektronischdatenspeicherung (webhosting), der Internetzugangdienstleister und der Betreibern des Webdiskussionsforums. Der Autor spricht weiter über Institutionalsicherstellung des Rückgriffs von Extremismus im Internet und über die Internationalmitarbeit in diesem Gebiet, vor allem über Zusatzprotokoll zum Abkommen über Computerkriminalität, das sich mit den Fragen über Definitionen des Tatbestandes, den Umfang der Kriminalisierung der Taten mit der rassistischen und ausländerfeindlichen Beschaffenheit, die durch Netz-Computer begehen sind, und die Maßnahmen zur Mitarbeit in dem Gebiet des Strafrechts, beschäftigt. Die Aufmerksamkeit ist vornehmlich den Tatbeständen gewidmet. Im Verschluss behandelt der Autor die Redefreiheit in den USA und in Europa, über die Unterschiede zwischen amerikanischer und europäischer Stellung und über die Toleranz/Intoleranz der rassistischen und ausländerfeindlichen Ausdrücke.

Schlagwörter: der Extremismus, die Kriminalität mit dem extremistischen Unterton, der Missbrauch des Internets, das Zusatzprotokoll zum Abkommen über Computerkriminalität, die Toleranz, die Redefreiheit

Klíčová slova: extremismus, kriminalita s extremistickým podtextem, zneužívání internetu, Dodatkový protokol k Úmluvě o počítačové kriminalitě, tolerance, svoboda projevu

2008 ACTA UNIVERSITATIS CAROLINAE – IURIDICA 4 PAG. 51–63

NĚKTERÉ MEZINÁRODNĚPRÁVNÍ ASPEKTY ZÁVAZKOVÝCH VZTAHŮ VZNIKLÝCH V KYBERPROSTORU

TOMÁŠ KUBEC
Obvodní soud pro Prahu 6

1. ÚVOD

Prudký rozvoj informatiky a telekomunikace v posledních letech, spolu s čím dál větší všeobecnou dostupností internetu, přinesl řadu nových možností a do značné míry odstranil hranice mezi zeměmi. Tento rozvoj s sebou pochopitelně nese i řadu negativ a problémů. Nové možnosti se jednak zákonitě nabídly i těm, kteří se pohybují na hranici, či častěji, za hranicí, zákona a jednak přinesly situace, na které nebyla (a dost dobře nemohla být) legislativa ani výkonná moc připravena. Mezi problémové okruhy zasluhující zvýšenou pozornost spadá zejména: výrazný **nárůst přeshraničního prvku** a tedy mezinárodněprávního charakteru vztahů, nové formy **kontraktace a projevu vůle** obecně (smlouvy uzavírané po internetu, veřejnoprávní úkony činěné elektronickou formou, atd.), **nové formy plnění** (software a audiovizuální nahrávky nakupované a zároveň dodané po internetu), paralelní platební a **quasi-platební systémy a technická složitost** při vyšetřování trestné činnosti a posuzování sporů. Na následujících stránkách bych se rád zaměřil na nastíněné tematické okruhy, aniž bych ovšem aspiroval na úplné pokrytí těchto témat nebo snad dokonce nalezení jednoznačných odpovědí na vznikající otázky. Naopak budu rád, pokud se čtenář nad nastolenými otázkami a problémy zamyslí a pokusí si najít i vlastní odpověď.

2. PŘESHRANIČNÍ PRVEK

V důsledku nadnárodní topologie internetu je v rámci komunikace po síti otázka států do značné míry opomíjena a upozaďována. Tento stav je naprosto vyhovující pro samotný technický chod sítě a drtivou většinu komunikace po ní, včetně transakcí a právních vztahů, které proběhnou bez problému. Těch je sice většina, ale v případech, kdy dojde k nějakému sporu nebo poškození účastníka komunikace, může hrát přeshraniční prvek klíčovou roli. Je tomu tak z řady důvodů: z právního hlediska je důležitý pro posouzení rozhodného (aplikovatelného) práva, určení pravomoci a příslušnosti konkrétních národních soudů a vymožitelnosti. Další roli hraje přeshraniční prvek z hlediska možnosti technické realizace řešení problému a administrativ-

ních překážek, tedy např. jaká je ochota zahraničních orgánů spolupracovat při řešení situace či vyšetřování trestné činnosti, jaké jsou možnosti platebního styku apod.

Jako dobrý příklad mnohonásobného přeshraničního prvku může posloužit nedávný případ z mého okolí, který naštěstí proběhl zcela bez komplikací: český státní občan, trvale žijící ve Švýcarsku (tzv. švýcarský rezident), pracující pro americkou společnost v rámci její švýcarské pobočky, si ze zaměstnání objednal zboží od rakouské společnosti, jejíž server (počítač, na kterém běžel internetový obchod) byl fyzicky umístěn v Německu. Dodací adresa byla ve Velké Británii, kam dotyčný odjížděl na delší pracovní cestu. Protože objednávku odesílal z počítače v práci, nebyl přímo připojen k internetu přes internetového poskytovatele připojení (ISP), ale byl připojen k vnitropodnikové sítí, která byla realizována částečně po internetu formou virtuální privátní sítě (VPN) s internetovou bránou (iGW) v Kanadě, odkud objednávka technicky vzato odešla. Zboží platil platební kartou vydanou ve Spojených státech, k účtu vedenému rovněž ve Spojených státech. Zboží bylo dodáno prostřednictvím kurýrní služby, jejíž sídlo a místo registrace bohužel neznám. Dost dobře mohlo jít o firmu, která sídlila ještě v jiném státě. K dokonalému zkomplikování situace snad chybí jen to, že by internetový obchod užíval jinou doménu prvního řádu (znaky za poslední tečkou ve webové adrese jako .cz nebo .sk, identifikující stát), takže by registračně pařil k jinému státu než jeho provozovatel.

V daném případě se vyskytuje sedm (resp. možná osm) států, které se navíc v některých částech obchodu opakují, mohlo tedy reálně jít o ještě více států a celá situace se mohla zkomplikovat. V případě, že by v obdobném případě nastal nějaký problém a věc by měla být řešena soudní cestou, šlo by právě kvůli přeshraničnímu charakteru sporu o poměrně složitý případ a v případě spotřebitelů a obchodů s poměrně malou hodnotou bude patrně ve většině případů ztráta oželena, protože domáhání se nápravy by bylo příliš složité a neefektivní. Zatímco v případě nakupování po internetu nebude komplikace způsobená přeshraničním prvkem zpravidla záměr prodávajících, v případě počítačové kriminality je tomu jinak. Pachatelé trestné činnosti po internetu cíleně vyhledávají přeshraniční prvek, byť spíše než na otázku rozhodného práva a pravomoci se zaměřují na to, aby komunikace proběhla přes co nejvíce států, které neochotně nebo vůbec nespolupracují s ostatními státy při vyšetřování trestné činnosti, monitorování datové komunikace a vydávání a postihování pachatelů trestné činnosti.

3. PRAVOMOC A PŘÍSLUŠNOST

V případě vzniklého sporu, který se nepodaří odstranit smírnou cestou, což by mělo být vždy preferované řešení, mimo jiné i z důvodu efektivity řešení sporu, bude jednou z prvních otázek otázka, který soud v kterém státě má věc rozhodovat, tedy otázka pravomoci a příslušnosti soudu. Tu obvykle řeší jednak mezinárodní úmluvy a jednak vnitrostátní právo. Mezinárodní úmluvy mohou být pouze mezi dvěmi státy (dvoustranné úmluvy), nebo mohou vázat více států (mnohostranné úmluvy). Specifickým případem je pak právo Evropského společenství, které má pro české uživatele kyberprostoru velký význam a o kterém je pojednáno dále.

Zásadní vnitrostátní normou je v České republice Zákon o mezinárodním právu soukromém a procesním, publikovaný ve sbírce pod číslem 97/1963 Sb. (dále jen Zákon o mezinárodním právu). Sporná práva v kyberprostoru budou v drtivém případu práva majetková – ať budou vyplývat z uzavřených smluv nebo např. z odpovědnosti za škodu (smluvní i deliktní). Proto, pakliže nestanoví něco jiného mezinárodní úmluva, jíž je Česká republika vázána, bude nejčastěji aplikován § 37 Zákona o mezinárodním právu. Podle něj je pravomoc českých soudů v majetkových sporech dána, je-li dána podle českých předpisů jejich příslušnost. Příslušnost je pak primárně upravena v § 84 a násl. Občanského soudního řádu, publikovaného ve sbírce pod číslem 97/1963 (dále jen o.s.ř.). Obecným pravidlem dle tohoto ustanovení je, že k řízení je příslušný obecný soud účastníka, proti němuž návrh směřuje (žalovaného), což je zpravidla soud, kde žalovaný sídlí (pokud není dána výlučná příslušnost nebo příslušnost na výběr daná). Pouze v případě, že existuje příslušný soud v české republice, je dána pravomoc českých soudů ve věci rozhodovat. Toto je pro českého uživatele nakupujícího na zahraničních internetových obchodech spíše nevýhodné – pravomoc českých soudů je dána jen tehdy, pokud je on sám žalován. Ochrany proti nepoctivým obchodníkům se musí domáhat u zahraničního soudu. Poněkud příznivější situace je v případě náhrady škody (včetně náhrady škody z počítačové trestné činnosti). Zde lze totiž využít příslušnosti na výběr dané zakotvené v § 87 o.s.ř. Podle ust. § 87 odst. 1 písm. b) o.s.ř. je pak dána i příslušnost soudu, v jehož obvodu došlo ke skutečnosti, která zakládá právo na náhradu škody. Na rozdíl od běžných škod v reálném světě, kde místo vzniku škody a místo, kde došlo ke skutečnosti, která zakládá právo na náhradu škody, zpravidla splývají, při vzniku škody v kyberprostoru tomu často tak nebude. Protiprávní jednání se může odehrát na jiném konci světa, nežli nastane následek. Navíc může nastat protiprávní jednání (typicky komisivní) v jednom místě, kde se nachází škůdce, dojít k modifikaci dat (která sama kauzálně vede ke vzniku škody) v druhém místě a samotná škoda (ve smyslu majetkové újmy nastalé v majetkové sféře poškozeného, která je vyjádřitelná v penězích) nastat v třetím místě. Mezi skutečnost, která zakládá právo na náhradu škody a vznikem škody tedy nelze postavit rovnítko. Pokud akceptujeme výklad, že pod takovou skutečnost zakládající právo na náhradu škody podřadíme nejen samotné jednání v místě škůdce (v zahraničí), ale i jeho zaznamenatelný projev v jiném místě (v naší republice), lze často dovodit pravomoc českých soudů. Pakliže ovšem došlo pouze ke vzniku škody na území České republiky bez dalšího, pravomoc českých soudů dovodit nelze. Jinou otázkou už je i v případě pravomoci bohužel vymahatelnost případného rozsudku. Zejména v rámci Evropské unie se však i tato oblast v posledních letech výrazně zlepšila.

Specifickou možností je tzv. sjednaná pravomoc. Podle § 37 odst. 2 Zákona o mezinárodním právu lze pravomoc českých soudů v majetkových sporech založit také písemnou úmluvou stran. Nutno zdůraznit, že lze založit pravomoc českých, nikoliv zahraničních soudů (to neplatí pro právnické osoby, kde to lze). V praxi tedy bude tato možnost využitelné jen zřídka. V případě deliktní odpovědnosti nepřichází v úvahu vůbec, v případě nakupování po internetu budou zahraniční prodejci asi jen těžko navrhovat pravomoc českých soudů. Častější případ bude explicitní sjednání pravomoci zahraničního soudu státu, kde sídlí prodejce. Takové ustanovení je sice v případě

fyzických osob (a v režimu Zákona o mezinárodním právu) podle českého práva neplatné, pravomoc zahraničního soudu bude však stejně dána podle sídla osoby prodávajícího.

Zvláštní režim nabízí právo evropské unie. Zásadním procesním předpisem je nařízení Rady ES č. 44/2001 o příslušnosti a uznávání a výkonu soudních rozhodnutí v občanských a obchodních věcech, tzv. Nařízení Brusel I. To obecně zakotvuje pravomoc soudů členského státu, kde má žalovaný bydliště, bez ohledu na svou státní příslušnost. Narozdíl od naší úpravy není tedy rozhodná státní příslušnost, ale sídlo (resp. bydliště) žalovaného, tedy kterého státu je rezidentem. To samo o sobě by většinou neznamenalo valný rozdíl. Zajímavější je však zvláštní příslušnost zakotvená v článku 5 Nařízení Brusel I. Podle něj lze mimo jiné žalovat u soudu místa, kam podle smlouvy zboží bylo nebo mělo být dodáno nebo kde služby podle smlouvy byly nebo měly být poskytovány. To už je pro nakupování po internetu pro české uživatele kyberprostoru podstatně příznivější zpráva, protože v případě, že mělo být zboží dodáno nebo měla být služba poskytnuta na našem území, bude založena pravomoc našich soudů.

V případech odpovědnosti za škodu z protiprávního jednání je založena pravomoc, resp. příslušnost, dle místa, kde došlo nebo může dojít ke škodné události. Jde-li o trestný čin a byla podána obžaloba, pak je dána příslušnost soudu, u něhož byla podána obžaloba, je-li tento soud podle práva pro něj platného oprávněn rozhodovat o občanskoprávních nárocích. Tato úprava je tedy obecně pro poškozeného spíše výhodnější, nežli úprava Zákona o mezinárodním právu.

Velmi významná je ochrana spotřebitele nakupujícího na internetu zakotvená v Oddílu 4 Nařízení Brusel I. Podle něj má spotřebitel (ve věcech týkajících se smlouvy uzavřené spotřebitelem pro účel, který se netýká jeho profesionální nebo podnikatelské činnosti a s výjimkou přepravních smluv) na výběr, zda zažaluje dodavatele u soudů členského státu, na jehož území má dodavatel sídlo, nebo u soudu místa, kde má bydliště on sám. Naopak dodavatel tuto možnost nemá a musí žalovat u soudu dle bydliště spotřebitele.

Kromě výlučné pravomoci konkrétního soudu (např. ve věcech, jejichž předmětem jsou věcná práva k nemovitostem a nájem nemovitostí, patentů a některých společenstevních věcech), lze rovněž založit pravomoc soudu členského státu dle článku 24 Nařízení Brusel I: „Není-li soud jednoho členského státu příslušný již podle jiných ustanovení tohoto nařízení, stane se příslušným, jestliže se žalovaný dostaví k jednání k tomuto soudu. To neplatí, pokud se žalovaný dostaví proto, aby namítal nepříslušnost soudu, nebo je-li jiný soud podle článku 22 výlučně příslušný." Nutno dodat, že český překlad je nepřesný, kdy výraz „enters an appearance" překládá jako „dostaví k jednání k tomuto soudu". Ve skutečnosti je tím míněna jakákoliv aktivita žalovaného směřující k jeho obraně (např. písemné vyjádření k žalobě), s výjimkou námitky nepříslušnosti daného soudu. Pokud tedy nejde o věc s výlučnou příslušností a není dána pravomoc resp. příslušnost místního soudu, ale žalovaný se jí takto dobrovolně podrobí, může tento soud věc rovněž projednat a ve věci rozhodnout.

I podle Nařízení Brusel I. lze sjednat příslušnost konkrétního národního soudu, pokud má alespoň jedna ze stran bydliště nebo sídlo na území tohoto členského státu. Pomocí tohoto ustanovení však nelze obcházet ochranu spotřebitelů tak, že by prodejce

v obchodních podmínkách zakotvil příslušnost pro něj výhodného místa soudu a spotřebiteli by nezbylo než to buď akceptovat nebo nenakupovat. Sjednání příslušnosti u spotřebitelských smluv je totiž speciálně upraveno a případná dohoda v neprospěch spotřebitele odporující této úpravě je právně neúčinná (Článek 23).

Jak vidno, v rámci právní úpravy Evropské unie je postavení uživatele kyberprostoru a zejména spotřebitele pohybujícího se na internetu podstatně bezpečnější než dle naší obecné vnitrostátní úpravy, a to i z hlediska náhrady škod. Právo EU se aplikuje na vztahy mezi rezidenty Evropské unie, tedy zejména při nakupování v internetových obchodech sídlících v některém z členských států Evropské unie, nebo při jakémkoliv právním vztahu mezi rezidenty Evropské unie. V ostatních případech se (pokud nebude jiná úprava v rámci mezinárodní úmluvy) aplikuje méně výhodný režim Zákona o mezinárodním právu.

4. ROZHODNÉ PRÁVO

Podobně jako u pravomoci soudů se také rozhodné právo dovozuje ze Zákona o mezinárodním právu, pokud nestanoví něco jiného mezinárodní úmluva, jíž je Česká republika vázána. Pro dotčenou oblast bude nejvýznamnější ust. § 9 a násl. Zákona o mezinárodním právu upravující závazková práva (což se týká i deliktních závazků, nejen smluvních). Rozhodným právem je pak primárně právo, jež si účastníci zvolí. Teprve pak se aplikují kolizní normy pro určení rozhodného práva. Často se tak stává, že v rámci nákupu po internetu je jako rozhodné právo zvoleno právo státu, kde sídlí prodejce. Může tak nastat situace, kdy je sice dána pravomoc českých soudů, vztah se však řídí zahraničním právem. Tím se případné řízení před soudem komplikuje zejména o ztišování zahraničního práva (zásada iura novit curia platí pro vnitrostátní právo). To je obtížné jednak pro horší dostupnost překladů zahraničních norem a jednak pro určité vytržení z kontextu národní legislativy. Vzhledem k jistým odlišnostem právního chápání je podstatně obtížnější interpretovat správně zahraniční normu bez hlubších znalostí národního chápání práva a kontextu obecných právních norem, tedy v podstatě vytrženou z kontextu.

Teprve v případě, že právo není sjednáno (což platí vždy v případech deliktní odpovědnosti), dovozuje se rozhodné právo podle příslušných kolizních ustanovení. Obecným pravidlem pak je, že se řídí vztahy účastníků právním řádem, jehož použití odpovídá rozumnému uspořádání daného vztahu. Podle § 10 odst. 2 písm. a) Zákona o mezinárodním právu se zpravidla řídí smlouvy kupní a smlouvy o dílo právem místa, kde je sídlo (bydliště) prodávajícího nebo zhotovitele díla v době uzavření smlouvy. Bude tedy patrně nezbytné i na nákupy po internetu aplikovat právo dle sídla prodejce a to bez ohledu na to, zda je založena pravomoc českých soudů či nikoliv. Tento přístup komplikuje případné řízení a staví spotřebitele do nevýhodné pozice, ale není to přesto důvod odchýlit se od uvedeného pravidla.

V rámci Evropské unie to patrně změní připravované nařízení o rozhodném právu – nařízení o právu rozhodném pro smluvní závazkové vztahy (Řím I, vedený pod COD 2005/0261). To sice bude patrně pro kupní smlouvy i pro smlouvy o poskytování slu-

žeb zakotvovat v případě nesjednání rozhodného práva jako rozhodné právo právo sídla prodávajícího (resp. poskytovatele služeb), ale budou určité výjimky. Zejména spotřebitelské smlouvy uzavřené spotřebitelem za účelem, který nelze považovat za výkon povolání nebo živnostenské činnosti, se budou řídit právem členského státu, v němž má spotřebitel obvyklé bydliště, nikoliv však ve všech případech: „Použije se za podmínky, že smlouva byla uzavřena s obchodníkem, který vykonává povolání nebo živnostenskou činnost v členském státě, v němž má spotřebitel obvyklé bydliště, nebo který všemi prostředky zaměřuje tyto činnosti na tento členský stát nebo na více zemí, mezi nimiž je i tento členský stát, a že smlouva spadá do rámce těchto činností, ledaže by obchodník neznal místo spotřebitelova obvyklého bydliště a tato neznalost není způsobena jeho nedbalostí". Bude se to patrně tedy týkat zejména internetových obchodů prodávajících zboží či služby do více zemí (typicky třeba Rakousko a zároveň Německo), které budou mít stránky v jazyce cílové země a upravené dodací podmínky do této země. Nákup v čistě německém internetovém obchodě českým spotřebitelem bude proto nejspíše posuzován stejně podle německého práva. Konkrétní úprava samozřejmě závisí na finální podobě Nařízení Řím I.

Pokud jde o odpovědnost za vnik škody, tak rozhodné právo upravuje ust. § 15 Zákona o mezinárodním právu. Dle něj nároky na náhradu škody, nejde-li o porušení povinnosti vyplývající ze smluv a jiných právních úkonů, řídí se právem místa, kde škoda vznikla, nebo místa, kde došlo ke skutečnosti, která zakládá nárok na náhradu škody. Dle mého názoru je třeba toto ustanovení vykládat tak, že se nevztahuje na smluvní závazkové vztahy, na odpovědnost za škodu způsobenou protiprávním jednáním však ano. Striktně vzato je protiprávní jednání také právní úkon, ale doslovný výklad by toto ustanovení omezil jen na objektivní odpovědnost v důsledku právních skutečností, což se mi jeví jako příliš restriktivní výklad. Podle formulace pak lze usuzovat, že rozhodným právem může být jak právo místa, kde vznikla škoda (nastal následek), tak místa protiprávního jednání a použije se právo odpovídající rozumnému uspořádání věcí, tedy zpravidla místo škody.

Deliktní odpovědnost za škodu není v rámci připravovaného Nařízení Řím I. upravena neboť toto nařízení se má vztahovat jen na smluvní závazkové vztahy. Pakliže v jejich rámci vznikne právo na náhradu škody, bude se řídit právem rozhodným pro smlouvu.

Z evropské legislativy stojí z hlediska rozhodného práva za povšimnutí i Směrnice evropského parlamentu a rady č. 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu („Směrnice o elektronickém obchodu") ('Directive on electronic commerce'), byť přímo rozhodné právo neřeší. Směrnice po národních legislativách požaduje, aby jejich právní řády umožňovaly uzavírání smluv elektronickou cestou, byť umožňuje členským státům zakotvit výjimky v oblasti nakládání s nemovitostmi, dále pak u smluv, které musejí být schváleny veřejnou mocí a smluv v oblasti rodinného a dědického práva. Dále stanoví základní definice pro oblast právní úpravy elektronického obchodu, jako např. „služby informační společnosti" či „poskytovatel", které bude třeba inkorporovat do národních úprav. Ačkoliv směrnice výslovně stanoví, že

nevytváří dodatečná pravidla mezinárodního práva soukromého ani neupravuje pravomoc soudů, umožňuje lépe nalézat kolizní kriteria. Důležité pro hledání rozhodného práva či pravomoci je, že *„místem usazení společnosti poskytující služby prostřednictvím internetových stránek na internetu není místo, kde se nachází technické zařízení, jehož prostřednictvím společnost provozuje internetové stránky, ani místo, kde jsou internetové stránky přístupné, ale místo, kde společnost vykonává svou hospodářskou činnost"*.

Pro nalezení rozhodného práva je někdy podstatné místo plnění, a to buď kvůli zákonné kolizní normě (v českém Zákoně o mezinárodním právu se to zejména týká přepravních a zasilatelských smluv) nebo kvůli dohodě stran. Otázka místa plnění se komplikuje u nehmotných statků, které jsou prodávány i dodávány po internetu. Je totiž nesprávným zjednodušením chápat jako místo plnění toliko bydliště či aktuální místo pobytu odběratele. Přesnější pojetí je výklad, že místem plnění je místo, kam si odběratel přenesl nebo nechal přenést binární data reprezentující dotčený statek – tedy například místo, kde se nachází počítač, u nějž uživatel sedí. Ani tento výklad ovšem není zcela bezproblémový. Např. je otázkou, zda je ze strany dodavatele plněno okamžikem, kdy umožní dispozici s daty nebo teprve okamžikem, kdy dojde k přenosu a odběratel si data „stáhne" (místo odeslání objednání a místo cíle přenosu se pak může lišit). Tento problém odpadá, když jsou data na základě objednávky uživateli – odběrateli bezprostředně zaslána, a to např. formou elektronické pošty nebo okamžitým přenosem po obdržení platby. Tento postup však není pravidlem – často odběratel po zaplacení dostane přístupové informace a je na něm, kdy a kam si data přenese. Toto místo pak může být jiné, nežli místo, kde sídlí a nežli místo, z kterého odeslal objednávku. Ještě komplikovanější situace je, kdy dojde k přenosu dat, ale nikoliv přímo k uživateli (tedy tam kde fyzicky je), ale na nějaký třetí počítač, např. v systémech UNIX je zcela běžné, že uživatel je připojen pomocí tzv. terminálu z jiného počítače, který je zcela jinde, běžně v jiné zemi. Pro obvyklé situace bude patrně postačovat výklad „kam si uživatel data stáhl", ale mohou, jak bylo nastíněno, nastat podstatně komplikovanější situace.

Z uvedeného je patrné, že ne všechny přeshraniční prvky jsou významné, popřípadě zakládají mezinárodněprávní charakter vztahu. Obecně velký význam, jak pro pravomoc tak pro rozhodné právo, hraje státní příslušnost nebo sídlo všech účastníků vztahu, v některých případech má význam místo dodání. V případech odpovědnosti za škodu má velký význam místo vzniku škody, popř. místo jednání vedoucího ke vzniku škody. Pokud by vznikly spory ohledně provedení platby (např. neoprávněné čerpání z platební karty), může hrát roli i místo sídla banky, která transakci provedla. Pokud by vznikly spory ohledně řádnosti dodání, může hrát roli i místo sídla dopravce, který zboží dopravoval od prodejce k objednateli.

Za normálních okolností nehraje roli fyzické umístění serveru, na kterém je provozován internetový obchod, stejně jako umístění internetové brány z privátní sítě a stejně jako doména prvního řádu. Ta by mohla mít patrně význam tehdy, kdy by šlo o podvod a nesprávnou doménou prvního řádu byl účastník vztahu uveden v omyl.

5. NOVÉ FORMY KONTRAKTACE A PROJEVU VŮLE

Do nedávné doby se prakticky projev vůle omezoval na osobní (prezenční), ať ústní nebo písemný a na projev vůle na dálku, a to písemnou cestou. Komunikace po internetu přináší řadu specifik, zejména co se týče formy projevu vůle. Právní úkon je projev vůle směřující zejména ke vzniku, změně nebo zániku těch práv nebo povinností, které právní předpisy s takovým projevem spojují. To platí i pro projev vůle elektronickou cestou, které jsou ze své povahy prakticky vždy písemné. Náležitostí písemného právního úkonu je podle českého práva podpis (§ 40 odst. 2 o. z.). Ten už ale v pravém slova smyslu být připojen nemůže. Zákon i na to pamatuje a umožňuje použití elektronického podpisu. Ve většině internetových obchodů se ovšem objednávka potvrzuje stisknutím tlačítka „Objednat", „Odeslat objednávku", a podobně. Tím má být projev vůle vyjádřen. Podpis, ani formou prostého textu však připojen není. Přesto řada právních řádů podpis explicitně vyžaduje a mohou tak v případě přeshraničních obchodů vznikat spory o platnosti uzavření smlouvy. Tento nedostatek se snad dá výkladově zhojit jen tím, že je u objednávky vyplněno i jméno kupujícího, přesto je dodržení náležitosti pochybné.

Zdánlivě slibnou inovací pro nakupování a kontraktaci po internetu obecně byl již zmíněný elektronický podpis. Dříve se jako prostředek dokázání původnosti zprávy připojoval vlastnoruční podpis, popřípadě jeho mechanická náhrada v případech, kdy je to obvyklé. Podpis totiž nese jisté individuální znaky, které lze jen s obtížemi věrohodně napodobit a tak bylo možno určit s poměrně velkou jistotou původnost zprávy. Tento princip nelze ale využít u elektronické komunikace, neboť data (a tedy i podpis) se dají snadno kopírovat.

Tyto nevýhody, tedy nedostatečnou identifikaci a nezjistitelnost modifikace odstraňuje takzvaný bezpečný elektronický podpis. Jeho podstatou je to, zjednodušeně řečeno, že každý, kdo má k dispozici elektronický podpis, má dva soubory, tzv. klíče, jeden veřejný a jeden soukromý, který si střeží. Pomocí soukromého klíče lze ke zprávě připojit binární dodatek, který je vytvořený matematickou kombinací dat soukromého klíče a zprávy. Kdokoliv pak pomocí veřejného klíče a příslušného softwaru může ověřit, že zpráva byla podepsána soukromým klíčem odpovídajícím veřejnému klíči a že nebyla pozměněna. Nemůže z toho ale odvodit soukromý klíč a tedy jej nemůže zneužít pro padělání podpisů. Pro tyto účely je zpravidla používána tzv. asymetrická kryptografie, konkrétně většinou algoritmus RSA založený na faktorizaci velmi velkých čísel. Ten je založen na tom, že je výpočetně poměrně snadné vynásobit dvě velmi dlouhá prvočísla. Rozložit získaný součin zpět na původní čísla je ovšem výjimečně výpočetně náročné a tak to na seberychlejším počítači trvá velmi dlouhou dobu. Tímto postupem je skutečně zajištěna velmi vysoká pravděpodobnost autenticity komunikace.

Přesto se ale elektronický podpis v běžném životě na internetu (snad s výjimkou on-line bankovnictví) zatím příliš nerozšířil. Důvodem může být hned několik příčin: Aby byl elektronický podpis reálně použitelný, musí mít příjemce zprávy k dispozici veřejný klíč odesilatele a musí mít jistotu, že tento klíč je pravý (není nic snadnějšího než vygenerovat pár klíčů na falešnou identitu a pak s tímto klíčem platně podpisovat

zprávy). Triviálním řešením je předání klíče osobně. To je však ve většině případů komunikace po internetu nereálné. Dalším řešením je získání klíče od důvěryhodné osoby nebo podepsání klíče takovou důvěryhodnou osobou, která tím, že připojí svůj elektronický podpis, ověří pravost klíče. K tomu slouží certifikační autority, či v dikci zákona č. 227/2000 Sb., o elektronickém podpisu, poskytovatelé certifikačních služeb. Získání klíče od poskytovatele certifikačních služeb s sebou nese jisté obtíže: poskytovatel musí subjekt ověřit, to znamená, že je nutná osobní návštěva. Certifikát je zpoplatněný a má omezenou časovou platnost. Další problém je mezinárodní uznávání elektronických podpisů, kdy uznávání faktické a uznávání právní (v případě právního sporu) se zdaleka ne vždy kryje. Český zákon o elektronickém podpisu a evropská legislativa na uznávání myslí, konkrétně ust. § 16 zákona o elektronickém podpisu předpokládá automatické uznávání certifikátů vydaných v rámci Evropské unie a dále certifikátů, jenž jsou vydány jako kvalifikované v jiném než členském státu Evropské unie, pokud je poskytovatel buďto akreditován v jiném členském státě nebo pokud poskytovatel z Evropské unie převezme odpovědnost za platnost a správnost certifikátu ve stejném rozsahu jako u svých kvalifikovaných certifikátů nebo pokud to vyplývá z mezinárodní smlouvy. Mimo rámec Evropské unie již právní uznávání našich certifikátů není zdaleka jisté.

6. NOVÉ FORMY PLNĚNÍ

Internet přináší nové, zcela imateriálně dodávané statky, jako jsou např. software a audiovizuální nahrávky nakupované a zároveň dodané po internetu, za poplatek zpřístupněné on-line informace, výměnné a burzovní systémy atp. Ty mohou přinášet nové, dosud právně ne dostatečně ošetřené situace. Kupř. prodej nahrávek a distribuce softwaru nejsou vzásadě nic nového. Donedávna však byly vždy spojeny s dodáním hmotného nosiče, na kterém bylo dílo zaznamenáno. Potřeba hmotného média odpadla s prodejem audiovizuálních nahrávek a softwaru po internetu tak, že si je kupující nechá zaslat elektronickou cestou nebo získá možnost si je po sítí přenést k sobě (stáhnout). Jak již bylo naznačeno shora, nese to s sebou jisté problémy, např. místo plnění v klasickém právním chápání lze určovat jen s obtížemi. V případě neoprávněného nakládání s takovýmito obchodovanými daty může být stejně tak i problém s určením místa vzniku škody. V případě odstoupení od smlouvy nebo zrušení smlouvy může být zásadní problém s vracením plnění – zatímco u nehmotných statků na hmotných nosičích lze nosič vrátit a lze ověřit jeho neporušení a nevybalení, u čistě imateriálních statků to nelze a „vrácení" plnění může být ryze imaginární. Poněkud lepší, i když pramálo zmapovaná, je možnost uplatňování odpovědnosti z vad, což se může týkat i softwaru dodávaného čistě elektronickou formou. V případě přeshraničního vztahu se tedy můžeme setkat s řadou poměrně obtížně řešitelných otázek, které ovšem bude nutno zodpovědět pro určení rozhodného práva, pokud si je strany nesjednaly, popř. pravomoci národních soudů.

7. PARALELNÍ PLATEBNÍ A QUASI-PLATEBNÍ SYSTÉMY

S rozvojem obchodování po internetu logicky rostla potřeba efektivního platebního styku. Kromě ze své podstaty velmi zranitelného systému platebních karet a bankovních převodů se tak začaly rozvíjet další platební systémy. Vedle zlepšených a zabezpečených způsobů peněžních transakcí po internetu (jaké třeba nabízí v ČR eBanka) se začaly vyskytovat i platební systémy, kde zúčtovací jednotkou nejsou reálné peníze, ale vlastní elektronické peníze – „peněžní" jednotky nebo ekvivalent hmotnosti zlata (systémy). Tyto systémy se používají od mikroplateb (např. nákupy melodií do mobilního telefonu), kde se prostředky často sbírají za věrnost návštěvníkům stránek (a odpovídající počet shlédnutí reklam) až po velké převody peněz. Některé systémy jsou zcela nesměnitelné, většinou však existuje pevný nebo pohyblivý kurz k nějaké reálné měně. Elektronické peníze se pak dají nakoupit například prostřednictvím platební karty. Kromě nákupů drobných služeb (zejména informací a audiovizuálních nahrávek) se tyto peníze začaly čím dál více používat i k placení per se.

S používáním elektronických peněz, nejen v mezinárodněprávním kontextu, se pojí řada potenciálních problémů.

Z veřejnoprávních problémů je vedle samotné otázky legality takového systému třeba zmínit riziko daňových úniků, praní špinavých peněz, nedostatek úpravy ochrany a pojištění vkladů a v neposlední řadě snížení efektivnosti monetární a částečně fiskální politiky. Tyto problémy by se vyskytly v citelné míře zejména tehdy, kdy by poměr elektronických peněz k standardní měně dosáhl nezanedbatelnou výši. Pak by docházelo k citelnému ovlivnění měnových kurzů, ale i úrokových sazeb a hospodářského růstu. Protože se fakticky jedná, s výjimkou mikroplateb a podobných bagatelních systémů, o náhražku tuzemské měny, je provozování systému elektronických peněz v České republice nelegální podle § 144 trestního zákona, který zakotvuje skutkovou podstatu ohrožování oběhu tuzemských peněz. Toto ustanovení stanoví, že ten, kdo neoprávněně vyrobí nebo vydá náhražky tuzemských peněz, nebo kdo takové náhražky neoprávněně dává do oběhu, bude potrestán odnětím svobody až na šest měsíců nebo peněžitým trestem.

Dalším problémem je, že se elektronické peníze používají čím dál častěji k platbám v kyberprostorovém podsvětí. Platba na e-gold je zcela běžným způsobem honorování hackerských aktivit. Její vysoká anonymita, nedostupnost a neprůhlednost ve vztahu k orgánům státní moci a značná flexibilita tyto systémy pro takové zneužití přímo předurčuje. Takřka samozřejmostí je, že transakce se realizují na neexistující nebo odcizené identity.

Ze soukromoprávních aspektů je třeba zdůraznit problematičnost a neupravenost směny elektronických peněz za standardní měnu. V mezinárodním hledisku jsou pak převody elektronických peněz ve většině států neupraveny nebo dokonce nelegální (v řadě zemí je podobně jako v České republice provozování paralelního měnového systému nezákonné). Uživatel takového systému je tedy více ohrožen a vystaven většímu nebezpečí finanční ztráty.

Celkově lze tedy doporučit se takovýmto systémům, snad s výjimkou mikroplateb, vyhnout.

8. TECHNICKÁ SLOŽITOST

Mezinárodní prvek vnáší do oblasti závazkových vztahů v kyberprostoru obtíže nejen právní, ale i technické a administrativní. Přes neustále se rozvíjející kooperaci mezi státy na vládní, policejní i soudní a legislativní úrovni, jsou hranice v hmotném světě pořád podstatně citelnější bariérou než je tomu v kyberprostoru. Na tyto bariéry pak naráží osoba, která se snaží domoci svého práva, ať už vyplývajícího z občanskoprávního vztahu nebo práva poškozeného na náhradu škody v případě trestné činnosti. Kromě již uvedených právních překážek, zejména nutnosti aplikovat zahraniční právo nebo se účastnit řízení před zahraničním soudem, musí taková osoba čelit dalším překážkám. Při komunikaci se zahraničními soudy a jinými orgány je velmi pravděpodobné, že bude muset kvůli vzdálenosti a národním specifikům vyhledat pomoc zahraničního advokáta, byť nebude zastoupení účastníka povinné. Narozdíl od komunikace po internetu, kde vládne angličtina, musí počítat s náklady na překlady do místního jazyka, což nese nejen finanční ale i časové náklady. V případě technicky složitějších případů bude nezbytná znalecká expertíza, která spolu opět nese náklady a ztrátu času. Pakliže bude potřeba spolupráce poskytovatelů internetového připojení, bude u zahraničních poskytovatelů v rámci občanskoprávního řízení bez pomoci soudu velmi obtížné získat potřebné informace o datových přenosech.

V případě náhrad škody z trestné činnosti, kdy pachatelé záměrně komplikují situaci přenosy mezi mnoha státy, bude potřeba spolupráce policie řady států a rovněž spolupráce poskytovatelů internetového připojení v těchto zemích. Pokud spolupráce není dostatečně rychlá, dopadení pachatele a následné vymožení náhrady škody je velmi nepravděpodobné. Další komplikací je fakt, že policie není dostatečně odborně ani materiálně vybavená pro vyšetřování počítačové kriminality. Osobně jsem byl svědkem situace, že při provedení neodkladného úkonu – výslechu poškozeného cizince, který nafotografoval na digitální fotoaparát pachatele trestného činu, nemělo celé místní oddělení Policie ČR jediný počítač s USB konektorem, aby bylo možno fotografie z fotoaparátu přenést. Ačkoliv se i tato situace zlepšuje, počítačoví zločinci jsou minimálně o několik kroků napřed. Situace českých soudů je o něco lepší než situace policie. Jednak je technické vybavení soudů na poněkud vyšší úrovni a hlavně na činnost soudu není kladen takový technický nárok jako na policii. Samotné dokazování počítačové kriminality je totiž v řízení před soudem již věcí znaleckou a na soud jsou tak kladeny menší odborné i technické nároky, které se víceméně omezují na případnou vizuální reprodukci.

K obtížnosti situace přispívá, že se počítačová trestná činnost stává čím dál sofistikovanější a zároveň rychlejší. Pachatelé trestné činnosti využívají odcizené identity, odcizené platební karty a přístupy k účtům, přístupy na servery i internetové domény. Po spáchání trestné činnosti proto bez obav z odhalení opouštějí zneužité údaje a začínají používat nové. Pouhé sledování takovýchto aktivit v rámci jedné země v dostatečném tempu je tedy velmi obtížné. Bez perfektní nadnárodní spolupráce pak nemožné.

9. ZÁVĚR

Pro bezpečný pohyb v kyberprostoru je (samozřejmě kromě nezbytné opatrnosti a dostatečného technického zabezpečení uživatelů) potřeba co nejtěsnější a hlavně nejrychlejší spolupráce národních policií, státní správy i soudů všech států. Je nepochybné, že i při pozitivním trendu v tomto směru budou stále státy, které budou zločincům v kyberprostoru značně ulehčovat život, ale zrychlení a zlepšení spolupráce zvýší bezpečnost v každém případě. Jako nereálné se mi jeví někdy navrhované rozšíření pravomoci národních soudů zemí, které počítačovou trestnou činnost důsledně stíhají, vůči pachatelům, kteří se zdržují v zemích, které tuto kriminální oblast ignorují, pakliže není založena jejich pravomoc jinak. Jednak se mi jeví takový postup, s výjimkou nejvážnějších trestných činů jako je např. genocida, jako poněkud sporný a jednak by měl patrně minimální efekt s ohledem na to, že by pachatelé stejně nebyli vydáni. Dalším nezbytným krokem je technické a odborné posílení orgánů činných v trestním řízení tak, aby vůbec bylo možno zločin v kyberprostoru vyšetřovat. V neposlední řadě je potřeba pružně přizpůsobovat legislativu technickému pokroku, aby byly podchyceny situace na které právní úprava nemohla myslet, popř. aplikace stávající úpravy se jeví jako nevhodná a obsoletní. Zároveň je důležité akcentovat ochranu spotřebitele, jehož postavení by bez ní bylo v kyberprostoru ještě podstatně slabší než v hmotném světě.

LITERATURA

http://eur-lex.europa.eu/
Hellman, D. New Directions in Cryptography. IEEE Transaction On Information Theory, 1976.
Chleboun, M. Stav internetové kriminality v Česku. http://www.lupa.cz/.
Knapp, V. a kol. Občanské právo hmotné I. Praha: Codex, 1997.
Knapp, V. a kol. Občanské právo hmotné II. Praha: Codex, 1997.
Kubec, T. Povaha internetu z hlediska práva. Obchodní právo, 2000, č. 9.
Kubec, T. Právo elektronického obchodu v mezinárodním kontextu. Praha, 2004.
Kučera, Z. Mezinárodní právo soukromé. Brno: Doplněk, 2004.
Miklík, A. Vyšetřování kyberzločinů: jaká je realita?
http://www.Wikipedia.org/.

EINIGE INTERNATIONAL-RECHTLICHE GESICHTSPUNKTE DES SCHULDVERHÄLTNISSES, DAS IN KYBERNETISCHEM RAUM ENTSTEHEN

Zusammenfassung

Der Autor spricht in dem Artikel über rasende Entwicklung der Informatik und Telekommunikation in der letzten Zeit und über das, was das mitbringt. Unter die problematischen Bereiche, die erhöhte Aufmerksamkeit verdienen, nach der Meinung des Autors fallen: ausdrucksvolle Zunahme des grenzübergreifenden Elements und somit international-rechtlicher Charakter der Beziehungen, neue Formen von Kontraktion und Willensbestimmung allgemein (die Verträge, die im Internet kontrahiert sind), neue

Formen der Leistung (Software und audiovisuelle Aufnahmen, die durch Internet eingekauft und geliefert werden), das Zahlungssystem und Quasizahlungssystem und die technische Kompliziertheit der Untersuchung und Betrachtung der Streite. Im Verschluss schlägt der Autor vor, was man verbessern kann, um die Bewegung im Kyberraum zu entschärfen.

Schlagwörter: grenzübergreifendes Element, die Gerichtsbarkeit, die Zuständigkeit, entscheidendes Recht, die Willensbestimmung, elektronische Unterschrift, die Form der Leistung, elektronisches Geld

Klíčová slova: přeshraniční prvek, pravomoc, příslušnost, rozhodné právo, projev vůle, elektronický podpis, forma plnění, elektronické peníze

2008 ACTA UNIVERSITATIS CAROLINAE – IURIDICA 4 PAG. 65–78

PEER-TO-PEER SÍTĚ Z HLEDISKA TRESTNÍHO PRÁVA

TOMÁŠ MINÁRIK
Ministerstvo obrany České republiky

1. ÚVOD

Peer-to-peer sítě, přesněji sítě založené na architektuře peer-to-peer (dále jen „P2P sítě"), jsou významným technickým, kulturním a sociálním fenoménem přelomu tisíciletí. Umožňují svým uživatelům, jejichž počet lze nyní vyjádřit osmiciferným číslem, vzájemně si poskytovat data, přičemž významná část těchto uživatelů při poskytování dat porušuje práva k autorským dílům, která jsou těmito daty reprezentována. Toto masové porušování působí vrásky na čele představitelům hudebního, audiovizuálního a softwarového průmyslu, kteří se cítí být ochuzováni o své zisky z výroby a distribuce nehmotných produktů. Zejména hudební vydavatelství se potýkají s dlouhodobým trendem poklesu počtu prodaných nosičů a s tím souvisejících tržeb a tento pokles kladou z velké části za vinu P2P sítím. Z pohledu těchto „obchodníků s obsahem" tedy představují P2P sítě hrozbu, které je nutno čelit.

Oproti tomu uživatelé P2P sítí jsou nadmíru spokojeni, protože se za vedlejší náklady na internetové připojení mohou dostat k obsahu, za který by při pořizování jiným způsobem zaplatili nemalou cenu, nehledě na to, že některý obsah je v daném místě a čase dostupný opravdu pouze prostřednictvím P2P sítě. Za současného právního a technického stavu se jim vyplatí i riziko spojené s případným porušováním práva, protože jen málokteré z nich za porušení stihne sankce (civilní, administrativní, trestní).

Tento rozpor mezi autory, obchodníky a jejich (potenciálními) zákazníky je neblahý pro celou společnost. Platné právo je hromadně porušováno a sankce jsou zřídkavé, ale doposud těžko předvídatelné. Mimoto se někdo musí věnovat vymáhání práva a ať náklady s ním spojené nakonec nese nositel práva, jeho porušovatel nebo stát, pro společnost jako celek je to ztráta. Nabízí se proto i otázka, zda neexistuje praktičtější právní úprava, potažmo distribuční model, které by ve svých důsledcích znamenaly větší celkový užitek pro společnost, berouce v úvahu i účinnou podporu autorské tvorby.

Přestože se v tomto příspěvku zaměřuji na právní aspekty užívání P2P sítí, zejména na aspekty současného trestního práva hmotného a procesního, pokusil jsem se zhodnotit situaci i z hlediska možného technického a právního vývoje. Jedná se přitom o otázky navýsost etické a politické, neboť se týkají objemu a způsobu přerozdělová-

ní prostředků od uživatelů k tvůrcům nehmotných statků a možností vymáhání práva v informační společnosti.

2. DEFINICE „PEER-TO-PEER SÍTĚ"

Peer-to-peer znamená v angličtině „rovný s rovným", což ve zkratce vystihuje podstatu architektury P2P sítě. V takové síti spolu komunikují uživatelé (klienti) přímo, bez zprostředkování komunikace pomocí specializovaných počítačů – serverů. Definičním znakem čisté P2P sítě je pravidlo, že každý počítač k ní připojený slouží **zároveň jako klient i jako server**[1], tedy že všechny připojené počítače jsou si podle jejího protokolu „rovny". Proto se také místo pojmu „klient" používá označení „peer".

Základní výhodou P2P architektury oproti tradiční architektuře klient-server je to, že celková dostupná přenosová kapacita P2P sítě roste s počtem připojených uživatelů. Oproti tomu v tradičních sítích je přenosová kapacita limitována kapacitou serverů, takže nárůst počtu klientů snižuje efektivitu sítě. Co je zde řečeno o přenosové kapacitě, může u některých P2P sítí platit i pro výpočetní výkon a úložný prostor.

Čisté P2P sítě se vyskytují velmi vzácně, protože málokterá síť používá protokol, který by vůbec nepočítal s pojetím serveru a klienta. V některých P2P sítích tak existují specializované počítače, které slouží například k počátečnímu navázání komunikace mezi klienty. Některé P2P sítě mimoto využívají prvky tradiční architektury, například DNS (Domain Name System).

P2P sítě lze třídit podle mnoha kritérií, ale z hlediska forenzního je nejdůležitějším kritériem úroveň centralizace takové sítě. Důvod je nasnadě: čím více je síť centralizovaná, tím více údajů o jejích uživatelích bývá soustředěno na jednom místě. Nejstarší sítě měly jediné centrum, ve kterém byly uloženy údaje o klientech a jimi poskytovaných souborech a které klientům zprostředkovávalo spojení. Proti takovým sítím se dalo právně zakročit a vyřazením centra vyřadit z provozu celou síť, jak se stalo například v případě Napster.[2] Novější sítě mají center více (např. DC++, BitTorrent). V těchto případech se dá nanejvýš zakročit proti konkrétním uživatelům porušujícím právo, což se sice děje, ale pouze namátkově.[3] Opatrnější porušovatelé navíc používají sítě zajišťující anonymitu (např. Freenet). Tyto sítě zatím nejsou příliš rozšířené, protože anonymita bývá na úkor efektivity stahování, ale jistě by se více rozmohly při zesilování represe.

Určitý prvek anonymizace se vyskytuje v sítích typu friend-to-friend (dále jen „F2F"). V F2F sítích může uživatel navázat přímý kontakt pouze s těmi uživateli, které zná, ať už osobně, nebo z kyberprostoru, a kterým důvěřuje („friends"). Ostatní uživatelé jej mohou kontaktovat pouze zprostředkovaně, skrze nepřerušenou linii „přátel", přičemž jeho identita jim zůstává skryta a data putující linií „přátel" bývají zašifrována.

---

[1] http://en.wikipedia.org/wiki/Peer-to-peer, všechny internetové odkazy ověřeny 29. 12. 2008.
[2] http://news.bbc.co.uk/1/hi/entertainment/852283.stm.
[3] http://www.cpufilm.cz/rozsudky.html.

Pro úplnost je ještě nutno uvést, že P2P sítě mohou sloužit i jiným účelům, než je výměna souborů. Nejznámějším takovým účelem je internetová telefonie (např. program Skype). V češtině se proto pro takové typy P2P sítí, ve kterých probíhá hromadná výměna datových souborů mezi uživateli, někdy používá přesnější pojem **„výměnné sítě"**. Vzhledem k tématu této práce jsou v ní oba pojmy používány jako rovnocenné.

3. ZNEUŽÍVÁNÍ VÝMĚNNÝCH SÍTÍ K PROTIPRÁVNÍM AKTIVITÁM

P2P sítě jsou mezi širokou veřejností proslulé zejména jako nástroj k porušování autorského práva. Takovým nástrojem skutečně mohou v rukou nepoučených nebo nepoučitelných uživatelů být. V krajních případech může dokonce existovat takový zájem státu na ochraně autorského práva nebo práv souvisejících, který opravňuje veřejnou moc k použití prostředků trestní represe. Situaci lze nejlépe ilustrovat popisem typického chování člena P2P komunity.

Dejme tomu, že si dnes v České republice majitel počítače s internetovým připojením nainstaluje program umožňující mu připojit se k nějaké výměnné P2P síti, konkrétně například DC++. Program po spuštění uživateli nabídne, aby se připojil k některé z centrál (v terminologii DC++ „hub") a seznámil se se soubory, které nabízejí ke stažení ostatní uživatelé připojení k tomuto hubu. Některé huby vyžadují, aby uživatel sdílel (tj. dovoloval ostatním uživatelům stáhnout od něj) určitý minimální objem dat (např. 20 GB), jinak na hub není vpuštěn.

Práva znalý uživatel, kterému můžeme říkat třeba Pepa456, tedy „nasdílí"[4] 20 GB free softwaru, freewaru a jiného programového vybavení, jehož licence mu k tomuto jednání dává právo, a připojí se k hubu. Tam může buď zkoumat, jaké soubory nabízí jiný konkrétní připojený uživatel, nebo vyhledávat soubory podle názvů. Dá vyhledat film „Skafandr a motýl" a nalezne jej u uživatele Tonda123. Začne film stahovat k sobě do počítače, který za tímto účelem nechá zapnutý přes noc, a ráno si ještě od Tondy123 stáhne poslední album svého oblíbeného pěveckého ansámblu. U počítačové hry, kterou Tonda123 také nabízí ke stažení, zaváhá a s pomocí internetového vyhledávače zjistí, že tato hra je v několika obchodech nabízena za 1499 Kč. S mírným povzdechem ji oželí a svůj počítač konečně vypne.

Uživatel Pepa456, ač to může laikovi připadat podivuhodné, se popsaným jednáním nedopustil žádného porušení práva (alespoň v ČR ne). Ne tak uživatel Tonda123. Ponechme teď stranou případný mezinárodní prvek a nahlédněme pro vysvětlení do autorského zákona[5].

AZ upravuje mimo jiné práva autora k jeho autorskému dílu, práva související s právem autorským a ochranu těchto práv (§ 1 AZ). Autorské dílo coby předmět prá-

[4] Neboli „užije dílo sdělováním veřejnosti" nebo přesněji „zpřístupní dílo veřejnosti v nehmotné podobě" ve smyslu § 18 odst. 1, 2 autorského zákona.

[5] Zákon č. 121/2000 Sb., autorský zákon (dále jen „AZ"); všechny předpisy jsou citovány ve znění k 29. 5. 2008, není-li uvedeno jinak.

va autorského je definováno v § 2 odst. 1 AZ jako „*...dílo literární a jiné dílo umělecké a dílo vědecké, které je* ***jedinečným výsledkem tvůrčí činnosti*** *autora a je* ***vyjádřeno v jakékoli objektivně vnímatelné podobě*** *včetně podoby elektronické, trvale nebo dočasně, bez ohledu na jeho rozsah, účel nebo význam.*“ Následuje demonstrativní výčet druhů děl. Zajímavé je v AZ dvojí možné pojetí počítačového programu; ten může jednak **být autorským dílem** podle § 2 odst. 1 AZ, spadá-li pod tam uvedenou definici jako jedinečný výsledek tvůrčí činnosti autora, jednak může být za autorské dílo **považován** (§ 2 odst. 2 AZ), jestliže je pouze „*původní v tom smyslu, že je autorovým vlastním duševním výtvorem.*“[6]

Nejčastějšími autorskými díly, která uživatelé P2P sítí nabízejí ke stažení, jsou hudební nahrávky (díla hudební), filmy (díla audiovizuální) a software (počítačový program spadající pod § 2 odst. 1 nebo 2 AZ). Je možno objevit i knihy v elektronické podobě (díla literární), obrázky a fotografie (díla výtvarná a fotografická), ale tyto soubory pro svou menší velikost a žádanost netvoří podstatnou část přenesených dat. Mohou však být významné při páchání jiné trestné činnosti, například extremistických nebo mravnostních trestných činů.

Autorská díla jsou autorským zákonem v různém rozsahu chráněna. Pomiňme ochranu autorských práv osobnostních (§ 11 AZ), která obvykle uživatelé P2P sítí nenarušují. Soustřeďme se na právo dílo užít (§ 12 AZ), které patří k právům majetkovým. Bez souhlasu uděleného autorem, nestanoví-li zákon jinak, nelze dílo mimo jiné rozmnožovat, rozšiřovat, pronajímat, půjčovat, vystavovat ani sdělovat veřejnosti, což jsou zákonem výslovně vyjmenované formy užití. Toto právo trvá obecně po dobu života autora a 70 let po jeho smrti (§ 27 odst. 1 AZ), pak se teprve dílo stane tzv. volným dílem (§ 28 odst. 1 AZ) a každý je může bez dalšího volně užít.

Z práva autorského však existují výjimky (§§ 29–39 AZ). Pro účely uživatelů výměnných P2P sítí je nejdůležitější tzv. **volné užití díla** (§ 30 AZ). Podle § 30 odst. 1 až 2 AZ se totiž „*za užití díla podle tohoto zákona ... nepovažuje užití pro osobní potřebu fyzické osoby, jehož účelem není dosažení přímého nebo nepřímého* ***hospodářského nebo obchodního prospěchu****, nestanoví-li tento zákon jinak. Do práva autorského tak nezasahuje ten, kdo* ***pro svou osobní potřebu*** *zhotoví záznam, rozmnoženinu nebo napodobeninu díla.*“ Tato výjimka se vztahuje pouze na zveřejněné dílo (§ 29 odst. 2 AZ). Podle komentáře k AZ[7] § 30 nezakládá nikomu subjektivní právo na pořízení rozmnoženiny, pouze stanoví podmínky, za nichž je dané jednání vyjmuto z režimu autorského práva. Při pořizování rozmnoženiny díla pro osobní potřebu tedy nelze obcházet účinné technické prostředky ochrany práv ve smyslu § 43 odst. 3 AZ.

Aby byly kompenzovány ztráty, které autorům a jiným osobám vzniknou užíváním děl pro osobní potřebu fyzické osoby, existuje v ČR institut zvaný *právo na odměnu v souvislosti s rozmnožováním díla pro osobní potřebu a vlastní vnitřní potřebu* (§ 25 AZ, provedený vyhláškou Ministerstva kultury ČR č. 488/2006 Sb.). Jedná se vlastně o formu zdanění prázdných paměťových médií (a dalších položek), na které je možno ko-

[6] Knappová, M., Švestka, J., Dvořák, J., a kol. Občanské právo hmotné. díl III. Čtvrté, aktualizované vydání. Praha: ASPI, 2007, str. 239.

[7] Telec, I., Tůma, P. Autorský zákon. Komentář. 1. vydání. Praha: C. H. Beck, 2007, str. 348.

pie pro osobní potřebu ukládat, a přerozdělení této „daně" kolektivním správcům ve smyslu AZ. Mezi veřejností si odměna vysloužila přezdívku „výpalné" podle spojení „vypalovat na CD/DVD" (odměna činí např. 40 haléřů, resp. 1 Kč, bez DPH, za nepřepisovatelné CD, resp. DVD). Mnohým se totiž zdá nespravedlivé, že odměnu platí i ti, kdo na médium ukládají jiná data než díla rozmnožená pro osobní potřebu. Některým se také nelíbí, jakým způsobem jsou prostředky získané kolektivními správci přerozdělovány autorům (obvykle podle tržní úspěšnosti autora). Podle jiných zase odměna dává porušovatelům autorského práva jakési morální ospravedlnění jejich činnosti („za prázdná DVD platím, tak si na ně můžu vypálit, co chci").

Proto kdo se připojí k výměnné P2P síti a stáhne si na pevný disk svého počítače film, hudbu, knihu nebo obrázek, tedy dílo ve smyslu AZ, k němuž trvají majetková práva a licence jeho volné šíření zakazuje, užívá dílo pro osobní potřebu dovoleným způsobem. Konkrétně pořizuje rozmnoženinu díla podle § 30 odst. 2 AZ. Podle názoru Telce a Tůmy[8] je dokonce oprávněn pořídit rozmnoženinu této rozmnoženiny (např. „vypálit" film na DVD), pokud to bude pro jeho osobní potřebu a bude stále splňovat podmínky tzv. tříkrokového testu v § 29 odst. 1 AZ. Žádnou z těchto rozmnoženin nesmí pak rozšiřovat, pronajímat, půjčovat, vystavovat ani sdělovat veřejnosti (tedy ani sdílet na P2P síti, neboli zpřístupňovat dílo veřejnosti počítačovou sítí – § 18 odst. 2 AZ).

Výše uvedená výjimka „užití pro osobní potřebu" se však nevztahuje na důležitou skupinu souborů stahovaných v P2P sítích, jíž jsou **počítačové programy** neboli software (dále jen „programy"), včetně počítačových her. Programy jsou obecně chráněny jako dílo literární (§ 65 odst. 1 AZ) od okamžiku, kdy byly vyjádřeny v objektivně vnímatelné podobě (§ 9 odst. 1 AZ). Programy lze třídit podle jejich licencí na free software a proprietární software, který zahrnuje shareware, freeware a placený software[9]. Důležité je, že některé licence mohou dovolit uživateli programu takové jednání, které AZ obecně zakazuje. Podléhá-li program např. licenci GNU GPL, lze jej užívat, šířit, zkoumat a pozměňovat za podmínky, že výsledný program bude také podléhat licenci GNU GPL.

Podle § 30 odst. 3 AZ programy nelze užít pro osobní potřebu mimo režim AZ. Pořízení byť jediné rozmnoženiny v rozporu s licenční smlouvou, ač pro vlastní osobní potřebu, se považuje za zásah do autorského práva[10]. U programů se uplatní pouze § 66 AZ, omezení rozsahu práv autora k počítačovému programu. *Oprávněný uživatel* rozmnoženiny programu (definice v § 66 odst. 6 AZ) smí do programu zasahovat a rozmnožovat jej za účelem jeho plného využívání (konkrétně viz § 66 odst. 1–3 AZ). Podle § 43 odst. 1 AZ ale ani on nesmí obcházet **účinné prostředky ochrany práv**, což může být třeba nutnost mít vloženo DVD v mechanice při spuštění programu. „Účinné prostředky ochrany práv" je poměrně zavádějící zákonný termín, jehož význam je vyložen v § 43 odst. 3 AZ. Obejít účinné prostředky ochrany práv, a to nejen k softwaru, ale i k jiným digitalizovaným dílům, lze nejsnáze s pomocí speciálního programu zvaného „crack", který tuto ochranu odstraní. Cracky se sice v P2P sítích

[8] Telec, I., Tůma, P. Autorský zákon. Komentář. 1. vydání. Praha: C. H. Beck, 2007, str. 347.

[9] Stručné definice viz například na http://en.wikipedia.org nebo http://cybercrime.webgarden.cz.

[10] Kříž, J., Holcová, I., Kordač, J., Křestanová, V. Autorský zákon a předpisy související – komentář. 2. aktualizované vydání podle stavu k 1. 9. 2005. Praha: Linde Praha a.s., 2005, str. 126; výklad platí i pro současné znění.

vyskytují, ale díky své malé velikosti se dají najít jinde na internetu[11]. Použití cracku je zakázáno v § 43 odst. 1 AZ, jiné druhy nakládání s crackem jsou zakázány v § 43 odst. 2 AZ.

Některá díla mohou být chráněna i **elektronickou informací o správě práv k dílu** (§ 44 odst. 2 AZ), kterou je zakázáno bez svolení autora měnit a odstraňovat (§ 44 odst. 1 písm. a) AZ). Taktéž je mimo jiné zakázáno sdělovat veřejnosti (tj. sdílet na P2P síti) dílo s odstraněnou informací o správě práv (§ 44 odst. 1 písm. b) AZ).

Shrňme tedy úpravu v autorském zákoně a aplikujme ji na P2P sítě. **Legální** samo o sobě je připojit se k P2P síti. Legální je i sdílet volná díla, tj. díla, jejichž poslední autor zemřel před více než 70 lety, což prakticky přichází v úvahu pouze u některých děl literárních. Jinak je možno sdílet pouze taková díla, u nichž to dovoluje licenční smlouva. Je povoleno stahovat pro osobní potřebu jakékoli dílo kromě děl uvedených v § 30 odst. 3 AZ.

Nelegální je sdílení všech autorských děl, kterým dosud nevypršela doba ochrany, a stahování počítačových programů či elektronických databází. Nelegální je taktéž stahování cracků, tedy nástrojů k obcházení účinných prostředků ochrany práv, a samozřejmě jejich aplikace. S tím úzce souvisí i zákaz měnit a odstraňovat elektronickou informací o správě práv k dílu, a takto upravené dílo užívat (např. sdílet). Všechna tato jednání jsou samozřejmě nelegální pouze tehdy, jsou-li v rozporu s příslušnou licenční smlouvou.

Blanketní dispozicí § 152 odst. 1 trestního zákona[12], je do trestního práva vlastně „vtaženo" celé právo autorské. Neznamená to ale, že by každé porušení autorského práva mělo být postihováno podle trestního zákona. Je třeba brát v potaz zejména zásadu subsidiarity trestního práva, která je dlouhodobě vyjadřována jak v judikatuře, tak v praxi, a má se výslovně objevit v připravovaném trestním zákoně[13] coby náhrada materiálního znaku trestného činu v současném pojetí (§ 12 odst. 2 NTZ). V situaci, kdy existuje poměrně kvalitní soukromoprávní ochrana autorů, nelze k prosazování soukromých zájmů zneužívat prostředky trestní represe, jestliže chybí veřejný zájem opravňující jejich použití.[14]

Jiným případem je šíření závadných materiálů (např. extremistická propaganda, dětská pornografie) prostřednictvím P2P sítí. U těchto činů bývá trestní represe plně na místě. Převážná většina P2P komunity má k pachatelům těchto činů negativní postoj, o čemž svědčí například pravidla na většině DC++ hubů a zakazování přístupu („banning") uživatelům za sdílení závadných materiálů[15]. Otázkou je, do jaké míry jde o morální postoj provozovatelů hubu a do jaké míry se provozovatelé pouze snaží ne-

[11] http://www.crackdb.org/.
[12] Zákon č. 140/1961 Sb., trestní zákon (dále jen „TZ").
[13] Návrh trestního zákoníku (dále jen „NTZ") podle sněmovního tisku č. 410, volební období (2006 –). Čísla paragrafů NTZ jsou uváděna podle této verze. Dokument je dostupný na http://www.psp.cz/sqw/text/tiskt.sqw?O=5&CT=410&CT1=0.
[14] K prolínání práva autorského a trestního viz zásadní nález I. ÚS 69/06 (k trestnosti reprodukce děl bez smlouvy s kolektivním správcem autorských práv).
[15] Viz např. http://bestofallhub.com/Pravidla.php.

upoutávat zbytečně pozornost orgánů činných v trestním řízení. Je však zřejmé, že extremisté a konzumenti dětské pornografie nebudou své „záliby" příliš prosazovat na veřejných P2P sítích, ale spíš budou využívat soukromých sítí typu F2F a spoléhat na osobní kontakt.

V souvislosti s dětskou pornografií je třeba upozornit na úpravu účinnou od 1. 12. 2007, a sice §§ 205–205a TZ. Kromě zásadního zpřísnění trestních sazeb zavedla tato novela i trestnost přechovávání dětské pornografie pro vlastní potřebu. K zesilování represe vedl zákonodárce především růst technických možností informačních a komunikačních technologií (dále jen „ICT")[16]. Zatímco dříve existovala dětská pornografie ve formě „papírových" fotografií, negativů, nanejvýše videokazet, které byly ve větším množství relativně nákladné a neskladné, dnes je možno na průměrný pevný disk nového počítače uložit miliony fotografií a tisíce souborů videa. Tomu odpovídá i objem šířené dětské pornografie, ať už osobním kontaktem nebo pomocí počítačových sítí.

Vraťme se ale ke vztahu práva autorského a trestního. Poněvadž měl být návrh trestního zákoníku založen na formálním, nikoli materiálně-formálním pojetí trestného činu, a později se počítalo s oběma variantami, obsahuje § 268 odst. 1 NTZ oproti současné úpravě dvě důležitá slova navíc: „*Kdo neoprávněně zasáhne **závažným způsobem** do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovému záznamu, rozhlasovému nebo televiznímu vysílání nebo databázi, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.*" Bude zajímavé sledovat, jak se s tímto novým znakem vypořádá praxe a zejména judikatura, pokud tedy bude zákoník přijat. Co se P2P sítí týče, pravděpodobně bude finančně vyjádřen minimální práh následku umožňující orgánům činným v trestním řízení zahájit trestní stíhání, potažmo uložit trest.

Tím se dostáváme k zajímavému tématu, kterým je určování výše škody a bezdůvodného obohacení.

4. URČOVÁNÍ VÝŠE ŠKODY A BEZDŮVODNÉHO OBOHACENÍ ZPŮSOBENÝCH PROTIPRÁVNÍM ČINEM V P2P SÍTI

Předpokládejme nyní, že uživatel Tonda123 nějakým způsobem získá a „nasdílí" ve výměnné síti kopii filmu, který byl před několika dny uveden do kin v ČR. Mohl ji získat například tzv. „camcordingem", tedy natočením filmu promítaného v kině na vlastní kameru. Tento postup je výslovně označen v § 30 odst. 3 AZ („*pořízení záznamu audiovizuálního díla při jeho provozování ze záznamu nebo jeho přenosu*") jako výjimka z volného užití, a proto je obvykle zakázaný. Filmy také do P2P sítí unikají pomocí rozmnoženin šířených pro účely filmové kritiky (tyto rozmnoženiny se dají poznat podle nápisu „FOR YOUR CONSIDERATION" probíhajícího spodkem obrazu) nebo cestou nespolehlivých osob spolupracujících na výrobě nebo distribuci filmu.

[16] Důvodová zpráva k zákonu č. 271/2007 Sb.

Předpokládejme dále, že uživatel Tonda123 byl ze všech „pirátů" nejrychlejší a svou kopii filmu dokázal první den rozšířit[17] k 10 dalším uživatelům, od kterých se kopie dále lavinovitě šířila skrze P2P sítě k desetitisícům dalších uživatelů v ČR a neznámému počtu v zahraničí. Bude prokázáno, že tak učinil sice „ze sportu", ale přesto lze dovodit jeho srozumění s tím, že kopie bude rozšířena ke značnému počtu uživatelů P2P sítí. Nyní vyvstávají dvě otázky. Jaká celková škoda byla jeho činem způsobena autorům, potažmo nabyvatelům licence k filmu (distribuční společnost, provozovatelé kin), a za jaký díl této škody odpovídá Tonda123?

Náhrada škody a vydání bezdůvodného obohacení při porušení autorského práva podléhá obecné úpravě občanského zákoníku (§ 40 odst. 4 AZ). Skutečná škoda, *damnum emergens*, při porušení autorského práva prakticky nemůže vzniknout, protože samotné autorské dílo nelze poškodit ani zničit[18]. Celková škoda tak může být tvořena **pouze ušlým ziskem**, který spočívá v příjmu, který autorovi ušel tím, že v důsledku protiprávního jednání jiné osoby došlo ke znemožnění užití díla autorem samotným nebo třetí osobou s jeho souhlasem[19]. Podle § 40 odst. 4 AZ se autor místo skutečně ušlého zisku může *„domáhat náhrady ušlého zisku ve výši odměny, která by byla obvyklá za získání takové licence v době neoprávněného nakládání s dílem"*.

Od ušlého zisku je nutno odlišit **bezdůvodné obohacení** na straně neoprávněného uživatele díla, které je tvořeno úsporou nákladů na získání licence obvyklou cestou a které má navíc sankční funkci a výši (*„dvojnásobek odměny, která by byla za získání takové licence obvyklá v době neoprávněného nakládání s dílem"*). Podle Telce a Tůmy[20] **je náhrada autorské odměny ušlé neoprávněným užitím díla nárokem z odpovědnosti za bezdůvodné obohacení a nikoli odpovědnosti za škodu**. Totéž vyslovuje i nedávná judikatura (NS 4 Tz 124/2004, NS 5 Tdo 160/2005). Tato zásada platí i v trestním řízení. Lze tedy vyslovit s určitou humornou nadsázkou, že sdílení nikomu neškodí.

Podle současné úpravy nelze v adhezním řízení rozhodovat o bezdůvodném obohacení[21] (srovnej § 43 odst. 3 trestního řádu[22]). „Poškození" autoři nebo nabyvatelé licencí by tak vůbec neměli mít postavení poškozeného podle TŘ. Zároveň ale podle jiného komentáře k autorskému zákonu[23] je možno pod pojem „škoda" pro účely trestní odpovědnosti (např. podle § 152 odst. 1, 2 TZ) zahrnout i bezdůvodné obohacení. To je ale možná zbytečně extenzivní výklad. Judikatura totiž uznává charakter bezdůvodného obohacení coby neoprávněného prospěchu jako znaku skutkové podstaty trestného činu, např. u trestného činu podílnictví podle § 251 odst. 1 TZ[24]. Musíme tedy opustit

[17] Samozřejmě se nemyslí rozšiřování díla ve smyslu § 14 odst. 1 AZ, ale zpřístupňování díla veřejnosti ve smyslu § 18 odst. 1, 2 AZ. Výraz „šíření" je v článku použit proto, že působí přirozeněji.

[18] Telec, I., Tůma, P. Autorský zákon. Komentář. 1. vydání. Praha: C. H.Beck, 2007, str. 434.

[19] Tamtéž.

[20] Tamtéž.

[21] Musil, J., Kratochvíl, V., Šámal, P., a kol. Kurs trestního práva. Trestní právo procesní. 3. přepracované a doplněné vydání. Praha: C. H. Beck, 2007, str. 866.

[22] Zák. č. 141/1961 Sb., o trestním řízení soudním (trestní řád), dále jen „TŘ".

[23] Kříž, J., Holcová, I., Kordač, J., Křesťanová, V. Autorský zákon a předpisy související – komentář. 2. aktualizované vydání podle stavu k 1. 9. 2005. Praha: Linde Praha a.s., 2005, str. 146; výklad platí i pro současné znění.

[24] Rozsudok Najvyššieho súdu SSR zo dňa 30. 10. 1979, sp. zn. 1 Cz 82/79.

výše položené otázky o výši škody a ptát se raději: Jak moc se jednotliví uživatelé P2P sítě bezdůvodně obohatili na úkor autorů?

Bezdůvodné obohacení **nevzniká** na straně fyzických osob, které si film legálně stáhly (pořídily rozmnoženinu a neobešly účinné technické prostředky ochrany práv), užívají jej pro osobní potřebu a dále jej nešíří (nesdělují veřejnosti). Nazvěme tyto osoby pracovně „koncoví uživatelé". Bezdůvodné obohacení naopak **vzniká** těm osobám, které film v P2P síti šíří („šiřitelé"), a to ve výši dvojnásobku obvyklé odměny (§ 40 odst. 4 AZ). Tuto odměnu je v uvedeném případě (film) možno vyčíslovat podle tzv. licenčních distribučních smluv uzavíraných mezi autory, případně jinými majiteli práv k dílu, a distributory.

Tonda123 je v zajímavé situaci. Jeho bezdůvodné obohacení se má posuzovat podle § 40 odst. 4 AZ podle práva občanského. Ale ke vzniku bezdůvodného obohacení podle teorie občanského práva není třeba zavinění[25]. Není dokonce ani třeba žádného jednání obohaceného („protiprávního úkonu") a tím pádem ani kauzálního nexu. Jaký tedy bude vztah bezdůvodného obohacení a následku trestného činu Tondy123 podle § 152 odst. 1 TZ? Tato otázka má i praktický význam pro kvalifikaci, protože zvlášť přitěžující podmínkou v § 152 odst. 2 písm. a) TZ je získání „značného prospěchu", za nějž lze bezdůvodné obohacení považovat.

Při stanovování trestní odpovědnosti je především třeba dodržet zásadu odpovědnosti za zavinění. Můžeme proto prospěch získaný trestným činem vypočítávat podle § 40 odst. 4 AZ jako bezdůvodné obohacení, ale zároveň musíme sledovat naplnění všech znaků skutkové podstaty trestného činu, a to včetně protiprávnosti, jednání, příčinného vztahu, následku, zavinění atd.

Tonda123 byl první, kdo sdílel kopii filmu v P2P síti. Musel být srozuměn s tím, že tato kopie se prostřednictvím protiprávních činů dalších šiřitelů časem rozšíří ke všem uživatelům, kteří film chtějí vidět. Tento následek jeho jednání nastal a on jej úmyslně zavinil. Sledujme nyní **příčinný vztah** mezi jednáním a následkem z hlediska práva trestního. Jednání Tondy123 bylo právně relevantní příčinou (*conditio sine qua non*) celkového následku, v okamžiku spáchání činu dokonce jedinou příčinou. Do hry vstupují další šiřitelé, bez nichž by se film nikdy nedostal ke všem koncovým uživatelům. Poněvadž ale Tonda123 s jejich činností byl srozuměn, není příčinný vztah přerušen.[26] Slabým modifikátorem je pouze gradace příčinné souvislosti, která může odpovědnost Tondy123 přesunout více či méně na následné šiřitele. V zásadě je ale za celkové rozšíření díla plně odpovědný.

Následní šiřitelé sdíleli film až ve chvíli, kdy už jeho kopie putovala kyberprostorem mezi mnoha dalšími počítači. Proto je u jejich činů příčinný vztah do značné míry oslaben nedostatkem zavinění a díky gradaci příčinné souvislosti. Oni byli srozuměni s tím, že si od nich film někdo stahuje, a za **bezprostřední šíření** filmu k přímému sousedovi odpovídají. Zároveň odpovídají za sdílení díla *per se* (sdělování veřejnosti,

[25] Knappová, M., Švestka, J., Dvořák, J., a kol. Občanské právo hmotné. Díl II. Čtvrté, aktualizované vydání. Praha: ASPI, 2005, str. 570.

[26] Novotný, O., Vanduchová, M. a kol. Trestní právo hmotné – I. Obecná část. 5., jubilejní, zcela přepracované vydání. Praha: ASPI, a.s., 2007, str. 178.

§ 18 odst. 1, 2 AZ). Avšak už neodpovídají za rozšíření filmu v celé síti a potažmo v celém veřejném kyberprostoru, protože správně předpokládali, že jejich činnost je pro finální rozšíření filmu prakticky bezvýznamná, což je z odpovědnosti za další šíření vyjímá. Přičitatelný následek jejich činu je tak výrazně méně významný než u prvního šiřitele a to podle mého názoru v drtivé většině případů vylučuje jejich trestní odpovědnost a mění ji na administrativní [§ 105a odst. 1 písm. a) AZ], přičemž občanskoprávní odpovědnost zůstává nedotčena.

Celkové bezdůvodné obohacení určované pro účely trestního řízení proti Tondovi123 bude vždy předmětem hrubého odhadu. Bez vynaložení nepřiměřených prostředků totiž nelze určit přesný počet počítačů, do kterých byl film stažen, a prakticky nemožné je zjistit, jaký počet osob takto získanou kopii filmu zhlédl. Navíc lze jen těžko odhadnout možnost šíření filmu v zahraničí.

Jistě by se daly najít ještě komplikovanější scénáře, jako například šíření různých jazykových verzí díla nebo různě kvalitních kopií postupně uvolňovaných do P2P sítě, nicméně předpokládaný rozsah tohoto příspěvku nás nutí ke stručnosti.

Vytváření ohromných sítí a rozvoj nehmotných statků v informační společnosti staví trestní právo před zajímavé problémy. Při posuzování následků protiprávního šíření autorských děl se dotýkáme limitů zásady individuální odpovědnosti. Aby bylo nalezeno vhodné řešení, bude nutno nahlížet tyto problémy z co největšího počtu úhlů.

5. PROCESNÍ OTÁZKY ZNEUŽÍVÁNÍ P2P SÍTÍ

Spácháním trestného činu vzniká státu právo na potrestání pachatele. Toto právo ale může stát plně realizovat pouze tehdy, pokud trestný čin vyjde najevo, je spolehlivě objasněn, pachatel zjištěn a je mu ve spravedlivém procesu prokázána vina.

Trestná činnost páchaná pomocí P2P sítí (v převážné většině podřaditelná pod § 152 odst. 1 TZ) je na první pohled velmi rozšířená. Počet odsouzených zneužívatelů P2P sítí ale zatím asi není příliš vysoký, soudě také podle počtu rozhodnutí zveřejněných na stránkách České protipirátské unie[27] i jinde. Oficiální statistika bohužel dosud chybí, trestné činy podle § 152 TZ nejsou ve Statistické ročence kriminality za rok 2006 nijak rozlišeny.[28]

Předpokládáme tedy **vysokou latenci** tohoto druhu kriminality. K jejímu odhalování může docházet jednak v důsledku vlastních poznatků orgánů činných v trestním řízení (specializovanou složkou pro tyto případy je v České republice Skupina informační kriminality při Službě kriminální policie a vyšetřování), ale častěji v důsledku oznámení a podnětů jiných osob a orgánů (např. Česká protipirátská unie, Ochranný svaz autorský).

Aby bylo možno trestný čin náležitě zjistit a jeho pachatele potrestat, je potřeba získat důkazy, a to postupem souladným s trestním řádem (zák. č. 141/1961 Sb., o trest-

[27] http://www.cpufilm.cz/rozsudky.html#kabel.
[28] http://portal.justice.cz/ms/soubor.aspx?id=38671, str. 75.

ním řízení soudním, dále jen „TŘ"). Typickými zajišťovacími úkony k obstarání důkazů jsou v případech zneužívatelů P2P sítí odposlech a záznam telekomunikačního provozu a zjišťování údajů o uskutečněném telekomunikačním provozu (§ 88–88a TŘ), následně domovní prohlídka (§ 82–85c TŘ) a vydání, případně odnětí věci (§ 78–79 TŘ).

Zjišťováním údajů o uskutečněném telekomunikačním provozu (§ 88a TŘ) lze především identifikovat osobu, která platí za internetové připojení počítače, s jehož pomocí byl trestný čin spáchán. Příkaz ke zjišťování údajů vydává předseda senátu a v přípravném řízení soudce. Na rozdíl od odposlechu a záznamu telekomunikačního provozu (§ 88 TŘ) není zjišťování údajů vázáno na vymezený okruh trestných činů. Postup při zjišťování údajů je upraven v § 97 odst. 3 zákona č. 127/2005 Sb., o elektronických komunikacích: *„Právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna* ***uchovávat provozní a lokalizační údaje*** *a tyto údaje je na požádání povinna* ***poskytnout*** *orgánům oprávněným k jejich vyžádání podle zvláštního právního předpisu."* Prováděcím předpisem je vyhláška Ministerstva informatiky a Ministerstva vnitra č. 485/2005 Sb., z níž mimo jiné vyplývá povinnost poskytovatelů uchovávat tyto údaje po dobu 6 měsíců (s drobnými výjimkami). Zjišťováním údajů o uskutečněném telekomunikačním provozu nelze zjistit, jaké konkrétní soubory byly přeneseny.

To lze pouze pomocí institutu odposlechu a záznamu telekomunikačního provozu (§ 88 TŘ), který je dále rozpracován v § 97 zák. č. 127/2005 Sb. a vyhlášce Ministerstva vnitra č. 336/2005 Sb. Tento institut je ale vázán na přísnější podmínky než zjišťování údajů o uskutečněném telekomunikačním provozu. Předpokladem pro jeho použití je, aby bylo vedeno trestní řízení pro zvlášť závažný úmyslný trestný čin nebo pro jiný úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva. Další podmínkou je důvodný předpoklad, že budou odposlechem získány skutečnosti významné pro trestní řízení a sledovaného účelu nelze dosáhnout jinak nebo by bylo jinak jeho dosažení podstatně ztížené. Příkaz k úkonu vydává předseda senátu a v přípravném řízení soudce. Tento příkaz se nevyžaduje, dá-li k odposlechu souhlas uživatel odposlouchávané stanice, avšak tento postup lze použít pouze u taxativně vymezených trestných činů (§ 88 odst. 5 TŘ).

První podmínka je v případě některých trestných činů podle § 152 TZ splněna, neboť Česká republika je smluvní stranou Dohody TRIPS[29], která ve svém čl. 61 zavazuje ČR kriminalizovat úmyslné porušení autorského práva v komerčním měřítku. Po zásadní novele § 88 TŘ provedené zák. č. 177/2008 Sb. lze obvykle splnit i druhou podmínku podle § 88 odst. 1 TŘ – „získávání skutečností významných pro trestní řízení" (srovnej dřívější znění § 88 odst. 1 TŘ, které mluvilo o „sdělování skutečností" a nešlo je tak aplikovat na stahování souborů).

Informaci o tom, zda a co daná IP adresa protiprávně sdílí, může policejní orgán ověřit i jednodušeji – připojením se k P2P síti a sledováním chování daného uživatele. Půjde o **sledování** podle § 158d TŘ nespadající pod odst. 3, protože přehled sdíleného obsahu uživatel zveřejnil. Na základě této informace pak může policejní orgán

[29] Dohoda o obchodních aspektech práv k duševnímu vlastnictví, Příloha 1C Dohody o zřízení Světové obchodní organizace, podepsané 15. dubna 1994 v Marrakeši (publikována pod č. 191/1995 Sb.).

požádat soudce o vydání příkazu ke zjišťování údajů o uskutečněném telekomunikačním provozu a po zjištění, kde se daný počítač nachází, o příkaz k domovní prohlídce za účelem zajištění věci důležité pro trestní řízení.

Pokud P2P síť využívá protokol typu torrent (BitTorrent apod.), může být velmi těžké prokázat odpovědnost konkrétního uživatele za sdílení chráněného díla. Přestože každý uživatel při stahování díla přes torrent sdílí již staženou část díla, a tedy zároveň porušuje autorské právo, je velmi obtížné tyto části díla identifikovat a získat tak důvodné podezření podle § 82 odst. 1 TŘ.

I když se podaří získat příkaz k domovní prohlídce, může předmětný počítač užívat více osob a vinu nelze konkrétnímu uživateli prokázat. Pachatelé trestné činnosti ve výměnných sítích ale bývají bez kriminální minulosti a větších zkušeností s trestním stíháním, a proto může být naopak snazší získat jejich doznání.

Co se týče postupu některých kolektivních správců práv nebo jiných osob, které instalují vlastní „nástražný" hub sítě P2P za účelem získání důkazů proti uživatelům, kteří se k tomuto hubu připojí, v úvahu připadá jeho kvalifikace jako trestného činu porušování tajemství dopravovaných zpráv podle § 239 odst. 1 písm. b) TZ, respektive § 240 odst. 1 písm. a) TZ. Jestliže tyto osoby z obsahu zpráv nebo z provozních a lokalizačních údajů v rozporu se zákony (např. TŘ, celní zákon, zákony upravující působení zpravodajských služeb) úmyslně získávají důkazy o tom, že se uživatelé dopouštějí porušování autorských práv, porušují tím jejich právo listovního tajemství zaručené přímo v čl. 13 Listiny základních práv a svobod (vyhlášena pod č. 2/1993 Sb.) a nepřímo specifikované v § 89 odst. 1 zákona č. 127/2005 Sb., o elektronických komunikacích, přičemž před účinností tohoto zákona byl předmět telekomunikačního tajemství definován ještě podrobněji v § 84 odst. 3 zák. č. 151/2000 Sb., o telekomunikacích.

Takto získané údaje jsou přesto použitelné jako důkaz v trestním řízení proti uživatelům porušujícím autorská práva; výjimkou by byla situace, kdy by orgány veřejné moci v rozporu se zákonem k jejich obstarávání soukromou osobou aktivně daly podnět.

6. MOŽNOSTI BUDOUCÍHO VÝVOJE V OBLASTI VÝMĚNNÝCH SÍTÍ

Výměnné sítě mají na společnost dva nesporně negativní dopady. Prvním je ztráta respektu široké veřejnosti k autorskému právu, tedy pokles úrovně jejího právního vědomí v důsledku malé praktické vymahatelnosti práva. Druhým negativním dopadem je naopak růst nákladů na vymáhání práva, který také společnosti jako celku neprospívá.

Pozitivní dopady jsou méně zřejmé. Nejčastěji se uvádí snadnější šíření kulturních statků ve společnosti. Díla se dostanou i k lidem, ke kterým by se při nižším stupni rozvoje ICT nedostala. Výměnné sítě jsou tak úspěšné prostě proto, že jsou levným distribučním kanálem, i s ohledem na (ne)vymahatelnost platného práva. Úspěšně tak konkurují legálním způsobům distribuce a dlouhodobě působí na snižování cen pro „spotřebitele".

Snižování zisků autorů a prostředníků (distributorů obsahu) v důsledku kopírování děl „zadarmo" zároveň nemusí nutně být negativním jevem. Marže rostly téměř po celé dvacáté století. Lze argumentovat tím, že současný stav je jen návratem ke spravedlivému zisku zejména distributorů.

Vycházejíce z těchto předpokladů, můžeme se pokusit odhadnout možnosti budoucího vývoje a uvažovat o řešení stávajících i budoucích problémů pomocí práva, respektive o omezených možnostech práva tyto problémy řešit.

Technické prostředky ochrany práv nemohou být skutečně účinné v situaci, kdy existují počítače s otevřenou architekturou, která umožňuje vynalézavým uživatelům tuto ochranu odstranit. Jakmile je ochrana poprvé prolomena, dílo se dá dále šířit bez ní. Nedovedu si v budoucnu představit situaci, v níž by technické prostředky ochrany práv získaly praktický význam.

Systém **„nepovinné kolektivní licence"** za užívání internetu ke stahování a sdílení jakéhokoli obsahu, jak jej navrhuje Electronic Frontier Foundation (EFF)[30] a jak o něm diskutují odborníci[31], nebyl dosud v České republice předmětem vážnější diskuze. Osobně jej nepovažuji za vhodný, protože podle mého názoru není pro „konzumenty" dostatečně motivující. Proč by někdo platil sebemenší částku za něco, co může mít zadarmo?

Deregulace, tedy určité zmírnění autorského práva vůči „spotřebitelům", například povolení nekomerčního sdílení chráněných děl, by vedla k menší míře porušování práva a dalšímu zlevnění licencí k autorským dílům, přičemž ale nelze dost dobře odhadnout výpadek příjmů na straně autorů. Tento výpadek by musel být kompenzován z veřejných rozpočtů, jestliže by si společnost chtěla udržet kvantitu a potažmo kvalitu autorské tvorby. Autor těchto řádků se sice netají hlubokým odporem ke „kultuře pro masy", která vzkvétá v situaci, kdy jsou v oblasti kultury stále více prosazovány mechanismy volného trhu, tj. když jsou autoři odměňováni přímo úměrně tomu, kolik jedinců je za jejich tvorbu ochotno platit, nicméně učinit autory z velké části závislými na podpoře státu, veřejných institucí a mecenášů, jak tomu bylo v době před existencí autorského práva, také není v moderní demokracii schůdné.

Zřejmě tedy bude zvolen pragmatický přístup. Legální distribuce může P2P sítím konkurovat kvalitou, za níž lidé budou ještě ochotni platit. Film na DVD si za 999 korun koupí jen opravdu zarytý fanoušek nebo bohatý člověk, ale u 40–50 korun za DVD už lze očekávat strmý nárůst prodeje. Ani P2P sítě totiž nejsou zcela zadarmo. Stahování zabírá přenosovou kapacitu. Uskladnění vyžaduje kapacitu pevného disku nebo jiného média, které ale může být dlouhodobě nespolehlivé. Vyhledávání zase zabírá čas. To vše uživatel dává za kopii díla mnohdy nevalné technické kvality. **Zlevnění licencí** je jedinou spolehlivou cestou k omezení porušování práva.

Pokles příjmů autorů a distributorů, který se pravděpodobně bude dále prohlubovat, si možná vyžádá využití jiného zdroje prostředků pro podporu autorské tvorby. Autoři se stanou více závislými na veřejných rozpočtech. Aby výše prostředků nebyla každoročně ovlivňována rozmary úředníků, je některými odborníky navrhován **po-**

[30] http://www.eff.org/wp/better-way-forward-voluntary-collective-licensing-music-file-sharing.
[31] http://citp.princeton.edu/symposium/.

vinný poplatek z internetového připojení[32], který by byl přerozdělován obdobně jako odměna podle § 25 AZ. Tento poplatek by zároveň působil ke zvýšení nákladů na stahování děl přes P2P sítě, čímž by snížil atraktivitu tohoto distribučního kanálu. Někteří z těchto odborníků navrhují, aby v případě zavedení povinných poplatků bylo uživatelům internetu povoleno sdílet jakýkoli obsah. Tato myšlenka zní lákavě, nicméně pro její realizaci ještě podle mého názoru nenastaly vhodné podmínky.

Bude správné zachovat určitou úroveň **trestněprávní ochrany** autorských práv, která by ale měla přicházet v úvahu jen u závažných porušení práva, zejména při snaze udělat si z porušování práva „živnost". Nevýznamné případy by měly být řešeny cestou občanskoprávní a/nebo administrativní. Také odhadování výše způsobené škody, respektive bezdůvodného obohacení, by napříště mělo být citlivější. Jestliže má někdo na pevném disku svého počítače program bez licence a zároveň má tentýž program zálohován na jednom DVD, zdá se absurdní dovozovat, že se dvojnásobně obohatil. Podobná citlivost je na místě i v případě, že osoba má na svém domácím počítači nainstalován velmi drahý komerční software, který ale může reálně využívat jen k prohlížení rodinných fotografií.

Vynakládání větších prostředků na **represi** a vymáhání práva by bylo kontraproduktivní. Díky tomu, že stahování většiny děl probíhá v souladu s pravidlem volného užití, sdílená díla by se jednoduše přesunula na počítače do zahraničí, kde tak silná represe zavedena nebyla, a ke stahování by docházelo nadále. Silnější represe by vyžadovala mezinárodní, snad i celosvětovou koordinaci, a to včetně harmonizace právních úprav. Avšak i kdyby se docílilo této koordinace, začaly by se ve větší míře používat anonymní sítě a náklady na vymáhání práva by se nemusely projevit ve výrazném snížení počtu pirátských kopií.

Proto se domnívám, že současný stav sice může být vnímán jako nevyhovující, ale že k jeho uspokojivému vyřešení nepomůže ani deregulace, ani zvýšená represe. Měla by být zvolena cesta minimálních změn, a to alespoň do doby, než se trh přizpůsobí stavu technického rozvoje. Možnosti práva považuji za velmi omezené.

PEER-TO-PEER NETWORKS FROM A CRIMINAL LAW PERSPECTIVE

Summary

The article describes the legal status of peer-to-peer filesharing in the Czech Republic, with a particular focus on criminal law. It touches on some contentious issues of the borderline between private and public law. Finally, it contains a brief overview of possible legal solutions to the filesharing problem.

Keywords: Peer-to-peer, P2P, file exchange network, file sharing, criminal law, copyright law, unjust enrichment

Klíčová slova: Peer-to-peer, P2P, výměnná síť, sdílení, trestní právo, autorské právo, bezdůvodné obohacení

[32] Peukert, A. A Bipolar Copyright System for the Digital Network Environment. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=801124.

2008 ACTA UNIVERSITATIS CAROLINAE – IURIDICA 4 PAG. 79–90

K NEOPRÁVNĚNÉMU PODNIKÁNÍ V KYBERNETICKÉM PROSTORU
(aneb o internetových sázkových kancelářích v českém právu)

DANIEL PATĚK
Katedra obchodního práva Právnické fakulty Univerzity Karlovy

PETRA PAŤKOVÁ
advokátní kancelář

1. ÚVOD

Vývoj informačních a komunikačních technologií (a rozmach jejich užívání) podstatně rozšiřuje u mnoha oborů podnikání možnost dalšího rozvoje a to především v prostoru internetu. Tak se podnikatelům nabízí možnost účinněji a levněji nabízet a mnohdy i přímo poskytovat své produkty (služby a zboží) prostřednictvím této celosvětové sítě mnohem většímu množství osob, než umožňují klasické provozovny (kamenné obchody). S tím souvisí prudký nárůst smluv uzavíraných se spotřebiteli z jiných států a z toho plynoucí přeshraniční poskytování služeb a zasílání zboží. Kromě zřejmých výhod z tohoto jevu plynoucích[1] se však objevují i jistá rizika. Zřízení internetových stránek, jež je levnější než zajištění a vybavení klasické provozovny, sice přináší podnikateli značné úspory a umožňuje vstup dalších hráčů na trh, na druhou stranu se však zvyšuje riziko, že se prostřednictvím on-line obchodů budou na spotřebitele obracet osoby bez potřebného podnikatelského oprávnění (a často i bez požadované odborné kvalifikace považované za jeden z předpokladů kvality poskytovaných produktů). S tím též roste počet osob, které vstupují na trh s primárním úmyslem dosáhnout zisku ryze protiprávními cestami – úmyslným poskytováním služeb a dodáváním zboží s nižší než deklarovanou kvalitou či vyžadováním záloh se záměrem slíbený produkt nedodat. S rozvojem podnikání v prostředí internetu však může být ohrožována nejen snaha poskytovat dostatečnou ochranu spotřebiteli, ale přímo dotčeny mohou být i zájmy států, jejichž spotřebitelé takto pořizují určité produkty, primárním zde je riziko daňových úniků. Daňovým únikem v této souvislosti přitom rozumíme nejen klasické porušení právních povinností vyplývajících pro poplatníka či plátce z daňových předpisů, ale i situaci, kdy spotřebitelé ve zvýšené míře uspokojují své potřeby u dodavatelů z jiných států, kdy tito nejsou povinni odvádět daně domov-

[1] Např. zvýšení konkurenčního prostředí (vyšší výběr produktů a tlak na snižování ceny) nebo vyšší komfort spotřebitele, který může pohodlně ze své židle před počítačem porovnat nabídky jednotlivých prodejců, kteří mnohdy nabízejí i možnost komfortního porovnání jednotlivých jimi nabízených produktů.

skému státu spotřebitelů. V takovém případě se nejedná o porušení práva, avšak v konečném důsledku se snižuje objem daní vybraných daným státem, což pochopitelně bývá ze strany kompetentních státních orgánů vnímáno jako jev negativní[2].

Konkrétní reakce na fenomén podnikání v kybernetickém prostoru se pochopitelně liší stát od státu ale i v závislosti na konkrétní oblasti podnikání. Obvykle platí, že existují oblasti podnikatelské činnosti, jejichž speciální právní úprava je přísnější než obecný režim podnikání[3]. To je případ též sázkových kanceláří, které budou předmětem zájmu tohoto článku. Přesněji řečeno zkoumán bude pohled českého práva na internetové (on-line) sázkové kanceláře, jimž prostředí internetu zaprvé umožňuje rozvíjet podnikatelskou činnost bez nutnosti vynakládání značných výdajů na kamenné provozovny a za druhé jim umožňuje „přeshraniční poskytování služeb" a to za situace, kdy mnohé národní právní úpravy činí z této činnosti výsostnou oblast pro stát (státní monopoly) nebo pro tuzemské subjekty.

Záměrem tohoto článku tedy není komplexně rozebrat problematiku podnikání v kybernetickém prostoru, ale demonstrovat ji na konkrétním zvoleném druhu podnikatelské činnosti a to internetových sázkových kanceláří. Tato oblast je totiž nyní žhavým tématem jak na úrovni České republiky tak na úrovni Evropské unie. V ČR se tak děje v souvislosti se snahami zakázat či výrazně regulovat (limitovat) možnost internetového sázení. Na komunitární úrovni pak jsou obdobné snahy jednotlivých členských států podrobovány kritickému pohledu pod zorným úhlem svobody volného pohybu služeb. V této souvislosti je třeba zmínit snahu Evropské komise zmapovat (z hlediska právního i ekonomického) evropský trh internetových sázkových kanceláří, čemuž má napomoci zejména zpráva Švýcarského institutu srovnávacího práva[4], která má sloužit jako podklad pro další postup. V současné době totiž není komunitárními předpisy oblast hazardních her harmonizována, proto nelze jednoduše konstatovat, jaká národní regulace je v souladu s komunitárním právem a která je s ním v rozporu. Přesto je nezbytné konfrontovat pravidla stanovená členskými státy pro činnost on-line sázkových kanceláří s obecnými požadavky vyplývajícími ze svobody volného pohybu služeb zakotvené v článku 49 SES.

2. PRÁVNÍ REGULACE SÁZKOVÝCH KANCELÁŘÍ

Veřejnoprávní úprava podmínek podnikání sázkových kanceláří na území ČR je obsažena v zákoně č. 202/1990 Sb., o loteriích a jiných podobných hrách (dále

---

[2] Nemusí se jednat jen o příjmy daňové povahy, ale i o správní poplatky či jiné formy povinných plateb ze strany podnikatelů. Například v dále zkoumané oblasti provozování hazardních her se jedná o odvod na státní dozor ve výši 1 % z příjmu ze sázkových her (sníženého o vyplacené výhry) dle § 29 zákona č. 202/1990 Sb.

[3] Na našem území zakotvený především v živnostenském zákoně (č. 455/1991 Sb.).

[4] Swiss Institute of Comparative Law – Study of Gambling Services in the Internal Market of the European Union (Final Report) – 14 June 2006 (dále jen „SICL Report"). Tato zpráva popisuje platnou úpravu hazardních her jednotlivých členských států, zabývá se i ekonomickými charakteristikami tohoto trhu a jeho možným růstem (zejména v souvislosti s přeshraničním poskytování služeb) a snaží se postihnout možné bariéry volného poskytování služeb (a jejich zdůvodnění národními zákonodárci). Podle výslovného vyjádření se však jedná pouze o studijní podklad pro další činnost Evropské komise a nejde o snahu jednoznačně určit, která z úprav je či naopak není v souladu s požadavky komunitárního práva.

jen „loterijní zákon")[5]. Provozování sázkových kanceláří je jako u ostatních činností regulovaných tímto zákonem založeno na licenčním principu, tj. k takové činnosti musí být vydáno dotyčnému subjektu povolení Ministerstvem financí. Povolení může být vydáno pouze subjektu, který splňuje podmínky stanovené loterijním zákonem a zároveň může i samotné povolení obsahovat konkrétní limity činnosti takového podnikatelského subjektu. Překročí-li některý subjekt provozující sázkovou kancelář tyto mantinely, může být sankcionován ze strany státu (v prvé řadě v rovině správněprávní a to peněžitou pokutou). Pokud však bude někdo provozovat sázkovou kancelář, aniž by k takové činnosti měl uděleno povolení, nastupuje i sankce trestněprávní, neboť v takovém případě bude naplněna skutková podstata trestného činu neoprávněného provozování loterie a podobné sázkové hry podle § 118a trestního zákoníku[6]. Zákonodárce v tomto případě formuluje právě vzhledem ke zvláštnímu zájmu na zachování přísné kontroly hazardních her skutkovou podstatu speciální k trestnému činu neoprávněného podnikání podle § 118 trestního zákoníku. Na rozdíl od obecného trestního postihu neoprávněného podnikání se v případě neoprávněného provozování sázkových kanceláří nevyžaduje větší rozsah takové činnosti, trestným činem proto bude bude i jednorázový akt (např. přijímání sázek v rámci jediné sportovní akce) při naplnění potřebného stupně nebezpečnosti pro společnost[7]. Trestnost takového jednání zůstává zachována též v navrhovaném znění nového trestního zákoníku[8]. Na druhou stranu je nutné připomenout, že české právo nezná trestní odpovědnost právnických osob, které nejčastěji budou provozovateli neoprávněných sázkových kanceláří. Trestní stíhání proto bude možné pouze u fyzických osob, jež jménem nebo v zastoupení takové právnické osoby tuto činnost provozovaly.

---

[5] Za sázkové kanceláře přitom lze podle § 2 tohoto zákona považovat osoby, které provozují následující druhy sázkových her: f) sázkové hry, při nichž je výhra podmíněna uhodnutím sportovních výsledků nebo pořadí ve sportovních soutěžích, závodech a výše výhry je závislá na poměru počtu výherců k celkové výši vkladů (sázek) a předem stanovenému podílu výher; h) sázkové hry, při nichž je výhra podmíněna uhodnutím sportovních výsledků nebo pořadí ve sportovních soutěžích, závodech nebo uhodnutím jiných událostí veřejného zájmu, pokud sázky na tyto události neodporují etickým principům. Výše výhry je přímo úměrná výhernímu poměru, ve kterém byla sázka přijata a výši vsazené částky (kursové sázky) a k) sázkové hry, při nichž je výhra podmíněna uhodnutím pořadí ve výkonnostních zkouškách koní dostihových plemen (dostihové sázky), a výše výhry je závislá na poměru počtu výherců k celkové výši vkladů (sázek) a předem stanovenému podílu výher nebo výše výhry je přímo úměrná výhernímu poměru, ve kterém byla sázka přijata, a výši vsazené částky.

[6] (1) Kdo neoprávněně provozuje loterii nebo podobnou sázkovou hru, bude potrestán odnětím svobody až na dvě léta nebo peněžitým trestem. (2) Odnětím svobody na jeden rok až pět let bude pachatel potrestán, a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny, nebo b) získá-li takovým činem značný prospěch.

[7] Šámal, P., Púry, F., Rizman, S. Trestní zákon. Komentář. II. díl. 6. vydání. Praha: C. H. Beck, 2004, str. 769. Stupeň nebezpečnosti přitom nebude snižovat skutečnost, že v důsledku konkrétních výsledků sportovních akcí, na než byly neoprávněně přijaty sázky, vyplatil provozovatel větší sumu, než na sázkách přijal. Rozhodující je, že tak činil s úmyslem výdělečným. Nelze zohlednit roli náhody, jež vedla k tomu, že prospěchu nebylo pachatelem dosaženo.

[8] Viz ust. § 219 (Neoprávněné provozování loterie a podobné sázkové hry) návrhu trestního zákoníku: „(1) Kdo neoprávněně provozuje, organizuje, propaguje nebo zprostředkovává loterii nebo podobnou sázkovou hru, bude potrestán odnětím svobody až na tři léta nebo zákazem činnosti. (2) Odnětím svobody na jeden rok až šest let bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny, nebo získá-li takovým činem pro sebe nebo pro jiného značný prospěch. (3) Odnětím svobody na tři léta až deset let bude pachatel potrestán, získá-li činem uvedeným v odstavci 1 pro sebe nebo pro jiného prospěch velkého rozsahu."

Trestní zákoník pochopitelně sám neupravuje ani ve vztahu k provozování sázkových her, kdy se jedná o provozování oprávněné a kdy nikoliv, ale tuto otázku je nutné primárně zodpovědět na základě úpravy v loterijním zákoně. Ten obsahuje základní limit v § 1 odst. 6, podle něhož může být provozovatelem loterie nebo jiné podobné hry jen právnická osoba se sídlem na území České republiky, které oprávněný orgán vydal povolení k provozování loterie nebo jiné podobné hry. Kromě již zmiňovaného licenčního principu se zde objevují další dvě zákonné podmínky a to právní status subjektu (coby právnické osoby) a jeho domicil[9]. Vyloučení fyzických osob z určitých oblastí podnikatelské činnosti nebývá v českém právu neobvyklé[10] a ani v oblasti komunitárního práva nejsou takové restrikce předmětem nesouhlasné pozornosti ze strany Evropského soudního dvora. Odlišný závěr však platí v případě požadavku na umístění sídla na našem území (viz dále).

Pro oblast zájmu tohoto článku se však loterijní zákon nespokojil s vyloučením fyzických osob, ale okruh „licencovatelných" právnických osob dále omezuje a to na stát či státní organizace[11] nebo akciové společnosti se stanovenou minimální výší základního kapitálu[12] a s jedinou přípustnou formou akcií – akcií na jméno (§ 4 odst. 6, 8 a 9 loterijního zákona). Zákonodárce tak brání emitování též akcií na majitele u akciových společností provozujících sázkové kanceláře a tím do jisté míry nepřímo brání anonymizaci akcionářské struktury takové společnosti. Složení akcionářů je přitom též z pohledu loterijního zákona významné. V ust. § 4 odst. 5 loterijního zákona je totiž odpor zákonodárce vůči cizímu prvku na poli hazardních her dále vyjádřen vyloučením z okruhu licencovatelných osob též právnických osob umístěných na území ČR, jež mají zahraniční majetkovou účast, a právnických osob, v nichž mají tyto společnosti majetkovou účast. Vzhledem k tomu, že nejsou stanoveny minimální hodnoty, od nichž je teprve zahraniční účast relevantní jakožto překážka udělení licence, lze konstatovat, že pro českou dceřinou společnost bude neodstranitelnou překážkou udělení licence i sebenepatrnější majetková účast zahraniční osoby v mateřské společnosti. Averze loterijního zákona vůči jakékoliv přeshraničnosti hazardních her (resp. souvisejících aktivit) na území ČR je vystupňována odstavcem 11 téhož ustanovení, podle

---

[9] Vzhledem k uložené povinnosti zachovávat shodu mezi skutečným a registrovaným (rejstříkovým) sídlem a vzhledem k možnému sankčnímu zrušení společnosti s likvidací v případě nesouladu obou sídel lze konstatovat, že česká právní úprava nepřímo vede k povinnému přemístění společnosti na území ČR – tedy vlastně vylučuje podnikání zahraničních subjektů (§ 19c odst. 2 obč. zák. ve spojení s § 29 odst. 6 obch. zák.).

[10] Výlučně právní formu akciové společnosti tak musí mít například obchodník s cennými papíry (§ 6 odst. 1 zákona č. 256/2004 Sb., o podnikání na kapitálovém trhu) nebo zajišťovna (§ 3 odst. 3 zákona č. 363/1999 Sb., o pojišťovnictví; pojišťovna podle druhého odstavce téhož ustanovení může mít též formu družstva).

[11] V případě sázkových her podle § 2 písm. f) a k).

[12] V případě sázkových her podle § 2 písm. f) činí minimální výše základního kapitálu 100 000 000 Kč a v případě sázkových her podle § 2 písm. h) činí minimální výše základního kapitálu 10 000 000 Kč. V případě sázkových her podle § 2 písm. k), tj. dostihových sázek, není akciová společnost výslovně zmíněna a na první pohled by se mohlo zdát, že se v tomto případě akciová společnost nemůže ucházet o licenci. Avšak loterijní zákon zde připouští jako provozovatele stát nebo jím pověřenou organizaci, aniž by však hovořil o státní organizaci. Pouze obsahuje jakési doporučení, když uvádí, že pověření bude uděleno zpravidla (nikoliv výlučně) organizaci, která je osobou oprávněnou v oblasti chovu koní dostihových plemen. Za prvé nelze vyloučit, že takovou osobou bude i akciová společnost a za druhé neukládá zákon existenci takového oprávnění jako conditio sine qua non udělení povolení k provozování dostihových sázek.

něhož je zakázáno „provozování cizozemských loterií včetně prodeje cizozemských losů, účast na sázkách v zahraničí, při nichž jsou sázky placeny do zahraničí, a sbírka sázek pro sázkové hry provozované v zahraničí nebo zprostředkování sázek na sázkové hry provozované v zahraničí". Následuje zákaz provozování tuzemských loterií a jiných podobných her, při nichž jsou sázky placeny v zahraničí. Ministerstvo financí sice může (k zajištění vzájemnosti) povolit z tohoto zákazu výjimku, ale není nám známo, že by výjimka tohoto charakteru byla stanovena.

3. JE TEDY ON-LINE BETTING PŘÍPUSTNÝ V ČR?

Z výše uvedeného jasně plyne, že provozovat sázkovou kancelář lze jedině na základě vydaného povolení (a v souladu s ním) a že takové povolení můžeme být vydáno pouze omezenému okruhu subjektů. Ovšem při formulaci odpovědi na otázku obsaženou v nadpisu této kapitoly narážíme na základní problém, že loterijní zákon výslovně neupravuje provoz internetových sázkových kanceláří, tzn. nenalezneme ani kategorický zákaz, ani jeho povolení, resp. povolení se stanovením podmínek, za nichž je tento provoz souladný s právem ČR.

Subjekty žádající Ministerstvo financí v souladu s úpravou loterijního zákona o povolení k provozování internetových sázkových kanceláří v současné době narážejí na praxi tohoto ministerstva, které vychází z výkladu právní úpravy, podle níž není v současné době na našem území přípustné internetové podnikání v oblasti hazardních her. Tento autoritativní výklad zákona[13] vede k tomu, že dosavadní žádosti tohoto charakteru jsou zamítány, resp. ministerstvo využívá své možnosti podle § 21 odst. 1 loterijního zákona stanovit podmínky provozování kurzových sázek a schválit herní plán sázkových kanceláří tak, že žádné osobě dosud neschválilo herní plán obsahující možnost přijímat sázky prostřednictvím internetu.[14] Tudíž nelze předpokládat, že za stávajícího stavu bude některému subjektu uděleno povolení připouštějící provozování sázkových her na internetu, které je nezbytnou podmínkou oprávněnosti takového provozu (posuzováno podle loterijního zákona).

Ovšem konstatováním, že česká úprava ve spojitosti s výkladovou praxí příslušného správního orgánu vylučuje určitý druh podnikatelské činnosti, se téma oprávněnosti této činnosti nevyčerpává, neboť po vstupu ČR do EU je nutné brát v potaz též zásadu přednosti komunitárního práva[15] a zvažovat, zda v jeho rámci nejsou dána pravidla prolamující výše uvedený restriktivní národní pohled. V našem případě je tímto pravidlem jedna ze základních svobod a to svoboda volného pohybu služeb. Je tedy třeba položit si otázku, zda český přístup neodnímá neoprávněně tuto svobodu subjektům, které oprávněně provozují internetové sázkové kanceláře podle právní úpravy

[13] Není nám známo, že by tento výklad byl podroben přezkumu ze strany správního soudnictví.

[14] Například ředitel společnosti Fortuna Martin Todt uvádí: „My jsme opakovaně žádali o licenci k internetovému sázení, žádost byla vždy zamítnuta s tím, že odporuje zákonu". In: Mášová, H. Loterijní kolotoč. Se státním dohledem tady nelegálně podnikají zahraniční sázkové firmy. Článek ze 17. 4. 2008 publikovaný na http://ekonom.ihned.cz/c4-10005650-24082290-40B000_d-loterijni-kolotoc.

[15] Viz C-6/64 Costa nebo C-34/73 Variola.

jiného členského státu a které mají v úmyslu využít výhod internetu a nabídnout možnost vsazení i osobám na území naší republiky. Svoboda volného pohybu služeb, která představuje jakousi sběrnou kategorii ve vztahu ke svobodám volného pohybu zboží, kapitálu a osob[16], se vztahuje na služby poskytované za úplatu (čl. 49 a násl. SES), což je v případě on-line sázkových kanceláří nepochybně naplněno. Z komunitárního výkladu[17] této svobody vyplývají pro národní zákonodárce zejména tyto limity. Přiznat právo poskytovat služby výlučně vlastním státním příslušníkům je přípustné, jestliže je služba poskytována v souvislosti s výkonem veřejné moci, resp. podobné opatření odůvodňuje veřejná bezpečnost nebo ochrana zdraví. Obdobně je omezena možnost stanovit pro poskytování určitého typu služeb povinnost poskytovatele mít umístěné na území daného státu sídlo. Sice se nejedná o přímou diskriminaci cizozemců, ale též toto je považováno za zásadně neospravedlnitelné omezení.[18] Kromě diskriminačních opatření jsou nepřípustným omezením svobody poskytování služeb i předpisy ztěžující poskytování služby, jež neslouží veřejnému zájmu – zejména nejsou přiměřené[19] tomu, co objektivně zasluhuje zachování veřejného zájmu nebo nepřihlížejí ke srovnatelným požadavkům, které poskytovatel již splnil v členském státu svého sídla.[20]

Vzhledem k vzrůstajícímu významu fenoménu internetového sázení a hazardních her vůbec nepřekvapuje, že se již i jednotlivé národní úpravy tohoto oboru podnikání staly předmětem zájmu ESD z pohledu konformity s principy plynoucími ze svobody poskytování služeb.[21] Z těchto rozhodnutí lze též dovozovat jednotlivé skupiny důvodů, které ESD považuje za přípustné pro ospravedlnění omezení svobody poskytování služeb:

- ochrana veřejného pořádku (podvody a jiné druhy trestné činnosti),[22]
- ochrana spotřebitele (jeho ochrana před zneužíváním lidské slabosti k hazardním hrám, riziko gamblingu),[23]
- ochrana morálních a kulturních hodnot,[24]
- zabránění zneužití hráčské vášně jakožto zdroje soukromého zisku.[25]

Tyto důvody přitom nesmí být pouze tvrzeny, ale musí být přímo podloženy konkrétním zdůvodněním. V této souvislosti ESD výslovně konstatoval, že se stát nemůže dovolávat zájmu na omezení hazardních her jakožto důvodu pro uplatňování restrikcí za situaci, kdy podporuje činnost subjektů v oblasti hazardních her (např. státní monopol široce inzerující své služby). I pro citlivou oblast hazardních her tak byla potvrze-

---

[16] Tichý, L. a kol. Evropské právo. 1. vydání. Praha: C. H. BECK, 1999, str. 365.
[17] Viz Tichý, L. a kol. Evropské právo. 1. vydání. Praha: C. H. BECK, 1999, str. 369–371.
[18] Viz C-33/74 van Binsbergen.
[19] Podrobněji k testu přiměřenosti viz rozhodnutí C-55/94 Gebhard, bod 37.
[20] Častým nešvarem orgánů jednotlivých členských států přitom je, že při posuzování žádostí a činnosti zahraničních provozovatelů hazardních her nepřihlížejí k tomu, že již prokázali splnění často obdobných předpokladů již v řízení před svými domovskými orgány dohledu.
[21] Rozhodnutí C-275/92 Schindler, C-124/97 Läära, C-67/98 Zenatti, C-243/01 Gambelli, C-338, 359, 360/04 Placanica. Blíže k jednotlivým judikátům viz Lyčka, M.: Rien va plus – právní úprava loterií v Evropské unii a aplikace těchto zásad na právní úpravu v České republice. Právní rozhledy, 2007, č. 16, str. 586–597.
[22] Rozhodnutí C-275/92 Schindler, bod 60, a C-124/97 Läära, bod 32.
[23] Rozhodnutí C-124/97 Läära, bod 32, C-6/01 Anomar, bod 73.
[24] Rozhodnutí C-275/92 Schindler, bod 60.
[25] Rozhodnutí C-275/92 Schindler, bod 57.

na platnost zákazu diskriminace.[26] Jiným omezením ze strany státu pak musí předcházet analýza vhodnosti a přiměřenosti takového omezení. Na druhou stranu však ESD výslovně konstatuje, že důsledné zachovávání (či spíše prosazení) svobody poskytování služeb nemusí nevyhnutelně vést k dosažení stejného stupně regulace hazardních her, stejné úrovně ochrany dotčených zájmů a tím i stejné míry omezení svobody poskytování služeb. ESD naopak zdůrazňuje, že i při zohlednění kautel plynoucích ze svobody poskytování služeb se může systém ochrany lišit v jednotlivých členských státech, aniž by to zakládalo rozpor právní úpravy některého z nich s komunitárním právem.[27]

V případě ČR uvádí zpráva Švýcarského institutu srovnávacího práva, že v kontextu našeho práva nejsou důvody těchto omezení relevantním způsobem uváděny.[28] Z ustanovení § 31 loterijního zákona[29] však lze dle našeho názoru dovodit, že důvodem negativního postoje k internetovému sázení je zájem na zamezení přístupu k hazardu dětem a mladistvým[30]. Nutno dále podotknout, že často uváděná motivace zabránit daňovým únikům či snižování daňových příjmů takovým ospravedlnitelným důvodem dle názoru ESD není.[31]

Navzdory výše uvedenému zastává Ministerstvo financí názor, že osoby, které jsou držiteli příslušné licence vydané jiným členským státem EU, nabízí na českém území své služby (sázkové kanceláře) neoprávněně. Tento závěr vyústil v podání několika trestních oznámení na tyto provozovatele.[32] Tato trestní oznámení však byla doposud odkládána s tím, že se dotčení operátoři trestného činu nedopustili.[33] Právní názor orgánů činných v trestním řízení je přitom dle všeho založen na neexistenci zákazu provozování internetových sázek, na závěrech ESD a na skutečnosti, že všechny zkoumané zahraniční subjekty byly držiteli licence vydané jiným členským státem. K tomu lze navíc uvést, že za stávající právní úpravy není zahraničním subjektům byť z prostoru EU umožněno získat povolení Ministerstva financí.[34] Problematika relevance licence vydané jiným členským státem pochopitelně není řešena jen na našem území. Například německé soudy též nejprve (obdobně jako Ministerstvo financí) považovaly za zcela nerozhodné, zda je či není žadatel držitelem licence i v jiném členském státu. V poslední době však při přezkumu rozhodnutí o postihu zahraničních poskytova-

[26] Rozhodnutí C-243/01 Gambelli, bod 65.

[27] Rozhodnutí C-275/92 Schindler, bod 61, a C-124/97 Läära, bod 35.

[28] Tj. nejen v právním předpisu, ale ani v důvodové zprávě nebo judikatuře – SICL Report, s. 135.

[29] Kursových sázek se nesmí účastnit ten, kdo nedovršil 18 let věku. Za účelem prověření této okolnosti je provozovatel oprávněn požadovat předložení průkazu totožnosti.

[30] Ostatně téhož důvodu se dovolávají předkladatelé restriktivního návrhu senátní novely loterijního zákona.

[31] Rozhodnutí C-243/01 Gambelli, bod 61 a 62. Srov. stanovisko senátora J. Novotného prosazujícího restriktivní novelu loterijního zákona, podle něhož vsadí Češi v rámci nepovolených (?) internetových sázek ročně 12–15 miliard korun, z nichž 4–5 miliard představuje zisk nezdaňovaný v ČR. In: Novotný, J. Hazard by měly regulovat obce. Článek z Lidových novin, 13. 6. 2008, str. 11.

[32] Dle telefonického zjišťování na Ministerstvu financí byla podána v letech 2005 a 2006 celkem tři trestní oznámení na tyto provozovatele (celkem 19 subjektů) – adresována Nejvyššímu státnímu zastupitelství v Brně a následně postoupena příslušným orgánům (Městskému státnímu zastupitelství v Brně, Obvodnímu státnímu zastupitelství pro Prahu 5 a Obvodnímu státnímu zastupitelství pro Prahu 9) k prošetření.

[33] Informace poskytnutá Ministerstvem financí prostřednictvím ředitele odboru pana Petra Vrzáně (viz Martin Staněk, ČTK, 14. 12. 2007).

[34] Členský stát přitom nemůže uplatnit trestní sankci za nesplněnou administrativní formalitu, pokud splnění této formality bylo odepřeno nebo znemožněno členským státem v rozporu s právem Společenství (C-338, 359 a 360/2007 Placanica, bod. 69). V tomto případě pravděpodobně nelze bez dalšího aplikovat tento názor ESD, neboť vydání licence nelze považovat za prostou administrativní formalitu.

telů za neoprávněné podnikání Ústavní soud zpochybňuje eurokonformnost takového postihu[35] a považuje za nutné vzít v potaz, zda osoba nabízející služby v SRN má platné povolení vydané v jiném členském státě.[36]

Za dané situace proto může provozovatel, jenž je držitelem licence opravňující k provozu internetové sázkové kanceláře vydané jiným členským státem, poskytovat své služby na území ČR, aniž by toto jeho jednání zakládalo trestní odpovědnost za spáchání trestného činu neoprávněného provozování loterie a podobné sázkové hry podle § 118a trestního zákoníku. Ostatně i kdyby hrou osudu obstála česká úprava znemožňující zahraničním subjektům provozovat u nás na základě licence jiného členského státu on-line sázkové kanceláře, a tedy by tato jejich činnost byla na jisto postavena jako neoprávněná, přesto platí, že naplnění skutkové podstaty tohoto trestného činu vyžaduje po subjektivní stránce úmysl, který musí zahrnovat i znak „neoprávněně".[37] A tedy by v důsledku právního omylu těchto osob (či obvykleji osob jejich jménem vystupujících) nebylo možné dovozovat trestní odpovědnost.

Z pohledu často diskutované soutěže jednotlivých národních úprav práva obchodních společností je pak zřejmé, že další výhodu získávají ty právní řády, které získání této („internetové") licence umožňují. Prvním takovým členským státem nabízejícím licence zahrnující i poskytování služeb v oblasti internetového hazardu byla Malta a to již k okamžiku svého vstupu do EU (1. 5. 2004), dalším významným reprezentantem je Velká Británie, jež v r. 2005 nahradila Gambling Act z r. 1968 moderním předpisem, který nabýval účinnosti postupně až do konce roku 2007.

4. BUDOUCNOST LOTERIJNÍHO ZÁKONA

Již 90. léta byla svědkem prudkého rozvoje internetového sázení. V České republice se možnost internetového sázení objevuje o něco později – až v únoru r. 2004 prostřednictvím společnosti Betsson.com.[38] Zatímco členské státy dosud v rámci EU nedosáhly konsensu ohledně míry regulace této oblasti podnikání[39] a nepřijaly tomu odpovídající předpisy stanovící alespoň minimální míru harmonizace, jednotlivé subjekty provozující internetové sázkové kanceláře zatím mohutně rozvíjejí svou podnikatelskou činnost, přičemž oslovují potenciální zákazníky bez ohledu na hranice členských států a různorodost jejich právních úprav. Navíc vzhledem k zákazu internetového sázení v USA[40] je pravděpodobné, že většina osob podnikajících v oblasti internetového sázení bude umístěna především na území EU a bude na jejím území vyvíjet podnikatelskou činnost.

---

[35] Rozhodnutí Ústavního soudu ze dne 28. 3. 2006, 1BvR 1054/01.

[36] Rozhodnutí Ústavního soudu ze dne 27. 4. 2005, 1 BvR 223/05, nebo ze dne 1. 12. 2004, 1 BvR 1446/04. Obdobné vyznění přináší i rozhodnutí francouzského Kasačního soudu ze dne 10. 7. 2007 ve věci Parimutuel Urbain (PMU – monopolní organizace v oblasti sázení na koňských dostizích) v. ZeTurf (internetový poskytovatel z Malty).

[37] Šámal, P., Púry, F., Rizman, S. Trestní zákon. Komentář. II. díl. 6. vydání. Praha: C. H. Beck, 2004, str. 770.

[38] Mášová, H. Loterijní kolotoč. Se státním dohledem tady nelegálně podnikají zahraniční sázkové firmy. Článek ze 17. 4. 2008 publikovaný na http://ekonom.ihned.cz/c4-10005650-24082290-40B000_d-loterijni-kolotoc.

[39] SICL report, str. 1400.

[40] Unlawful Internet Gambling Enforcement Act 2006.

Globální rozvoj internetového hazardu přitom má podle závěrů zprávy Švýcarského institutu srovnávacího práva[41] nadále pokračovat díky následujícím faktorům, jejichž existenci lze předpokládat i na území ČR:

- vzrůstající počet osob majících přístup k nezbytným technologiím
- tyto technologie jsou stále více uživatelsky přátelské (user-friendly)
- rozvoj elektronických platebních systémů umožňujících provedení platby stejnou technologií, kterou je uzavřena sázka klientem
- dospívá generace, pro níž je užívání výše uvedených technologií součástí každodenního života
- částky vynaložené na trávení volného času stále narůstají.

Sázení v prostředí internetu poskytuje zákazníkům nové výhody, zejména pohodlí a diskrétnost, které odbourávají či snižují existující bariéry (psychologické nebo ekonomické). Tak se zvyšuje počet subjektů na straně poptávky sázkových služeb a to bohužel i u dětí a mladistvých, u kterých je vzhledem k jejich objektivní nedostatečné vyzrálosti zvýšeno riziko propadnutí tzv. gamblerství. Dosavadní restriktivní přístup státu však vede především k tomu, že české subjekty mají na rozdíl od zahraničních konkurentů svázané ruce, a tak je internetové sázení příčinou odlivu peněz z ČR – nejen v podobě neodvedených daní ze zisku dosaženého zahraničním subjektem, jenž daňové povinnosti vůči českému státu nepodléhá, ale i v podobě zbylé částky, kdy peněžní prostředky získávají v důsledku sázení zahraniční subjekty od českých zákazníků a tento tok není alespoň částečně kompenzován nabídkou služeb sázkových kanceláří ze strany českých provozovatelů vůči spotřebitelům v zahraničí.[42]

Není tedy divu, že se regulace internetového sázení stává středem zájmu i v České republice a lze předpokládat, že v dohledné podobě bude tato oblast podnikání výslovně upravena v loterijním zákoně.[43] Již v r. 2006 připravovalo Ministerstvo financí návrh nového loterijního zákona upravujícího i internetové sázení, ale z jeho přijetí nakonec sešlo. Další návrh z r. 2007 již obsahoval zákaz internetového sázení, nebyl však schválen vládou. V současné době existují dva možné zdroje této nové úpravy a to senátní a vládní návrh. Návrh novely loterijního zákona pocházející od senátorů vedených Josefem Novotným, který se snaží účinněji čelit rizikům spojeným s hazardními hrami, se nezabývá jen internetovými loteriemi a podobnými hrami, avšak v této oblasti zaujímá návrh kategorický postoj, když provozování těchto her na internetu má být zcela zakázáno.[44] Hlavním důvodem přitom je skutečnost, že není možné zajistit, aby se sázkových her nemohli účastnit nezletilí. Návrh bude projednáván v Senátu ve druhém čtení v polovině července[45]. Bude-li nakonec tento návrh přijat, je

[41] SICL report, str. 1401. Podle informací na str. 1406 této zprávy jsou při sázení využívány prostředky dálkové komunikace dokonce ve 28 % případů. Ovšem je nutné zohlednit, že se do tohoto objemu započítávají i sázky zadávané telefonicky, což je forma známá a využívaná několik desetiletí.

[42] Podle některých odhadů již bylo z ČR takto odvedeno již 20 mld. Kč. In: Mášová, H. Loterijní kolotoč. Se státním dohledem tady nelegálně podnikají zahraniční sázkové firmy. Článek ze 17. 4. 2008 publikovaný na http://ekonom.ihned.cz/c4-10005650-24082290-40B000_d-loterijni-kolotoc.

[43] Ať již v novele stávajícího zákona nebo v zákoně novém.

[44] Mášová, H. Loterijní kolotoč. Se státním dohledem tady nelegálně podnikají zahraniční sázkové firmy. Článek ze 17. 4. 2008 publikovaný na http://ekonom.ihned.cz/c4-10005650-24082290-40B000_d-loterijni-kolotoc.

[45] Novotný, J. Hazard by měly regulovat obce. Článek z Lidových novin, 13. 6. 2008, str. 11.

zřejmé, že budou následovat stížnosti k Evropské komisi[46], jež povedou k přezkumu eurokonformity takového přístupu. Pod gescí Ministerstva financí se pak pracuje na přípravě nového zákona regulujícího internetové sázení. Chvályhodná je snaha učinit novou úpravu již od počátku předmětem veřejné diskuse, když byl ve spolupráci se společností Ernst & Young spuštěn dne 1. 5. 2008 projekt,[47] v jehož rámci se do poloviny července může kdokoliv vyjádřit v diskusi nad novou úpravou.[48] Návrh zákona by měl být předán vládě do konce letošního roku a předpokládá se, že účinnosti by nová úprava nabyla do konce r. 2010.

Není pochyb o tom, že případné nepřípustné omezení svobody volného pohybu služeb v oblasti internetového sázení (resp. hazardních her obecně) v České republice se dříve nebo později stane předmětem zájmu ze strany Evropské komise. Již v současné době totiž Komise vyvíjí intenzivní aktivity směřující zatím jen k zjišťování případných překážek volného poskytování služeb v této oblasti. Evropská komise totiž obdržela několik desítek stížností na porušování svobody volného pohybu služeb ze strany jednotlivých členských států. Její postup je následující: Po přezkoumání stížnosti zašle nejprve členskému státu upozornění, následuje zaslání odůvodněného stanoviska[49] a posledním krokem je podání žaloby na porušení zakladatelské smlouvy k ESD. V současné době zvažuje Komise podání žalob k ESD vůči těmto členským státům: Finsku, Švédsku, Dánsku, Maďarsku a Francii. Žaloby by měly být podány zhruba v polovině roku 2008.[50] Šetření probíhají i u nových členských států (např. Rumunska, Polska i ČR), ale u těchto zemí Komise zpravidla naráží na nedostatek důkazů. „Hitem" poslední doby je zahájení výše uvedené procedury[51] vůči Německu, které od počátku tohoto roku zakazuje internetový provoz hazardních her.

Obecně je možné konstatovat, že členské státy omezují on-line sázení ze dvou důvodů – buď jako formu ochrany státního provozovatele sázek před konkurencí[52] nebo z důvodu ochrany veřejného zájmu. První důvod Komise neakceptuje a je podle ní důvodem pro podání žaloby k ESD. Ve druhém případě bude Komise zkoumat každou jednotlivou situaci a konečné rozhodnutí bude záležet na konkrétních skutkových okolnostech. Komise bude primárně posuzovat, zda je deklarovaný veřejný zájem uváděný členským státem jako vysvětlení pro zákaz či omezení on-line sázek dosta-

[46] Tento záměr již avizoval jménem Asociace evropských poskytovatelů her a sázek Ondřej Schmidt ze společnosti bwin. In: Mášová, H. Loterijní kolotoč. Se státním dohledem tady nelegálně podnikají zahraniční sázkové firmy. Článek ze 17. 4. 2008 publikovaný na http://ekonom.ihned.cz/c4-10005650-24082290-40B000_d-loterijni-kolotoc.

[47] Jehož hlavní platformou jsou internetové stránky http://www.hernizakon.cz/.

[48] Blíže http://www.mfcr.cz/cps/rde/xchg/mfcr/xsl/tiskove_zpravy_39519.html – speciálně se přitom počítá s účastí odborníků, profesních sdružení i provozovatelů sázkových her a loterií.

[49] V této fázi se nachází řízení vůči Nizozemí.

[50] Pokud budou žaloby podány v očekávaném termínu (polovina roku 2008), lze rozhodnutí ESD očekávat za cca 1–2 roky, tj mezi lety 2009 a 2010. Informace jsou čerpány ze stránek EU: http://ec.europa.eu/internal_market/services/gambling_en.htm a z informací telefonicky zjištěných u Evropské komise.

[51] V lednu 2008.

[52] V tomto případě Komise identifikovala dva přístupy členských států – buď je státnímu provozovateli přiznán monopol na provozování on-line sázek anebo (pokud státní provozovatel není technologicky dostatečně vybavený) jsou on-line sázky úplně zakázány. Zatím ve všech případech, kde se Komise rozhodla žalovat, uplatňují členské státy první přístup (monopol na on-line sázení).

tečně konzistentně uplatňován (např. pokud je deklarovaným veřejným zájmem ochrana před závislostí, nelze akceptovat zákaz on-line sázek, pokud členský stát zároveň zaujímá liberální postoj pro provozování výherních automatů, které Komise považuje za nebezpečnější z pohledu ochrany hráčů před závislostí[53]).

5. ZÁVĚREM

Internetové sázení je navzdory nejisté právní situaci a vesměs odmítavému postoji Ministerstva financí realitou. Úspěšná snaha prosadit naprostý zákaz internetového sázení[54] by proto čelila vážným problémům při prosazování tohoto zákazu v praxi, nehledě na to, že navzdory různorodým postojům k internetovému hazardu netvoří v Evropě striktně restriktivní postoj významný názorový proud.[55] Přímo zpráva Švýcarského institutu srovnávacího práva zmiňuje obvyklé pokušení státu zakázat nové formy podnikatelské činnosti, buď pod vlivem lobbistických snah soutěžitelů etablovaných ve stávajících konturách daného odvětví nebo pod vlivem odpůrců hazardních her, kteří brání akceptaci nové formy hazardu a využívají tak možnosti, aby v této dílčí otázce prezentovali svůj záporný pohled, tj. v tomto případě se nejedná o „kvalifikovaný" odpor proti internetovému sázení ale projev generálního nesouhlasu, který nerozlišuje mezi on-line a „off-line" hazardem. Nezbývá nyní než doufat, že výsledkem názorových střetů v Parlamentu i mimo něj bude moderní úprava on-line sázení, která bude v maximální možné míře eliminovat rizika spojená s tímto fenoménem[56], nebude diskriminovat a omezovat zahraniční provozovatele způsobem z pohledu komunitárního práva nepřípustným a nebude nepřiměřeně limitovat české subjekty ve srovnání s jejich evropskými konkurenty.

TO THE UNAUTHORIZED BUSINESS ACTIVITY IN CYBERSPACE
(OR ELSE TO ON-LINE BETTING IN CZECH LEGISLATION)

Summary

The article deals with the activity of the foreign subjects providing on-line betting in the Czech Republic. It describes problems arising out the facility of internet betting crossing the borders and facing the restrictive attitude of the Czech legislation to these type of activities of foreign subjects. EU harmonization has not been reached in this field of business activity yet but each EU member state has to respect the general limits resulting from the decisions of European Court of Justice. Therefore Parliament of the Czech Republic is limited in the scale of possible restriction of on-line gambling. The article confronts these limits with the intention of senators to enacted an amendment of Lottery Act 1990.

[53] A v této souvislosti je nutné připomenout fenomén výherních automatů jakožto mnohdy oblíbených dodatečných zdrojů obecních rozpočtů.
[54] Dle návrhu senátní novely loterijního zákona.
[55] SICL Report, str. 1401.
[56] Například vyloučením dětí a mladistvých zakotvením požadavku předchozí fyzické registrace každého sázejícího na pobočce provozovatele, což ostatně předpokládají i dosavadní návrhy z řad provozovatelů.

Key words: on-line betting, gambling, unauthorized business activity, tax evasion and avoidance, freedom to provide services, cross-border providing of services, protection of consumers, European Commission, legal regulation of business, practise of European Court of Justice

Klíčová slova: internetové sázkové kanceláře, hazardní hry, neoprávněně podnikání, daňové úniky, svoboda volného pohybu služeb, přeshraniční poskytování služeb, ochrana spotřebitele, Evropská komise, právní podmínky podnikání, judikatura ESD

2008 ACTA UNIVERSITATIS CAROLINAE – IURIDICA 4 PAG. 91–106

K PROBLÉMU PŮSOBNOSTI TRESTNÍHO PRÁVA NA INTERNETU

RADIM POLČÁK
Katedra právní teorie Právnické fakulty Masarykovy Univerzity
Pracovní skupina pro právo a informační technologie Právnické fakulty Masarykovy Univerzity

1. ONTOLOGIE PRÁVA VE VZTAHU K INTERNETU

Odpověď na otázku, zda právo na internetu existuje či nikoli, se zdá být na první pohled jasná. Podivnou a nepředpokládanou tezi, že na internetu právo neplatí, však nerazí jen rozevlátí vizionáři či anarchistické zájmové organizace, ale mohli jsme se již několikrát setkat s její realizací státními orgány, které právo autoritativně aplikují. V několika případech tak i orgány jako je například policie či soudy odmítly autoritativně uplatnit právo v situaci, kdy se někdo domáhal jeho dodržování v prostředí informačních sítí. Dále si pak představíme i jiné případy, kdy bylo právo sice autoritativně aplikováno, jeho vynucení však bylo z technických, ekonomických či sociálních důvodů nemožné – o materiální legitimitě a platnosti takto aplikovaného práva je pak důvod rovněž pochybovat.

V České republice například policie odložila případ trestného činu pomluvy s poukazem na to, že se uskutečnil na internetovém diskusním fóru a nelze tedy prokázat spáchání trestného činu. Vyšetřovatel se v tomto případě nezabýval zjištěním všech skutečností, které mohou být pro posouzení skutku rozhodné a k odložení případu si vystačil v podstatě jen s výslechem podezřelého. Rozhodnutí o odložení případu pak napadl ministr spravedlnosti stížností pro porušení zákona a Nejvyšší soud ČR této stížnosti vyhověl[1]. Z rozhodnutí, v němž Nejvyšší soud ČR poskytnul vyšetřovateli i obsáhlý návod, jak ve věci dále postupovat, vybíráme: „Podstata porušení zákona v daném případě spočívá v tom, že vyšetřovatel učinil rozhodnutí o zastavení trestního stíhání obviněného Ing. J. Z. z výše uvedeného důvodu, aniž náležitě zjistil skutkový stav a provedl veškeré dostupné důkazy, které se v této věci nabízely. (...) Dále bylo třeba vyžádat znalecký posudek z oboru výpočetní techniky se zaměřením na software a provést příslušné zkoumání zajištěných internetových stránek nalézajících se pod internetovou adresou, jakož i zřízené internetové schránky na jméno Z. S., s cílem získat údaje směřující k identifikaci osoby, která uvedené stránky a schránku zřídila, včetně údajů, jež by umožnily určit osobu, jež předmětný pomlouvačný text na tyto stránky umístila."

[1] Viz rozhodnutí č. 4 Tz 265/2000, publikováno na adrese www.nsoud.cz.

Zajímavý případ s tragickým koncem se odehrál v Číně[2], kde se nejprve jednačtyřicetiletému hráči on-line hry „The Legend of Mir 3" Qiu Chengweiovi podařilo společně s jeho přítelem Zhu Caoyuanem v této hře získat unikátní meč. Aniž by Zhu svému spoluhráči cokoli řekl, prodal tento virtuální meč na internetové aukci za 7200 juanů (cca 19 000,– Kč). Když šel Qui oznámit tento skutek na policii, bylo mu sděleno, že na virtuální vlastnictví se zákony nevztahují a policie tak tento skutek odmítla řešit. Qui byl pak natolik rozezlen, že Zhua napadl a několika bodnými ranami ho usmrtil.

Nejprve si představíme základní koncepce existence a legitimity práva na internetu a budeme rovněž demonstrovat argumentaci, kterou lze k prosazení příslušných právních názorů použít. Výklad to není v žádném případě samoúčelný – představené argumenty se totiž mohou velmi dobře hodit při řešení konkrétních právních problémů před úředními orgány, obecnými a ústavními soudy či před soudy mezivládních organizací. S tímto výkladem je pak v každém případě nutné začít v USA, kde se internet nejen zrodil, ale kde je díky místní právní kultuře[3] možné nalézt i plodné středisko vývoje právních názorů na nejrůznější otázky související s realizací společenských vztahů v prostředí informační sítě.

USA jsou zemí, kde mají hluboké kořeny myšlenkové směry jako liberalismus či dokonce libertariánství. Jednou ze základních myšlenek liberalismu je přitom odstranění nejrůznějších forem regulace omezující jednotlivce v realizaci jejich záměrů a dosažení odpovídajícího prospěchu, ať už materiálního či jiného. Přesně v tomto duchu se nesou aktivity jednoho z nejvýznamnějších hnutí za tzv. svobodný internet, organizace Electronic Frontier Foudation, jejímž zakladatelem je známý rocker a pozdější úspěšný podnikatel John Perry Barlow. Již od počátku svého vzniku, tj. od roku 1990, se tato organizace významně angažuje v boji proti právnímu či jinému omezování svobody jedince na internetu, a to zejména formou veřejné osvěty a právní pomoci v soudních sporech. Jejím základním dokumentem je takzvaná Deklarace nezávislosti kyberprostoru[4], jejímž ústředním motivem je problém právní regulace a činnost států a jejich orgánů autoritativně aplikujících právo. Z deklarace vybíráme následující pasáže (překlad autor):

„Vy, vlády všech průmyslových světů, Vy unavení obři z masa a oceli. Já, přicházející z Kyberprostoru, nového sídla Mysli, Vás v zájmu budoucnosti vyzývám: Nechte nás být! Nejste mezi námi vítáni. Nemáte žádnou moc nad místy, kde přebýváme.

Nemáme vládu ani po žádné netoužíme. Mluvím k Vám tedy z pozice autority ne větší, než jakou má sama Svoboda. Vyhlašuji, ze globální společenství, jež budujeme, nezávisí na tyranii a zákazech, kterými jste nás svázali. Nemáte morální právo nás řídit a nemáte ani nástroje, kterých bychom se museli bát.

---

[2] O případu informoval server The Register, viz Haines, L. Onliner gamer stabbed over 'stolen' cybersword. TheRegister.com, 30. 3. 2005, u nás pak případ komentoval například server Lupa.cz – viz Vyletal, M. Online hry hýbou internetem, psychikou a peněženkami hráčů. Lupa.cz, 12. 8. 2005.

[3] Narozdíl od kontinentální Evropy, kde je souzení se zpravidla výrazem nedostatečné schopnosti člověka dohodnout se a řešit problémy pokojnou cestou, je v USA soudní řešení konfliktů naprosto běžné a velmi populární. Není tedy divu, že čeština ani neobsahuje ekvivalent k anglickému výrazu 'litigeous' označujícímu hádavého člověka chtivého podávat soudní žaloby.

[4] Plný text deklarace viz homes.eff.org/~barlow/Declaration-Final.html.

Moc vlád je odvozena ze souhlasu těch, kterým vládnou. Náš souhlas jste však nežádali a nikdy jej neobdržíte. Nechceme Vás. Neznáte nás jako neznáte náš svět. Kyberprostor leží mimo hranice Vašeho poznání. Nemyslete si, že jej můžete tvořit a dotvářet jako by se jednalo o nějakou další Vaši veřejnou zakázku. Nemůžete. Vznikl přirozeným vývojem a roste dík našemu společnému úsilí.

Dovoláváte se problémů okolo nás, a říkáte, je potřeba je řešit. Používáte je k ospravedlnění svých výpadů vůči nám. Mnoho z nich však neexistuje. Když se objeví skutečný konflikt nebo jiná špatnost, poznáme to a vypořádáme se s nimi vlastními prostředky. Máme novou společenskou smlouvu. Takové vládnutí se nezakládá na podmínkách Vašeho světa, ale toho našeho a náš svět je jiný.

Pojmy Vašeho práva jako vlastnictví, vyjadřování, subjektivita, pohyb nebo okolnosti, se na nás nevztahují. Všechny jsou založeny na hmotné podstatě a zde žádná hmotná podstata není.

Nemáme těla a na rozdíl od Vás se řád mezi námi nevytváří prostřednictvím násilí. Věříme v nastolení pořádku díky etice, osvícenému individualismu a smyslu pro všeobecné blaho. Můžeme se volně přemísťovat mezi Vašimi jurisdikcemi a tak jediné pravidlo, které skutečně ustavuje naše společenství, je zlaté pravidlo morálky. Na tomto základě chceme řešit všechny problémy a nepřijímáme způsoby, které se nám snažíte vnutit.

Vaše rostoucí nepřátelské a koloniální snahy nás staví to stejné role, jakou měli i v minulosti ti, kteří toužili po svobodě, sebeurčení a kteří se rozhodli odmítnout formální autority. Nedáváte nám jinou možnost než vyhlásit naše virtuální identity nezávislými na Vaší vládě i přes to, že naše těla jí i nadále podléhají. Naše myšlenky však nikdo omezovat nebude, neboť je rozprostřeme po celé planetě.

Založíme v kyberprostoru novou civilizaci Mysli. Snad bude humánnější a spravedlivější než svět, který Vaše vlády doposud vytvořily."

Z uvedených pasáží deklarace, která se s postupem času stala všeobecně přijímaným manifestem svobody internetu, lze vyčíst hned několik momentů zásadních pro otázku působnosti práva. Především je to argument neexistence společenské smlouvy mezi adresáty právních norem a jejich tvůrcem, tj. státem.[5] Tento argument je postaven na premise, že na internetu vzniká zcela nové společenství, jehož zřízení, pokud má disponovat autoritou, musí být založeno na nové společenské smlouvě, prostřednictvím které se adresáti právních norem vzdají části vlastní svobody ve prospěch suveréna. Deklarace přitom hovoří o neexistenci společenské smlouvy, jakož i o neexistenci vůle internetového společenství takovou smlouvu uzavřít.

V návaznosti na nezájem internetové komunity o autoritu státu se pak objevuje další argument nepotřebnosti právní či jiné autoritativní regulace internetu. V deklaraci je doslova uvedeno, že řada problémů zmiňovaných jako důvod k realizaci státní moci na internetu neexistuje a pokud už nějaké problémy jsou, má internetové společenství dostatečné nástroje i snahu k tomu je řešit. Právo a státní donucení jsou pak v tomto smyslu zbytečné.

[5] Za původce teorie společenské smlouvy v právním myšlení je považován Thomas Hobbes. Dílem, které tuto teorii definovalo a posloužilo za základ jejího pozdějšího masivního rozvoje, je spis Leviathan – viz Hobbes, T. Leviathan. Project Gutenberg. Kniha je volně ke stažení na adrese http://www.gutenberg.org/dirs/etext02/lvthn10.txt.

Poslední ze závažných a co do legitimity práva a státu relevantních argumentů je zaměřen na neschopnost států, uzavřených v tradičních prostorových hranicích jurisdikce, efektivně právo vynucovat. Deklarace hovoří o tom, že státy, přestože by se o to mohly pokoušet, nemají nástroje, jak své právo efektivně v prostředí informační sítě vynutit, tzn. jak (fyzicky) donutit adresáty norem, aby se podle nich chovali[6]. Doslova je pak zmíněn moment plošného rozprostření myšlenek (dat) nejen přes všechny jurisdikce ale též přes místa, která žádné jurisdikci nepodléhají a tím k zamezení možnosti jejich postihu.

Na uvedené argumenty, jež si s postupem času získaly značnou publicitu a oblibu mezi uživateli služeb celosvětové informační sítě, nelze přitom odpovědět prostě tak, že právo platí, protože je to napsáno v zákoně. Není totiž pravda, že právem je to, co říká zákon.[7] Obsah či smysl zákona sice může být považován za základní kámen platného práva, často se však setkáme se situací, kdy obsah práva zjišťujeme i jinak než ze zákona nebo naopak, kdy zákon sice nějaké normy obsahuje, ty však nejsou platným právem.[8] Výše uvedené argumenty jsou tedy pro samotnou existenci práva na internetu důležité a chceme-li s právem na internetu pracovat, je třeba se s nimi odpovídajícím způsobem vypořádat.

Předně je třeba zdůraznit, že autoritativně vynucované právo má smysl (je legitimní) tam, kde společnost není sama o sobě dostatečně organizována, což brání její reprodukci nebo dalšímu rozvoji. Prostřednictvím autoritativní organizace neboli regulace tedy může dojít k odstranění společenských problémů, dosažení pokojného stavu a nastartování dalšího rozvoje. Právo by tedy na internetu nemělo smysl tehdy, pokud by v síťovém společenství buďto neexistovaly konflikty nebo pokud by případné konflikty byly řešeny samoorganizačními mechanismy k všeobecnému užitku.

Jak můžeme vidět na celé řadě příkladů jako jsou šíření dětské pornografie, podvody v elektronickém bankovnictví, spekulace s doménovými jmény apod., nejsou přirozené samoorganizační mechanismy již zjevně s to zvládat veškeré problematické či entropické momenty ve vývoji celosvětové informační sítě.[9] Přirozená schopnost společnosti organizovat se na podkladě tradičních sociálních norem či ekonomických pravidel, jakkoli v mnoha případech funkční, tedy v konkrétních oblastech nestačí a prostředí jako celek si tedy žádá autoritativní zásah zvenčí.

Právě uvedené však neznamená, že by právo v prostředí informačních sítí disponovalo nějakou paušální či všeobjímající legitimitou. Nelze tedy prostým poukazem na jednotlivé problematické momenty síťového společenství prostě odmítnout Barlowovy argumenty a jednoduše konstatovat, že právo má na internetu stejný důvod

[6] Obzvláště problematickým se tento moment jeví být v rovině trestního práva, které je tradičně založeno na individuálním násilném postihu pachatele – k problému srov. Thomas, D. Criminality on the Electronic Frontier. In: Cybercrime, London: Routledge, 2003, str. 17 a násl.

[7] Základní ontologickou otázku po tom, co je platným právem, nelze spolehlivě zodpovědět jen na základě nahlédnutí do Sbírky zákonů – k problému viz např. Holländer, P. Filosofie práva. Plzeň: Aleš Čeněk, 2006, str. 17 a násl.

[8] K tomu srov. např. Radbruch, G. Statutory Lawlessness and Supra-Statutory Law (1946). Oxford Journal of Legal Studies, 2006, ročník 26, č. 1, str. 1 a násl.

[9] K tomu srov. např. Kerr, O. S. Virtual Crime, Virtual Deterrence: A Skeptical View of Self-Help, Architecture, and Civil Liability. Journal of Law, Economics & Policy, 2005, č. 1, str. 1 a násl.

k existenci jako v off-line prostředí. Naopak je třeba hovořit o legitimní existenci práva jen tam, kde si etická, sociální, ekonomická či technická pravidla nedokáží poradit s výskytem problematických či chaotických elementů. V tomto směru lze tedy citovat vedoucího současného teoretika práva informačních sítí, profesora Lawrence Lessiga, který v závěru své zásadní monografie Free Culture doslova říká (překlad autor)[10]:

„Právo by jistě mělo regulovat určité oblasti naší kultury, ale mělo by regulovat kulturu pouze tam, kde je taková regulace dobrá. Právníci však stále jen zřídka konfrontují svou moc, respektive moc, kterou šíří, s jednoduchou pragmatickou otázkou: ‚Bude to tak dobré?' Kdykoli má právo dále rozšiřovat svoji působnost, slyšíme je namísto toho říkat spíše ‚Proč ne?'

My bychom se však měli ptát, ‚Proč?' Ukažte mi, že je Vaše regulace kultury potřebná. Ukažte mi, jak je dobrá. A pokud mi nejste schopní ukázat obojí, držte své právníky stranou."

Výše uvedené otázky legitimity práva nás s praktickou nutností vedou k postupnému přehodnocování tradičních mechanismů právní regulace a jejich přetváření na mechanismy, které by se daly nazvat synergickými formami organizace nikoli pod přímou vládou ale za užití práva.[11] Různé typy autorit – zejména pak autority státní, technické a ekonomické – tak v zájmu reprodukce a rozvoje informační sítě k sobě postupně hledají cestu[12] a namísto ignorace či vzájemné konkurence se snaží své působení koordinovat.[13] Význam tohoto sice pomalého[14] přesto však nezadržitelného vývoje přitom není zásadní jen pro samotné prostředí celosvětové informační sítě, ale může naznačit cesty, kterými se bude právo v budoucnosti obecně ubírat. Kritické i konstruktivní studium ekonomických, technických, etických či sociální souvislostí působení práva tak v současné době začíná pro právníky na všech úrovních znamenat nikoli jen užitečnou možnost ale doslova nutnost. Stejně tak státy a jejich orgány autoritativně aplikující právo se již nemohou spoléhat na luxus formální platnosti, obecné působnosti a faktické vynutitelnosti práva bez ohledu na uvedené souvislosti.[15]

---

[10] Viz Lessig, L. Free Culture. New York: The Penguin Press, 2004, str. 305. Kniha je k volnému stažení pod licencí Creative Commons na adrese http://www.free-culture.cc/freeculture.pdf.

[11] K tomu srov. např. Galindo, F. A. Code of Practice for the Globalisation of Electronic Commerce and Government. Journal of Information, Law and Technology, 2002, č. 1, z česky psaných pramenů pak viz Polčák, R., Škop, M., Macek, M. Normativní systémy v kyberprostoru (úvod do studia). Brno: Masarykova univerzita v Brně, 2005, str. 92 a násl.

[12] Běžná je již například spolupráce státu s dodavateli informační infrastruktury v oboru potírání kriminality – nejrůznější technické prostředky tak mohou být vybaveny relativně jednoduchými a nenákladnými mechanismy, které buďto zcela znemožní páchání trestné činnosti nebo významně usnadní její vyšetřování – k tomu srov. např. Katyal, K. Digital Architecture as Crime Control. Yale Law Journal, 2003, č. 112, str. 2261 a násl.

[13] K tomu srov. např. Kleinwächter, W. From Self-Governance to Public-Private Partnership: The changing Role of governments in the Management of the Internet's Core Resources. Loyola of Los Angeles Law Review, 2003, č. 36, str. 1103 a násl.

[14] Možná zde není zcela na místě hovořit o pomalém vývoji v situaci, kdy se právo ICT teprve pozvolna dostává do třetí dekády své existence. Je přeci řada právních institutů, jejichž vývoj postupně probíhá po stovky či dokonce tisíce let.

[15] Viz Samuelson, P. Five Challenges for Regulating the Global Information Society. In: Regulating the Global Information Society, London: Routledge, 2000.

2. OTÁZKA ROZHODNÉHO PRÁVA A JURISDIKCE

Spíš než právně teoretický problém důvodu existence a legitimity práva na internetu je v aktuální praxi častěji diskutována otázka konkrétního rozsahu působnosti právních řádů jednotlivých států.[16] Chceme-li tedy *de iure* posoudit určitou situaci, je třeba mít předně jasno v otázce, které právo (právo kterého státu) bude pro řešení příslušného právního problému rozhodné, dále který státní orgán (nejčastěji který soud) je oprávněn vydat o něm pravomocné rozhodnutí a konečně pak, který orgán může takové rozhodnutí vymoci či přímo vykonat.

Právní řády určující práva a povinnosti jednotlivým subjektům jsou v současnosti až na malé výjimky stále pod výhradní kontrolou jednotlivých států. Za dobu své existence si tak právo muselo vybudovat mechanismy, jak rozhodovat právní problémy, které mají nějakou vazbu k více než jednomu státu. Hovoříme tak o takzvaných právních vztazích s mezinárodním prvkem, přičemž takovým prvkem může být například rozdílná státní příslušnost účastníků, umístění věci, o kterou ve vztahu jde, místo, kde má být splněn závazek, místo, kde došlo k porušení práva, atd.

Uvedené mechanismy rozdělení působnosti práva mezi jednotlivé státy a jurisdikce jednotlivých státních orgánů (většinou soudů) jsou sice intenzivně budovány již stovky let, i v dnešní době se však můžeme setkat se situacemi, kde určení rozhodného práva nebo příslušného soudu představuje obtížný právní problém. Pořád lze však spoléhat na více či méně stabilní kritéria pevně daných hranic státního území, fyzického umístění jednotlivých věcí, místa pobytu osob apod. Internet nám však valnou většinu těchto solidních kritérií bere, neboť se jedná o prostředí bez zjevných vnitřních hranic.[17] Je sice pravda, že lze v každý konkrétní okamžik vystopovat fyzické umístění určité informace – příslušná lokace je však mnohdy nahodilá, velmi krátkodobá a pro informaci jako takovou a její právní efekt zpravidla naprosto irelevantní. Z hlediska příslušného právního vztahu je tedy obvykle lhostejné, kde se informace fyzicky nachází – urazí-li nás tak například něčí www stránka, na kterou se může jednoduše připojit kterýkoli náš známý, je nám vzhledem k ochraně našich subjektivních práv jedno, zda jsou příslušná data fyzicky umístěna v České republice, v Německu či v některém státě rovníkové Afriky anebo na všech uvedených místech zaráz.

O tom, zda má smysl činit z hlediska práva a jeho působnosti rozdíl mezi off-line a on-line právními problémy, se vedla a stále ještě vede zanícená debata. Zatímco zastánci konzervativního proudu argumentují tím, že je vždy v určité formě možné zjistit vztah informací a subjektů k území nějakého státu a není tedy důvod hledat speciální řešení, představitelé v současnosti dominantní teorie zastávají názor, že je třeba při řešení otázek působnosti práva a jurisdikce státních orgánů postupovat diferencovaně a hledat jiná a specifická kritéria rozdělení působnosti a jurisdikce než na základě vazby ke státnímu území. Na úrovni špiček právní vědy se tato debata rozhořela nejprve

[16] K podrobnému vymezeni problému viz např. Wilske, S., Schiller, T. International Jurisdiction in Cyberspace: Which States May Regulate the Internet? Federal Communications Law Journal, 1997–1998, ročník 50, č. 1, str. 117 a násl.

[17] K tomu viz např. Post, D. Governing Cyberspace. The Wayne Law Review, 1996, č. 43, str. 155.

v USA, a to mezi profesory Postem a Goldsmithem. Druhý z nich, zastánce konzervativního přístupu, k tomu uvádí (překlad autor)[18]:

„Mezinárodní transakce v kyberprostoru se nijak neliší od těch, které známe z ‚reálného' prostředí. Zahrnují jednotlivce umístěné v určitém prostoru pod jurisdikcí nějakého státu, kteří komunikují, ať už s dobrým nebo špatným efektem, s jinými jednotlivci rovněž umístěnými v reálném prostoru pod jurisdikcemi jiných států. Nenacházíme žádné normativní argumenty, které by podporovaly imunizaci kyberprostoru od klasické teritoriální regulace. A máme všechny důvody se domnívat, že státy mohou vykonávat svou autoritu na klasické teritoriální bázi a dostatečně tak regulovat transakce v kyberprostoru."

Na tyto argumenty pak reagoval Post replikou, kde na příkladu jednoho z prvních sporů o tzv. internetovou jurisdikci, případu známém jako „digitalbooks.com", ilustroval neudržitelnost tradičního přístupu k řešení problému rozhodného práva a působnosti soudů. Svoji repliku uzavřel následovně (překlad autor)[19]:

„Myslím si, že opravdu záleží na tom, že Digitalbooks.com je 'v kyberprostoru'. Domnívám se, že otázky založené jeho činností jsou rozdílné a složitější než jaké by byly v situaci, pokud by se podobný případ objevil mimo kyberprostor. Nemyslím si pak, že bychom mohli otázky rozhodného práva a jurisdikce v tomto případě vyřešit prostou aplikací 'tradičních právních nástrojů,' které používáme v reálném světě. (...) Tradiční právo a zavedené principy si sice zaslouží respekt, ale čas od času musí být přehodnoceny. Podle mého ten čas právě nastal."

Postův přístup s větší či menší ochotou postupně přejímala doktrína i soudy nejprve ve Spojených Státech a posléze i v Evropě.[20] To však neznamená, že by tím byl problém stanovení rozhodného práva a jurisdikce soudů vyřešen. Můžeme sice argumentovat, že pro stanovení takzvané internetové jurisdikce potřebujeme diferencovaný přístup, jiné metody a specifická základní kriteria, není však jednoduché obecně odpovědět na otázku, jaká kriteria to pro konkrétní případy jsou. Americké i evropské soudy se tak musejí i nadále relativně složitě potýkat s otázkou stanovení vlastní jurisdikce a následného určení rozhodného práva.

Ačkoli v současné době není a v dohledné době ani nebude možné spolehlivě odpovědět na otázku, jak v konkrétních případech řešit problém tzv. internetové jurisdikce, pokusíme se dále alespoň ukázat jednotlivé možnosti a přiblížit způsoby, jak se s tímto problémem doposud vypořádávaly soudy v Evropě i v zámoří.

---

[18] Viz Goldsmith, J. L. Against Cyberanarchy. Chicago Law Review, 1998, č. 65, str. 1250.

[19] Viz Post, D.G. Against Against Cyberanarchy. Berkeley Technology Law Journal, 2002, ročník 17, č. 1, str. 23.

[20] Srov. např. Reed, C. Internet Law. Cambridge: Cambridge University Press, 2004, str. 218 a násl. nebo z francouzských publikací Cosson, J.-B. Standard Private International Law Tested by the Networks. In: Internet International Law, Bruxelles: Bruylant, 2005, str. 53 a násl.

3. PROBLÉM DELIMITACE TRESTNÍCH JURISDIKCÍ

Trestní právo chrání především vitální zájmy státu a společnosti. Z tohoto důvodu platí princip neoddělitelnosti otázky jurisdikce a rozhodného práva – jinými slovy, trestní soud, je-li příslušný k rozhodnutí ve věci, rozhoduje vždy podle práva svého státu. Uvedené platí i naopak – vztahuje-li se tedy trestní právo hmotné určitého státu na nějaký skutek, znamená to, že o skutku může rozhodnout i soud tohoto státu.[21]

Trestní legislativa má hranice působnosti i jurisdikce orgánů činných v trestním řízení nastaveny relativně široce. Typicky tak lze stíhat v určité zemi trestné činy, které byly na území příslušného státu nejen přímo spáchány, ale i takové, jejichž následky se na tomto území projeví a v určitých případech i činy, které s tímto územím mají jen nepřímou souvislost. I v české republice tak existuje celá řada trestných činů, které lze orgány činnými v trestním řízení stíhat i v případě, nacházel-li se jejich pachatel v době jejich spáchání mimo naše území – zákon č. 140/1961 Sb., trestní zákon, ve znění pozdějších předpisů, řeší tyto otázky v § 17 – § 21. Obdobným způsobem je působnost trestního práva hmotného upravena i v nově připravovaném trestním zákoně, který je v době, kdy vznikala tato publikace, ještě ve stadiu vládního návrhu paragrafového znění. Lze však optimisticky očekávat, že případné politické debaty nebudou mít vliv na znění ustanovení § 4 – § 9 upravujících jeho působnost.

Vzhledem k tomu, že působnost trestní legislativy vyspělých států je vymezena obdobně jako v případě českého trestního zákona, setkáváme se často u tzv. mezinárodních internetových trestných činů se situací, kdy lze trestný čin stíhat zaráz na území více států. Z internetové trestné činnosti jsou přitom nejhojnější případy, kdy se samotný skutek odehraje na území jednoho státu, jeho účinky však nastanou na území státu jiného – např. skupina hackerů provede útok na server fyzicky umístěný v jiném státě.

V uvedených případech je zpravidla možné stíhat pachatele v obou resp. ve všech dotčených zemích. Tato situace je však namísto pro orgány činné v trestním řízení spíše příznivá pro samotného pachatele, neboť vyšetření trestného činu a následné provedení příslušných úkonů je nezřídka otázkou komplikované, zdlouhavé a často i prakticky neefektivní mezinárodní spolupráce.[22] Ačkoli se policejní a soudní orgány snaží při vyšetřování a usvědčování pachatelů internetových trestných činů vzájemně spolupracovat, často jim v tom kromě rozdílné legislativy brání i složité procesní postupy.[23] V častých případech, kdy klíčovou roli při zjišťování pachatelů a zajištění důkazů hraje čas, je tedy prakticky nemožné pachatele odhalit a usvědčit.

---

[21] K tomuto základnímu principu trestního práva viz např. Akehurst, M. Jurisdiction in International Law. In: British Yearbook of International Law. London: Oxford University Press, 1972–73, str. 179 a násl.

[22] Znám je například případ, kdy český policejní vyšetřovatel dožádal šetření o počítačovém trestném činu v Bulharsku. Tamní orgány nejprve informovaly podezřelého o tom, že je na jeho činnost vedeno vyšetřování a požádaly jej o stanovisko. Podezřelý samozřejmě v reakci na to zastavil své aktivity, zlikvidoval veškeré důkazy, které se nacházely v paměti jeho systému, a vyšetřovatelům pak přišel oznámit, že o žádné trestné činnosti neví.

[23] Praktické problémy přeshraniční internetové kriminality trefně popsal francouzský soudce Jean-Wilfrid Nöel in Nöel, J.-W. Internet and Judicial Investigation. In: Internet International Law. Bruxelles: Bruylant, 2005, str. 233 a násl.

Vedle případů, kdy mají orgány činné v trestním řízení na území více států snahu spolupracovat, se však můžeme setkat i s takovým pozitivním konfliktem působnosti trestního práva, který může vést až ke sporu mezi státy o to, čí orgány jsou příslušné ve věci rozhodnout.

Prvním z moderních konfliktů tohoto typu řešeným na úrovni mezinárodního práva veřejného byl případ známý pod označením Lotus.[24] Jednalo se o spor mezi Francií a Tureckem o trestní jurisdikci nad posádkou francouzského parníku Lotus. Ten se v roce 1927 v tureckých teritoriálních vodách srazil s tureckým parníkem, v důsledku čehož přišlo o život několik tureckých námořníků. Otázka trestní odpovědnosti francouzské posádky, která srážku zavinila, pak byla předmětem sporu francouzské a turecké vlády právě na základě pozitivního konfliktu působnosti jejich trestních legislativ. I přes to, že v době spáchání trestného činu byli francouzští námořníci pod teritoriální působností francouzského práva, dal stálý dvůr mezinárodní spravedlnosti nakonec zapravdu Turecku, když ve svém rozhodnutí konstatoval, že „...trestné činy, jejichž pachatel se v době jejich spáchání vyskytoval na území jiného státu, je třeba považovat za spáchané tam, kde se vyskytl jeden z jejich základních elementů, konkrétně jejich účinek."

Uvedenou koncepci nikoli fyzické, ale efektivní přítomnosti pachatele na území určitého státu lze velmi dobře aplikovat i na případy mezinárodní internetové kriminality.[25] Orgány činné v trestním řízení tak toto řízení obvykle vedou i v případech, kdy se na území jejich jurisdikce pachatel v době spáchání trestného činu nenacházel ani zde přímo ke spáchání trestného činu nedošlo, ale kde se projevil nebo mohl projevit efekt trestného jednání. Tato extenzivní interpretace se tak uplatňuje i v případech, kdy v místě fyzického pobytu pachatele není skutek trestný, naopak je však trestný tam, kde se projevily jeho účinky.[26]

V jednom z prvních případů přeshraniční internetové kriminality posuzoval Nejvyšší soud státu New York otázku, zda při provozování portálu s hazardními hrami umístěném ve státě Antigua, jehož zákazníky jsou však obyvatelé státu New York, může dojít k založení trestněprávní odpovědnosti. Při diskusi otázky jurisdikce a působnosti trestního práva státu New York soud doslova uvedl[27] (překlad autor): „Pokud by tento soud přisvědčil argumentaci žalovaných, že aktivity zaměřené na obyvatele státu New York spadají pod jinou jurisdikci, vyvolalo by to jistě řadu nežádoucích dopadů. Takový přístup by totiž nejen hrubě poškodil soustavný a odhodlaný postup tohoto státu proti nepovolenému hazardu, ale obecně by zbavil odpovědnosti kohokoli,

[24] Rozhodnutí PCIJ, Ser. A., No. 10, 1927, plný text rozhodnutí včetně disentů viz např. http://www.worldcourts.com/pcij/eng/decisions/1927.09.07_lotus/ Podrobnou analýzu sporu viz v Berge, G. W. The Case of the S. S. Lotus. Michigan Law Review, 1928, ročník 26, č. 4, str. 361 a násl.

[25] K tomu viz např. Kohl, U. Eggs, Jurisdiction and the Internet. International and Comparative Law Quarterly, 2000, č. 52, str. 577 a násl.

[26] Podrobný výklad k problematice založení jurisdikce na základě analýzy efektu viz např. Brenner, S. W., Koops, B.-J. Approaches to Cybercrime Jurisdiction. Journal of High Technology Law, 2004, ročník 4, č. 1, str. 19 a násl.

[27] Případ je znám jako People v. Interactive Gaming Corp., referenční číslo QDS:22310325, 1999 N.Y. Misc. Lexis 425 (Sup. Ct. N.Y.Co., 24. července, 1999), plný text je možné nalézt např. na adrese http://www.loundy.com/CASES/People_v_WIGC.html.

kdo by páchal na internetu skutky, které jsou v tomto státě jinak trestné. Počítačový server nemůže přitom sloužit jako nějaký štít proti odpovědnosti, o to méně pak v tomto případě, kdy obžalovaní přímo zaměřili svou pozornost do státu New York, kde provozovali řadu protiprávních aktivit."

Vzhledem ke shora popsaným problémům je však v praxi internetové kriminality spíše běžné, že hlavní slovo mají orgány činné v trestním řízení na území, kde se pachatel aktuálně zdržuje. Vzájemnou delimitaci pravomocí, spíše však vzájemné procesní závazky tak v mezinárodním respektive celosvětovém měřítku upravují většinou jen smlouvy o spolupráci v trestním řízení, které však mají případ od případu rozdílnou kvalitu i procedury.

Určitou výjimku z uvedené právní praxe představuje Úmluva Rady Evropy o kyberkriminalitě, která byla otevřena k podpisu 23. 11. 2001 v Budapešti.[28] Základním momentem Úmluvy jsou především definice jednotlivých skutkových podstat trestných činů,[29] jež se členské státy zavazují ve svých jurisdikcích stíhat.[30] Jedná se o následující typy trestných činů:

- nedovolené získání přístupu k systému
- nedovolené narušování komunikace
- poškozování dat
- narušování běhu informačních systémů
- zneužití technických prostředků k výše uvedeným činům (včetně jejich držení)
- padělání za užití počítače
- počítačový podvod
- výroba, distribuce, získávání a držení dětské pornografie na datových nosičích
- porušování autorských práv a práv souvisejících
- pomáhání nebo návod k uvedeným činům

K uvedenému katalogu je však třeba dodat, že v mnohých případech mají jednotlivé státy možnost uplatnit výhradu a nestíhat určité typy uvedených jednání – je tedy například možné na základě výhrady nezahrnout do národní trestní legislativy například skutkové podstaty vyhledávání a držení dětské pornografie na datových nosičích.

Členské státy se v Úmluvě rovněž zavázaly provést taková legislativní opatření, která jejich orgánům umožní tyto trestné činy vyšetřovat a zajišťovat k tomu odpovídající důkazy.[31] Obě skupiny závazků, tj. závazek zavést do národní trestní legislativy příslušné skutkové podstaty trestných činů a závazek uzákonit odpovídající procesní pravomoci orgánů činných v trestním řízení pak mají jednoznačný cíl zabránit situaci, kdy by některý z nově definovaných tzv. kyberkriminálních činů postrádal v některém členském státě trestnost nebo by zdejší orgány činné v trestním řízení nedisponovaly

[28] Plný text Úmluvy v anglickém jazyce viz na adrese http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

[29] Precizní definice jednotlivých skutkových podstat internetové trestné činnosti představuje přitom jeden z hlavních problémů omezujících působnost trestního práva v kyberprostoru. K tomu srov. Plays, J. Internet and Judicial Investigation: Difficulties in Judicial Practice. In: Internet International Law, Bruxelles: Bruylant, 2005, str. 245 a násl.

[30] Specifikace skutkových podstat jsou provedeny v čl. 2–11 Úmluvy.

[31] Závazek zavést do právního řádu příslušná opatření najdeme v čl. 14–21 Úmluvy.

procesními oprávněními nutnými k tomu čin vyšetřit a prokázat. Dodrží-li tedy státy tyto své základní závazky, měl by zde odpadnout problém existence tzv. bezpečných přístavů pro pachatele internetové trestné činnosti.

Co do závazků týkajících se delimitace jurisdikcí nebo vzájemné spolupráce je již však Úmluva o kyberkriminalitě mnohem zdrženlivější. Obsahuje sice celou hlavu věnovanou otázkám jurisdikce a vzájemné spolupráce orgánů členských států, nejedná se však o skutečnou delimitaci jurisdikcí nebo o založení povinnosti provádět na dožádání úkony v trestním řízení jako například zajištění důkazů, zajištění podezřelých apod.

Jak vyplývá zejména ze znění článku 5, neřeší úmluva pozitivní konflikt působnosti orgánů více států v trestním řízení, což je možné považovat v souvislosti s provedeným výkladem za podstatný problém. Otázka delimitace jurisdikce by však v opačném případě zřejmě narazila na limity diskrece jednotlivých států a ústavněprávní limity zejména v otázkách vydávání vlastních občanů k trestnímu stíhání do zahraničí.[32]

Podstatným přínosem Úmluvy je naopak zavedení mechanismů, které z procesního hlediska usnadňují vyšetřování trestných činů a shromažďování důkazů. Články 23–34 tak upravují postupy a vzájemnou asistenci v procesech vydávání pachatelů kyberkriminálních činů a spolupráci při vyšetřování a získávání důkazního materiálu. Článek 35 pak zavádí institut kontaktních center s nepřetržitým provozem, jejichž úkolem je formou agenturní činnosti koordinovat vzájemnou spolupráci orgánů činných v trestním řízení.

Úmluva Rady Evropy o kyberkriminalitě představuje jednu z prvních iniciativ založených s cílem minimalizovat negativní dopad delokalizace internetových aktivit na efektivitu práva.[33] Přestože je dosah Úmluvy v některých směrech omezený (zejména co do delimitace jurisdikcí a místní působnosti norem trestního práva hmotného), představuje její koncepce nesporný a relativně významný krok kupředu. Skutečnému naplnění cílů Úmluvy[34] však stále brání relativně nízký počet stran, které ji ratifikovaly[35] a recipovaly do vnitrostátního práva. Opatrně optimisticky však lze hodnotit skutečnost, že Úmluva byla již podepsána většinou evropských států včetně ČR[36] a její ratifikace je tak mnohdy spíše otázkou času[37]. Za velice významný pokrok při budování mezinárodní trestní jurisdikce nad kyberprostorem pak lze považovat skutečnost, že Úmluvu po-

[32] K problému viz. De Vel, G. The Convention on Cybercrime. In: Internet International Law, Bruxelles: Bruylant, 2005, str. 225 a násl.

[33] Důležitost mezinárodní harmonizace národních trestních legislativ a praxe trestního řízení byla opakovaně zdůrazňovaná i v rámci ženevského jednání Mezinárodní telekomunikační unie zaměřeného na problematiku kyberkriminality. Jednotlivé poznatky shrnuje článek Schjolberg, S., Hubbard, A. M. Harmonizing National Legal Approaches on Cybercrime. Geneva: ITU (publikace č. CYB/04). 2005. Volně ke stažení na adrese http://www.itu.int/osg/spu/cybersecurity//docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf.

[34] Viz text preambule Úmluvy.

[35] K vývoji Úmluvy viz zpráva z jednání Komise Rady Evropy pro Kyberkriminalitu č. T-CY (2006) 11 – relativně vysoký počet států, které k úmluvě nepřistoupily, ale účastní se jednání Komise, však napovídá o zvyšujícím se zájmu států o tuto problematiku.

[36] Do českého trestního zákonodárství se příslušné závazky z Úmluvy měly recipovat především prostřednictvím nového trestního zákoníku, který však z politických důvodů nebyl doposud schválen.

[37] Celkový počet států, které úmluvu ratifikovaly, je prozatím 19. Na ratifikaci se dále čeká ve 24 státech včetně ČR.

depsaly a ratifikovaly USA – lze tedy očekávat, že ostatní státy budou tento příklad v zápětí následovat. Architekti Úmluvy přitom předpokládají, že další rozvoj internetové trestní jurisdikce bude probíhat prostřednictvím dodatkových protokolů k Úmluvě, které postupně postihnou další konkrétní typy trestné činnosti či dokonce přestupků.

4. KRÁTCE K PROBLÉMU SPRÁVNÍ A FINANČNÍ JURISDIKCE

Zatímco trestní i soukromé právo se mají možnost při vyrovnávání se s nově nastolenými problémy internetové jurisdikce opřít o více či méně tradiční mechanismy a principy, správní právo bylo s příchodem společenských vztahů nové kvality zastiženo, obrazně řečeno, s kalhotama napůl staženýma. Normy správního práva či též jednoduchého práva státního si tak neměly až na výjimky možnost postupně zvykat na existenci vztahů, jejichž aspekty nutí státní orgány uvažovat v mezinárodním měřítku, neboť jednoduchá konstrukce takových vztahů, tj. adresát-orgán, takový postup nikdy přímo nevyžadovala. S rozvojem přeshraničních on-line vztahů se tedy musí správní právo včetně práva finančního potýkat s již popsanou krizí efektivity a legitimity prakticky bez předchozích zkušeností s řešením přeshraničních otázek.[38]

V oboru finančního práva představují aktuálně problém především kriteria místa zdanitelného plnění a domicilu subjektů internetových transakcí. Hrozí přitom riziko, že podobně, jako mohou pachatelé trestné činnosti unikat postihu plynulým přesouváním mezi jurisdikcemi nebo svým umístěním mimo jurisdikce, lze se analogicky vyhnout i zdanění či působnosti jiného.[39]

Kritérium místa zdanitelného plnění lze přímo srovnat s určovatelem *loci solutionis*. U čistě internetových transakcí, tj. nikoli tam, kde internet slouží pouze ke komunikaci projevů vůle, je pak *locus solutionis* značně problematickým určovatelem[40] umožňujícím navíc rozsáhlé spekulace. I přes snahu správních orgánů se přitom tento problém doposud nedaří uspokojivě řešit.[41]

Problém určení místa plnění je v současné době aktuální mimo jiné i v loterijním právu. Jako zásadní se příkladně jeví být otázka, kde nastává místo plnění v případě kursové sázky internetové sázkové kanceláře usazené pod jurisdikcí cizího státu, tzn. zda je takovou sázku třeba posuzovat jako podanou na území cizího státu (tj. v místě domicilu kanceláře) nebo zda je nutné ji řešit jako by byla poskytnuta pobočkou kanceláře na území sázejícího. Obě možnosti mají pak dalekosáhlé dopady nejen na vztah mezi kanceláří a sázejícím ale též na otázky administrativní regulace činnosti kanceláří, jejich zdanění apod.

---

[38] Výjimkou je v tomto směru snad jen problematika cel a dalších administrativních překážek mezinárodního obchodu a koordinace preventivních opatření k zamezení dvojího zdanění.

[39] K tomu srov. Brunori, D. The Politics of State Taxation: Saving the Internet from the Taxman. State Tax Notes, 2003, ročník 29, č. 6, str. 1 a násl.

[40] K diskusi charakteru tohoto hraničního určovatele a problémům při jeho aplikaci na soukromoprávní vztahy viz Polčák, R. Právo na internetu – spam a odpovědnost ISP. Brno: Computer Press, 2007, str. 15 a násl.

[41] Srov. např. poziční dokument Komise publikovaný pod číslem COM(1998) 374 (Communication from the Commission on Electronic commerce and indirect taxation) a reakci ECOSOC pod č. OJ C 407 ze dne 28. 12. 1998.

Spory o správní jurisdikci nad sázkovými kancelářemi jsou v současné Evropě velmi časté a lze si je představit i jako jakýsi předvoj dalších přeshraničních administrativně-právních konfliktů. Problém zde spočívá především ve spojení principu svobody pohybu služeb a rozdílné kvality národních správních legislativ umocněném delokalizací celosvětové informační sítě. V řadě států jako například ve Francii nebo v Maďarsku je tak například loterijní a sázková činnost v určitých oblastech předmětem státního monopolu, jinde se jedná o koncesovanou, vázanou či dokonce volnou činnost. Usadí-li se pak sázková kancelář na území některého se států s mírnější administrativní regulací a začne-li nabízet své služby po internetu, má v porovnání s konkurenty z ostatních států mnohem výhodnější tržní pozici, přičemž díky internetu může obsáhnout i zákazníky v mnohem rigoróznějších jurisdikcích nebo i tam, kde je tato činnost předmětem státního monopolu. Státy se proti takovému jednání brání různě – české Ministerstvo financí se tak vydalo před časem cestou soudní a podobné řešení přijaly k ochraně loterijních a sázkových zákonů i jiné státy jako například Francie. V Maďarsku došlo dokonce k legislativnímu řešení tohoto problému formou prostého zákazu poskytování příslušných služeb prostřednictvím internetu bez ohledu na domicil poskytovatele. Toto legislativní řešení však ještě, než mohl příslušný zákon nabýt platnosti, bude muset projít přes maďarský Ústavní soud a je velmi pravděpodobné, že jeho aktuální podoba bude shledána protiústavní a v rozporu s mezinárodními závazky Maďarska plynoucími z členství v ES.[42] Soudní řešení problému internetového sázení však, jak je možné vidět na příkladu několika již pravomocně rozhodnutých sporů, nemusí vést ke kýženému úspěchu – problémem je zde vykonatelnost příslušných soudních rozhodnutí.

Jeden z nejznámějších případů kolize správních legislativ v otázce internetového sázení byl pravomocně rozhodnut ve Francii a týkal se dostihových sázek. Na ty má na Francouzském území monopol společnost Pari Mutuel Urbain. Sázky na francouzské dostihy však začala po internetu nabízet i společnost Zeturf usazená na Maltě.[43] Francouzské soudy sice pravomocně zakázaly společnosti Zeturf provozovat on-line sázky na francouzské dostihy,[44] rozhodnutí však nebylo na Maltě uznáno a vykonáno pro rozpor s maltskými zákony.[45] Společnost Zeturf tedy nadále poskytuje uvedené služby, a to podle maltských zákonů.[46]

---

[42] O ústavní stížnosti, která čeká na rozhodnutí u maďarského Ústavního soudu, podrobně referoval na konferenci Kyberprostor 2006 vedoucí Centra pro ICT právo Právnické fakulty Univerzity v Pécsi, Dr. Zsolt Balogh.

[43] Relativně benevolentní správní úprava pro poskytování on-line sázek na Maltě způsobila, že většina evropských on-line sázkových kanceláří je usazena právě zde. Sázkový průmysl je tak jedním z významných zdrojů maltské ekonomiky.

[44] Rozhodnutí Odvolacího soudu v Paříži ze dne 4. 1. 2006 č.j. 05/15773, rozhodnutí lze ve formě scanu nalézt na adrese http://www.droit-technologie.org/jurisprudences/CA_paris_%20-040106.zeturf.pdf.

[45] Sporu se věnovala řada francouzských odborných i laických médií – viz např. Devillard, A. Zeturf.com contre PMU, les paris judiciaires sont ouverts. 01net.com, 13. 7. 2005, publ. on-line na adr. http://www.01net.com/article/284722.html, faktická rekapitulace sporu viz Marchand, M.-J. Quand Zeturf se moque des monopoles. Droit-NTIC.com, 3. 7. 2006, publ. on-line na adr. http://www.droit-ntic.com/news/afficher.php?id=366.

[46] Není přitom příliš pravděpodobné, že by Francie v této věci podala žalobu proti Maltě u Evropského soudního dvora – argumenty proti principu volného pohybu služeb by se v tomto případě hledaly jen těžko. Rozhodnutí francouzského soudu sice diskutuje i otázku proporcionality, není však pravděpodobné, že by se Evropský soudní dvůr k této argumentaci přihlásil.

Zatímco *locus solutionis* je typickým hraničním určovatelem v oblasti administrativní regulace poskytování služeb a finančněprávní úpravy nepřímých daní, je domicil či *patria* důležitým kritériem zejména pro obor přímých daní. Můžeme sice v této věci odkázat na diskusi možností uplatnění tohoto kriteria v oboru soukromého práva,[47] je však třeba poukázat na zásadní odlišnost v otázce hraničního určovatele místa tzv. jiné provozovny (other establishment). K úvaze o odlišné a mnohem restriktivnější interpretaci pojmu jiné provozovny pro potřeby finančního či správního práva nás přitom vede především diametrálně odlišná teleologie příslušných norem. Zatímco dominantním cílem kolizních norem soukromého práva je rozumné uspořádání vztahů rovných subjektů, můžeme v případě práva správního hovořit spíše o relevanci principů právní jistoty, ochrany adresáta nebo o zákazu svévole. Kritérium provozovny či jiné provozovny je tedy nutné posuzovat odlišně, hovoříme-li o něm v souvislosti se soukromoprávním závazkem nebo se správní povinností. Adekvátní správní interpretací tak bude taková, která vyjde z *a priori* jasných kriterií a v jejímž důsledku dojde jen k minimálnímu omezení autonomie příslušného subjektu. Je tedy třeba prozatím odmítnout, na rozdíl od mezinárodního práva soukromého, možnost založení správní jurisdikce například na základě registrace doménového jména s určitou národní doménou první úrovně.[48] Případná nová či nestandardní kritéria pro určení domicilu tak budou muset mít zřejmě oporu nikoli jako v případě soukromého práva v extenzivní interpretaci ale přímo v *expressis verbis* projevené vůli státu, ať už ve formě zákona nebo mezinárodní úmluvy.[49]

5. NĚKOLIK ZÁVĚREČNÝCH POZNÁMEK K TZV. INTERNETOVÉ JURISDIKCI

Při hledání odpovědí na obtížné otázky související s tzv. internetovou jurisdikcí je třeba připravit se na paradox klasického příkladu hard case, tj. věšení Picassova obrazu. Můžeme si tak představit učebnicovou situaci, kdy paní domu zakoupí za pár korun ve vetešnictví reprodukci Picassova obrazu a zavěsí ji na volné místo na zdi na chodbě hned vedle dveří na WC. Když ji pak přijde navštívit známý kunsthistorik, náhodou obraz na zdi objeví a sdělí majitelce, že šťastně nezakoupila reprodukci ale originál. Paní tedy vezme obraz a přemístí jej do obývacího pokoje na nejčestnější místo hned nad televizí.

Poslední řešení, tedy umístění obrazu v obývacím pokoji, je možné objektivně považovat za rozumné. To však neznamená, že bychom o předchozím řešení, tj. zeď ved-

[47] Viz Polčák, R. Právo na internetu – spam a odpovědnost ISP. Brno: Computer Press, 2007, str. 32 a násl.

[48] Shodně viz Reed, C. Internet Law. Cambridge: Cambridge University Press, 2004, str. 238. Stejné stanovisko je možné nalézt i v čl. 42–42.10 Komentáře k Modelové úmluvě o daních OECD. Text úmluvy viz http://www.oecd.org/dataoecd/52/34/1914467.pdf, text komentáře viz http://www.hmrc.gov.uk/manuals/intmanual/INTM159000.htm.

[49] Detailní analýzu problematiky zdanění příjmů z internetového podnikání a návrh alternativních kriterií k delimitaci správní jurisdikce obsahuje materiál OECD nazvaný Are the Current Treaty Rules for Taxing Business Profits Appropriate for e-Commerce?, který je volně ke stažení na adrese http://www.oecd.org/dataoecd/58/53/35869032.pdf.

le dveří na WC, mohli prohlásit, že bylo zvoleno chybně. Stejně tak nemáme jistotu, že nepřijde ještě vzdělanější odborník, který obraz později opět neprohlásí za padělek, v důsledku čehož bude opět dobrý důvod pověsit jej jinam (třeba ne hned vedle WC, ale například do kuchyně) a obývák dekorovat něčím hodnotnějším. Zbývá ale dodat, že tato nejistota však rozhodně není důvodem k tomu umístit obraz do sklepa a počkat, jak se situace vyvine.

Vztáhneme-li na aktuální situaci okolo jurisdikce či obecně působnosti práva na internetu uvedený příklad, můžeme konstatovat, že problém již zde visí a opatrně s ním začínáme manipulovat. Důležité však je uvědomit si, že k tomu, abychom nalezli jeho alespoň částečně stabilní (správné) řešení, budeme především potřebovat mnohem více empirických informací, ať už se bude jednat o informace právní, sociologické, technické či ekonomické. Diskutujeme-li tedy nyní právní otázky související s působností práva na internetu, nemělo by být naše úsilí posuzováno jako snaha s ambicí permanence či dokonce objektivní a absolutní správnosti, ale spíše jako hledání co nejlepších řešení za daných okolností. Hodí se tedy v tomto kontextu uzavřít konstatováním, že právo je sice objektivně uměním dobrého a spravedlivého, subjektivně se však často jedná spíše o umění možného.[50]

THE PROBLEM OF PENAL JURISDICTION OVER THE INTERNET

Summary

When assessing the applicability of law in cyberspace, it is not possible to simply follow the traditional criteria and to state that the law universally applies. As demonstrated on multiple examples, there are new emerging factors that affect not just the ways of assessment of particular elements of territorial or subject-matter applicability of law but its applicability over artificially created environments in general. Even the state itself often hesitates to enter the cyberspace with its imperative laws and enforcement agencies.

However, there are at the moment solid grounds for the law to reason its existence and regulative powers in social environments that emerge in virtual spaces. The empirical data show growing presence of chaotic elements such as various forms of destructive hacking, dissemination of child pornography, privacy infringements etc. that are unable to be countered by self-organizing mechanisms. Up to that, various relevant interests now present and active in cyberspace, out of which we should stress namely those of commercial nature, are not ex definitione capable to protect the basic principles and core values of the society.

Despite of the fact that the penal law aims to protect the aforementioned basic values and core interests of the states, its particular applicability in cyberspace remains more than questionable. The reason for that we find namely in still remaining problem of passive and active territorial conflict of penal jurisdictions over cyberspace. This conflict causes that on-line criminals might either find safe harbours or that they might rely on technical and namely formal complexity of the processes of cross border investigation, extradition, etc.

The Council of Europe was constantly showing during the last couple of years remarkable efforts in countering cybercrime. These efforts finally led to relatively successful adoption of International Conven-

[50] Nosnou je tato teze především pro pragmatickou právní metodologii a není případná jen pro otázky internetové jurisdikce ale prakticky pro všechny oblasti oboru práva informačních technologií. K pojmu a vývoji pragmatické metody viz např. Dickstein, M. Pragmatism Then and Now. In: Revival of Pragmatism. London: Duke University Press, 1998, str. 1 a násl.

tion on Cybercrime. Unfortunately (but not surprisingly), this convention addresses namely the removal of safe harbours for cybercriminals by harmonizing the general list of typical criminal activities in cyberspace. As to the jurisdictional issues, it only adopts a system of exchange of information and motivates the member states to closely cooperate on investigation and prosecution of cybercrime. Consequently, we still have to work with more or less traditional interpretational patterns using the criteria of locus conducti, locus delicti, locus damni etc. With this respect, it is to be said that more precise or more suitable criteria for delimitating penal jurisdictions are not likely to be developed and adopted in foreseeable future. The reason is, besides high sensitivity of the issue of limiting the state jurisdictions in their vital area of interest, also constitutional grounds that in many times protect individuals from penal jurisdictions of foreign states.

Therefore, we might conclude that the issue of penal territorial internet jurisdiction does not have any firm, fixed or stable solutions and it is very unlikely that such solutions will be developed and implemented in foreseeable future. Consequently, we have to work with pragmatic method when dealing with investigation and prosecution of cybercrime. In other words, we focus on particular situations and try to develop for them particular ad hoc solutions without having an ambition for objectivity or permanence of such solutions. Only that kind of approach might sooner or later lead into the establishment of more solid and stable grounds for penal jurisdiction over the internet.

Key words: cyberspace; cyberlaw; cybercrime; jurisdiction; applicability of law

Klíčová slova: kyberprostor; kyberkriminalita; počítačová kriminalita; jurisdikce; působnost práva

2008 ACTA UNIVERSITATIS CAROLINAE – IURIDICA 4 PAG. 107–129

ODPOVĚDNOST PROVIDERŮ SE ZAMĚŘENÍM NA ODPOVĚDNOST HOST-PROVIDERA A ACCESS-PROVIDERA

JIŘÍ ŘÍHA
Katedra trestního práva Právnické fakulty Univerzity Karlovy v Praze
Obvodní soud pro Prahu 2

V prostředí internetu je třeba řešit řadu zcela zásadních právních otázek, které v jiných prostředích nevytanou ani na mysl. V souvislosti s rozvojem internetu jednak se rozvíjejí zcela nové typy kriminality, jednak dostávají zcela nový rozměr stávající typy kriminality. Na provádění jakékoliv činnosti v prostředí internetu, ať legální či nelegální, se účastní mnoho subjektů, nejde prakticky nikdy výhradně o činnost jednotlivce, jak je tomu často (či zpravidla) u běžné kriminality (např. u krádeže, ublížení na zdraví apod.). Pachatel páchající trestné činy prostřednictvím internetu může (či dokonce musí) při svém trestném činu (např. při neoprávněném šíření díla chráněného autorským právem) využít služeb celé řady subjektů – např. (1) provozovatele internetové kavárny (či školy), (2) poskytovatele připojení této kavárny (školy) k internetu, (3) provozovatele serveru, na němž jsou umístěny internetové stránky, na nichž je umístěn protiprávní obsah, dokonce ale obsah nemusí být umístěn hned na prvních stránkách, je na nich umístěn jen odkaz (4) na jiné stránky, které jsou umístěny na jiném serveru (5). Takto bychom pak mohli počet subjektů stále rozšiřovat. Můžeme uvažovat i o odpovědnosti provozovatele internetových vyhledavačů (vlastně podobně jako 4 a 5). Zde je nastíněna velice primitivní struktura jiných subjektů odlišných od přímého pachatele, jejichž odpovědností se musíme zabývat. Prakticky vždy vyvstane otázka odpovědnosti subjektů uvedených shora pod body (2) a (3). Někdy se celá problematika zkráceně shrnuje jako otázka „***odpovědnosti za cizí obsah***", jde především o to, nakolik v rámci svého legálního a společensky prospěšného podnikání mají být shora nastíněné subjekty odpovědné za osoby, které jejich služeb využijí ke spáchání vlastních trestných činů a v jakých případech mají uvedené subjekty povinnost zasáhnout. Tím bychom se měli zabývat v tomto příspěvku.

1. VYMEZENÍ NĚKTERÝCH POJMŮ

V příspěvku budeme pracovat s pojmy, z nichž některé nejsou běžně užívány hovorovou či dokonce spisovnou češtinou, vesměs jde o pojmy v anglickém jazyce, které mají svůj specifický obsah a které se mezi odborníky na kybernetiku a informační služby obvykle nepřekládají.

Předně je třeba rozlišovat **internet**, což je nejobecnější pojem pro celosvětovou počítačovou síť, která spojuje jednotlivé menší sítě pomocí sady protokolů IP (Internet Protocol), od pojmu **World Wide Web** (WWW, někdy jen zkráceně Web, příp. i W3), kterým se rozumí informační síť, organizovaná jako obrovský hypertextový dokument.[1] Často se termínem internet rozumí právě síť world wide web. Internet je ovšem mnohem starší, umožňuje přenos dat i jiným způsobem[2] než jen prostřednictvím hypertextových dokumentů, které původně sloužily pro sdělování informací a později i jako uživatelské rozhraní pro veřejné služby a aplikace (jde o nepřeberné množství služeb od elektronické pošty, přes správu bankovních účtů, komunikaci s úřady, až po přenos zvuku, obrazu, či hraní her). **Webové stránky** jsou zobrazovány v prohlížečích (angl. browser – např. Internet Explorer, Netscape Navigator, Firefox, Mozilla), které dokáží převést zdrojový kód stránek (ve formátu HTML[3], PHP, Javascript etc.) uložený na serverech do výsledné podoby, která se nám zobrazí na obrazovce. Pro webové stránky je typické propojení pomocí hypertextového odkazu (tzv. **hyperlink**, popř. jen link), kterým se odkazuje na jiné dokumenty umístěné na webu. Odkazuje se obvykle pomocí slovně vyjádřených názvů internetových stránek na tzv. URL (Uniform Resource Locator), tedy internetový ekvivalent pro adresu, výraz, který jedinečným způsobem identifikuje soubor v internetu (např. http://www.prf.cuni.cz/). Slovně vyjádřené adresy (doménová jména) jsou tzv. **DNS servery** (Domain Name System) převáděny (podobně jako je tom u v telefonním seznamu) na skutečné číselně vyjádřené internetové adresy, díky nimž je vyvolán skutečný adresovaný počítač s konkrétní **IP-Adresou** (Internet Protocol – Adresa)[4], se žádaným obsahem. IP-Adresy mohou být statické nebo dynamické, statické jsou přiděleny nastálo určitým počítačům (především webovým či e-mailovým serverům), zatímco dynamické jsou přiděleny DHCP serverem počítačům klientů jen po dobu připojení k internetu jejich prostřednictvím z množiny volných IP adres, po odpojení takového počítače se číselný kód vrací k dalšímu využití ISP.[5]

Příspěvek se zaměřuje na odpovědnost tzv. providerů, mezi nimiž je třeba rozlišovat. **Provider** je obecně poskytovatel internetových služeb. Pod termínem Internet Service Provider (ISP) se původně rozumělo několik poskytovatelů připojení k internetu, kteří byli připojeni k centrální síti, tzv. backbone (páteři), a na něž se hierarchicky připojovaly další instituce. Později v rámci privatizace internetu se výrazně rozšířil počet těchto poskytovatelů (ISP), na něž se napojovaly počítače podniků,

---

[1] Tak např. encyklopedie Wikipedia dostupná dne 10. 6. 2008 na internetu – http://cs.wikipedia.org/wiki/internet. Podobně také Universum: všeobecná encyklopedie. Praha: Odeon, 2002. Díl 2 (G–L), str. 302 (heslo internet); též Díl 4. (Ř–Ž), str. 700 (heslo www). Podobně Ottova encyklopedie – Česká republika. Díl 5., str. 180 (heslo internet – včetně přehledného popisu rozvoje užívání internetu v České republice).

[2] Např. FTP – File Transfer Protocol, přenos souborů; SMTP – Simple Mail Transfer Protocol, elektronická pošta (e-mail), přenos e-mailů; POP3, IMAP – protokoly (služby) pro přístup k e-mailu.

[3] HyperText Markup Language.

[4] V současnosti jde o verzi 4 v podobě 32 bytového čísla sestávajícího pro snadnější orientaci ze čtyř čísel od 0 do 255 oddělených tečkou, vzhledem k nedostatku adres bude zaváděna verze 6. Stránky www.prf.cuni.cz jsou umístěny na serveru s IP-Adresou: 195.113.8.11. Odpojením takového počítače se číselný kód vrací k dalšímu využití ISP.

[5] DHCP (Dynamic Host Configuration Protocol) se dnes nejčastěji používá pro dynamické (okamžité, automatické) přidělování IP-adres jednotlivým osobním počítačům v počítačových sítích bez potřeby registrace, má-li ale DHCP server seznam MAC adres a k nim příslušných IP-Adres, nevrací jednou přidělenou IP adresu konkrétnímu počítači do množiny IP-Adres volně přidělovaných.

škol, vědeckých institucí i jednotlivých fyzických osob, tzv. WAN (Wide Area Network). Spojení více počítačů v rámci jednoho podniku, školy apod. se nazývá LAN (Local Area Network). Termínem ISP se dnes někdy rozumí takový poskytovatel připojení k internetu, který zároveň nabízí další služby (např. velcí telekomunikační operátoři).[6] Za **Access-Provider** (doslova poskytovatele přístupu) je označován ten, kdo pouze umožňuje přístup k cizím internetovým zdrojům, obvykle tedy, kdo zajišťuje technický přenos dat. **Host-Provider** (doslova poskytovatel hoštění; někdy též Hosting, někdy i **Service-Provider**) umožňuje přístup k cizím informacím, které má umístěny na svých počítačích, zejména poskytuje jiným uživatelům tzv. prostor na internetu (zpravidla úplatně, ať již přímo či prostřednictvím reklamy, především reklamních bannerů), tedy vlastně umožní jiným subjektům uložit na svých serverech jejich soubory obsahující jejich informace a zajistí přístup k nim prostřednictvím internetu. Prakticky jen u těchto dvou providerů nás zajímá otázka možnosti odpovědnosti za cizí obsah umístěný na internetu. To je rozdíl od **Content-Provideru** (doslova poskytovatel obsahu), za kterého se považuje každý, kdo na internetu nabízí své vlastní informace, svůj vlastní obsah, ať již umístěný na vlastním počítači připojeném k síti internetu, či na počítači jiného (host-providera).

2. EVROPSKÉ PŘEDPISY

Při řešení otázky odpovědnosti tzv. providerů, resp. poskytovatelů služeb informační společnosti, jsou pro nás důležité předpisy evropských společenství. Evropský parlament přijal dne 8. června 2000 **Směrnici Evropského parlamentu a Rady 2000/31/ES** o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu na vnitřním trhu („směrnice o elektronickém obchodu"). Evropská unie tak plní své vlastní cíle, které má vytyčeny především ve Smlouvě o založení Evropského společenství, snaží se o vytvoření těsnějších vazeb mezi evropskými státy a občany a o zajištění hospodářského a sociálního pokroku, naplnění základních cílů ES/EU, mimo jiné též zajištění volného pohybu zboží a služeb, k čemuž má přispět i rozvoj služeb informační společnosti, jenž byl dosud omezován řadou právních překážek řádného fungování vnitřního trhu spočívajících v rozdílech mezi vnitrostátními právními předpisy jednotlivých členských států ES/EU, jejichž právní řády bylo proto potřeba koordinovat a přizpůsobovat. Směrnice si kladla za cíl stanovit pro zaručení právní jistoty a důvěry spotřebitelů jasný obecný rámec pro řešení některých právních aspektů elektronického obchodu na vnitřním trhu a vytvořit právní rámec pro zajištění volného pohybu služeb informační společnosti mezi členskými státy, cílem ovšem nebylo harmonizovat trestní právo jako takové.[7]

Tato směrnice navazuje na některé dřívější Směrnice Evropského parlamentu a Rady, především na Směrnici 98/34/ES, ze dne 22. června 1998, o postupu při poskytování

[6] Tak narozdíl od jiných Access-Providerů – srov. Marberth-Kubicky, A. Computer- und Internetstrafrecht. München: C.H.Beck, 2005, str. 7.

[7] K tomu všemu srov. čl. I body 1. a 2. uvedené Směrnice Evropského parlamentu a Rady 2000/31/ES.

informací v oblasti technických norem a předpisů, popř. Směrnici 98/84/ES, ze dne 20. listopadu 1998, o právní ochraně služeb s podmíněným přístupem a služeb tvořených podmíněným přístupem, které již obsahují definici služeb informační společnosti, na což Směrnice 2000/31/ES také odkazuje. **Službou informační společnosti** se rozumí široká škála hospodářských činností, které probíhají tzv. on-line, např. on-line prodej zboží, služby umožňující uzavírání smluv on-line, služby on-line poskytující informace nebo obchodní sdělení, služby, které poskytují nástroje umožňující vyhledávání dat, přístup k datům a získávání dat, služby spočívající v předávání informací prostřednictvím komunikační sítě, v poskytování přístupu ke komunikační síti nebo v shromažďování informací poskytovaných příjemcem služby, elektronická pošta. Směrnice stanoví též, co pod uvedený pojem nespadá – např. televizní vysílání, rozhlasové vysílání, činnosti, které nelze vykonávat na dálku. „**Poskytovatelem**" ve smyslu Směrnice je každá fyzická nebo právnická osoba, která poskytuje určitou službu informační společnosti, „**příjemcem služby**" pak každá fyzická nebo právnická osoba, která k profesním či jiným účelům využívá služeb informační společnosti, zejména pro vyhledávání či zpřístupňování informací, a „**spotřebitelem**" každá fyzická osoba, která jedná za účelem nespadajícím do její profesní či obchodní činnosti.

Tato směrnice vedle řady dalších otázek řeší námi zkoumanou otázku „**odpovědnosti za cizí obsah**", tedy slovy směrnice **odpovědnosti poskytovatelů služeb informační společnosti v oddílu 4.** (články 12 – pouhý přenos, čl. 13 – caching, čl. 14 – hosting a čl. 15 – neexistence obecné povinnosti dohledu). Jde o důležitá omezení odpovědnosti poskytovatelů informačních služeb, aby se vytvořil vhodný prostor pro podnikání, odstranily se překážky fungování vnitřního trhu ztěžující rozvoj přeshraničních služeb a narušujících hospodářskou soutěž. Přílišné přepětí odpovědnosti poskytovatelů informačních služeb, zvláště při nejednotné právní úpravě v jednotlivých zemích ES/EU, by bylo brzdou hospodářského rozvoje ve srovnání s USA či asijskými státy. To bylo důvodem omezení odpovědnosti poskytovatelů informačních služeb. Poskytovatelé služeb jsou pouze za určitých okolností povinni jednat, aby předešli a zabránili protiprávnímu jednání. Směrnice si klade za cíl vytvořit vhodný podklad pro vypracování rychlých a spolehlivých metod na odstranění protiprávních informací a na znemožnění přístupu k nim, což měly zajistit členské státy vzájemnou spoluprací a následně vnitrostátní úpravou. V oddílu 4. stanovené odchylky v úpravě odpovědnosti poskytovatelů informačních služeb jsou vázány na pasivitu takového poskytovatele, zahrnují proto **pouze případy, v nichž je činnost poskytovatele služeb informační společnosti omezena na technický postup provozování komunikační sítě a na zprostředkovávání přístupu k této síti, na níž jsou informace poskytnuté třetími osobami přenášeny nebo dočasně ukládány za jediným účelem zlepšení účinnosti přenosu, přičemž jeho činnost má čistě technickou, automatickou a tedy pasivní podobu.** Poskytovatel služeb informační společnosti tedy nezná a ani nekontroluje přenášené či ukládané informace. Výjimečná úprava (často uváděné tzv. privilegování) se vztahuje na „prostý přenos" a na ukládání do vyrovnávací paměti (tzv. „caching"), pokud se přenášená informace nepozměňuje, což se ovšem netýká zásahů technické povahy během přenosu, neboť takto se nemění celistvost přenášené informace, zvlášť je upravena též odpovědnost za uložení cizích informací (Host-Provi-

der). Pokud ale naopak poskytovatel služeb úmyslně spolupracuje s jedním z příjemců svých služeb, aby se dopouštěl protiprávního jednání, poskytuje více než „prostý přenos" nebo ukládání do vyrovnávací paměti („caching"), nemůže se pak dovolávat výjimky z odpovědnosti stanovené Směrnicí.

Jinými slovy Směrnice nedopadá na taková jednání poskytovatelů internetových služeb, která mají aktivní povahu a která bychom z hlediska trestněprávní teorie označili jako konání, tedy (v souladu s českou teorií zjednodušeně řečeno) vůlí řízený pohyb, ovšem za předpokladu aktivního směřování k trestněprávně relevantnímu následku i ze strany takového poskytovatele internetových služeb.[8] V takovém případě by se jednalo zřejmě o některou z forem účastenství na trestném činu (v širším smyslu, tedy včetně spolupachatelství). Taková jednání jsou z úpravy Směrnice vyloučena, Směrnice tedy na ně nedopadá. Směrnice dopadá pouze na jednání spočívající v zavedení procesů technické povahy. Dalo by se při zohlednění německé trestněprávní teorie hovořit o omezení odpovědnosti poskytovatelů za tzv. neutrální jednání, jimiž se rozumí právně dovolené činnosti, které samy o sobě nesměřují ke spáchání činu, přesto si osoby provádějící taková jednání mohou být vědomy možnosti, že jejich jinak neutrální jednání bude využito ke spáchání trestného činu a pro ten případ jsou s tím srozuměny, resp. nijak proti tomu nezasáhnou.[9] Jde tak mnohem spíše o problematiku opomenutí, o problematiku, kdy takoví poskytovatelé musí zasáhnout proti osobám zneužívajícím jejich jinak právně neutrální jednání, neboli o otázku, zda jsou garanty – dozorci dohlížejícími nad zdrojem nebezpečí, které je v jejich správě. Směrnice při tom výslovně uvádí, že taková určitá neutrální jednání nemají být trestná.

Úprava nastíněných otázek je v zásadě podobná té, kterou již dříve měli Němci ve svém Teledienstegesetz (TDG), resp. Mediendienste-Staatsvertrag (MDStV), podobně měl odpovědnost poskytovatelů upraven též americký Digital Millenium Copyright Act (DMCA) z roku 1998.[10]

---

[8] Zde se jeví zjednodušená definice jednání (resp. konání a opomenutí) užívaná v české trestněprávní teorii jako nevhodná. Zřejmě přesnější by v tomto ohledu byly definice užívané německou teorií, především pak sociální definice jednání užívaná Jescheckem. Srov. k tomu více v Říha, J. Změníme s novým trestním zákoníkem též systém znaků trestného činu? Navrhovaný trestní zákoník z pohledu německého systému znaků trestného činu – srovnávací studie. AUC Iuridica, 2002, č. 4, str. 21 a násl. Zdá se též, že činnost poskytovatele by měla být vnímána spíše jako konání, neboť provider poskytuje službu informační společnosti, musel tedy nutně alespoň v některém období vyvinout aktivní činnost, aby např. mohl fungovat přenos dat, musí svá zařízení spravovat a udržovat, musel např. instalovat potřebný software, nicméně konkrétní přenos dat, popř. jiná poskytovaná služba je již poskytována automaticky prostřednictvím jeho zařízení, poskytovatel do tohoto automatického procesu obvykle aktivně nezasahuje a využívá tak své předchozí aktivní činnosti. Lze tak přistoupit na to, že v daném konkrétním případě by naopak musel aktivně zasáhnout, aby zamezil spáchání takového činu, jde o otázku jeho odpovědnosti jako garanta odpovědného za určitý potenciální zdroj nebezpečí. Více k tomu srov. Říha, J. Postavení garanta u nepravých omisivních deliktů. Trestněprávní revue, 2003, č. 8, str. 227 a násl., č. 9, str. 259 a násl.

[9] Takto se označují jednání všedního dne, např. prodej sekery v obchodě s vědomím, že by mohla být využita k vraždě, a současným srozuměním s touto variantou, praktické je to zejména při činnostech advokátů, daňových poradců, bankovních úředníků. Obvykle se uznává, že jde o jednání sociálně adekvátní, popř. že chybí důvod pro objektivní přičítání, nebo že není protiprávnost takového jednání. Srov. za všechny Wessels, J., Beulke, W. Strafrecht: Allgemeiner Teil. 32. Auflage. Heidelberg: C. F. Müller, 2002, str. 190. Ovšem objevily se i hlasy volající po trestní odpovědnosti podle zavinění takového jednajícího – srov. Leipziger Kommentar, Strafgesetzbuch (Großkommentar). (Red. Jähnke, B., Laufhütte, H. W., Odersky, W.). 11. Auflage. Berlin, New York: Walter de Gruyter, 1993–1994, Roxin, C., § 27 marg. č. 19.

[10] Tento zákon z 28. 10. 1998 navazuje na rozsáhlý autorský zákon (Copyright Act) z roku 1976, má reagovat na nové technologie, především pak na internet. Námi sledovaná problematika je upravena v části druhé, která se nazývá Online Copyright Infringement Liability Limitation Act (OCILLA) a která doplňuje

V **článku 12** Směrnice stanoví odpovědnost za tzv. **prostý přenos**, jinými slovy odpovědnost **Access Providera**, neboli poskytovatele připojení. V případě poskytování služby informační společnosti spočívající v přenosu informací poskytnutých příjemcem služby komunikační sítí nebo ve zprostředkování přístupu ke komunikační síti, nemá být poskytovatel služby odpovědný za přenášené informace, pokud: a) není původcem přenosu; b) nevolí příjemce přenášené informace a c) nevolí a nezmění obsah přenášené informace. Při tom přenos informací a zprostředkování přístupu v uvedeném smyslu zahrnuje také automatické krátkodobé přechodné ukládání přenášených informací, pokud toto ukládání slouží výhradně pro uskutečnění přenosu v komunikační síti a pokud jeho délka nepřesahuje obvyklou dobu přenosu. Soudní nebo správní orgány mohou v souladu s právním řádem členských států požadovat od poskytovatele služby, aby ukončil porušování práv nebo mu předešel. Není tedy tímto ustanovením vyloučeno ani podávání soukromoprávních žalob na zdržení se určité činnosti (např. poskytování služby spočívající v přenosu závadných dat). Smyslem ustanovení bylo omezit, či spíše vyloučit odpovědnost subjektů poskytujících uvedené služby (Access Providerů, E-mailových serverů, internetových kaváren, zprostředkovatelů připojení apod.) za cizí informace, ovšem za splnění shora uvedených podmínek. Bylo by sice pro ně v řadě případů technicky možné, pokud by takoví poskytovatelé služeb museli dohlížet nad příjemci jimi poskytovaných služeb (např. šíření dětské pornografie, podněcování rasové nenávisti), avšak nebylo by to ku prospěchu rozvoje služeb a obchodu vzhledem k vysokým nákladům na taková opatření (náročnost na lidské zdroje při zavádění kontrol, na vytváření softwaru apod.) a vzhledem k značné rizikovosti takového podnikání a z toho vyplývající neochotě taková rizika podstupovat. To je také v souladu s níže uvedeným čl. 15 této Směrnice.

V **článku 13** je upraveno tzv. **caching**, neboli ukládání do vyrovnávací paměti. Cílem tohoto ustanovení je zajistit vyloučení odpovědnosti poskytovatele služby informační společnosti, která spočívá v přenosu informací poskytovaných příjemcem služby a při níž dochází k automatickému dočasnému a přechodnému ukládání, jež slouží pouze pro co možná nejúčinnější následný přenos informace na žádost jiných příjemců služby. Opět směrnice stanoví další předpoklady, podobně jako u Access-providera, za kterých takový poskytovatel služby nebude odpovědný. Předně nesmí přenášenou informaci změnit (a), dále vyhoví podmínkám přístupu k informaci (b), musí dodržovat pravidla o aktualizaci informace, která jsou stanovena způsobem obecně uznávaným a používaným v průmyslu (c), nesmí překročit povolené používání technologie obecně uznávané a používané v průmyslu s cílem získat údaje o užívání informace (d), a nakonec musí ihned přijmout opatření vedoucí k odstranění jím uložené informace nebo ke znemožnění přístupu k ní, jakmile zjistí, že informace byla na výchozím místě přenosu ze sítě odstraněna nebo k ní byl znemožněn přístup nebo soud nebo jiný správní orgán nařídil odstranění této informace nebo znemožnění přístupu

---

Copyright Act o čl. 512. Tato úprava omezuje odpovědnost poskytovatelů služeb, providerů, aby mohli fungovat s přijatelným rizikem, při splnění podmínek se dostávají do tzv. save harbour (bezpečného přístavu) a neodpovídají za obsah stránek, pro které poskytli prostor třetí straně, neodpovídají za to, co přesahuje jejich možnosti kontroly.

k ní (e). Poměrně významný bod je poslední, protože zde je uvedena vlastně výslovně povinnost takového poskytovatele služby zasáhnout, tedy vykonat určitou činnost, jsou-li splněny uvedené podmínky. To souvisí také s odstavcem druhým téhož článku, podle něhož není úpravou v prvním odstavci dotčena možnost soudního nebo správního orgánu požadovat od poskytovatele služby v souladu s právním řádem členských států, aby ukončil porušování práv nebo mu předešel.

Omezení odpovědnosti zprostředkujících poskytovatelů služeb podle této směrnice se nedotýká možnosti podávání různých druhů (civilních) žalob na zdržení se jednání (bod 45. zdůvodnění). Tyto žaloby na zdržení se jednání mohou vést zejména k rozhodnutím soudů nebo správních orgánů vyžadujících ukončení protiprávních jednání nebo předcházení protiprávním jednáním včetně odstranění protiprávních informací nebo zamezení přístupu k nim.

V **článku 14** je upraveno omezení odpovědnosti **Host-Providera**. Podle odstavce prvního nemá Host-Provider, neboli poskytovatel služby informační společnosti spočívající v ukládání informací poskytovaných příjemcem služby, být odpovědný za informace ukládané na žádost příjemce, pokud: a) poskytovatel nebyl účinně seznámen s protiprávní činností nebo informací a ani s ohledem na nárok na náhradu škody si není vědom skutečností nebo okolností, z nichž by byla zjevná protiprávní činnost nebo informace, nebo b) poskytovatel, jakmile se o tomto dozvěděl, jednal s cílem odstranit tyto informace nebo k nim znemožnit přístup. Pro Host-Provider platí tedy v zásadě neodpovědnost za cizí obsah, který má na svých počítačích uložen, avšak jakmile zjistí protiprávní činnost nebo se o ní dozví, musí neprodleně přijmout veškerá opatření k odstranění daných informací nebo znemožnění přístupu k nim. V souvislosti s jejich odstraněním nebo znemožněním přístupu k nim musí zároveň dodržovat zásadu svobody projevu a s ní spojené postupy stanovené na vnitrostátní úrovni. Směrnice zároveň ponechává členským státům možnost vymezit zvláštní požadavky, které je třeba neprodleně splnit před odstraněním informací nebo znemožněním přístupu k nim. Odstavec 2 čl. 14 pak vylučuje použitelnost prvého odstavce (tedy omezení/vyloučení odpovědnosti provideru), pokud je příjemce závislý na Host-Provideru nebo podléhá jeho dohledu. Zároveň není dotčena možnost soudního nebo správního orgánu požadovat od Host-provideru v souladu s právním řádem členských států, aby ukončil protiprávní jednání nebo mu předešel, ani možnost členských států zavést postupy, které umožní odstranění nebo znemožní přístup k informaci. Podle článku 15 sice poskytovatel služeb (Host-Provider) není povinen aktivně monitorovat uložené informace, avšak nadále trvá povinnost zakročit, jsou-li zde konkrétní informace o závadnosti obsahu informací uložených u Host-Providerů.

Článek 15 stanoví **neexistenci obecné povinnosti dohledu**. Členským státům je uloženo, aby neukládaly poskytovatelům služeb uvedených v článcích 12, 13 a 14 obecnou povinnost dohlížet na jimi přenášené nebo ukládané informace nebo obecnou povinnost aktivně vyhledávat skutečnosti a okolnosti poukazující na protiprávní činnost. Jde o velice důležité ustanovení. Platí, co bylo řečeno k článku 12, provider by sice mohl vynaložit značné úsilí, aby zjistil neoprávněnost přenášených či ukládaných informací, avšak šlo by o přenášení povinností, které má v zásadě plnit stát, na soukromé subjekty, zaváděla by se svým způsobem povinná cenzura prováděná takovými

soukromými subjekty, což by také mimo jiné vedlo k enormnímu zvýšení nákladů na provoz uvedených služeb, navíc též k rizikovosti podnikání v tomto oboru (za předpokladu, že by provider neodhalil protiprávnost přenášené či ukládané informace, tedy že by jeho protiopatření byla neúčinná či neúspěšná). V konečném důsledku by to vedlo k podstatnému omezení rozvoje těchto služeb. V případě zjištění konkrétních informací o závadnosti informací zůstává odpovědnost za zamezení jejich šíření či dokonce odstranění, jak bylo uvedeno shora u jednotlivých providerů. Členské státy mohou poskytovatelům služeb informační společnosti (providerům) uložit povinnost, aby neprodleně informovali příslušné orgány veřejné moci o pravděpodobných protiprávních činnostech vykonávaných příjemci služeb nebo o protiprávních informacích, které tito příjemci, rozšiřují, nebo aby sdělili příslušným orgánům veřejné moci na jejich žádost informace, na jejichž základě lze zjistit totožnost příjemců jejich služeb, s nimiž uzavřeli dohodu o shromažďování informací.

Směrnice také stanoví, že **dohled** ze strany státu nad službami informační společnosti probíhá na místě původu činnosti, přičemž příslušný orgán tuto ochranu musí zajišťovat nejen pro občany své země, ale i pro všechny občany Společenství. Rozhodující roli při tom hraje tzv. místo usazení poskytovatele, kterým je místo účinného výkonu hospodářské činnosti prostřednictvím stálé provozovny po neurčitou dobu, v případě provozování internetových stránek tak nehraje roli místo, kde se nachází technické zařízení, jehož prostřednictvím společnost provozuje internetové stránky, ani místo, kde jsou internetové stránky přístupné (což je prakticky celý svět), ale místo, kde společnost vykonává svou hospodářskou činnost. Na druhou stranu směrnice nechce zasahovat nijakým způsobem do zavedených pravidel mezinárodního práva soukromého s jeho kolizními normami a stanovenou pravomocí soudů. Zároveň členské státy mohou v souladu s podmínkami vymezenými v této směrnici uplatňovat své vnitrostátní předpisy trestního práva a trestního řízení.

3. VYBRANÉ ZAHRANIČNÍ ÚPRAVY

Dříve, než se budeme zabývat úpravou odpovědnosti providerů v České republice, je vhodné nahlédnout do sousedních zemí, především pak do **Spolkové republiky Německo**, která má již tradičně jednu z nejpropracovanějších úprav. V SRN se této problematice koncepčně a dlouhodobě věnuje zákonodárce, ale též judikatura, na kterou pak zákonodárce reaguje v případě jejího posunu nevhodným směrem. Německá úprava byla též vzorem pro koncepci shora uvedené Směrnice 2000/31/ES. Jedněmi z nejdůležitějších předpisů v této oblasti byl Teledienstgesetz (TDG), přesněji Gesetz über die Nutzung von Telediensten[11], a Teledienstdatenschutzgesetz (TDDSG), přesněji Gesetz über den Schutz personenbezogener Daten bei Telediensten[12], jako součásti „multimediálního zákona" účinného dokonce již od 1. 8. 1997![13] Dalším dů-

[11] Doslova zákon o užívání „tele-služeb".
[12] Doslova zákon o ochraně osobních dat v „tele-službách".
[13] Tzv. IuKDG = Informations- und Kommunikationsdienstegesetz. Srov. k tomu Marberth-Kubicky, A. Computer- und Internetstrafrecht. München: C.H.Beck, 2005, str. 13.

ležitým dokumentem byl Mediendienstestaatsvertrag z roku 1997 (MDStV – státní smlouva o mediálních službách), který představoval protějšek na úrovni jednotlivých spolkových zemí k TDG a TDDSG platných na úrovni celého spolku. Ustanovení jsou často doslovně shodná.

Podle těchto předpisů se **„tele-službami"** rozumí informační a komunikační služby, které jsou určeny k individuálnímu využití a které spočívají na telekomunikačním přenosu. Z našeho pohledu byla zajímavá ustanovení o odpovědnosti providerů především v TDG v oddílu třetím (§§ 8–11), resp. v MDStV v oddílu druhém (§§ 6–9), která byla doslovně shodná (snad až na několik nepodstatných formulačních odlišností). Uvedená ustanovení vycházela z podobných principů, která později převzala Směrnice 2000/31/ES.

Uvedená úprava byla nahrazena novým zákonem – Telemediengesetz[14] (TMG) z 26. 2. 2007 (BGBl. I S. 179), který rušil dosavadní předpisy TDG, TDDSG i MDStV. Zákon byl přijat k provedení Směrnice 2000/31/ES. Pojem „telemedia" je nadřazeným pro všechny „tele-služby" a mediální služby, které dosud podléhaly samostatným úpravám (v TDG a MDStV) a jejichž úpravu tak nový zákon sjednocuje. K „tele-médiím" patří veškeré elektronické informační a komunikační služby, jde tedy o velmi široký pojem, který má zahrnout mimo jiné i budoucí dosud neznámé technické aplikace, s nimiž se dosud nepočítalo.

Nová úprava v námi sledované oblasti odpovědnosti providerů téměř doslovně přebírá úpravu z dosavadní TDG, resp. MDStV. Odpovědnost je upravena nově v oddílu třetím v §§ 7–10 TMG. Vzhledem k převzetí dřívější úpravy, kterou se inspirovala i již shora uváděná Směrnice, lze úpravu pouze ve stručnosti nastínit. Němci rozlišují odpovědnost Content-, Access- a Host-Providera.

Nejprve v § 7 TMG jsou uvedena základní ustanovení. V prvním odstavci je upravena odpovědnost Content-Providera, která se řídí obecnými zákony.[15] Jde tak o „centrální" odpovědnostní normu. Provozovatel webových stránek podle ní odpovídá jako Content-Provider za všechny informace, které umístil na svých internetových stránkách. Kdo nabízí vlastní informace na svých webových stránkách, musí být za ně též odpovědný. Nehraje při tom vůbec žádnou roli, zda je tzv. soukromou osobou (v zásadě spotřebitelem), či podnikatelem.[16] Takový provozovatel internetových stránek tedy na rozdíl od Access- či Host-Providera není nijak privilegován (odpovídá shodně jako v „offline-světě"). Druhý odstavec § 7 TMG stanoví zásadu, že poskytovatelé služeb uvedení v §§ 8–10 (Access- a Host-Provider) nejsou povinni jimi přenášená a ukládaná data kontrolovat a aktivně vyhledávat informace a poznatky o jejich protiprávním obsahu. Jde o úpravu problému uvedeného v čl. 15 Směrnice 2000/31/ES.

V § 8 TMG je upraveno postavení Access-Provideru, jenž není odpovědný za cizí informace, které v komunikační síti přenáší či zpřístupňuje, pokud zároveň jejich zpro-

[14] Doslova zákon o „tele-mediích".

[15] „Poskytovatelé služeb jsou za vlastní informace, které umožňují využít, odpovědní podle obecných zákonů."

[16] Srov. např. Siebert, S. Die rechtsichere Webseite. B.4U Verlag. (elektronická publikace dostupná 1. 6. 2008 na http://www.eRecht24.de/).

středkování nepodněcuje, nevybírá adresáta zprostředkovávané informace, či zprostředkovávanou informaci nevybírá či nemění. Jde o ustanovení odpovídající čl. 12 Směrnice 2000/31/ES. Pokud by byly naplněny uvedené výjimky (zpracování informace, její výběr, určení adresáta apod.), nedopadalo by na Access-Providera ustanovení § 8 TMG vylučující jeho odpovědnost. Přenos informací zahrnuje také automatické krátkodobé dočasné ukládání přenášených informací (§ 8 odst. 2 TMG).

V SRN je zřejmě nejznámějším případem Acces-Providera řešeným ještě za staré právní úpravy podle TDG (v původním znění s úpravou v § 5 odst. 3) tzv. případ Compuserve, resp. jednatele německé dceřiné společnosti Felixe Somma, který byl stíhán pro trestný čin šíření pornografických materiálů podle § 184 StGB, které mělo spočívat ve zpřístupnění těchto materiálů na místě přístupném osobám mladším 18 let prostřednictvím diskusních fór provozovaných mateřskou společností Compuserve USA. Jednatel Felix Somm byl nejprve rozsudkem AG München uznán vinným a odsouzen k dvouletému trestu odnětí svobody, neboť o uvedených pornografických dílech se dozvěděl a byl povinen zabránit jejich zpřístupnění účinným zásahem, který byl technicky přijatelný. Podle rozhodnutí soudu prvního stupně nepřicházelo v úvahu omezení odpovědnosti Access-Providera podle tehdejšího § 5 odst. 3 TDG (pozdějšího § 9 téhož zákona, nyní § 8 TMG), protože Compuserve Deutschland nebyl pouhým zprostředkovatelem přístupu, ale je mu třeba přičítat postavení i jeho mateřské společnosti Compuserve USA, tedy též Host-Providera. Toto rozhodnutí vzbudilo vlnu nevole a bylo podrobeno tvrdé kritice z různých pozic. Odvolací soud LG München I pak jednatele Somma zprostil viny, když jednak dospěl k závěru, že jednateli nebyl prokázán úmysl, jednak společnosti Compuserve Deutschland jednoznačně přiznal postavení Acces-Provideru, na nějž se vztahovalo omezení odpovědnosti ve smyslu tehdejšího § 5 odst. 3 TDG s odůvodněním, že pro Compuserve Deutschland to byly cizí obsahy, k nimž tato společnost pouze zprostředkovala přístup. Jakkoliv výrok rozsudku byl vnímán pozitivně, jeho odůvodnění bylo opět podrobeno kritice, což přispělo k precizování ustanovení o neodpovědnosti Access-Providera do nového znění v § 9 TDG.

Shodně jako ve Směrnici 2000/31/ES je upravena odpovědnost za tzv. caching v § 9 TMG, k dočasnému ukládání informací se přistupuje obdobně jako k odpovědnosti Access-Providera.

Odpovědnost Host-Providera je upravena v § 10 TMG, který svým zněním odpovídá čl. 14 Směrnice 2000/31/ES. I v SRN je Host-Provider v zásadě neodpovědný za cizí informace, které pro uživatele ukládá na svých počítačích, pokud zjednodušeně řečeno neví o protiprávnosti jednání nebo informace. Zároveň je zde upravena povinnost pro případ, že zjistí protiprávní činnost nebo protiprávnost informace, bezodkladně odstranit závadnou informaci nebo zabránit k ní přístup. Jakmile tedy bude mít Host-Provider znalost o protiprávním obsahu uloženém na jeho počítačích, má povinnost konat, tedy zasáhnout – informaci odstranit, nebo znemožnit k ní přístup, jinak by mohl odpovídat za tzv. cizí obsah. Např. provozovatel diskuzního fóra je povinen odstranit závadný protiprávní obsah, jakmile se o něm dozví, jinak za něj odpovídá. Při tom postačí, aby o protiprávnosti byl informován zaměstnanec či spolupracovník podnikatele – Host-Providera. Nemusí být tedy informován přímo jednatel, aby podnikatel byl za cizí obsah odpověd-

ný[17] (ovšem v trestněprávní rovině musí být u fyzické osoby, jednatele, dáno též zavinění, obvykle dokonce úmyslné). Lze pak ale dovodit i trestněprávní odpovědnost konkrétních fyzických osob (v SRN nemají trestněprávní odpovědnost právnických osob). Uvedený princip zasáhnout v případě upozornění na protiprávnost uložené informace ovšem může znamenat v praxi značné komplikace pro poskytovatele takových služeb. Znamená to přinejmenším takovou informaci vyhodnotit a podle toho se zachovat, což ovšem nemusí být v konkrétním případě snadné, a to jednak vyhodnocení po faktické, obsahové stránce (např. zda je věc nabízená v aukci kradená, jde o padělek apod.), jednak po právní stránce (zda se jedná o věc extra commercium – např. chráněné zvíře či rostlinu; zda nabízené věci či informace spadají pod určitý právní pojem či nikoli – např. pornografie apod.). Jednoduché řešení daného problému, zdá se, není, o čemž vypovídá též bohatá judikatura německých soudů.

V **Rakousku** nalezneme v současné době úpravu odpovědnosti poskytovatelů telekomunikačních služeb v tzv. E-commerce Gesetz (ECG), zákoně č. 152/2001 BGBl. I, který nabyl účinnosti 1. 1. 2002. Sledovaná problematika je upravena v 5. oddílu v §§ 13–19 a již na první pohled je obsáhlejší než Směrnice 2000/31/ES, či německý TMG.

Ustanovení § 13 ECG vylučuje odpovědnost Access-Providera za stejných podmínek jako zmíněná Směrnice či německý TMG (proto lze odkázat na výklad shora). Nové je ovšem ustanovení § 14, které upravuje vyloučení odpovědnosti tzv. vyhledávačů (např. google.com, seznam.cz apod.) Podle uvedeného ustanovení poskytovatel služeb (ve smyslu tohoto zákona), který poskytuje uživatelům služby spočívající ve vyhledání cizích informací pomocí vyhledavače nebo jiného elektronického prostředku, není odpovědný, pokud zprostředkování zadané informace nepodnítil, adresáta zadané informace nezvolil, zadanou informaci ani nezvolil a ani nezměnil. To neplatí, pokud osoba, od níž zadaná informace pochází, podléhá poskytovateli služeb nebo je jím dozorována. V tomto ustanovení je tak výslovná úprava toho, co se v SRN (a zřejmě i v dalších zemích bez výslovné úpravy) dovozuje výkladem, totiž že poskytovatel služby spočívající v provozování vyhledavače je odpovědný jako pouhý Access-Provider (a nikoli jako Host-Provider). Ovšem v SRN se někdy dovozuje i v těchto případech odpovědnost provozovatele, má-li znalost o protiprávnosti zprostředkovávaného obsahu, která musí být bez dalšího zřejmá (pak ovšem jde o obdobu odpovědnosti jako u Host-Providera).[18]

Podle § 15 ECG je vyloučena odpovědnost poskytovatele služeb spočívajících v tzv. meziukládání informací (caching), shodně jako je tomu ve Směrnici či TMG. Ustanovení § 16 ECG upravující (ne)odpovědnost Host-Providera je obsahově opět zcela shodné s § 10 TMG (resp. čl. 14 Směrnice).

Kromě toho mají Rakušané výslovně řešené vyloučení odpovědnosti za linky v § 17 ECG. Podle tohoto ustanovení poskytovatel služeb, který prostřednictvím elektronic-

[17] Siebert, S. Die rechtsichere Webseite. B.4U Verlag. (elektronická publikace dostupná 1. 6. 2008 na http://www.eRecht24.de/), str. 89, který německým podnikatelům poskytujícím „tele-mediální" služby proto radí, aby měli nastavené účinné organizační opatření, aby mohli včas a účinně reagovat na poznatky o možných porušeních práva.

[18] Srov. Marberth-Kubicky, A. Computer- und Internetstrafrecht. München: C. H. Beck, 2005, str. 115 (zřejmost dovozuje autorka např. z pravomocného odsuzujícího rozsudku).

kého odkazu zřídí přístup k cizí informaci, není za tuto informaci odpovědný, 1. pokud o protiprávní činnosti nebo informaci nemá žádnou skutečnou vědomost a s ohledem na nárok na náhradu škody si není vědom žádné skutečnosti či okolnosti, z níž by byla protiprávnost činnosti nebo informace zřejmá, 2. pokud neprodleně, jakmile toto zjistí nebo se o tom dozví, učiní opatření, aby elektronický odkaz odstranil. Opět jde o přeformulování ustanovení, jež dopadá tentokrát na Host-Providera, na odpovědnost za odkazy v rámci webových stránek. Odpovědnost u takovýchto provozovatelů se musí v SRN řešit výkladem, což vede ke kontroverzím a nejednotnému názoru na konečné řešení. Z německé judikatury lze dokonce dovodit v některých případech pro toho, kdo umístí na své stránky odkaz na cizí obsah, odpovědnost shodnou jako u Content-Providera, pokud se takový poskytovatel služby dostatečným způsobem nedistancuje od cizího obsahu, na nějž odkazuje[19], resp. pokud dokonce navozuje dojem, že jde o jeho vlastní obsah, vlastní sdělení. Tato otázka není Směrnicí 2000/31/ES výslovně řešena a úprava je zatím ponechána na jednotlivých státech (ovšem původně bylo plánováno, že i tomuto tématu bude věnována samostatná Směrnice).

V § 18 ECG je vyloučena povinnost poskytovatelů služeb uvedených v §§ 13–17 dohlížet na informace jimi zprostředkované, ukládané nebo zpřístupňované, jakož i povinnost aktivně protiprávní obsah vyhledávat. Poté se poskytovatelům ukládá spolupracovat s různými orgány (soudy, policií, správními úřady). Podle § 19 ECG zůstávají nedotčeny předpisy, podle nichž soud či úřad může nařídit zdržet se, odstranit či zabránit porušování práva. Podle druhého odstavce § 19 se předcházející ustanovení užijí i na poskytovatele služeb, kteří tak činí bezplatně.

4. ÚPRAVA V ČESKÉ REPUBLICE

Česká republika neměla dlouhou dobu žádnou speciální úpravu, která by se týkala odpovědnosti providerů. Vzhledem k přípravě na vstup České republiky do Evropské unie bylo mimo jiné třeba transponovat shora uvedenou Směrnici Evropského parlamentu a Rady 2000/31/ES. Na základě usnesení vlády č. 474 z 19. 5. 2003, kterým vláda vzala na vědomí Bílou knihu o elektronickém obchodu, byl vypracován návrh zákona o některých službách informační společnosti a o změně některých zákonů, kterým měla být upravena též materie obsažená v uvedené směrnici, jež dosud nebyla do českého právního řádu transponována (především se jednalo o námi sledované články 12–14). Návrh byl předložen Poslanecké sněmovně Parlamentu České republiky ve volebním období 2000–2004 jako tisk č. 579/0, zákon se nepodařilo projednat a schválit předtím, než Česká republika vstoupila do Evropské unie (1. 5. 2004), schválen byl až později a jako zákon č. 480/2004 Sb., o některých službách informační společnosti, nabyl platnosti a účinnosti od 7. 9. 2004 (zákon tak neposkytl adresátům žádnou legisvakanční lhůtu, i přes to, že za porušení tohoto zákona hrozí až několikamilionové pokuty).

[19] Např. LG Hamburg, sp. zn. 312 O 85/98 (z 12. 5. 1998). Často se navíc připomíná, že pouhé strohé distancování se, např. že „nejsme odpovědní za obsah cizích stránek", nestačí k vyloučení odpovědnosti za cizí obsah z pozice Content-Providera, zvláště to platí v těch případech, kdy jsou linky zařazené do textu na podporu vlastních názorů (např. při propagaci nacismu).

Již důvodová zpráva tohoto zákona přiznávala, že do přijetí tohoto zákona nebyla u nás odpovědnost providera výslovně řešena, byla upravena pouze v dohodě mezi poskytovatelem služeb (providerem) a uživatelem. Taková dohoda byla ale nedostatečná, nemohla vylučovat odpovědnost za protiprávní jednání, kterou je třeba řešit zákonem. Proto je třeba výslovné úpravy podmínek odpovědnosti providera za obsah jím přenášených či ukládaných informací. Zákon si kladl také za cíl upravit šíření obchodních sdělení elektronickými prostředky, a proto je někdy nesprávně nazýván „antispammovým zákonem". Otázka šíření „spamu" (nevyžádané pošty) také vyvolala největší reakce, a to jak ze strany adresátů zákona (především s ohledem na přísná sankční ustanovení v § 11 a 12), tak ze strany úřadů (např. tehdejšího Ministerstva informatiky[20]), zatímco podle mého názoru primární úprava odpovědnosti providerů se výraznějšího zájmu odborné ani laické veřejnosti nedočkala.

Vrátíme-li se zpět před účinnost tohoto zákona, dovozovala se odpovědnost providerů za škodu z ustanovení občanského zákoníku, především pak z ustanovení § 415 zák. č. 40/1964 Sb., občanského zákoníku, v účinném znění (dále jen OZ), které upravuje povinnost předcházet škodám, jde tak o generálně-preventivní ustanovení, jež navazuje na všeobecně uznávanou právní zásadu zákaz škodit jinému („neminem laedere"). Povinností každého je počínat si tak, aby nedocházelo ke škodám na zdraví, majetku, právech jiného, přírodě či životním prostředí. U providera mohlo být shledáno, byť i nedbalostní, porušení této povinnosti, pokud včas nezasáhl, neboli nechoval se tak, aby jinému nevznikla škoda (např. při šíření pomluvy v diskuzním fóru, popř. děl podléhajících ochraně autorských práv apod.). Za primárního škůdce odpovídajícího podle § 420 OZ byl považován ten, kdo se uvedeného protiprávního jednání skutečně dopustil, např. umístil na server Host-Providera protiprávní obsah (hudbu, filmy, software). Odpovědnost Host-Providera (podobně by tomu mohlo být u Access-Providera) byla pak dovozována ze zmíněného ustanovení § 415 OZ ve spojení s ustanovením § 420 OZ, jako odpovědnost sekundární, když porušení právní povinnosti ze strany provideru jako předpoklad odpovědnosti podle § 420 OZ bylo shledáváno právě v porušení povinností uložených providera ustanovením § 415 OZ. Zavinění se sice presumuje, bylo však dovozováno, že provider by se své odpovědnosti zprostil (§ 420 odst. 3 OZ), pokud by prokázal, že o protiprávnosti obsahu, který byl na jeho počítačích umístěn (popř. který on zpřístupnil), nevěděl, vylučována tak byla odpovědnost za nevědomou nedbalost s odůvodněním, že po provideru nelze spravedlivě požadovat, aby monitoroval a zkoumal cizí obsah (srov. dnešní v důsledcích shodnou výslovnou úpravu). Zvažovala se též odpovědnost objektivní s možností liberace podle ustanovení § 420a OZ, podle něhož by provider mohl odpovídat za škodu způsobenou jinému provozní činností (činností mající provozní povahu), avšak užití tohoto ustanovení bylo nakonec z různých důvodů odmítnuto. Pokud jde o rozsah povinnosti k náhradě škody, vycházelo se z ustanovení § 438 odst. 1 (a příp. 2) OZ, podle něhož měl za případně vzniklou škodu odpovídat v zásadě společně a nerozdílně s primárním škůdcem, není-li

[20] Viz např. odpovědi na nejčastěji kladené otázky dostupné ke dni 1. 6. 2008 v archivu Ministerstva vnitra na internetových stránkách: http://www.mvcr.cz/micr/scripts/detail.php_id_1769.html.

zvláštních důvodů, pro které by odpovídal podle své účasti na způsobení škody.[21] Není mi ovšem znám případ, který by uvedeným způsobem soudy řešily.

Je otázka, zda z uvedené povinnosti předcházet škodám by i za dřívější úpravy bylo možno dovozovat trestněprávní povinnost konat, jak vyplývá z ustanovení § 89 odst. 2 zák. č. 140/1961 Sb., trestního zákona, v účinném znění (dále jen TZ). Provider jako poskytovatel určitých služeb informační společnosti je svým způsobem dohlížitel nad určitým zdrojem nebezpečí, za který můžeme považovat internet, jenž je v zásadě společnosti prospěšný, ale může vyvolávat nebezpečí pro právem chráněné právní statky (např. ohrožovat či porušovat zájem společnosti na ochraně před šířením pornografie vůči dětem mladším 18 let). Vzhledem k tomu bychom na takového poskytovatele mohli nahlížet jako na garanta dozorce ve smyslu německé právní nauky, kterému vzniká zvláštní povinnost konat na základě předchozího nebezpečného jednání (tzv. ingerence).[22] Povinnost konat plynoucí z ingerence zná i naše nauka, která vychází z tzv. klasické triády, podle níž zvláštní povinnost konat může vyplývat ze zákona, ze smlouvy či z ingerence. U nás odpovědnost z ingerence není příliš propracovaná, lze tak odkázat na nauku německou, podle níž předchozí nebezpečné jednání musí splňovat určitou kvalitu, aby bylo způsobilé založit zvláštní povinnost konat. Předně takové předchozí nebezpečné jednání musí způsobit blízké (adekvátní) nebezpečí vzniku poruchy, dále musí takový pozdější garant jednat v rozporu se svou právní povinností a za další zde musí být příčinná souvislost mezi porušenou povinností a vzniklým nebezpečím a též mezi účelem porušené normy a vzniklým nebezpečím. Domnívám se, že zde obvykle chybí blízké, adekvátní nebezpečí vyvolané providerem, který své služby obvykle založil na poskytování služeb v souladu s právním řádem (snad bychom mohli hovořit o abstraktně nebezpečném jednání, českou terminologií o vzdáleném nebezpečí). Zpravidla tedy nedochází ze strany providera k porušení právní povinnosti, protože provádí jednání, které je v zásadě v souladu s právním řádem, sociálně adekvátní, společností přijímané jako prospěšné, žádná zvláštní povinnost spočívající v dohlížení nad chováním třetích osob mu uložena nebyla a ani dodatečně mu nevznikala (až do přijetí zákona č. 480/2004 Sb.). Snad by bylo možno dovozovat vznik garanční povinnosti z panství nad věcmi (postaru), resp. z povinnosti zajistit bezpečný provoz, zabránit nebezpečím plynoucím z věcí, objektů či zařízení spadajících do okruhu působnosti takového subjektu, popř. z povinnosti dobrovolně převzaté. V případě těchto garančních povinností se nežádají tak přísná omezení, jako u ingerence, může jít též o vznik povinnosti na základě původního sociálně adekvátního, právně dovoleného jednání. Tak je vnímáno postavení internetových providerů (vlastně jen Access- a Host-Providera) i v SRN, kde jsou zařazováni právě do této skupiny garantů[23], neboť

[21] K celému srov. např. Matejka, J., Čermák, J. Odpovědnost poskytovatelů volného prostoru na internetu za cizí obsah. Právník, 2001, č. 11, str. 1108 a násl. Popř. zkrácená verze článku dostupná na stránkách internetu ke dni 1. 6. 2008 na portále LUPA: http://www.lupa.cz/clanky/odpovednost-poskytovatelu-web-hostingu-za-cizi-obsah/.

[22] Více k tomu srov. Říha, J. Postavení garanta u nepravých omisivních deliktů. Trestněprávní revue, 2003, č. 8, str. 227 (1. část), č. 9, str. 259 an. (2. část).

[23] Srov. např. Wessels, J., Beulke, W. Strafrecht: Allgemeiner Teil. Die Straftat und ihr Aufbau. 36. Auflage. Heidelberg: C. F. Müller, 2006, str. 275; Kühl, K. Strafrecht: Allgemeiner Teil. 4. Auflage. München: Vahlen, 2002, str. 731; Rudolphi se jednoznačně staví proti takové variantě – Systematischer Kommentar zum Strafgesetzbuch. Band I. Allgemeiner Teil (§§ 1 bis 79b). 7. a 8. vydání. Bonn: Luchterhand, 2003 – výklad k § 13, marg. č. 30a.

mají povinnost zasáhnout právě při zjištění protiprávnosti informací uložených na jejich počítačích, nemají ale povinnost aktivně tuto protiprávnost vyhledávat. Ovšem bez zákonného zmocnění by takové zařazení bylo obtížně myslitelné.

Nápravu neutěšeného stavu, kdy nebyla právní odpovědnost providerů jednoznačně upravena, přinesl **zákon č. 480/2004 Sb., o některých službách informační společnosti**. Od 7. 9. 2004 je upraveno jednak omezení odpovědnosti providerů, avšak také jsou stanoveny jejich povinnosti konat, z nichž bude nadále možné dovozovat i případnou trestněprávní odpovědnost za omisivní trestné činy. Zákon byl dosud třikrát novelizován, nejvýznamnější novelizace se týkala úpravy šíření obchodních sdělení v ustanovení § 7, které bylo od počátku centrem pozornosti. Úprava odpovědnosti providerů, která je obsažena v ustanoveních §§ 3 až 6, nedoznala dosud změny. Těmito ustanoveními jsou do našeho právního řádu převzaty články 12–15 Směrnice 2000/31/ES.

Zákon nejprve vymezuje předmět úpravy, poté definuje nejdůležitější pojmy, jako služba informační společnosti, poskytovatel služby a uživatel, a to v návaznosti na uvedenou Směrnici 2000/31/ES, resp. Směrnici 98/34/ES ve znění Směrnice 98/48/ES. **Službou informační společnosti** je tak jakákoliv služba poskytovaná elektronickými prostředky (jde zejména o síť elektronických komunikací, o elektronická komunikační zařízení, koncová telekomunikační zařízení a o elektronickou poštu) na individuální žádost uživatele podanou elektronickými prostředky, poskytovaná zpravidla za úplatu, přičemž služba je poskytnuta elektronickými prostředky, pokud je odeslána prostřednictvím sítě elektronických komunikací a vyzvednuta uživatelem z elektronického zařízení pro ukládání dat. Poskytovatele služby zákon definuje tautologicky jako osobu poskytující některou z uvedených informačních služeb. Uživatele definuje podobně tautologicky jako osobu, která uvedenou službu využívá (demonstrativně k tomu dodává konkretizaci v podobě vyhledávání či zpřístupňování informací).

Ustanovení **§ 3** uvedeného zákona přebírá z čl. 12 Směrnice 2000/31/ES omezení odpovědnosti **Access-Provideru**, neboli poskytovatele služby, jež spočívá v přenosu informací poskytnutých uživatelem prostřednictvím sítí elektronických komunikací nebo ve zprostředkování přístupu k sítím elektronických komunikací za účelem přenosu informací (např. poskytovatel připojení k síti internetu, ať prostřednictvím dial-up, či pevným připojením). Access-Provider zásadně neodpovídá za obsah přenášených informací, což ovšem zákon výslovně neuvádí, zákon uvádí, že Access-Provider odpovídá podle § 3 odstavce 1 pouze pokud: a) přenos sám iniciuje, b) zvolí uživatele přenášené informace, nebo c) zvolí nebo změní obsah přenášené informace. Pokud tedy provider do přenášené informace nijakým způsobem aktivně nezasahuje a chová se vlastně pasivně, přijme informaci a nepozměněnou ji prostřednictvím dříve nastavených automatických procesů pošle uživatelem určenému příjemci (jinému uživateli), neodpovídá za její obsah. Přenos informací a zprostředkování přístupu podle odstavce 1 zahrnuje také automatické krátkodobě dočasné ukládání přenášených informací. Access-Provider nemá povinnost aktivně zjišťovat obsah přenášené informace (např. zda nejde o dětskou pornografii, propagaci nacismu, autorským právem chráněné dílo), jak vyplývá z ustanovení § 6, ani za protiprávnost obsahu nijak neodpovídá. Dokonce to platí i v případě, že se dozví o protiprávnosti takového obsahu (srov. § 5 odst. 1 a contrario).

Zákon bohužel výslovně neuvádí možnost žalovat na zdržení se jednání spočívajícího v přenášení protiprávního obsahu, jak to uvádí Směrnice 2000/31/ES v čl. 12 odst. 3 ve spojení s bodem 45 zdůvodnění. Vzniká tak problém, zda je taková žaloba možná, zda může být úspěšná a zda je případně Access-Provider následně odpovědný za obsah přenášených informací, pokud se nepodrobí vykonatelnému rozhodnutí. Pokud jde o první otázku, je nepochybné, že právo na přístup k soudu je u nás zabezpečeno již na ústavněprávní úrovni (především čl. 90 Ústavy, čl. 36 odst. 1 Listiny základní práv a svobod), podat civilní žalobu tak nepochybně možné bude. Bude ale taková žaloba úspěšná? Zákon sice nikde neuvádí, že by Access-Providera mohla taková povinnost být uložena, na druhou stranu činností Access-Providera je zasahováno do práv osoby, jež se brání, a jejich oprávnění žalovat na zdržení se takového jednání plyne z jiných právních norem [např. v případech porušení práv nekalou soutěží srov. § 53 zák. č. 513/1991 Sb., obchodního zákoníku; v případech porušení autorských práv srov. zák. č. 121/2000 Sb., autorský zákon – § 40 písm. b), c), d) a zejména f)]. V případech, kdy taková výslovná úprava chybí, bylo by možno se též dovolávat již zmíněného ustanovení § 415 OZ (povinnost předcházet škodám). Nebylo by zřejmě možné dovolávat se přímo Směrnice 2000/31/ES, neboť by se takto jednotlivec domáhal uložení povinnosti vůči jinému jednotlivci na základě ustanovení směrnice, domáhal by se tedy přímého horizontálního účinku směrnice, který se zásadně dosud nepřipouští (na rozdíl od vertikálního účinku).[24] Určitým řešením by mohla být žaloba poškozeného subjektu na náhradu škody vůči státu pro nečinnost státu spočívající v nevydání právního předpisu ke splnění závazku vyplývajícího z práva ES podle čl. 235 SES.

Uvedená problematika je předmětem sporu i v sousedním SRN, kde mají obdobnou úpravu odpovídající Směrnici 2000/31/ES. Vcelku se zde nepochybuje o tom, že Access-Provider je z hlediska trestního práva a z hlediska civilního nároku na náhradu škody neodpovědný za cizí obsah, který on pouze přenáší. Stále je zde ale snaha prolomit tuto zásadu v tom směru, že je v civilním řízení žalováno na zdržení se zpřístupňování, resp. přenášení informací se závadným obsahem (např. dětskou pornografií). Dosud soudy takové pokusy jednomyslně odmítají.[25]

Ustanovení **§ 4** zákona č. 480/2004 Sb. přejímá článek 13 Směrnice 2000/31/ES o omezení odpovědnosti providera za dočasně meziukládané informace (tzv. **caching**). Proxy-Cache-Servery mají zajistit omezení datového provozu a zrychlit datový přenos

[24] Tak např. rozsudek Pfeiffer a další – C-397/01 až 403/01. Judikatura Evropského soudního dvora (ESD) se v tomto směru ale vyvíjí a zcela výjimečně připouští tzv. incidenční horizontální účinek směrnice v případě, kdy se jednotlivec domáhá ochrany svých práv vůči druhému jednotlivci, kterému ovšem směrnice žádnou povinnost neukládá (např. věc CIA Security – C-194/94). Jde ovšem o otázku složitou, která není jednoznačně řešena a bylo by proto zajímavé sledovat případné řízení o předběžné otázce u ESD tohoto se týkající.

[25] Srov. např. rozhodnutí LG Kiel z 23. 11. 2007, sp. zn. 14 O 125/07 (žaloba na blokování webových stránek Access-Providerem byla zamítnuta, neboť Access-Provider nemůže být pachatelem ani účastníkem protiprávního jednání, je zde nedostatek jeho protiprávního jednání), (nepravomocné rozhodnutí) LG Düsseldorf z 13. 12. 2007, sp. zn. 12 O 550/07 (kterým soud vyjádřil podobný závěr jako shora uvedený, tedy jednak že Acces-Provider neporušuje žádnou povinnost, navíc právně ani skutkově mu není možné uložit, aby zabránil protiprávním jednáním na cizích webových stránkách). Podobně též OLG Frankfurt, usn. z 22. 1. 2008, sp. zn. 6 W 10/08.

krátkodobým meziukládáním přenášených dat, což probíhá obvykle automaticky a bez znalosti přenášených a ukládaných dat. V tomto směru lze odkázat na to, co bylo uvedeno výše k čl. 13 Směrnice. Pro providera v případě přechodně ukládaných informací vyplývají z podmínek, za nichž je vyloučena jeho odpovědnost, též důležité povinnosti konat. Takový provider musí především přijmout opatření vedoucí k odstranění jím uložené informace nebo ke znemožnění přístupu k ní, jakmile zjistí, že informace byla na výchozím místě přenosu ze sítě odstraněna nebo k ní byl znemožněn přístup nebo soud nařídil stažení informace či znemožnění přístupu k této informaci. Pokud by provider nesplnil tuto povinnost, mohli bychom dovozovat jeho odpovědnost za protiprávní obsah uložené informace. Z ustanovení § 4 písm. e) zák. č. 480/2004 Sb. tak jednoznačně vyplývá povinnost providera zasáhnout, jsou-li splněny podmínky v tomto písmenu uvedené. Zde již máme dokonce výslovně uvedenou povinnost providera reagovat nejen na vlastní zjištění či oznámení o odstranění informace nebo zamezení přístupu k ní, ale především povinnost reagovat na soudní rozhodnutí. Uvedené ustanovení tedy jednoznačně počítá se žalobami na odstranění závadných informací i na zdržení se zpřístupňovat takové informace (ovšem např. oproti SRN nepočítá s možností, aby o tom rozhodl správní úřad). Provider pak má povinnost konat, nesplní-li ji, vystavuje se nebezpečí postižení pro omisivní delikt (ať již civilněprávní – odpovědnost za způsobenou škodu, či dokonce trestněprávní).

Ustanovení § **5** zákona č. 480/2004 Sb. upravuje odpovědnost **Host-Providera**, tedy poskytovatele služby spočívající v ukládání informací poskytovaných uživatelem. Uvedené ustanovení v podstatě přejímá článek 14 Směrnice 2000/31/ES. Host-Provider zásadně neodpovídá za obsah informací u něj uložených uživatelem, odpovídá pouze tehdy, pokud a) mohl vzhledem k předmětu své činnosti, okolnostem a povaze případu vědět, že obsah ukládaných informací nebo jednání uživatele jsou protiprávní, nebo b) se prokazatelně dozvěděl o protiprávní povaze obsahu ukládaných informací nebo o protiprávním jednání uživatele a neprodleně neučinil veškeré kroky, které lze po něm požadovat, k odstranění nebo znepřístupnění takovýchto informací. Z toho se dá logicky dovodit zvláštní povinnost konat pro takového Host-Providera spočívající v odstranění nebo znepřístupnění informace, pokud se dozví, že obsah uložené informace je protiprávní, nebo k jejímu uložení došlo protiprávním jednáním uživatele. Host-provider pak musí jednat bez zbytečného prodlení a musí k odstranění či znepřístupnění informací učinit veškeré kroky, které lze po něm spravedlivě požadovat. Zdá se, že jde o jakési vyjádření péče řádného hospodáře (obdobu římsko-právního diligens pater familias), avšak pouze pro případ, že se dozví o protiprávnosti obsahu či předchozího jednání uživatele. Pak je zde ještě první varianta, za níž odpovídá Host-provider, a sice případ, kdy vzhledem k předmětu své činnosti, okolnostem a povaze případu měl a mohl vědět, že obsah ukládaných informací nebo jednání uživatele jsou protiprávní.

Ustanovení § **6** zákona č. 480/2004 Sb. pak přejímá úpravu čl. 15 Směrnice 2000/31/ES. Podle tohoto ustanovení nejsou poskytovatelé služeb uvedení v § 3 až 5 zákona č. 480/2004 Sb. povinni jednak dohlížet na obsah jimi přenášených nebo ukládaných informací, jednak aktivně vyhledávat skutečnosti a okolnosti poukazující na protiprávní obsah informace. Z hlediska odpovědnosti za omisivní trestné činy (ale též

civilněprávní odpovědnosti za opominutí) jde o velice významné ustanovení, které doplňuje shora uvedená ustanovení o odpovědnosti poskytovatelů služeb uvedených v § 3 až 5 zákona. Provideři tak nemají povinnost aktivně zkoumat a dohlížet na obsah informací, které ukládají či přenášejí zpravidla v automatických procesech bez účasti lidského faktoru. Je tak umožněno reálné fungování internetu, výměny dat, systém není zatěžován cenzurou ani nákladnými automatickými prostředky, které by vyhledávaly jednotlivé náznaky nepřípustných obsahů. Není tedy možné dovozovat odpovědnosti (ať trestněprávní či civilněprávní) za opomenutí dohledu nad jimi spravovanými technickými zařízeními a za umožnění např. šíření dětské pornografie, obsahů podporujících hnutí k potlačení lidských práv apod. Takovou odpovědnost lze dovodit pouze za splnění podmínek ustanovení § 3 až 5 zákona, tedy např. u Host-Providera v případě, že se prokazatelně dozvěděl o takovém jednání, přičemž způsob, jakým se o tom dozví, nemá spočívat v jeho aktivní činnosti – vyhledávání a dohlížení.

Právě u Host-Providera nastává závažný problém, co se považuje za „prokazatelné dozvědění" se o protiprávní povaze obsahu ukládaných informací nebo o protiprávním jednání uživatele. Postačí v takovém případě jakékoliv upozornění ze strany třetí osoby, nebo má jít o upozornění nějak kvalifikované? Zcela nepochybné to bude, pokud bude Host-Provideru doručeno pravomocné soudní (ať již civilní, správní či trestní) rozhodnutí o protiprávnosti určité informace – např. závadnosti obsahu internetových stránek uložených na jeho počítačích (dětská pornografie, propagace fašismu, neoprávněné šíření autorským právem chráněných děl apod.). Na základě takového rozhodnutí by měl Host-Provider konat a informace odstranit či zamezit k nim přístup. Ovšem postačovat by měla též znalost získaná z jiného zdroje, např. od třetích osob. Podle českého zákona se provozovatel musí o protiprávní povaze „prokazatelně dozvědět", což může činit v praxi problém při prokazování takové znalosti. Bude pak stačit, že informace byla Host-Providera prokazatelně odeslána? Tak se vykládá obdobné ustanovení německé, které užívá ovšem poněkud širší pojem („Kenntnis erlangt haben"). Zvláště u právnických osob by mohla být účinnost úpravy při naprosto pasivním přístupu k takovým informacím ze strany třetích osob výrazně snížena, pokud bychom vykládali české ustanovení příliš restriktivně, tedy v opačném smyslu (i pro jednotlivce by pak ale stačila jednoduchá obrana spočívající např. v tvrzení, že e-maily nebo psané dopisy nečte). Zřejmě správnější se jeví výklad, že postačuje, aby taková informace byla doručena do sféry Host-providera. Rozhodně ale Host-Provider nemusí sám závadné informace vyhledávat, z čehož plyne, že je mu třeba sdělit i přesný odkaz na závadnou informaci, aby ji sám nákladně nemusel vyhledat a její protiprávnost ověřit.[26] Další podmínkou povinnosti Host-providera odstranit závadné informace či znemožnit přístup k nim je na jeho straně objektivní (technická) možnost takového postupu, navíc pouze tehdy, lze-li to po něm (spravedlivě) požadovat.[27] Tyto kroky musí být též proporcionální ke sledovanému cíli, není možné zablokovat řadu internetových stránek jen proto, že malá část obsahuje protiprávní obsah.

[26] Podobně v SRN BGH CR 2004, 48, 50. Srov. též Marberth-Kubicky, A. Computer- und Internetstrafrecht. München: C.H.Beck, 2005, str. 112.

[27] Taková podmínka sice v německém § 10 TMG chybí, nicméně obvykle je požadována naukou i judikaturou.

Host-Provider, či Access-Provider zpravidla nebude odpovědný jako pachatel trestné činnosti, kterým obvykle bude pouze Content-Provider, ale může odpovídat za účastenství na jeho trestné činnosti, především by mohl být odpovědný pro poskytnutí pomoci spočívající v umožnění spáchání činu zajištěním prostoru na internetu či umožněním přístupu k němu – např. k trestné činnosti spočívající v šíření dětské pornografie, propagaci nacismu apod.

Zvláštností české úpravy oproti té ve Směrnici 2000/31/ES je pozitivní vyjádření případů, kdy provider odpovídá za obsah informací. Z toho je třeba dovodit, že v ostatních případech neodpovídá za obsah informací. Směrnice ale vychází z vyjádření negativního, tedy provider v určených případech nemá odpovídat za obsah informací. To, co uvádí Směrnice, bylo také cílem při sjednocování právních úprav jednotlivých států, cílem bylo jednoznačně uvést, že provider zásadně neodpovídá tzv. za cizí obsah. Z českého předpisu (z. č. 480/2004 Sb.) to vyplývá především ze slov „odpovídá... jen pokud", tedy pouze ve vyjmenovaných případech, v ostatních (a contrario) nikoli. Nicméně vhodnější by byla úprava opačná, tedy vymezená negativně. Směrnice totiž předvídá pouze případy, kdy provider nemá nikdy odpovídat (proto jde o omezení odpovědnosti providerů), v ostatních výslovně nevypočtených případech naopak odpovídat má (či spíše může), zatímco my dopředu v opačném gardu stanovíme podmínky, za nichž odpovídá, v ostatních případech pak nikdy odpovídat nebude. To může činit jednak problémy při výkladu uvedených ustanovení (při užití rozšiřujícího výkladu, popř. při užití analogie), jednak v sobě nese taková úprava riziko výskytu nepředvídaných případů.

Podobně jako uvedená Směrnice nestanoví ani český předpis odpovědnost **Content-Providera**, a to na rozdíl např. od úpravy německé. Je to zvláštní tím spíše, že právě český zákonodárce vychází z pozitivní koncepce, tedy stanoví výslovně případy, kdy má provider odpovídat. Směrnici toto nemusíme vyčítat, protože k věci přistupuje negativně, stanoví, kdy provider odpovídat nemá. Pokud tedy o Content-Provideru nehovoří, vychází z toho, že jeho odpovědnost není třeba omezovat (resp. vylučovat). Pokud naopak český zákonodárce vyjmenovává případy, kdy provider má odpovídat, měl to tedy učinit i u Content-Providera, jinak oprávněně vyvstává otázka, jak to s jeho odpovědností je. V tomto směru bych tedy vycházel z historického výkladu a z výkladu teleologického, z nichž je patrná inspirace Směrnice 2000/31/ES původní německou úpravou, navíc směrnice má omezit snahy o příliš širokou odpovědnost providerů tím, že stanoví případy, kdy neodpovídají tzv. za cizí obsah, cílem nebylo komplexně upravit odpovědnost providerů, ani vyloučit odpovědnost hlavního původce závadných informací. Proto i česká pozitivní úprava v konečném důsledku má omezit příliš širokou odpovědnost vyplývající z obecných ustanovení ostatních předpisů u některých providerů, a sice u Host-Providera, u Access-Providera a u Proxy-Cache-Serverů. Na rozdíl od zahraničí (především Německa) není u nás rozvinutá judikatura o odpovědnosti providerů, nerozlišuje se striktně, kdy jde o vlastní obsah, kdy o cizí obsah, podobně je tomu u dalších důležitých otázek. Proto s ohledem na zahraniční zkušenosti by bylo možno shrnout probíranou problematiku následovně.

Odpovědnost Content-Providera není u nás výslovně upravena, a proto se užijí obecné předpisy. Široce můžeme Content-Providera označit jako subjekt poskytující

vlastní obsah, budeme-li se soustředit na webové stránky, pak jde především o subjekt, který umísťuje obsah na tyto stránky, stránky spravuje i aktualizuje, obsah stránek může měnit, může rozhodnout, co na stránkách bude uvedeno a co ne, obsah umístěný na stránkách nabízí k užití (ať již bezplatnému či úplatnému). To je v podstatě základní podoba internetových stránek – jde např. o stránky určitého podniku, osobní stránky fyzické osoby, stránky občanského sdružení a další. Obvykle jsou stránky umístěny na jiných počítačích, tzv. serverech poskytujících Web-Hosting, neboli na počítačích Host-Providerů, mohou být ale umístěny i na vlastním počítači, který pak působí jako server. Nezáleží, jde-li o soukromé stránky, či stránky s obchodním zaměřením. Nejčastěji jsou na stránkách umístěny texty, mohou tam být i soubory hudební, filmové či grafické.

Odpovědnost takto jednoznačně určených Content-Providerů je vcelku jednoduchá, již shora bylo uvedeno, že náš právní řád nemá žádné privilegované ustanovení, kterým by omezoval či vylučoval odpovědnost Content-Providerů.[28] Platí proto obecné předpisy (zejména trestní zákon, občanský zákoník, obchodní zákoník především s úpravou nekalé soutěže, autorský zákon a mnoho dalších). Pokud jde o trestnou činnost, je zde internet pouze nástrojem, jak tuto trestnou činnost spáchat, Content-Provider bude za své jednání plně odpovídat. Lze souhlasit s myšlenkou, podle níž, „co je protiprávní offline, je protiprávní i online".[29] Trestná činnost takto páchaná může být velice různorodá. Nejčastěji se lze setkat s již několikrát zmíněným šířením dětské pornografie, popř. s podporou a propagací hnutí směřujících k potlačení práv a svobod člověka, můžeme ale také najít podněcování, či schvalování trestného činu, velice často jsou na internetových stránkách porušována autorská práva, a to nejen umístěním hudebních souborů, či videosouborů, ale též protiprávním kopírováním textů či fotografií, časté mohou být i verbální trestné činy (např. pomluva). Ve všech těchto případech jde ovšem o možnou odpovědnost za trestné činy spáchané konáním, nikoli opomenutím. Užijí se tak obecná pravidla odpovědnosti za takové činy, zvláštností je zde pouze užitý prostředek k páchání trestné činnosti – internet, který může vyvolávat některé dílčí problémy při řešení obecných otázek (např. pokud jde o místní působnost trestního zákona především s ohledem na místo spáchání činu a vznik následku/účinku). Tomu se ale nebudeme s ohledem na téma článku věnovat. Obvykle se tedy Content-Provider dopustí jako pachatel úmyslného komisivního deliktu, ať již ohrožovacího či poruchového.

Situace se poněkud komplikuje u interaktivních stránek. Je otázkou, zda užití odkazu (**hyperlinku**[30]) má automaticky za následek, že ten, kdo umístil takový odkaz na

---

[28] Samozřejmě za předpokladu, že nezvolíme opačný přístup s tím, že zák. č. 480/2004 Sb. odpovědnost Content-Providera na rozdíl od odpovědnosti ostatních providerů výslovně nestanoví, a proto není odpovědný, což by byl ovšem ve svém důsledku výklad absurdní a tedy nesprávný (srov. již shora).

[29] Otevřel, P. Odpovědnost za obsah na internetu (1. díl). Právo IT, 25. 6. 2007, dostupné na internetu k 1. 6. 2008 pod odkazem: http://www.pravoit.cz/rservice.php?akce=tisk&cisloclanku=2007060001.

[30] Za tímto účelem se ještě rozlišují tzv. Surface-Link (hyperlink odkazující na homepage cílové adresy) a Deep-Link (hyperlink, který neodkazuje přímo na homepage, ale na nějakou hlouběji vnořenou stránku, na kterou by se jinak musel dostat pomocí odkazu z homepage). V obou případech jde podle německé judikatury o přípustný způsob komunikace v rámci internetu, kde každý musí s odkazováním na vlastní stránky (byť ne přímo na homepage) počítat – srov. např. BGH, z 17. 7. 2003, sp. zn. I ZR 259/00.

svých stránkách, odpovídá za protiprávní obsah cizích stránek. Užívání odkazů je pro prostředí internetu typické. Výslovná úprava této problematiky v našem právním řádu chybí. Inspiraci můžeme čerpat např. v úpravě rakouské, která ale má výslovnou úpravu a která nakládá s odpovědností za odkazy na protiprávní obsah podobně jako s odpovědností Host-Providera (srov. shora), nebo v nauce a judikatuře německé, podle níž je rozhodující, zda z odkazu lze dovodit, že odkazující uvedený obsah bere za vlastní. Chybí-li nám výslovná úprava, je třeba k danému problému přistupovat z hlediska obecných zásad. Bude proto třeba zkoumat jednotlivé znaky skutkových podstat, nakolik jsou naplněny, především znak jednání a zavinění, popř. zda nejsou naplněny znaky ustanovení rozšiřujících dosah skutkových podstat uvedených ve zvláštní části (účastenství). Nikdo zřejmě nebude pochybovat o naplnění znaků skutkové podstaty trestného činu podpory a propagace hnutí směřujících k potlačení práv a svobod člověka podle § 260 odst. 1 tr. zák. jedincem, jenž vytvoří vlastní internetovou stránku, která se bude skládat pouze z několika desítek odkazů na různé jiné internetové stránky s takto závadným obsahem, tedy oslavujícím např. fašismus. Naopak, pokud sepíše pojednání o takových hnutích, v němž se od jejich myšlenek jednoznačně distancuje, a pro příklad uvede též odkaz na některé stránky obsahující protiprávní obsah, neměl by se dopustit uvedeného trestného činu, protože jeho cílem nebyla propagace a ani podpora takových hnutí.

Často užívané pouhé vyjádření, že se autor zříká odpovědnosti za protiprávní obsah cizích stránek (tzv. **disclaimer**), by samo o sobě nemělo mít valný význam, není-li podpořeno skutečným obsahem vlastní stránky. Podobně je tomu i s dalšími delikty, jako je třeba porušování autorského práva – např. tím, že na vlastních stránkách jsou Content-Providerem umístěny odkazy na neoprávněně šířené hudební soubory, videosoubory, počítačové programy, či jiné soubory, jež jsou umístěny na jiných počítačích. I zde by bylo možno dovodit přímou trestní odpovědnost s ohledem na formulaci § 152 tr. zák., resp. § 14[31] zák. č. 121/2000 Sb., autorského zákona.[32]

V případech tzv. inline-linkingu a framingu je třeba jednak řešit otázku přípustnosti takového postupu a jednak odpovědnosti za protiprávní obsah. Inline-link znamená, že cizí obsah je vtažen do obsahu vlastní stránky, aniž by na první pohled bylo zřejmé, že stránky obsahují též cizí informace – např. ve zdrojovém kódu vlastních stránek se využije odkaz na obrázek umístěný na zcela jiném serveru, než je umístěn zdrojový kód vlastních stránek. Obrázek pak na první pohled budí dojem, že je umístěn spolu se zdrojovým kódem na témže serveru. Podobně je tomu s tzv. framingem. Stránky mohou být rozděleny na rámce (frames), přičemž v jednom rámci mohou být zobrazeny internetové stránky jiného uživatele, přesto se bude takové zobrazení jevit jako vytvořené uživatelem, který vytvořil tyto rámce. V uvedených případech je URL, na nějž je odkazováno, zcela skryto. Takový postup může porušovat autorská práva pů-

[31] § 13 odst. 1: „Rozmnožováním díla se rozumí zhotovování dočasných nebo trvalých, přímých nebo nepřímých rozmnoženin díla nebo jeho části, a to jakýmikoli prostředky a v jakékoli formě."

[32] Shodně v SRN např. rozhodnutí LG München I, ze dne 25. 2. 2000, sp. zn. 4 HKO 6543/00, podle něhož nabídka ke stažení software chráněného ochrannou známkou, je nepřípustná, byť by byl soubor stahován prostřednictvím hyperlinku odkazujícího na webové stránky třetího subjektu.

vodních tvůrců obsahu, jenž je uvedenými způsoby neoprávněně a skrytě vtažen do jiných stránek.[33] Odpovědnost za cizí obsah by bylo opět možno dovodit, pokud autor stránek takovým provázáním s jinými stránkami (Inline-linking, Framing) vyjadřuje svůj vlastní obsah, resp. cizí obsah si přisvojuje. Tak tomu může být při nekalosoutěžních jednáních – např. podnikatel na své stránky uvedeným způsobem umístí odkazy na výrobky konkurence, aby takto rozšířil svou nabídku.

5. ZÁVĚR

V článku jsem se pokusil nastínit současnou právní úpravu odpovědnosti providerů, především pak Host-Providera a Access-Providera, a to jak u nás, tak v sousedním Rakousku a Německu. Odpovědnost uvedených providerů je omezena současným zákonem č. 480/2004 Sb., který se u nás netěší zdaleka takovému zájmu, jako obdobná právní úprava např. v SRN, i když je zřejmé, že problémy s užíváním internetu jsou ve všech zemích obdobné. I proto bylo vhodné seznámit se s úpravou německou a čerpat z německé nauky, resp. spíše judikatury, poznání, které vzhledem k obdobné právní úpravě by bylo využitelné i v našich podmínkách. Z tohoto pohledu je také nezbytná znalost evropské Směrnice 2000/31/ES, která byla důvodem přijetí naší úpravy této problematiky. Ze srovnání je též patrné, že v některých směrech náš zákon této směrnici zcela neodpovídá.

Mám za to, že odpovědnost Access-Providera, nevystupuje-li aktivně, jak bylo v článku rozvedeno, je za splnění podmínek § 3 zák. č. 480/2004 Sb. prakticky vyloučena, a to včetně jeho odpovědnosti za omisivní delikty. Naproti tomu u Host-Providera bychom mohli uvažovat o odpovědnosti za omisivní delikty v případech, kdy podle § 5 téhož zákona byl povinen konat a svou povinnost nesplnil. Pak bychom u něj zřejmě mohli uvažovat o účastenství na úmyslně spáchaném trestném činu Content-Providera. Na konci jsme se zabývali též problematikou odpovědnosti Content-Providera, jehož postavení není v našem řádu vůbec upraveno, což lze zvláště při užité koncepci pozitivního vymezení odpovědnosti providerů v zákoně č. 480/2004 Sb. považovat za nedostatek. Nakonec jsme se zabývali též problematikou odkazů na cizí obsah a odpovědnosti za něj.

[33] V SRN k tomu srov. judikaturu – např. rozhodnutí LG Hamburg, ze dne 12. 7. 2000, sp. zn. 308 O 205/00 (se shodným výsledkem). Známé je též rozhodnutí ve věci Online-Lexikon, OLG Hamburg, z 22. 2. 2001, sp. zn. 3 U 247/00 (nedovolené rozšiřování databáze).

DIE VERANTWORTUNG DER PROVIDER MIT DER RICHTUNG AUF DIE VERANTWORTUNG DER HOST-PROVIDER UND ACCESS-PROVIDER

Zusammenfassung

Der Autor versucht in seinem Artikel gegenwärtige Rechtsregelung der Verantwortung der Provider entwerfen, vor allem Host-Provider und Access-Provider. Der Autor betont die Bedeutung der Richtlinie des Europaparlaments und des Rates 2000/31/EG über bestimmte rechtliche Aspekte der Dienste Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt. Im übrigen widmet er sich einigen ausländischen Regelungen, namentlich Bundesrepublik Deutschland und Österreich. Nachfolgend zugliedert er das tschechische Gesetz n. 480/2004 Sb. über einige Dienste der Informationsgesellschaft. Im Verschluss wertet der Autor die tschechische Regelung und weist dahin, dass unser Gesetz in einigen Aspekten der Richtlinie nicht entspricht.

Schlagwörter: die Verantwortung für fremden Inhalt, die Richtlinie des Europaparlaments und des Rates 2000/31/EG über bestimmte rechtliche Aspekte der Dienste Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt, Access-Provider, caching, Host-Provider, der Teledienst, das Gesetz über einige Dienste der Informationsgesellschaft, Content-Provider

Klíčová slova: odpovědnost za cizí obsah, směrnice Evropského parlamentu a Rady 2000/31/ES o některých právních aspektech služeb informační společnosti, zejména elektronickém obchodu, na vnitřním trhu, Access-Provider, caching, Host-Provider, tele-služba, zákon č. 480/2004 Sb. o některých službách informační společnosti, Content-Provider

NĚKTERÉ PRÁVNÍ ASPEKTY FORENZNÍ ANALÝZY DIGITÁLNÍCH DAT

LILJANA SELINŠEK[1]
Právnická fakulta Univerzity v Mariboru, Slovinsko

1. ÚVOD

Není pochyb o tom, že žijeme v digitálním věku, kdy je stále více činností založeno na sofistikované počítačové technologii, jež téměř nepozorovatelně ovlivňuje náš každodenní život. Moderní technologie se používají v lékařství, ekonomii, vzdělávání, státních záležitostech, všech druzích dopravy apod. Moderní člověk při telefonování, cestování, komunikaci prostřednictvím elektronické pošty apod. zanechává zpravidla elektronickou stopu o těchto činnostech, která se v případě potřeby může stát rovněž důkazem v některých právních řízeních. Vedle svých pozitivních stránek, projevujících se zejména usnadněním každodenního života, však mají moderní technologie i svou stinnou stránku spočívající ve zneužití těchto technologií k různé trestné činnosti. S rozvojem počítačových technologií se bohužel staly propracovanější a lépe koordinované i techniky počítačové kriminality.

Tento vývoj klade stále vyšší nároky na obor, jenž byl založen pro účely vyhledávání důkazů v digitální podobě a jejich převádění do člověku srozumitelného jazyka: forenzní analýzu digitálních dat. Bylo by chybou spojovat forenzní analýzu digitálních dat pouze s trestnou činností páchanou prostřednictvím moderních technologií. Vzhledem k tomu, že stále více relevantních skutečností je v digitální podobě,[2] měly by se digitální důkazy stát stále relevantnějšími důkazními prostředky při všech druzích soudního řízení. Je třeba zdůraznit, že forenzní analýza digitálních dat a digitální důkazy jsou užitečné nejen při vyšetřování počítačové kriminality a jiných forem trestné činnosti, ale i při prokazování řady dalších skutečností, například vůle smluvních stran v občanskoprávních věcech.

Ve společnosti založené na moderních technologiích by se forenzní analýza digitálních dat měla nepochybně stát jednou z hlavních vyšetřovacích metod a digitální důkazy by měly být hlavními důkazními prostředky, v mnoha evropských zemích se

[1] Překlad: Mgr. Alžběta Soperová.

[2] Každoročně je po celém světě zasláno přes tři biliony elektronických zpráv. Více než 90 % dokumentů vytvořených v různých organizacích je v elektronické podobě, a méně než 30 % těchto dokumentů je vytištěno. Viz zpráva Cybex, 2007, str. 25.

však v obou případech jedná o poměrně neznámou a exotickou oblast vyšetřování trestných činů[3] a soudního řízení. Na jednu stranu je to pochopitelné, neboť forenzní analýza digitálních dat je novým vědním oborem a digitální důkazy se od klasických podstatně liší. Vzhledem k rychlému a obrovskému rozvoji technologií by však právo mělo co nejdříve přijmout metody forenzní analýzy digitálních dat a digitální důkazy jako realitu i ve státech, kde této oblasti není věnována pozornost. K tomu jsou nezbytné změny na úrovni legislativy, soudní praxe a vzdělávání stávajících a budoucích pracovníků. Avšak předtím, než bude možné podniknout jakékoli konkrétní kroky, je třeba zodpovědět základní teoretické otázky týkající se vztahu mezi forenzní analýzou digitálních dat a (trestním) právem. Tento článek se zaměřuje na některé z nich, jež zůstávají nedořešeny i v mnoha evropských zemích. V rámci níže uvedených témat se pokusíme nalézt odpovědi nebo upozornit na zvláštní témata, jimž je třeba věnovat pozornost:

- Co je forenzní analýza digitálních dat a je namístě ji upravit zákonem a případně jak?
- Kdo má provádět forenzní analýzu digitálních dat při vyšetřování trestní věci?
- Kdy by měl odborník na forenzní analýzu digitálních dat vstoupit do trestního řízení?
- Jak zajistit, aby byly výsledky forenzní analýzy digitálních dat použitelné u soudu?

2. CO JE FORENZNÍ ANALÝZA DIGITÁLNÍCH DAT A JE NAMÍSTĚ JI UPRAVIT ZÁKONEM A PŘÍPADNĚ JAK?

Forenzní analýza digitálních dat se liší od většiny tradičních forenzních disciplín. Od doby objevení technologie analýzy DNA neměla žádná metoda tak rozsáhlý potenciální účinek na konkrétní druhy vyšetřování a trestního stíhání jako forenzní analýza digitálních dat. Jedná se o vysoce technický obor, související s řadou vědních oborů a oblastí: informatikou (počítačovou vědou), matematikou, fyzikou, elektrotechnikou, strojírenstvím a systémovým inženýrstvím, právem apod. Vzhledem ke všem těmto technickým detailům a složitým procesům mají právníci často problémy používat, či dokonce jen porozumět procesům používaným při vyšetřování prostřednictvím forenzní analýzy digitálních dat.[4] Použití vědy a inženýrství při konkrétním vyšetřování představuje složitý proces vyžadující profesionální úsudek a často se proto uvádí, že forenzní analýza digitálních dat je někdy spíše uměním než vědou.[5]

Existuje řada definic forenzní analýzy digitálních dat (též počítačová forenzní analýza, digitální forenzní analýza, forenzní analýza IT, atd.). Jednu z nejvýstižnějších vypracovali Broucek a Turner, kteří popisují forenzní analýzu digitálních dat jako *pro-*

[3] Například slovinská policie řešila v letech 2001–2006 celkem 487 957 trestních případů. Z toho byly k prozkoumání počítačového vybavení použity metody forenzní analýzy digitálních dat v celkem 212 případech. Z toho vyplývá, že slovinská policie používá metody forenzní analýzy digitálních dat přibližně v 0,05 % vyšetřovaných případů.

[4] Viz Ieong, R.S.C. FORZA – Digital forensics investigation framework that incorporate legal issues. (FORZA – Rámec vyšetřování prostřednictvím forenzní analýzy digitálních dat zahrnující právní aspekty.) Digital Investigation, Elsevier 3S, 2006, str. 29, (k dispozici na stránce www.dfrws.org/2006/proceedings/4-Ieong.pdf, ke dni 21. 7. 2008).

[5] Ryan, D. J., Shpantzer, G. Legal Aspects of Digital Forensics (Právní aspekty forenzní analýzy digitálních dat.) (k dispozici na www.danjryan.com/Legal%20Issues.doc, ke dni: 21. 7. 2008), str. 2.

cesy či postupy zahrnující sledování, shromažďování, analýzu a předkládání digitálních důkazů jako součást „předběžného" a/nebo následného („post mortem") vyšetřování trestné činnosti nebo nezákonného či jiného protiprávního jednání páchaných prostřednictvím internetu, tj. on-line.[6] Forenzní analýza digitálních dat však může být samozřejmě užitečná i při vyšetřování jiné trestné činnosti, bez přístupu na internet, tedy off-line. Jednoznačná je rovněž definice forenzní analýzy digitálních dat jako *disciplíny kombinující prvky práva a informatiky za účelem shromažďování a analýzy dat z počítačových systémů, sítí, bezdrátových komunikačních prostředků a paměťových zařízení způsobem, který je přijatelný jako důkaz u soudu.*[7]

Pojem forenzní analýza digitálních dat je těsně spjat s digitálními důkazy.[8] Obdobně jako v případě forenzní analýzy digitálních dat existuje mnoho definic pojmu „digitální důkaz", nejčastěji se však používá definice, již v roce 1999 navrhla pracovní skupina SWGDE,[9] která popisuje digitální důkaz jako *jakoukoli informaci s průkazní hodnotou ve vztahu k dané události, uložená nebo přenášená v digitální podobě.* Tato definice je velmi přesná, neboť ji lze použít na jakoukoli digitální technologii (zahrnuje počítače, mobilní telefony, digitální kamery, data z elektronických bezpečnostních systémů a jakékoli jiné technologie, jež mohou být případně spojeny s počítačovou kriminalitou nebo mohou případně poskytnout digitální důkazy).

Podstatnou otázkou spojenou s právními aspekty forenzní analýzy digitálních dat však je, zda by právníci neměli nejen znát výše uvedené definice, ale i rozumět tomu, jak počítače fungují. Sheetz jasně uvádí, že při jakékoli diskusi o forenzní analýze digitálních dat je třeba pochopit, jak počítače zpracovávají informace a jak souvisejí s okolním světem.[10] S tímto názorem musíme souhlasit. Právníci používající digitální důkazy v jakémkoli právním řízení by měli znát základní principy fungování počítačů a jiných digitálních přístrojů a měli by být rovněž obeznámeni se základními zásadami forenzní analýzy digitálních dat a technickými vlastnostmi digitálních důkazů. Nejsou třeba podrobné technické znalosti, avšak k přijetí správného (správných) rozhodnutí v případech, kde jsou použity digitální důkazy, je základní povědomí v tomto směru nezbytné. Jedná se především o to, že řádné posouzení průkazní hodnoty digitálních důkazů může vycházet pouze z pochopení takových vlastností digitálních důkazů, jež je odlišují od těch klasických.

Podíváme-li se na druhy a povahu digitálních důkazů podrobněji, je třeba nejprve uvést, že existují dva základní druhy údajů shromažďovaných metodami forenzní analýzy digitálních dat: trvalá a proměnlivá data. Trvalá data jsou data uložená na lokálním pevném disku nebo jiném médiu a zůstávají zachována i po vypnutí počítače. Pro-

---

[6] Viz Broucek, V., Turner, P. Winning the battles, losing the war? Rethinking methodology for forensic computer research. (Vyhrajeme bitvy, prohrajeme válku? Přehodnocení metodiky forenzního počítačového výzkumu.) Journal in Computer Virology, 2006, č. 2, str. 4.

[7] Srov. www.us-cert.gov/reading_room/forensics.pdf.

[8] Obdobně jako jiné forenzní oblasti, i forenzní analýza digitálních dat se provádí především s cílem získat důkazy použitelné u soudu.

[9] SWGDE je zkratka pracovní skupiny Scientific Working Group on Digital Evidence, www.swgde.org.

[10] Viz Sheetz, M. Computer Forensics. An Essential Guide for Accountants, Lawyers and Managers. (Počítačová forenzní analýza. Základní příručka pro účetní, právníky a manažery.) New Jersey: John Wiley & Sons, 2007, str. 14.

měnlivá data jsou data ukládaná v paměti (RAM) nebo existující při přenosu.[11] Základní vlastností proměnlivých dat je, že budou při vypnutí počítače ztracena, takže vyšetřovatel musí znát spolehlivé způsoby jejich zachycení; právník si přitom musí být vědom faktu, že vyšetřovatel musí tuto skutečnost znát; jinak budou shromážděné důkazy s velkou pravděpodobností nespolehlivé. Aby zajistili, že svou prací poskytnou řádný základ pro soudní přezkum, musí odborníci na forenzní analýzu digitálních dat zohlednit základní zásady forenzní analýzy digitálních dat.[12] Jednou ze základních zásad je, že při vyhledávání prostřednictvím forenzní analýzy digitálních dat musí být použita kopie (nikdy originál) dotčeného digitálního média, která však musí být s originálem zcela totožná. Během vyhledávání musí být věnována zvláštní péče zachování důkazu. Ten nesmí být žádným způsobem pozměněn. Digitální důkazy lze především snadno duplikovat nebo modifikovat, často bez zanechání jakýchkoli stop, a mohou tak představovat zvláštní problémy co se týče odborné způsobilosti. Opominutí zmrazit důkaz před otevřením souborů (spolu se skutečností, že samotným otevřením se soubory změní) může rozhodující důkaz znehodnotit, čehož si musí být vyšetřovatelé a právníci pracující na daném případu vědomi. Přestože technické stránky forenzní analýzy digitálních dat a digitálních důkazů mohou být pro právníky poněkud imaginární či složité, musí znát povahu těchto důkazů, pokud je chtějí správně vyhodnotit.[13]

Pravdou je, že forenzní analýza digitálních dat může velmi pracná a únavná. Přestože údaje lze jen těžko zničit, je na druhé straně často obtížné je najít. Nalezení relevantního důkazu v obrovském množství dat může být problematické (zejména pokud jsou kódována, označena zavádějícím způsobem nebo ukryta mezi mnoha nevinnými soubory). Ještě větší problém vznikne v případě, kdy kontrola počítače není dostačující, neboť digitální důkazy jsou uloženy na různých serverech napojených na internet a mohou se tudíž nacházet v různých zemích (z nichž každá má vlastní právní řád). Odborníci na forenzní analýzu digitálních dat však mají k dispozici řadu softwarových nástrojů a pomůcek, jejichž prostřednictvím mohou analyzovat počítač nebo jiná digitální zařízení podezřelého. Nejznámějšími komerčními nástroji jsou EnCase od Guidance Software a Forensic Toolkit (FTK) od AccessData, nejznámějším open source forenzním nástrojem je však Sleuth Kit.[14]

---

[11] Podrobnější informace získáte např. na webovém serveru United States Computer Emergency Readiness Team (US-CERT), www.us-cert.gov.

[12] Tyto zásady jsou technické povahy a formulují je některé nejvýznamnější forenzní instituce. Velmi dobrou praktickou příručku týkající se elektronických důkazů získaných prostřednictvím počítače vypracovalo sdružení ACPO (Association of Chief Police Officers, www.acpo.police.uk). Je k dispozici na internetu na adrese: www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf.

[13] Více informací týkajících se povahy digitálních důkazů naleznete např. v publikaci Sheetz, M. Computer Forensics. An Essential Guide for Accountants, Lawyers and Managers. (Počítačová forenzní analýza. Základní příručka pro účetní, právníky a manažery.) New Jersey: John Wiley & Sons, 2007.

[14] Pomocí těchto nástrojů je možné obnovit smazaná data, zjistit kdy byly soubory změněny, vytvořeny či smazány, určit, jaká paměťová zařízení byla připojena ke konkrétnímu počítači, jaké aplikace byly nainstalovány (i pokud již byly odinstalovány), jaké internetové stránky uživatel navštívil apod. Není však možné obnovit data, pokud již bylo příslušné digitální médium (fyzicky) zničeno. Pokud bylo digitální médium bezpečně přepsáno, je obnova dat buď velmi obtížná, nebo nemožná. Další účinnou obranu představuje kryptografie (šifrování), která činí data nečitelnými a tudíž nepoužitelnými. Pokud je správně použito a šifrovací klíče jsou bezpečně uschovány, lze šifrování dat jen těžko prolomit. Více informací ohledně šíře forenzní analýzy digitálních dat naleznete v publikaci Casey (2004). Každopáně každý, kdo sleduje seriál Kriminálka v Las Vegas a podobné vědeckofantastické filmy ví, že z technického hlediska jsou forenzní nástroje a techniky účinné, nikoli však všemocné.

Právníci nepotřebují vědět, jak tyto forenzní nástroje fungují, musí jim však být zřejmé, zda jsou dostatečně spolehlivé k tomu, aby poskytly digitální důkazy, které budou natolik průkazné, že budou moci být použity jako základ pro soudní rozhodnutí.

Vrátíme-li se k původní otázce, zda by měla být forenzní analýza digitálních dat upravena zákonem (a pokud ano, jak), je třeba zdůraznit, že to není potřebné. Forenzní analýza digitálních dat je určitým druhem služby. Vzhledem k tomu, že se jedná o jednu z mála forenzních oblastí, jež jsou zajímavé i pro soukromý sektor,[15] kde hrají významnou úlohu pravidla hospodářské soutěže, jakékoli omezení této služby by mohlo být velice problematické. Otázka, zda by měla být forenzní analýza digitálních dat upravena zákonem, by však neměla být zaměňována s otázkou, zda je třeba zákonem regulovat digitální důkazy a zda by měly právní předpisy stanovit některá omezení ohledně toho, kdo může provádět vyšetřování prostřednictvím forenzní analýzy digitálních dat, resp. příslušnou odbornou činnost. Těmito dvěma otázkami se zabývají následující kapitoly.

3. KDO BY MĚL PROVÁDĚT VYŠETŘOVÁNÍ PROSTŘEDNICTVÍM FORENZNÍ ANALÝZY DIGITÁLNÍCH DAT?

Otázka, kdo by měl shromažďovat a analyzovat digitální důkazy, je nejpalčivější ve fázi přípravného řízení, tj. ve fázi, kdy je věc v rukou policie a/nebo státních zástupců. Menší země se v tomto ohledu potýkají s problémy spojenými s nedostatkem finančních zdrojů. Forenzní analýza digitálních dat je zpravidla velmi nákladná. Vedle výkonného hardwaru a softwaru vyžaduje stálé vzdělávání příslušných pracovníků, což rovněž vyžaduje nemalé náklady. Zatímco větší a bohatší země si mohou dovolit financovat ze státního rozpočtu neziskové instituce jako laboratoře zabývající se forenzní analýzou digitálních dat, menší země čelí finančním omezením a následně nedostatku vyškolených odborníků. Ve Slovinsku se například objevily úvahy o možnosti překonat tento problém zapojením soukromého sektoru ve fázi shromažďování digitálních důkazů v (přípravném) trestním řízení (jako druh operativní pomoci policii, resp. státnímu zástupci). Tato myšlenka sice dosud nezískala významnější podporu, musíme však souhlasit s panem Goranem Oparnicou ze společnosti INsig2,[16] který uvedl, že dříve či později si vláda bude muset zvolit mezi dvěma zly: buď vůbec nevyšetřovat, nebo zapojit do části vyšetřování soukromý sektor. Druhá možnost je patrně lepší, navzdory všem souvisejícím problémům. Před uvedením jakéhokoli takového systému do praxe je samozřejmě nutné stanovit příslušná pravidla, aby se zabránilo jeho zneužití.

---

[15] Metody forenzní analýzy digitálních dat jsou užitečné nejen při vyšetřování trestných činů a jiných sporů končících před soudem, ale jsou vhodné rovněž k řešení některých případů porušení bezpečnosti, ztráty dat nebo obdobných (nikoli nezbytně kriminálních) případů, k nimž dochází v obchodních společnostech i jiných institucích. Abychom byli přesní, v těchto případech nelze hovořit o „forenzní" analýze digitálních dat, neboť pojem *forenzní* znamená *příslušející fóru, soudní, rovněž veřejný*, obsahově se však jedná o totožnou věc.

[16] INsig2 d.o.o. je chorvatská společnost zabývající se mimo jiné vyšetřováním prostřednictvím forenzní analýzy digitálních dat Viz www.insig2.hr.

Druhá otázka spojená s problematikou „kdo" by měl tuto analýzu provádět souvisí s dilematem týkajícím se potřebné kvalifikace odborníků na forenzní analýzu digitálních dat. Respektive konkrétněji: potřebují nějaké zvláštní vzdělání? Nebo postačí, pokud budou mít v tomto oboru praktické zkušenosti? Měli by být držiteli nějakého zvláštního (státního nebo soukromého) osvědčení? a podobně. Tyto poměrně složité otázky jsou aktuální v mnoha evropských zemích a souvisejí s některými jinými nedořešenými dilematy v rámci právních aspektů forenzní analýzy digitálních dat. Lze konstatovat, že neexistuje žádná konečná a univerzální odpověď, pro další diskusi o této problematice jsou však významná některá zjištění z průzkumu společnosti Cybex.[17] Podle tohoto průzkumu se právníci i odborníci na forenzní analýzu digitálních dat shodují, že k vedení vyšetřování prostřednictvím forenzní analýzy digitálních dat jsou potřebné praktické zkušenosti a podmínkou, již musí odborník na počítačovou forenzní analýzu splňovat, je vysokoškolské vzdělání v oboru informatika, inženýrství nebo matematika. Forenzní odborníci navíc považují za nezbytné, aby dotčená osoba získala osvědčení o znalosti forenzní analýzy digitálních médií vydané veřejným orgánem. Vysokoškolsky vzdělaný odborník by měl dále mít alespoň dva roky praxe a ti, kdo nemají vysokoškolské vzdělání, by měli absolvovat pět let praxe v příslušném oboru. Pro všechny odborníky je rovněž povinné další odborné vzdělávání, aby byli schopni sledovat nejnovější vývoj. Zatímco forenzní odborníci považují za vhodné řešení osvědčení vydané veřejným orgánem, právníci se na druhé straně domnívají, že odborník na počítačovou forenzní analýzu by měl být příslušníkem policie a měl by být držitelem osvědčení o znalosti forenzní analýzy digitálních médií vydaného soukromou institucí.[18] Z těchto zjištění vyplývá, že panuje poměrně vysoká míra konsensu ohledně otázky potřebného vzdělání a kvalifikace odborníků na forenzní analýzu digitálních dat, respondenti se však neshodují ve věci systému certifikace těchto odborníků. V každém případě by bylo vhodné uplatňovat při řešení této problematiky globální přístup, neboť víceméně jednotná kritéria platná pro odborníky na forenzní analýzu digitálních dat na celém světě by příznivě ovlivnila další vývoj tohoto oboru.

4. KDY BY MĚL ODBORNÍK NA FORENZNÍ ANALÝZU DIGITÁLNÍCH DAT VSTOUPIT DO TRESTNÍHO ŘÍZENÍ?

V rámci tohoto tématu je třeba zdůraznit dvě věci. Zaprvé, jak již bylo uvedeno, forenzní analýza digitálních dat a digitální důkazy nesouvisí jen s počítačovou kriminalitou a jinými formami trestné činnosti páchané prostřednictvím moderních technologií. Naopak! Digitální důkazy získané prostřednictvím metod forenzní

[17] Španělská společnost Cybex provedla specializovaný výzkum na téma „Přípustnost elektronických důkazů u soudu. Boj proti počítačové kriminalitě". Výsledky tohoto projektu financovaného v rámci programu AGIS byly zveřejněny v roce 2007 a jsou k dispozici na adrese www.cybex.es/agis2005/elegir_idioma_pdf.htm. Do projektu se zapojilo 16 zemí: Německo, Rakousko, Belgie, Dánsko, Španělsko, Finsko, Francie, Řecko, Nizozemsko, Irsko, Itálie, Lucembursko, Portugalsko, Spojené království, Rumunsko a Švédsko.

[18] Viz zpráva Cybex, 2007, str. 41.

analýzy digitálních dat mohou být relevantní v řadě trestních věcí – a to i u těch, kde počítače ani digitální zařízení při trestném činu vůbec nefigurovaly. Philips a Kent uvádějí jako příklad nedávný trestní případ z Británie, kdy byl muž uškrcen na cestě domů ze své oblíbené místní nálevny a zdálo se, že neexistuje žádný zřejmý motiv. Z oblasti krku oběti byly získány stopy DNA a policie vyzvala její rodinné příslušníky a přátele, aby dobrovolně odevzdali vzorek své DNA a mohli tak být vyloučeni z okruhu podezřelých. Švagr zemřelého nejprve žádosti nevyhověl, pak však neochotně souhlasil, když zjistil, že se stal hlavním podezřelým. Analýza DNA nepřinesla žádné výsledky, neboť silný déšť v noci, kdy se stala vražda, smyl většinu stop a nebyl tudíž k dispozici dostatek materiálu ke zjištění shody. Během dalšího vyšetřování byl zabaven švagrův počítač. Přitom příslušné orgány postupovaly v souladu se standardními postupy uznávanými všemi soudy ve Spojeném království. Odborník na počítačovou forenzní analýzu prozkoumal švagrův počítač a zjistil, že den před vraždou zadal do internetového vyhledávače výraz „jak zabít člověka". Tento jednoduchý digitální důkaz se tak ukázal jako podstatný pro vyřešení trestného činu vraždy,[19] který rozhodně není druhem trestné činnosti páchané prostřednictvím moderních technologií. Odpověď na otázku „kdy" je tedy v každém případě „často". Digitální důkazy se vyskytují všude kolem nás a mají mnoho podob, takže lze jejich prostřednictvím prokázat různé okolnosti.

Zadruhé je však třeba zmínit ještě jiné stanovisko. Někteří odborníci upozorňují, že, zejména v případech méně závažné trestné činnosti by měla být forenzní analýza digitálních dat použita pouze tehdy, není-li k dispozici dostatek jiných, tedy klasických důkazů. Tento názor vychází z takzvané ekonomické analýzy práva, která uvádí, že nákladné metody prokazování skutečností by se měly použít pouze pokud není k dispozici levnější cesta k dosažení stejného výsledku.[20]

5. JAK ZAJISTIT, ABY BYLY VÝSLEDKY FORENZNÍ ANALÝZY DIGITÁLNÍCH ÚDAJŮ POUŽITELNÉ U SOUDU?

Existuje pouze jeden způsob, jak zajistit, aby výsledky forenzní analýzy digitálních dat byly použitelné u soudu – musí být shromážděny zákonným způsobem, tedy v souladu s platnými právními předpisy. Nestačí zajistit usvědčující digitální důkazy; musí se tak stát zákonnou cestou.[21] V řadě států však nejsou stanovena zvláštní

[19] Viz Philips, A., Kent, J. eDisclosure: Lawyers are Treading a Risky Path. (Digitální důkazy: právníci se vydávají rizikovou cestou.) publikováno na www.7safe.com/assets/pdfs/eDisclosure%20white%20paper.pdf (práce byla vypracována v únoru 2007) (ke dni: 18. 7. 2008), str. 1.

[20] Více informací o těchto aspektech naleznete v publikaci Moore, T. The Economics of Digital Forensics. (Ekonomie forenzní analýzy digitálních dat.) (k dispozici na www.weis2006.econinfosec.org/docs/14.pdf, ke dni 21. 7. 2008), str. 1–10.

[21] Například ve Slovinsku smí soud vycházet při svém rozhodování v konkrétní trestní věci pouze z důkazů, jež byly shromážděny podle příslušných ustanovení Ústavy a trestního řádu. Důkazy získané způsobem porušujícím lidská práva nebo v rozporu s trestním řádem jsou absolutně neplatné a musí být vyloučeny (analýzu nákladů a přínosů nelze v tomto případě použít). Zákonný způsob shromažďování důkazů je však v trestním řádu v mnoha případech upraven pouze obecně a často proto není zřejmé, zda jsou určité vyšetřovací techniky a opatření dovolené či nikoli. Vzhledem k nedostatečné praxi to platí zejména

pravidla týkající se shromažďování, uchovávání, ukládání a analýzy digitálních důkazů. V těchto zemích platí pro digitální důkazy obdobně stejné předpisy jako pro klasické důkazy, což může přinášet problémy. Digitální důkazy jsou zejména natolik odlišné od těch klasických, že nepochybně vyžadují zvláštní právní úpravu.[22] Je však třeba zdůraznit, že zákonodárci musí postupovat velmi obezřetně. Pokud by byly digitální důkazy zakotveny v legislativě chybně, došlo by k ještě horší situaci, než když nejsou předmětem žádné zvláštní úpravy.[23]

Zvláštní skupinu tvoří digitální důkazy získané od třetích osob, např. obětí, správců sítě, osob odpovědných za bezpečnost informačních technologií ve společnostech nebo soukromých forenzních institucí. Ve skutečnosti je soukromé shromažďování digitálních důkazů stále běžnější. To je na jednu stranu pochopitelné, neboť v řadě zemí si nejsou donucovací orgány jisté, kdy a jak by měly být metody forenzní analýzy digitálních dat použity. Ve Slovinsku není například shromažďování důkazů soukromými subjekty právně upraveno, což však neznamená, že je takový způsob získávání důkazů nezákonný. Trestní řád především obecně nezakazuje soukromým subjektům shromažďovat informace, které mají povahu důkazů, pokud takové shromažďování není v rozporu s trestním řádem, trestním zákonem a jinými právními předpisy. Je proto možné použít digitální důkazy shromážděné soukromými subjekty jako relevantní důkazní prostředek v soudním řízení, pouze však pokud byly získány zákonným způsobem.

Nakonec je třeba upozornit ještě na jednu věc. Přestože odborníci na forenzní analýzu digitálních dat (zpravidla) nejsou právníci, měli by být do určité míry obeznámeni se základními instituty trestního práva procesního. Pokud nebude digitálním důkazům ve fázi jejich shromažďování věnována řádná péče a pozornost, mohou se stát bezcennými. Jak již bylo uvedeno, digitální důkazy jsou velmi proměnlivé a lze je snadno a rychle změnit. Pokud k tomu dojde, ztratí předmětný důkaz průkazní hodnotu a stane se nepoužitelným. Nejen legislativa, ale i znalosti odborníků na forenzní analýzu digitálních dat jsou klíčové k tomu, aby výsledky vyšetřování prostřednictvím forenzní analýzy digitálních dat byly použitelné u soudu. Pokud nebudou digitální důkazy shromážděny v souladu s příslušným zákonem stanoveným postupem, bude forenzní analýza digitálních dat pouze plýtváním časem a penězi.

---

v oblasti digitálních důkazů. Forenzní analýza digitálních dat je mladý obor, který (dosud) není ve Slovinsku příliš znám ani obecně přijímán soudy, takže hranice mezi zákonným a nezákonným shromažďováním digitálních důkazů nejsou přesně stanoveny. Podrobnější informace viz Selinšek, L. Legal Collecting of Digital Evidence. (Zákonné shromažďování digitálních důkazů.) In: Zbornik Pravne fakultete Univerze v Mariboru. Maribor, 2007, 3. ročník, (dokument v anglickém jazyce), str. 226–227.

[22] Ze studie společnosti Cybex vyplývá, že žádná ze zemí zapojených do projektu nemá systematickou právní úpravu digitálních důkazů, a to ani v trestním, ani v občanském procesním právu. V některých státech platí samostatná ustanovení týkající se výhradně digitálních důkazů, jiné státy však nemají ani taková ustanovení, takže digitální důkazy podléhají stejnému režimu jako ostatní, tzv. klasické důkazy. Mnoho právníků z celé Evropy se domnívá, že stávající právní situace v jejich zemi není ideální a vyžaduje provedení změn tak, aby právo odpovídalo reálnému stavu technologií. Viz zpráva Cybex, 2007, str. 31–32.

[23] Jak vysvětluje Sheetz, digitální důkazy nejsou ve skutečnosti nic jiného než série elektronických impulsů uložených ve více či méně stabilní podobě. Tyto uložené impulzy tvoří důkaz (viz Sheetz, M. Computer Forensics. An Essential Guide for Accountants, Lawyers and Managers. (Počítačová forenzní analýza. Základní příručka pro účetní, právníky a manažery.) New Jersey: John Wiley & Sons, 2007, str. 14). Narozdíl od klasických důkazů tedy nemůžeme digitální důkaz vidět, nemůžeme si na něj sáhnout ani jej cítit – můžeme vidět pouze jeho transkripci ze strojového do člověku srozumitelného jazyka.

6. ZÁVĚR

Výše přednesené otázky jsou pouze částí rozsáhlejší problematiky a měly být zohledněny při formování základu konstruktivního vztahu mezi forenzní analýzou digitálních dat a (trestním) právem. Podstatné je, že moderní technologie by se neměly stát překážkou dalšího účinného fungování orgánů činných v trestním řízení; a naopak, trestní právo by nemělo bránit využívání moderních technologií v soudním řízení. Styčné body mezi forenzní analýzou digitálních dat a trestním právem mohou být správně vymezeny pouze na základě vzájemného porozumění. Odborníci na forenzní analýzu digitálních dat musí ovládat nejen základní zásady trestního práva procesního, ale rovněž pravidla zákonného shromažďování digitálních důkazů; naopak právníci (státní zástupci, soudci a rovněž obhájci) musí být obeznámeni se základními postupy shromažďování, uchovávání, ukládání a analýzy digitálních důkazů, a tedy základními principy forenzní analýzy digitálních dat. Tato vzájemná znalost je zárukou správného a řádného použití výsledků vyšetřování prostřednictvím forenzní analýzy digitálních dat v soudním řízení, které je nejen vítané, ale dříve i později bude rovněž naléhavě nutné – neboť žijeme v digitálním věku.

LITERATURA

1. Broucek, V., Turner, P. Winning the battles, losing the war? Rethinking methodology for forensic computer research. (Vyhrajeme bitvy, prohrajeme válku? Přehodnocení metodiky forenzního počítačového výzkumu.) Journal in Computer Virology, 2006, č. 2, str. 3–12.
2. Casey, E. Digital Evidence and Computer Crime. (Digitální důkazy a počítačová kriminalita.) Londýn: Elsevier Academic Press, 2004.
3. Zpráva z výzkumného projektu společnosti: The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime (Přípustnost elektronických důkazů u soudu: boj proti počítačové kriminalitě), Cybex, Španělsko, 2007.
4. Ieong, R. S. C. FORZA – Digital forensics investigation framework that incorporate legal issues. (FORZA – Rámec vyšetřování prostřednictvím forenzní analýzy digitálních dat zahrnující právní aspekty.) Digital Investigation, Elsevier 3S, 2006, str. 29–36 (k dispozici na stránce www.dfrws.org/ 2006/proceedings/4-Ieong.pdf , ke dni 21. 7. 2008).
5. Moore, T. The Economics of Digital Forensics. (Ekonomie forenzní analýzy digitálních dat.) (k dispozici na www.weis2006.econinfosec.org/docs/14.pdf, ke dni 21. 7. 2008).
6. Philips, A., Kent, J. eDisclosure: Lawyers are Treading a Risky Path. (Digitální důkazy: právníci se vydávají rizikovou cestou.) publikováno na www.7safe.com/assets/pdfs/eDisclosure%20white%20paper.pdf (práce byla vypracována v únoru 2007) (ke dni: 18. 7. 2008).
7. Ryan, D. J., Shpantzer, G. Legal Aspects of Digital Forensics. (Právní aspekty forenzní analýzy digitálních dat.) (k dispozici na www.danjryan.com/Legal%20Issues.doc, ke dni: 21. 7. 2008).
8. Selinšek, L. Legal Collecting of Digital Evidence. (Zákonné shromažďování digitálních důkazů.) In: Zbornik Pravne fakultete Univerze v Mariboru. Maribor, 2007, 3. ročník, str. 217–230 (dokument v anglickém jazyce).
9. Sheetz, M. Computer Forensics. An Essential Guide for Accountants, Lawyers and Managers. (Počítačová forenzní analýza. Základní příručka pro účetní, právníky a manažery.) New Jersey: John Wiley & Sons, 2007.

Summary

The article is dealing with some legal aspects of digital forensics from the viewpoint of the countries where digital forensics is not (yet) often used investigation method, and digital evidences are not everyday evidence means. The questions discussed in the article should be answered at the beginning of the establishment the proper and legally accepted relation between digital forensics and law (the stress is, however, on criminal law, because the author is working in this field). The main goal of the article is to open some questions and to offer some possible answers. However, it has to be stressed that there is no universal answers on the questions about relation between digital forensics and law. While digital forensics is based on the similar principles and rules all around the world, the law is pretty much specific for almost each country. Besides, different levels of technical and informational development of the countries have to be taken into consideration. Even if questions from the article are already solved in some countries, they have just opened in the other ones, so it can be stated these questions are going to be relevant for some time.

Keywords: digital forensics, digital evidence, digital forensic expert, digital forensic examination, criminal procedure law

Klíčová slova: digitální analýza forenzních dat, digitální důkaz, odborníci na forenzní alalýzu digitálních dat, trestní právo procesní

ACTA
UNIVERSITATIS
CAROLINAE

IURIDICA 4/2008

ČESKÝ PRÁVNÍ ŘÁD A OCHRANA KYBERPROSTORU (vybrané problémy)

Obálku navrhla Jarmila Lorencová
Graficky upravila Kateřina Řezáčová
Vydala Univerzita Karlova v Praze
Nakladatelství Karolinum, Ovocný trh 3, 116 36 Praha 1
Praha 2008
Sazba a zlom: DTP Nakladatelství Karolinum
Vytiskla tiskárna Nakladatelství Karolinum
Periodicita: 4×/rok
Vydání 1. Náklad 400 výtisků

MK ČR E 18585
ISSN 0323-0619

ISSN 0323-0619