Polčák, Radim. Nekalá soutěž na internetu - vymezení, typologie a příklady nekalosoutěžních praktik založených na nepřiměřeném lákání a parazitismu. Obchodní právo : časopis pro obchodně právní praxi, Praha : Prospektrum, ISSN 1210-8278, 2005, 14, 5, od s. 2-8

Úvod

Působí-li soutěžitel v prostoru celosvětové sítě Internet, nemůže na svůj soutěžní úspěch čekat se založenýma rukama a spoléhat pouze na kvalitu vlastního produktu a síťový efekt[1]. Nové technické možnosti komunikace a prezentace informací tak s sebou přinesly i prudký rozvoj nových technik lákání spotřebitelů, zejména pak inovace v oboru reklamních médií. Z hlediska ochrany soutěžních vztahů je třeba si nových metod užívaných v reklamě všímat především tehdy, jsou-li způsobilé narušit soutěžní prostředí, a to zejména formou takového působení na adresáty, které vylučuje nebo omezuje jejich rozumný úsudek v tom, jaké produkty, za jakých podmínek nebo v jakém množství budou předmětem jejich spotřeby. S postupující penetrací se stala celosvětová síť Internet vyhledávaným reklamním prostředím, zcela zřejmě i z důvodu toho, že „v dnešním světě přesyceném informacemi volí reklama opět nové metody, aby jimi zaujala pozornost možných spotřebitelů.[2]“

V případě nejběžnější formy takzvané internetové reklamy, tj. reklamních proužků a rámečků, je situace obdobná jako v případě televizních či novinových inzerátů a audiovizuálně prezentované reklamní sdělení tak i zde může být „vtipné, nudné, trapné i sprosté.[3]“ Autor si tak dovolí v dalším výkladu pominout takové případy internetové reklamy, které oproti mediální reklamě jiných forem nevykazují žádné podstatné zvláštnosti a dají se na ni aplikovat již existující poznatky právní vědy[4].

Bannery a pop-up okna

Doposud převažující forma internetové reklamy, tj. již zmíněné proužky či rámečky, až na výjimky ve výše popsaném smyslu nevybočuje z již známých reklamních standardů. Za jednu z takových výjimek je možné považovat skutečnost, že reklamní proužek, rámeček nebo takzvané reklamní pop-up okno zpravidla obsahuje nejen reklamní sdělení, ale slouží i jako prostředek interakce mezi soutěžitelem a spotřebitelem. Zaujme-li tak některá ze

[1] k pojmu viz Katz, M. L., Shapiro, C. Network Externalities, Competition and Compatibility. American Economic Review, ročník 1985, číslo 7, str. 424 a násl.
[2] viz Hajn, P. Šokující reklama a její sankcionování. Právo a podnikání, ročník 1997, číslo 2, str. 21.
[3] viz Kulhánek, M. Záporné expresivní výrazy v reklamě. Právo a podnikání, ročník 1997, číslo 11, str. 26.
[4] srov. např. Hajn, P. Co je (a co není) dovoleno v reklamě. Profit Speciál, ročník 1992, číslo 10, str. 12 a násl.

jmenovaných reklamních forem spotřebitele natolik, že na ni klikne, dojde zpravidla k jeho přesměrování na www prezentaci soutěžitele, o jehož reklamu se jedná. V této souvislosti tak může dojít k nemravnému zmatení spotřebitele tím, že příslušný reklamní element se tváří nikoli jako reklama ale například jako funkční prvek nebo dokonce systémové sdělení.

Příklad:
Velice oblíbená je například imitace systémových oken se závažný sdělením – takové okno navenek vypadá stejně jako okna operačního systému upozorňující uživatele na chyby v běhu aplikačních programů nebo systémových služeb, a to včetně textu příslušného sdělení. Z pop-up okna tak můžeme například obdržet vemlouvavou informaci ve stylu „POZOR! Na Vašem počítači se mohou vyskytovat kritické chyby (ang. WARNING! You may have critical errors on your PC.)
Záludná je tato forma reklamy jednak v tom, že spotřebitel je oklamán, neboť očekává aplikační nebo systémovou odezvu, ale také z důvodu toho, že je reklamní odkaz aktivován v případě, klikne-li i mimo tlačítko se souhlasným projevem, tj. kamkoli do příslušného okna nebo reklamního proužku (tzn. i tehdy, klikne-li spotřebitel do místa vypadajícího jako tlačítko s odmítavým projevem jako „Ne“ nebo „Storno“). Přehlédnout šedý nápis v levém spodním rohu okna vysvětlující, že se jedná o reklamu, je přitom velice jednoduché – uživatel navíc nemusí být apriori srozuměn s tím, že reklamní charakter okna znamená jeho jednostrannou funkčnost.
Obranu proti výskytu reklamních oken, reklamních proužků a jim podobných reklamních instrumentů poskytují specializované aplikace[5]*. Jejich nasazením sice není možné dosáhnout úplného odstranění reklamy z internetových prezentací, omezení jejich výskytu je však při nasazení těchto aplikací velmi podstatné.*

Spamming, linking

Široce rozšířenou reklamní praktikou je takzvaný spamming[6]. Jedná se o metodu šíření reklamního sdělení prostřednictvím e-mailu velkému počtu adresátů. Jeho nemravnost spočívá v tom, že adresát je, aniž by k tomu dal souhlas, tímto sdělením obtěžován a škodlivý důsledek má podobu nákladů, které musí adresát vydat v souvislosti s přijímáním a manipulací s nevyžádanými reklamními e-maily včetně nákladů na zmařený čas. Kromě práva proti nekalé soutěži je v současné době tato forma reklamního působení regulována i preskriptivními normami veřejného práva[7] – problém však v této souvislosti představuje

[5] viz např. Goldmann, M. Pryč s webovou reklamou! Chip, ročník, 2004, číslo 2, str. 78 a násl.
[6] k pojmu viz např. Frimmel, M. Elektronický obchod / právní úprava. Praha: Prospektrum, 2002, str. 147 a násl. – k právní kvalifikaci a možnostem obrany viz tamtéž
[7] speciální úprava zakazující spamming pod hrozbou veřejnoprávních sankcí, tj. zejména pokut, je obsažena v zákoně č. 480/2004 Sb. o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti)

zejména lokalizovaný charakter internetové jurisdikce, neboť valná většina spamů je odesílána ze serverů umístěných pod takzvanou banánovou (případně rýžovou) jurisdikcí[8].

Specifickou formou nekalého internetového reklamního působení stojícího na pomezí nekalého lákání a parazitismu je takzvaný linking. Jedná se o automatické (takzvaný aktivní linking) nebo manuální (takzvaný pasivní linking) přesměrování komunikace, přičemž nekalosoutěžním není link (odkaz) sám o sobě, ale celé spojení informace o odkaze, odkazu samotného a cílového místa takového odkazu. Ačkoli ve známém českém právním prostředí se zatím nevyskytnul případ, kdy by soud posuzoval protiprávnost pasivního linkingu (tedy pouhého umístění odkazu na www prezentaci), není z hlediska právního žádná významná překážka tomu, aby se tak stalo. Zahraniční soudy, zejména pak soudy ve Spojených státech amerických, již mají ve věcech pasivních i aktivního linkingu rozvinutou kvalitní judikaturu. Typickými případy linkingu jsou zejména takové, kdy je ve formě odkazu zpřístupněn nekalosoutěžní nebo jinak protiprávní informační obsah.

Příklad:
Jeden z precedentních případů, který rozhodoval soud v Americkém státě Utah[9], se týkal pasivního odkazu umístěného na stránkách soukromé obchodní společnosti. Ta původně poskytovala uživatelům možnost ze svých www stránek stáhnout publikaci o církevních obřadech. Vlastník majetkových autorských práv[10] k tomuto dílu však dosáhl soudního rozhodnutí, kterým bylo žalovanému další šíření tohoto díla zakázáno. Žalovaný tak v souladu s rozhodnutím soudu toto dílo ze své www prezentace odstranil, namísto něj tam však umístil 3 odkazy na jiné stránky (zřejmě fyzicky umístěné mimo jurisdikci příslušného soudu), kde toto dílo bylo nadále k dispozici. Soud v tomto případě klasifikoval linking jako porušení práv duševního vlastnictví, vzhledem k povaze věci by však dle názoru autora bylo možné při výskytu obdobného případu v českém právním prostředí postupovat nejen podle restriktivních ustanovení práva autorského, ale též podle ustanovení práva proti nekalé soutěži.

Argumentem hovořícím proti odpovědnosti za pasivní odkaz by mohlo být, že s odpovědností subjektu udržujícího odkaz je tomuto subjektu přičtena i odpovědnost či spoluodpovědnost za cílový obsah jako takový, a to i v případě, kdy subjekt nemá možnost tento obsah ovlivnit. Vzhledem k tomu, že subjekt s prezentací, na níž se pasivní odkaz nachází, *de facto* pomáhá uživatelům v přístupu k cílovým datům, je však konstrukce spoluodpovědnosti dle názoru autora na místě – nesporně se totiž z objektivního hlediska jedná o usnadnění cesty k cílovému místu a tudíž o podíl na šíření tam obsažených informací. Diskutabilní je však situace, kdy si spotřebitel příslušnou prezentaci s pasivními odkazy vytváří sám vlastním

[8] srov. Polčák, R.: Delokalizovaná jurisdikce a možnosti argumentace extenzivního výkladu § 87 písm. b) OSŘ. Jurisprudence, číslo 1, ročník 2004, str. 9 a násl.
[9] reference k rozhodnutí: 75 F. Supp. 2d 1290 (D. Utah, Dec. 6, 1999)
[10] k pojmu viz např. Telec, I. Tvůrčí práva duševního vlastnictví. Brno: Doplněk, 1994, str. 112 a násl.

dotazem automatické vyhledávací službě (takzvanému portálu nebo vyhledávači[11]) – zde je zřejmě možné domnívat se, že jakýmsi rozmělněním spoluodpovědnosti mezi vyhledávač a uživatele nabývá tato spoluodpovědnost značně neurčitých rysů a v praxi by byl problém ji prokazovat[12].

Aktivní linking je metoda, při níž je uživatel (spotřebitel) na určité cílové místo přesměrován automaticky. Aktivního linkingu je jako nekalosoutěžního nástroje často využíváno ve spojení s nekalosoutěžní registrací doménových jmen. Soutěžitel si tak příkladně zaregistruje doménové jméno podobné nebo shodné s firmou nebo označením produktu svého konkurenta a uživatelé, kteří se ke konkurenčnímu produktu snaží jeho prostřednictvím dostat, jsou pak automaticky přesměrování na konkurenční www prezentaci.

Meta-tagging

Typickým případem nekalosoutěžního využití technik, jež jsou k dispozici v prostředí celosvětové sítě Internet, je i zneužití takzvaných meta-tagů[13]. Jedná se opět o kombinaci parazitismu a klamavého lákání spotřebitele, přičemž tato technika se objevila jako důsledek rozšířeného použití již zmíněných takzvaných vyhledávačů, které odpovídají na dotaz uživatelů tím, že nabízejí odkazy na www prezentace pokud možno co nejvíce vyhovující zadanému dotazu. Vyhledávač funguje automaticky a relevantním kriteriem pro výběr odkazů a jejich přiřazení k příslušnému dotazu jsou vzhledem k dotazu (tj. k zadaným klíčovým slovům) zejména:

1) doménové jméno prezentace,
2) výskyt klíčových slov v prezentaci,
3) výskyt klíčových slov v meta-tagu prezentace
4) výskyt klíčových slov v odkazech na prezentaci.

V porovnání s tím, jak je použití firmy případně produktových označení konkurentů v doménovém jménu *prima facie* viditelné stejně jako výskyt těchto výrazů v samotné prezentaci, představuje zařazení těchto pojmů do meta-tagu mnohem hůře zjistitelný způsob

[11] jedná se o známé služby jako např. www.seznam.cz, www.google.com, www.yahoo.com a jiné

[12] výjimkou byl v tomto směru veřejnoprávní spor vedený proti známému vyhledávači Yahoo u francouzských soudů – vyhledávači bylo pravomocným rozhodnutím zakázáno nadále zpřístupňovat odkazy www prezentací propagujících nacismus v případech, kdy o ně požádá uživatel přistupující k vyhledávači z místa identifikovaného francouzskou národní doménou 1. úrovně

[13] jedná se o informaci, která se uživatelům přistupujícím k prezentaci nezobrazuje, ale která má právě pro potřeby internetových vyhledávačů a jim podobných služeb vymezit za užití klíčových slov, jaký je informační obsah příslušné prezentace

parazitismu. Uživatel, který zadá klíčovým slovem například název produktu tak může být naveden i na stránku konkurence, která s příslušným produktem, respektive jeho označením, nemá nic společného. Konkurent tak nekalým způsobem může těžit z renomé značky, na jehož budování se nikterak nepodílel. Zde je však třeba podotknout, že meta tag slouží jako informace pro vyhledávání www prezentací s užitím klíčových slov a případné použití konkurenčních označení je možné tehdy, má-li k tomu subjekt vzhledem k materii prezentace oprávněný důvod.

Příklad:
Rakouský Nejvyšší soud[14] posuzoval žalobu proti vynálezci (první žalovaný), jehož některé patenty odkoupil a používal žalobce a proti konkurentu žalobce, který od prvního žalovaného rovněž odkoupil několik patentů[15]. Předmětem sporu byly stránky obou žalovaných, na nichž byla uveřejněna informace o 32 patentech prvního žalovaného doplněná o poznámku, že některé z patentů koupil žalobce, přičemž v závorce bylo pak uvedeno označení chráněné ochrannou známkou, pod nímž žalobce nabízí své produkty. Označení produktů žalobce pak oba žalovaní použili v meta tagu svých www prezentací. Soud v tomto případě žalobu zamítnul s poukazem na oprávněný důvod obou žalovaných toto označení užít, neboť „Používá-li třetí osoba ochrannou známku v meta-tagu, neporušuje tím právo na ochranu proti nekalé soutěži ani právo k ochranné známce, pokud má oprávněný zájem používat ochrannou známku a pokud používání ochranné známky nemá nevhodný účinek. To je zejména ten případ, kdy domovská stránka obsahuje informace o ochranné známce, na nichž má třetí osoba oprávněný zájem (např. informace o prodeji patentů třetí osoby majiteli ochranné známky). Pokud tomu tak není, může majitel ochranné známky žádat po spolusoutěžiteli, aby se postaral o výmaz odpovídajících záznamů registrovaných u nejdůležitějších vyhledávacích programů.“

Trójské koně, dialery

Jednou z nejnebezpečnějších nových forem nekalosoutěžního jednání spočívajícího v nemravném lákání spotřebitelů jsou násilné a skryté formy reklamy a vynucování si spolupráce. Iniciace těchto nekalosoutěžních postupů probíhá nejčastěji za užití takzvaného trójského koně, což je programový kód, jenž se nepozorovaně (ať už v souvislosti s návštěvou www prezentace nebo s instalací některé aplikace) dostane do systému počítače. V něm pak po své aktivaci vykonává nejrůznější činnosti, a to bez vědomí uživatele. Způsob, jímž takzvané trójské koně působí, se tak v mnohém podobá působení destrukčních programových kódů, tj. virů.

[14] rozhodnutí ve věci č.j. (4 Ob 308/00y)
[15] komentář k rozhodnutí viz Pospíšil, M. Rakousko: Rozhodnutí rakouského Nejvyššího soudního dvora zabývající se známkoprávní a soutěžněprávní přípustností používání „meta-tagů“. IT právo, 2002. http://www.itpravo.cz/index.shtml?x=91526

Trójské koně je možné dělit podle typu činnosti, kterou po své aktivaci bez vědomí uživatele provádějí. Typické tak jsou například kódy měnící výchozí nastavení internetových prohlížečů tak, že po spuštění systému je uživatel bez ohledu na nastavení, která sám provedl, přesměrován na určitou www prezentaci. Objevují se však i mnohem rafinovanější varianty těchto programů, které zasahují až do www stránek vygenerovaných některým z internetových vyhledávačů – uživatel, který se pak snaží kliknutím na příslušný odkaz dobrat na cílové místo označené vyhledávačem, je namísto toho automaticky přesměrován na zcela jinou www prezentaci nastavenou trójským koněm.

Dalším typickým způsobem použití trojského koně je takzvaný spyware. Jedná se o programový kód, který po své aktivaci bez vědomí uživatele zasílá informace o jeho systému, nainstalovaném software, navštívených www prezentacích nebo příkladně o kontaktech v uživatelově adresáři či číslech kreditních karet, na sběrnou adresu. Využití těchto dat pak může mít v lepším případě charakter nekalosoutěžní marketingové analýzy, v horším případě se může dokonce jednat o závažnou majetkovou trestnou činnosti jako vykrádání bankovních kont apod.

Zvláště nemravnou formu použití trójského koně představují takzvané dialery. Jedná se o kódy, které se uplatní v případě, je-li uživatel připojen k síti Internet za užití vytáčené telefonní linky[16]. Za normální situace je toto připojení účtováno běžným poplatkem, o němž je uživatel informován v ceníku poskytovatele telekomunikačních služeb. Dialer však po aktivaci změní bez vědomí uživatele nastavení přípojného bodu tak, že namísto původně nastaveného čísla poskytovatele připojení k síti Internet je automaticky vytočeno číslo jiné služby, která je zpoplatněna mnohonásobně vyšší sazbou. Uživatel (spotřebitel) je tak v tomto případě nikoli jen nekale přichýlen (nalákán) ke službám soutěžitele, ale je k jejich odběru, navíc za krajně nevýhodných podmínek, bez vlastní vůle a dokonce i bez vlastního vědomí donucen násilným technickým zásahem[17].

Příklad:

V případě, který se po odvolání a kasaci (revizi) dostal až ke Spolkovému soudnímu dvoru[18] se jednalo právě o situaci, kdy dialer skrytý v aplikačním programu změnil nastavení síťového připojení v osobním počítači tak, že jeho uživatel se bez vlastního vědomí připojoval

[16] k pojmu viz např. Dočekal, D. Podvodné programy utrácejí za váš telefon. Digiweb, www.digiweb.cz , 12. 2. 2003

[17] k technickým aspektům použití dialerů srov. Peterka, J. Kauza nadměrných telefonních účtů. Lupa, www.lupa.cz , 10.3. 2003.

[18] případ č.j. III ZR 96/03

k internetu nikoli prostřednictvím poskytovatele služeb, kterého si původně vybral, ale prostřednictvím tzv. žluté linky s mnohonásobně vyšší cenou. Žalovanou byla v tomto případě zákaznice telekomunikačního operátora, která svoji telefonní linku využívala nejen k hovorům, ale i k internetovému připojení. Její syn si z internetu stáhnul program, jehož deklarovanou funkcí bylo zlepšení parametrů internetového připojení. Když však zjistil, že program kromě základních vlastností připojení upravil i telefonní číslo přípojného bodu, rozhodl se jej odinstalovat. V informacích programu o deinstalaci bylo uvedeno, že po odstranění program v systému uživatele nezanechá žádné své součásti a že všechna nastavení uvede do původní podoby. Program však obsahoval tzv. trójského koně, který v systému zůstal i po deinstalaci a nepozorovaně změnil nastavení přípojného bodu tak, že namísto svého poskytovatele připojení se uživatelka nadále připojovala k jinému poskytovateli na tzv. žlutou linku s výrazně zvýšenou sazbou. V důsledku působení dialeru tak účtovala telekomunikační společnost uživatelce a pozdější žalované mnohonásobně vyšší poplatky za užívání telekomunikační sítě, než bylo obvyklé. Žalovaná tyto poplatky odmítla zaplatit a celý spor skončil u soudu.

Soud zde poukázal na to, že žalobce využil jednání 3. osoby (provozovatele žluté linky, který distribuoval i software s dialerem) k tomu, aby od něj žalovaná odebrala služby s vyšší sazbou[19]. Bylo-li takové jednání úmyslným jednáním v rozporu s dobrými mravy, je tedy odpovědnost za něj přičitatelná kromě provozovatele žluté linky i samotnému žalobci, neboť ten z něj těžil[20].

V otázce obsahu smlouvy, která se na vyšel jak z ostatních ustanovení smlouvy, tak z obecných kontraktačních norem civilního práva a došel k důležitému závěru, že v uvedeném případě nemohlo jít na straně žalované[21] o nevědomou nedbalost, když nezpozorovala, že se do jejího systému dostal skrytý dialer. Skutková zjištění navíc ukazovala na to, že žalovaná z obezřetnosti příslušný software odstranila, přičemž spoléhala na informace jeho poskytovatele (který byl totožný s provozovatelem žluté linky) v tom směru, že odinstalací bude příslušný program zcela odstraněn a všechna nastavení uvedena do původního stavu.

Kombinací všech uvedených skutkových zjištění a jejich právní kvalifikace, tj.

1) *distribuce software s dialerem je úmyslným jednáním proti dobrým mravům,*[22]

---

[19] tato kvalifikace byla odůvodněna § 278 BGB, který upravuje odpovědnost dlužníka za jednání osob použitých k plnění dluhu

[20] soud při této kvalifikaci zohlednil i to, že v porovnání s běžnými telekomunikačními službami plynou z poskytování připojení k tzv. žlutým linkám telekomunikačním operátorům poplatky ve vyšších sazbách

[21] v této otázce soud logicky a nikoli překvapivě konstatoval, že jednání syna lze žalované přičíst

[22] soud jej podřadil pod rozsah ustanovení § 826 BGB – odpovídajícím ustanovení je § 424 zákona č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů

2) *existující smluvní konstrukce smlouvy o poskytování telekomunikačních služeb nedopadá na spojení uskutečněná v důsledku aktivace dialeru a*
3) *použití dialeru je kromě jeho tvůrce a provozovatele tzv. žluté linky přičitatelná i telekomunikačnímu operátorovi,*

dospěl soud k závěru, že zatímco žalobce vznáší nárok na zaplacení zvýšených poplatků za užívání služeb žluté linky, existuje analogicky s tím nárok žalované vůči žalobci na náhradu škody způsobené v důsledku úmyslného jednání proti dobrým mravům přičitatelného žalobci. Z tohoto důvodu tedy nebylo možné přiznat žalobci jeho nárok v plné výši a žalované byla uložena povinnost uhradit poplatky za telekomunikační služby jen do výše běžných poplatků za uskutečněná spojení (tj. takových, k jejich úhradě by byla povinna, nebyl-li by dialer instalován[23]).

Závěrem

Provedený příkladný výčet agresivních a parazitních nekalosoutěžních praktik si v žádném případě nekladl za cíl zmapovat tuto problematiku do hloubky a bezezbytku. Jeho cílem bylo spíše poukázat na skutečnost, že specifické formy nekalých soutěžních praktik vyskytujících se v prostředí celosvětové informační sítě nemají charakter neprávních či mimoprávních skutečností a nestojí tak mimo rozsah příslušných preskriptivních či ochranných norem (v tomto případě) práva proti nekalé soutěži. Na příkladech ze zahraniční justiční praxe je přitom možné vidět, že efektivní *de iure* obrana proti „virtuálním[24]“ protiprávním skutečnostem nemusí nutně stát jen na takzvaně nových normách pozitivního práva, ale je možné k ní přistoupit i kvalitní interpretací a aplikací stávajícího normativního aparátu. Relativně abstraktní charakter norem práva proti nekalé soutěži pak k takovému postupu přímo vybízí.

[23] v tomto směru pomohla Spolkovému soudu i ustálená judikatura v otázce odpovědnosti za závazek založený protiprávním jednáním – v takových případech je třeba využít všechny možnosti k tomu, aby se na právní postavení osoby, jejíž závazek byl založen v důsledku úmyslného protiprávního jednání, hledělo, jakoby závazek vůbec nevzniknul

[24] k problematice a nepřesnostem v používání pojmu virtuální viz např. Lévy, P. Becoming Virtual – Reality in the Digital Age. New York: Plenum Trade, 2002.