

## 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 jakékoli 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 vyhledávačů (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 užívané 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.<sup>1</sup> Často se termínem internet rozumí právě síť world wide web. Internet je ovšem mnohem starší, umožňuje přenos dat i jiným způsobem<sup>2</sup> než jen prostřednictvím hypertextových dokumentů, které původně sloužily pro sdělování informací a později i jako uživatelské rozhraní pro veřejné služby a aplikace (jde o nepřeborné 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<sup>3</sup>, 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 tomu u telefonního seznamu) na skutečné číselně vyjádřené internetové adresy, díky nimž je vyvolán skutečný adresovaný počítač s konkrétní **IP-Adresou** (Internet Protocol – Adresa)<sup>4</sup>, 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.<sup>5</sup>

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,

<sup>1</sup> 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).

<sup>2</sup> 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.

<sup>3</sup> HyperText Markup Language.

<sup>4</sup> 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](http://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.

<sup>5</sup> 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).<sup>6</sup> 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.<sup>7</sup>

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

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

<sup>7</sup> K tomu všemu srov. čl. 1 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 přenášena informace nepozměňuje, což se ovšem netýká zásahů technické povahy během přenosu, neboť takto se nemění celistvost přenášené informace, zvláště 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.<sup>8</sup> 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.<sup>9</sup> 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 – dozorcí 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.<sup>10</sup>

<sup>8</sup> 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 odpovědnosti za určitý potenciální zdroj nebezpečí. Více k tomu srov. Říha, J. Postavení garanta u nepravých omešivních deliktů. Trestněprávní revue, 2003, č. 8, str. 227 a násl., č. 9, str. 259 a násl.

<sup>9</sup> 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 jednatelce – 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.

<sup>10</sup> 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. Námí 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 sítí, 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 sítí 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. safe 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 prvního odstavce (tedy omezení/vyloučení odpovědnosti providera), 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 člancích 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 stále 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<sup>11</sup>, a Teledienstdatenschutzgesetz (TDDSG), přesněji Gesetz über den Schutz personenbezogener Daten bei Telediensten<sup>12</sup>, jako součásti „multimediálního zákona“ účinného dokonce již od 1. 8. 1997!<sup>13</sup> Dalším dů-

<sup>11</sup> Doslova zákon o užívání „tele-slужeb“.

<sup>12</sup> Doslova zákon o ochraně osobních dat v „tele-slужbách“.

<sup>13</sup> Tzv. luKDG = 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-slужbami“ 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<sup>14</sup> (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-slужby“ 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.<sup>15</sup> 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.<sup>16</sup> 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 uvedených 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-Providera, jenž není odpovědný za cizí informace, které v komunikační síti přenáší či zpřístupňuje, pokud zároveň jejich zpro-

<sup>14</sup> Doslova zákon o „tele-médiích“.

<sup>15</sup> „Poskytovatelé služeb jsou za vlastní informace, které umožňují využít, odpovědní podle obecných zákonů.“

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

středkování nepodněcuje, nevybírám adresáta zprostředkovávané informace, či zprostředkovávanou informaci nevybírám 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.), nedopadlo 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-Providera, 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 diskusního 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<sup>17</sup> (ovšem v trestněprávní rovině musí být u fyzické osoby, jednatele, dáno též zavinění, obvykle dokonce úmyslné). Lze pak ale dovést 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 vyhledávače nebo jiného elektronického prostředku, není odpovědný, pokud zprostředkování zadané informace nepodnítl, 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 vyhledávače 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 zprostředkovaného obsahu, která musí být bez dalšího zřejmá (pak ovšem jde o obdobu odpovědnosti jako u Host-Providera).<sup>18</sup>

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-

<sup>17</sup> Siebert, S. Die rechtsichere Webseite. B4U 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 porušeníh práva.

<sup>18</sup> 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<sup>19</sup>, 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 naříditi zdržet se, odstranit či zabránit porušování práva. Podle druhého odstavce § 19 se předcházející ustanovení užití 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, nabytí platnosti a účinnosti od 7. 9. 2004 (zákon tak neposkytl adresátům žádnou legisvakanci lhůtu, i přes to, že za porušení tohoto zákona hrozí až několikamilionové pokuty).

<sup>19</sup> 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 výslovně 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 „antispamovým 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<sup>20</sup>), 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 providera 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

<sup>20</sup> 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](http://www.mvcr.cz/micr/scripts/detail.php_id_1769.html).

zvláštních důvodů, pro které by odpovídal podle své účasti na způsobení škody.<sup>21</sup> 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 společností 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).<sup>22</sup> 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 způsobitelné 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, společnost 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<sup>23</sup>, neboť

<sup>21</sup> 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-poskytovateluw-web-hostingu-za-cizi-obsah/>.

<sup>22</sup> 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).

<sup>23</sup> 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 Směrnicí 2000/31/ES, resp. Směrnicí 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 úplat, 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 základních 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).<sup>24</sup> 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 Směrnicí 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 pornografii). Dosud soudy takové pokusy jednomyslně odmítají.<sup>25</sup>

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

<sup>24</sup> 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. incidentní 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.

<sup>25</sup> Srov. např. rozhodnutí LG Kiel z 23. 11. 2007, sp. zn. 14 O 125/07 (žaloba na blokování webových stránek Access-Providere 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 případech 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 postihu 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 nepřijatelných 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 dovést 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-mail 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.<sup>26</sup> 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.<sup>27</sup> Tyto kroky musí být též proporcionální ke sledovanému cíli, není možné zablokovat řadu internetových stránek jen proto, že malá část obsahuje protiprávní obsah.

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

<sup>27</sup> 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 otázk. Proto s ohledem na zahraniční zkušenosti by bylo možno shrnout probíranou problematiku následovně.

Odpovědnost Content-Providera není u nás výslovně upravena, a proto se užití 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.<sup>28</sup> 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“.<sup>29</sup> 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 páčání 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**<sup>30</sup>) má automaticky za následek, že ten, kdo umístil takový odkaz na

<sup>28</sup> 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 odpovídající, což by byl ovšem ve svém důsledku výklad absurdní a tedy nesprávný (srov. již shora).

<sup>29</sup> 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&cislocianku=2007060001>.

<sup>30</sup> 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 prostředím 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<sup>31</sup> zák. č. 121/2000 Sb., autorského zákona.<sup>32</sup>

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 něž je odkazováno, zcela skryto. Takový postup může porušovat autorská práva pů-

<sup>31</sup> § 13 odst. 1: „Rozmnožováním díla se rozumí zhotovování dočasných nebo trvalých, přímých nebo nepřímých rozmnoženin díla nebo jeho části, a to jakýmkoli prostředky a v jakékoli formě.“

<sup>32</sup> 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 nepřipustná, 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.<sup>33</sup> 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 užití 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.

<sup>33</sup> V SRN k tomu srov. judikaturu – např. rozhodnutí LG Hamburg, ze dne 12. 7. 2000, sp. zn. 308 O 205/00 (se shodným výsledkem). Známe 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-slужba, zákon č. 480/2004 Sb. o některých službách informační společnosti, Content-Provider