Vysoká škola ekonomická v Praze
Fakulta informatiky a statistiky
Vyšší odborná škola informačních služeb v Praze

Jan Přikryl

Právní normy upravující spam v ČR a jejich realizace

Bakalářská práce

2007

Prohlášení

Prohlašuji, že jsem bakalářskou práci na téma Právní normy upravující spam v ČR a jejich realizace zpracoval samostatně a použil pouze zdrojů, které cituji a uvádím v seznamu použité literatury.

V Praze dne: Podpis:

Poděkování

Děkuji PhDr. Haně Slámové za vedení, pomoc a cenné rady při vypracování bakalářské práce. Zároveň děkuji Mgr. Martinu Plíškovi, řediteli Odboru legislativně-právního Úseku pro vnější vztahy Ministerstva Informatiky ČR, a Ing. Miloši Šnytrovi, inspektoru Úřadu pro ochranu osobních údajů, za poskytnutí cenných rozhovorů, ze kterých jsem čerpal aktuální informace a postřehy potřebné pro vypracování bakalářské práce.

1 Obsah

2 Anotace

V první části mé práce se zabývám vývojem spamu jako takového, popisuji základní způsoby obrany proti němu a snažím se nastínit motivaci rozesílatelů spamu.

Druhá část je věnována statistikám spamu ve světě a v ČR.

Ve třetí části analyzuji právní normy, které upravují spam v ČR resp. EU. Informuji také o chystaných zákonech a o směru, kterým se rozhodla vydat Evropská unie v boji proti šíření spamu.

Tématem poslední části mé práce je realizace právních norem v ČR, postup od podání stížnosti po její šetření. Popisuji zákonem stanovené pravomoci a povinnosti odpovědného Úřadu. Uvádím i statistiky z činnosti Úřadu a příklady řešených případů.

3 Úvod

Asi nebudu daleko od pravdy, když řeknu, že každý pravidelný uživatel Internetu, který má zřízenu e-mailovou schránku se již setkal s nějakou formou spamu. Nejčastěji je nám v obsahu spamu nabízena nějaká služba či výrobek za cenu, která je nesrovnatelně nižší než kdekoli jinde na trhu. Proto spamming ve své podstatě představuje velmi nepříjemnou formu agresivního direct-marketingu. Přestože podle odhadů tvoří objem odeslaného spamu více než tři čtvrtiny celosvětové elektronické pošty, spamu navzdory snahám o jeho regulaci stále přibývá. Proto jsem se rozhodl popsat jakým způsobem nás stát chrání před spamem, a proč nás tato ochrana spamu dosud nezbavila.

Za účelem získání co možná nejrelevantnějších a nejaktuálnějších informací jsem se setkal s Mgr. Martinem Plíškem, ředitelem Odboru legislativně-právního Úseku pro vnější vztahy Ministerstva Informatiky ČR a s Ing. Milošem Šnytrem, inspektorem Úřadu pro ochranu osobních údajů. Informace od nich získané se staly stavebním kamenem bakalářské práce.

Cílem práce je zanalyzovat právní normy, které v ČR upravují problematiku nevyžádaných obchodních sdělení, a popsat realizaci těchto norem.

3.1 Historie spamu

Většina současných uživatelů v ČR se domnívá, že rozesílání spamu je mladá oblast, neboť ještě před pár lety na tento fenomén ve svých e-mailových schránkách nenarazili. Ovšem v ČR došlo k rozšíření počtu uživatelů Internetu a elektronické pošty se značným zpožděním oproti jiným státům v čele s USA. A právě USA, kde vznikl Internet, jsou také kolébkou spamu. Pro mnohé bude překvapením, že první nevyžádaný e-mail byl odeslán již v roce 1978 (tehdy ještě v síti ARPANET) jistým panem G. Thuerkem, který se tímto způsobem snažil sehnat práci. Nicméně známější případ spamu se datuje k roku 1988, kdy jistý student marylandské univerzity poslal do diskuzí řetězovou zprávu z kategorie „pyramidových her“. Předmět zprávy obsahoval slova „Make money fast“. Odsud také pochází označení pro podobné zprávy - MMF.

Ovšem o historicky první spam komerčního charakteru se „zasloužila“ až advokátní kancelář Cantor & Siegel působící v oblasti imigračního práva, která 12.4. 1994 rozeslala reklamu do veškerých v té době existujících internetových diskuzí (odhaduje se, že jejich počet se pohyboval mezi 6-7 tisíci). Předmětem tohoto spamu byla reklama lákající adresáty, aby se zapojili do loterie, jejíž vítěz získá zelenou kartu zajišťující jejímu držiteli trvalý pobyt v USA. „Jako "odměnu" za tento čin obdržel odesílatel 35 000 silně odmítavých reakcí, které zaplnily 73 GB diskového prostoru providera této advokátní kanceláře. Tento případ bývá uváděn jako jeden z prvních příkladů střetu kooperativního, značně liberálního a v zásadě nezištného způsobu fungování s mnohem drsnějším způsobem fungování komerčního světa, založeného na konkurenci a snaze prosadit se a zvítězit nad druhým. Skutečnost, že první byli právníci, byla velmi příznačná." (19)

Jak vznikl název spamu? Kupodivu se nejedná o zkratku nějakého všeříkajícího sousloví označujícího hromadné rozesílání nevyžádaných zpráv, nýbrž slovo spam označuje Spiced Pork And Ham, což je druh konzervovaného masa (v podstatě lančmít) amerického potravinového výrobce Hormel Foods. Pro pochopení souvislosti mezi lančmítem a otravným spamem však musíme opustit kolébku počítačového spamu a vydat se do Anglie. V roce 1970 zde anglická kultovní formace Monty Python natočila skeč v rámci své série Monty Python’s Flying Circus. Autor skeče, komik a člen této formace John Cleese nám v něm představuje manželský pár, který se vydal najíst do jednoho motorestu, ale číšník jim nabízí ke všem druhům jídla pouze spam, i když jej manželé nechtějí. Do českých titulků byl spam přeložen nepřesně jako prejt. Na závěr scénky Vikingové v přilbách s rohy začnou zpívat: „Spam, spam, spam. Lovely spam! Wonderful spam!“ Sám John Cleese kdysi jako host Mezinárodního filmového festivalu v Karlových Varech řekl: „Bylo to naprosto střelené, ale Britům se to moc líbilo. A protože lidé od počítačů mají Monty Python dost rádi, z nějakého důvodu tu nepříjemnou poštu nazvali spam. Takže to slovo rozšířili tihle počítačoví podivíni, kteří si ho vypůjčili z Pythonů. Jinak se však spam dá normálně koupit v samoobsluze, vůbec ho nemusíte shánět přes Internet.“(10)

3.2 Motivace spamerů

Většina zkušenějších uživatelů si při prohlížení doručené pošty nejprve zkontroluje adresu odesílatele a ihned jednoduše odhalí, že se jedná o spam a takový e-mail bez rozmýšlení

mažou, většinou dokonce aniž by jej otevřeli. Samozřejmě, pokud by podobným způsobem jednali veškeří uživatelé, spameři by rázem ztratili motivaci rozesílat nevyžádanou poštu a spam jako takový by pravděpodobně postupně nadobro zmizel z poštovních schránek, diskuzí či mobilních telefonů.

Skutečná situace je ovšem diametrálně odlišná, existuje stále velké procento nepoučitelných uživatelů, které předmět e-mailu zaujme a proto jej neváhají otevřít, následně navštíví propagované stránky či dokonce otevřou přiloženou přílohu, která velmi často obsahuje vir. A právě tato nezanedbatelná část uživatelů se stará o hlavní motivaci spamerů. Ostatní formy reklamy, jako třeba inzerát v tisku, reklamní letáky, televizní reklamní spoty, billboardy či bannery stojí firmy spoustu finančních prostředků. Spam je naproti tomu minimálně nákladný (paradoxně přivádí náklady adresátovi, který platí za stažení doručené pošty), stačí sehnat pouze potřebné adresy, což není velký problém. Velké množství programů prohledává 24 hodin denně nejrůznější stránky a diskuze a ukládá si e-mailové adresy v nich obsažené.

Vzhledem k tomu, že spameři pro odesílaní spamu využívají neplacené poštovní servery, nemusí oslovovat konkrétní skupinu uživatelů, kteří by mohli projevovat zájem o jejich často pochybné služby. Jednoduše rozešlou spam na všechny získané adresy a doufají, že se někdo chytí. Pokud ne, nevadí, náklady přece nese adresát a poštovní server! To vše je natolik motivující, že spamery od rozesílaní neodradí ani uzákoněná nelegálnost nevyžádaných obchodních sdělení.

3.3 Jak se bránit spamu?

3.3.1 Prevence

Na prvním místě je prevence. Může se to zdát jako ohraná písnička, ale v tomto případě to platí dvojnásob. V této souvislosti vznikl dokonce jakýsi edukativně-informační leták, který vzešel ze součinnosti holandského ministerstva pro informatiku a Organizace pro ekonomickou spolupráci a rozvoj (OECD). Jak jsem se již zmínil, spameři využívají speciálních programů, které doslova „sklízí“ (i v angličtině je zavedený pojem „address harvesting“) e-mailové adresy z webových stránek či diskuzí. Proto by se měl každý uživatel vyvarovat zbytečnému zveřejňování své adresy. Leták OECD dokonce doporučuje, aby si

každý uživatel, pokud tak ještě neučinil, zřídil současně několik různých elektronických adres. Svou hlavní adresu by pak měl předávat s rozmyslem a pouze partnerům, kterým důvěřuje, že ji nezneužijí.

Pokud svou elektronickou adresu uživatel někde zveřejňuje, doporučuje se využít nějakou z forem jejího maskování, která stěžuje slídícímu programu identifikaci naší adresy. „Takovéto maskování adres se označuje termínem "munging" - od anglické zkratky MUNG: "Mash Until No Good".“ (8) Nejčastější formou maskování je jednoduché nahrazení klíčového znaku „@” anglickým výrazem „at“ (za zmínku stojí, že na webových stránkách naší školy se přešlo na tento jednoduchý způsob maskování během letošního semestru). Znak „zavináče“ je totiž pro většinu slídících programů rozhodující pro identifikaci elektronické adresy.

Zřejmě nejúčinnější formou technické obrany je filtrování pošty pomocí některého z anti-spamových filtrů. Filtrování pošty je založeno na rozpoznání spamu při jeho přijetí. Spam lze rozpoznat dvěma základními způsoby. První spočívá v rozpoznání spamu na základě jeho obsahu, druhý na základě seznamu, do kterého odesílatel patří. Další osud e-mailu, který byl identifikován jako spam, závisí na vlastní konfiguraci filtru. Poštovní server může spam trvale smazat nebo pouze přesunout do vyhrazené složky, kde se pošta identifikovaná jako spam znovu překontroluje.

3.3.2 Rozpoznání spamu na základě obsahu

Existuje mnoho programů, které analyzují obsah přijaté pošty. Odhalují spam na základě existence konkrétních slov nebo celých frází v hlavičce i obsahu, ale i na základě formální chyby jakou může být například nesmyslné datum odeslání v budoucnosti nebo úplná absence hlavičky e-mailu. Podezřelými slovy mohou být například: „viagra“ nebo „stocks“. Pokud program narazí na některý ze zmíněných příznaků, bodově jej ohodnotí. Pokud je příznaků více, body se sčítají a narůstá tak jakési „skóre“ analyzovaného e-mailu, které se nakonec porovná s uživatelem nastavenou mezní hodnotou. Převýší-li „skóre“ mezní hodnotu, e-mail je označen jako spam.

Spameři jsou však vždy o krok napřed a vymýšlejí nejrůznější přepisy podezřelých slov, jako příklad uvádím slovo „stox“, jež je fonetickým přepisem podezřelého slova „stocks“ nebo slovo „st0ck“. Spameři zašli dokonce až tak daleko, že si platí lingvisty, kteří pro ně sestavují

takové texty, aby e-maily, které je obsahují, prošly anti-spamovými filtry. V poslední době spameři začali své nabídky zobrazovat v obrázcích, aby znemožnili analýzu obsahu přijaté pošty na základě obsažených slov.

Filtrační programy zareagovaly tím, že za spam začali považovat všechno, co neobsahovalo žádný text. Spameři opět nezůstali pozadu a za reklamní obrázek začali vkládat libovolný text náhodně posbíraný z webových stránek. I na tuto fintu dokázal filtrační software zareagovat a začal používat OCR (Optical Character Recognition – optické rozpoznávání znaků), což je „metoda, která pomocí scanneru umožňuje digitalizaci tištěných textů, s nimiž pak lze pracovat jako s normálním počítačovým textem.“ (27) Spameři proto začali využívat prvky, které jsou založené na deformaci textu v grafickém provedení, což znemožňuje využití metody OCR. Na předchozím sledu vzájemných „protiopatření“ jsem chtěl ukázat, že spameři jsou lidé opravdu zběhlí v oblasti informačních technologií a je pravděpodobné, že budou neustále o krůček napřed.

Jednou z nejúčinnějších metod využívanou dokonalejšími filtrovacími programy je „Bayesovo filtrování, které je založeno na učícím se algoritmu, který je schopen naučit se z předem rozdělených zpráv (spam, ne-spam) určité znaky (na základě statistiky), a ty pak aplikovat. Dokáže tak poměrně přesně rozdělit (klasifikovat) příchozí poštu na spam a normální komunikaci.“ (11) Ovšem účinnost Bayesova filtrování závisí na přesnosti uživatelem předaných vzorků, i proto se vyplatí pečlivě oddělovat nevyžádanou poštu od vyžadované.

Nejnovější programy obsahují dokonce i heuristické postupy, jejichž kombinace s předešlými technikami zaručuje již velmi vysokou šanci na odhalení spamu.

Většina filtrů umožňuje nastavení „citlivosti“, nejběžnější jsou tři stupně citlivosti: nízká, střední a vysoká citlivost. Uživatelem zvolená vysoká citlivost mu sice zaručuje, že do jeho schránky neprojde takřka žádná nevyžádaná pošta, ale zároveň filtr nemusí propustit ani poštu, která je naopak žádaná. Proto by se měl každý uživatel zamyslet nad tím, co je pro něj větší zlo. „Obecně se však dá říci, že spolehlivost takovýchto filtrovacích programů nemusí být vždy uspokojivá, u těch nejlepších se pohybuje kolem 60-70% (důležitý je přitom nejen co nejvyšší počet zachycených spamů, ale také co nejnižší počet falešných hlášení, kdy je jako spam označena pro uživatele důležitá relevantní zpráva).“ (19)

3.3.3 Rozpoznání spamu na základě databáze odesílatelů

Greylisting

V případě greylistingu poštovní server zjišťuje, zda příchozí pošta pochází z důvěryhodných či pochybných serverů. Pošta z důvěryhodných zdrojů je bez odkladu doručena, zatímco v opačném případě poštovní server poštu podle nastavení po určitou dobu nepřijímá (např. 1h). SMTP protokol je nastaven tak, že se pokouší podle konfigurace odmítnutou poštu několikrát znovu odeslat. Pokud po uplynutí nastavené doby pošta z neznámého serveru přesto znovu dojde, poštovní server příjemce poštu doručí do uživatelovi schránky. Tato metoda je účinná díky tomu, že spamery využívané skripty pro odesílání hromadné nevyžádané pošty jsou naprogramovány jako jednorázové, nebo-li spam je odeslán jednou, aby za sebou spameři mohli ihned zahladit stopy, které by mohly vyzradit původ odesílatele. Proto se uvádí, že servery využívající greylisting mají 95% úspěšnost. Nicméně i greylisting má svou nevýhodu, neboť občas dochází ke zpoždění doručení e-mailu z neznámých serverů a také jej lze pochopitelně obejít využitím vhodných odesílajících serverů.

Blacklisting

Blacklisting je jednoduchá metoda, při které správce serveru určí seznam poštovních serverů a domén, ze kterých nebude přijímat poštu. Mezi známé blacklisty patří například MAPS (Mail Abuse Prevention System - hned několik databází členěných podle druhu spamu) nebo ORDB (Open Relay DataBase – databáze „open relay“ serverů). Výhodou a zároveň nevýhodou blacklistů je právě jejich jednoduchost, díky které jsou nenáročné na provoz, ale na druhou stranu jsou také nepříliš účinné. Navíc tu existuje možnost, že se do blacklistu dostane poštovní server či doména, která tam být nemá.

Whitelisting

Je pravým opakem blacklistingu. Jedná se tedy o databázi poštovních serverů a domén, od nichž příjemcův poštovní server e-mail vždy přijme, i kdyby po obsahové stránce splňoval veškeré charakteristiky spamu. Výhody a nevýhody jsou analogické s blacklistingem.

3.3.4 Stížnosti

Výše zmíněné obranné postupy jsou sice do jisté míry účinné, avšak spamu nás nadobro rozhodně nezbaví (alespoň prozatím ne), pouze sníží počet přijatých spamů a zmírní tak částečně naše problémy vzniklé v souvislosti s „nezničitelným“ spamem jako takovým. Jak tedy naložit s podezřelou poštou, která přesto projde do naší schránky? Předně, již z hlavičky e-mailu lze často rozpoznat, že se jedná o spam. Takový e-mail by uživatel neměl vůbec otevírat a okamžitě jej smazat.

Na spam se rozhodně nevyplatí odpovídat. Rozhořčené odpovědi adresátů spamera pouze utvrdí, že vaše adresa je funkční. Je třeba si uvědomit, že spameři nabízející pochybné výrobky v naprosté většině lžou. Spamer se snaží působit na adresáta ohleduplným dojmem a proto připojuje do obsahu pošty výzvy pro odstranění adresátovy adresy z jeho databáze, pokud adresát nemá zájem o jeho nabídky. Nicméně to logicky nedává smysl, neboť tak žádá o odstranění z databáze, do které se adresát s největší pravděpodobností nikdy dobrovolně nepřihlásil. Proto na výzvy o zaslání e-mailu s předmětem „remove“ či klinutí na odkaz „unsubscribe“ zásadně nereagovat! Podobnou žádostí o odstranění z databáze uživatel v lepším případě ničeho nedocílí, v tom horším případě odesílateli pouze potvrdí, že jeho poštovní schránka je aktivní.

Nicméně z výzkumu společností Mirapoint a Radicati Group je patrné, že osvěta v této oblasti je stále nedostatečná. Přes 18 procent uživatelů se totiž stále naivně snaží zamezit přílivu spamu do svých schránek klikáním na zmíněné odhlašovací odkazy „unsubscribe“ či „remove“. (5)

Další možností, jak naložit se spamem, který se dostal do naší schránky je stížnost providerovi poštovní schránky a především stížnost Úřadu pro ochranu osobních údajů. Stížnost providerovi poštovní schránky je sice možná, ale provider nemá ze zákona povinnost stížnost prošetřovat, proto tato možnost existuje spíše v teoretické rovině a záleží čistě na samotném providerovi, zda uskuteční nějaké kroky proti odesílateli nevyžádané pošty, na kterého si adresát stěžuje. V případě druhé varianty má adresát jistotu, že se ÚOOÚ bude stížností zabývat, neboť je to jeho povinnost vyplývající ze zákona „o některých službách informační společnosti“. Adresát může stížnost úřadu podat písemnou, telefonickou či elektronickou formou, nebo může na Úřad přijít osobně. Podrobněji podávání stížností na ÚOOÚ popisuji v kapitole realizace zákonů.

3.4 Druhy spamu

3.4.1 E-mailový spam

Z názvu je zřejmé, že se jedná o nejrozšířenější druh spamu rozesílaného prostřednictvím elektronické pošty, se kterým se asi každý uživatel e-mailové schránky již nedobrovolně seznámil. O tom, že spamer sklízí adresy z internetových diskuzí, webových stránek či elektronických konferencí díky speciálně naprogramovaným programům (robotům), již byla řeč. V poslední době spameři přišli na svět s novou účinnou metodou „generování nahodilých potenciálních elektronických adres“. Účinnost této metody mohla být prakticky využita až v současnosti, kdy provideři evidují stále narůstající počet uživatelů e-mailových schránek. Adresy jsou generovány nahodilou kombinací znaků resp. slov a doménových jmen.

3.4.2 Komentářový spam (někdy také usenet-spam či diskuzní spam)

Velmi populární jsou v současné době diskuze umístěné na konci článků v elektronických časopisech či různých blozích. Čtenáři daného článku mají jedinečnou možnost přidat svůj názor k danému tématu, popřípadě jej konfrontovat s názory ostatních uživatelů. Díky jednoduchosti vložení příspěvku se tyto diskuze staly vděčným terčem spamerů resp. jejich robotů. „Praktické zkušenosti ukazují, že každá zpráva zaslána již do více než 20 skupin je pro většinu uživatelů nerelevantní, a získává tak - bez ohledu na obsah - charakter spamu.“ (19)

3.5 Co je na spamu tak špatného?

Pominu-li fakt, že je vzhledem k jeho nevyžádanosti a množství nesporně otravný, hlavní důvod, proč je spam tolik zatracován, jsou peníze. Zatímco spameři našli ve spamu zalíbení díky minimálním nákladům na straně odesílatele, takřka celé náklady nese adresát spolu s poštovními servery, jejichž jsou adresáti zákazníky, a firmami. Je smutné, že se za produkt, o který nemá nikdo zájem, platí milióny.

Jaké jsou tedy náklady adresáta spamu? Nezasvěcený jedinec by mohl namítnout, že spam ho stojí pouze čas, potřebný pro smazání nevyžádané pošty z jeho poštovní schránky, ale ne nadarmo se říká: „Time is money.“ Navíc je třeba si uvědomit, že ve většině případů uživatel za čas strávený na Internetu platí. Další peníze je třeba vynaložit za anti-spamové filtry, ale také za anti-virové programy, neboť spamy jsou velmi často nositeli nejrůznějších virů a červů. Navíc v případě, že vir resp. červ vykoná poslání, za jehož účelem byl naprogramován, uživatel platí daleko větší částky, pokud tedy jde vůbec o penězi vyčíslitelnou ztrátu. Spameři si navíc v poslední době usnadňují práci šířením škodlivého kódu, po jehož spuštění útočník převezme kontrolu nad nakaženým systémem nic netušícího uživatele a učiní z něj tzv. botnet („Botnetem se rozumí napadený počítač, který spamer využívá k rozesílání hromadných e-mailů pomocí instalace skrytého softwaru, který bez vědomí majitelů z počítače učiní e-mailový server.“(27)). Zatímco pro spamery je tato metoda z pochopitelných důvodů velice výhodná, nic netušící oběti přichází o šířku přenosového pásma, výkon PC a tím samozřejmě i o peníze. Navíc uživatel se, aniž by o tom měl tušení, spolupodílí na trestné činnosti, neboť botnety využívají nejen spameři, ale i tzv. phisheři či šiřitelé spywaru. Spam může být také prostředníkem některé z nebezpečných forem phishingu („podvodná technika používaná na Internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.)“ (6)).

Ohromné částky stojí spam podniky, které jsou za ochranu před ním ochotny mnohdy utrácet víc než za anti-virové programy. Se zajímavou studií přišla nezávislá společnost Nucleus Research, která vyčíslila průměrnou ztrátu firmy bez anti-spamového filtru na jeden doručený nevyžádaný e-mail na 10 Kč. Do této částky jsou započítány technické náklady (paměť, Internet), ale i čas zaměstnance, kterému spam přijde do osobní poštovní schránky. Společnost Nucleus Research odhaduje, že větší firma, která dosud nevyužívá některý z anti-spamových filtrů, přijde „díky“ spamu ročně o padesát tisíc korun na zaměstnance. (13)

Je tedy zřejmé, že investice do anti-spamových filtrů se v budoucnu žádná větší firma ve vlastním zájmu nevyhne.

Další, kdo tratí na spamu, jsou provideři freemailových služeb. Pod nátlakem ohromného množství spamu jsou nuceni neustále zvyšovat kapacitu poštovních schránek (1-2GB je dnes naprosto běžná kapacita poštovní schránky), i když tvrdí, že to dělají pro vyšší komfort uživatele, pravda je, že za tím nestojí nikdo jiný než všudypřítomný spam. Navíc provozují vlastní anti-spamové filtry a řeší stížnosti uživatelů týkající se nevyžádané pošty.

V neposlední řadě na spamu tratí i stát, který financuje provoz institucí, které se touto problematikou zabývají.

Podle střízlivých odhadů dosáhly celosvětové náklady vzniklé v důsledku spamu 39 miliard EUR. Následující tabulka uvádí náklady předních členských států EU za rok 2005, jak je odhaduje společnost Ferris na základě svého výzkumu.

Ferris (2005), v miliardách EUR		
1	Německo	3,5
2	VB	1,9
3	Francie	1,4

(27)

4 Statistiky, situace na poli nevyžádané reklamy v ČR a v zahraničí

Přes veškerou snahu providerů, firem vyvíjejících anti-spamové filtry, tvůrců zákonů i snahu o osvětu uživatelů - spamu neustále přibývá. Za posledních 5 let došlo k výraznému nárůstu spamu. Zatímco v roce 2001 pouhých 7 procent celosvětové pošty tvořilo spam, v roce 2003 se spam podílel již 50 procenty na všech odeslaných e-mailech, v roce 2004 to bylo už 60 procent, desetiprocentní nárůst pokračoval i následující rok, kdy objem spamu dosáhl sedmdesáti procent. S blížícím se koncem roku 2006 je již zřejmé, že podíl spamu přesáhne tři čtvrtiny celosvětové pošty. (28)

Sophos reveals 'dirty dozen' spam relaying countries

2004			2005			leden - říjen 2006		
1	USA	42,1%	1	USA	26,8%	1	USA	22,6%
2	Jižní Korea	13,4%	2	Jižní Korea	18,4%	2	Čína	18,4%
3	Čína	8,4%	3	Čína	17,4%	3	Jižní Korea	7,9%
4	Kanada	5,7%	4	Francie	3,9%	4	Francie	5,3%
5	Brazílie	3,3%	5	Kanada	2,7%	5	Španělsko	4,6%
6	Japonsko	2,6%	6	Brazílie	2,4%	6	Polsko	4,1%
7	Francie	1,4%	7	Španělsko	2,3%	7	Brazílie	3,6%
8	Španělsko	1,2%	8	Japonsko	2,0%	8	Německo	2,8%
9	VB	1,1%	9	VB	1,5%	9	Itálie	2,4%
10	Německo	1,0%	10	Německo	1,3%	10	Taiwan	1,8%
11	Taiwan	1,0%	11	Polsko	1,2%	11	Japonsko	1,8%
12	Mexiko	0,9%	12	Rakousko	0,9%	12	VB	1,8%
	ostatní	17,8%		ostatní	19,5%		ostatní	22,9%

(28)

To, že USA jsou největším producentem spamu je známá věc, v roce 2004 se na celkové produkci spamu podílely 42%. Se značným odstupem je následuje Jižní Korea se 13,4%, která tak potvrzuje pověst země s největším množstvím širokopásmových přípojek na osobu. Trochu překvapivě se až za Jižní Koreou umístila Čína s 8,4%. Kromě těchto statistik přišla

společnost Sophos spolu s žebříčkem za rok 2004 i s tvrzením, že se ukazuje malá účinnost anti-spamového zákona přijatého v USA v roce 2003.

Následující rok byl ve znamení oslabování pozice USA (26,8%) ve prospěch Jižní Korey (18,4%), ale především Číny (17,4%).

Podobný trend je patrný i v prvních třech čtvrtinách roku 2006. Čína (18,4%) se dotahuje na USA (22,6%) a pokud bude podobný trend pokračovat, lze očekávat že v polovině roku 2007 by z Číny mohlo pocházet největší množství spamu. Naopak Jižní Korea (7,9%) znatelně ztrácí ve prospěch převážně evropských internetových mocností, jakými jsou Francie (5,3%), Španělsko (4,6%)a trochu překvapivě Polsko (4,1%).

Q 1 2006 (Sophos)		
1	Asie	42,8%
2	Severní Amerika	25,6%
3	Evropa	25,0%
4	Jižní Amerika	5,1%
5	Australasie	0,8%
6	Afrika	0,6%
7	ostatní	0,1%

(28)

Předchozí tabulka zobrazuje největší producenty spamu podle kontinentů. Jak vidno, spameři z Evropy odesílají stejně nevyžádané pošty jako spameři ze Severní Ameriky. Naproti tomu Asie je neotřesitelně v čele tohoto nelichotivého žebříčku.

Spam je stejně jako jiné marketingové nástroje ovlivněn sezónností, a proto není překvapením, že v předvánočním období se naše poštovní schránky plní nevyžádanou poštou více než kdy jindy. Zatímco v říjnu letošního roku spameři odesílali denně průměrně 63 miliard nevyžádaných sdělení, v prosinci by se na základě odhadů společnosti Iron Port Systems měl denní objem rozeslaného spamu vyšplhat na závratných 78 miliard. Zajímavé je také srovnání s loňským rokem, kdy v říjnu to bylo „pouhých“ 31 miliard a v prosinci 38. (7)

Spamu zkrátka neubývá, naopak studie firmy Barracuda Networks informuje, že jen od září letošního roku objem spamu vzrostl o 67 procent. Ze studie vyplývá, že největší podíl na dynamickém růstu nevyžádané reklamy má „akciový spam“ (více v následující podkapitole) a

také stále častější metoda spamerů, která spočívá v šíření spamu přes botnety (viz předchozí text). Společnost Sophos udává, že v roce 2004 tyto botnety produkovaly dvě pětiny celkového spamu. Podle společnosti Symantec se v roce 2005 botnety postarali již o polovinu celkového objemu rozeslaného spamu, přičemž denně bylo botnetem infikováno v průměru 9 163 počítačů. (28)

Následující tabulka uvádí žebříček rozložení případů napadení botnety podle zemí. 26% z celkového počtu napadených počítačů botnetem pochází z USA, avšak daleko překvapivější je, že na druhém místě se umístila Velká Británie s 22%.

Napadení botnety Q 3-4 2006 (Symantec)		
1.	USA	26%
2.	VB	22%
3.	Čína	9%
4.-6.	Francie	4%
4.-6.	Jižní Korea	4%
4.-6.	Kanada	4%
7.-9.	Taiwan	3%
7.-9.	Španělsko	3%
7.-9.	Německo	3%
10.	Japonsko	2%

(28)

4.1.1 Situace v ČR

Situace v ČR se začíná již velmi přibližovat celosvětovým statistikám. Zatímco v minulých letech jsme za celosvětovým průměrem ještě znatelně „zaostávali“, letos by měl podíl nevyžádané reklamy v českých poštovních schránkách dosáhnout již srovnatelných sedmdesáti procent.

Asi každý příjemce spamu si musel všimnout, že takřka všechny spamy jsou psány v angličtině. Vysvětlení je prosté: spam je jednoznačně zaměřen na severoamerický trh. To je také důvodem proč spameři z afrických a hlavně asijských zemí odesílají poštu v angličtině. Jak jsem se již zmínil, největším světovým producentem spamu jsou USA, proto většina

anglicky psaného spamu přichází do schránek českých uživatelů v nočních hodinách, protože v USA je tou dobou pracovní doba a tedy i čas, kdy si většina uživatelů čte doručenou poštu.

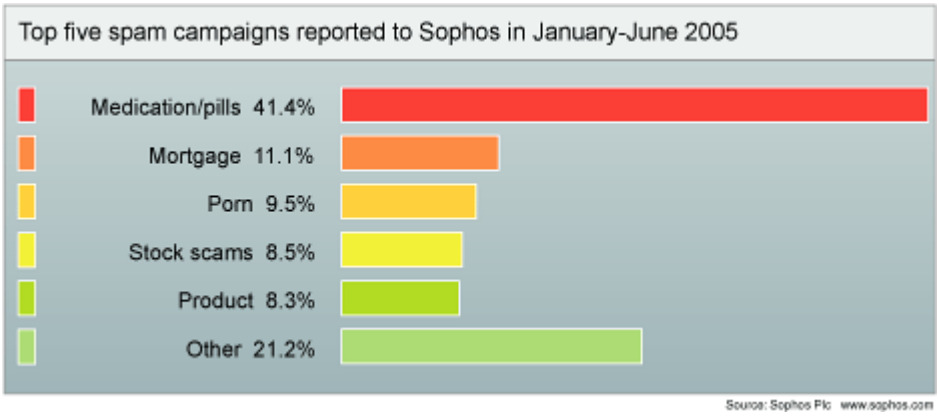
O postavení USA – největšího exportéra spamu – svědčí i žebříček Top Level Domén, ze kterých nevyžádaná pošta přichází do českých poštovních schránek.

TLD		
1.	**.com**	55,0%
2.	**.net**	17,6%
3.	**.info**	2,9%
4.	**.cz**	1,3%

(14)

Postavení domény .com je dáno i největšími světovými poštovními servery jakými jsou Yahoo, Hotmail a Google.

4.2 Předmět spamu



(28)

Tento graf nám v přehledném procentuálním vyjádření ukazuje, co spameři nejčastěji nabízeli ve svých nevyžádaných e-mailech v první polovině roku 2005. Jeho autorem je firma Sophos. Pilulky na zvýšení potence jako Viagra a další medikamenty (např. „zaručeně“ zvětšující mužské přirození) tvoří stále největší podíl (přes 40% světového spamu). Hned na druhé pozici za nabídkou medikamentů se umístily nabídky nejrůznějších levných úvěrů a hypoték s podílem přes 10%. Třetí pozici s podílem blížícím se desetiprocentní hranici těsně uhájila

nevyžádaná pornografie před nastupujícím fenoménem – takzvaným „akciovým spamem“. Tento spam je sice „až“ na čtvrté pozici, nicméně jeho nárůst v první polovině byl vskutku enormní, neboť dle společnosti Sophos rostl měsíčně v průměru o 10 procent.

„Akciový spam podle analytika Sophosu Gregga Mastorrase představuje novou finanční hrozbu pro naivní on-line investory. Nevyžádané zprávy v tomto případě obsahují o akciích některé firmy falešné informace, které mají přimět potenciální investory k jejich nákupu. Jakmile podvodníci své podíly prodají a přestanou akcie propagovat, jejich cena klesne a investoři přijdou o peníze.“ (28)

O důvodech rozesílání obrázkového spamu jsem se již zmiňoval, není tedy až takovým překvapením, že nyní tvoří již většinu spamu doručeného do poštovních schránek. Uvádí se dokonce, že jen za poslední čtvrtletí objem obrázkového spamu narostl pětinásobně.

4.2.1 A jaká je situace v tuzemsku?

Zástupci českých portálů na základě svých statistik tvrdí, že nevyžádaná reklamní sdělení, která přicházejí do schránek českých uživatelů, nabízejí nejčastěji přípravky na zlepšení sexuální potence. Podle analytiků pracujících pro portál Atlas.cz tvoří tento druh reklamy patnáctiprocentní podíl z celkového objemu spamu. Na druhém místě se již delší dobu udržují nabídky inzerující internetový prodej „značkového“ softwaru. Nejčastěji se jedná o produkty firem Microsoft a Adobe. Přestože ceny těchto produktů se pohybují běžně v řádech tisíců korun, pochybní inzerenti je nabízí za několikanásobně nižší ceny. Podezření, že se jedná o pirátské kopie, je proto zcela na místě. Následují nejrůznější anti-depresiva, prášky na spaní, léky pro utlumení bolesti či dokonce pro zlepšení nálady. Z výčtu je patrné, že se jedná o léky, které jsou běžně k dostání jen na lékařský předpis. V minulých letech tolik „oblíbené“ nelegální nabídky léků jsou však nyní na ústupu. Lze očekávat, že z pozice třetího nejrozšířenějšího spamu v ČR budou brzy vytlačeny ve světě již dnes hojně rozšířeným „akciovým spamem“. Již nyní se v našich poštovních schránkách začínají objevovat nabídky, jak snadno a rychle zbohatnout díky „výhodným“ investicím. (3)

5 Právní úprava spamu v ČR

První pokus o právní ošetření problematiky spamu v ČR se uskutečnil v roce 1997, kdy byl u nás již dva roky v provozu komerční Internet. Nicméně tehdejší snaha skončila nezdarem kvůli problematickému vymezení oblasti spamu. Ostatně spam tehdy rozhodně nebyl palčivým problémem vyžadujícím neprodlené právní vymezení. Na počátku 21. století však šíření spamu dostalo nečekané rozměry, a tak se hledalo řešení, jak tento fenomén právně ošetřit. V roce 2002 vzniklo z dnešního pohledu jakési dočasné řešení, červnu nabyl účinnosti zákon č. 138/2002 Sb., který kromě jiného novelizuje zákon „o regulaci reklamy“ (zákon č. 40/1995 Sb.). Novelizace obsahovala rozšíření zákona „o regulaci reklamy“ o pasáž:

§ 2, odst. 1, písm. e):

Zakazuje se .... šíření nevyžádané reklamy, pokud vede k výdajům adresáta nebo pokud adresáta obtěžuje, ...

Podle této pasáže měli činovníci odpovědných úřadů řešit akutní případy, přičemž daný úřad (příslušný živnostenský úřad) mohl sáhnout po udělení pokuty do výše dvou miliónů korun. Avšak je zřejmé, že tato kratičká pasáž byla naprosto nedostatečná, aby mohla právně postihnout tak problematickou a citlivou oblast, jakou rozesílání nevyžádané reklamy bezesporu je. Například není zřejmé, co se myslelo obtěžováním adresáta, přece každého obtěžuje něco jiného. Stejně tak výdaje adresáta jsou dost záhadnou formulací, neboť to se vztahuje nejspíš na všechny formy reklamy na Internetu, vzhledem k tomu, že uživatel Internetu platí za stahování každé reklamy i za vlastní připojení. Jediné, co je vcelku srozumitelné je termín „nevyžádaná“, neboť tím se vylučuje aplikace ustanovení § 2 písm. e) na reklamu, která je šířena prostřednictvím WWW stránek. „Přestože i reklamní bannery mohou být obtěžující a jejich doručení nepochybně zvyšuje náklady, je třeba připomenout, že § 2 odst. 1 písm. e) se vztahuje toliko na nevyžádanou reklamu, kdežto reklama prostřednictvím protokolu HTTP je doručována výhradně na vyžádání (request).“(15)

5.1 Zákon č. 480/2004 Sb. „o některých službách informační společnosti“

Přes nepopiratelné zlepšení situace odborná veřejnost netrpělivě vyhlížela opravdu plnohodnotné právní řešení problematiky nevyžádaných reklamních sdělení. Takové právní řešení měl přinést zákon č. 480/2004 Sb. „o některých službách informační společnosti“, který nabyl účinnosti 7.9.2004. Zákon, který je považován za jeden z nejkratších v české legislativě (plné znění zákona je součástí přílohy), se týká řady oblastí, jako například odpovědnosti providera za obsah ukládaných a přenášených dat. Kupodivu menší prostor je věnován problematice šíření nevyžádaných obchodních sdělení, ale i tak nastalo zlepšení oproti těm několika slovům, které tuto problematiku dosud „řešily“ v rámci zákona „o regulaci reklamy“. O tom, že je část zákona, která se zabývá problematikou spamu, ostře sledována zasvěcenou veřejností, svědčí i poněkud nepřesná „přezdívka“, kterou si zákon ihned vysloužil – antispamový zákon.

Autorem zákona je Ministerstvo Informatiky ČR. Zákon, který pomáhal vytvořit ještě někdejší ministr informatiky Vladimír Mlynář, vychází ze dvou následujících směrnic EU:

- Směrnice Evropského Parlamentu a Rady 2000/31/ES ze dne 8. června 2000 „o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu“ (Směrnice o elektronickém obchodu, 2000/31/EC).

- Směrnice Evropského Parlamentu a Rady 2002/58/ES ze dne 12. července 2002 „o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací“ (Směrnice o soukromí a elektronických komunikacích, 2002/58/EC).

Ještě než začnu rozebírat samotný zákon, je třeba zmínit, že české právo může postihovat pouze subjekty sídlící v ČR, proto se i tento zákon vztahuje pouze na organizace a společnosti, které působí na území České republiky. A to je podstatné, vzhledem k faktu, že většina nevyžádaných sdělení přichází ze zahraničí.

5.1.1 Pro účely tohoto zákona se rozumí - § 2

f) obchodním sdělením všechny formy sdělení určeného k přímé či nepřímé podpoře zboží či služeb nebo image podniku fyzické či právnické osoby, která vykonává regulovanou činnost nebo je podnikatelem vykonávajícím činnost, která není regulovanou činností; za obchodní sdělení se považuje také reklama podle zvláštního právního předpisu.

První věta paragrafu 2 odst. f) nám jednoznačně definuje, že zákon se vztahuje pouze na sdělení obchodního charakteru. Znamená to, že ostatní formy spamu, jakými jsou nejrůznější politické a náboženské propagandy, jsou proti vůli většiny uživatelů z právního hlediska „vyžádané“. Samozřejmě spam obsahující obchodní sdělení jednoznačně dominuje v našich poštovních schránkách, ale je možné, že zákon v tomto znění může působit jako pobídka pro tyto nekomerční instituce, aby zaplavili naše poštovní schránky spamem neobchodního charakteru. Za nevyžádané obchodní sdělení se považuje také reklama podle zákona „o regulaci reklamy“ (zákon č. 40/1995 Sb.).

Za obchodní sdělení se nepovažují údaje umožňující přímý přístup k informacím o činnosti fyzické či právnické osoby nebo podniku, zejména doménové jméno nebo adresa elektronické pošty; za obchodní sdělení se dále nepovažují údaje týkající se zboží, služeb nebo image fyzické či právnické osoby nebo podniku, získané uživatelem nezávisle, …

První věta předchozího odstavce, která upřesňuje právní pojem obchodního sdělení, vyvolala ihned po zveřejnění zákona vlnu rozporuplných reakcí. Nezřídka se mezi odbornou veřejností (v čele s ÚOOÚ) objevovaly dokonce výrazy jako „díra v zákoně“ apod. Stanovení, že "za obchodní sdělení se nepovažují údaje umožňující přímý přístup k informacím o činnosti fyzické či právnické osoby nebo podniku, zejména doménové jméno nebo adresa elektronické pošty", mělo umožnit firmám informovat zákazníky o změně sídla nebo jiných údajů (adresa, telefonní číslo, e-mail, webová adresa). Ale MI ČR si při tvorbě zákona neuvědomilo, že to lze využít pro „elegantní“ obejití zákona. Podle zákona totiž následující doménové jméno není obchodním sdělením (podobně lze zapsat i elektronickou adresu):

http://www.nejlevnejsi_lyze_v_praze_jiz_od_500kc_prijdte_se_podivat.cz/stepanska_1234_praha_1_tesime_se_na_vasi_navstevu

Co se týče problematiky tzv. prokliku, MI ČR zastává názor, že bez něj by firmy jen těžko mohly klientům sdělit své údaje. Pokud by doménové jméno, popřípadě URL byly skutečně považovány za spam, jednalo by se dle názoru MI ČR o jasné omezování podnikání. Zkrátka vždy bude existovat určitý rozpor mezi podnikateli a adresáty (pokaždé si bude alespoň jedna strana, ale většinou obě stěžovat), a je třeba na základě kompromisu nastavit vhodný „poměr“. Co se týče výše zmíněné „díry v zákonu“, několikařádkové doménové jméno obsahující nabídku zboží včetně ceny představuje podle MI ČR jednoznačné obcházení zákona, neboť

doménové jméno v tomto případě obsahuje prokazatelně daleko více informací než je třeba. (1)

Naproti tomu ÚOOÚ to považuje za jednoznačnou chybu v legislativě (již nyní řeší první případ tohoto druhu (viz. kapitola realizace zákonů)) a chystá se podat návrh na změnu při nejbližší možné příležitosti (2).

5.1.2 Šíření obchodních sdělení - § 7

(1) Obchodní sdělení lze šířit elektronickými prostředky jen za podmínek stanovených tímto zákonem.

(2) Podrobnosti elektronického kontaktu lze za účelem šíření obchodních sdělení elektronickými prostředky využít pouze ve vztahu k uživatelům, kteří k tomu dali předchozí souhlas.

(3) Nehledě na odstavec 2, pokud fyzická nebo právnická osoba získá od svého zákazníka podrobnosti jeho elektronického kontaktu pro elektronickou poštu v souvislosti s prodejem výrobku nebo služby podle požadavků ochrany osobních údajů upravených zvláštním právním předpisem, může tato fyzická či právnická osoba využít tyto podrobnosti elektronického kontaktu pro potřeby šíření obchodních sdělení týkajících se jejích vlastních obdobných výrobků nebo služeb za předpokladu, že zákazník má jasnou a zřetelnou možnost jednoduchým způsobem, zdarma nebo na účet této fyzické nebo právnické osoby odmítnout souhlas s takovýmto využitím svého elektronického kontaktu i při zasílání každé jednotlivé zprávy, pokud původně toto využití neodmítl.

(4) Zaslání elektronické pošty za účelem šíření obchodního sdělení je zakázáno, pokud

a) tato není zřetelně a jasně označena jako obchodní sdělení,

b) skrývá nebo utajuje totožnost odesílatele, jehož jménem se komunikace uskutečňuje, nebo

c) je zaslána bez platné adresy, na kterou by mohl adresát přímo a účinně zaslat informaci o tom, že si nepřeje, aby mu byly obchodní informace odesílatelem nadále zasílány.

Elektronické prostředky jsou podle tohoto zákona především síť elektronických komunikací, elektronická komunikační zařízení, koncová telekomunikační zařízení a elektronická pošta. To znamená, že obchodní sdělení lze podle prvního odstavce paragrafu 7 zasílat elektronickou poštou, faxem, prostřednictvím SMS zprávy nebo i po telefonu (tzv. telemarkenting).

Druhý odstavec zavádí obecnou aplikaci principu OPT-IN, který je založen na tom, že potenciální adresát musí dát nejdřív souhlas se zasíláním obchodních sdělení a až poté mu takové zprávy mohou být zaslány. Následující odstavec v určitých situacích povoluje benevolentnější princip OPT-OUT. Ten umožňuje rozesílání obchodních sdělení bez nutnosti předchozího svolení, přičemž uživatel má po obdržení takové zprávy právo svým nesouhlasem zastavit příjem těchto sdělení. Princip OPT-OUT je praktikován pouze v situaci, kdy potenciální adresát již je zákazníkem dané fyzické či právnické osoby, v tom případě tato fyzická či právnická osoba již nemusí mít adresátův souhlas pro další zasílání svých komerčních sdělení.

V této podobě kombinace OPT-IN a OPT-OUT přístupu kopíruje směrnice EU. Princip OPT-OUT byl však do zákona zabudován až 1.8.2006, kdy „vyšla“ v účinnost novela zákona č. 455/1991 Sb., která jako „vsuvku“ obsahovala i zmíněnou úpravu „antispamového zákona“. Kromě popsané změny ještě uzákonila, že problematickou oblast šíření obchodních sdělení elektronickou cestou upravuje výhradně zákon č. 480/2004 Sb.

Původní zákon, který nabyl účinnosti 7.9.2004 aplikoval pro veškeré případy pouze princip OPT-IN. Zákonodárci se před dvěma lety rozhodli pro přísnější postup v této oblasti, než jaký byl navrhován ve směrnicích EU. Přísnější pojetí se ovšem Evropské unii znelíbilo natolik, že přinutila Českou republiku upravit stávající zákon o zmíněný princip OPT-OUT v případě, že se již jedná o zákazníka nějaké firmy. Změnu ovšem na základě zkušeností z praxe uvítal i ÚOOÚ.

Nicméně Evropskou unií vynucená novela zákona č. 480/2004 Sb. jednoznačně zvýhodňuje firmy na úkor zákazníků. Firmy nyní mohou každému svému zákazníkovi, který se prokázal elektronickou adresou, zasílat množství obchodních nabídek. Navíc ve většině případů on-line obchodů je elektronická adresa zákazníka vyžadována. Samozřejmě, že zákazník má ze zákona právo odmítnout tato obchodní sdělení, ale oproti dřívějšku nyní musí sám jednat, pokud tato sdělení již nechce přijímat.

Princip OPT-IN se vztahuje podle vyjádření MI ČR i na firemní adresy typu info@blabla.cz, tedy v případě, že se nejedná o zákazníka firmy. „Zákon chrání shodně emailové schránky určené právnické osobě jako emailové schránky fyzických osob. Ani na firemní adresy nelze bez předchozího souhlasu obchodní sdělení posílat.“ (42)

Já osobně bych v tomto případě rozhodnutí ponechal na konkrétním šetření ÚOOÚ. Firemní elektronické adresy jsou přece jen určené pro příjem obchodních nabídek, na druhou stranu, každá firma si může na své webové stránky vložit explicitní souhlas se zasíláním obchodních nabídek na konkrétní adresu.

Jakým způsobem uživatel udělí prokazatelný souhlas se zasíláním obchodních sdělení?

Ze znění zákona vyplývá, že firma elektronickou poštou v podstatě nemá možnost oslovit potenciálního zákazníka (tedy jedince, který ještě zákazníkem firmy není) a požádat jej o souhlas se zasíláním obchodních sdělení. Osoba, od které by firma souhlas chtěla získat, musí být plně informována, aby mohla udělit prokazatelný souhlas. Jelikož plná informovanost jednoznačně zahrnuje předmět podnikání firmy a nabídek, které by následná obchodní sdělení obsahovala, musela by už prvotní žádost o souhlas potenciálního zákazníka obsahovat předmět podnikání a předmět nabídek firmy, čímž by se ovšem taková žádost stala sama o sobě obchodním sdělením a narazila by na uzákoněný princip OPT-IN. (2)

Jak tedy získat prokazatelný souhlas legální cestou? Firmy asi nejčastěji využívají registraci na svých webových stránkách. Součástí formulářů, které uživatel při registraci vyplňuje bývá většinou políčko, po jehož aktivním vyplnění uživatel souhlasí se zasíláním obchodních sdělení dané firmy. Důležité je ustanovení směrnice EU (konkrétně směrnice 2002/58/ES), které říká, že zmíněné políčko nesmí být „předvyplněno“. Uživatelé totiž mnohdy smluvní podmínky obsažené v registraci kvůli přílišné délce nečtou, a tak přehlídnou podobné políčko, které bývá „skryté“ někde na konci či uprostřed nepřehledného textu. Pro tyto případy bylo uzákoněno, že výchozí situace znamená „nesouhlas“ s rozesíláním dalších obchodních nabídek dané firmy. Podle interpretace ÚOOÚ pro potvrzení předběžného souhlasu se zasíláním obchodních sdělení v rámci registrace „je postačujícím potvrzením informační e-mail, generovaný na základě registrace, a případně včetně jeho akceptace.“ (2) Tato interpretace se však stala okamžitě velmi rozebíraným tématem v rámci internetových diskuzí. Zajímavá je teorie, podle které tak může nastat situace, kdy někdo při registraci uvede elektronickou adresu někoho jiného, navíc automaticky generovaný e-mail potvrzující

adresátovu registraci by mohl uvíznout v anti-spamovém filtru a dotyčnému by pak mohla začít chodit obchodní sdělení, která si nevyžádal. Z hlediska ochrany soukromí zákazníků se tedy jeví jako bezpečnější varianta, která požaduje zákazníkovu potvrzující odpověď.

Nicméně podle MI ČR je potvrzující odpověď adresáta na automaticky generovaný e-mail potvrzující adresátovu registraci obtěžující a nehodlá tak toto uzákonit podobně, jako tomu je například v sousedním v Německu. Závisí tedy jen a jen na firmě, nicméně registrace je podle MI ČR dostatečně výmluvným souhlasem. (1)

Z pohledu druhé strany, uživatel, který má zájem o příjem obchodních sdělení, má situaci značně ulehčenou. Není problém, zaslat dané firmě e-mail, ve kterém explicitně žádá o zasílání nabídek jejich produktů. Stejně tak objednávka či poptávka se považuje za souhlas a nejen odpověď na takovou objednávku či poptávku není z pochopitelných důvodů nevyžádaná, ale i následující nabídky ze strany firmy jsou již v souladu se zákonem, neboť uživatel je již zákazníkem. Uživatelé, kteří mají zájem o libovolné obchodní sdělení, mohou řešit udělení takového obecného souhlasu zveřejněním svého souhlasu na webových stránkách.

Specifikace požadavků na obsah obchodního sdělení

Poslední odstavec paragrafu 7 specifikuje požadavky, které musí obchodní sdělení splňovat, v případě, že získal korektní souhlas adresáta. Odeslaný e-mail musí být jasně označen jako obchodní sdělení a nesmí tajit či skrývat totožnost odesílatele. Každé obchodní sdělení pak musí obsahovat instrukce, jak zamezit zasílání dalších obchodních sdělení od daného odesílatele.

Výjimku tvoří podle § 8 odst. 3 obchodní sdělení rozeslané osobou vykonávající regulovanou činnost (např. advokát, notář, lékárník, lékař, ...), které musí kromě požadavků specifikovaných v § 7 odst. 4 navíc „obsahovat název profesní samosprávné komory zřízené zákonem, u níž je osoba vykonávající regulovanou činnost zapsána, odkaz na profesní pravidla uplatňovaná v členském státu Evropské unie, v němž je osoba vykonávající regulovanou činnost usazena, a způsob trvalého veřejného přístupu k informacím o příslušné profesní samosprávné komoře zřízené zákonem, jejímž je osoba vykonávající regulovanou činnost členem.“ (zákon č. 480/2004 Sb.)

Reklamní patičky

Ihned po nabytí účinnosti zákona č. 480/2004 se ukázala jako velmi problematická oblast reklamních patiček, které freemailoví provideři připojují na konec každého e-mailu odeslaného uživatelem. Mnohým se z výkladu zákona zdálo být zřejmé, že se po přiložení patičky stane z individuálního e-mailu nevyžádané obchodní sdělení. Freemailoví provideři by se tak dostávali do rozporu se zákonem. MI ČR se proto rozhodlo zveřejnit reakci na podobné teorie (konkrétně na článek „Česká republika přijímá zákony postihující rozesílání spamu“ zveřejněný v týdeníku Computerworld 31/2004). Pokud uživatel uzavřením smlouvy s poskytovatelem freemailu dává souhlas ke vkládání reklamních patiček, a pokud tyto reklamní patičky jsou označeny jako reklamní sdělení a jasně odděleny od soukromého obsahu e-mailu (nebo SMS), freemailoví provideři jednají v souladu se zákonem. (23)

Jiří Peterka v článku „Kauza reklamních patiček“ zveřejněném 4.10.2004 na Živě.cz poukázal na rozpor ve výkladu zákona v oblasti reklamních patiček mezi MI ČR a ÚOOÚ, zatímco podle MI ČR je vkládání reklamních patiček v souladu se zákonem, ÚOOÚ jejich vkládání považuje za protiprávní akt. Na základě mé schůzky s panem Šnytrem na ÚOOÚ však usuzuji, že úřad během dvou let, které od té doby uplynuly, přehodnotil svůj postoj. Pan Šnytr totiž považuje reklamní patičky za jakousi protislužbu za zdarma poskytované freemailové služby. Nebo-li uživatel touto formou v podstatě platí za jinak zdarma poskytované služby. (2)

5.2 Co se chystá, co neprošlo

5.2.1 Co se mohlo změnit, ale nezměnilo

MI ČR se již v minulosti snažilo vztáhnout zákon i na nekomerční druhy spamu, jako jsou agitace politických stran či nejrůznějších náboženských sekt apod. Spam nekomerčního charakteru se MI ČR snažilo začlenit do připravovaného trestního zákoníku jako elektronickou formu obtěžování, přičemž by se na něj vztahovala trestní sazba ve výši až 1 roku odnětí svobody. Tím bychom se znatelně vzdálili legislativě uplatňované v EU a naopak přiblížili některým státům v USA, kde je spam trestným činem. Nicméně snaha MI ČR nevyšla a v návrhu trestního zákoníku se problematika spamu vůbec neobjevila. Pan Plíšek se mi však svěřil, že tuto snahu MI ČR nevzdává a s očekávaným znovuotevřením trestního

zákoníku se bude znovu snažit prosadit uzákonění nekomerčního spamu jako trestného činu (byť se sazbou „pouze“ do 1 roku). (1)

ÚOOÚ se snahou MI ČR zmíněnou v předchozím odstavci nesouhlasí. Především podle ÚOOÚ může být trestný obsah spamu, nikoli jeho forma. Jako trestný čin si ÚOOÚ dokáže představit jiné formy kybernetické škodlivé činnosti jako je například phishing, který může být obsažen ve spamu. Navíc si ÚOOÚ uvědomuje problematické šetření případů nekomerčního spamu, proto je zastáncem současného stavu, kdy je za protiprávní považováno pouze nevyžádané obchodní sdělení. (2)

Tato oblast je velice diskutabilní, podle množství názorů v diskuzích na nejrůznějších internetových blozích, většina uživatelů požaduje rozšíření nevyžádaných sdělení i o spam nekomerčního charakteru. Otázkou ovšem je, jak právně definovat nekomerční spam. Například, pošlu-li pozvánku na koncert mé kapely dvaceti kamarádům, jednalo by se už o nevyžádané sdělení? Je možné, že pro některé ano, ale pro ostatní určitě ne. Negativní postoj ÚOOÚ je z tohoto hlediska pochopitelný, šetření individuálních stížností by vyžadovalo konkrétní rozhodování a bylo by dost problematické (nejspíš by záviselo na objemu rozeslaných sdělení a na množství podaných stížností). Problém je i to, že ani současné směrnice EU nepovažují nekomerční spam za protizákonný, a tak je možné, že i v případě uzákonění nevyžádaného sdělení nekomerčního charakteru by se opakovala situace, jaká již nastala v OPT-IN resp. OPT-OUT problematice (viz předchozí text), kdy se česká legislativa vydala přísnější „cestou“.

5.3 Kudy se bude ubírat unijní politika v oblasti nevyžádaných obchodních sdělení?

Již v roce 2004 EU doplnila směrnici 2002/58/EC o sdělení, ve kterém klade důraz na nutnost zvyšování povědomí uživatelů a celkovou spolupráci všech subjektů, které se pohybují v této oblasti. Již probíhají různé programy, které mají za cíl právě zvyšování povědomí nejen o spamu (např. program „Bezpečnější Internet plus“, který je zaměřen na vzdělávání dětí v EU nebo „workshop OECD o spamu“). Ze statistik je patrné, že většina objemu celosvětového spamu nepochází z EU, proto Evropská komise zahájila dialog

s mimoevropskými zeměmi. Spolupráce EU a USA již úspěšně probíhá, komunikace se rozběhla také s asijskými státy (Čína, Japonsko, ...).

15.11.2006 přišla Evropská komise se zásadním dokumentem, který by měl nastínit přístup EU vůči spamu, ale i doprovodným problémům, které jsou se spamem spojovány. Dokument s názvem „Sdělení komise evropskému parlamentu, radě, hospodářskému a sociálnímu výboru a výboru regionů“ obsahuje nástin nové politiky v oblasti boje proti spamu, špionážnímu a škodlivému softwaru. Na základě provedených analýz a statistik došla Evropská komise k závěru, že spam již přerostl dosavadní právní úpravu celé problematiky, kterou zosobňovala především směrnice 2002/58/EC. Proto je na začátek roku 2007 naplánované přijetí nové ucelené politiky boje proti kybernetické trestné činnosti. Tato chystaná politika se opírá o několik zásadních oblastí, kterými se bude primárně zabývat:

- Ze strany soukromého sektoru bude vyžadována mnohem větší iniciativa. Počítá se se zavedením samoregulace, kdy se pomocí zavedení jakési „pečeti důvěryhodnosti“, pomocí které budou moci zákazníci rozlišovat společnosti. Největší nároky budou ovšem kladeny na poskytovatele poštovních služeb, kteří budou tlačeni ke zkvalitnění filtrování e-mailů a celkově se více zapojili do aktivit vedoucích ke zlepšení bezpečnosti na Internetu. Sem spadá také osvěta svých zákazníků, zavedení vlastní bezpečnostní politiky, ale i oznamovací povinnost odpovědnému orgánu členské země. (27)

- Od členských států se očekává větší informační propojení odpovědných orgánů a přidělení odpovídajících prostředků pro příslušné orgány (zde Komise poukazuje na úspěšný příklad Nizozemska), které musí mít jasně vymezenou pravomoc při prosazování práva, a výzkum. Důležitá je i spolupráce mezi orgány třetích zemí. Orgány by měly aktivně postupovat v případech žádostí o pomoc ze zahraničí. Členské státy by se měly také zapojit do nadnárodních aktivit. (27)

V souvislosti s chystanými opatřeními, která povedou jednoznačně ke zpřísnění koordinovaného boje EU proti spamu, se jeví jako těžko pochopitelné nedávné vynucení „změkčení“ zákona č. 480/2004 právě ze strany EU. Z tohoto hlediska je docela pravděpodobné, že budeme v brzké době opět donuceni vrátit se zpět k tvrdšímu principu OPT-IN za každých okolností.

5.4 USA

Jelikož spam pocházející z USA tvoří většinu nevyžádané elektronické pošty ve schránkách českých uživatelů, právní normy ošetřující tento fenomén v USA mají velký vliv na situaci v ČR v oblasti spamu. Poslední platná právní úprava spamu v USA má účinnost od 1.1.2004. Americký Kongres schválil koncem roku 2003 zákon, který dnes nikdo nenazve jinak než CAN-SPAM. CAN-SPAM je zkratka názvu „Controlling the Assault of Non-Solicited Pornography and Marketing“, v českém překladu přibližně „Regulace přílivu nevyžádané pornografie a obchodních sdělení“. Nicméně při pohledu na zkratku je zřejmé, že cílem bylo zkombinovat alespoň částečně relevantní slova, jejichž počáteční písmena složí stěžejní slovo SPAM. Anglické podstatné jméno CAN v překladu označuje plechovku či konzervu, proto sousloví CAN-SPAM má představovat jakési „zakonzervování spamu“ nebo jakousi „plechovku na spam“, nebo-li v tomto případě mluvíme nikoli o zkratce, nýbrž o akronymu. To nejpodstatnější z obsahu zákona lze shrnout do několika bodů (4):

- e-mail musí disponovat korektními hlavičkami, odesílatel musí jasně označovat obchodní sdělení a uvádět platné adresy
- odesílatel nesmí skrývat nebo falšovat odchozí adresy a celkovou identitu odesílatele a také nesmí používat zavádějící předmět zpráv
- odesílatel musí adresátovi poskytnout jednoduchý mechanismus pro odhlášení ze seznamu adresátů a to na náklady odesílatele
- je zakázán „e-mail harvesting“ nebo-li sklízení elektronických adres po Internetu, stejně tak jako jejich umělé generování
- rozesílání obchodních sdělení je založeno na rozdíl od EU na principu OPT-OUT, nebo-li firmy mohou rozesílat své komerční nabídky komukoli, kdo disponuje elektronickou adresou, přičemž musí respektovat předchozí body
- zákon také nařizuje jednotlivým federálním úřadům, vedení registrů uživatelů, kteří výslovně odmítli příjem nevyžádaných obchodních sdělení; registr je „obdobou seznamu "zakázaných" telefonních čísel, který vede FTC a který zakazuje telefonním obchodníkům volat na čísla, jež do tohoto seznamu zákazníci vložili“ (20)

- zákon určuje maximální sazbu za rozesílání nevyžádaných sdělení v USA odnětí svobody až do výše pěti let, nebo pokutu do výše dvou milionů dolarů

Jak vidno trestní sazba je přísnější než v ČR, na druhou stranu v USA platí benevolentnější princip OPT-OUT a právě díky uzákonění tohoto „mírného“ principu přišli kritici zákona s tvrzením, že akronym CAN-SPAM je v podstatě příhodný, neboť „You CAN SPAM.“ odpovídá českému „Můžete spamovat.“ Podle firmy Sophos (viz kapitola statistiky), vývoj objemu celosvětového spamu po přijetí CAN-SPAMu dává za pravdu kritikům. Navíc americký zákon stejně jako legislativa v ČR resp. EU nedosahuje za hranice země.

5.5 Aktivity v oblasti práva na mezinárodní scéně

Kromě EU, OECD jsou na mezinárodním poli v oblasti spamu aktivní ještě americká FTC (Federální obchodní komise) a mezinárodní ITU (Mezinárodní telekomunikační unie). Již v červenci 2004 ITU sezvala zástupce 60 zemí na konferenci, kde se diskutovalo mimo jiné o problematice spamu. Na základě této nadnárodní diskuze vznikla výzva vládám, aby přijaly nové zákony, popřípadě upravily staré zákony týkající se problematiky spamu, a jednoznačně určily odpovědné úřady pro kontrolu dodržování zákona. Měl to být první stupeň směrem ke smělému cíli. ITU se domnívá, že teprve až dostatečné množství zemí začlení anti-spamové právní řešení do svých legislativ, utvoří se dostatečná základna pro schválení mezinárodní listiny, která by zaručovala vynutitelnost zákona i za hranicemi země. Podle ITU je také důležité spolupracovat a předávat zkušenosti mezi odpovědnými úřady z různých zemí, neboť dosavadní právní úpravy spamu jsou stále mírně řečeno tristní. (2)

FTC v druhé polovině roku 2004 představila na mezinárodní scéně projekt s názvem „Akční plán na stíhání spamu“, v jehož rámci sestavila mezinárodní pracovní tým zabývající se problematikou spamu. Součástí plánu je výzva k dalšímu školení inspektorů příslušných regulačních orgánů a také zlepšení a hlavně zrychlení kontaktu při mezinárodním vyšetřování.

OECD již rozjela informační kampaň zacílenou na veřejnost, jejímž úkolem je osvěta a vzdělávání veřejnosti v oblasti kybernetické trestné činnosti a Internetu jako takového.

6 Realizace zákonů

Dozorem nad dodržováním paragrafů vztahujících se k šíření obchodních sdělení podle § 7 zákona č. 480/2004 Sb. je zákonem pověřen Úřad pro ochranu osobních údajů (ÚOOÚ), který při výkonu dozoru postupuje podle Zákona „o státní kontrole“ (zákon č. 552/1991 Sb.). Výjimku tvoří osoby vykonávající regulované činnosti, na jejichž povinnosti vyplývající z § 8 odst. 3 dohlíží příslušná profesní samosprávná komora, pod kterou spadají. Profesní samosprávná komora při výkonu dozoru nad povinnostmi vyplývajícími z § 8 odst. 3 postupuje podle zákona, který upravuje příslušnou regulovanou činnost (např. zákon č. 523/1992 Sb. „o daňovém poradenství a Komoře daňových poradců České republiky“, zákon č. 220/1991 Sb. „o České lékařské komoře, České stomatologické komoře a České lékárnické komoře“, zákon č. 85/1996 Sb. „o advokacii“).

6.1 ÚOOÚ

6.1.1 Pravomoc a povinnosti Úřadu vyplývající ze zákona

Volba ÚOOÚ je výhodná z několika důvodů. Šíření obchodních sdělení je velmi často doprovázeno dalšími často nekalými formami marketingu, které jsou založeny na manipulaci s osobními údaji. Z tohoto hlediska je proto výhodné, aby celá oblast spadala pod jeden úřad. Další důvod je ten, že bude-li „vyžádanost“ či „nevyžádanost“ obchodních sdělení posuzovat jediný úřad, mnohem snáz si během praxe vytvoří vhodný „metr“, s jehož pomocí bude posuzovat jednotlivé případy. Tento důvod byl ostatně jedním z hlavních motivů, proč došlo k současné centralizaci, neboť do schválení současného zákona č. 480/2004 Sb. problematika v té době ještě „nevyžádané reklamy“ spadala pod dozor živnostenských úřadů, a vzhledem k množství živnostenských úřadů bylo velmi obtížné nastavit společný „metr“ v posuzování konkrétních případů.

Na základě § 11 zákona č. 480/2004 Sb. je určena sankce, kterou může ÚOOÚ udělit za správní delikt. V případě nedodržení povinností vyplývajících z § 7 zákona č. 480/2004 Sb. je úřad oprávněn uvalit pokutu až do výše deseti milionů korun (v případě nedodržení povinností vyplývajících z § 8 zákona č. 480/2004 Sb. je příslušná profesní samosprávná komora

oprávněna udělit pokutu do výše jednoho milionu korun), výše pokuty závisí na závažnosti správního deliktu, způsobu jeho spáchání a následcích a okolnostech, za nichž byl spáchán. V případě, že právnická osoba prokáže, že vynaložila veškeré úsilí, aby porušení právní povinnosti zabránila, právnická osoba za správní delikt neodpovídá. Vybírání či případné vymáhání pokut probíhá podle zákona „o správě daní a poplatků“ (zákon č. 337/1992 Sb.) a provádí je celní úřad. Příjem z pokut je i příjmem orgánu dozoru, který pokutu uložil. Při řízení ve věcech, které upravuje zákon č. 480/2004 Sb. se postupuje podle správního řádu (zákon č. 71/1967 Sb.).

Na rozdíl od běžného postupu, kdy účinnost nově vyhlášené právní normy začíná až po čtrnácti dnech, zákon č. 480/2004 Sb. s podobným přechodným obdobím nepočítal, neboť účinnost zákona začala bez prodlení dnem vyhlášení. MI ČR tím dalo jasně najevo, že si přeje okamžitou adaptaci postupů Úřadu na novou právní úpravu a bezodkladné pokutování subjektů, které po nabytí účinnosti zákona (tzn. po 7.9.2004) rozesílají nevyžádaná obchodní sdělení. Přes stanovisko MI ČR se ÚOOÚ rozhodl po celý zbytek roku 2004 subjekty rozesílající nevyžádaná obchodní sdělení nepokutovat. ÚOOÚ tyto subjekty pouze upozorňoval o porušení zákona a vyžadoval provedení nápravných opatření. Přechodné období ÚOOÚ zavedl především kvůli veřejnosti, aby si na nový zákon zvykla, ale využil ho i úřad. Jedním z důležitých aspektů efektivního zavedení právní normy do praxe je totiž stanovení vhodného a především jednotného „metru“, na základě kterého bude Úřad rozhodovat, co je spam, a co nikoli. I samotný zákon ponechává v určitých oblastech problematiky šíření nevyžádaných sdělení určitou volnost, i když jak jsem se zmínil, v některých případech se jedná spíše o „mezeru v zákonu“. Vlastní kontrolní činnost započala až rokem 2005.

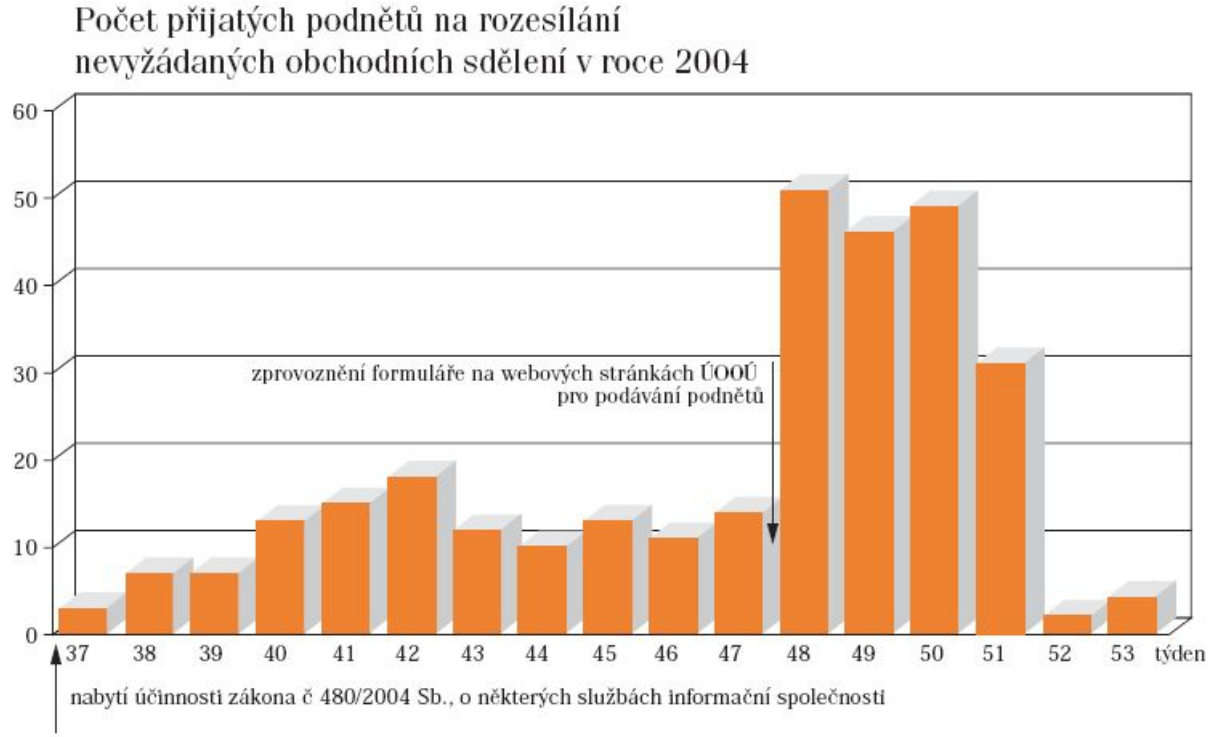
6.1.2 Informační činnost Úřadu

Jednou z důležitých činností úřadu je osvěta občanů o jejich právech v oblasti ochrany jejich soukromí, úřad si je totiž dobře vědom, že investice do občanů nebo-li potenciálních „zákazníků“ úřadu se mu do budoucna vyplatí, protože informovaný občan se dokáže sám bránit proti zásahům do jeho soukromí. Úřad se stal distributorem informačního letáku OECD s výmluvným názvem „Jak se bránit proti nevyžádaným e-mailům“. Součástí letáku je uvedení čtenáře do problematiky spamu, definice spamu a především postupy, jak se nevyžádané poště vyhnout. K dispozici je i na webových stránkách ÚOOÚ. Úřad poskytuje

konzultace a právě v souvislosti s nabytím účinnosti zákona č. 480/2004 Sb. byla tato služba úřadu hojně využívána, kdy fyzické i právnické osoby kontaktovali úřad s žádostí o výklad zákona a aplikaci práva Úřadem. Úřad také pravidelně pořádá semináře ve spolupráci s MI ČR. Na základě neustále se snižujícího počtu žádostí o výklad zákona č. 480/2004 Sb. v roce 2005 lze usoudit, že odborná veřejnost již tuto problematiku pochopila.

6.1.3 Podávání stížností a jejich vyřizování

Vzhledem k velkému množství stížností, podaných Úřadu k prošetření po nabytí účinnosti „anti-spamového zákona“, se úřad rozhodl vytvořit informační systém pro sběr a zpracování těchto podnětů. Na začátku listopadu 2004 zprovoznil ÚOOÚ na svých webových stránkách formulář, pomocí něhož mohou uživatelé snadno podávat stížnosti. Navíc aplikace, která tyto stížnosti zpracovává a třídí, šetří pracovníkům úřadu spoustu času. Velkým zjednodušením pro podavatele stížnosti je to, že stížnosti na nevyžádaná obchodní sdělení, jejichž autorem je subjekt vykonávající regulovanou činnost, jsou předávány příslušné profesní samosprávné komoře. Stížnost se však může vztahovat i na subjekt, který sídlí v některém z unijních států. V takovém případě ÚOOÚ předá podnět odpovědnému Orgánu daného státu.



(2)

Z grafu je patrné rapidní navýšení počtu úřadem přijatých stížností, ke kterému došlo po zprovoznění formuláře pro podávání podnětů na rozesílání nevyžádaných obchodních sdělení na webových stránkách ÚOOÚ. Po vyplnění a odeslání formuláře je stížnost zařazena do jakéhosi pořadníku. Každá stížnost dostane své pořadové číslo a příslušný pracovník se jí bude zabývat, až přijde na řadu. Analýza nevyžádaného e-mailu začíná u hlavičky, kterou má podle pokynů osoba podávající stížnost vložit do formuláře. Z hlavičky se příslušný pracovník úřadu snaží identifikovat odesílatele, což je nejobtížnější fází šetření. Spamer se za sebou snaží „zamést“ stopy všemi možnými způsoby, krádeží identity (např. botnety), která je naprosto běžnou praxí v těchto případech, počínaje. Nejjednodušším způsobem, jak zjistit, zda se nejedná o falešnou adresu, je zaslání kontrolní zprávy na adresu odesílatele. Pak se přistupuje k analýze obsahu e-mailu.

ÚOOÚ šetří případy šíření nevyžádaných obchodních sdělení vždy pouze na základě stížnosti (formulář, dopis). ÚOOÚ má ze zákona povinnost zabývat se každým byť individuálním podnětem bez rozdílu. Vzhledem k nedostatečnému počtu inspektorů úřadu, kteří se zabývají problematikou šíření nevyžádaných sdělení, se domnívám, že by se měl zákonem určit minimální počet stížností na jednoho odesílatele potřebný pro zahájení šetření. Tato změna by byla efektivní i vzhledem ke způsobu udílení pokut úřadem. Z rozhovoru s panem Šnytrem na ÚOOÚ jsem se dozvěděl, že výše pokuty závisí především na počtu stížností, zatímco forma není tolik důležitá. (2)

Nový předseda ÚOOÚ, který na úřadu působí od 1.1.2005, se velké vytížení pracovníků rozhodl řešit především organizačními změnami, navýšil stav inspektorů o 8 pracovníků. Plánuje také vytvoření specializované pobočky v Brně, která by měla zrychlit administrativní činnost při provádění dozoru nad subjekty v moravském a slezském regionu.

Podavatel, který pro podání stížnosti využije formulář, by měl pro urychlení šetření vyplnit všechny pole formuláře. Nejdůležitější součástí stížnosti na nevyžádaný e-mail je nejen jeho obsah, ale především hlavička, která obsahuje zásadní informace potřebné pro zahájení šetření. Nejvhodnějším řešením je zaslání celého e-mailu po předchozím uložení do formátu .msg nebo .eml. ÚOOÚ také doporučuje, aby se podavatel stížnosti předem ujistil, že skutečně odesílateli obchodního sdělení v minulosti nedal souhlas se zasíláním. „Ze zkušenosti víme, že v některých případech příjemce sdělení tuto skutečnost již zapomněl nebo si ji ne zcela dostatečně uvědomil. Zpráva mohla přijít i omylem, překlepnutí v e-mailové adrese je poměrně běžným jevem. Doporučujeme tedy před podáním stížnosti

prověřit i tuto variantu.“ (2) Podavatel stížnosti by si měl také uvědomit, že vyřízení daného případu není otázka dnů, nýbrž řádově několika měsíců. Je to způsobeno množstvím podobných žádostí, kterých dochází běžně několik set do měsíce. Podavatel není účastníkem správního řízení a od úřadu obdrží v případě vedení takového řízení pouze vyrozumění na elektronickou adresu, kterou podavatel vyplnil do formuláře. Ve vyrozumění ho úřad informuje, zda došlo k porušení zákona a jaká bude učiněna náprava. Pokud tedy došlo ke správnímu deliktu, inspektor, který prováděl šetření, postoupí výsledky šetření dalšímu sankčnímu řízení. ÚOOÚ nemá pravomoc rozhodovat o nárocích satisfakční povahy, jako je omluva nebo finanční odškodnění, v těchto případech se podavatel musí obrátit na soud. ÚOOÚ také musí dohlížet nad dodržováním uložených nápravných opatření.

6.1.4 Aktivity Úřadu na mezinárodní scéně

ÚOOÚ resp. příslušná profesní samosprávná komora fungují ze zákona také jako kontaktní místo pro členské státy EU a pro Evropskou Komisi. V rámci této funkce mají stanovené povinnosti informačního charakteru. Mezi tyto povinnosti spadá poskytování podrobných informací o šetřených případech a také poskytování kontaktů na další instituce či subjekty, které mohou být v této oblasti nápomocny. ÚOOÚ se také aktivně zapojuje do mezinárodních programů, které se zabývají problematikou kybernetické trestné činnosti. Pracovníci úřadu se zapojili do aktivit pracovní skupiny CNSA (Contact Network of Spam Authorities), která vznikla z podnětu Evropské Komise. Spolupráce s CNSA byla stvrzena 8.12.2004, kdy ÚOOÚ oficiálně podepsal „Protokol o spolupráci“, jehož hlavním bodem je především prosazování unijní směrnice 2002/58/EC, konkrétně pasáží, které se dotýkají problematiky spamu. Velmi aktivní organizací v oblasti spamu je OECD, z jejíž iniciativy vznikla pracovní skupina TFS (Task Force on Spam). Součástí této skupiny jsou i dva odborníci z ÚOOÚ, kteří se spolupodíleli na přípravě jakési příručky na obranu proti spamu – „Anti-spam Toolkit“. OECD resp. TFS se snaží udržovat pevné styky s dalšími organizacemi, jako např. APEC (Asia-Pacific Economic Cooperation) či ITU (International Telecommunication Union), protože si je vědoma nadnárodní povahy spamu. (2)

V roce 2005 se konaly tři důležité schůze, kterých se také zúčastnili zástupci ÚOOÚ (2):

- na konci června 2005 hostila Ženeva Celosvětový summit ITU o informační společnosti, na tomto summitu se odborníci z celého světa zabývali mezinárodním problémem obrany proti spamu; výsledkem jednání bylo zjištění, že spam se stal

součástí organizovaného zločinu, a protože jej nelze regulovat, informační společnost se bude muset zamyslet nad budoucností Internetu jako takového

- v Bruselu se 6.4.2005 sešli na páté schůzi regulátoři členských zemí a diskutovali především o spolupráci členských zemí EU v problematice spamu; především se rozebíraly postupy předávání informací při šetření případů

- 7.7.2005 hostil opět Brusel v pořadí již šestou schůzi regulátorů členských zemí, kteří se zabývali rozšiřujícímu se využívání spywaru, který je často součástí spamu, a obraně proti němu, včetně nutného zapojení providerů internetových služeb

ÚOOÚ udržuje již delší dobu vynikající pracovní vztahy se španělskou obdobou českého ÚOOÚ. V polovině července 2005 proběhlo další z řady pravidelných setkání s pracovníky španělské agentury pro ochranu dat. Během tohoto setkání se kromě jiných oblastí řešil i boj proti spamu. Odborníci z obou úřadů si předávali vlastní zkušenosti s řešením případů nevyžádaných obchodních sdělení. Pan Šnytr mě například informoval o elegantním řešení udělení souhlasu se zasíláním obchodních sdělení pomocí vizitek, který je úspěšně praktikován právě ve Španělsku. Předáte-li v ČR někomu svou vizitku, na které je vaše elektronická adresa, příjemce vaší vizitky může asi stěží u případného šetření prokázat, že jste mu tím dali souhlas se zasíláním obchodních sdělení. Ve Španělsku mají zástupci firem u sebe vždy vizitky, na jejichž zadní straně je umístěno razítko například s nápisem „souhlasím se zasíláním obchodních sdělení“, kdo se pod nápis podepíše, jednoznačně souhlasí se zasíláním obchodních sdělení.

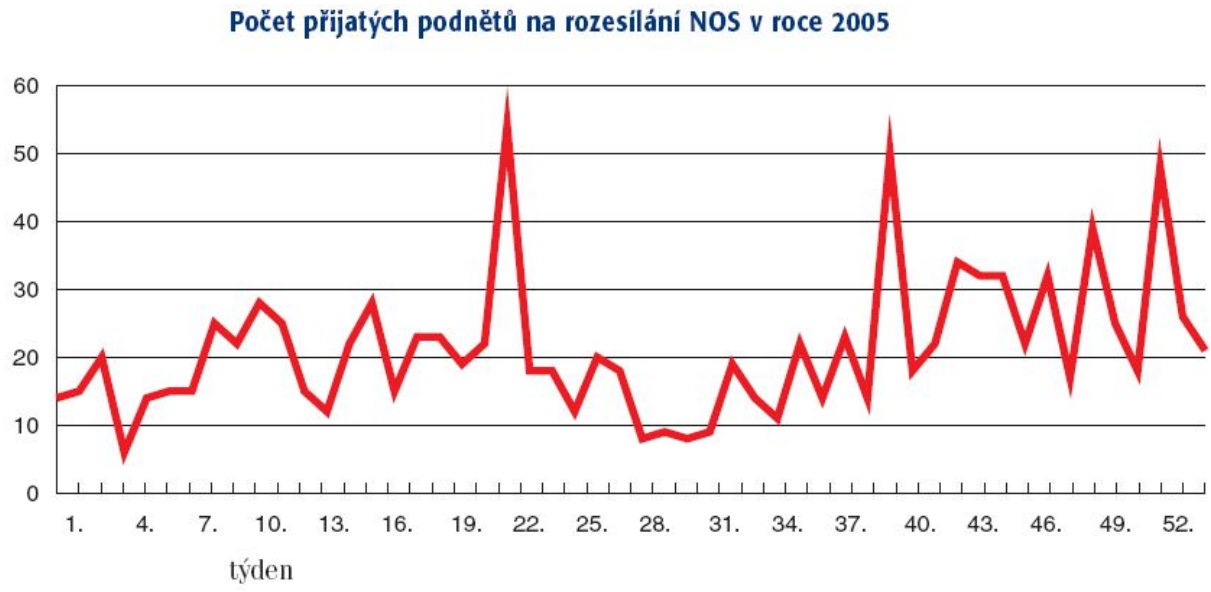
6.2 Statistiky podaných stížností a případů spáchání správních deliktů v ČR

Jak jsem se již zmínil, v roce 2004 ÚOOÚ subjektům rozesílajícím nevyžádaná obchodní sdělení ještě neuděloval pokuty. Do konce roku Úřad nicméně evidoval 306 stížností. Subjekty, kterých se stížnost týkala, pouze upozorňoval na porušení zákona a vyžadoval provedení nápravných opatření. V roce 2005 přišlo na ÚOOÚ 1105 stížností, z toho v 18 případech se Úřadu podařilo prokázat, že subjekt naplnil skutkovou podstatu některého ze správních deliktů podle zákona „o některých službách informační společnosti“ a šestnácti

z nich byly uloženy pokuty. Pouze ve dvou případech došlo k zastavení řízení. Z celkového počtu 1105 stížností jich bylo přibližně 15 % neoprávněných. Za první tři čtvrtletí roku 2005 obdržel Úřad také 25 podnětů od zahraničních stěžovatelů. (2)

Statistika podnětů podaných na nevyžádaná obchodní sdělení zaslaných na ÚOOÚ		
	7.9. - 31.12.2004	**1.1. - 31.3.2005**
e-mail	117	12
běžná pošta	9	1
formulář ÚOOÚ	180	211
celkem	306	224
z toho oprávněné	29	29
z toho ze zahraničí	7	9

(2)



(2)

Mezi prvními subjekty, které byly pokutovány za šíření nevyžádaných obchodních sdělení pomocí elektronických prostředků, se objevily společnosti Azzurra Tours, Alka-Tour Brno, BuBu žampiony a Scarabeus. První tři jmenované firmy se podělily o pokuty ve výši od 5 do 20 tisíc korun. Zmíněné tři firmy šířily nevyžádaná obchodní sdělení e-mailem bez prokazatelného souhlasu adresátů. Obsahem těchto e-mailů byly nabídky zájezdů resp. dodávky organického hnojiva. O doposud nejvyšší udělenou pokutu za šíření nevyžádaných

obchodních sdělení v ČR se „zasloužila“ společnost Scarabeus, která nabízela bezplatnou prezentaci v databázi podnikatelských subjektů a institucí (na internetové adrese www.rejstrikfirem.cz), bez předchozího prokazatelného souhlasu příjemců. Společnosti byla udělená pokuta ve výši 160 000 Kč. (2)

V současné době se vyšetřuje jeden z největších případů rozesílání nevyžádaných obchodních sdělení na území ČR. Spamer (v tomto případě nejmenovaný hotel) rozesílal nevyžádanou reklamu v e-mailech, přičemž se snažil obejít zákon využitím „mezery“ v zákoně, o které jsem psal v předešlém textu. Spamer bez předchozího souhlasu adresátů rozesílal e-maily, které obsahovaly obchodní sdělení „zabalené“ do URL adresy. Tento případ se stále prošetřuje, ale již nyní se spekuluje o uložení rekordní pokuty českému spamerovi. (2)

V průběhu šetření jednotlivých případů se inspektoři setkali i s problémy, které jim komplikovaly hladký průběh šetření. Problematické bylo především identifikování spamerů, neboť se ukázalo, že inspektoři při šetření postrádají pravomoci, které by jim usnadnily šetření. Inspektor nemá oprávnění dotazovat se třetích stran, proto je velmi problematické například zjistit, kdo byl v daný moment připojen k Internetu, neboť nemůže nahlídnout do databází internetových providerů. Inspektoři by proto uvítali, kdyby se na ně přesunula část operativních kompetencí, které má k dispozici policie.

6.3 Příklady procesů se spamery v zahraničí

Prvním odsouzeným spamerem se stal jistý Howard Carmack, veřejnost mu během soudního procesu přidělila přezdívku „Buffalo Spamer“. Poprvé byl odsouzen v roce 2003, ale byl propuštěn na kauci. O rok později čelil dalším žalobám, tentokrát byl obviněn z rozeslání 825 miliónů nevyžádaných e-mailů, přičemž použil elektronické adresy obyvatel Buffala, odtud pochází přezdívka. Byl odsouzen za rozesílání nevyžádaných obchodních sdělení, za krádež identity a za zpronevěru k sedmi letům odnětí svobody a k uhrazení škod způsobených spamerskými aktivitami v celkové výši 14,5 milionů dolarů. Jednalo se o důležitý precedenční rozsudek, u kterého se předpokládalo, že by měl mít odstrašující účinek na ostatní spamery. Aktivní v podávání soudních žalob na rozesílatele spamu je společnost Microsoft, která v roce 2005 obvinila 200 údajných spamerů. Dalším velkým a nápadným soudním procesem, který proběhl kde jinde než v USA, a který by měl odradit další spamery, se stal proces s Jeremy

Jaynesem, jenž denně rozesílal přes 20 milionů nevyžádaných e-mailů. Během své činnosti nashromáždil majetek v celkové odhadované výši 24 milionu dolarů. I jemu se dostalo precedenčního rozsudku ve výši 9 let vězení. (12)

7 Závěr

Největší nedostatky vidím v realizaci zákona. Inspektoři ÚOOÚ trpí především nedostatkem pravomocí při vyšetřování (zejména právo ptát se třetích osob je nezbytné). Po vzoru Nizozemí by Úřad měl dostat více prostředků na sestavení odděleného týmu, který by se zabýval výlučně šířením nevyžádaných obchodních sdělení. Také poznatky Úřadu vzešlé z praxe by měly být více zohledňovány při navrhování úprav zákonů.

Zákon má sice své chyby, ale ty se odstraní v nejbližších novelách. Problém spammingu však nevyřeší dílčí úpravy stávající legislativy, ale spíš celková změna pohledu na problematiku nevyžádané reklamy. Taková radikální změna ovšem už není v kompetenci českých zákonodárců, neboť ČR je vázána unijními direktivami. I EU si uvědomuje, že čtyři roky staré unijní direktivy upravující problém nevyžádaných obchodních sdělení již nejsou odpovídající současné formě šíření spamu, a proto již vytvořila novou ucelenou politiku boje nejen proti spammingu, ale proti kybernetické trestné činnosti jako takové.

Nejdůležitějším bodem bude synchronizace politik všech unijních států, a zajištění spolupráce národních orgánů dozoru při šetření konkrétních případů. Tady ovšem cesta za vymýcením spamu z e-mailových schránek nekončí. Spam je celosvětový problém, tudíž je třeba součinnost se všemi „velmocemi“ v rozesílání spamu, tedy především s USA, s Čínou a s Jižní Koreou. Cílem je, aby si mohly národní orgány dozoru z celého světa předávat stížnosti uživatelů a spolupracovat na řešení jednotlivých případů. Mezinárodní organizace společně s EU již zahájily jednání, ale všechny zúčastněné strany si uvědomují, že to bude „běh na dlouhou trať“, který možná nikdy neskončí.

Vše směřuje v radikální vyústění, kdy se uživatelé Internetu kvůli nezvladatelné kybernetické trestné činnosti budou muset vzdát sice neomezeného, ale zároveň nezabezpečeného Internetu ve prospěch Internetu nového – omezeného, zato zabezpečeného.

8 Seznam použitých zdrojů

1. Schůzka s Mgr.Martinem Plíškem, ředitelem Odboru legislativně-právního Úseku pro vnější vztahy Ministerstva Informatiky ČR

2. Schůzka s Ing. Milošem Šnytrem, inspektorem Úřadu pro ochranu osobních údajů

3. Autor neznámý. Analýza spamu za 2. pololetí 2005 [online]. © ATLAS.cz [cit.2006-12-28]. Dostupné z: <http://press.atlas.cz/clanek.aspx?rubrika=26&clanek=59134>

4. Autor neznámý. CAN-SPAM Act of 2003 [online]. © 20.12.2006 SPAMLAWS.com [cit.2006-12-25]. Dostupné z <http://www.spamlaws.com/federal/108s877.shtml>

5. Autor neznámý. Krátké zprávy © 28.3.2005 PCSVĚT.cz [cit.2006-12-28]. Dostupné z: <http://www.pcsvet.cz/art/shorts.php?page=111>

6. Autor neznámý. Phishing [online]. © 29.12.2006 Wikipedie [cit.2006-12-30]. Dostupné z: <http://cs.wikipedia.org/wiki/Phishing>.

7. Autor neznámý. Pod stromeček spam? [online]. © 20.12.2006 ISDN server [cit.2006-12-25]. Dostupné z: <http://www.isdn.cz/clanek.php?cid=8120>

8. Autor neznámý. Spam [online]. © 17.11.2006 Wikipedie [cit.2006-12-10]. Dostupné z: <http://cs.wikipedia.org/wiki/Spam>.

9. Business Software Alliance .[www portál]. Dostupné z: <http://www.bsa.cz/> [cit.2006-10-26]. Webová prezentace Business Software Alliance (BSA), což je přední organizace, která se zabývá prosazováním bezpečného a legálního digitálního světa. BSA vzdělává spotřebitele v oblasti správy softwaru a ochrany autorských práv, bezpečnosti informačních technologií, obchodování, elektronického ochodu a v ostatních záležitostech souvisejících s internetem.

10. DĚDEK Jan. John Cleese: Chtěl bych být sýr [online]. © 9.7.2005 NOVINKY.cz [cit.2006-12-12]. Dostupné z: <http://kina.seznam.cz/03/57/79.html>

11. FALTÝNEK Lukáš. Linux, viry a spam [online]. © 2005 LinuxEXPRES [cit.2006-12-26]. Dostupné z: <http://www.linuxexpres.cz/index.php?show=001053003006>

12. FARGHALI Hany. Americký spamer půjde jako první do vězení [online]. © 1.6.2004 iHNED.cz [cit.2006-12-20]. Dostupné z: <http://digiweb.ihned.cz/4-10076440-14450390-i00000_d-1f>

13. FARGHALI Hany, ČEPICKÝ Miroslav. Spam: hrozba, ale i dobrý obchod [online]. © 15.11.2005 iHNED.cz [cit.2006-12-25]. Dostupné z: <http://ekonomika.ihned.cz/2-17209510-001000_d-60>

14. FARGHALI Hany. Dvě třetiny e-mailů v Česku jsou spam [online]. © 28.7.2005 iHNED.cz [cit.2006-12-25]. Dostupné z: <http://digiweb.ihned.cz/3-22611205-spam-i00000_d-4a>

15. Federal Trade Commission For The Consumer [www portál]. Dostupné z: <http://www.ftc.gov/spam/> [cit.2006-10-26]. Server obsahující informace o současných právních sporech vedených institucí Federal Trade Commission proti nevyžádaným obchodním sdělením a o odpovědnostech spammerů.

16. CHLEBOUN, Michal. Spamování – kouzlo kreativity [online]. © 27.2.2004 LUPA.cz.,[cit.2006-10-26]. Dostupné z: <http://www.lupa.cz/clanky/spamovani-kouzlo-kreativity/>.

17. ISVS.cz (Praha).[www portál]. Dostupné z: <http://www.isvs.cz/> [cit.2006-10-26]. Informační server ISVS.cz soustřeďuje veškeré významné informace z oblasti realizace státní informační politiky a z oblasti budování a provozování informačních systémů veřejné správy.

18. ITprávo.cz (Praha).[www portál]. Dostupné z: <http://www.itpravo.cz/> [cit.2006-10-26]. Informační server, který shromažďuje a publikuje články, polemiky, recenze, zprávy z domova a ze světa z oboru práva informačních technologií.

19. KOLAJA Marcel, BARTOŠEK Miroslav. Jemný úvod do (anti)spamové problematiky [online]. © 29.9.2006 ÚVT MU [cit.2006-10-26]. Dostupné z: <http://www.ics.muni.cz/zpravodaj/articles/251.html/>.

20. KRIM Jonathan. Zákon může vést k založení antispamového registru [online]. © 23.9.2003 ROOT.cz [cit.2006-12-25] Dostupné z:

<http://www.root.cz/clanky/hlasovani-o-omezeni-emailovych-reklam-senat/?SID=B2C8610523B5A570BFE833E72DC715F1>

21. MATEJKA, Ján. Co vlastně přinesl zákon o některých službách informační společnosti? [online]. © 18.10.2004 LUPA.cz.,[cit.2006-10-26]. Dostupné z: <http://www.lupa.cz/clanky/co-vlastne-prinesl-zakon-o-nekterych-sluzbach-informacni-spolecnosti/>.

22. MATEJKA, Ján. Spamming a jeho právní úprava [online]. © 17.7.2003 LUPA.cz.,[cit.2006-10-26]. Dostupné z: <http://www.lupa.cz/clanky/spamming-a-jeho-pravni-uprava/>.

23. Ministerstvo informatiky ČR (Praha).[www portál]. Dostupné z: <http://www.micr.cz/> [cit.2006-10-26]. Informační server Ministerstva informatiky ČR.

24. MOUČKA Bohuslav, PEŠA Radim. A zase spam [online]. © červen 2004 ÚVT MU [cit.2006-10-26]. Dostupné z: <http://www.ics.muni.cz/zpravodaj/articles/308.html>.

25. PETERKA Jiří. Boj proti spamu v praxi [online]. © 18.5.2006 LUPA.cz [cit.2006-12-25]. Dostupné z: <http://www.lupa.cz/clanky/boj-proti-spamu-v-praxi/>

26. PETERKA Jiří. Jak bude stát bojovat proti spamu? [online]. © 27.9.2004 ŽIVĚ.cz [cit.2006-12-25]. Dostupné z: <http://www.zive.cz/h/Byznys/AR.asp?ARI=118787&CAI=2034>

27. Sdělení Komise Evropskému parlamentu, Radě, Hospodářskému a sociálnímu výboru a Výboru regionů [online]. © 15.11.2006 [cit.18.12.2006]. Dokument ve formátu pdf, dostupný z:

<http://eur-ex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0494:FIN:CS:PDF>

28. SOPHOS [www portál]. Dostupné z: <http://www.sophos.com> [cit.2006-11-26]. Domovská stránka společnosti, zabývající se bezpečností

29. ŠTĚDROŇ Bohumír. Vláda chce bojovat proti spamu [online]. © 5.2.2004 LUPA.cz.,[cit.2006-10-26]. Dostupné z: <http://www.lupa.cz/clanky/vlada-chce-bojovat-proti-spamu/>.

30. Úřad pro ochranu osobních údajů (Praha).[www portál]. Dostupné z: <http://www.uoou.cz> [cit.2006-10-26]. Domovská stránka nezávislého orgánu pro ochranu osobních údajů.

9 Příloha

9.1 Zákon 480/2004 Sb. v plném znění

480/2004 Sb.

ZÁKON
ze dne 29. července 2004

o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti)

Změna: 444/2005 Sb.
Změna: 214/2006 Sb.

Parlament se usnesl na tomto zákoně České republiky:

ČÁST PRVNÍ

O NĚKTERÝCH SLUŽBÁCH INFORMAČNÍ SPOLEČNOSTI

§ 1

Předmět úpravy

Tento zákon upravuje v souladu s právem Evropských společenství 1) odpovědnost a práva a povinnosti osob, které poskytují služby informační společnosti a šíří obchodní sdělení.

§ 2

Pro účely tohoto zákona se rozumí

a) službou informační společnosti jakákoliv služba poskytovaná elektronickými prostředky na individuální žádost uživatele podanou elektronickými prostředky, poskytovaná zpravidla za úplatu; služba je poskytnuta elektronickými prostředky, pokud je odeslána prostřednictvím sítě elektronických komunikací a vyzvednuta uživatelem z elektronického zařízení pro ukládání dat,

b) elektronickou poštou textová, hlasová, zvuková nebo obrazová zpráva poslaná prostřednictvím veřejné sítě elektronických komunikací, která může být uložena v síti nebo v koncovém zařízení uživatele, dokud ji uživatel nevyzvedne,

c) elektronickými prostředky zejména síť elektronických komunikací, elektronická komunikační zařízení, koncová telekomunikační zařízení a elektronická pošta,

d) poskytovatelem služby každá fyzická nebo právnická osoba, která poskytuje některou ze služeb informační společnosti,

e) uživatelem každá fyzická nebo právnická osoba, která využívá službu informační společnosti, zejména za účelem vyhledávání či zpřístupňování informací,

f) obchodním sdělením všechny formy sdělení určeného k přímé či nepřímé podpoře zboží či služeb nebo image podniku fyzické či právnické osoby, která vykonává regulovanou činnost 2) nebo je podnikatelem 3) vykonávajícím činnost, která není regulovanou činností; za obchodní sdělení se považuje také reklama podle zvláštního právního předpisu. 4) Za obchodní sdělení se nepovažují údaje umožňující přímý přístup k informacím o činnosti fyzické či právnické osoby nebo podniku, zejména doménové jméno nebo adresa elektronické pošty; za obchodní sdělení se dále nepovažují údaje týkající se zboží, služeb nebo image fyzické či právnické osoby nebo podniku, získané uživatelem nezávisle,

g) automatickým krátkodobě dočasným ukládáním ukládání informací poskytnutých uživatelem, ke kterému dochází výhradně za účelem uskutečnění přenosu prostřednictvím sítě elektronických komunikací, přičemž doba uložení informace nepřesahuje dobu, která je pro zajištění přenosu obvyklá,

h) automatickým dočasným meziukládáním ukládání informací poskytnutých uživatelem, které slouží výhradně pro co možná nejúčinnější následný přenos těchto informací na žádost jiných uživatelů.

Odpovědnost poskytovatelů zprostředkovatelských služeb

§ 3

Odpovědnost poskytovatele služby za obsah přenášených informací

(1) Poskytovatel služby, jež spočívá v přenosu informací poskytnutých uživatelem prostřednictvím sítí elektronických komunikací nebo ve zprostředkování přístupu k sítím elektronických komunikací za účelem přenosu informací, odpovídá za obsah přenášených informací, jen pokud

a) přenos sám iniciuje,

b) zvolí uživatele přenášené informace, nebo

c) zvolí nebo změní obsah přenášené informace.

(2) Přenos informací a zprostředkování přístupu podle odstavce 1 zahrnuje také automatické krátkodobě dočasné ukládání přenášených informací.

§ 4

Odpovědnost poskytovatele služby za obsah automaticky dočasně meziukládaných informací

Poskytovatel služby, jež spočívá v přenosu informací poskytnutých uživatelem, odpovídá za obsah informací automaticky dočasně meziukládaných, jen pokud

a) změní obsah informace,

b) nevyhoví podmínkám přístupu k informaci,

c) nedodržuje pravidla o aktualizaci informace, která jsou obecně uznávána a používána v příslušném odvětví,

d) překročí povolené používání technologie obecně uznávané a používané v příslušném odvětví s cílem získat údaje o užívání informace, nebo

e) ihned nepřijme 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 či znemožnění přístupu k této informaci.

§ 5

Odpovědnost poskytovatele služby za ukládání obsahu informací poskytovaných uživatelem

(1) Poskytovatel služby, jež spočívá v ukládání informací poskytnutých uživatelem, odpovídá za obsah informací uložených na žádost uživatele, jen

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

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

(2) Poskytovatel služby uvedený v odstavci 1 odpovídá vždy za obsah uložených informací v případě, že vykonává přímo nebo nepřímo rozhodující vliv na činnost uživatele.

§ 6

Poskytovatelé služeb uvedení v § 3 až 5 nejsou povinni

a) dohlížet na obsah jimi přenášených nebo ukládaných informací,

b) aktivně vyhledávat skutečnosti a okolnosti poukazující na protiprávní obsah informace.

Šíření obchodních sdělení

§ 7

(1) Obchodní sdělení lze šířit elektronickými prostředky jen za podmínek stanovených tímto zákonem.

(2) Podrobnosti elektronického kontaktu lze za účelem šíření obchodních sdělení elektronickými prostředky využít pouze ve vztahu k uživatelům, kteří k tomu dali předchozí souhlas.

(3) Nehledě na odstavec 2, pokud fyzická nebo právnická osoba získá od svého zákazníka podrobnosti jeho elektronického kontaktu pro elektronickou poštu v souvislosti s prodejem výrobku nebo služby podle požadavků ochrany osobních údajů upravených zvláštním právním předpisem 5) , může tato fyzická či právnická osoba využít tyto podrobnosti elektronického kontaktu pro potřeby šíření obchodních sdělení týkajících se jejích vlastních obdobných výrobků nebo služeb za předpokladu, že zákazník má jasnou a zřetelnou možnost jednoduchým způsobem, zdarma nebo na účet této fyzické nebo právnické osoby odmítnout souhlas s takovýmto využitím svého elektronického kontaktu i při zasílání každé jednotlivé zprávy, pokud původně toto využití neodmítl.

(4) Zaslání elektronické pošty za účelem šíření obchodního sdělení je zakázáno, pokud

a) tato není zřetelně a jasně označena jako obchodní sdělení,

b) skrývá nebo utajuje totožnost odesílatele, jehož jménem se komunikace uskutečňuje, nebo

c) je zaslána bez platné adresy, na kterou by mohl adresát přímo a účinně zaslat informaci o tom, že si nepřeje, aby mu byly obchodní informace odesílatelem nadále zasílány.

Regulované činnosti

§ 8

(1) Osoby vykonávající regulované činnosti mohou za použití elektronických prostředků v rámci činností, které jsou obsahem regulované činnosti, šířit obchodní sdělení, a to v souladu s § 7 a v souladu s příslušnými pravidly vydávanými obchodními, profesními a spotřebitelskými sdruženími, která upravují zejména nezávislost, důstojnost, čest povolání a poctivý přístup k zákazníkům.

(2) Osoby vykonávající regulované činnosti, jež nejsou členy profesních samosprávných komor zřízených zákonem, při šíření obchodních sdělení za použití elektronických prostředků v rámci činností, které jsou obsahem regulované činnosti, postupují v souladu s § 7.

(3) Obchodní sdělení osob vykonávajících regulované činnosti musí obsahovat název profesní samosprávné komory zřízené zákonem, u níž je osoba vykonávající regulovanou činnost zapsána, odkaz na profesní pravidla uplatňovaná v členském státu Evropské unie, v němž je osoba vykonávající regulovanou činnost usazena, a způsob trvalého veřejného přístupu k informacím o příslušné profesní samosprávné komoře zřízené zákonem, jejímž je osoba vykonávající regulovanou činnost členem.

Vnitřní trh

§ 9

(1) Na poskytovatele služby, který poskytuje služby prostřednictvím podniku nebo organizační složky umístěné na území České republiky, se použijí ustanovení tohoto zákona a

zvláštních právních předpisů upravujících podmínky zahájení a výkonu činnosti, která je předmětem poskytované služby, zejména právních předpisů upravujících vznik podnikatelského oprávnění, požadavky na odbornou způsobilost, požadavky na obsah a kvalitu poskytované služby a odpovědnost poskytovatele služby za porušení těchto povinností.

(2) Na poskytovatele služby, který je usazen v jiném členském státě Evropské unie a poskytujícího tuto službu na území České republiky, se nevztahují právní předpisy uvedené v odstavci 1, pokud tento zákon nebo zvláštní právní předpis nestanoví jinak.

(3) Ustanovením odstavce 2 nejsou dotčeny povinnosti poskytovatele služby vyplývající ze zvláštních právních předpisů na ochranu veřejného pořádku, veřejného zdraví, bezpečnosti státu a ochranu spotřebitele.

(4) Dříve, než soud nebo jiný orgán příslušný k zajištění plnění nebo vynucení povinností poskytovatele služby vyplývající ze zvláštních právních předpisů na ochranu veřejného pořádku, veřejného zdraví, bezpečnosti státu a ochranu spotřebitele učiní nezbytná opatření, informuje o tom Komisi Evropských společenství (dále jen "Komise") a požádá členský stát Evropské unie, v němž je poskytovatel služby usazen, o přijetí takových opatření, která budou mít za následek, že soud již nebude muset činit opatření podle tohoto odstavce.

(5) Jestliže se v naléhavých případech soud odchýlí od odstavce 4, podá o této skutečnosti bez zbytečného odkladu informaci s odůvodněním Komisi a členskému státu Evropské unie, v němž je poskytovatel služby usazen.

Dozor nad dodržováním zákona

§ 10

(1) Orgánem příslušným k výkonu dozoru nad dodržováním tohoto zákona (dále jen "orgán dozoru") je

a) pro šíření obchodních sdělení podle § 7 Úřad pro ochranu osobních údajů,

b) pro povinnosti vyplývající z § 8 odst. 3 příslušná profesní samosprávná komora zřízená zákonem.

(2) Orgán dozoru působí jako kontaktní místo pro členské státy Evropské unie a Komisi.

(3) Kontaktní místo pro členské státy Evropské unie a Komisi

a) podává obecné informace o smluvních právech a povinnostech, jakož i o postupech pro podávání stížností a pro opravné prostředky v případě sporů včetně praktických aspektů využívání těchto postupů,

b) poskytuje údaje o orgánech, sdruženích nebo subjektech, od nichž lze získat další informace či praktickou pomoc.

(4) Při výkonu dozoru postupuje orgán dozoru uvedený v odstavci 1 písm. a) podle zvláštního právního předpisu. 6)

(5) Při výkonu dozoru postupují orgány dozoru uvedené v odstavci 1 písm. b) podle zvláštních právních předpisů. 7)

Správní delikty

§ 11

(1) Právnické osobě, která

a) používá elektronické prostředky k šíření nevyžádaných obchodních sdělení,

b) využila podrobnosti elektronického kontaktu pro elektronickou poštu podle zvláštního právního předpisu 5) a neposkytla svému zákazníkovi možnost jasně, zřetelně, jednoduchým způsobem, zdarma nebo na její účet udělit či odmítnout souhlas s využitím jeho elektronického kontaktu pro potřeby šíření obchodních sdělení při zaslání každé jednotlivé zprávy,

c) šířila obchodní sdělení bez prokazatelného souhlasu adresáta,

d) pro účely šíření obchodních sdělení zaslala elektronickou poštu, která nebyla jasně a zřetelně označena jako obchodní sdělení,

e) pro účely šíření obchodních sdělení zaslala elektronickou poštu, která skrývá identitu odesílatele, jehož jménem se komunikace uskutečnila,

f) pro účely šíření obchodních sdělení zaslala elektronickou poštu, která utajuje identitu odesílatele, jehož jménem se komunikace uskutečnila, nebo

g) pro účely šíření obchodních sdělení zaslala elektronickou poštu, která uvádí neplatnou adresu, na niž by adresát mohl odeslat žádost o ukončení takové komunikace, se uloží pokuta do výše 10 000 000 Kč.

(2) Právnické osobě, která

a) vykonává regulovanou činnost a její obchodní sdělení neobsahuje název profesní samosprávné komory zřízené zákonem, u níž je zapsána,

b) vykonává regulovanou činnost a její obchodní sdělení neobsahuje odkaz na profesní pravidla uplatňovaná v členském státu Evropské unie, v němž je usazena, nebo

c) vykonává regulovanou činnost a její obchodní sdělení neobsahuje způsob trvalého veřejného přístupu k informacím o příslušné profesní samosprávné komoře zřízené zákonem, jejímž je členem, se uloží pokuta do výše 1 000 000 Kč.

§ 12

(1) Právnická osoba za správní delikt neodpovídá, jestliže prokáže, že vynaložila veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránila.

(2) Při stanovení výše pokuty právnické osobě se přihlédne k závažnosti správního deliktu, zejména ke způsobu jeho spáchání a jeho následkům a k okolnostem, za nichž byl spáchán.

(3) Odpovědnost právnické osoby za správní delikt zaniká, jestliže orgán dozoru o něm nezahájil řízení do 1 roku, kdy se o něm dozvěděl, nejpozději však do 3 let ode dne, kdy byl spáchán.

(4) Na odpovědnost za jednání, k němuž došlo při podnikání fyzické osoby 8) nebo v přímé souvislosti s ním, se vztahují ustanovení tohoto zákona o odpovědnosti a postihu právnické osoby.

(5) Pokuty ukládá a vybírá orgán dozoru a vymáhá je celní úřad podle zvláštního právního předpisu. 9) Příjem z pokut, a to i vymožených, je příjmem rozpočtu, ze kterého je hrazena činnost orgánu dozoru, který pokutu uložil.

Společná ustanovení

§ 13

(1) Při vybírání a vymáhání pokut se postupuje podle zvláštního právního předpisu. 9)

(2) Pokud tento zákon nestanoví jinak, vztahuje se na řízení ve věcech upravených tímto zákonem správní řád. 10)

ČÁST DRUHÁ

Změna občanského zákoníku

§ 14

Zákon č. 40/1964 Sb. , občanský zákoník, ve znění zákona č. 58/1969 Sb. , zákona č. 131/1982 Sb. , zákona č. 94/1988 Sb. , zákona č. 188/1988 Sb. , zákona č. 87/1990 Sb. , zákona č. 105/1990 Sb. , zákona č. 116/1990 Sb. , zákona č. 87/1991 Sb. , zákona č. 509/1991 Sb. , zákona č. 264/1992 Sb. , zákona č. 267/1994 Sb. , zákona č. 104/1995 Sb. , zákona č. 118/1995 Sb. , zákona č. 94/1996 Sb. , zákona č. 227/1997 Sb. , zákona č. 91/1998 Sb. , zákona č. 165/1998 Sb. , zákona č. 159/1999 Sb. , zákona č. 363/1999 Sb. , zákona č. 27/2000 Sb. , zákona č. 103/2000 Sb. , zákona č. 227/2000 Sb. , zákona č. 367/2000 Sb. , zákona č. 229/2001 Sb. , zákona č. 501/2001 Sb. , zákona č. 317/2001 Sb. , zákona č. 125/2002 Sb. , zákona č. 135/2002 Sb. , zákona č. 136/2002 Sb. , zákona č. 320/2002 Sb. , zákona č. 476/2002 Sb. , zákona č. 8 8/2003 Sb. , zákona č. 37/2004 Sb. , zákona č. 47/2004 Sb. a nálezu Ústavního soudu vyhlášeného pod č. 278/2004 Sb. , se mění takto:

1. V § 53 odstavec 4 zní:

"(4) Při jednání prostřednictvím některého prostředku komunikace na dálku musí být spotřebiteli s dostatečným předstihem před uzavřením smlouvy poskytnuty zejména tyto informace:

a) obchodní firma nebo jména a příjmení a identifikační číslo dodavatele, sídlo právnické osoby a bydliště v případě fyzické osoby, u zahraniční osoby rovněž adresu podniku nebo

organizační složky na území České republiky, byly-li zřízeny, údaj o zápisu v obchodním rejstříku nebo jiné obdobné evidenci, včetně spisové značky, pokud je přidělena, a kontaktní údaje, zejména poštovní adresu pro doručování, telefonní číslo, případně adresu pro doručování elektronické pošty,

b) údaje o příslušném kontrolním orgánu, podléhá-li činnost dodavatele režimu povolování,

c) název a hlavní charakteristiky zboží nebo služeb,

d) cena zboží nebo služeb, z níž jednoznačně vyplývá, zda je uvedena včetně všech daní a poplatků, mají-li k ní být připočítávány,

e) náklady na dodání,

f) způsob platby, dodání nebo plnění,

g) poučení o právu na odstoupení, s výjimkou případů podle odstavce 8,

h) náklady na použití komunikačních prostředků na dálku,

i) doba, po kterou zůstává nabídka nebo cena v platnosti.
K informacím podle písmen a) a b) zajistí dodavatel trvalý veřejný přístup; nedodržení této povinnosti se považuje za nepředání informací podle § 53 odst. 7.".

2. V § 53 se za odstavec 4 vkládá nový odstavec 5, který zní:

"(5) Podá-li spotřebitel objednávku prostřednictvím některého prostředku komunikace na dálku, je dodavatel povinen prostřednictvím některého prostředku komunikace na dálku neprodleně potvrdit její obdržení; to neplatí při uzavírání smlouvy výlučně výměnou elektronické pošty nebo obdobnou individuální komunikací. Objednávka a potvrzení jejího obdržení jsou považovány za doručené, pokud se s nimi strany, jimž byly určeny, mohou seznámit.".

Dosavadní odstavce 5 až 8 se označují jako odstavce 6 až 9.

3. V § 53 odst. 7 se slova "podle ustanovení odstavců 4 a 5" nahrazují slovy "podle ustanovení odstavců 4 a 6".

4. V § 53 odst. 8 se slova "podle odstavce 6" nahrazují slovy "podle odstavce 7".

5. Za § 53 se vkládá nový § 53a, který včetně poznámky pod čarou č. 2c) zní:

"§ 53a

(1) Při použití elektronických prostředků 2c) musí být součástí návrhu kromě informací podle § 53 odst. 3 rovněž informace o tom, zda je smlouva po svém uzavření dodavatelem archivována a zda je přístupná, informace o jednotlivých technických krocích vedoucích k uzavření smlouvy, informace o jazycích, v nichž lze smlouvu uzavřít, informace o možnosti zjištění a opravování chyb vzniklých při zadávání dat před podáním objednávky a informace o kodexech chování, které jsou pro něj závazné nebo které dobrovolně dodržuje, a jejich

přístupnosti při použití elektronických prostředků; to neplatí při jednání výlučně výměnou elektronické pošty nebo obdobnou individuální komunikací.

(2) Před podáním objednávky musí být při použití elektronických prostředků spotřebiteli umožněno zkontrolovat a měnit vstupní údaje v ní obsažené, které do objednávky vložil; to neplatí při jednání výlučně výměnou elektronické pošty nebo obdobnou individuální komunikací.

(3) Smlouva a všeobecné obchodní podmínky musí být spotřebiteli poskytnuty ve formě, která umožňuje archivaci a reprodukci.

(4) Pro odstoupení od smlouvy platí § 53 odst. 7 obdobně. 2c) § 2 písm. c) zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti).".

6. V § 54 se slova "podle § 53 odst. 2 až 8" nahrazují slovy "podle § 53 odst. 2 až 9 a § 53a".

ČÁST TŘETÍ

Změna zákona o regulaci reklamy

§ 15

Zákon č. 40/1995 Sb. , o regulaci reklamy a o změně a doplnění zákona č. 468/1991 Sb. , o provozování rozhlasového a televizního vysílání, ve znění pozdějších předpisů, ve znění zákona č. 258/2000 Sb. , zákona č. 231/2001 Sb. , zákona č. 256/2001 Sb. , zákona č. 138/2002 Sb. , zákona č. 320/2002 Sb. , zákona č. 132/2003 Sb. , zákona č. 217/2004 Sb. a zákona č. 326/2004 Sb. , se mění takto:

1. V § 2 odst. 1 písmeno e) včetně poznámky pod čarou č. 5a) zní:

"e) šíření nevyžádané reklamy, pokud vede k výdajům adresáta nebo pokud adresáta obtěžuje; na šíření reklamy elektronickými prostředky a jeho omezení se vztahuje zvláštní právní předpis, 5a) za reklamu, která obtěžuje, se považuje reklama směřující ke konkrétnímu adresátovi za podmínky, že adresát dal předem jasně a srozumitelně najevo, že si nepřeje, aby vůči němu byla nevyžádaná reklama šířena. 5a) § 7 zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti).".

2. V § 7 písm. d) se za slova "v ostatních případech" vkládají slova " , s výjimkou nevyžádané reklamy šířené elektronickými prostředky 32a) podle zvláštního právního předpisu 5a) ".

Poznámka pod čarou č. 32a) zní:

"32a) § 2 písm. c) zákona č. 480/2004 Sb. , o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti).".

ČÁST ČTVRTÁ

Změna zákona o ochraně osobních údajů a o změně některých zákonů

§ 16

V § 2 zákona č. 101/2000 Sb. , o ochraně osobních údajů a o změně některých zákonů, se na konci textu odstavce 2 doplňují slova "a další kompetence stanovené zvláštním právním předpisem. 1) ".

Poznámka pod čarou č. 1) zní:

"1) § 10 odst. 1 písm. a) zákona č. 480/2004 Sb. , o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti).".

ČÁST PÁTÁ

Změna zákona o zdravotní péči v nestátních zdravotnických zařízeních

§ 17

V zákoně č. 160/1992 Sb., o zdravotní péči v nestátních zdravotnických zařízeních, ve znění zákona č. 161/1993 Sb. , zákona č. 258/2000 Sb. , zákona č. 285/2002 Sb. , zákona č. 320/2002 Sb. , zákona č. 96/2004 Sb. a zákona 121/2004 Sb. , se za § 21a vkládá nový § 21b, který zní:

"§ 21b

Provozovatelé nestátních zdravotnických zařízení, kteří jsou fyzickými osobami a ke dni 31. prosince 2003 účtovali v soustavě jednoduchého účetnictví, splní svoji zákonnou povinnost stanovenou v § 5 odst. 2 písm. e) zákona č. 160/1992 Sb. , ve znění účinném přede dnem nabytí účinnosti zákona č. 121/2004 Sb. , pokud k 1. lednu 2004 vedou daňovou evidenci nebo účetnictví podle zvláštního právního předpisu.".

ČÁST ŠESTÁ

ÚČINNOST

§ 18

Tento zákon nabývá účinnosti dnem jeho vyhlášení.

Zaorálek v. r.

Klaus v. r.

Gross v. r.

1) Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o určitých aspektech služeb informační společnosti, zejména elektronického obchodního styku v rámci vnitřního trhu. Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací.

2) § 3 písm. f) a g) zákona č. 18/2004 Sb., o uznávání odborné kvalifikace a jiné způsobilosti státních příslušníků členských států Evropské unie a o změně některých zákonů (zákon o uznávání odborné kvalifikace).

3) § 2 odst. 2 obchodního zákoníku.

4) Zákon č. 40/1995 Sb. , o regulaci reklamy a o změně a doplnění zákona č. 468/1991 Sb. , o provozování rozhlasového a televizního vysílání, ve znění pozdějších předpisů.

5) Zákon č. 101/2000 Sb. , o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

6) Zákon č. 552/1991 Sb. , o státní kontrole, ve znění pozdějších předpisů.

7) Například zákon č. 254/2000 Sb., o auditorech, ve znění pozdějších předpisů, zákon č. 523/1992 Sb. , o daňovém poradenství a Komoře daňových poradců České republiky, ve znění pozdějších předpisů, zákon č. 220/1991 Sb. , o České lékařské komoře, České stomatologické komoře a České lékárnické komoře, zákon č. 85/1996 Sb. , o advokacii, ve znění pozdějších předpisů.

8) § 2 odst. 2 zákona č. 513/1991 Sb. , obchodní zákoník, ve znění pozdějších předpisů.

9) Zákon č. 337/1992 Sb. , o správě daní a poplatků, ve znění pozdějších předpisů.

10) Zákon č. 71/1967 Sb. , o správním řízení (správní řád), ve znění pozdějších předpisů.