

Je jedním z našich nejvýznamnějších odborníků na „počítačové“ právo, stál u zrodu zákona o elektronickém podpisu, který je považovaný za jeden z nejlepších v Evropě, je členem poradního sboru předsedy Úřadu pro ochranu osobních údajů a členem kolegia ministra informatiky, přednáší na VŠE v Praze a VUT v Brně – **prof. Ing. Vladimír Smejkal, CSc.**, autor řady knih, skript a mezioborových článků z oblasti informatiky a práva. Vladimír Smejkal je rovněž soudním znalcem v oborech ekonomika, kybernetika a kriminalistika (ochrana dat a autorské právo). Je členem Společnosti pro kriminalistiku a v roce 2004 byl jmenován členem Legislativní rady vlády. ►

# PROBLÉMEM

Jarmila Frejtichová

# INTERNETU JE ABSENCE

# ODPOVĚDNOSTI



### **Jak se masové rozšíření počítačů a internetu odrazilo v legislativě?**

Počítače a především internet přinesly novou kvalitu a zcela nové možnosti do lidského života. Domnívám se, že jde o jeden z největších přelomů v dosavadní historii lidstva. Pronikání IT do společnosti se tedy nutně odráží i v legislativě, která musí reagovat na možnosti provádění veřejné správy prostřednictvím moderních informačních technologií (jak se dnes poněkud módně říká e-government). Podobně musí legislativa reagovat i na to, že v soukromoprávních vztazích se nakládá s informacemi, autorskými právy nebo že lze smlouvy uzavírat na dálku, zejména prostřednictvím internetu.

Ideálem je legislativa technologicky neutrální, která by byla obecně platná a kterou by nebylo třeba měnit vzhledem k vývoji vědy a techniky. Ne vždy je to ale možné – například v odvětví trestního práva. Často jsou právníci kritizováni za to, že reagovali se zpožděním, že nepředvíдали další vývoj chování lidí – ať už v souvislosti s IT nebo třeba s lehkými topnými oleji. Jenže to je hluboký omyl. Právo sice představuje normativní systém, ale tento systém, dle mého názoru, není schopen předem předvídat vývoj technologií nebo všechny možné změny v chování lidí. Nutně tedy, a to se týká především vývoje lidského poznání a technologických možností, může legislativa teprve následně reagovat na jejich výskyt či změny a činit taková opatření, aby byl odstraněn nežádoucí, třeba i jen potenciální stav.

### **Jaké nové druhy kriminality s sebou počítače a internet přinesly?**

Hlavními druhy „nové“ kriminality jsou podvody, spočívající v pozměnění dat, programu, identity uživatele a podobně, dále útoky na technické a programové prostředky, respektive data – jedná se zejména o činnost hackerů, viry, útoky typu DoS a DDoS; mezi počítačovou kriminalitu patří i porušování autorských práv, a to jednak k počítačovým programům, jednak ke všem druhům děl, která jsou často protiprávně šířena v digitální podobě na internetu. Zmínil bych ještě neoprávněné nakládání s osobními údaji v informačních systémech a konečně řadu dalších deliktů, které jsou páčány v důsledku levného, snadného a účinného šíření informací prostřednictvím internetu (pomluvy, poškozování cizích práv, nekalá soutěž a porušování práv k ochranné známce, obchodnímu jménu a chráněnému označení původu, šíření toxikomanie, hanobení národa, etnické skupiny, rasy a přesvědčení, podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod, podpora a propagace hnutí směřujících k potlačení práv a svobod člověka).

### **Které z „počítačových“ zločinů považujete za nejnebezpečnější?**

Neumím vybrat nejnebezpečnější – to záleží na okolnostech. Například útok typu DDoS, který „sestřelí“ počítač řízení letového provozu nebo zavře pacientům na JIP kyslík, představuje naplnění skutkové podstaty trestného činu obecného ohrožení a dovedu si představit teroristický útok spáchaný tímto způsobem. Na druhou stranu pomlouvačné informace šířené o fyzické nebo i právnické osobě mohou vést k sebevraždě člověka nebo útoku na banku vedoucí k jejímu úpadku. Takové případy se již u nás staly.

### **Co znamená anonymita internetu pro kriminalitu a boj proti ní?**

Jak jsem uvedl výše, anonymita internetu, současně s jeho další podstatnou vlastností, tzv. distančním přístupem, tedy možností páchat trestné činy na dálku, jsou vysoce kriminogenními faktory. Něco jiného je si vzít klacek a jít skolit majitele nadité peněženky do lesíku u Hlavního nádraží a něco zcela jiného je stisknutím kláve-

sy okrást banku nacházející se na druhém konci světa. Druhá možnost je z hlediska dopadení pachatele a zajištění důkazů, postačujících k odsouzení, daleko obtížnější, byť ne absolutně nemožná. Dle mého názoru se bude muset vytvořit jasný předěl mezi anonymními a neanonymními uživateli a k některým věcem, zdrojům, na některé adresy nebo do celého určitého adresního prostoru (např. do připravovaného IPv6?) by se měli dostat pouze identifikovatelní (nikoliv nutně identifikovaní!) uživatelé. Současné celosvětové trendy za zvyšování bezpečnosti se budou muset nutně odrazit i v přístupu k internetu.

### **Jak se podle vás bude vyvíjet internet v budoucnu? Podaří se najít nějaký rozumný obchodní model na internetu? Stane se velmi výnosnou profesí vyhledávání opravdu relevantních informací? Nebo bude internet rájem grafomanů a šilenců?**

V současné době je internet jak cenným zdrojem informací, tak rájem grafomanů a šilenců. Největší problém je ověřit pravost a přesnost informací. Absolutní anonymita či možnost falešné identity, kterou internet podporuje či umožňuje, je podle mého názoru hlavní překážkou dalšího rozvoje internetu rozumným směrem.

Co se týká obchodování na internetu, zde je situace obtížná již ze samotné podstaty tohoto média. Plnohodnotně lze obchodovat pouze s těmi komoditami, které nejsou závislé na transportu kupovaných věcí (zboží). Můžeme obchodovat s informacemi a právy (k cenným papírům, k nemovitostem, k programům atd.), ale nemůžeme si prostřednictvím protokolu TCP/IP nechat doručit pizzu nebo automobil. Internet je v drtivé většině případů pouze tržištěm (ovšem zajímavým tržištěm – viz takový eBay) nebo zásilkovým obchodem, někdy docela nudným. Dokud nebude objevena skutečně reálná teleportace předmětů, obávám se, že se bude internetový obchod rozvíjet pouze tam, kde bude podstatou obchodování práce s informacemi.

### **Dá se nějak řešit rozpor mezi „globalitou“ internetu a rozdílnou legislativou jednotlivých států?**

Dá, ale mezinárodní společenství si to bohužel zatím uvědomuje velice málo. Navíc jakákoliv snaha vnést určitý řád a pořádek do internetu je obvykle ihned označována za „zavádění cenzury“ – což je ale úplně o něčem jiném. Určité dílčí kroky jsou činěny v rámci „acquis communautaire“ Evropských společenství, což ale vzhledem k tomu, že těžiště internetového provozu je především v USA a v Asii, není příliš podstatné. Domnívám se, že se velice blíží doba, kdy bude muset být přijata mezinárodní smlouva o internetu podobně, jako byla v roce 1962 přijata Úmluva o volném moři, v roce 1967 Smlouva o zásadách činnosti států při výzkumu a využívání kosmického prostoru nebo v roce 1985 Úmluva o mezinárodní železniční přepravě.

### **Co soudíte o pokusech o cenzuru internetu?**

Je třeba rozlišovat skutečnou cenzuru, tak jak je prováděna v totalitních režimech, a to, co je za pokusy o cenzuru internetu označováno v rozvinutých demokraciích. Podle mého názoru se mylně zaměňuje cenzura s požadavkem odpovědnosti (také lze říci s neodmítnutelností odpovědnosti). Souhlasím s tím, že mezi základní lidská práva patří právo na svobodu vyjadřování. Ale jen pokud tímto vyjadřováním neporušují jiná práva dalších osob; pak musí nastoupit standardní represivní mechanismus správního nebo trestního řízení. Tak to funguje bez ohledu na technologii – tedy jak na papíru, tak na internetu. Problém je právě v absenci odpovědnosti, což je na internetu daleko snadnější, než v reálném světě; pokud

budou existovat na internetu servery, webové stránky či jiné informační zdroje, za které nebude nikdo nést odpovědnost, respektive bude se skrývat, pak snaha o jejich odstranění či identifikaci nemůže být – zdůrazňuji v demokratických režimech – označována za pokusy o cenzuru.

### Jak hodnotíte nový antispamový zákon?

Zákon o některých službách informační společnosti je trochu typický europrodukt. Řada věcí v něm je zbytečných, protože by šly odvodit ze stávajícího právního řádu, ale ničemu neškodí. Směrnice ES, které zákon převádí do našeho právního řádu, ale mohly být zapracovány novelami existujících zákonů, nemusel být vydáván zákon nový, samostatný a o několika málo paragrafech.

Vlastní antispamové ustanovení (§ 7) je nicméně vysoce žádoucí. Vzhledem k tomu, že podobná právní úprava bude muset být přijata ve všech zemích EU, dá se očekávat snížení nevyžádaných sdělení přicházejících z těchto zemí. Ale protože drtivá většina spamů pochází ze zámoří, stejně – dokud nedojde k přijetí mnou zmiňované mezinárodní úmluvy o internetu – to pomůže tak z 10 %.

### V čem je největší úskalí dodržování autorského zákona v oblasti IT?

Ve snadnosti, s jakou se lze zmocnit digitalizovaného či digitálního autorského díla (audio či videonahrávky, programu, ale i čehokoliv jiného, co je chráněno autorským zákonem), aniž by kopie byla sebemeně kvalitní nežli originál, dokonce ani většinou nelze zjistit, že ke zkopírování (tj. krádeži) došlo.

### Domníváte se, že by bylo vhodné zvýšit trestní sazbu, je-li trestný čin proveden pomocí IT?

To jsme s dr. Tomášem Sokolem navrhovali již dříve; podle našeho názoru jde o stejně nebezpečnou zbraň jako mnoho jiných. Pokud

je informační trestný čin spáchán na internetu, tj. takzvaně jiným obdobně účinným způsobem jako prostřednictvím rozhlasu či televize, vyšší trestní sazba existuje již ve stávajícím zákonu. Nový návrh trestního zákona, který zahrnuje i Úmluvu Rady Evropy o počítačové kriminalitě, je přísnější nežli stávající, a navíc obsahuje řadu nových skutkových podstat, tj. definic trestných činů, spáchaných v souvislosti s počítači.

### Dá se nějakým způsobem charakterizovat psychologický portrét pachatele počítačových zločinů?

Jsou to až na výjimky vysoce kvalifikovaní, vzdělaní lidé, často na poměrně významných funkcích, kteří využili své kvalifikace, ale i příležitosti a nedostatečně fungující kontroly v organizaci, k provedení určité nelegální operace, většinou s cílem se obohatit. Vyskytují se – zejména u programátorů – ale i cíle jiné, např. touha (si) něco dokázat, motiv pomsty apod. Velice často svým činem kompenzovali pachatele neúspěchy (nebo domnělé neúspěchy) v pracovní nebo společenské oblasti (konkrétně např. v oblasti vztahů s druhým pohlavím).

### Jaké „počítačové“ zločiny se vám obzvlášť zapsaly do paměti?

Bankovní počítačový podvod v Brně, kdy jsem si byl jistý, kdo je pachatelem, ale během několikahodinového výslechu na policii se nám dotýčný – kvalifikovaný počítačový technik – smál do očí. Bohužel především díky málo razantnímu postupu konkrétních policistů bylo vyšetřování neúspěšné.

### Podarí se v budoucnu zefektivnit boj proti počítačovým virům?

Mohlo by, pokud bude trvalý tlak na odstranění anonymity na internetu a současně pokud budou všichni dopadení pachatelé exemplárním způsobem odstiháni.

### Je dost odborníků pro oblast boje s počítačovou kriminalitou a jaká je jeho úspěšnost?

Podle mého názoru jich není dost – alespoň těch skutečných. Co se týká úspěšnosti – počítačový zločin je poměrně latentní, tj. skrytý. Existují, byť spekulativní, odhady, že na jeden odhalený zločin existuje 100 až 10 000 neodhalených.

### Existují nějaké pověry spjaté s právem v oblasti IT, které vás obzvlášť štve?

Jedna: že zápis na papíru, tj. listina, je bezpečnější, nežli zápis učiněný elektronicky a podepsaný tzv. zaručeným elektronickým podpisem. S tím souvisí i nesmyslný, leč stále často přetrvávající výklad, že „písemně“ znamená na papíru; ve skutečnosti to znamená „zapsáno“ – bez ohledu na nosič informací.

### Myslíte si, že internetové bankovníctví u nás je dostatečně zabezpečené?

Technicky možná ano, byť i k tomu lze mít výhrady. Rozhodně ale ne organizačně, respektive procesně; klienti nejsou dostatečně proškoleni, jaká jim hrozí rizika, případně jsou smlouvy postaveny tak, aby klienti veškerá rizika nesli sami. Chápu sice utilitární chování bank, ale není to správné a dalo by se to považovat za zneužití dominantního postavení nebo za jiné jednání poškozující spotřebitele.

### Používáte elektronické bankovníctví?

V plném slova smyslu ne – ale to berte jako profesionální deformaci. Mám nicméně nastavený mechanismus, který mne nenutí chodit do banky osobně. Je to kombinace více bezpečnostních postupů a faktorů současně.



**Do jaké míry přispívá k počítačové kriminalitě v bankovním sektoru sna-  
ha bank utajit tyto činy před veřejností?**

Ta snaha je legitimní; nikdo nemá rád, když se jeho špinavé prádlo pere na veřejnosti. Problémem je, když to banka ani neoznámí orgánům činným v trestním řízení (protože ví, že se u nás všechno rozkecá). Pak se může vytvářet názor o nepostižitelnosti bankovních počítačových podvodů, což není, a to zdůrazňuji, není pravda.

**Před časem vzbudil rozruch váš návrh určitého „prověřování“ žadatelů  
o registraci domén. Co vás k této iniciativě vedlo a jak byste si představoval tento postup v praxi?**

Velice jednoduše: každá žádost bude prověřena, zda jí nejsou zjevně porušována práva jiných subjektů, a to pohledem do běžných, veřejnosti dostupných informačních zdrojů, jako je evidence ochranných známek a obchodní rejstřík. V případě, že zde bude existovat



starší právo, bude žadatel muset dokazovat, že je oprávněn k registraci stejnojmenné domény, přičemž prioritou dne a hodiny žádosti mu bude, podobně jako tomu je třeba u ochranných známek, v případě úspěchu zachována. Všechny ostatní, nekonfliktní žádosti budou po tomto prověření okamžitě provedeny.

Toto je velice minimalistický postup, který by nicméně zamezil většině zjevných porušování cizích práv. Bohužel jsem byl zcela nesmyslně obviněn ze snahy zavádět cenzuru na internetu a ministerstvo informatiky se poté zaleklo jakkoliv se ve věci angažovat. Nicméně změna ve vedení CZ.NIC, kterou považuji za prospěšnou, by mohla vrátit tuto myšlenku do hry.

**Jak hodnotíte situaci kolem elektronického podpisu u nás?**

Z legislativního hlediska je velmi dobrá, dokonce bych řekl až výborná. Před rokem byl náš zákon o elektronickém podpisu vyhodnocen jako jeden z nejkompatibilnějších v zemích EU a poslední novela obsahuje novinky, kterými se dostáváme úplně na špičku (časové razítko, elektronické značky a především elektronické veřejné listiny). Chybí ale větší množství uživatelů, neboť chybějí aplikace a ty nejsou proto, že je málo uživatelů. Tento začarovaný kruh by měla prorhnout vláda, např. vydáváním elektronických občanských průkazů nebo alespoň elektronických průkazek sociálního pojištění, které budou obsahovat i data pro podepisování (klíč a certifikát). Bohužel negativní roli zde hraje i váhavý postup drtivé většiny zdravotních pojišťoven a finančních institucí.

**Jak hodnotíte působení ministerstva informatiky? Byl jeho vznik a existence přínosem? Co říkáte na názory z řad ODS, že by mělo být zrušeno?**

Nacházíme-li se v době informační společnosti a informační systé-

my se nás dotýkají prakticky na každém kroku, pak by bylo divné, nemít ústřední správní orgán, který by se touto problematikou zabýval. Mohli bychom se totiž jinak stejně ptát, proč tedy máme například ministerstvo dopravy nebo ministerstvo zdravotnictví. Problematicku státu a informatiky sleduji několik desítek let a byl jsem velkým kritikem bývalých institucí, jako Úřad pro státní informační systém resp. jeho nástupce, Úřad pro veřejné informační systémy. Tyto instituce neměly ani jasně vymezenou náplň, ani štěstí na své personální obsazení. Hlavním problémem ale bylo jejich opomíjené postavení v rámci soustavy orgánů státu. Nejednalo se o ministerstvo, v jehož čele by stál člen vlády – tudíž je nikdo nebral moc vážně a ani několik málo užitečných myšlenek, které se zde zrodily, se nepodařilo uskutečnit. Zřízením ministerstva informatiky dal stát jasně najevo, že to tentokrát myslí s informační společností a s e-governmentem vážně.

Pouze a jen člen vlády může svým kolegům „vnucovat“ změny legislativy nebo realizovat průřezové projekty (typu portál veřejné správy) s dostatečnou účinností.

Hlasy v ODS o tom, že by mělo být ministerstvo zrušeno bez náhrady, jsou zcela zpozdilé. Návrhy na opětné sloučení s ministerstvem dopravy nereflktují špatnou zkušenost z minulosti; navíc dnes považuji za legitimní otázku, zda by v takovém případě nemělo být spíše zrušeno ministerstvo dopravy a začleněno do ministerstva informatiky. A konečně k nápadu, že činnost ministerstva informatiky bude dělat nějaké oddělení na Úřadu vlády, lze podotknout, že takové oddělení nebude mít naprosto žádnou pravomoc (Úřad vlády nemá příkazovací pravomoc vůči resortům), a obávám se, že ani kapacitu na cokoli jiného, nežli za peníze daňových poplatníků objíždět zahraniční konference a dívat se, jak to jinde dělají lépe. Jinou otázkou je, zda by nemohlo být ministerstvo informatiky více koncentrováno, zda by nemělo některé činnosti outsourcovat, zda by nemělo anektovat ještě jiné instituce apod. Ale to je o něčem trochu jiném – o reengineeringu či personálním auditu, nikoliv o vyhlídce vaničky i s dítětem. Přiznám se, že nechápu trvalou nechuť ODS vůči informatice, když jinak s mnoha jejími návrhy – především v oblasti ekonomické, sociální a daňové – se ztotožňuji.

Co se týká fungování ministerstva informatiky, pak již zmíněný portál je vynikajícím produktem. Je třeba ocenit legislativní činnost, a to nejen v souvislosti s elektronickým podpisem, ale také vzhledem k zákonu o elektronických komunikacích, byť tento byl v Parlamentu poněkud pošramocen. Uvítal bych razantnější postup vůči jiným resortům v případech, kdy jejich počínání je „antiinformatické“; ale je mi jasné, že za daného rozložení sil ve vládě to asi nebude možné.

**Na čem nyní pracujete?**

S prof. Raisem z Brna připravujeme druhé vydání naší knihy Řízení rizik, s dr. Vaníčkem a doc. Matesem čekáme na schválení definitivního znění zákona o elektronických komunikacích, k němuž budeme psát komentář pro nakladatelství C. H. Beck, kde nás bude také čekat třetí vydání „právně-informatické bible“ Právo informačních a telekomunikačních systémů. Kromě toho musím odevzdat skripta o informačních systémech veřejné správy a samozřejmě pracovat na legislativních problémech, ať již v rámci Legislativní rady vlády, či – jak doufám – na přípravě nového univerzálního zákona o doručování a podávání, který by měl vzniknout v gesci ministerstva informatiky. Přednáším na VŠE v Praze a na VUT v Brně a vedu svoji znaleckou kancelář ([www.znalci.cz](http://www.znalci.cz)). A mám-li ještě trochu času, hýčkáám svého kocoura Felixe, kterému bude letos již 12 let a před několika lety byl v televizi jako největší kocour u nás. 5 0001/jaf ■