

ACTA UNIVERSITATIS BRUNENSIS

IURIDICA

No 344

SPISY PRÁVNICKÉ FAKULTY

MASARYKOVY UNIVERZITY V BRNĚ

řada teoretická

Svazek 344

PRÁVO A EVROPSKÁ INFORMAČNÍ SPOLEČNOST



muni
PRESS

PRÁVO A EVROPSKÁ INFORMAČNÍ SPOLEČNOST

Radim Polčák

Masarykova univerzita, 2009
Brno

Recenzoval: prof. JUDr. Pavel Holländer, DrSc.

Monografické dílo je publikováno jako výsledek dílčího řešení výzkumného záměru Právnické fakulty Masarykovy univerzity č. 0086 „Evropský kontext vývoje českého práva po roce 2004“.

© Radim Polčák, 2009

Masarykova univerzita, 2009

ISBN 978-80-210-4885-0 (brož.)

ISBN 978-80-210-4886-7 (CD-ROM)

OBSAH

Předmluva.....	9
1 Právo z informační perspektivy.....	13
1.1 Informace a entropie.....	13
1.2 Informace jako tvrzení a jako pravidlo.....	15
1.3 Specifika práva jako informačního systému.....	18
1.4 Problém binárního hodnocení informací v právní praxi.....	21
1.5 Základní východiska informačního pojetí práva.....	25
2 Organizace, regulace a legitimita práva v informačních sítích.....	28
2.1 Komplexita internetu.....	28
2.2 Pojmy organizace a regulace.....	31
2.3 Zlatý věk informační sítě.....	34
2.4 Legitimita práva v informačních sítích.....	36
3 Exkurz - československá informační teorie práva.....	42
3.1 Zákonost jako primitivní informační kultura.....	42
3.2 Stroje na právo v československé doktríně – Knapp šedesátých let.....	45
3.3 Právní informatika a instrumentální využití informačních technologií – Knapp sedmdesátých a osmdesátých let.....	50
3.4 Závěrečné poznámky k historii československé právní informatiky.....	51
4 Informační sítě a teritorialita práva.....	55
4.1 Problém delokalizace právních vztahů.....	55
4.2 Trestné činy.....	60
4.3 Soukromoprávní závazky.....	68
4.4 Locus delicti.....	70
4.5 Locus solutionis.....	76
4.6 Patria ve formě „jiná provozovna“.....	78
4.7 Správní jurisdikce.....	83
4.8 Závěrečné poznámky k teritorialitě práva i informačních sítích.....	87
5 Pojem a právní aspekty informační společnosti.....	89
5.1 Pojem informační společnosti.....	89
5.2 Přírozeně hodnotová povaha informační společnosti.....	94

5.3	Strategie budování evropské informační společnosti	97
5.4	Strategie budování informační společnosti v ČR	102
5.5	Strategie budování informační společnosti na úrovni mezinárodního společenství	105
5.6	Závěrečné poznámky k pojmu informační společnosti	107
6	Právní informační toky	109
6.1	Promulgace	109
6.2	Doručování individuálních právních aktů	114
6.3	Elektronická podání	119
6.4	Závěrečná poznámka k právním informačním tokům	125
7	Služby informační společnosti v justici - eJustice	126
7.1	Autoritativní aplikace práva jako informační proces	126
7.2	Elektronizace a proporcionalita efektivity	128
7.3	Pojem elektronického spisu	132
7.4	Kritické momenty elektronizace	135
7.5	Obecné otázky elektronizace	137
7.6	Vybrané konkrétní otázky elektronizace	139
7.7	Závěrečná poznámka k evropskému rozměru elektronizace justice	143
8	Struktura informační společnosti – definiční normy	145
8.1	Pojem definičních norem	145
8.2	Lessigův kód	147
8.3	Regulace prostřednictvím definičních norem	149
8.4	Kódování základních hodnot	153
8.5	Závěrečná poznámka k poměru kódu a právních pravidel	157
9	Struktura informační společnosti - definiční autority	159
9.1	Pojem definičních autorit	159
9.2	Exkurs: Hackeři	162
9.3	Pojem ISP	165
9.4	Odpovědnost ISP	171
9.5	Doménové autority	177
9.6	Vyhledávače	184
	Literatura	188
	Věcný rejstřík	197

PŘEDMLUVA

Znovuzrození právní kybernetiky aneb Inspirace knihou Radima Polčáka

Padesátá léta dvacátého století ohlašují revoluci v řadě vědních oborů – objevem DNA genetika radikálně mění základy biologických věd, matematický obraz kategorie informace v živých i neživých systémech vede ke zrodu kybernetiky. Navzdory dobovému odsudku těchto kopernikovských objevů, označujících je za buržoasní pavědu, na počátku šedesátých let, v dobách politického „tání“ („zlatá šedesátá“, nebyla jenom desetiletím Beatles, Rolling Stones, nové vlny kinematografie, ale i vlny nadšení z nových možností poznání, nových možností vědy), objevuje se v československé teorii práva ojedinělý titul, kniha Viktora Knappa, *O možnosti použití kybernetických metod v právu* (NČSAV, Praha 1963), jež otevírá nový pohled na možnosti vědeckého poznávání „světa práva“.¹ Konečně, úzkou vazbu mezi kybernetikou a právem už v samotných počátcích kybernetického bádání zřetelně formuloval i její zakladatel, Norbert Wiener: „Celý náš právní systém má charakter konfliktu. Je to jakási rozmluva, které se účastní alespoň tři strany – dejme tomu v civilním sporu je to žalobce, žalovaný a právní řád, který je reprezentovaný soudcem a porotou. Tento spor lze považovat za hru v plném slova smyslu, jak ji vymezil J. von Neuman. Je to hra, v níž se žalobce a žalovaný snaží pomocí metod omezených právním řádem, získat na svou stranu sympatie soudce a poroty. V takové hře se advokát jedné strany, na rozdíl od přírody samé, může snažit a také se vědomě snaží, aby vnesl chaos do informací strany, proti níž vystupuje. Snaží se prokázat, že její tvrzení jsou absurdní a vědomě ruší přenos zpráv mezi jeho protivníkem na jedné straně a soudcem a porotou na straně druhé.“²

¹ Knappova práce se stává inspirací pro rozvoj oboru. Viz kupř. A. Kisza, *Model cybernetyczny powstawania i dzialania prawa*. Práce Wroclawskiego towarzystwa naukowego, Wroclaw 1970.

² N. Wiener, *The Human Use of Human Beings*. Cybernetics and Society. 2. Ed., New York 1954. Cit. dle českého vydání: *Kybernetika a společnost*. NČSAV, Praha 1963, s. 111.

Právní kybernetika šedesátých let nesla v sobě ambici zkoumat strukturu tvorby i aplikace práva pojmy odlišnými od tradičních pojmů právní vědy, pojmy entropie, informace, komunikace. Srpen 1968 neznamenal pak pouze nevíтанou přítomnost sovětských tanků a obrněných transportérů v ulicích českých, moravských a slovenských měst, nýbrž – kromě řady jiných věcí – i uzavření prostoru svobodného hledání ve společenských vědách.

Po letech odmlčení se pak právní kybernetika v závěru let sedmdesátých mění na obor zaměřením užší, na právní informatiku, jež si klade za cíl zkoumání automatizovaných systémů právních informací, zejména pak selekčního nástroje jejich vyhledávání, jenž je spatřován v indexování právních dokumentů předpokládajícím tezaurus právních pojmů. Budování tezauru otevírá prostor výzkumu právního jazyka.³ Paralelně právně-informatické bádání inspiruje k teoretické analýze kvantitativních parametrů právního řádu, jakož i informatické analýze právního jazyka, analýze, jež počínaje touto dobou pokračuje až do současnosti.⁴

V letech osmdesátých z prostředí matematiky vychází impulz k hledání aplikací neklasických logik a algebraické lingvistiky v oboru právního myšlení, jako možné cesty k rozvoji konkrétního uplatnění umělé inteligence.

³ Viz kupř. V. Knapp, Právní pojmy a právní terminologie (Právní pojmosloví a názvosloví). Státní správa, č. 4, 1978; tentýž, Některé otázky tvorby tezauru automatizovaného systému právních informací. (Poznámky o právním jazyku), Právník č. 1, 1979.

⁴ Viz kupř. F. Cvrček, F. Novák, J. Donát, Informační systém o čs. právních předpisech - CS LEGSYS. Právník, č. 5, 1991; F. Novák, Péče o právní řád. Právník, č. 10-11, 1995; F. Cvrček, F. Novák, Výzkum v oboru právní informatiky. Právník, č. 2, 1996; F. Novák, Právně informatická podpora legislativy – strukturně analytický přístup. Právník, č. 11, 2001; F. Cvrček, Legisvakance v české legislativní praxi. Právník, č. 7, 2001; F. Cvrček, Základní kvantitativní parametry českého právního řádu. Právník, č. 4, 2006; F. Novák, Parametrizace právního řádu ČR – metodologická východiska. Právník, č. 7, 2006; F. Cvrček, Automatické rozpoznávání právních termínů. Právník, č. 4, 2007; F. Novák, Legislativní dokument, jeho vnitřní struktura, kontextové okolí a možnosti statistické analýzy. Právník, č. 6, 2007; F. Cvrček, Význam rubrik pro rozpoznávání právních termínů v textech právních předpisů. Právník, č. 5, 2008; F. Cvrček, Popis právního řádu na základě lingvistické a právně formální analýzy textů právních předpisů. Právník, č. 6, 2008; F. Novák, Kvantitativní deskriptce práva – základní východiska a parametry legislativy ČR (v období 1918–2006 a 2002–2006). Právník, č. 8, 2008; F. Novák, Legislativa ČR v roce 2007 – kvantitativní přehled. Právník, č. 2, 2009.

Co u nás zůstalo přítomno pouze v diskusích nadšenců, v zahraničí se zformovalo v ucelený směr vědeckého bádání.⁵

Něžná revoluce, pád železné opony, v oboru informatickém předznamenal přístup k moderním informačním technologiím, mnoholeté právně-informatické bádání vstupem full-textových prohlížečů v okamžiku pozbylo na relevanci, právní informatiku a s ní spjaté vědecké bádání nahradily komerčně mimořádně úspěšné automatizované systémy právních informací.

Fenomén internetu v letech devadesátých přináší pojem kyberprostoru, nese sebou zrod řady jevů, jež nutí k domýšlení jejich právních důsledků. Objevuje se nový impulz právně-kybernetického bádání.

Radim Polčák se ve své knize vrací ke Knappovým začátkům, upozorňuje na straně jedné na dobovost jeho úvah, na straně druhé zároveň na jejich komplexitu a dopad informatického vnímání práva na pochopení řady jevů spjatých s jeho působením ve společnosti. V tomto směru Polčák na Knappa navazuje, jeho cílem není parciální, nýbrž mnohostranný průnik do vztahů kyberprostoru, informatiky a práva. Právní filozofie mu slouží jako poznávací východisko, Humova teze představuje pro něj metodologický základ členění informací. Základní právně-teoretické pojmy podrobuje informatické analýze: Formuluje řadu tezí. Ilustrativně vybírám v této souvislosti tři: Dle první „platnost sama o sobě nevyovídá o kvalitě pravidla, resp. o jeho schopnosti snížit společenskou entropii“. Dle další „můžeme sice vymezit informaci jako protiklad k entropii a organizaci jako protiklad k chaosu, při definici pojmu regulace však žádnou jednoznačnou paralelu či kontradiktornost v tomto směru nalézt nelze“. Dle třetí „smyslem současných oficiálních komunikačních kanálů, jimiž stát informuje adresáty právních pravidel, ani zdaleka není organizovat společnost pod jurisdikcí příslušného suveréna“, nýbrž „naopak, a poněkud paradoxně, tyto kanály slouží *per se* pouze k legitimaci platnosti příslušného normativního obsahu“. Upozorňuje na řadu konsekvencí informatických aplikací pro fungování práva, počínaje elektronickými podáními, přes elektronické doručování rozhodnutí, až po vytváření elektronického spisu, nebo elektronické přidělování soudní agendy

⁵ Viz kupř. G. Sartor, *Artificial Intelligence and Law: Legal Philosophy and Legal Theory*. Oslo 1993, příp. časopis *Artificial Intelligence and Law* (Ed. K.D. Ashley; G. Sartor; A. Os-kamp), nakl. Springer.

Předmět jeho úvah začasťe určují protiklady a napětí. Polčák naléhavě upozorňuje na rozpor mezi univerzalitou kyberprostoru a teritoriálním i personálním omezením vnitrostátního práva, dopadající jak na obor práva soukromého, tak i veřejného, zvláště pak práva trestního.

Za mimořádně důležitý považují pohled na informační společnost, jenž přerůstá původní přístup Wienerův, dle něhož „informační infrastruktura a wienerovská matematicko-logická metodika zpracování informací jsou samy o sobě bezhodnotové“. Polčákova argumentace vede ale k formulaci odlišné teze: „informační společnost není *per se* bezhodnotová“ – omezení svobody informací a nastolení autoritativních systémů představují spojené nádoby. Nakonec, myslím, že i úvaha o poměru kódu a právních pravidel je ve své hlubinné úrovni vlastně úvahou o vztahu morálky a práva ...

Kniha Radima Polčáka stojí za přečtení: je zvidavou sondou do mnoha průsečíků kybernetiky, informatiky, kyberprostoru a práva, je v ní přítomno nadšení z nových výzev, jakož i, což je pro mne, jenž nepatří již – žel – mezi ročníky nejmladší, zvláštní hodnotou, je v ní přítomno spojení intelektuálního étosu s morálním imperativem.

Pavel Holländer

1 PRÁVO Z INFORMAČNÍ PERSPEKTIVY

1.1 INFORMACE A ENTROPIE

Kybernetika je popisována jako věda o organizaci systémů, o řízení procesů, o umělých organismech a podobně. To vše je samozřejmě pravda, ale právníkovi zřejmě k pochopení jejího smyslu a účelu nejlépe poslouží jednoduchá a o to brilantnější úvaha Neffova, totiž, že kybernetika je o podstatě života a jeho umělém napodobování⁶.

Dnes známe kybernetiku spíše jako teoretickou či častěji aplikovanou vědu technického charakteru. I z tohoto důvodu není již pro právníky nikterak zvlášť zajímavá – snad jen pouze tehdy, pokud přinese jako produkt cosi použitelného k usnadnění rutinní právnické praxe. Původně však stála kybernetika někde na pomezí přírodní vědy a filozofie a sám její zakladatel Norbert Wiener se ve svých publikacích vedle řešení konkrétních problémů zhusta zabýval z hlediska filozofického i její samotnou koncepcí a směřováním.

Původním cílem kybernetiků bylo, jak uvedeno výše, pochopit podstatu života a následně se pokusit o jeho umělé napodobení. Patří-li tedy dnes mezi nejvíce viditelné obory kybernetiky robotika a mechatronika, jedná se stále o pokračování vytyčeného kurzu, tj. inspirace životem a vytváření jeho umělých (tj. lidmi vytvořených anorganických) obrazů.

Zkoumání živých organismů bylo od počátku vedeno snahou o objevení jejich unikátních znaků ve srovnání s neživou anorganickou přírodou. Přitom jsme došli k objevu, že život, na rozdíl od všeho ostatního, nepodléhá druhému zákonu termodynamiky, tj. entropii.

Entropie jako univerzální zákon způsobuje, že libovolné systémy, pokud jsou ponechány ladem, s postupem času ztrácejí svoji organizovanost a dochází k jejich rozkladu. Mezi právníky se stal populárním příklad, který

⁶ Viz Neff, V. Filozofický slovník pro samouky. Praha: Mladá fronta, 1993, str. 182 a násl.

jsme použili už dříve⁷, ten se zvětrávajícím pivem. Je-li pivo (správně) natočené, tedy zorganizované do sklenice, má určitý stupeň vnitřní organizovanosti, který se však s postupem času ztrácí, tj. pivo větrá, ztrácí chuť⁸ a podobně. Obdobně pak mají například i nejrůznější chemické sloučeniny svůj poločas rozpadu, po jehož uplynutí dojde k jejich rozkladu na jednotlivé složky (které se pak rozpadají dále).

Entropie je ve své podstatě termodynamickým zákonem, z čehož vyplývá, že fyzikálně tento děj souvisí s teplotou zkoumaného objektu. Jednoduše tak lze dospět k závěru, že entropii můžeme potlačit tím, že objekt zkoumání zmrazíme – v tomto stavu zůstane stále stejný. Podařilo-li by se nám tedy zmrazit naše pivo na absolutní nulu a takto jej i uchovat, udrží si navěky své (skvělé) vlastnosti.

Pojem entropie ve vztahu k živým organismům výtečně rozpracovává laureát Nobelovy ceny za fyziku Erwin Schrödinger⁹. K pojmu přitom uvádí (překlad autor):

„Dovoľte mi nejprve zdůraznit, že v případě entropie nejde o nějaký mlhavý koncept či myšlenku, ale o měřitelnou fyzikální hodnotu. (-) Za teploty rovnající se absolutní nule (něco okolo -273°C) je entropie zkoumaného vzorku nulová. Když vzorek převedeme do jiného stavu pomalými drobnými vratnými kroky (-), entropie vzroste o to, co můžeme vypočítat podílem každé drobné části tepla, kterou jsme museli vzorku dodat a absolutní teploty, v níž k dodání došlo a následným sečtením takto získaných hodnot. (-) Z toho můžeme vidět, že entropii měříme v kaloriích na stupeň Celsia (cal/C).“

Zde je možné namítnout, že i živý organismus stárne a že každý život končí smrtí, tj. že ani život tedy entropii není s to odolat. Pro jednotlivý organismus to samozřejmě platí, ale život sám nemá přirozenou tendenci zaniknout, ale naopak dále se rozvíjet. Tato tendence se pak projevuje rozmnožováním živých organismů, jejich generačním vývojem reagujícím

⁷ Viz Kühn, Z., Bobek, M., Polčák, R. Judikatura a právní argumentace. Praha: Auditorium, 2006, str. 143.

⁸ V tomto bodě je třeba přiznat, že toto kritérium může být značně subjektivní a bylo použito spíše pro ilustraci. Je nesporné, že existuje řada značek, jimž zvětrání nejen neškodí, ale naopak prospívá – když takové pivo necháme (před jeho vyelitím do kanálu) trochu zvětrat, může se nám dokonce zdát, že jeho chuť se mírně vylepšila.

⁹ Citace byla převzata z populární útlé publikace Schrödinger, E. What is Life. Cambridge: Cambridge University Press, 1992. Dílo je dostupné i on-line na adrese <http://home.att.net/~p.caimi/Life.doc>.

na měnící se podmínky¹⁰ a podobně. Ne nadarmo jsou pak nejsilnějšími pudy živých organismů pud sexuální a též pud sebezáchovy – ve skutečnosti se přitom nejedná o nahodilé pudy každého jednotlivce, ale o přirozené projevy života jako takového¹¹.

Necháme však úvah o tom, jaká síla má život k tomu, aby entropii odhodlaně čelil, a zaměříme se spíše na to, jaký prostředek k tomu život používá. Jinými slovy nás zajímá, jaký nástroj je s to entropii zastavit nebo ji dokonce snížit. Odpověď na tuto otázku je přitom jednoduchá – tím nástrojem je informace¹². Dle jedné z definic informace je dokonce možné ji považovat za přímý protiklad entropie.

Sám Norbert Wiener o informaci píše¹³: „Právě tak, jako entropie je mírou dezorganizace a neuspořádanosti, informace je mírou organizace, uspořádanosti, a že informaci tedy lze chápat jako zápornou entropii; a že stroj, obdobně jako živý organismus nebo informacemi řádně řízené lidské společenství, je zařízení, jež bojuje proti obecné tendenci k vzrůstu entropie.“

1.2 INFORMACE JAKO TVRZENÍ A JAKO PRAVIDLO

Není nikterak překvapivé, že podobně, jako je tomu v přírodních procesech, funguje informace i v sociálním prostředí. Nemůžeme zde sice hovo-

¹⁰ Schopnost adaptace považují dokonce někteří autoři za nejdůležitější vlastnost života – srov. např. Grand, S. *Creation – Life and How to Make it*. Cambridge: Harvard University Press, 2001, str. 104 a násl.

¹¹ Tyto pudy můžeme vidět nejen u živých organismů, ale dokonce i u jejich jednotlivých elementů – až zarážející je pak například sledovat snahu o přežití a reprodukci na základní úrovni života, tj. u jednotlivých částí genetického kódu – k tomu viz například strhující pojednání o lidském genomu v Ridley, M. *Genom*. Praha: Portál, 2001, str. 109 a násl.

¹² Tuto zásadní kvalitu informace reflektují mimo jiní i kritické směry v právním myšlení, které odmítají absolutní a restriktivní pojetí práv duševního vlastnictvím – z mnoha publikací na toto téma viz například Drahos, P., Braithwaite, J. *Information Feudalism – Who Owns the Knowledge Economy?* New York: New Press, 2007. K argumentům založeným na organizační kvalitě informace přitom neexistují relevantní protiargumenty, a to ani ekonomického charakteru.

¹³ Viz Wiener, N. *Cybernetics: Or the Control and Communication in the Animal and the Machine*. Cambridge: MIT Press, 1961, str. 11.

řit o zákonech termodynamiky, ale organizační role informace je mezi lidmi stejná jako kdekoli v živé či neživé přírodě. Sociální systém, kde funguje tvorba, zpracování a distribuce informací, je tak organizovanější, adaptabilnější a v konečném důsledku schopnější přežít a reprodukovat. Naopak společnost, které z nějakého důvodu chybí organizující informace, má přirozenou tendenci podléhat entropii, ztrácet schopnost obstát v soutěži s ostatními a vnitřně se rozkládat.

K tomu, abychom pochopili a mohli popsat důležitost informace pro organizaci společnosti jakožto sociálního organismu, je třeba provést nejprve základní analýzu jednotlivých typů informací. Jako metoda nám v tomto případě může ideálně posloužit tzv. Humova teze¹⁴ dělící svět na doménu bytí (*is*) a mětí (*ought*). V právním myšlení, a nejen tam, našla tato teze dalekosáhlé uplatnění. Nespojitelnost bytí a mětí, tedy i výroků a pravidel, formulovaná a argumentovaná na základní úrovni filozofického systému, se později stala východiskem řady zásadních myšlenkových směrů. I v právním myšlení tak mezi sebou stále soupeří pozitivistické pojetí práva postavené právě na Humově tezi a oddělující od sebe empirickou (tj. *is*) kategorii morálky a normativní (tj. *ought*) kategorii právních pravidel s přístupem přirozenoprávním naopak založeným na odmítnutí této teze a na spojení uvedených dvou základních právních kategorií, tedy práva a morálky.

Přijmeme-li Humovu systematiku, alespoň jako metodologické východisko, můžeme rozlišit informace na dva základní typy – na takové, které popisují skutečnost (tedy to, co je) a pak na instrukce, tedy informace o tom, co být má. Informace o skutečnosti nazýváme výroky a přiřazujeme jim hodnotu pravdivosti.

Pokud vztáhneme kategorii pravdivosti k pojmu informace a budeme vycházet z výše uvedené Wienerovy definice, docházíme k závěru, že pravdivost je nutným předpokladem toho, abychom nějaké sdělení mohli označit za informaci. Jen pravdivá informace je totiž způsobilá snižovat míru entropie příslušného systému. Dostane-li tedy adresát pravdivou informaci, zvyšuje se jeho schopnost reagovat na okolní prostředí a naopak se snižuje pravděpodobnost chybného rozhodnutí. Typickým příkladem mohou být

¹⁴ K základní distinkci mezi bytím a mětím srov. Hume, D. A Treatise on Human Nature. Project Gutenberg, 2003. Volně ke stažení na adrese www.gutenberg.org/etext/4705.

informace o počasí – jsou-li pravdivé, zvyšuje se pravděpodobnost, že jejich adresáti vhodně zvolí oděv a takto adaptovaní budou bezpečnější, výkonnější či spokojenější.

Naopak sdělení, které je nepravdivé, nemůže být *ex definitione* informací, neboť jeho efektem není snížení míry entropie, ale naopak její zachování nebo dokonce zvýšení. Když tedy používáme výrazů jako například „nepravdivá informace,“ jde vlastně o *contradictio in adiecto* – nazýváme-li nějaké sdělení informací, má toto pojmenování implikovat její pravdivost a tím i organizační charakter.

Druhým typem informací jsou ty, které namísto skutečnosti popisují povinnost, tj. pravidla. I tyto informace hrají při organizaci společenského života ústřední roli, neboť i na jejich základě je společnost vnitřně organizována. Nejedná se přitom pouze o normy sdružené do jednotlivých normativních systémů ale též o další pravidla, jakými jsou principy, politiky, standardy apod.¹⁵ Na rozdíl od výroků nepopisují pravidla skutečnost a nelze jim přiřadit hodnotu pravdivosti. Namísto pravdivosti tedy pro kvalitu pravidel používáme kategorii platnosti.

Opět se nabízí srovnání pojmu pravidla s pojmovým vymezením informace. Je-li informace jen takovým sdělením, jehož efektem je snížení entropie, měli bychom za pravidlo v informačním smyslu označit rovněž pouze takové, jehož aplikace má právě tento efekt. Zatímco však jsme výše postavili rovnítko mezi pojmy „pravdivý výrok“ a „informace“, nemůžeme přeci podobně srovnat pojmy „platné pravidlo“ a „informace“, nebo platnost sama o sobě nevypovídá o kvalitě pravidla, resp. o jeho schopnosti snížit společenskou entropii.

K tomu, abychom mohli konstatovat informační kvalitu pravidla, nepostačí tedy jeho prostá formální existence, tj. platnost ve formálním smyslu¹⁶, ale musíme nutně hodnotit jeho materii, resp. způsobilost jeho materie redukovat sociální entropii. Zatímco u výroků je hodnocení jejich informační kvality záležitostí relativně jednoduchou, nedaří se nám stále se shodnout dokonce ani na kritériích posuzování informační kvality pravidel,

¹⁵ Srov. Dworkin, R. M. Když se práva berou vážně. Praha: OIKOYMENH, 2001, str. 43.

¹⁶ K pojmu formální platnosti viz např. Bulín, H. Konstrukce pojmu „právních pramenů“ vůbec a pramenů římského práva zvláště z hlediska ryzí nauky právní, in Weinberger, O., Kubeš, V. (eds.) Brněnská škola právní teorie. Praha: Karolinum, 2003, str. 169.

tj. jejich legitimacy. Zde můžeme připomenout velké teze dějin právního myšlení vymezující informační kvalitu, tj. legitimitu práva, za užití různých kritérií od morálky¹⁷ přes ekonomický efekt¹⁸ až po prostou formální platnost¹⁹. Není přitom náhoda, že striktní formalistický pozitivismus důsledně vycházející z Humovy teze má nejbliže ke spojení kategorie formální platnosti s kategorií legitimacy – zde je však třeba opět připomenout empiricky ověřenou skutečnost, že formálně legitimované pravidlo nemusí mít nutně informační, tedy protientropický, charakter.

K dvojímu chápání informace, tedy jako výroků a pravidel, je třeba ještě dodat, že se v dalším textu budeme zhusta zpronevěřovat výše naznačenému terminologickému purismu. Termín „informace“ tedy budeme s benevolentní licencí k nepřesnosti nadále používat i v kontradiktorních spojeních jako „nepřesná“ či „nepravdivá informace.“ To nám pak umožní zahrnout pod pojem informace i nepravdivé výroky a nelegitimní pravidla, jimiž se z pragmatických důvodů hodláme rovněž zabývat.

1.3 SPECIFIKA PRÁVA JAKO INFORMAČNÍHO SYSTÉMU

Normativní informace, tj. pravidla organizující společnost, mají přes svoji společnou teleologii, tj. snižování míry entropie, různou povahu i formu. Z tohoto důvodu přistupujeme k jejich členění do tzv. normativních systémů. Nejčastější používanou klasifikací je v tomto případě sankční škála, přičemž rozlišujeme mezi normativním systémem práva, u nějž je sankce vymezena a uplatňována státem, sociálními normami sankcionovanými společenstvím, etickými normami působícími pod sankcí svědomí²⁰ a ko-

¹⁷ Srov. Fuller, L. *Morálka práva*. Praha: OIKOYMENH, 1998, str. 37 a násl.

¹⁸ Srov. Posner, R. *The Economics of Justice*. Cambridge: Harvard University Press, 1983, str. 51 a násl.

¹⁹ Srov. Kelsen, H. *Všobecná teorie norem*. Brno: MAsarykova univerzita v Brně, 2000, str. 151 a násl.

²⁰ K tomu podrobně viz např. Hegel, G.W. *Základy filosofie práva*. Praha: Academia, 1992, str. 165.

nečně normami Božími chráněnými sankcí vyšší moci. Z informační perspektivy můžeme rovněž vidět určité společné znaky uvedených normativních systémů, z nichž můžeme rozlišit:

- Tvůrce normativních informací
- Formu normativních informací
- Komunikační prostředek
- Adresáta normativních informací

Specifickým tvůrcem normativních informací právního normativního systému je stát. Přirozenoprávní pohled na právo vnímá v tomto směru stát pouze jako jednotku formulující a distribuující přirozeně existující normativní informace. Touto optikou je tedy právotvorná kompetence státu²¹ pouze oprávněním artikulovat příslušná právní pravidla, resp. dávat těmto pravidlům objektivně vnímatelnou formu a tuto pak komunikovat směrem k adresátům.

V pozitivistickém vidění práva je stát nejen hlásnou troubou právních pravidel, ale přímým a originárním původcem normativních informací. V takovém pojetí tedy stát příslušné normativní informace nejen formuluje a komunikuje, ale přímo a původně vytváří.

Formou právních normativních informací jsou jednotlivé prameny práva. Jako pramen práva přitom označujeme nejen samotnou formu vyjádření právního pravidla, ale též metodu komunikace k adresátovi. Normativní právní akt je tedy příkladně psaným vyjádřením právních pravidel, současně jeho textová forma vymezuje i způsob, jímž se s ním mohou seznámit jeho adresáti.

Pro prameny práva obecně platí, že jejich forma může být různá. Vedle psaných pramenů práva, jejichž primárním smyslem je nést normativní informaci, se tak setkáváme též například s právními obyčejí vyjádřenými nedefinovatelnou formou sestávající částečně z jednání společnosti a částečně z konkludentní aplikační praxe státu. Vzhledem k ambici objektivní

²¹ Kritickou analýzu konceptu legislativy viz např. v Dworkin, R. *Law's Empire*. Oxford: Hart Publishing, 1998, str. 313 a násl.

dává v tomto směru právo jednoznačně přednost tzv. formálně určitým formám – i z tohoto důvodu se můžeme stále častěji setkávat s formální fixací méně určitých pramenů práva, jako jsou právní obyčeje nebo právní principy, do preciznějších forem, jimiž jsou normativní právní akty nebo precedenty.

Jak již bylo zmíněno, souvisí s formou vyjádření právního pravidla též forma, v níž se takové vyjádření dostane ke svému adresátovi. Formálně určité prameny práva pak mají tu výhodu, že je lze komunikovat relativně snadno prostřednictvím standardních a co do kvantity prakticky neomezených kanálů. Takovou komunikaci, která má obvykle písemnou formu, pak lze pro potřeby adresátů i libovolně archivovat, což je důležité především z hlediska formální legitimacy příslušných pravidel.

Oproti ostatním normativním systémům má však právo tendenci k takové formalizaci svých pramenů a jejich komunikace, která mnohdy ztrácí svou původní úlohu, tj. informovat adresáty. To je odrazem výše naznačeného formalistického pojetí informační kvality pravidla jako jeho prosté formální závaznosti. Příslušný informační zdroj, tedy pramen práva, tak v tomto případě do značné míry ztrácí ambici skutečně informovat adresáty a jeho použití je zaměřeno na prostou formální legitimaci příslušného pravidla²².

Tuto tendenci můžeme dobře pozorovat například na Sbírce zákonů České republiky. Skutečnost, že jsou ve Sbírce zákonů chronologicky publikovány především novely právních předpisů, způsobuje, že kromě zpravení několika právních profesionálů o tom, co je nového, již tento kanál prakticky neplní žádnou další informační funkci. Namísto toho, aby tento oficiální pramen skutečně informoval adresáty právních pravidel o jejich právech a povinnostech, tedy slouží akt publikace ve Sbírce zákonů pouze k formálnímu (nikoli už skutečnému) naplnění jedné z formálních náležitostí právo tvorby, tj. publikace a následné dostupnosti právních pravidel - viz dále.

Systém práva se od ostatních normativních systémů liší z informační perspektivy i *a priori* hodnocením informačně-percepčních schopností svých adresátů. Princip *ignorantia legis neminem excusat* totiž předpokládá

²² Můžeme v tomto případě spekulovat, do jaké míry je formálně publikované ale fakticky nečitelné pravidlo skutečně legitimní – stručnou diskusi této otázky provádí např. Zdeněk Kühn in Kühn, Z. Může absence publikace úplného znění zákona odůvodnit jeho protiústavnost? Jiné právo, on-line, jinepravo.blogspot.com, 25. 11. 2007.

totální a dokonalou znalost právních pravidel jejich adresáty. Vzhledem k tomu, že je tento princip založen na výše zmíněné formální publicitě základních pramenů práva, má sám nutně formální charakter. Můžeme tedy stran specifických znaků právního normativního systému uzavřít, že stát jako původce normativních informací (ať už jen ve formě jejich tvorby nebo jen prosté artikulace) v tomto případě používá formálně určitých informačních a komunikačních medií, jejichž skutečný informační efekt nelze srovnat s efektem formální závaznosti. Zatímco se tedy informační struktury ostatních normativních systémů (především systému sociálních norem) přizpůsobují mase a kvalitě normativních informací a využívají k tomu dostupných technologií, ustrnul informační vývoj práva v pozici, která je sice formálně bezpečná ale informačně nefunkční. To pak vede k prohlubování propasti mezi formálními zdroji právních normativních informací a zdroji fakticky užívanými v praxi, které se budeme věnovat v dalších kapitolách.

1.4 PROBLÉM BINÁRNÍHO HODNOCENÍ INFORMACÍ V PRÁVNÍ PRAXI

Zaměříme-li se optikou informační teorie na praktické právní procesy, tj. především na procesy aplikace práva, můžeme opět konstatovat užitečnost metodologického oddělení informací o skutečnosti (výrok) a o povinnosti (pravidlo). V těchto procesech totiž řešíme zpravidla problém poznání pravdy (skutku) a následně její právní kvalifikace, tj. vyvození odpovídajících povinností²³. Zatímco skutkové informace precizují náš rozhodovací proces a umožňují nám adaptovat naše úsilí na okolnosti příslušného přípa-

²³ Zjišťování skutkového stavu a jeho následná subsumpce pod hypotézy příslušných norem samozřejmě nepředstavují nějakou rigidní posloupnost – jedná se spíše o obousměrný komplexní proces postupného vytváření právního obrazu skutečnosti označovaný také někdy jako hermeneutická spirála – k tomu srov. např. Holländer, P. *Filosofie práva*. Plzeň: Aleš Čeněk, 2006, str. 206 a násl.

du, normativní informace poskytuje východisko k jeho perspektivnímu autoritativnímu řešení²⁴.

Z hlediska informační teorie je tedy možné vidět celý proces aplikace práva jako informační proceduru. Vstupními informacemi jsou poznatky o skutkovém stavu a informace o pravidlech, na výstupu se pak po náležitém zpracování objeví informace o *ad hoc* normativním následku. Pokud bychom tento proces chtěli dále rozebrat, bude na straně skutku zdrojem poznání:

- Důkaz (u skutečností prokazatelných)
- Důkaz předpokladu + právní norma (u předpokládaných skutečností, tj. domněnek a fikcí)
- Archiv (u skutečností známých)

Zjevný problém aplikace informační teorie na praktické právní procesy můžeme odhalit z výše uvedeného vcelku jednoduše. Zakladatel moderní kybernetiky Norbert Wiener se totiž zhlédl v metodách matematické logiky²⁵ a nejinak tomu bylo u jeho pokračovatelů včetně právních kybernetiků. Logika, jejímž ústředním motivem je pravda a pravdivost, tedy logika výroková, však pracuje pouze s binárním pojetím pravdy. O výrociích tedy můžeme konstatovat jen, že jsou pravdivé nebo nepravdivé.

Binární pojetí pravdivosti se hodí snad jen pro zjednodušené didaktické příklady typu „je 5 hodin“ nebo „venku prší.“ Život nám však nepřináší tvrzení, o nichž bychom mohli prohlásit, že jsou stoprocentní pravda nebo naopak stoprocentní lež. Takové informace pak hodnotíme spíše pravděpodobnostní úvahou, respektive pracujeme s nimi jako s metaforami. Z hle-

²⁴ Takové řešení se pak samo stává další organizující informací, když v závislosti na kvalitě přináší do práva další regulativ. Na tom je vedle precedenčních systémů založeno například i kontinentální soudnictví pracující s argumentační závazností judikatury.

²⁵ Wiener ve své stěžejní práci skládá holt Leibnizovi, když píše: „Pokud bych měl jmenovat z významných postav historie vědy někoho kmotrem kybernetiky, musel by to být rozhodně Leibniz. Jeho filozofie se totiž soustředila okolo dvou úzce spjatých konceptů – okolo univerzálního symbolismu a matematické logiky.“ Viz Wiener, N. *Cybernetics: On the Control and Communication in the Animal and the Machine*. Cambridge: MIT Press, 1961, str. 12.

diska výrokové logiky se samozřejmě o výroky nejedná (nelze jim přiřadit hodnotu pravda/nepravda), ale často jsou tím jediným, co máme k dispozici pro objasnění skutkového stavu. Dokonce i didaktické příklady typu „krtek umí létat“ lze téměř vždy zrelativizovat²⁶, nemluvě o tvrzeních jako „jsem věrný manžel“ nebo „nechtěl jsem mu tu židli rozbít o hlavu.“ Z toho vyplývá, že informační pojetí skutkové informace má smysl pouze tehdy, pracujeme-li s takovou informací na bázi pravděpodobnosti jejího myšleného významu i její pravdivosti (nikoli tedy s ambicí o ní prostě konstatovat, že je pravdivá nebo naopak nepravdivá).

Problému reprezentace skutečnosti prostřednictvím formálních znaků (výroků, výrazů) se věnuje i výjimečná čtyřdílná česká monografie Umělá inteligence, kde se můžeme dočíst, že²⁷ „zřejmě univerzální tvrzení v běžném životě mají řadu implicitních (nevyřčených) předpokladů, které mnohdy ani při nejlepší vůli nemůžeme vyjmenovat. Jde například o všemožné výjimky, které tvoří jeden ze zdrojů nemonotónnosti běžného uvažování. Samozřejmě, tato zkušenost motivovala vznik dalších formálních systémů, jako je např. nemonotónní logika.

Jiným problémem (-) je nekompromisnost jediných dvou přípustných pravdivostních formulí – pravda a lež. Mnohdy se náš úsudek opírá o pravděpodobnostní hodnocení situace. V takovém případě je třeba uvažovat daleko širší škálu možných hodnot – tímto zobecněním se zabývá neostrá (fuzzy) logika.“

Obdobně jako s výrokovou logikou u skutkových informací pracuje informační teorie práva s deontickou logikou jako s metodou pro zpracování informací povinnostních. Namísto kategorie pravda/nepravda se v tomto případě opět jedná o binární hodnocení, tentokrát však kategoriemi platnost/neplatnost.

I tehdy, pokud bychom odhlédli od permanentního problému interpretace jednotlivých právních pravidel²⁸, musíme i v tomto případě konstatovat, že metody logiky, zde deontické, nejsou s to komplexně pojmout a zpracovat právo. Stejně jako u výroků totiž ani zde nemůžeme celé řadě pravidel

²⁶ V tomto případě můžeme odmítnout výrokový charakter tohoto tvrzení jednoduchým poukazem na to, že když už se člověku podaří krtku na zahradě chytit, naučit ho létat není až takový problém – ani toto tvrzení tedy vlastně nemůže mít hodnotu pravda/nepravda a není výrokem.

²⁷ Viz Mařík, V. Štěpánková, O. Lažanský, J. Umělá inteligence, 1. díl. Praha: Academia, 1993, str. 97.

²⁸ Mezi jeho složky nepochybně počítáme například přirozené limity právního jazyka, rozdílnou úroveň předvedění interpretů, apod.

přihradit kategorii platí/neplatí. Kategorii absolutní platnosti/neplatnosti tak můžeme přiřadit jen ideálním normám, nikoli už však právním principům, standardům a dalším kategoriím, které tvoří bytostnou součást systému práva. Důkazem výše uvedeného může být například styčný bod jinak konkurenčních teorií právních principů Ronalda Dworkina a Roberta Alexyho, kterým je logická distinkce mezi právním principem a právní normou. Zatímco u normy můžeme sledovat binární kvalitu platí/neplatí, principu tyto hodnoty z podstaty přiřadit nelze²⁹.

Je-li konečně implikací platnosti práva jeho závaznost, nelze binární model hodnocení opět použít. S absolutní závazností/nezávazností se totiž setkáme opět pouze u ideálních norem, zatímco praktická právní pravidla často vykazují spíše znaky relativní závaznosti argumentační³⁰. Ani v tomto případě tedy není použití logických metod pro právo ideální a jejich aplikace se tak omezuje na relativně omezenou skupinu právních problémů.

Právě uvedené vytrvale odmítaly logicizující směry právního myšlení, které byly bohatě zastoupeny v socialistickém Československu. Prvoplánová jednoduchost a logičnost komunistické zákonosti byla základem častých přímočarých publikací, kde byly (místy složitě) logicky vyvozovány dopředu zřejmé závěry. Ještě v roce 1985 se tak můžeme na téměř patnácti stranách dočíst o tom, proč je soudní rozhodnutí „*funkcí daného skutkového stavu (S_d), dále též normativní úpravy na daný skutkový stav spadající, tj. stavu právního (N_p) a konečně postupu soudce při hodnocení skutkové a právní stránky projednávané věci (H_{sp})*.“ Tento závěr je pak doplněn o závěrečné konstatování, že „*[r]ozvedení a hodnocení jednotlivých argumentů této funkce včetně jejich hodnot by pro svou složitost vyžadovalo svým obsahem již zcela samostatné rozvedení*.“³¹

²⁹ Srovnání obou koncepcí právních principů se zdůrazněním logické distinkce viz in Holländer, P. *Filosofie práva*. Plzeň: Aleš Čeněk, 2006, str. 143 a násl.

³⁰ Jako příklad můžeme uvést závaznost ustálené soudní interpretace, tj. judikatury – pravidlo vytvořené či dotvořené judikaturou je závazné do té míry, že je při jeho změně třeba argumentovat důvody takové změny. Nejedná se přitom podobně jako u precedentu o závaznost absolutní ale pouze o povinnost soudu se s takovým pravidlem argumentačně vypořádat – srov. Kühn, Z., Bobek, M., Polčák, R. *Judikatura a právní argumentace*. Praha: Auditorium, 2006, str. 39 a násl.

³¹ Toto je skutečný (a jediný) závěr článku Steiner, V. *Logická formalizace právních norem a vztahů*. *Právník*, ročník 124, 1985, číslo 11, str. 1008. Zde je na místě dodat, že skutečnost, že autor, zřejmě z nedostatku místa, uvedené rozvedení dále nerozvedl, jej určitě připravilo o nehybnou slávu a věčné místo v Pantheonu Spravedlnosti.

1.5 ZÁKLADNÍ VÝCHODISKA INFORMAČNÍHO POJETÍ PRÁVA

Shrneme-li, co bylo uvedeno výše, představuje informační teorie práva teoretickou reflexi organizačního charakteru systému právních pravidel. Informační pojmání práva tedy stojí na předpokladu, že právo je souborem státních informací perspektivní povahy organizujících život lidských společenství. Veškeré právní procesy mají pak touto optikou charakter vytváření, sběru, zpracování a distribuce právních informací.

Legislativu lze tedy ve výše uvedeném smyslu charakterizovat jako zpracování informací o potřebách společnosti do formy organizující informace, tj. zákona. I soudce je v tomto směru možné vidět jako zpracovatele (procesor) informací o skutku a právu, z nichž následně vytváří imperativ stranám a v případě publikace může z tohoto procesu vzejít i všeobecné pravidlo. Můžeme si tak vytvořit například následující diagram právních informačních toků:

Společenská objednávka – politik (formuluje společenskou objednávku) – věcný záměr (informační zdroj komunikovaný v rámci přípravy zákona) – legislativec (převede věcný záměr do návrhu paragrafového znění zákona) – zákonodárce (projedná a legitimuje zákon) – sbírka (informační zdroj komunikovaný veřejnosti) – soudce (interpret zákona) – soudní rozhodnutí (informační zdroj komunikovaný stranám) – adresát rozhodnutí.

Jak je vidět, představuje definiční problém práva jako informačního systému už základní disproporce mezi ideální (teoretickou) kategorií informace a její (praktické) komunikovatelné formy. Kelsen tak v souvislosti s právní normou hovoří o nutnosti oddělit od sebe normu a formu, v níž je projevena a komunikována, tj. normativní výpověď³². Jinými slovy je třeba

³² Kelsen k tomu doslova uvádí: „Norma, která je smyslem volního aktu, je významem věty, která je produktem aktu mluvení, kterým smysl volního aktu přichází k vyjádření. Právě tak musí být rozlišován poznávací akt, jehož smyslem je výpověď od aktu vyslovení, kterým je smysl aktu poznání vyjádřen.“ Viz Kelsen, H. Všeobecná teorie norem. Brno: Masarykova univerzita v Brně, 2000. Str. 175.

při analýze oddělit od sebe obsah zákona a jeho text – v našem diagramu pak ještě navíc obsah společenské objednávky od věcného záměru a obsah judikátu od jeho písemného vyhotovení. Důvod k tomu je prozaický a spočívá v omezenosti výrazových prostředků práva na strohé jazykové výrazy, tj. ve výše diskutovaném problému monotónní reprezentace.

Ve srovnání s jinými disciplínami, jejichž smyslem je přinášet společnosti organizující informace³³ trpí právo žalostným deficitem výrazových prostředků. Kvůli ambici monotónnosti a snaze o matematickou (či spíše logickou) preciznost se právní systém zbavil možnosti použít prakticky všech jinde běžných výrazových prostředků kromě strohému jazyka. Adresát právních norem tak nemůže poznat svoji povinnost či odpovědnostní následek svého přestupku z impozantní fresky nebo z tónů hudební skladby, ba dokonce nemůže být právní informace komunikována ani formou jazykových obrazů. Je pak logicky nadmíru složité převést ideální pravidlo (i jen jednoduchou normu) do formy strohému jazykovému vyjádření. I z tohoto důvodu se právo řadě *expressis verbis* výpovědí prostě vyhýbá³⁴ a tam, kde se právotvůrce pokusí o precizní vyjádření příslušného významu, je často výsledkem studená omáčka jako v následujícím příkladu³⁵:

§ 9 písm. c) vyhlášky č. 331/1997 Sb.: „[Pro účely této vyhlášky se rozumí] studenou omáčkou nebo dresinkem tekutý nebo emulzní výrobek používaný jako chuťová příloha k pokrmům a salátům, vyrobený zejména z jedlých olejů, zahušťovadel, stabilizátorů, emulgátorů, zeleniny, ovoce, koření a mléčných výrobků.“

Podobně, jako jsme nuceni pasovat ideální pravidla do často nevyhovujících jazykových vyjádření, musíme i jednotlivé právní informace, jakkoli složité, prostě namačkat do jednoduchých logických kategorií „pravda/nepravda“ nebo „platí/neplatí.“ Důvodem je výše popsána snaha o výrazové

³³ Takovými disciplínami jsou například výtvarné umění, tanec, film nebo třeba televizní vysílání.

³⁴ Příkladem může být absence definice podpisu – přestože se jedná o jeden z nejvíce používaných právních institutů, není jeho podoba nikde vymezena a není tedy paradoxně typickým právním instrumentem.

³⁵ Sofistikovaně rozpracovává tento „problém studené omáčky“ Dworkin, když popisuje interpretační dilemata nešťastného Herkula – viz Dworkin, R. *Law's Empire*. Oxford: Hart Publishing, 1998, str. 313 a násl.

zjednodušení a objektivní preciznost práva, které by mimo jiné umožnily i následnou automatizaci právních informačních procesů.

Oba problematické momenty, tedy okleštění práva o výrazové prostředky a omezení kvalifikace právních informací na jednoduché binární kategorie, představují na jedné straně pro právo a jeho kvalitu (včetně samotné legitimacy) neopomenutelnou hrozbu. Na druhé straně ale tyto tendence svědčí vytvoření jednoduchých kauzálních matematicko-logických metod ke zpracování právních informací. Logické či logicizující pojetí práva pak umožní i jeho kódování do formy zpracovatelné stroji a tím zpřístupní lákavou možnost nahradit živý procesor právních informací (právníka, policistu, ...) přesnou a neunavitelnou mašinou.

Jestliže se právo, ať už na úrovni teoretické, legislativní či aplikační, výše uvedeným tendencím vytrvale a úspěšně brání, je na místě ptát se, co jej k tomu vede. I přes politicky motivované snahy svázat právo jednoduchými kategoriemi a následně jej svěřit strojům³⁶, totiž doposud nenastala situace, kdy bychom mohli prohlásit, že si právo nechává ono sešňěrovávání líbit.

Důvodem toho, proč je právo i přes formalizující snahy přirozeně idealistické a proč vytrvale odmítá přijmout jednoduché kategorie platnosti a pravdivosti, pak může být, na první pohled poněkud paradoxně, jeho informační charakter. V kruhu se tak dostáváme zpět k informaci jako základní jednotce práva a k jejím přirozeným vlastnostem. Mezi nimi totiž vyniká především tendence ke snižování míry entropie u adresátů a právě tato základní teleologie má podle našeho názoru na svědomí, že se právo vytrvale odmítá podříditi uměle vytvořeným kategoriím formální logiky. Z toho pak vyplývá i závěr, že informační pojetí práva nemůže být primárně založeno na binárním chápání kvality právních informací (ať už kategoriemi platnost/neplatnost nebo pravdivost/nepravdivost) a na zpracování objektu zkoumání za užití matematicko-logických formulí. Ani tento na první pohled exaktní přístup k právu se tedy nemůže odklonit od humanitních metod.

³⁶ Těmto tendencím se věnujeme dále v historickém exkurzu.

2 ORGANIZACE, REGULACE A LEGITIMITA PRÁVA V INFORMAČNÍCH SÍTÍCH

2.1 KOMPLEXITA INTERNETU

Vybereme-li si libovolnou z definic informace, jistě bude její součástí alespoň náznak základní její existenční teleologie v tom smyslu, že účelem informací je organizování elementů do systematických celků³⁷. Čeština podobně jako jiné jazyky přitom výraz „organizace“ používá hned ve dvou významech, tj. pro označení procesu ale též instituce. Organizací tedy rozumíme proces utváření systému ale též jeho výsledek, tedy i systém jako takový.

Jakkoli se však oba významy toho slova mohou od sebe lišit, jejich základ je stejný – zatímco organizace ve smyslu procedury označuje komunikaci a implementaci informace, organizace v institucionálním smyslu je výrazem pro její důsledek. V přírodních vědách se pak pro živé formy organizací v institucionálním smyslu používá rovněž výrazu organismus, který opět označuje elementy spojené vzájemnými vazbami do funkčního (to díky informací) celku³⁸.

Výskyt či míru informace v určitém systému lze konstatovat dvěma způsoby. Prvním je analýza jednotlivých elementů se zaměřením na to, zda tyto elementy jsou tvůrci, nosiči či příjemci informací. Logicky pak lze dovést závěr, že informovanost (organizovanost) takového systému bude souhrnem informovanosti jednotlivých elementů. Tento závěr však mnohdy není na místě – nikoli snad proto, že bychom byli schopní teoreticky zdůvodnit jeho vady, ale z toho důvodu, že lze jednoduchým pozorováním odhalit, že tomu tak není. Na vině je přitom tajemná vlastnost středně velkých a zej-

³⁷ Srov. např. Burgin, M. *Information Theory: a Multifaceted Model of Information*, Entropy, číslo 5, 2003, str. 146 a násl.

³⁸ Organizující informací živého světa je genetický kód – k tomu srov. populárně-naučnou publikaci známého genetika a popularizátora této vědy Ridley, M. *Genom*. Praha: Portál, 2001.

ména pak velkých systémů, kterou označujeme jako komplexitu³⁹. Příhodnější metodou ke zjištění míry informovanosti určitého systému tak obvykle nebývá zkoumání jednotlivých elementů ale naopak komplexní analýza celku.

Komplexita je, stručně řečeno, jevem, na jehož základě vykazují velké systémy (organizace v institucionálním významu) vlastnosti odpovídající mnohem vyšší míře informovanosti jednotlivých elementů, než kterou jsme schopní konstatovat jejich důslednou analýzou. Příkladem komplexního systému tak může být třeba mraveniště – mravenci jsou sami o sobě schopní rozeznat, distribuovat a aplikovat jen velmi omezené množství informací. V porovnání s mnohem většími tvory by se dokonce nabízelo poněkud laciné přesto však případné konstatování, že mravenci jsou vlastně docela hloupí. Přestože se jejich schopnosti liší podle jejich funkce a najdeme tedy mravence plnící různé úkoly a pracující s odlišnými typy informací, provedeme-li sumu všech jejich zjištěných schopností, nebude výsledek stále nikterak oslnivý. Změníme-li však měřítko pohledu na mravence z elementárního na komplexní a budeme-li namísto jednotlivých mravenců zkoumat celé mraveniště, zjistíme, že míra organizovanosti (informovanosti) celého systému je doslova úžasná. Způsob, kterým jsou tyto nepatrní tvorové přidělování k jednotlivým činnostem (dělbů práce) či mechanismus shromažďování a následného rozdělování zdrojů (logistiku) by jim mohla závidět většina podniků nebo veřejných korporací. Architektura mraveniště, jeho jednoduchost a zároveň konstrukční dokonalost pak může dohnat k pocitu méněcennosti nejednoho architekta či stavitele. To vše však uvidíme až tehdy, povzneseme-li se nad úroveň elementů a přistoupíme-li k analýze funkčního celku.

Jiným příkladem mohou být takzvané celulární automaty⁴⁰. Jedná se v podstatě o jednoduché matematické simulace, kdy je nejprve definováno prostředí (například černobílá čtvercová mřížka), do něž je pak ve formě jednoduchého vzorce vložena organizující informace. Když se pak tímto

³⁹ K pojmu viz např. populární publikaci Peter Coveneye a Rogera Highfielda *Frontiers of Complexity: The Search for Order in a Chaotic World*, která byla přeložena do češtiny a vydána jako Coveney, P., Highfield, R. *Mezi chaosem a řádem*. Praha: Mladá Fronta, 2003, str. 217 a násl.

⁴⁰ Viz tamtéž, p. 112 a násl.

způsobem celý automat „nastartuje“,“ dochází zpravidla ke generačnímu vývoji vykazujícímu v komplexním pohledu fascinující vlastnosti – mnohdy to vypadá, jako by namísto banálně jednoduchého vzorce určoval rozložení černých a bílých polí nějaký malíř nebo filmový režisér.

Nejznámějším příkladem je automat známý jako Game of Life navržený Johnem Hortonem Conwayem⁴¹. Je rozložen na čtvercové mřížce a pravidla generační selekce jsou následující:

- Živá buňka s počtem živých sousedů menším než dva zaniká.
- Živá buňka s počtem živých sousedů větším než tři zaniká.
- Živá buňka s počtem živých sousedů dva nebo tři přežívá do další generace.
- Mrtvá buňka s počtem živých sousedů tři se mění na živou.

Aplikací těchto jednoduchých pravidel v jednotlivých generacích vývoje celulárního automatu dochází k vytvoření obrazce libovolné velikosti. Původní informaci organizující jednotlivé elementy (vzorec) můžeme sice i zde analyzovat, ale nic překotně zajímavého tím nezjistíme. Stejně tak nezjistíme prakticky nic ani analýzou jednotlivých elementů – jedná se totiž pouze o bílé nebo černé čtverce. Odhlédneme-li však od elementární roviny, můžeme v komplexním pohledu poznat ohromující krásu a dynamiku tohoto ve své podstatě úplně jednoduchého procesu.

Oba uvedené příklady, tj. mraveniště a celulární automat, nás vedou k poznání, že informovanost či organizovanost určitého systému nemusí být nutně jen záležitostí jednotlivých jeho elementů, ale systém sám (nikoli jen jeho elementy) může být díky komplexitě původcem i adresátem organizujících informací. Není přitom vždy nutné a mnohdy ani možné poznat organizující mechanismy analýzou jednotlivých elementů příslušného systému, mnohdy postačí či je dokonce nutné míru a kvalitu celkové organizace prostě empiricky konstatovat na základě komplexního pohledu.

Z výše uvedeného vyplývá, že internet je v současné době díky jeho složitosti možné vidět jako komplexní systém. Chceme-li tedy zkoumat informační mechanismy zajišťující jeho organizaci, právo nevyjímaje, je na místě aplikovat přístup naznačený výše. Nelze však bezesbytku a *a priori*

⁴¹ Podrobněji se vysvětlení funkce automatu věnuje například internetová stránka Wonders of Math, jež je součástí internetového portálu math.com. Na adrese <http://www.math.com/students/wonders/life/life.html> je pak možné i vizuálně spustit tento automat s libovolným počátečním nastavením (systém nabízí dokonce i několik přednastavených startovacích obrazců).

vyjít ze skutečnosti, že internet je informačním prostředím a z definice je tedy možné považovat jej za perfektně organizovaný. Ne každé sdělení, zpráva či instrukce je totiž informací ve smyslu její základní definice (viz předchozí kapitola), ba co víc, dokonce podstatná část nejrůznějších dat a instrukcí, jimiž je celosvětová síť tvořena, je redundantních či chybných.

Namísto statické analýzy tak komplexního jevu, jakým je internet, je tedy třeba přistoupit k analýze jeho dynamiky, tj. spíše sledovat změnu v organizaci celého systému a na základě toho pak dojít k závěru, zda se v čase toto prostředí stává organizovanějším (dochází k jeho vývoji) či zda v jaké míře podléhá univerzální entropii⁴².

Vzhledem k tomu, že prakticky všechny objektivní ukazatele týkající se rozvoje internetu, jako jsou například počet uživatelů, objem obchodní výměny, škála dostupných služeb apod. vykazují trvalý růst, lze s určitou mírou zobecnění konstatovat, že internet jako komplex technologických nástrojů a sociálních vztahů se stále pozitivně vyvíjí. Z tohoto poznatku pak lze implikovat závěr, že můžeme internet považovat za organizovaný systém, který v celkovém pohledu nepodléhá entropii. Oproti takovému názoru je však možné argumentovat poukazem na zvyšující se míru výskytu chaotických tendencí v informačních sítích, ať už jde o chaotizaci komunikační infrastruktury, dat nebo instrukcí.

2.2 POJMY ORGANIZACE A REGULACE

Z informační perspektivy můžeme vidět regulaci jako jednou z forem organizace v procedurálním smyslu. Jedná se tedy o specifickou formu distribuce informací jednotlivým elementům určitého systému. Specifikem regulace je přitom forma, kterou jsou informace vytvářeny, distribuovány a zpracovávány. Konkrétním specifickým rysem regulace pak je existence

⁴² K metodě viz např. Salomon, J.-J. Technologický úděl, Praha: Filosofía, 1997, str. 235 a násl.

subjektu nadaného schopností a možností vytvářet a efektivně distribuovat normativní informace, tj. autority⁴³.

Autoritu můžeme v uvedeném kontextu vidět jako subjekt, na základě jehož činnosti jsou do systému jednostranně dodávány informace, které tento systém přímo organizují. Charakteristickým rysem informačního působení autority je zejména skutečnost, že kvalita tohoto subjektu se do jím vytvářených informací promítá ve formě specifické vlastnosti takových informací, tj. jejich normativity. Informace organizující systém pod vládou autority tedy mohou mít normativní charakter a odpovídající zpracování jejich adresáty je zajištěno již samotnou existencí a nejrůznějšími aktivitami takové autority.

Vztaženo na obor práva je z tradičně pozitivistického hlediska právo-tvornou (organizující) autoritou stát a jeho institucionální kvalitou zajišťující jeho právním informacím potřebnou relevanci jsou základní legitimita státní moci a nejrůznější formy zajišťovacích aktivit (výkon soudnictví, přímé a nepřímé státní donucení, apod.)⁴⁴. Díky tomu mohou mít státní informace normativní charakter a forma zpracování jejich adresáty může mít podobu následování příslušných pravidel.

Ačkoli spolu pojmy organizace a regulace úzce souvisejí, nemusí nutně a vždy platit vztah naznačený v úvodu podkapitoly, tj. že regulace je formou organizace. Regulace jako proces totiž není vymezena na základě kvality příslušných informací, ale pouze jejich formálními znaky, tj. zejména regulativností odvozenou od legitimacy a činnosti autority. Z tohoto důvodu hovoříme o regulaci i tam, kde příslušné informace neodpovídají své základní definici, tj. jsou například redundantní nebo obecně nevedou k organizaci příslušného systému. Z hlediska definice tak pro regulaci není důležité, jak kvalitní normativní informace jsou, ale zda za jejich vytvořením a následnou realizací stojí legitimní autorita. V tomto směru tak můžeme

⁴³ K problematice regulace a normativního působení na společnost ve vztahu ke specifickým rysům informačních sítí srov. např. Mara, A. Norm Origin and development in Cyberspace: Model of Cybernorm Evolution, Washington University Law Quarterly, číslo 78, str. 59 a násl.

⁴⁴ K tomu srov. především publikace právních pozitivistů, z nichž můžeme vybrat např. Kelsen, H. Všeobecná teorie norem. Brno: Masarykova univerzita v Brně, 2000, str. 151 a násl.

hovořit o regulaci i tehdy, pokud je neefektivní nebo je jejím efektem entropie.

Právo nabízí hned celou řadu případů, kdy regulační aktivita nevede k organizaci příslušného systému, tj. státní regulace nezpůsobuje zvýšení organizace společnosti ale naopak⁴⁵. Nedostatek efektivity práva však v tomto případě nesledujeme poměřením obsahu jednotlivých norem s jejich praktickou realizací, ale organizačním efektem, tj. na základě zjištění, do jaké míry vedou autoritativně vytvářené informace (právní pravidla) v komplexním pohledu k redukci společenské entropie a v návaznosti na to k dalšímu pozitivnímu společenskému vývoji.

Můžeme sice vymezit informaci jako protiklad k entropii a organizaci jako protiklad k chaosu, při definici pojmu regulace však žádnou jednoznačnou paralelu či kontradiktornost v tomto směru nalézt nelze. Jedná se tedy z informační perspektivy o pojem popisující formální proces bez ohledu na jeho vnitřní kvalitu či výsledný efekt. Stejně jako může být výsledkem regulace organizovaný systém, může být jeho výsledkem i entropie či v terminální fázi dokonce chaos – vše přitom záleží na kvalitě informací vytvářených a distribuovaných příslušnou autoritou.

Pojmem, který je snad možné postavit jako přímý protiklad regulace tak není chaos ale anarchie. Ve svém pravém významu totiž *an-archeia* znamená neorganizovanost, entropický charakter či chaos ale stav, kdy v systému nebo na něj nepůsobí žádná autorita. Podobně jako v případě regulace, není ani anarchie pojmem označujícím kvalitu určitého prostředí, ale pouze jeho formální znaky, v tomto případě tedy absenci autoritativní aktivity.

Z právě uvedeného tak vyplývá logický závěr, že mezi informovaností, komplexním rozvojem určitého systému a mírou jeho regulace či naopak anarchičnosti není přímá spojitost. Systém, v němž působí autorita, tedy může být dobře organizovaný, může úspěšně čelit entropii a vyvíjet se. Stejně dobře ale může autoritativně regulovaný systém podléhat entropii a vyvíjet se negativně směrem k chaosu. Podobně i anarchický systém se může zdárně organizovat a pozitivně vyvíjet, může však být i entropický a chaotický.

⁴⁵ Příkladem může být i jen vzájemná rozpornost norem pozitivního práva – k tomu srov. Fuller, L. Morálka práva, Praha: OIKOYMENH, 1998, str. 65 a násl.

2.3 ZLATÝ VĚK INFORMAČNÍ SÍTĚ

Jak může volně vyplynout z výše uvedeného, nepředstavuje regulace jediný postup pro vytváření a distribuci organizujících informací do určitého systému. Přestože je v mnoha případech značně obtížné formulovat exaktní a prokazatelné důvody, proč tomu tak je⁴⁶, nelze nevidět jev, který lze označit jako samoorganizaci či méně přesně jako samoregulaci⁴⁷. V tomto procesu se systém brání entropii autonomním vytvářením a distribucí informací jednotlivým elementům, respektive nastolením situace, kdy se jednotlivé elementy informují navzájem. I v tomto případě mohou mít informace normativní charakter, ale namísto autority je jejich efektivita zajištěna přímo jejich organizující kvalitou.

Postupný vývoj lidské společnosti ličí v úvodu své básně Čtvero věků Ovidius. Jako první popisuje etapu zlatého věku⁴⁸:

*Zlatý vzešel pak nejprve věk, kdy zákona, soudce
člověk byl prost a od sebe sám ctíl věrnost a právo.
Nebylo trestu ni strachu, a hrozivá slova se nečtla,
vyrytá v kov, a prosící dav se nemusel báti
soudcových úst: ač neměli obhájce, bezpečni byli.*

Když se v úryvku Ovidiový básně píše o samovolném respektu k věrnosti a právu, jedná se právě o situaci, kdy je systém i bez regulace (zákon) a autority (soudce) organizován a příslušné normativní informace (věrnost, právo) jsou distribuovány horizontálně a akceptovány jednotlivými elementy společnosti a v důsledku toho je pak celá společnost organizována. V dalších dobách popsanych Ovidiovým dílem pak společnost čím dál tím

⁴⁶ Jak bylo uvedeno, můžeme tvorbu a distribuci organizujících informací často prostě vidět jako důsledek složitosti určitého systému, aniž bychom tento jev byli schopni důsledně analyzovat – na vině může být přitom zejména již diskutovaná komplexita. K ilustraci mohou posloužit již zmíněné příklady mraveniště či celulárního automatu.

⁴⁷ Pojem samoregulace nebo autoregulace je ve své podstatě *contradictio in adiecto*, neboť definičním znakem je autorita a ta v případě samoorganizace určitého systému prostřednictvím samovolně vznikajících a distribuovaných informací neexistuje.

⁴⁸ Citace byla převzata z díla Naso, P. O. Proměny, přel. Ferdinand Stiebitz. Praha: Státní nakladatelství krásné literatury, hudby a umění, 1958, str. 13.

víc ztrácela komplexní schopnost samoorganizace, což se projevilo ztrátou efektivity organizujících informací, konflikty a stále gradující potřebou organizovat společnost zásahem zvenčí⁴⁹.

Podobnost společenského vývoje v kyberprostoru s Ovidiovým dílem je až zarážející. Ačkoli autority v prvních fázích vývoje informačních sítí měly čistě technický charakter a sociální regulace tak neexistovala, normativní informace organizující sociální interakce se v tomto prostředí vytvářely v čistě horizontální struktuře a byly prakticky bez výjimek organicky šířeny a zpracovávány jednotlivými členy společenství. Řada autorů na tuto dobu vzpomíná s neskryvanou nostalgií⁵⁰.

Vzhledem k existenci takzvaných definičních autorit (viz dále) nelze o takovém prostředí hovořit jako o plně anarchickém. Odhlédneme-li však od technických pravidel (definičních norem), je možné konstatovat, že zdejší sociální organizace měla anarchický charakter – i přes to však sociální vztahy realizované v tomto prostředí vykazovaly v porovnání s off-line světem až pozoruhodnou míru slušnosti a snad i noblesy. V souhrnu bychom tedy za užití informační metodologie mohli hovořit o anarchickém stavu, v němž byl systém vysoce organizován a díky tomu se prudce vyvíjel.

Podobně, jako je možné dlouze diskutovat o důvodech, proč zlatá doba postupně přešla ve stříbrnou, pak v bronzovou a nakonec v železnou, lze dlouze a bezvýsledně spekulovat o důvodech, proč se v anarchickém avšak dobře organizovaném systému společenských vztahů v informačních sítích začaly vyskytovat chaotické elementy, tj. jevy narušující organizaci a působící entropicky. Kromě prudce rostoucího rozsahu internetu a tím jeho vulgarizace dané značným zvýšením počtu zde realizovaných společenských vztahů mohou být na vině v diskutabilní intenzitě i takové faktory jako společenské či hospodářské změny, kulturní konflikty ale například i náhoda či nahodilost. Bez ohledu na důvody však můžeme opět empirickými

⁴⁹ Vzhledem k tomu, že k regulaci nedošlo, autor vyřešil situaci, která vygradovala chaotickou dobou železnou, relativně jednoduchým způsobem – Bohové téměř celé toto nešťastné pokolení vyhubili potopou.

⁵⁰ Srov. např. Boyle, J. Shamans, Software and Spleens. Cambridge: Harvard University Press, 1996, str. 5 a násl.

metodami zjistit, že chaotické elementy se na internetu vyskytují čím dál častěji a jejich celkový dezorganizační efekt sílí.

Konstatování entropických tendencí se může jevit být v kontrapozici s úvodním tvrzením, že internet se jako komplex vyvíjí pozitivně. Komplexní vývoj je však v tomto případě souhrnem pozitivních (organizujících) a negativních (entropických) procesů, z nichž mají při celkovém hodnocení ty pozitivní stále očividně navrch. Zmíněné entropické tendence však s postupem času nabývají na významu a v posledních několika málo letech tak lze pozorovat zájem na jejich autoritativním (státním i nestátním) řešení.

2.4 LEGITIMITA PRÁVA V INFORMAČNÍCH SÍTÍCH

USA jsou zemí, kde mají hluboké kořeny myšlenkové směry jako liberalismus či dokonce libertariánství. Jednou ze základních myšlenek liberalismu je přitom odstranění nejrůznějších forem regulace omezující jednotlivce v realizaci jejich záměrů a dosažení odpovídajícího prospěchu, ať už materiálního či jiného. Přesně v tomto duchu se nesou aktivity jednoho z nejvýznamnějších hnutí za tzv. svobodný internet, organizace Electronic Frontier Foundation, jejímž zakladatelem je známý rocker a pozdější úspěšný podnikatel John Perry Barlow. Již od počátku svého vzniku, tj. od roku 1990, se tato organizace významně angažuje v boji proti právnímu či jinému omezování svobody jedince na internetu, a to zejména formou veřejné osvěty a právní pomoci v soudních sporech. Jejím základním dokumentem je takzvaná Deklarace nezávislosti kyberprostoru⁵¹, jejímž ústředním motivem je problém právní regulace a činnost států a jejich orgánů autoritativně aplikujících právo. Z deklarace vybíráme následující pasáže (překlad autor):

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

⁵¹ Plný text deklarace viz homes.eff.org/~barlow/Declaration-Final.html

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

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

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

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

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

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

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

Z uvedených pasáží deklarace, která se s postupem času stala všeobecně přijímaným manifestem svobody internetu, lze vyčíst hned několik momentů zásadních pro otázku působnosti práva. Především je to argument neexistence společenské smlouvy mezi adresáty právních norem a jejich tvůrcem, tj. státem⁵². Tento argument je postaven na premise, že na internetu vzniká zcela nové společenství, jehož zřízení, pokud má disponovat autoritou, musí být založeno na nové společenské smlouvě, prostřednictvím které se adresáti právních norem vzdají části vlastní svobody ve prospěch suveréna. Deklarace přitom hovoří o neexistenci společenské smlouvy, jakož i o neexistenci vůle internetového společenství takovou smlouvu uzavřít.

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

Poslední ze závažných a co do legitimacy práva a státu relevantních argumentů je zaměřen na neschopnost států, uzavřených v tradičních prostorových hranicích jurisdikce, efektivně právo vynuocovat. Deklarace hovoří o tom, že státy, přestože by se o to mohly pokoušet, nemají nástroje, jak své právo efektivně v prostředí informační sítě vynutit, tzn. jak (fyzicky) donutit adresáty norem, aby se podle nich chovali⁵³. Doslova je pak zmíněn moment plošného rozprostření myšlenek (dat) nejen přes všechny jurisdikce ale též přes místa, která žádné jurisdikci nepodléhají a tím k zamezení možnosti jejich postihu.

Na uvedené argumenty, jež si s postupem času získaly značnou publicitu a oblibu mezi uživateli služeb celosvětové informační sítě, nelze přitom odpovědět prostě tak, že právo platí, protože je to napsáno v zákoně. Není

⁵² Za původce teorie společenské smlouvy v právním myšlení je považován Thomas Hobbes. Dílem, které tuto teorii definovalo a posloužilo za základ jejího pozdějšího masivního rozvoje, je spis *Leviathan* – viz Hobbes, T. *Leviathan*. Project Gutenberg, 2002. Kniha je volně ke stažení na adrese <http://www.gutenberg.org/dirs/etext02/lvthn10.txt>.

⁵³ Obzvláště problematickým se tento moment jeví být v rovině trestního práva, které je tradičně založeno na individuálním násilném postihu pachatele – k problému srov. Thomas, D. *Criminality on the Electronic Frontier*. In *Cybercrime*, ed. Thomas, D., Loader, B. D. London: Routledge, 2003, str. 17 a násl.

totiž pravda, že právem je to, co říká zákon⁵⁴. Obsah či smysl zákona sice může být považován za základní kámen platného práva, často se však setkáme se situací, kdy obsah práva zjišťujeme i jinak než ze zákona nebo naopak, kdy zákon sice nějaké normy obsahuje, ty však nejsou platným právem⁵⁵. Výše uvedené argumenty jsou tedy pro samotnou existenci práva na internetu důležité a chceme-li s právem na internetu pracovat, je třeba se s nimi odpovídajícím způsobem vypořádat.

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

Jak můžeme vidět na celé řadě příkladů, jako jsou šíření dětské pornografie, podvody v elektronickém bankovníctví, informační obtěžování apod.⁵⁶, nejsou přirozené samoorganizační mechanismy již zjevně s to zvládat veškeré problematické či entropické momenty ve vývoji celosvětové informační sítě⁵⁷. Přirozená schopnost společnosti organizovat se na podkladě tradičních sociálních norem či ekonomických pravidel, jakkoli v mnoha případech funkční, tedy v konkrétních oblastech nestačí a prostředí si tedy žádá autoritativní zásah zvenčí.

⁵⁴ Základní ontologickou otázkou po tom, co je platným právem, nelze spolehlivě zodpovědět jen na základě nahlédnutí do Sbirky zákonů – k problému viz např. Holländer, P. *Filosofie práva*. Plzeň: Aleš Čeněk, 2006, str. 17 a násl.

⁵⁵ K tomu srov. např. Radbruch, G. *Statutory Lawlessness and Supra-Statutory Law* (1946). *Oxford Journal of Legal Studies*, roč. 26, číslo 1, str. 1 a násl.

⁵⁶ Řada z forem společensky nebezpečného jednání v prostředí informační sítě je kvalitativně nových a nejde tedy jen o realizaci standardních aktivit novými metodami – k tomu viz např. Smejkal, V. a kol. *Právo informačních a telekomunikačních systémů*. Praha: C.H. Beck, 2004, str. 752 a násl.

⁵⁷ K tomu srov. např. Kerr, O. S. *Virtual Crime, Virtual Deterrence: A Skeptical View of Self-Help, Architecture, and Civil Liability*, *Journal of Law, Economics & Policy*, roč. 1, číslo 1, str.1 a násl.

Právě uvedené však neznamená, že by právo v prostředí informačních sítí disponovalo nějakou paušální či všeobjímající legitimitou. Nelze tedy prostým poukazem na jednotlivé problematické momenty síťového společenství⁵⁸ prostě odmítnout Barlowovy argumenty a jednoduše konstatovat, že právo má na internetu stejný důvod k existenci jako v off-line prostředí. Naopak je třeba hovořit o legitimní existenci práva jen tam, kde si etická, sociální, ekonomická či technická pravidla nedokážou poradit s výskytem problematických či chaotických elementů.

V tomto směru lze tedy citovat vedoucího současného teoretika práva informačních sítí, profesora Lawrence Lessiga, který v závěru své zásadní monografie *Free Culture* doslova říká (překlad autor)⁵⁹: „*Právo by jistě mělo regulovat určité oblasti naší kultury, ale mělo by regulovat kulturu pouze tam, kde je taková regulace dobrá. Právníci však stále jen zřídka konfrontují svou moc, respektive moc, kterou šíří, s jednoduchou pragmatickou otázkou: ‚Bude to tak dobré?‘ Kdykoli má právo dále rozšiřovat svoji působnost, slyšíme je namísto toho říkat spíše ‚Proč ne?‘*

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

Výše uvedené otázky legitimacy práva nás s praktickou nutností vedou k postupnému přehodnocování tradičních mechanismů právní regulace a jejich přetváření na mechanismy, které by se daly nazvat synergickými formami organizace nikoli pod přímou vládou ale za užití práva⁶⁰. Různé typy

⁵⁸ V tomto směru je potřeba upozornit na skutečnost, že empirické odůvodnění regulačních zásahů je třeba podložit i statisticky – kvalitní metodika pro informační sítě se však v tomto směru stále vyvíjí a jednotlivé statistické výstupy tak trpí nízkou mírou unifikace a tím i vzájemné porovnatelnosti. K problému viz např. Brenner, S. W. *Cybercrime Metrics: Old Wine, New Bottles?* *Virginia Journal of Law and Technology*, roč. 9, číslo 13, str. 1 a násl.

⁵⁹ Viz Lessig, L. *Free Culture*. New York: The Penguin Press, 2004, str. 305. Kniha je k volnému stažení pod licencí Creative Commons na adrese <http://www.freeculture.cc/freeculture.pdf>.

⁶⁰ K tomu srov. např. Galindo, F. A. *Code of Practice for the Globalisation of Electronic Commerce and Government*. *Journal of Information, Law and Technology*, číslo 1, z česky psaných pramenů pak viz Polčák, R. Škop, M., Macek, M. *Normativní systémy v kyberprostoru (úvod do studia)*, Brno: Masarykova univerzita v Brně, 2005, str. 92 a násl.

autorit – zejména pak autority státní, technické a ekonomické - tak v zájmu reprodukce a rozvoje informační sítě k sobě postupně hledají cestu⁶¹ a namísto ignorace či vzájemné konkurence se snaží své působení koordinovat⁶². Význam tohoto sice pomalého⁶³ přesto však nezadržitelného vývoje přitom není zásadní jen pro samotné prostředí celosvětové informační sítě, ale může naznačit cesty, kterými se bude právo v budoucnosti obecně ubírat. Kritické i konstruktivní studium ekonomických, technických, etických či sociální souvislostí působení práva tak v současné době začíná pro právníky na všech úrovních znamenat nikoli jen užitečnou možnost ale doslova nutnost. Stejně tak státy a jejich orgány autoritativně aplikující právo se již nemohou spoléhat na luxus formální platnosti, obecné působnosti a faktické vynutitelnosti práva bez ohledu na uvedené souvislosti⁶⁴.

⁶¹ Běžná je již například spolupráce státu s dodavateli informační infrastruktury v oboru potírání kriminality – nejrůznější technické prostředky tak mohou být vybaveny relativně jednoduchými a nenákladnými mechanismy, které buďto zcela znemožní páčání trestné činnosti nebo významně usnadní její vyšetřování – k tomu srov. např. Katyal, K. Digital Architecture as Crime Control. *Yale Law Journal*, číslo 112, str. 2261 a násl.

⁶² K tomu srov. např. Kleinwächter, W. From Self-Governance to Public-Private Partnership: The changing Role of governments in the Management of the Internet's Core Resources. *Loyola of Los Angeles Law Review*, číslo 36, str. 1103 a násl.

⁶³ Možná zde není zcela na místě hovořit o pomalém vývoji v situaci, kdy se právo ICT teprve pozvolna dostává do třetí dekády své existence. Je přeci řada právních institutů, jejichž vývoj postupně probíhá po stovky či dokonce tisíce let.

⁶⁴ Viz Samuelson, P. Five Challenges for Regulating the Global Information Society, in *Regulating the Global Information Society*, ed. Chris Marsden. London: Routledge, 2000.

3 EXKURZ - ČESKOSLOVENSKÁ INFORMAČNÍ TEORIE PRÁVA

3.1 ZÁKONNOST JAKO PRIMITIVNÍ INFORMAČNÍ KULTURA

Kybernetika, vedena architekturou prvních umělých organismů,⁶⁵ byla nucena při zpracování informací spoléhat na binární modely a jednoduchý, přitom však precizní jazyk. Informační stroje, počítače, totiž pro svou jednoduchost nedokážou operovat s komplexními informacemi, přičemž míra únosné komplexnosti je překročena již u valné většiny pojmů běžného jazyka. Z tohoto důvodu ani při dnešní složitosti a operačním výkonu počítačů nemůže být o jejich chápání řeč – počítač tak již dnes sice dokáže díky tzv. fuzzy logice rozpoznat mluvenou řeč a dokonce ji převést do písemného projevu, jejím pojmům v běžné konverzaci však nedokáže porozumět.

Hodí se zde použít příměr k šachu. Těm nejvýkonnějším počítačům se již dnes může poradit (s trochou štěstí) porazit šachové velmistry. Než dosáhly tohoto stupně dokonalosti, trvalo jim to, řekněme, několik desítek let. Šach se přitom hraje na 64 čtvercích s počátečním počtem 32 figur dvou barev (figury mají přesně určené možnosti pohybu) a smyslem hry je donutit ke kapitulaci soupeřova krále. U práva si počtem figur (právních výrazů) vlastně nejsme úplně jisti – snad je to několik desítek tisíc a možnosti jejich pohybu často závisí spíše na schopnostech těch, kdo s nimi manipulují. Herní pole není rozdělené na přesné čtverce dvou barev a jeho velikost nelze ani odhadovat. K tomu nemáme navíc jasno ani v tom, jakého výsledku chceme dosáhnout - chce se říci: „Zvítězit by měla spravedlnost“ (porovnejme preciznost specifikace tohoto cílového stavu se specifikací kapitulace šachového krále).

Předávání informací ke strojovému zpracování vyžaduje, aby byly tyto informace pocházející z běžného života kódovány (zjednodušeny) k jejich následnému pochopení strojem. Pro zadávání instrukcí tedy vznikly progra-

⁶⁵ Od počátku byly počítače budovány na základech matematické logiky pro operace binárního charakteru a tento model přetrvává dodnes. Zásadní změnu architektury mohou přinést až kvantové počítače, které jsou však v současné době ve stadiu teoretických modelů.

movací jazyky a pro zpracovávaná data pak byly navrženy datové formáty. Obojí je přitom v porovnání s běžnými informačními procesy, jakými jsou třeba lidské rozhovory, až směšně primitivní. Dokonce ani sofistikované programovací jazyky, tedy pojítka mezi strojovým kódem a uživatelem-programátorem, nejsou ničím jiným než sadou několika jednoduchých jednovýznamových (monotónních) instrukcí, jejichž charakter je stejně kauzální jako jejich použití. Stejně tak rozsáhlé datové soubory sice mohou být automatizovaně zpracovávány, třeba tak, že je v nich vyhledáván určitý text, to však pouze mechanicky bez reflexe jejich obsahu.

Z uvedeného vyplývá, že pokud bychom mohli vytvořit jazyk složený z jednoduchých nemetaforických pojmů, které by precizně popisovaly skutečnost, bylo by pak možné při odpovídajícím výpočetním výkonu dosáhnout obsahového zpracování příslušných informací strojem – to ve smyslu možnosti vytvoření dokonalých programů (tedy sad instrukcí) i strojového pochopení skutečnosti, tj. obsahové reflexe dat (výroků). Jednalo by se v takovém případě vlastně o programovací jazyk (jednoduchý, precizní, nemetaforický), který by byl však použitelný i pro komunikaci běžných informací. Jeho fráze bychom pak mohli kauzálně (logicky) zpracovávat a nebyl by tedy problém „naučit“ jím časem komunikovat i počítače. O vytvoření takového jazyka se svého času pokoušel už Gottfried Willhelm von Leibnitz. Úsilí, genialita, v pravdě pansofické vědomosti ani východisko, jímž byla v mnoha ohledech precizní němčina, jej však neušetřily od neúspěchu. Od jeho pokusu tedy máme důvod se domnívat, že tento úkol je prostě nad lidské síly.

Pro výše uvedený problém se právní informatika, která se z kybernetiky přímo vyvinula, musela zaměřit právě na takové právní informace, které bylo možné precizně vyjádřit a popsat jednoduchými binárními indexy typu pravda/nepravda a platí/neplatí. Jednoduché kauzální normativní konstrukce přitom svědčí nejen tvůrci, ale vyvolávají informační odezvu i u jejich adresátů. Primitivní jazykové konstrukce, odhlédneme od jejich obsahu, mohou být jednodušeji komunikovány a následně i přijímány a chápány těmi, jimž jsou určeny. Týkají-li se pak takové informace povinností, mají adresáti díky jejich jednoduchosti jasno a výsledkem je, co do formální organizace, pořádek.

Jednoduchost a kauzalita tak nejsou jen předpoklady automatizovaného zpracování informací ale též absolutního regulovaného pořádku. Jednoduchá pravidla, jejichž tvorba i aplikace mohou být pod přímou kontrolou suveréna, jsou dostatečně zřetelná a jasná i pro jejich adresáty. Navíc v tomto případě díky jednoduchosti příslušných informací nehrozí, že by se mohl v systému vyskytnout nějaký nežádoucí komplexní informační efekt, tj. například některá z nechtěných základních hodnot.

Bez ohledu na negativní konotace toho slova můžeme z pohledu jednotlivce označit touhu po jednoduché kauzální zákonnosti za prostý projev primitivismu.⁶⁶ Není tedy s podivem, že se jednoduše formulované ideologie s jasně čitelnými myšlenkami (informacemi) setkávají s největší odezvou právě v řadách primitivů. Tady je pak také třeba hledat kořeny přirozené primitivní potřeby po jednoduchých a jasných kauzálních pravidlech, jejichž vyjádření je srozumitelné a následná jejich aplikace je pak jasná a předvídatelná.

Na primitivní potřebě kauzality a z ní pramenící normativní jistoty není třeba hledat nic *a priori* špatného. Stejně jako sama výroková či deontická logika totiž kauzální systém norem může být co do své podstaty bezhodnotový. V tom však spočívá, hovoříme-li o systému právních norem, jeho zásadní problém – jedná se o instrument, který nedisponuje vnitřními (přirozenými) kontrolními a korekčními mechanismy, jejichž prostřednictvím by byla chráněna rozumnost, slušnost, spravedlnost a další komplexní (složitě, nejisté, nedefinovatelné) hodnoty.

Příkladem primitivního subsystému práva může být právní úprava silničního provozu. Tento víceméně technický systém norem má definiční ambici jednoduchosti, srozumitelnosti, bezhodnotovosti a kauzální aplikace. Stejně tak, jako můžeme jednoduchou a srozumitelnou kauzální normou vnést do tohoto primitivního normativního systému rozumný vnější element, jakým je na příklad ochrana tělesně postižených řidičů, můžeme však s takto jednoduchým systémem z pozice zákonodárce manipulovat i ve prospěch zájmů, které nemají přirozený, rozumný ani tradiční základ. Vzhledem k tomu, že je tento systém konstruován jako primitivní, očekává se pak od adresátů norem i těch, kteří je autoritativně aplikují, že nebudou

⁶⁶ K tomu srov. např. půvabný článek Lindworsky, S. J. Příčinné myšlení u primitivního člověka. Filosofická revue, roč. 1929, č. 1, str. 13 a n.

kvalitu norem hodnotit (přemýšlet nad nimi) a budou se tedy chovat jako primitivové a prostě následovat, co je napsané v zákoně.

3.2 STROJE NA PRÁVO V ČESKOSLOVENSKÉ DOKTRÍNĚ – KNAPP ŠEDESÁTÝCH LET

Jak vyplývá z výše uvedeného, představují zákonné právo a zákonnost jako alternativa právnosti vcelku kvalitní materiál ke kybernetickému uchopení a automatizovanému zpracování. Podobně i koncepce justičních orgánů jako informačních struktur přímo vybízí k nasazení informačních technologií v procesech autoritativní aplikace práva.

Česká právní věda se nevydala úplně ve stopách sovětské doktríny a nedošlo zde tedy k pokusům o teoretickou stavbu strojů na právo, které by při odpovídajícím nakódování byly s to automatizovaně řešit otázky zákonnosti. Právní informatika tak měla u nás od počátku především charakter podpůrný a instrumentální, to však nikoli na základě ideologickém, ale spíše kvůli prostému pragmatickému zhodnocení aktuálních možností použití kybernetických metod v právu.

V oboru informační teorie práva a právní informatiky hrála bezesporu ústřední roli osobnost Viktora Knappa. Nebudeme se na tomto místě zabývat jeho vlivem na československé právo obecně, ale zaměříme se spíše na směr, který udělal nově vzniklé disciplíně právní informatiky a kterého se nejjeden právní informatik drží dodnes.

Knapp již v době prvních počítačů odhalil obrovský potenciál informačních technologií a díky chápání práva jako informačního systému byl schopen formulovat na svou dobu unikátní vize budoucích aplikací. Ve svých prvních informačně-právních publikacích završených monografiích „O možnosti použití kybernetických metod v právu“ se přitom ještě zčásti hlásí k sovětské ideji stroje na právo. K možnosti automatizovaného zpracování právních informací však přistupuje mírně skepticky, když konstatuje výše rozebraný problém právního jazyka a právních výrazů.

K výše rozebranému problému monotónnosti právních výrazů Knapp uvádí: „*K tomu ovšem, aby kybernetické zkoumání a zpracovávání kvanti-*

tativní stránky určité kvality bylo možné, musí být příslušná věda (a logika) způsobilá vyjádřit nutné předpoklady tohoto zkoumání konečným počtem konečných logickomatematických formulí, tj. způsobem 'srozumitelným' kybernetickým strojům [...]. Jestliže určitá věda v určité době a v určitých otázkách tento předpoklad nesplňuje, může to být způsobeno v podstatě dvěma příčinami: V první řadě tím, že i pro praxi postačující poznání některých jevů a vztahů se opírá o nekonečný či spíše předem neurčitelný počet předpokladů, které tedy nejsou vyjádřitelné konečným počtem logickomatematických formulí. Tu se staví použití kybernetických metod v cestu překážky objektivní.“⁶⁷ Jedním dechem však Knapp dodává, že problém automatizace práva může tkvět ve zhojitelné neschopnosti právní vědy dosáhnout precizních definic a jednoznačných kauzálních formulí, kterou popisuje následovně: „Nemožnost vyjádření některých vztahů konečným počtem konečných logickomatematických formulí však zatím (zejména ve společenských vědách) spočívá většinou v subjektivních faktorech, tkvících v příslušné vědě samotné, která dosud nevypracovala potřebné předpoklady pro možnost použití kybernetických metod. Tato naposled zmíněná nemožnost je překonatelná dalším rozvojem té které vědy.“

Určitý pragmatismus je znát už z toho, že Knapp přiznává v právu existenci obou typů překážek, tj. subjektivních (odstranitelných) i objektivních a následně s nimi pracuje. Dokonce i idealistickou vizi primitivního komunistického práva/všespolečenského řádu, které nejenže bude aplikovatelné strojem, ale v konečné fázi nebude aplikační mechanismus potřebovat vůbec, zmírňuje konstatováním, že proces přetváření složité právnosti v komunistickou zákonnost a pozdější pořádek, bude zřejmě zdlouhavý.

K roli kybernetiky při postupném přerodu práva v jednoduchý společenský řád Knapp říká:⁶⁸ „Na jedné straně totiž – spolu se zdokonalováním kybernetických strojů – usnadňuje jejich aplikaci proces stálého zjednodušování práva; na druhé straně však týž proces zjednodušování práva, spolu s postupnou změnou jeho kvality, přetváření státních orgánů v přímé (společenské) orgány pracujících, přenášení funkcí státních orgánů na společenské organizace atd. zužuje sféru právní regulace společenských vztahů a tím samým zužuje i možnost aplikace kybernetických strojů. Navíc se právo v tomto procesu (než odumře úplně) stane tak jednoduchým, že nebude vyžadovat kybernetických metod stejně, jako jich nevyžadují

⁶⁷ Viz Knapp, V. O možnosti použití kybernetických metod v právu. Praha: Nakladatelství Československé akademie věd, 1963, str. 18-19.

⁶⁸ Viz tamtéž, str. 20.

jednoduché početní úkony. [...] Poznatků o možnosti aplikace kybernetických metod v právu bude pak pravděpodobně (i když jistě ne v plné míře) možno použít i při oněch metodách řízení společnosti, v něž se řízení společnosti pomocí práva promění resp. jimiž bude nahrazeno a, navíc, použití kybernetických metod v právu může být samo užitečné při přetváření práva v společenská (neprávní) pravidla chování.“

Z poslední pasáže je možné vyčíst obdivuhodné Knappovo pochopení síly státem plně kontrolovaných informačních a komunikačních technologií jako bezhodnotového regulačního nástroje, jehož materií může být prakticky cokoli. Státní informační technologie je tak v tomto případě chápána nikoli jen jako nástroj práva (zákonnosti), ale jako přímý regulační instrument samotné ideologie.⁶⁹

Přestože Knapp dále ideu primitivní zákonnosti resp. jednoduchého všespolečenského řádu nerozpracoval (můžeme jen domýšlet, zda z nezájmu nebo pro mentální rezervaci), byl na základě vpravdě geniálního pochopení potenciálu informačních metod a informačních technologií schopen formulovat pro právní informatiku řadu jiných prakticky realizovatelných zadání. S odstupem času nejzávažnější z nich se týkalo použití informačních metod a informačních technologií v procesu ideologické kontroly činnosti soudnictví.

K možnostem automatizované aplikace komunistické ideologie do rozhodovacích procesů soudů Knapp uvádí: „Logická kontrola tedy přes omezenost svých možností je důležitým prostředkem nejen k upřesnění statistických údajů, ale může být, jak již uvedeno, dost významným prostředkem kontroly dodržování socialistické zákonosti. Poněvadž pak logická kontrola, byť zatím nebyla prováděna kybernetickými stroji, nepochybně náleží k celkovému procesu použití kybernetické metody v soudní statistice, lze jistě bez nadsázky říci, že praxe a zkušenosti v justiční statistice ukázaly pozoruhodnou novou stránku použití kybernetických metod v právu a ukázaly zejména i to, že rozvážné jejich použití na vhodném místě může sloužit i velmi důležitým cílům politickým, jakým je bez jakékoli pochybnosti kontrola zachovávání socialistické zákonosti.“

Skutečnost, že aktuálně dostupné technologie a informační metody mohly být nástrojem vyšší kontroly státu nad činností soudů, vedla s postupem

⁶⁹ Stejná myšlenka se o čtyřicet let později objevuje důkladně rozpracovaná i v publikacích vedoucích osobností současného práva informačních technologií Lawrence Lessiga či Petera Kleve. Viz Lessig, L. *Code V.2*. New York: Basic Books, 2006, str. 281 a n. nebo Kleve, P. De Mulder, R. *Cod is Murphy's Law*. In *Cyberspace 2005*. Brno: Masarykova univerzita, 2006, str. 11 a n.

času až k vytvoření speciálních ministerských pracovišť, ba celých odborů, jejichž náplní práce byla informatizace justice. Jejich úkolem samozřejmě nebylo pouze kontrolovat soudy při aplikaci socialistické zákonnosti (většina technologií měla hodnotově neutrální instrumentální charakter – viz dále), snaha o ideologickou konzistenci soudní praxe však patřila mezi hlavní hybné síly státního aparátu při podpoře nových technologií. V řadě publikací se tak můžeme setkat s popisem teoretických konstrukcí i praktických metod nasazení informačních technologií při ideologické dezinfekci justičního systému.

Přestože i sám architekt československé právní informatiky od svých původních vizí postupně ustoupil, objevovaly se ještě v půli osmdesátých let publikace připomínající využitelnost právních informačních technologií a informačních metod pro aktivní distribuci komunistické ideologie.

O dvacet let později, než Knapp nastínil vizi automatizované logické kontroly jako metody plnění politického zadání, se tak z úst tehdejší ředitelky Odboru řízení a justiční informatiky Ministerstva spravedlnosti SSR v časopise *Socialistické soudnictvo* dovídáme, že⁷⁰: „[...] *sa zabezpečí riešenie a realizácia podsystemu úloh vyplývajúcich z usnesení najvyšších stranických a štátnych orgánov ČSSR a SSR, týkajúcich sa činnosti justice v SSR a vytvori sa automatizovaný informačný systém spracúvania a vyhodnocovania verbálnych informácií pre potrebu riadiacej činnosti Ministerstva spravdливosti SSR.*“ Pro úplnost je však třeba dodat, že takový systém nebyl naštěstí nikdy plošně zprovozněn.

Jak bylo naznačeno výše, sám Knapp se v pozdějších svých publikacích zaměřil spíše na instrumentální roli informačních technologií a ve své poslední velké monografii věnované informační teorii práva a nazvané „Právo a informace“ informace se již aktivní roli kybernetických metod při ideologizaci práva věnuje jen minimálně. V řadě otázek dokonce předvádí kopernikovský obrat, když opět s pozoruhodným instinktem naznačuje problémy nasazení informačních technologií. Na negativních příkladech nutně ukazujících na kapitalistické státy tak Knapp ilustruje byrokratizaci a odosobnění automatizovaných právních agend,⁷¹ problém ochrany osobnosti a osobních údajů⁷² nebo problémy kontroly justice exekutivou

⁷⁰ Viz Colotková, Z. Rozvoj automatizovanej sústavy justičnej informatiky. *Socialistické soudnictvo*, roč. 37, č. 9, str. 1 a n.

⁷¹ Viz Knapp, V. *Právo a informace*. Praha: Academia, 1988, str. 260.

⁷² Tamtéž, str. 259.

prostřednictvím kontroly justičních informačních systémů.⁷³ Za pozornost v tomto směru opět stojí, že se právní věda začala otázkami ochrany osobních údajů v informačních systémech a dalšími problémy nastíněnými Knappem v roce 1988 zabývat plošně až od poloviny devadesátých let. Nezávislost justičních informačních systémů a nebezpečí narušení principu dělby moci se dokonce v právní vědě začínají diskutovat až nyní po více než dvaceti letech.

Přestože se Knappův pohled na praktické problémy související s aplikací informačních technologií v právu postupně měnil, jeho základní náhled na kybernetiku a její instrumentální roli zůstal i později nezměněn. Nesouhlasil tak s Wienerem v tom, že organizační roli informace lze obdobně sledovat v přírodních i sociálních systémech a že je tedy na místě hovořit o kybernetice nejen jako o instrumentální disciplíně, ale jako o hodnotově založené filozofii. V tomto směru neměl Knappův přístup u nás konkurenci a právní informatika se tak od počátku vyvíjela jako univerzálně použitelné instrumentarium. Ojedinelým konkurenčním názorem, kterému však Knapp ani ostatní právníci nevěnovali náležitou pozornost, tak byl pouze překlad článku „K niektorým filozofickým otázkám kybernetiky“ publikovaný v časopise *Otázky marxistickej filozofie*.⁷⁴

V závěru tohoto článku, jehož autoři se hlásí k původní Wienerovské koncepci kybernetiky, se můžeme dočíst: „Podľa nášho názoru pokusy obmezit' sféru kybernetiky na technické problémy súvisia aj s nesprávnou informáciou ohľadom úloh a záverov kybernetiky. Neberie se tu do úvahy najmä, že kybernetika sa člení na tri hlavné smery alebo oblasti: teoretickú, technickú a použitú kybernetiku.

Na druhej strane negatívny postoj k myšlienkám kybernetiky v oblasti biologie a iných špeciálnych vied, ktoré sa považujú za mechanistické pokusy prenášať zákonitosti nižších foriem pohybu na oblasť vyšších foriem pohybu, má svoj metodologický podklad. Tento podklad spočíva v tom, že sa zdorazňujú a absolutizujú kvalitatívne rozdiely medzi formami pohybu hmoty a podceňuje sa materiálna jednota sveta. Takéto názory sú veľmi blízke metafyzickým koncepciám o hard and fast lines medzi rozličnými oblasťmi skutočnosti, ktoré boli práve také charakteristické pre prekonaný mechanizmus.“

⁷³ Tamtéž, str. 242 a n.

⁷⁴ Viz Stoljarov, V., Kannegiesser, K. H. K niektorým filozofickým otázkám kybernetiky. *Otázky marxistickej filozofie*, roč. 18, č. 1, str. 57.

3.3 PRÁVNÍ INFORMATIKA A INSTRUMENTÁLNÍ VYUŽITÍ INFORMAČNÍCH TECHNOLOGIÍ – KNAPP SEDMDESÁTÝCH A OSMDESÁTÝCH LET

Namísto řešení úlohy právní kybernetiky respektive právní informatiky v procesu postupné primitivizace československého práva se pozdější teorie i aplikovaná právní věda zaměřila spíše na vývoj právních informačních systémů a systémů právní statistiky. Místo ideologie se tedy do informační teorie práva začal s mladými právními vědci a rovněž díky Knappově postupnému obratu dostávat spíše pragmatismus a ekonomické myšlení. Komunistická právní informatika tak ustoupila od nereálných logicizujících vizí a soustředila se na vývoj informačního servisu pro zefektivnění procesů autoritativní aplikace práva – od poloviny sedmdesátých let se tedy až na výjimky stala specifickou aplikovanou informatickou disciplínou, jejíž materií je sice právo, avšak jeho kvalita je pro ni už zcela irelevantní.

Od poloviny sedmdesátých let se setkáváme s řadou často špičkových publikací rozebírajících jednotlivé aspekty nasazení informačních technologií jako asistence právních procesů. Aplikace právních informačních metod se přitom neomezuje jen na legislativu⁷⁵ a justiční aplikace, ale specifická pozornost je věnována i hospodářské praxi.⁷⁶ Zajímavá je přitom opět postupná pragmatická tendence pouštět od původních striktních ideových požadavků na primitivizaci práva prostřednictvím jednoduché zákonnosti a naopak rozšíření oboru právních informačních systémů o materii judikatury nebo o doktrinální publikace.

Od půle osmdesátých let se s masovým příchodem prvních mikropočítačů informační teorie práva až na výjimky definitivně přesouvá z filozofické či ideologické roviny k praktické každodenní aplikaci. Úsilí právních informatiků se tedy namísto ideových základů orientuje už plně na řešení partiikulárních problémů souvisejících s nasazením informačních technologií,

⁷⁵ Srov. např. Cejpek, J. Automatizované vyhledávání informací z českých a slovenských textů právních dokumentů. *Právník*, roč. 120, č. 4, str. 360 a n.

⁷⁶ Viz např. Bublávková, J. Automatizovaný systém pracovnoprávních informací a možnosti jeho využitia v právnej teórii a praxi. *Právník*, roč. 123, č. 5, str. 450 a n.

a to především v hospodářském právu. Dochází tak k vývoji prakticky použitelných právních informačních systémů a systémů pro statistické zpracování právních dat bez reflexe příslušné právní materie.

V této době se poprvé setkáváme rovněž se zcela novou nesespecifickou právní disciplínou, kterou je právo informačních technologií. Díky Viktoru Knappovi byla i v tomto případě česká právní věda mezi prvními, které zachytily nástup této nové právní problematiky.⁷⁷ Tehdejší perspektivní právně-vědecké kádry obeznámené s vývojem v oboru informačních technologií se však orientovaly spíše na řešení technických právně-informačních otázek a ani sám Knapp se novému oboru práva informačních a komunikačních technologií už nijak zvlášť nevěnoval.

3.4 ZÁVĚREČNÉ POZNÁMKY K HISTORII ČESKOSLOVENSKÉ PRÁVNÍ INFORMATIKY

Výše uvedené může zapůsobit jako smířlivý konec a posloužit i k morálnímu odůvodnění téměř bezvýjimečné personální i obsahové kontinuity dalšího vývoje právní informatiky, k němuž u nás po sametové revoluci došlo. Na první pohled to totiž vypadá, jakoby informační teorie práva začala pokusem o nahrazení ze zásady politicky nespolehlivého právníka dokonale naprogramovaným (roz. uvědomělým) strojem, aby později došla k závěru, že bude lépe namísto fantazírování následovat technický vývoj a ideologii nahradit univerzálně použitelným instrumentariem.

Díváme-li se obecně na československé právo (nikoli na právní informatiku) optikou informační teorie, můžeme opravdu dospět k závěru, že zde k ideovému vývoji skutečně došlo a že tedy určitá míra kontinuity může být

⁷⁷ Na rozdíl od německé doktríny prosazoval Knapp již od počátku metodologické oddělení práva informačních a komunikačních technologií, jako hmotněprávního oboru, od technické právní informatiky. V úvodu *Práva a informace* tak píše: „*Oba tyto problémové okruhy spolu těsně souvisejí a zčásti se prolínají (např. lze hovořit o právních aspektech provozování automatizovaných systémů právních informací), ale svými předměty se přece jen dosti výrazně odlišují a není vhodné je směřovat*“ – viz Knapp, V. *Právo a informace*. Praha: Academia, 1988, str. 8.

na místě. Původní poválečné komunistické pojetí práva bylo totiž založeno na kritice meziválečného formalismu a pozitivistického konceptu zákonosti následované požadavkem materiálního lidově-demokratického apendixu zákona.⁷⁸ Tuto ideologii pak vystřídala komunistická zákonnost s ambicí jednoduchosti (této koncepci jsme se podrobně věnovali výše) a s utopickou vizí postupného zjednodušení práva až k jeho naprostému vymizení, aby se nakonec právní teorie fakticky rozpustila do až americky pragmatického řešení partikulárních právních problémů především hospodářského charakteru.

Na rozdíl od obecného vývoje našeho právního systému, který jsme tu právě trestuhodně shrnuli do jednoho odstavce, má však právní informatika smůlu v tom, že referenční hledisko zde stojí stále ještě o řád výš než její měnící se objekt každodenního zájmu⁷⁹. Její konečnou bezhodnotovost a službu autoritářskému režimu tedy v tomto případě nelze omlouvat tím, že nakonec tak nějak sama od sebe dostala rozum.⁸⁰ Nemá být tudíž předmětem pranýřování její výstup (ten konečně prošel korekcí a těžko k jeho závěrečné podobě něco namítat), ale sama skutečnost, že na bezhodnotovosti a instrumentálnosti založila tato disciplína od počátku svoji existenci.

Původní Knappova vize kybernetických metod jako nástroje regulace použitelného univerzálně pro právo či pro jiný normativní systém totiž ve skutečnosti žádnou změnou neprošla. Přestože lze pochybovat o tom, že měl akademik Knapp její instrumentálnost původně na mysli jako její základní teleologii, nesla s sebou tato disciplína svoji univerzálnost a je třeba říci, že ji nese dál. Právě z tohoto důvodu si pak právní informatika a její představitelé možná ještě více než jiné právní obory zaslouží morální odsouzení.

⁷⁸ Obecně k pojmu materiálního apendixu pozitivního práva viz Holländer, P. *Filosofie práva*, Plzeň: Aleš Čeněk, 2006, str. 47 a násl. Lidově-demokratický obsah tohoto pojmu může ilustrovat následující výčet: „*Logický výklad znamená: 1) výklad zákona v duchu lidově demokratického zřízení, 2) výklad zákona ve smyslu cílů, které mu lidově demokratické zřízení dává.*“ – viz Boura, F. K otázce výkladu zákonů. *Právník*, roč. 88, č. 7-8, str. 297.

⁷⁹ Tímto referenčním hlediskem je samotná povaha informace (viz výše).

⁸⁰ Naproti tomu technickým disciplínám nebo například populární hudbě lze bezhodnotovost v tomto směru jen těžko vyčítat.

Na závěr tohoto krátkého ohlédnutí za příběhem československé informační teorie práva se tedy dostáváme zpět ke kořenům kybernetiky. Díky bouřlivému rozvoji jejích derivátů v průběhu uplynulých šedesáti let se právníkům dostaly do rukou mocné regulační nástroje, jejichž prostřednictvím lze přímo a efektivně ovlivňovat a kontrolovat lidské chování (podrobnější jejich výklad je proveden v následujících kapitolách). Jedině právníci obeznámení i s významem informace a potenciálem informačních technologií jsou přitom schopní odhalit skutečnou sílu jednotlivých právních informačních nástrojů a následně konfrontovat možnosti jejich použití s přirozeným charakterem informace, která jim dala vzniknout.⁸¹ Jedině právníci, respektive právníci-informatici, tak jsou s to posoudit, do jaké míry reflektuje ta která technologie či metoda přirozené kvality informace a základní (princiální) požadavky života jako takového. Představitelé právní informatiky jsou tedy zodpovědní nejen za vývoj univerzálních informačních nástrojů práva, ale nesou spoluodpovědnost i za konkrétní konečné výsledky jejich aplikace, které jsou jako jediní schopni a tím i povinni předvídat a zároveň kriticky hodnotit.

Proti příkrému odsouzení právních informatiků můžeme postavit námitku, že totiž i sama kybernetika není hodnotově orientována a má tedy rovněž instrumentální charakter. Opak je však pravdou, neboť základem kybernetiky je právě pochopení charakteru informace jako nositelky života. Příkladem kritické reflexe, k níž však naše právní informatika nikdy nepřistoupila, mohou být třeba Asimovovy zákony robotiky:⁸²

- Robot nesmí ublížit člověku nebo svou nečinností dopustit, aby mu bylo ublíženo.
- Robot musí poslechnout člověka, kromě případů, kdy je to v rozporu s prvním zákonem.

⁸¹ Příkladem takové kritické konfrontace může být třeba snad až příliš pesimistické pojednání Jamese Boylea o totální cenzuře, transgenickém otroctví a sebereflexi umělé inteligence – viz Boyle, J. *Shamans, Software & Spleens*. Cambridge: Harvard University Press, 1996, str. 144 a n.

⁸² Pro právníka jsou následující imperativy sice jen prázdnými formulemi, které se akorát hodí do prostředí, kde vznikly, tj. do literatury sci-fi – ukazují však na reálnou kritickou filozofickou reflexi kybernetické technologie. Můžeme je nalézt například zde: Asimov, I. *I, Robot*. Oxford: Oxford University Press, 2000. V češtině byly Asimovovy povídky vydány hned několikrát – poslední vydání viz Asimov, I. *Já, robot*. Praha: Triton, 2004.

- Robot se musí chránit před poškozením, kromě případů, kdy je to v rozporu s prvním nebo druhým zákonem.
- K nim pak ještě přibyl nultý zákon: Robot nesmí ublížit lidstvu nebo svou nečinností dopustit, aby mu bylo ublíženo.

Jak můžeme vidět, je tedy konečná kritika hodnotové neutrality právní informatiky zcela na místě. Aniž bychom měli ambice činit zde nějaké věčné či všeobjímající soudy, dovolíme si tak závěrem opatrně konstatovat, že komunistická právní informatika může vlastně posloužit i jako důkaz toho, že právo nemá bezhodnotových oborů⁸³. Více než paradoxní je přeci situace, v níž roboti mají v sobě zakódovanou úctu k životu a absolventi technických oborů vedle standardní akademické přísahy skládají ještě slib nezneužít svých vědomostí a schopností proti lidstvu, zatímco právníci vládnoucí silou, s níž se uměle ovládané přírodní síly nemohou rovnat, zde ještě mnohokrát umocněnou technologií pro tvorbu, zpracování a komunikaci normativních informací, se mohou stále ještě schovávat za bezhodnotový charakter některých svých disciplin.

⁸³ Obecně k úloze hodnot v různých vědních disciplínách viz např. Sullivan, J. W. N. *The Limitations of Science*. Clifton: Augustus M. Kelley Publishers, 1973, str. 239 a násl.

4 INFORMAČNÍ SÍŤE A TERITORIALITA PRÁVA

4.1 PROBLÉM DELOKALIZACE PRÁVNÍCH VZTAHŮ

Jedním z klíčových aspektů informační společnosti je existence informačních sítí, z nichž ústřední roli hraje celosvětová síť internet. Informační síť jako takové, ať už bráno z hlediska technického či společenského, samozřejmě nejsou novým společenským fenoménem, ale rychlost a dostupnost komunikačních prostředků jejich vznik a vývoj významně podporují.

Nejdůležitější aspekt virtualizace sociálních sítí za užití mechanismů informační společnosti můžeme nejen z právního hlediska vidět především v oddělení obsahu těchto sítí od fyzické infrastruktury. Zatímco tedy v dopisní či telefonické komunikaci stále zohledňujeme kvantitativní aspekt místa nebo typu použité komunikační technologie, při komunikaci prostřednictvím služeb celosvětové informační sítě internet se nezajímáme o to, kudy naše komunikační spojení prochází, jakým prostředkem je realizováno a často nás nezajímá ani to, kde se fyzicky nachází adresát našeho sdělení.

Tento aspekt virtualizace informačních sítí můžeme označit stručně též jako delokalizaci společenských vztahů na internetu⁸⁴. Změna vnímání delokalizovaných vztahů nespočívá ani tak v tom, že by technika pouze pomáhala překonávat fyzické vzdálenosti mezi účastníky právních vztahů (stát nevyjímaje), ale že dnes dostupné a hojně užívané informační a komunikační technologie dokonce vyjímají fyzický odstup z relevantních faktorů mezilidské komunikace⁸⁵. Není to tedy vzdálenost, co by určovalo pravidla pro vzájemnou komunikaci, ale pouze její forma (záleží na tom, zda strany zvolí SMS, videokonferenci nebo třeba některý z instant messengerů).

⁸⁴ Záměrně zde nepoužíváme pojem globalizace, neboť ten označuje proces zvyšování globální relevance – jednotlivé vztahy v informačních sítích však obvykle nemají globální charakter (naopak často je jejich přesunem do prostředí celosvětové informační sítě jen posílána jejich intimita).

⁸⁵ Srov. Škop, M. Hranice práva a kyberprostoru - Subverzivita kyberprostoru. Právník, roč. 144, číslo 5, str. 1157.

Především soukromoprávní pojmání fenoménu delokalizace může na první pohled vypadat jako oprašování římskoprávní doktríny distančních kontraktů. Dokonce i právotvůrce používá výrazu „dálkový přístup“ pro označení komunikačních metod využívajících služeb informační společnosti. Dálka či distance se v právu zohledňovala a zohledňuje jednak z důvodu *de iure* přiznané důležitosti osobního kontaktu⁸⁶, především však z důvodu souvislosti mezi fyzickou vzdáleností a rychlostí komunikace. Vzdálenost tedy podmiňovala užití takových komunikačních prostředků, které byly kromě omezeného rozsahu zatíženy též břemenem časové prodlevy.

Společenské vztahy včetně těch regulovaných právem, které vznikají nebo se realizují v prostředí celosvětové informační sítě, však ve skutečnosti díky použitým technologiím postupně ztrácí distanční aspekt. Ani účastníci těchto vztahů se vzájemnou fyzickou vzdáleností nezabývají – omezením v komunikaci jim je pouze požitá technologie.

Není výjimkou, že účastníci jednání různých kolektivních orgánů si krátký čas chatováním prostřednictvím on-line messengerů nebo SMS. Nekomunikují přitom jen s přáteli fyzicky vzdálenými, ale i s těmi, kteří v tu chvíli sedí ve stejné místnosti. Jiný příklad irelevance vzdálenostního aspektu mohou představovat služby internetového bankovníctví – klient může svůj účet obsluhovat z domova, může se však i vypravit do banky a stejnou operaci zde provést z veřejně dostupného terminálu.

S absencí fyzické vzdálenosti jako faktoru komunikace úzce souvisí i další výše naznačený aspekt delokalizace společenských vztahů, a to irelevantnost fyzického umístění subjektů a objektů právních vztahů vznikajících nebo realizovaných v prostředí informačních sítí. Služby celosvětové sítě internet ve spojení s komunikační infrastrukturou totiž umožňují (či dokonce ukládají) uživatelům zcela zapomenout na to, kde jsou například umístění adresáti jejich sdělení, kde se nacházejí data, o něž mají zájem nebo odkud se někdo snaží zaútočit na jejich systém. Uživatele často vůbec nezajímá (a technicky vzato ani zajímat nemusí), kde je fyzicky usazen poskytovatel jejich oblíbených služeb nebo kde je umístěna jeho

⁸⁶ Může se jednat například o osobní kontakt kontrahentů, ale též o kontakt mezi subjektem a sekundárním objektem příslušného právního vztahu, jak jej zohledňují ochranná ustanovení v distančních spotřebitelských smlouvách.

komunikační infrastruktura. Namísto tradičních identifikátorů off-line světa, jakými jsou například poštovní adresy poskytující vyjma P.O. BOXů precizní informace o fyzické lokalizaci dotčeného subjektu, se tak používají adresy založené na doménových jménech. Takové adresy však nemají co do fyzického umístění subjektů prakticky žádnou vypovídací hodnotu.

Aspektem takzvané virtuální identity⁸⁷ je mimo jiné i to, že její identifikace v kyberprostoru je prakticky libovolně volitelná a nemá prostorový význam. Můžeme tedy zvolit e-mailovou adresu s doménou první úrovně .com či .cz, ale stejně jednoduše si můžeme zřídit adresu s koncovkou .nu nebo třeba .to. Volbou národní domény první úrovně, především u adres komerčních www prezentací, se subjekty jistě snaží uživatelům alespoň naznačit příslušnost k určitému státu (viz dále) – rozhodně to však neznamená, že by se na jejich usazení v tomto státě dalo spoléhat.

Faktickou delokalizaci společenských vztahů v prostředí informačních sítí není možné brát *per se* jako negativní jev. Právě naopak, skutečnost, že informace mohou mezi subjekty proudit bez toho, aby byla vzájemná komunikace zatížena teritoriální bariérou, můžeme vidět jako veskrze pozitivní důsledek použití moderních informačních a komunikačních technologií.

Z hlediska právního je však delokalizaci třeba vidět naopak jako jeden z naprosto zásadních problémů aplikace práva v podmínkách informační společnosti. Faktická delokalizace společenských vztahů je totiž přímo rozporná s jedním z nejtradičnějších konceptů práva a současně s jedním z nejstarších principů mezinárodního práva veřejného, tedy s konceptem místní působnosti ve spojení s principem státní suverenity.

Je-li místní působnost práva vztahem mezi fyzickou lokalitou a právním pravidlem, pak v situaci, kdy fyzická lokalita je irelevantní kritérium, pozbývá tento koncept význam. Je-li pak státní suverenita vedle dalších znaků vymezena především územní výsostí, dochází v situaci ideálního stavu informační společnosti k tomu, že nad územím státu konstatujeme existenci jakési informační vrstvy, která je kvůli absenci možnosti lokalizovat informace imunní vůči této územní výsosti. Důvodem je fakt, že kyberprostor,

⁸⁷ K pojmu a jednotlivým aspektům virtuálních identit viz např. Robins, K. Kyberprostor a svět ve kterém žijeme. Revue pro média, roč. 2003, číslo 5, str. 17.

jak naznačeno výše, nezná fyzické hranice⁸⁸. Možnosti řešení problému místní působnosti jsou v zásadě tři, a to:

1. aplikace standardních kritérií místní působnosti v návaznosti na fyzickou lokalizaci informací
2. vytvoření nových kritérií pro aplikaci konceptu místní působnosti (tj. virtuální lokalizace právních vztahů)
3. přiznání existence informační vrstvy bez místní jurisdikce státu

První způsob je v současné době nejrozšířenější. Důvodem je absence specifické legislativy jakož i neochota orgánů autoritativně aplikujících právo narušovat standardní kritéria pro stanovení místní působnosti práva. O tom, zda má smysl činit z hlediska práva a jeho působnosti rozdíl mezi off-line a on-line právními problémy, se vedla a stále ještě vede zanícená debata. Zatímco zastánci konzervativního proudu argumentují tím, že je vždy v určité formě možné zjistit vztah informací a subjektů k území nějakého státu a není tedy důvod hledat speciální řešení, představitelé v současnosti dominantní teorie zastávají názor, že je třeba při řešení otázek působnosti práva a jurisdikce státních orgánů postupovat diferencovaně a hledat jiná a specifická kritéria rozdělení působnosti a jurisdikce než na základě vazby ke státnímu území. Na úrovni špiček právní vědy se tato debata rozhořela nejprve v USA, a to mezi profesory Postem a Goldsmithem. Druhý z nich, zastánce konzervativního přístupu, k tomu uvádí (příklad autor)⁸⁹:

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

⁸⁸ K tomu viz např. Post, D. Governing Cyberspace. The Wayne Law Review, číslo 43, str. 155.

⁸⁹ Viz Goldsmith, J. L. Against Cyberanarchy. Chicago Law Review, číslo 65, str. 1250.

Na tyto argumenty pak reagoval Post replikou, kde na fiktivním příkladu prodejce knih „digitalbooks.com“ ilustroval neudržitelnost tradičního přístupu k řešení problému rozhodného práva a působnosti soudů. Svoji repliku uzavřel následovně (překlad autor)⁹⁰:

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

Postův přístup s větší či menší ochotou postupně přejímají doktrína i soudy nejprve v USA a posléze i v Evropě⁹¹. Neznamená to však, že bychom mohli konstatovat existenci druhé z výše naznačených možností, tj. nastoupení alternativních hraničních určovatелů pro informační sítě. Jak bude rozvedeno dále, pohybují se soudy z důvodu absence specifické úpravy tam, kde je zájem o alternativní přístup, pouze v mezích více či méně standardních kritérií založených na teritorialitě, jako jsou například *locus delicti* či *locus rei sitae*.

Základní problém navýsost nutného vývoje v chápání *de iure* místní působnosti práva v informačních sítích každopádně spočívá v tom, že řada států, především těch mezinárodně významnějších, má přirozenou tendenci zakládat vlastní jurisdikci spíše než si ji omezovat. Objeví-li se tedy právní vztah s mezinárodním prvkem, lhotejno, zda jde o vztah soukromoprávní či veřejnoprávní, můžeme pozorovat snahu národních soudů dostat takový vztah pod vlastní jurisdikci. To je mimo jiné i důvod, proč třetí alternativa naznačená výše nepřipadá z hlediska států v úvahu.

⁹⁰ Viz Post, D.G. Against Against Cyberanarchy. Berkeley Technology Law Journal, roč. 17, číslo 1, str. 23.

⁹¹ Srov. např. Reed, C. Internet Law. Cambridge: Cambridge University Press, 2004, str. 218 a násl. nebo z francouzských publikací Cosson, J.-B. Standard Private International Law Tested by the Networks. In Internet International Law, ed. Georges Chatillon. Bruxelles: Bruylant, 2005, str. 53 a násl.

Vedle snah o extenzivní analogickou aplikaci hraničních určovatelů, o nichž se zmíníme dále, můžeme především ve státech s nižší mírou právní kultury a sebeuvědomění si národní identity pozorovat i opačný extrém, kdy se orgány autoritativně aplikující právo rády zba-vují břemena rozhodování s poukazem na skutečnost, že předmětný vztah „je na internetu.“ Namísto nedostatku místní působnosti práva je však v takových případech spíše argumentováno důkazní nouzí. V České republice tak například policie odložila případ trestného činu pomluvy s poukazem na to, že se uskutečnil na internetovém diskusním fóru a nelze tedy prokázat spáchání trestného činu. Vyšetřovatel se v tomto případě nezabýval zjištěním všech skutečností, které mohou být pro posouzení skutku rozhodné, a k odložení případu si vystačil v podstatě jen s výslechem podezřelého. Rozhodnutí o odložení případu pak napadl ministr spravedlnosti stížností pro porušení zákona a Nejvyšší soud ČR této stížnosti vyhověl. Z rozhodnutí, v němž Nejvyšší soud ČR poskytl vyšetřovateli i obsáhlý návod, jak ve věci dále postupovat, vybíráme: „*Podstata porušení zákona v daném případě spočívá v tom, že vyšetřovatel učinil rozhodnutí o zastavení trestního stíhání obviněného Ing. J. Z. z výše uvedeného důvodu, aniž náležitě zjistil skutkový stav a provedl veškeré dostupné důkazy, které se v této věci nabízely. (...) Dále bylo třeba vyžádat znalecký posudek z oboru výpočetní techniky se zaměřením na software a provést příslušné zkoumání zajištěných internetových stránek nalézajících se pod internetovou adresou, jakož i zřízení internetové schránky na jméno Z. S., s cílem získat údaje směřující k identifikaci osoby, která uvedené stránky a schránku zřídila, včetně údajů, jež by umožnily určit osobu, jež předmětný pomlouvačný text na tyto stránky umístila.*“

Další nutný vývoj místní působnosti práva a *de iure* založení hranic národní jurisdikce uvnitř informačních sítí si však namísto extenzí žádá s ohledem na právní jistotu naopak spíše zdrženlivé omezování působnosti vnitrostátních právních řádů na základě unifikovaných kritérií reflektujících zmíněný fenomén delokalizace. Pozitivní konflikt jurisdikcí může být totiž pro legitimitu a efektivitu práva stejně nebezpečný jako negativní konflikt resp. absence jeho místní působnosti.

4.2 TRESTNÉ ČINY

Trestní právo chrání především vitální zájmy státu a společnosti. Z tohoto důvodu platí princip neoddělitelnosti otázky jurisdikce a rozhodného práva – jinými slovy, trestní soud, je-li příslušný k rozhodnutí ve věci, rozhoduje vždy podle práva svého státu. Uvedené platí i naopak – vztahuje-li se

tedy trestní právo hmotné určitého státu na nějaký skutek, znamená to, že o skutku může rozhodnout i soud tohoto státu⁹².

Trestní legislativa má hranice působnosti i jurisdikce orgánů činných v trestním řízení nastaveny relativně široce. Typicky tak lze stíhat v určité zemi trestné činy, které byly na území příslušného státu nejen přímo spáchány, ale i takové, jejichž následky se na tomto území projeví a v určitých případech i činy, které s tímto územím mají jen nepřímou souvislost. I v České republice tak existuje celá řada trestných činů, které lze orgány činnými v trestním řízení stíhat i v případě, nacházel-li se jejich pachatel v době jejich spáchání mimo naše území.

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

V uvedených případech je zpravidla možné stíhat pachatele v obou resp. ve všech dotčených zemích. Tato situace je však namísto pro orgány činné v trestním řízení spíše příznivá pro samotného pachatele, neboť vyšetření trestného činu a následné provedení příslušných úkonů je nezdědkou otázkou komplikované, zdlouhavé a často i prakticky neefektivní mezinárodní spolupráce⁹³. Ačkoli se policejní a soudní orgány snaží při vyšetřování a usvědčování pachatelů internetových trestných činů vzájemně spolupracovat, často jim v tom kromě rozdílné legislativy brání i složité procesní postu-

⁹² K tomuto základnímu principu trestního práva viz např. Akehurst, M. Jurisdiction in International Law, in *British Yearbook of International Law*. London: Oxford University Press, 1972-1973, str. 179 a násl.

⁹³ Znám je například případ, kdy český policejní vyšetřovatel dožádal šetření o počítačovém trestném činu v Bulharsku. Tamní orgány nejprve informovaly podezřelého o tom, že je na jeho činnost vedeno vyšetřování a požádaly jej o stanovisko. Podezřelý samozřejmě v reakci na to zastavil své aktivity, zlikvidoval veškeré důkazy, které se nacházely v paměti jeho systému, a vyšetřovatelům pak přišel oznámit, že o žádné trestné činnosti neví.

py⁹⁴. V častých případech, kdy klíčovou roli při zjišťování pachatelů a důkazů hraje čas, je tedy prakticky nemožné pachatele odhalit a usvědčit.

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

Prvním z moderních konfliktů tohoto typu řešeným na úrovni mezinárodního práva veřejného byl případ známý pod označením Lotus⁹⁵. Jednalo se o spor mezi Francií a Tureckem o trestní jurisdikci nad posádkou francouzského parníku Lotus, který se v roce 1927 v tureckých teritoriálních vodách srazil s tureckým parníkem, v důsledku čehož přišlo o život několik tureckých námořníků. Otázka trestní odpovědnosti francouzské posádky, která srážku zavinila, pak byla předmětem sporu francouzské a turecké vlády právě na základě pozitivního konfliktu působnosti jejich trestních legislativ. I přes to, že v době spáchání trestného činu byli francouzští námořníci pod teritoriální působností francouzského práva, dal stálý dvůr mezinárodní spravedlnosti nakonec zapravdu Turecku, když ve svém rozhodnutí konstatoval, že „...trestné činy, jejichž pachatel se v době jejich spáchání vyskytoval na území jiného státu, je třeba považovat za spáchané tam, kde se vyskytl jeden z jejich základních elementů, konkrétně jejich účinek.“

Uvedenou koncepci nikoli fyzické, ale efektivní přítomnosti pachatele na území určitého státu lze velmi dobře aplikovat i na případy mezinárodní internetové kriminality⁹⁶. Orgány činné v trestním řízení tak toto řízení obvykle vedou i v případech, kdy se na území jejich jurisdikce pachatel v době spáchání trestného činu nenacházel ani zde přímo ke spáchání trestného činu nedošlo, ale kde se projevil nebo mohl projevit efekt trestného jednání. Tato extenzivní interpretace se tak uplatňuje tam, kde v místě fy-

⁹⁴ Praktické problémy přeshraniční internetové kriminality trefně popsal francouzský soudce Jean-Wilfrid Noël in Noël, J.-W. Internet and Judicial Investigation. In Internet International Law, ed. Georges Chatillon. Bruxelles: Bruylant, 2005, str. 233 a násl.

⁹⁵ Rozhodnutí PCIJ, Ser. A., No. 10, 1927, plný text rozhodnutí včetně disentů viz např. http://www.worldcourts.com/pcij/eng/decisions/1927.09.07_lotus/ Podrobnou analýzu sporu viz v Berge, G. W. The Case of the S. S. Lotus. Michigan Law Review, roč. 26, číslo 4, str. 361 a násl.

⁹⁶ K tomu viz např. Kohl, U. Eggs, Jurisdiction and the Internet. International and Comparative Law Quarterly, číslo 52, str. 577 a násl.

zického pobytu pachatele není skutek trestný, naopak je však trestný tam, kde se projeví jeho účinky⁹⁷.

V jednom z prvních případů přeshraniční internetové kriminality posuzoval Nejvyšší soud státu New York otázku, zda při provozování portálu s hazardními hrami umístěného ve státě Antigua, jehož zákazníci jsou však obyvatelé státu New York, může dojít k založení trestněprávní odpovědnosti. Při diskusi otázky jurisdikce a působnosti trestního práva státu New York soud doslova uvedl⁹⁸ (překlad autor): „*Pokud by tento soud přisvědčil argumentaci žalovaných, že aktivity zaměřené na obyvatele státu New York spadají pod jinou jurisdikci, vyvolalo by to jistě řadu nežádoucích dopadů. Takový přístup by totiž nejen hrubě poškodil soustavný a odhodlaný postup tohoto státu proti nepovolenému hazardu, ale obecně by zbavil odpovědnosti kohokoli, kdo by páchal na internetu skutky, které jsou v tomto státě jinak trestné. Počítačový server nemůže přitom sloužit jako nějaký štít proti odpovědnosti, o to méně pak v tomto případě, kdy obžalovaní přímo zaměřili svou pozornost do státu New York, kde provozovali řadu protiprávních aktivit.*“

Vzhledem ke shora popsáným problémům je však v praxi internetové kriminality spíše běžné, že hlavní slovo mají orgány činné v trestním řízení na území, kde se pachatel aktuálně zdržuje, respektive kde je umístěna jeho komunikační infrastruktura. Ojedinele se dokonce vyskytují i případy, kdy soud odmítne aplikovat své trestní právo v situaci, kdy protiprávní efekt jednání sice prokazatelně (byť jen zčásti) nastal na území domovského státu, pachatel však zde není přítomen a kvůli absenci možnosti zajištění jeho technických prostředků je prakticky nemožné jej efektivně stíhat⁹⁹.

Určitou výjimku z uvedené právní praxe představuje Úmluva Rady Evropy o kyberkriminalitě, která byla otevřena k podpisu 23. 11. 2001 v Bu-

⁹⁷ Podrobný výklad k problematice založení jurisdikce na základě analýzy efektu viz např. Brenner, S. W., Koops, B.-J. Approaches to Cybercrime Jurisdiction. Journal of High Technology Law, roč. 4, číslo 1, str. 19 a násl.

⁹⁸ Příklad je znám jako People v. Interactive Gaming Corp., referenční číslo QDS:22310325, 1999 N.Y. Misc. Lexis 425 (Sup. Ct. N.Y.Co., 24. července, 1999), plný text je možné nalézt např. na adrese http://www.louandy.com/CASES/People_v_WIGC.html.

⁹⁹ Ještě dál šel soudce trestního soudu v Bergamu, když v září 2008 zrušil předchozí nařízení prokurátora příkazující blokaci torrentového serveru Pirate Bay umístěného ve Švédsku, a to s poukazem na skutečnost, že prokuratura nařízením blokace (byť na Italském území) zasáhla do jurisdikce švédských orgánů činných v trestním řízení. Toto rozhodnutí je však svojí argumentací natolik výjimečné, že jej lze považovat spíše za anomální zajímavost.

dapešti¹⁰⁰. Základním momentem Úmluvy jsou především definice jednotlivých skutkových podstat trestných činů¹⁰¹, jež se členské státy zavazují ve svých jurisdikčních stíhat¹⁰². Jedná se o následující typy trestných činů:

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

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

Členské státy se v Úmluvě rovněž zavázaly provést taková legislativní opatření, která jejich orgánům umožní tyto trestné činy vyšetřovat a zajišťovat k tomu odpovídající důkazy¹⁰³. Obě skupiny závazků, tj. závazek zavést do národní trestní legislativy příslušné skutkové podstaty trestných

¹⁰⁰ Plný text Úmluvy v anglickém jazyce viz na adrese <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>.

¹⁰¹ Precizní definice jednotlivých skutkových podstat internetové trestné činnosti představuje přitom jeden z hlavních problémů omezujících působnost trestního práva v kyberprostoru. K tomu srov. Plays, J. Internet and Judicial Investigation: Difficulties in Judicial Practice, in *Internet International Law*, ed. Georges Chatillon. Bruxelles: Bruylant, 2005, str. 245 a násl.

¹⁰² Specifikace skutkových podstat jsou provedeny v čl. 2–11 Úmluvy.

¹⁰³ Závazek zavést do právního řádu příslušná opatření najdeme v čl. 14–21 Úmluvy.

činů a závazek uzákonit odpovídající procesní pravomoci orgánů činných v trestním řízení pak mají jednoznačný cíl zabránit situaci, kdy by některý z nově definovaných tzv. kyberkriminálních činů postrádal v některém členském státě trestnost nebo by zdejší orgány činné v trestním řízení nedisponovaly procesními oprávněními nutnými k tomu čin vyšetřit a prokázat. Dodrží-li tedy státy tyto své základní závazky, měl by zde odpadnout problém existence tzv. bezpečných přístavů pro pachatele internetové trestné činnosti.

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

Článek 22 – Jurisdikce

1 Strany se zavazují přijmout legislativu a další opatření nutné k založení jurisdikce nad činy uvedenými v člácích 2 až 11 této Úmluvy, jsou-li činy spáchány

na území Strany; nebo

na palubě lodi pod vlajkou Strany; nebo

na palubě letadla registrovaného podle práva Strany; nebo

státním příslušníkem Strany, je-li takový čin trestný podle práva státu, kde byl spáchán nebo je-li takový čin spáchán mimo jurisdikci kteréhokoli státu.

2 Strany si mohou vyhradit právo neaplikovat nebo aplikovat jen v určitých případech nebo za určitých okolností pravidla stanovení jurisdikce podle odstavce 1b až 1d nebo kterékoli jejich části.

3 Strany se zavazují přijmout legislativu a další opatření nutné k založení jurisdikce nad činy uvedenými v článku 24 odstavec 1 této Úmluvy v případech, kdy se pachatel nachází na jejich území a není na základě žádosti rozhodnuto o jeho vydání ke stíhání jiné Straně z důvodu jeho státní příslušnosti.

4 Tato Úmluva nevylučuje v žádném případě stanovení jurisdikce Stran dle jejich národního práva.

5 V případě, kdy více Stran nárokuje jurisdikci nad trestným činem dle této Úmluvy, budou zúčastněné Strany, je-li to vhodné, konzultovat s cílem nalézt nejvhodnější jurisdikci pro trestní řízení.

Jak vyplývá zejména ze znění článku 5, neřeší úmluva pozitivní konflikt působnosti orgánů více států v trestním řízení, což je možné považovat v souvislosti s provedeným výkladem za podstatný problém. Otázka delimitace jurisdikce by však v opačném případě zřejmě narazila na limity diskrece jednotlivých států a ústavněprávní limity zejména v otázkách vydávání vlastních občanů k trestnímu stíhání do zahraničí¹⁰⁴. Obě témata jsou přitom pro národní trestní právo natolik závažná a citlivá, že jejich řešení, například formou zdrženlivosti při výkonu trestní jurisdikce, nelze v dohledné době očekávat.

Dalším poněkud problematickým momentem je závazek stíhat určitý trestný čin tehdy, pokud je spáchán na území některé ze stran úmluvy nebo na území mimo územní výsost. Skutečnost, že je povinnost stíhat vázána na lokalitu spáchání činu, nikoli na místo jeho efektu, bohužel nereflektuje delokalizaci řady závažných trestných činů nebezpečných pro informační společnost. Pachatel totiž může spáchat určitý trestný čin a později tvrdit, že jej nespáchal z území některé ze smluvních stran. Je-li zatčen na území jiného státu, než tam, kde se projevil škodlivý efekt, byť je to území pokryté úmluvou, může se vyhnout stíhání prostou námitkou toho, že se v době spáchání trestného činu fyzicky nacházel například v některém ze států pod takzvanou banánovou jurisdikcí¹⁰⁵. Prokázat opak, tj. že byl ve skutečnosti pachatel v době spáchání trestného činu na území některé ze stran Úmluvy, může být značně problematické.

Důkazní nouze ohledně fyzické lokalizace pachatelů trestných činů představuje závažný problém vyšetřování počítačové kriminality. Použití útoků prostřednictvím tzv. zombie počítačů nebo i technicky mnohem triviálnějšího fňgování vlastní IP adresy¹⁰⁶ může účinně zabránit lokalizaci pachatele. Vedle problémů s jeho vypátráním pak může nejistota ohledně

¹⁰⁴ K problému viz. De Vel, G. The Convention on Cybercrime, in *Internet International Law*, ed. Georges Chatillon. Bruxelles: Bruylant, 2005, str. 225 a násl.

¹⁰⁵ Jedná se o hovorový pojem používaný na diskusních fórech především k označení států třetího světa, kde z důvodů závažných společenských, politických nebo hospodářských problémů zůstává problematika kyberkriminality zcela neřešena. Příkladem mohou být Somálsko, Zimbabwe, Bangladéš apod.

¹⁰⁶ Jeden z předních odborníků na problematiku místní působnosti práva na internetu Dan Svatešson dokonce na svých osobních stránkách nabízí jednoduchý podomácku vyrobený doplněk do prohlížeče Internet Explorer, který umožňuje jedním kliknutím libovolně měnit národní IP adresu počítače.

jeho fyzické přítomnosti na území určitého státu v době spáchání trestného činu vést i k výše naznačeným následným obtížím s jeho stíháním, a to dokonce i na území některé ze smluvních stran Úmluvy.

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

Úmluva Rady Evropy o kyberkriminalitě představuje jednu z prvních iniciativ založených s cílem minimalizovat negativní dopad delokalizace internetových aktivit na efektivitu práva¹⁰⁷. Přestože je dosah Úmluvy v některých směrech omezený (zejména co do delimitace jurisdikcí a místní působnosti norem trestního práva hmotného), představuje její koncepce nesporný a relativně významný krok kupředu. Skutečnému naplnění cílů Úmluvy¹⁰⁸ však stále brání relativně nízký počet stran, které ji ratifikovaly¹⁰⁹ a recipovaly do vnitrostátního práva. Opatrně optimisticky však lze hodnotit skutečnost, že Úmluva byla již podepsána většinou evropských států včetně ČR¹¹⁰ a její ratifikace je tak mnohdy spíše otázkou času¹¹¹. Za velice významný pokrok při budování mezinárodní trestní jurisdikce nad

¹⁰⁷ Důležitost mezinárodní harmonizace národních trestních legislativ a praxe trestního řízení byla opakovaně zdůrazňována i v rámci ženevského jednání Mezinárodní telekomunikační unie zaměřeného na problematiku kyberkriminality. Jednotlivé poznatky shrnuje článek Schjolberg, S., Hubbard, A. M. Harmonizing National Legal Approaches on Cybercrime. Geneva: ITU (publikace č. CYB/04). 2005. Volně ke stažení na adrese http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf.

¹⁰⁸ Viz text preambule Úmluvy.

¹⁰⁹ K vývoji Úmluvy viz zpráva z jednání Komise Rady Evropy pro Kyberkriminalitu č. T-CY (2006) 11 – relativně vysoký počet států, které k úmluvě nepřistoupily, ale účastní se jednání Komise, však napovídá o zvyšujícím se zájmu států o tuto problematiku.

¹¹⁰ Do českého trestního zákonodárství se příslušné závazky z Úmluvy měly recipovat především prostřednictvím nového trestního zákoníku, který však z politických důvodů nebyl doposud schválen.

¹¹¹ Celkový počet států, které úmluvu ratifikovaly, je prozatím 19. Na ratifikaci se dále čeká ve 24 státech včetně ČR.

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

4.3 SOUKROMOPRÁVNÍ ZÁVAZKY

Zatímco trestní právo se přímo dotýká vitálních zájmů státu, je smyslem práva soukromého ochrana soukromých zájmů subjektů jednajících ve vzájemně rovném postavení. Stát tak i v případě soukromého práva vykonává jurisdikci nad jednotlivými právními vztahy, ale v jejím prosazování je o poznání méně aktivní a jednotlivé konkrétní momenty mechanismu soukromoprávní regulace jsou v porovnání s trestní regulací pro vitální zájmy státu méně závažné a též méně citlivé.

Zatímco jsou pro trestněprávní úpravu typické principy jako například princip inkviziční či princip postupu *ex officio*, můžeme se v soukromém právu typicky setkat například s principem *vigilantibus iura scripta sunt* nebo s principem dispozičním. Důsledky zásadních rozdílů mezi soukromým a trestním právem můžeme pak vnímat i v oblasti mezinárodní delimitace místní působnosti práva, kdy v soukromém právu dochází k důslednému oddělení hmotného práva od otázek příslušnosti a práva procesního. Zatímco je tedy v trestním právu užito jednoho hraničního určovatele k založení pravomoci a příslušnost soudu jakož i k založení působnosti příslušného hmotného trestního práva, je třeba v soukromém právu přistupovat rozdílně k otázkám práva rozhodného a práva upravujícího proces uplatnění příslušného nároku.

Výjimečné tedy nejsou případy, kdy je k založení pravomoci užito například hraničního určovatele *patria*, zatímco je pro samotné posouzení individuálních nároků rozhodné právo určené dle hraničního určovatele *locus rei sitae* – státy s vyvinutou doktrínou mezinárodního práva soukromého se tedy nebrání (a kvůli vázanosti mezinárodním právem veřejným

často ani nemohou bránit) tomu, aby jejich soudy aplikovaly hmotné soukromé právo cizího státu. Delimitace jurisdikcí resp. působnosti hmotného práva soukromého jde přitom ještě dál, neboť je stranám dána možnost vzájemným ujednáním se z dosahu hmotného i procesního práva určitého státu zcela vymanit respektive obojí si vzájemně dohodnout.

V evropském právním prostoru byla kolizní kriteria pro stanovení rozhodného práva i pravomoci a příslušnosti orgánů jeho autoritativní aplikace harmonizována, a to nejprve ve formě úmluv a později i formou evropských nařízení. Struktura kolizního práva je tedy u členských států tvořena v oblasti procesní především nařízením Rady (ES) č. 44/2001 o příslušnosti a uznávání a výkonu soudních rozhodnutí v občanských a obchodních věcech, a v oblasti hmotného práva pak Nařízením Evropského parlamentu a Rady (ES) č. 593/2008 ze dne 17. června 2008 o právu rozhodném pro smluvní závazkové vztahy (Řím I) a nařízením Rady (ES) č. 864/2007 o právu rozhodném pro mimosmluvní závazkové vztahy (Řím II¹¹²). Subsidiárně se pak uplatňuje zákonné mezinárodní právo soukromé, u nás obsažené především v zákoně o mezinárodním právu soukromém, to však jen v relativně omezeném rozsahu případů nekrytých výše uvedenými předpisy.

Z hlediska důvodu vzniku závazků není prostředí informačních sítí ničím zvlášť specifické. I zde platí, že závazky vznikají z právního jednání nebo z jednání deliktního. Důležitým pro posouzení otázky po rozhodném právu a příslušném orgánu jeho autoritativní aplikace jsou pak rovněž tradiční kriteria označovaná jako hraniční určovatele. Vzhledem k tomu, že doposud nebyly doktrinálně podchyceny ani legislativně upraveny specifické hraniční určovatele pro prostředí informační sítě¹¹³, posuzujeme on-

¹¹² Mimosmluvní závazky byly původně v roce 1972 rovněž zahrnuty do návrhu Římské úmluvy. Harmonizace kolizních kriterií v oblastech jako jsou náhrada škody, nepříkázané jednatelství apod. se však ukázaly být natolik komplikovanými, že úmluva nakonec obsahovala pouze kolizní kriteria k určení práva rozhodného pro smluvní závazky. K tomu srov. Bogdan, M. Torts in Cyberspace: The Impact of the New Regulation Rome „II,“ MUJLT, roč. 2, číslo 1, str. 2. Ani Řím II přitom oblast mimosmluvních závazků plně nepokrývá – z jeho působnosti je vyňata řada oblastí specifikovaných v čl. 1(2).

¹¹³ Jedinou výjimkou doktrinálně vyvinutého hraničního určovatele je národní doména první úrovně (viz dále) – i ta je však pouze subsumována pod hraniční určovatel *legis patriae* ve variantě „jiná provozovna.“

line skutkové situace za užití tradičních určovatelů. Z nejčastěji využívaných a též nejvíce problematických vybíráme k dalšímu stručnému výkladu následující:

- *Patria* – stát, jehož příslušníkem je subjekt (u fyzických osob stát, jehož občanství má subjekt, u právnických osob stát, na jehož území je subjekt registrován)
- *Locus delicti* – místo, kde došlo ke škodní události – může znamenat místo, kde došlo k porušení právní povinnosti, ale též místo, kde se projevil škodlivý následek
- *Locus solutionis* – místo, kde byl nebo měl být plněn závazek

4.4 LOCUS DELICTI

Dojde-li na internetu k zásahu do subjektivního soukromého práva, nejčastěji pak do některého z práv absolutních¹¹⁴, lze vedle obecného soudu rušitele alternativně žalovat i u soudu v místě, kde došlo nebo mohlo dojít k výskytu škodlivého následku. Slovy čl. 5(3) nařízení (ES) č. 44/2001 je tedy možné žalovat „*ve věcech týkajících se deliktů nebo kvazideliktů odpovědnosti u soudu místa, kde došlo nebo může dojít ke škodné události.*“ Ať už se žalobce rozhodne pro obecné nebo alternativní fórum, bude příslušný soud rozhodovat zpravidla podle práva místa, kde škoda vznikla - Nařízení (ES) č. 864/2007 tak jako rozhodné právo u civilních deliktů označuje „*právo země, kde škoda vznikla, bez ohledu na to, ve které zemi došlo ke skutečnosti, jež vedla ke vzniku škody, a bez ohledu na to, ve které zemi nebo kterých zemích se projeví nepříme následky této skutečnosti.*“

Dojde-li ke škodní události na internetu, vyvstává zásadní otázka, jak ve smyslu uvedených ustanovení uvést jeho internetovou lokaci do souvislosti s jurisdikcí soudu určitého státu. Tento skutkový problém je přitom nejen zásadně důležitý pro určení fóra a rozhodného práva ale též mimořádně obtížný tam, kde škodlivý následek nastal na některém z právem chráně-

¹¹⁴ Do této kategorie řadíme především právo vlastnické, práva od něj odvozená a dále pak práva osobnostní jako je právo na ochranu osobnosti, jména, apod.

ných objektů informačního charakteru nebo tam, kde byla dominantním prostředkem k jeho dosažení některá ze služeb informační společnosti. Za místo škodní události se přitom navíc nemusí považovat jen místo, kde se škoda projevila, ale též místo, kde došlo k jednání nebo opomenutí, které škodní událost založilo¹¹⁵.

Vztah *loci delicti* k území určitého státu je v takových případech poznamenán výše nastíněným fenoménem delokalizace, především pak v tom směru, že je zde prakticky lhostejné, kde fyzicky došlo k nastoupení dominantního důvodu ke vzniku závazku *ex delictu*, tj. na území kterého státu došlo k protiprávnímu jednání nebo výskytu protiprávního stavu. Přenos informace jako důvodu ke vzniku deliktního závazku v informační síti mezi různými státy je totiž triviálně jednoduchý a tam, kde závazek vzniká protiprávním jednáním, je dokonce zcela otázkou libovůle škůdce.

Stejně problematické je i kritérium umístění projevu škodlivého následku, tj. místa nastoupení škodní události. Je-li tak příkladně poškozena reputace uživatele mezi jeho spoluhráči na internetovém pokerovém serveru, vyvstává otázka, ve kterém státě byl vlastně dotýčný subjekt poškozen – nabízí se v tomto případě hned několik relevancí víceméně vyrovnaných interpretací od domicilu poškozeného přes umístění serveru až po domicil většiny pohoršených uživatelů.

Z výše uvedených důvodů se stal *locus delicti* pravděpodobně nejproblematictějším ze všech hraničních určovatелů. V praxi můžeme zatím nalézt tři dominantní přístupy, a to:

- Extenzivní přístup
- Analytický přístup
- Restriktivní přístup

Přístup extenzivní považuje za místo internetové škodní události libovolné místo, kde se informace mohou stát způsobilými škodit. Touto interpretací tak lze, a to nejen u ohrožovacích deliktů, založit pravomoc prakticky jakéhokoli civilního soudu na základě konstatování, že se v obvodu tohoto soudu (resp. na území státu) lze připojit k internetu. Obdobně pak

¹¹⁵ Evropský soudní dvůr se k této otázce vyjádřil v roce 1976 v rozhodnutí Bier v. Mines de Potasse d'Alsace, publ. v European Court Reports č. 1735.

Ize prakticky libovolně konstatovat i působnost hmotného práva. Poněkud umírněnější variantou tohoto přístupu je doktrína dominantního efektu, kde je k výše uvedenému ještě třeba prokázat, že na určitém místě došlo k nejzávažnějšímu poškození práva nebo právem chráněného zájmu.

Jedním ze světově nejznámějších a rovněž nejdiskutovanějších precedenčních případů týkajících se určení fóra a rozhodného práva byl spor známý pod označením Gutnick v. Dow Jones¹¹⁶. Spor se týkal oznámení uveřejněného na zpravodajských internetových stránkách provozovaných žalovaným. V říjnu 2000 se na stránkách internetového časopisu *Baron's on-line* objevil článek s titulkem „Nekalé výdělký“, který referoval o podnikatelských aktivitách australského podnikatele židovského původu a pozdějšího žalobce Josepha Gutnicka. Gutnick se proti tomuto článku rozhodl bránit soudně, neměl však zájem žalovat vydavatele časopisu, společnost Dow Jones, u soudu v místě jejího sídla – řízení by totiž bylo nejen nákladné, ale především by byla vzhledem k existenci prvního dodatku Ústavy USA velmi malá pravděpodobnost úspěchu. Rozhodl se tedy podat žalobu v Austrálii a argumentoval právě kritériem místa vzniku škody. Újma mu tak podle jeho argumentace měla vzniknout právě v Austrálii, kde bylo možné si na internetu předmětný článek přečíst a kde žila židovská komunita, jejímž členem Gutnick byl a v jejímž rámci mohla jeho reputace nejvíce utrpět. Soud těmto argumentům přisvědčil, když uvedl, že (překlad autor) „za místo, kde se uskutečnila pomluva, je třeba považovat místo, kde došlo k újmě na cti poškozeného. (...) Informace šířené prostřednictvím WWW mají formu způsobitou naplnit skutkovou podstatu pomluvy teprve tehdy, jsou-li přesunuty do počítače osoby, která k nim přistupuje prostřednictvím svého WWW prohlížeče. Místem, kde dochází k újmě na cti je tedy právě to místo, kde uživatel stahuje informace z příslušného WWW serveru.“ Když však Gutnick žádal o uznání a výkon rozhodnutí v USA, byl mu tento odepřen s poukazem právě na první dodatek Ústavy USA týkající se svobody projevu – rozhodnutí tak bylo sice pravomocné ale prakticky nevykonatelné. Strany nakonec spor definitivně ukončily dohodou v hodnotě 440.000 USD.

Podobě jako u subjektivních práv osobnostních stojí otázka příslušnosti soudu a rozhodného práva i v ostatních případech deliktů odpovědnosti. Kromě osobnostních práv se přitom nejčastěji setkáváme se zásahy do práva vlastnického, na internetu pak konkrétně s porušováním různých typů práv duševního vlastnictví.

¹¹⁶ Spor rozhodoval nejprve v roce 2001 soud státu Victoria pod č.j. [2001] VSC 305, o odvolání pak rozhodoval Vrchní soud Austrálie v roce 2002 pod č.j. [2002] HCA 56. Plný text rozhodnutí Vrchního soudu Austrálie viz např. na adrese http://www.austlii.edu.au/au/cases/cth/high_ct/2002/56.html.

Evropské soudy řeší problém místa výskytu škodní události podobně jako je tomu v Austrálii či Kanadě¹¹⁷. Poškozený pak má možnost vybírat mezi celou řadou jurisdikcí a tehdy, pokud má možnost uplatnit více nároků současně (např. nárok z titulu ochranné známky, ochrany osobnosti a k tomu ještě postih nekalé soutěže), může dokonce různé nároky adresovat různým soudům podle toho, ve kterých státech je pro něj příznivější právní situace. Jedna škodní událost se tak dokonce může stát předmětem řízení ve více státech současně¹¹⁸. Oproti interpretační doktríně založené rozhodnutím Gutnick však mají v některých případech evropské soudy dokonce tendenci vůbec nepřihlížet k materiálnímu kritériu nejzávažnějšího projevu škodlivého následku a na základě formálního kritéria dostupnosti internetu aplikují extenzivní přístup prakticky bez jakýchkoli korektivů.

Příkladem ilustrujícím výše uvedené je spor mezi francouzskou společností SG 2 a německou společností Brokat o užití ochranné známky 'payline'.¹¹⁹ Německá společnost měla známku zaregistrovanou a používala ji k označení svého platebního systému Brokat-Payline. Francouzská společnost si však shodnou známku již dříve zaregistrovala ve Francii pro tentýž typ služeb a rozhodla se bránit proti jejímu užití na německých stránkách brokat.de. Francouzský soud v Nanterre posoudil celou záležitost tak, že místem škodní události je i Francie, neboť na jejím území lze prostřednictvím internetu ke stránce brokat.de přistupovat. Soud nepřesvědčily ani argumenty německé společnosti, že stránky jsou umístěny v Německu, jsou v němčině, služba, pro kterou je označení použito, je určena pro německé

¹¹⁷ Kanadské soudy přejaly argumenty užití v případě Gutnick a kloní se tak rovněž ke koncepci extenzivního stanovení jurisdikce. K tomu viz Paterson, M. Following the Right Lead: Gutnick and the Dance of Internet Jurisdiction. *Canadian Journal of Law and Technology*, roč. 4, číslo 1, str. 49 a násl.

¹¹⁸ Nejedná se přitom o porušení principu litispence založeného článkem 27 Nařízení, neboť z pohledu práva se jedná o zásahy do různých subjektivních práv a tudíž o různé škodní události. K tomu shodně viz Bogdan, M. Internet and Private International Law. In Polčák R. a kol. *Introduction to ICT Law (selected issues)*. Brno: Masarykova univerzita, 2007, str. 22 a násl.

¹¹⁹ Případ rozhodnul dne 13. 10. 1996 Apelační soud v Nanterre a vyjadřovala se k němu, zpravidla negativně, řada komentátorů – viz Kur, A. Identical Marks Belonging to Different Owners in Different Countries. (How) Can They Coexist in Cyberspace? *The Journal of World Intellectual Property*, ročník 3, číslo 2, str. 307–319 nebo též Bettinger, T., Thum, D. Territorial Trademark Rights in the Global Village - International Jurisdiction, Choice of Law and Substantive Law for Trademark Disputes on the Internet. *IIC*, číslo 31, str. 166–167. Uvedení případu do souvislosti s českým právem viz Slováková, Z. Protection of trademarks and the Internet with respect to the Czech law. *Journal of International Commercial Law and Technology*, ročník 2, číslo 1, str. 73.

zákazníky a že společnost o expanzi s touto službou do Francie ani neuvažuje. Bylo tedy vydáno poněkud pitoreskní a prakticky nevykonatelné rozhodnutí, jehož enunciatem zakázal francouzský soud německé společnosti užívat ochrannou známku 'payline' na francouzském území a to včetně jejího užití na internetu.

Jak je vidět, výše popsaný extenzivní přístup ke stanovení jurisdikce je sice možný a v Evropě i zámoří relativně oblíbený, problémy s uznáním a výkonem příslušného soudního rozhodnutí jej však činí pro praxi značně problematickým – to i v prostředí, kde jsou jednotlivé jurisdikce vzájemně propojeny delimitačními a transferovými pravidly jako je tomu v případě zemí EU¹²⁰. Významným argumentem proti jeho aplikaci zejména na otázky ochrany osobnosti je pak *reductione ad absurdum* vyložený praktický dopad této koncepce – může-li totiž být škodním místem území státu, kde lze informace stáhnout do počítače a posléze zobrazit, znamená to, že takovým místem je potenciálně každý stát světa. Jakákoli internetová publikace by tedy vzato *ad absurdum* musela být v souladu s právními řády všech států světa, což by však na původce publikace kladlo poněkud nepřiměřené nároky. Zejména s tímto argumentem proti extenzivnímu stanovení jurisdikce pak vystupují novináři a obecně publicisté. Jejich argument neúměrným zatížením svobody slova¹²¹ se přitom, alespoň co se týče soukromoprávní ochrany osobnosti, zdá být rozumný a odůvodněný.

Neúměrné rozšiřování počtu jurisdikcí, do nichž může spadat zásah do subjektivního práva na internetu, vedl k vytvoření přístupu, který můžeme označit jako analytický. Tato koncepce je založena na analýze příslušného právního vztahu, respektive formy, jíž byl na internetu založen. Místo škodní události je tedy určeno nikoli jen ve vztahu k samotné škodě či újmě ale i s ohledem na způsob, kterým k nim došlo nebo mohlo dojít. Nejznámější z analytických klasifikací míst škodních událostí je takzvaná škála

¹²⁰ Vedle stanovení pravidel pro založení jurisdikce včetně principů litispence obsahuje nařízení č. 44/2001 (dříve Bruselská úmluva) i sadu ustanovení zajišťujících tzv. volný pohyb civilních soudních rozhodnutí, zejména co do jejich uznávání a výkonu v evropském justičním prostoru.

¹²¹ Nemusí se nutně jednat přímo o omezení svobody slova, ale o neúměrné zatížení autora veřejného projevu povinností (a jí odpovídajícím strachem) znát soukromoprávní úpravu ochrany osobnosti všech států světa a vědět o potenciální existenci subjektů dotčených příslušnou publikací.

Zippo. Svůj název dostala po často citovaném americkém případě známém jako případ Zippo.

V případě Zippo Mfr. Co. v. Zippo Dot Com, Inc.¹²² rozhodoval soud o porušení práv k ochranné známce. Základní otázkou však bylo nejprve určení jurisdikce a rozhodného práva. Soud zde jako součást argumentace vytvořil tříprvkovou škálu možných případů zásahu do subjektivního práva, a to na základě posouzení kvality vzájemné komunikace. Doslova se v rozhodnutí uvádí (překlad autor): „Naše posouzení společně s analýzou doposud známých soudních rozhodnutí a dalších předložených důkazů nás vede k úvaze, že to, zda zde existuje příslušnost k projednávání věci, závisí na povaze a druhu výdělečné činnosti, kterou žalovaný provozuje v prostředí sítě Internet... Na jedné straně stupnice stojí případy, kdy žalovaný bez pochyby podniká v prostředí sítě internet. Pokud tedy žalovaný kontrahuje se subjekty pod cizí jurisdikcí, což obnáší vědomou a opakovanou výměnu dat prostřednictvím sítě Internet, je třeba konstatovat příslušnost soudu. Druhou stranu stupnice představují případy, kdy žalovaný pouze umístil určité informace na svoji WWW prezentaci, která je přístupná uživatelům pod cizí jurisdikcí. Taková pasivní WWW prezentace, která jen zprostředkovává informace těm, kteří o ně projeví zájem, nemůže být základem k prohlášení příslušnosti soudu. Mezi oběma krajními body stojí takzvané interaktivní WWW prezentace, kde může probíhat výměna informací mezi uživatelem a serverem, na němž je tato prezentace umístěna. V těchto případech je třeba zkoumat míru interaktivity a povahu informační výměny uskutečňované prostřednictvím WWW prezentace.“

Škála Zippo se stala základem pro posuzování případů tzv. internetové jurisdikce zejména v USA. V porovnání s evropským přístupem se toto řešení jeví být poněkud restriktivní, jeho nesporným kladem je však ochrana internetových publicistů před neúměrnou zátěží svobody slova nutností znát právní úpravy všech států, kam se příslušný informační obsah může prostřednictvím internetu dostat. I nadále však zjišťujeme, že většina složitých případů spadá do druhého stupně škály, tzn. je třeba hodnotit jejich vztah k území jednotlivých dotčených jurisdikcí *ad hoc*. I z tohoto důvodu se stále množí případy, kdy precedenční rozhodnutí Zippo nelze použít jako základ pro argumentaci¹²³. Lze tedy v této otázce poněkud pesimisticky

¹²² Rozhodnutí referenční číslo 952 F. Supp. 1119 (W.D. Pa. 1997) - plný text rozhodnutí viz např. na adrese

<http://cyber.law.harvard.edu/metaschool/fisher/domain/dncases/zippo.htm>

¹²³ K tomu srov. např. Awoyemi, B. Zippo is dying, should it be dead? The exercise of personal jurisdiction by U.S. federal courts over non-domiciliary defendants in trademark infringement lawsuits arising out of cyberspace. *Marquette Intellectual Property Law Review*, ročník 9, číslo 1, str. 37 a násl.

uzavřít, že univerzálně použitelná teorie určení *loci delicti* v současné době schází a pravděpodobně ještě nějakou dobu scházet bude¹²⁴.

Příklady známkových sporů, sporů z práv na ochranu osobnosti a další případy sporného zásahu do subjektivních práv na internetu ukazují, že i relativně jednoduchá škodní událost může znamenat co do určení jurisdikce a rozhodného práva obtížný právní problém. Za stávající situace se však jediným řešením jeví být postupná harmonizace v činnosti civilních soudů pod vlivem mezinárodní doktríny. Někteří autoři se sice pokoušejí prosadit pro konkrétní otázky řešení formou přímo použitelných mnohostranných mezinárodních úmluv¹²⁵, je však třeba s politováním konstatovat, že k úspěchu podobných iniciativ stále schází elementární politická vůle na straně jednotlivých států.

4.5 LOCUS SOLUTIONIS

Locus solutionis, tedy místo plnění, je typickým hraničním určovatelem kolizních norem stanovících působnost smluvního práva. Tam, kde internet slouží jen jako komunikační prostředek k uzavření smlouvy, nebývá obvykle se stanovením rozhodného práva a určením příslušného orgánu problém. Nastává-li tedy plnění mimo internet, je možné obvykle určit jeho místo na základě klasických kritérií v mezích státních hranic¹²⁶. Je-li však

¹²⁴ Srov. např. Yokoyama, D. T. You Can't Always Use the Zippo Code: The Fallacy of a Uniform Theory of Internet Personal Jurisdiction. *Depaul Law Review*, číslo 54, str. 1146 a násl.

¹²⁵ Z nejvýznamnějších iniciativ můžeme jmenovat například návrh úmluvy o příslušnosti ve věcech ochrany osobnosti, který na konferenci Cyberspace 2005 představil australský expert švédského původu Dan Svantesson. Svou představu později konkretizoval v monografii Svantesson, D. *Private International Law and the Internet*, Alpen aan den Rij: Kluwer Law International, 2007, str. 353 a násl.

¹²⁶ V případě nařízení (ES) č. 44/2001 je tak dle čl. 5(1b) místem plnění „v případě prodeje zboží místo na území členského státu, kam podle smlouvy zboží bylo nebo mělo být do-áno.“

předmětem plnění služba spočívající v poskytnutí určité informace, může být místo plnění sporné¹²⁷.

Vzhledem k tomu, že na řešení problému místa plnění na internetu není u nás odpovídající judikatura, můžeme jednotlivé možnosti pouze diskutovat. První z nich, tj. že za místo plnění lze považovat místo, kde se strana smlouvy v okamžiku plnění nachází, odpovídá tradičnímu pojetí *loci solutionis*. Na internetu však narážíme na problém libovolné volby místa plnění, neboť k internetu lze přistoupit z území kterékoli jurisdikce a volba místa je pak zcela na oprávněném. Povinný tedy nemá možnost místo plnění ovlivnit a dokonce ani předvídat. Tato skutečnost může být problematickou zejména v situacích, kdy by oprávněný volil *locus solutionis* spekulativně s úmyslem získat tím pro sebe nepřiměřenou výhodu, tj. přesunul by se například k přijetí plnění na území státu, jehož hmotné právo by mu vzhledem ke kvalitě plnění poskytovalo nejvyšší standard ochrany.

Další možností je svázat *locus solutionis* s místem, kde jsou informace připraveny k „vzvednutí“ oprávněným. Takovou metodu by bylo možné uplatnit tam, kde oprávněný aktivně přistupuje ke službě povinného a informace zde získává nebo tam, kde plnění probíhá přímo na infrastruktuře povinného. Příkladem mohou být reklamní služby, kdy je reklama jako taková umístěna na serveru povinného a může být na základě přístupu uživatelů zobrazena v libovolné jurisdikci. Argument proti takovému stanovení jurisdikce je přesně opačný k argumentu proti řešení postupu dle předchozího odstavce. Povinný stejně jako oprávněný totiž může takto kvalifikované místo plnění zpravidla libovolně volit a může s volbou opět spekulovat.

Zásadním problémem obou možných metod určení *loci solutionis* však jsou technické charakteristiky celé řady služeb informační společnosti. Technický charakter řady plnění totiž neumožňuje identifikovat jurisdikci podle místa, kde se v době plnění nachází oprávněný ani podle místa, kde je umístěna infrastruktura povinného. Spočívá-li tedy plnění například v umístění bannerové reklamy ve výměnném systému, nastává fyzicky plnění všude, kde je banner zobrazen nebo kde na něj uživatelé kliknou (tj. na

¹²⁷ U služeb je podle čl. 5(1b) místem plnění „místo na území členského státu, kde služby podle smlouvy byly nebo měly být poskytovány.“

počítačích uživatelů). Infrastruktura, kde je plnění poskytováno, pak může být rovněž rozprostřena přes desítky jurisdikcí, neboť banner může být v rámci výměnného systému zobrazován periodicky na stovkách stránek zaráz. Můžeme tedy v této otázce konstatovat, že nátura řady internetových závazků prakticky znemožňuje určité (předvídatelné) použití hraničního určovatele *locus solutionis*. Někteří autoři se přesto pokusili definovat základní kritéria pro použití určovatele *loci solutionis* v konkrétních případech poskytování síťových informačních služeb¹²⁸ - i zde však bývá závěr značně relativistický a obecně prakticky nepoužitelný.

Specifický problém představuje kritérium místa plnění u spotřebitelských smluv. Zde je předpokládána materiální nerovnost subjektů vyrovnána formální nerovností co do možností uplatnění alternativních kritérií ke stanovení příslušnosti soudů založených ve prospěch spotřebitele, jakož i omezením pro doložky o volbě fóra¹²⁹. Kritérium *loci solutionis* je zde až na výjimky nahrazeno hraničními určovateli *loci patriae*.

4.6 PATRIA VE FORMĚ „JINÁ PROVOZOVNA“

V českém právu si pod pojmem provozovna obvykle představíme klasickou organizační složku podniku. Použití tohoto pojmu v nařízení (ES) 44/2001 i v nařízení (ES) 874/2007 je tedy v takových souvislostech mírně problematické, neboť na rozdíl od českého práva¹³⁰ nezahrnuje jen standardní formy podřízených organizačních jednotek, jako jsou kanceláře nebo sklady, ale může nás vést i k extenzivní interpretaci, pod niž lze podřadit i takové formy podnikání, které nutně nesouvisejí s materiálním zázemím.

Někteří autoři v této souvislosti paušálně odmítají takovou extenzivní interpretaci, která by vedla k založení pravomoci soudů na základě kritérií,

¹²⁸ Viz Reed, C. *Internet Law*. Cambridge: Cambridge University Press, 2004, str. 223 a násl.

¹²⁹ Viz zejm. čl. 15 – čl. 17 Nařízení. Obdobná omezení se aplikují i na stanovení rozhodného práva.

¹³⁰ Srov. § 7 odst. 3 zákona č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů nebo § 17 odst. 1 zákona č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon), ve znění pozdějších předpisů.

jako je fyzické umístění serverů, na nichž se nacházejí příslušná data či na základě národních domén, pod nimiž jsou registrována příslušná doménová jména¹³¹. Takové paušální odmítnutí extenzivní interpretace čl. 5(5) nařízení (ES) 44/2001 resp. čl. 23(1) nařízení (ES) 874/2007 s poukazem na nedostatečnou určitost kritéria fyzického nebo virtuálního umístění dat však lze ve vztahu ke smyslu a účelu obou nařízení považovat za až příliš formalistické a tedy neadekvátní¹³². Při interpretaci pojmu jiné provozovny (v angl. verzi *other establishment*) je totiž třeba vyjít z jeho materiální podstaty a zkoumat *ad hoc* splnění jeho materiálních znaků, které s postupem času formulovala ustálená judikatura Evropského soudního dvora. V judikatuře se tak sice nesetkáme s přímou odpovědí na otázku, zda může fyzické umístění dat nebo jejich virtuální lokalita (např. adresa s národní doménou první úrovně) naplnit pojem jiné provozovny, je z nich však možné abstrahovat základní znaky, které by jiná provozovna měla ve smyslu založení příslušnosti místního soudu vykazovat. Ústředním momentem je pak znak relativní trvalosti a autonomie příslušné provozovny. K němu pak přistupuje znak materiální způsobilosti provozovny vykonávat samostatně určitou činnost.

Zásadním rozhodnutím Evropského soudního dvora k pojmu jiné provozovny bylo rozhodnutí o předběžné otázce ve věci Somafer SA v Saar-Ferogas AG¹³³. Zde soud interpretoval čl. 5(5) Bruselské úmluvy, konkrétně pak pojem jiné provozovny a jako základní znaky uvedl právě relativní autonomii a trvalost provozovny. Doslova pak soud konstatoval, že za místo jiné provozovny je možné považovat (překlad autor): „místo, které budí zdání trvalosti, tj. např. jako rozšíření domovské organizace, má vlastní management a je vybaveno k tomu, aby mohlo sjednávat obchody s třetími osobami, které přestože mohou vědět, že v případě nutnosti je založen vztah mezi nimi a domovskou organizací, jejíž orgány jsou v zahraničí, nemusejí s domovskou organizací jednat přímo ale mohou obchodovat v tomto místě.“

V otázce kritéria fyzického umístění dat můžeme tedy dojít k závěru, že skutečnost, že jsou data porušující práva či právem chráněné zájmy fyzicky

¹³¹ Srov. např. Sehnálek, D. Mezinárodněprávní aspekty regulace e-commerce. Disertační práce, Brno: Masarykova univerzita, 2006, str. 155.

¹³² Je v tomto směru nepochybné, a vyplývá to i z preambule Nařízení, že *ratio legis* zde přímo koresponduje s požadavkem rozumného uspořádání vztahů.

¹³³ Viz rozhodnutí č. 33/78 ze dne 22. listopadu 1978, publ. v European Court reports 1978, str. 02183.

umístěna v určitém státě, nezakládá *per se* jurisdikci místních soudů. Tuto tezi podporuje i autentická interpretace provedená *expressis verbis legis* v čl. 2(c) směrnice o elektronickém obchodu¹³⁴. Komunikační infrastruktura však může být provozována i způsobem, který naplňuje výše uvedené znaky jiné provozovny, tzn. jedná-li se o takový provoz, který funguje s určitou mírou autonomie vzhledem k podniku jako celku. S takovou situací se můžeme běžně setkat u podnikatelů, kteří provozují relativně autonomní tzv. datové sklady, datová či serverová centra, servisní střediska, a podobně, která relativně autonomně zajišťují pro podnik provoz síťové infrastruktury. U tzv. virtualizovaných globálních podniků¹³⁵ dochází často k tomu, že jsou různé činnosti provozovány z různých míst po světě – online obchod tedy může být usazen v některém z daňových rájů, sklady může mít rozesety dle geografických dispozic své činnosti a komunikační infrastrukturu může provozovat ze servisních středisek umístěných tak, aby byla denním provozem plynule pokryta potřeba nepřetržité údržby. Dojde-li pak činností některého ze servisních středisek k porušení právních povinností, není důvod odmítat jurisdikci soudu v místě, kde se příslušné středisko nachází¹³⁶.

V porovnání s fyzickým umístěním informací je mnohem problematičtější ale též zajímavější kritériem virtuální či spíše logické umístění dat, respektive lokalizace informací v prostoru vymezeném logicky (nikoli fyzicky). Koncepce virtuálních hranic států vymezených logickým kritériem (v tomto případě národní doménou první úrovně¹³⁷) je přitom z teoretického hlediska velmi lákavá. Reflektuje totiž již zmíněný fakt, že jakákoli delimitace působnosti práva v kyberprostoru je prakticky nezávislá na

¹³⁴ Článek 2(c) in finem 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) vyjímá pouhé použití komunikační infrastruktury z rozsahu čl. 5(5) Nařízení, když stanoví, že „existence a používání technických prostředků a technologií nezbytných k poskytování služby nevytváří samy o sobě usazení poskytovatele.“

¹³⁵ K pojmu virtualizace a virtualizovaného podniku viz např. monografii Lévy, P. *Becoming Virtual – Reality in the Digital Age*. New York: Plenum Trade, 2002.

¹³⁶ V tomto případě to může být bez ohledu na kriteria *legis patriae* nebo *legis causae*.

¹³⁷ Kromě národních domén první úrovně budeme jen těžko hledat jiné logické kritérium, které jednoznačně identifikuje informaci komunikovanou on-line s některým ze států.

prostorových hranicích jednotlivých států¹³⁸. Veškerá tradiční kritéria pro stanovení jurisdikce a rozhodného práva se tak potýkají s potřebou umělého (fiktivního) vytvoření souvislosti mezi daty komunikovanými prostřednictvím informační sítě a územím státní jurisdikce¹³⁹, což v důsledku vede ke kontraproduktivní fakticitě s negativním vlivem na efektivitu práva¹⁴⁰. Z omezení daných potřebou spojovat logické skutečnosti s fyzicky vymezenými kritérii působnosti práva pak profitují chaotické elementy kyberprostoru – noční můrou pro efektivitu práva tak v tomto směru může být například server s dětskou pornografií umístěný na skále uprostřed oceánu a připojený k internetu satelitní linkou.

Uvedený faktický problém by s přijetím alternativního kritéria logických (nikoli fyzických) hranic aplikace práva mohl být překonán. Nejde přitom jen o problematiku alternativního hraničního určovatele „jiná provozovna,“ neboť logicky by bylo možné definovat i jiné typy hraničních určovatelů jako *patria*¹⁴¹ či *locus delicti*. Jedině současná definice kritéria jiné provozovny je však ve spojení se znakem národní domény první úrovně k tomuto účelu v našem právním prostředí aktuálně použitelná a tedy se jí stručně z tohoto důvodu zabýváme.

Názor, že za jinou provozovnu je možné považovat usazení informací pod národní doménou první úrovně, není v tomto smyslu možné považovat jen za úlet či výstřelek vědy mezinárodního práva soukromého. Argumenty, s nimiž přichází i přední evropští experti na mezinárodní právo soukromé¹⁴² se především zakládají na subsumovatelnosti www prezentace pod národní doménou pod materiální kritéria definovaná pro jinou provozovnu Evrop-

¹³⁸ Toto tvrzení lze přitom podepřít argumenty nejen technickými ale i sociologickými – srov. Bernam, P.S. The Globalization of Jurisdiction. University of Pennsylvania Law Review, číslo 151, str. 417 a násl.

¹³⁹ Srov. např. Johnson, D. R., Post, D., G. Law and Borders: The Rise of Law in Cyberspace. Stanford Law Review, číslo 48, str. 1367 a násl.

¹⁴⁰ Na tento problém reaguje i Barlow ve své deklaraci, když hovoří o rozprostření myšlenek přes území jurisdikcí i mimo ně.

¹⁴¹ Vizionářsky se hovoří například o on-line cestovních pasech – srov. Bernam, P.S. The Globalization of Jurisdiction. University of Pennsylvania Law Review, číslo 151, str. 378 a násl.

¹⁴² Srov. Bogdan, M. Internet and Private International Law, in Polčák R. a kol. Introduction to ICT Law (selected issues). Brno: Masarykova univerzita, 2007, str. 26 a násl.

ským soudním dvorem. On-line prezentace je totiž relativně autonomní jednotkou disponující vlastními možnostmi komunikace¹⁴³.

Další zásadní materiální argument spočívá v tom, že registrací národní domény se příslušný subjekt (ať už z jakéhokoli důvodu) až na výjimky¹⁴⁴ hlásí k příslušnosti k určitému státu. Jsou-li pak nějaké informace komunikovány pod takto registrovaným doménovým jménem, může se jejich příjemce oprávněně domnívat, že jejich původce má k příslušnému státu vztah. Registrací doménového jména pod národní doménou lze tak získat i určitou výhodu spočívající ve ztotožnění informací se sociálním, kulturním či ekonomickým zázemím příslušného státu. Není pak v této souvislosti důvod uvažovat o tom, že by snad z tohoto ztotožnění měla být vydělena souvislost právní respektive souvislost s právem příslušného státu. Irelevantní je pak v tomto směru i rozlišování toho, zda národní doménová jména registruje doménová autorita soukromá či státní.

Z teoretického hlediska nikoli evidentní avšak možnou interpretací dobrovolné registrace doménového jména s národní doménou první úrovně je srovnání takového aktu s nikoli předpokládanou ale o to zajímavější dobrovolnou identifikací subjektu se státem a s legitimačním základem státního práva tvořeným společenskou smlouvou. Registraci doménového jména není samozřejmě možné *ipso suo* považovat za deklaraci občanství potvrzenou příslušnou doménovou autoritou, aspekt dobrovolnosti ve spojení s momentem identifikace je však mocným argumentem použitelným dokonce i proti paušálnímu odmítnutí působnosti práva na internetu z důvodu neexistující společenské smlouvy, jehož diskusi jsme provedli v úvodu tohoto článku.

¹⁴³ Zásadním je v tomto směru existence virtuální identity způsobilé zavazovat právnickou nebo fyzickou osobu, která prezentaci provozuje. K tomu srov. např. výklad ke konstrukci a platnosti on-line smluv in Katz, A. W. *Is electronic contracting different?* New York: Columbia University, 2004, dostupný on-line na adrese <http://www.columbia.edu/~ak472/papers/Electronic%20Contracting.pdf>.

¹⁴⁴ Je třeba přiznat, že některé národní domény získaly popularitu a jsou hojně registrovány bez toho, aby registřanti či uživatelé i jen uvažovali o spojení zde komunikovaných informací s příslušným státem. Takových domén je však minimum – jako příklad můžeme jmenovat národní doménu .tm, kterou sice provozuje turkmenská národní doménová autorita, její obliba je však dána tím, že zkratka „tm“ označuje ochrannou známku.

Stran praktické použitelnosti národní domény první úrovně jako identifikátoru použitelného pro hraniční určovatel místa jiné provozovny bude samozřejmě záležet především na ochotě národních soudů tuto interpretaci přijmout. Jak vyplývá z uvedené argumentace, je taková interpretace s ohledem na okolnosti *de iure* možná a především ve státech, jejichž soudy jsou pověstné extenzivní interpretací kolizních norem ve prospěch vlastní jurisdikce a užití vlastního rozhodného práva¹⁴⁵, dokonce i pravděpodobná.

4.7 SPRÁVNÍ JURISDIKCE

Zatímco trestní i soukromé právo se mají možnost při vyrovnávání se s nově nastolenými problémy internetové jurisdikce opřít o více či méně tradiční mechanismy a principy, správní právo bylo s příchodem společenských vztahů nové kvality zastíženo, obrazně řečeno, s kalhotama napůl staženými. Normy správního práva či též jednoduchého práva státního si tak neměly až na výjimky možnost postupně zvykat na existenci vztahů, jejichž aspekty nutí státní orgány uvažovat v mezinárodním měřítku, neboť jednoduchá konstrukce takových vztahů, tj. adresát-orgán, takový postup nikdy přímo nevyžadovala. S rozvojem přeshraničních on-line vztahů se tedy musí správní právo (včetně práva finančního) potýkat s již popsanou krizí efektivity a legitimacy prakticky bez předchozích zkušeností s řešením přeshraničních otázek¹⁴⁶.

V oboru finančního práva představují aktuálně problém především kritéria místa zdanitelného plnění a domicilu subjektů internetových transakcí. Hrozí přitom riziko, že podobně, jako mohou pachatelé trestné činnosti unikat postihu plynulým přesouváním mezi jurisdikcemi nebo svým umístěním mimo jurisdikce, lze se analogicky vyhnout i zdanění¹⁴⁷.

¹⁴⁵ Z evropských států můžeme jako příklad uvést soudy francouzské.

¹⁴⁶ Výjimkou je v tomto směru snad jen problematika cel a dalších administrativních překážek mezinárodního obchodu a koordinace preventivních opatření k zamezení dvojího zdanění.

¹⁴⁷ K tomu srov. Brunori, D. The Politics of State Taxation: Saving the Internet from the Taxman. *State Tax Notes*, roč. 29, číslo 6, str. 1 a násl.

Kritérium místa zdanitelného plnění lze srovnat s určovatelem *loci solutionis*, jehož stručná diskuse byla provedena výše. U čistě internetových transakcí, tj. nikoli tam, kde internet slouží pouze ke komunikaci projevu vůle, je tak i zde *locus solutionis* značně problematickým určovatelem umožňujícím navíc rozsáhlé spekulace. I přes snahu správních orgánů se přitom tento problém doposud nedaří uspokojivě řešit¹⁴⁸.

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

Spory o správní jurisdikci nad sázkovými kancelářemi jsou v současné Evropě velmi časté a lze si je tak představit i jako jakýsi předvoj dalších přeshraničních administrativně-právních konfliktů. Problém zde spočívá především ve spojení principu svobody pohybu služeb a rozdílné kvality národních správních legislativ umocněném delokalizací celosvětové informační sítě. V řadě států jako například ve Francii nebo v Maďarsku je tak například loterijní a sázková činnost v určitých oblastech předmětem státního monopolu, jinde se jedná o koncesovanou, vázanou či dokonce volnou činnost. Usadí-li se pak sázková kancelář na území některého ze států s mírnější administrativní regulací a začne nabízet své služby po internetu, má v porovnání s konkurenty z ostatních států mnohem výhodnější tržní pozici, přičemž díky internetu může obsáhnout i zákazníky v mnohem rigoróznějších jurisdikcích nebo i tam, kde je tato činnost předmětem státního monopolu. Státy se proti takovému jednání brání různě – české Ministerstvo financí se tak původně vydalo cestou soudní¹⁴⁹ a podobné řešení přijá-

¹⁴⁸ Srov. např. poziční dokument Komise publikovaný pod číslem COM(1998) 374 (Communication from the Commission on Electronic commerce and indirect taxation) a reakci ECOSOC pod č. OJ C 407 ze dne 28. 12. 1998.

¹⁴⁹ Masmédiu dokonce proběhla i poněkud neuvěřitelná zpráva, že bylo na jednu ze sázkových kanceláří nabízejících ze zahraničí služby po internetu podáno trestní oznámení.

ly k ochraně loterijních a sázkových zákonů i jiné státy jako například Francie. V Maďarsku došlo dokonce k legislativnímu řešení tohoto problému formou prostého zákazu poskytování příslušných služeb prostřednictvím internetu bez ohledu na domicil poskytovatele. Toto legislativní řešení však ještě, než mohl příslušný zákon nabýt platnosti, bude muset projít přes maďarský Ústavní soud a je velmi pravděpodobné, že jeho aktuální podoba bude shledána protiústavní a v rozporu s mezinárodními závazky Maďarska plynoucími z členství v ES¹⁵⁰. Soudní řešení problému internetového sázení však, jak je možné vidět na příkladu několika již pravomocně rozhodnutých sporů, nemusí vést ke kýženému úspěchu – problémem je zde vykonatelnost příslušných soudních rozhodnutí.

Jeden z neznámějších případů kolize správních legislativ v otázce internetového sázení byl pravomocně rozhodnut ve Francii a týkal se dostihových sázek. Na ty má na francouzském území monopol společnost Pari Mutuel Urbain. Sázky na francouzské dostihy však začala po internetu nabízet i společnost Zeturf usazená na Maltě¹⁵¹. Francouzské soudy sice pravomocně zakázaly společnosti Zeturf provozovat on-line sázky na francouzské dostihy¹⁵², rozhodnutí však nebylo na Maltě uznáno a vykonáno pro rozpor s maltskými zákony¹⁵³. Společnost Zeturf tedy nadále poskytuje uvedené služby, a to podle maltských zákonů¹⁵⁴.

Těžko přitom usuzovat, jak k tomu mohlo dojít, když v České republice nejsou právnické osoby trestně odpovědné.

¹⁵⁰ O ústavní stížnosti, která čeká na rozhodnutí u maďarského Ústavního soudu, podrobně referoval na konferenci Kyberprostor 2006 vedoucí Centra pro ICT právo Právnické fakulty Univerzity v Pécsi, Dr. Zsolt Balogh.

¹⁵¹ Relativně benevolentní správní úprava pro poskytování on-line sázek na Maltě způsobila, že většina evropských on-line sázkových kanceláří je usazena právě zde. Sázkový průmysl je tak jedním z významných zdrojů maltské ekonomiky.

¹⁵² Rozhodnutí Odvolacího soudu v Paříži ze dne 4. 1. 2006 č.j. 05/15773, rozhodnutí lze ve formě scanu nalézt na adrese

http://www.droit-technologie.org/jurisprudences/CA_paris_%20-040106.zeturf.pdf.

¹⁵³ Spor se věnovala řada francouzských odborných i laických médií – viz např. Devillard, A. Zeturf.com contre PMU, les paris judiciaires sont ouverts. 01net.com, 13. 7. 2005, publ. on-line na adr. <http://www.01net.com/article/284722.html>, faktická rekapitulace sporu viz Marchand, M.-J. Quand Zeturf se moque des monopoles. Droit-NTIC.com, 3. 7. 2006, publ. on-line na adr. <http://www.droit-ntic.com/news/afficher.php?id=366>.

¹⁵⁴ Není přitom příliš pravděpodobné, že by Francie v této věci podala žalobu proti Maltě u Evropského soudního dvora – argumenty proti principu volného pohybu služeb by se

Výše uvedená právní situace, kdy technické charakteristiky informační sítě společně s mezinárodněprávními závazky brání státům v ochraně trhu před internetovým sázením resp. před evropskou konkurencí, vyústila koncem roku 2008 ve faktickou rezignaci řady vrcholných správních orgánů zemí EU na další represivní postup. České ministerstvo financí tak příkladně ohlásilo dostupnost licencí pro internetové sázení. Tento krok sice nemůže omezit nebo zpřísnit podmínky pro působení zahraničních internetových sázkařských portálů na internetu, ale umožní liberalizovat postavení domácích sázkových kanceláří, které se nově budou moci účastnit dříve zapovězeného trhu internetového sázení.

Zatímco *locus solutionis* je typickým hraničním určovatelem v oblasti administrativní regulace poskytování služeb a finančněprávní úpravy nepřímých daní, je domicil či *patria* důležitým kritériem zejména pro obor přímých daní. Můžeme sice v této věci odkázat na výše provedenou diskusi možností uplatnění tohoto kritéria v oboru soukromého práva, je však třeba poukázat na zásadní odlišnost v otázce hraničního určovatele místa jiné provozovny. K úvaze o odlišné a mnohem restriktivnější interpretaci pojmu jiné provozovny pro potřeby finančního či správního práva nás přitom vede především diametrálně odlišná teleologie příslušných norem. Zatímco dominantním cílem kolizních norem soukromého práva je rozumné uspořádání vztahů rovných subjektů, můžeme v případě práva správního hovořit spíše o relevanci principů právní jistoty, ochrany adresáta nebo o zákazu svévole. Kritérium provozovny či jiné provozovny je tedy nutné posuzovat odlišně, hovoříme-li o něm v souvislosti se soukromoprávním závazkem nebo se správní povinností. Adekvátní správní interpretací tak bude taková, která vyjde z *a priori* jasných kritérií a v jejímž důsledku dojde jen k minimálnímu omezení autonomie příslušného subjektu. Je tedy třeba prozatím odmítnout možnost založení správní jurisdikce například na základě registrace doménového jména s určitou národní doménou první úrovně, jak byla diskutována výše¹⁵⁵. Případná nová či nestandardní kritéria pro určení

v tomto případě hledaly jen těžko. Rozhodnutí francouzského soudu sice diskutuje i otázku proporcionality, není však pravděpodobné, že by se Evropský soudní dvůr k této argumentaci přihlásil.

¹⁵⁵ Shodně viz Reed, C. *Internet Law*. Cambridge: Cambridge University Press, 2004, str. 238. Stejně stanovisko je možné nalézt i v čl. 42.1 – 42.10 Komentáře k Modelové úmluvě

domicilu tak budou muset mít zřejmě oporu nikoli jako v případě soukromého práva v extenzivní interpretaci ale v projevené vůli státu, ať už ve formě zákona nebo mezinárodní úmluvy¹⁵⁶.

4.8 ZÁVĚREČNÉ POZNÁMKY K TERITORIALITĚ PRÁVA I INFORMAČNÍCH SÍTÍCH

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

Poslední řešení, tedy umístění obrazu v obývacím pokoji, je možné objektivně považovat za rozumné. To však neznamená, že bychom o předchozím řešení, tj. zeď vedle dveří na WC, mohli prohlásit, že bylo zvoleno chybně. Stejně tak nemáme jistotu, že nepřijde ještě vzdělanější odborník, který obraz později opět neprohlásí za padělek, v důsledku čehož bude opět dobrý důvod pověsit jej jinam (třeba ne hned vedle WC, ale například do kuchyně) a obývací dekorovat něčím hodnotnějším. Zbývá ale dodat, že tato nejistota však rozhodně není důvodem k tomu umístit obraz do sklepa a počkat, jak se situace vyvine.

Vztáhneme-li na aktuální situaci okolo jurisdikce či obecně působnosti práva na internetu uvedený příklad, můžeme konstatovat, že problém již

o daních OECD. Text úmluvy viz <http://www.oecd.org/dataoecd/52/34/1914467.pdf>, text komentáře viz <http://www.hmrc.gov.uk/manuals/intmanual/INTM159000.htm>.

¹⁵⁶ Detailní analýzu problematiky zdanění příjmů z internetového podnikání a návrh alternativních kritérií k delimitaci správní jurisdikce obsahuje materiál OECD nazvaný *Are the Current Treaty Rules for Taxing Business Profits Appropriate for e-Commerce?*, který je volně ke stažení na adrese <http://www.oecd.org/dataoecd/58/53/35869032.pdf>.

zde visí a opatrně s ním začínáme manipulovat. Důležité však je uvědomit si, že k tomu, abychom našli jeho alespoň částečně stabilní (správné) řešení, budeme především potřebovat mnohem více empirických informací, ať už se bude jednat o informace právní, sociologické, technické či ekonomické. Diskutujeme-li tedy nyní právní otázky související s působností práva na internetu, nemělo by být naše úsilí posuzováno jako snaha s ambicí permanence či dokonce objektivní a absolutní správnosti, ale spíše jako hledání co nejlepších řešení za daných okolností. Hodí se tedy v tomto kontextu uzavřít konstatováním, že právo je sice objektivně uměním dobrého a spravedlivého, subjektivně se však často jedná spíše o umění možného¹⁵⁷.

¹⁵⁷ Nosnou je tato teze především pro pragmatickou právní metodologii a není případná jen pro otázky internetové jurisdikce ale prakticky pro všechny oblasti oboru práva informačních technologií. K pojmu a vývoji pragmatické metody viz např. Dickstein, M. Pragmatism Then and Now, in *Revival of Pragmatism*, ed. Dickstein, M. London: Duke University Press, 1998, str. 1 a násl.

5 POJEM A PRÁVNÍ ASPEKTY INFORMAČNÍ SPOLEČNOSTI

5.1 POJEM INFORMAČNÍ SPOLEČNOSTI

Vydeme-li ze skutečnosti, že unikátní funkcí informace je organizovat systémy, tj. čelit vzrůstu jejich entropie, docházíme k závěru, že předpokladem organizované společnosti je její informovanost. Informační infrastruktura tedy v tomto smyslu slouží jako technické zázemí využitelné k šíření organizujících informací ve společnosti. Kvalita této infrastruktury a jejího obsahu pak nutně určuje i míru efektivitu organizačních mechanismů.

Přístupů ke struktuře pojmu informační společnosti je nespočet¹⁵⁸. Pro potřeby tohoto textu přistoupíme k pojmu informační společnosti ze dvou perspektiv, a to kvantitativní a kvalitativní. Kvantitativní vymezení ji pojímá jako společenství, v němž je technicky umožněna bezproblémová a neomezená tvorba, distribuce a výměna informací¹⁵⁹. Je to tedy společenství, jehož jednotliví členové jsou spojeni navzájem informačními kanály, které jim umožňují volně komunikovat¹⁶⁰. Obdobně jsou pak jednotlivci spojeni i s autoritami, typicky s orgány veřejné moci¹⁶¹, a mohou tak bez prodlení

¹⁵⁸ Kvalitní přehled především historických přístupů k tomuto pojmu nabízí internetová encyklopedie Wikipedia – jak se můžeme dočíst pod heslem „information society“, vychází pojmové vymezení informační společnosti prakticky vždy ze základů oboru, jemuž je určena příslušná publikace.

¹⁵⁹ K východiskům a historii tohoto pojetí viz např. Zlatuška, J. Informační společnost. Zpravodaj ÚVT MU, ročník 8, číslo 4, str. 1 a násl.

¹⁶⁰ Struktura těchto kanálů je dána použitou technologií – k tomu viz např. Lévy, P. Cyberculture. London: University of Minnesota Press, 2001, str. 13 a násl.

¹⁶¹ Pro tento typ využití služeb informační společnosti se žilo souhrnné označení e-Government. Jako vhodné se jeví pojetí tohoto aspektu informační společnosti jednoduše jako cesty k posílení funkce veřejné správy jakožto služby společnosti – srov. Mates, P., Smejkal, V. E-government v českém právu. Praha: Linde, 2006, str. 9.

a bez omezení přijímat autoritativní (regulující) informace nebo se účastnit legitimačních procesů.

Kvantitativní pojetí informační společnosti je tedy zaměřeno především na informační infrastrukturu a všímá si na prvním místě rozvoje a dostupnosti¹⁶² technických prostředků tvorby, přenosu a zpracování informací. Typické pro tento typ nazírání informační společnosti pak je používání kvantifikovatelných kritérií, jako například datových objemů, počtu uživatelů, rychlosti strojového zpracování, propustnosti komunikačních linek apod.

Zvláštním typem kvantitativního pojetí informační společnosti je to, které se vedle technicky podporované komunikace zaměřuje též na automatizované zpracování informací¹⁶³. Centrálním momentem tohoto pojetí je procesor, tedy automat schopný rychlého zpracování (transformace) velkého množství informací. Informační společnost se pak touto optikou jeví nejen jako společenství užívající technologií k výměně informací mezi jednotlivými jeho členy, ale též jako societa, která disponuje technologiemi samostatně zpracovávajícími a vytvářejícími informace. Jednoduše řečeno není touto optikou viděn počítač či informační síť jen jako médium, ale jako informační subjekt, který informace přijímá, přetváří či přímo vytváří.

Rozdíl mezi komunikací a transformací informace můžeme ilustrovat na příkladu použití ICT v justici¹⁶⁴. Bereme-li informační technologie jen jako prostředek vzájemné komunikace, bude soud využívat služeb informační společnosti například pro komunikaci s účastníky nebo vlastní administrativou, pro vedení ekonomické či personální agendy, pro vedení spisu apod. Přijmeme-li však tezi, že součástí informační struktury soudu má být i procesor informací, otevíráme tím možnost automatizovaného zpracování rozhodovacích činností od relativně jednoduchých až po složité. Čím složitější je však proces zpracování

¹⁶² Jedním z klasických problémů je v tomto směru fenomén digital divide, tj. rozdílnosti šancí různých společenských či národnostních skupin v návaznosti na jejich přístup k informačním technologiím. Výklad problému společně s argumentací teze, že se nejedná jen o kvantitativní otázku podává např. Andr ez Guadamus in Guadamuz, A. The Digital Divide: It's the Content, Stupid! Computer and Telecommunications Law Review,  slo 304, str. 73 a n sl.

¹⁶³ N kter  z t chto p stupů trp  snad a  p li nou d v rou v s mantick  schopnosti automatů – srov. např.  t droň, B., Hlav c, L. New Cyberspace Managers in the Year 202, MUJLT, ro n k 2,  slo 1, str. 119 a n sl.

¹⁶⁴ K probl mu takzvan  elektronizace justice viz např. Pol c k, R. K elektronizaci justice. Jurisprudence, ro n k 17,  slo 6, str. 3 a n sl.

informace, tím více mají právníci tendenci hovořit nikoli o automatizaci ale pouze o asistenci příslušnému rozhodovacímu procesu¹⁶⁵.

Informační společnost v kvantitativním či infrastrukturním smyslu, přestože je tohoto pojmu v současné době zhusta používáno k označování konkrétních společenství či států, je ideální kategorií. Ideál dokonalé vzájemné informovanosti je přitom nedosažitelný. Hovoříme-li tedy dnes o informační společenosti například v souvislosti s penetrací službami operátorů mobilní telefonie, nelze pominout skutečnost, že tyto služby jsou způsobilé k přenášení jen velmi omezeného rozsahu sdělení, ať co do jeho kvality nebo kvantity. Podobně ani internet neposkytuje i přes již běžně dostupné možnosti širokopásmového přístupu zdaleka plnou informovanost jeho uživatelů – i zde jsou dobře zřetelné technologické limity, které se budou sice do budoucna významně posouvat, nikdy však zcela nevyminou.

Zatímco kvantitativní pohled na informační společnost se soustředí na infrastrukturu a technologie ke tvorbě, zpracování a distribuci informací, je kvalitativní či též obsahové vymezení informační společnosti zaměřeno na její obsah, tj. na kvalitu informací¹⁶⁶. Za informační společnost pak můžeme považovat takové společenství, které výše naznačené infrastruktury skutečně¹⁶⁷ a plně využívá k tvorbě, zpracování a komunikaci informací. Ideál informační společnosti je tedy postaven na předpokladu, že její členové nejenže plně využívají dokonalé informační infrastruktury, ale že jejím prostřednictvím komunikují skutečné informace (tedy sdělení způsobilá snižovat entropii). Tento pohled na informační společnost se tak zaměřuje především na to, jak kvalitní je informační výměna a jaký je její následný organizační efekt.

Spojíme-li oba zmíněné pohledy, docházíme k ideálu společnosti, v níž neomezeně probíhá tvorba, zpracování a distribuce informací. Dokonalá

¹⁶⁵ Srov. např. Verheij, B. *Virtual Arguments*, The Hague: T.M.C. Asser Press, 2005, str. 127.

¹⁶⁶ K tomuto pojetí viz např. Boyle, J. *Shamans, Software and Spleens*, Cambridge: Harvard University Press, 1996, str. 1 a násl.

¹⁶⁷ Kvalita informační společnosti je tedy v tomto případě určována mimo jiné i úrovní znalostí a motivace členů společnosti k využití informační infrastruktury – k tomu viz. Wilhelm, A. *Digital Nation – Towards an Inclusive Information Society*, Cambridge: The MIT Press, 2004, str. 17 a násl.

informační společnost je tudíž společenstvím s plnou mírou vnitřní informovanosti. Jako synonymum pro výraz „informační“ můžeme tedy v tomto případě použít pojmu „organizovaná.“

Oba pohledy na informační společnost jsou pro dosažení ideálu organizované společnosti srovnatelně relevantní. Nelze tedy, jak bývá často běžné, zaměřit pozornost veřejnosti a alokaci zdrojů například pouze na budování infrastruktury bez toho, aby současně probíhal vývoj mechanismů k podpoře informačních aktivit a ochraně před balastem nebo chaotizujícími elementy¹⁶⁸. Naopak samozřejmě nelze ani investovat společenské úsilí a zdroje do tvorby kvalitního informačního obsahu bez toho, aby byly zajištěny technologie k jeho odpovídající komunikaci.

Přes právě uvedené bývá kvalitativním pohledům na ideál informační společnosti věnována nesrovnatelně menší pozornost, než je tomu u přístupů kvantitativních. Zatímco se tedy otázkou budování informační společnosti razantně zabývají disciplíny, jako jsou informatika nebo ekonomie, zůstávají kvalitativní obory jako právní věda, filozofie či sociologie stát stranou, to povětšinou z vlastní viny. Výsledkem pak je výše naznačená situace, kdy společnost sice disponuje kvalitní infrastrukturou a službami, ty jsou však zatíženy balastním nebo dokonce chaotizujícím obsahem. Paradoxně pak dokonce může dojít i k tomu, že kvalitní informační infrastruktura nepřispívá k organizaci společnosti, ale naopak tím, že jsou jejím prostřednictvím šířeny chaotizující informace, zvyšuje míru společenské entropie (tj. nepořádku).

Následující příklad nelze v žádném případě pokládat za důkaz toho, že celosvětová informační síť obecně přispívá k chaotizaci společnosti. V konkrétních případech, kdy je informační infrastruktura používána bez souvislostí s právními, morálními, sociálními či třeba náboženskými pravidly, však může docházet k efektu, kdy kvantitativně se rozvíjející technologie bohatě živí prudký rozvoj nežádoucích společenských jevů. Informační síť tak může sloužit k rozvoji obchodu s dětskou pornografií, tvorbě a koordinaci mezinárodních zločineckých nebo teroristických sítí apod. Tyto aktivity často zaznamenávají prudký rozvoj

¹⁶⁸ Příkladem může být tlak na překotný rozvoj nových služeb informačních sítí, to však bez srovnatelného tlaku na jejich schopnost absorbovat sociální problémy či právní ochranu před zneužitím. Problematice společenského rozměru vývoje nových technologií se obecně věnuje Jean Jacques Solomon ve své monografii Solomon, J. J. Technologický úděl. Praha: Filosofie, 1997.

právě díky možnosti využívat infrastrukturu informační společnosti či jsou dokonce na této infrastruktuře bytostně závislé.

Vzhledem k tomu, že se nikdy nepodaří kvantitu a kvalitu informační společnosti, respektive příslušné aktivity vedoucí k jejich rozvoji, plně vyvážit, je třeba řešit otázku priority v časovém sledu a přidělování zdrojů. Taková otázka se jeví na první pohled obdobně jako problém se slepicí a vejcem – v tomto případě máme totiž rozhodnout, zda je třeba nejprve investovat do rozvoje odpovídající infrastruktury a následně korigovat či tříbit její využití nebo naopak nejprve vytvořit ochranné mechanismy, regulační či samoorganizační modely a teprve pak těmto mechanismům přidělit odpovídající technologie a infrastrukturu.

Přesto, že má tento text právní charakter a následné tvrzení může vyznít jako střelba do vlastních řad, domníváme se, že prioritou by i nadále měla zůstat kvantita. Argumentem k takovému tvrzení jsou četné příklady z praxe, kdy i v silně regulovaných společnostech dochází následkem nasazení informačních a komunikačních technologií k vývoji, který žádná z kvalitativních disciplin nebyla schopná dříve předpovědět¹⁶⁹. Přirozený vývoj¹⁷⁰ jde tedy často za hranice představitosti a kvalitativní disciplíny tak prostě nejsou s to vymezit budoucí problémy a navrhnout jejich řešení¹⁷¹. I v případech, kdy je možné předpovědět existenci určité informační technologie, tak jen zřídka můžeme předvídat, k jakým účelům (roz. ke zpracování či komunikaci jakých informací) jí bude nakonec užito.

Pionýrský charakter a nepředvídatelnost efektu vývoje informačních technologií můžeme přirovnat k základnímu výzkumu. Ani ten totiž často nepřináší výsledky, jejichž využití by šlo předem předpovědět nebo dokonce regulovat. To, zda základní výzkum přinesl nějaké

¹⁶⁹ Připomeňme například nepředvídaný význam a formy využití služby WWW a protokolu HTTP, která byla v raných fázích vývoje internetu považována za méněcenný doplněk důležitějších služeb jako FTP nebo Telnet. Dnes je WWW naproti tomu brána takřka jako synonymum pro internet.

¹⁷⁰ Zde je třeba upozornit, že přirozenost nelze v žádném případě spojovat pouze s ekonomickou kategorií maximalizace vlastního materiálního užítku. Pokud by tomu tak bylo, Internet by nikdy nedosáhl aktuálního svého rozsahu a důležitosti – srov. výklad k problematice sdílení a jeho motivům in Lessig, L. *Free Culture*. New York: Penguin Press, 2004, str. 31 a násl.

¹⁷¹ Totéž samozřejmě platí i proo stát a jeho regulační aktivity – srov. Salomon, J. J., *Technologický úděl*, Praha: Filosofía, 1997, str. 203 a násl.

ovoce nebo nikoli, tedy zpravidla nelze zhodnotit předem ale mnohdy až s odstupem mnoha let po jeho ukončení. Trefné srovnání s historickým vývojem přináší v tomto směru Stephen Saxby, když poukazuje na vývoj právního názoru na elektrickou energii¹⁷². Původně chápána právem jako zdroj světla, stala se později mnohem univerzálněji použitelnou kontrolovanou přírodní silou, jejíž využití šlo daleko za hranice představitosti nejen vědců, ale samozřejmě i filozofů nebo právníků.

Správnost důrazu na kvantitu je dle našeho názoru v tomto případě možné podpořit i poukazem na základní teleologii příslušných technických řešení. Smyslem vývoje informačních technologií je totiž usnadnit vzájemnou komunikaci účastníků společenského života. Tato teleologie přitom bez problémů projde testem kvalitativních disciplín, přičemž je třeba přiznat, že jakékoli podrobnosti jejich následného nasazení nemohou být těmito obory předvídaný nebo hodnoceny a o to méně pak ani předpisovány či omezo-
vány.

5.2 PŘIROZENĚ HODNOTOVÁ POVAHA INFORMAČNÍ SPOLEČNOSTI

Informační systémy z podstaty přebírají generické znaky svého základního elementu, tj. informace. Výše jsme konstatovali, že základní teleologii budování informační společnosti je instalace mechanismů k bezproblémovému vytváření, zpracovávání a předávání informací mezi jednotlivými účastníky společenského života. Je-li pak základním smyslem existence informace působit proti entropii, je i smyslem existence informačních technologií v konečném důsledku organizační (protientropický) efekt.

Informaci však můžeme vidět nejen jako opak entropie ale též jako nositelku života. Díky informaci tedy život nepodléhá entropii, ale má schopnost se naopak vyvíjet a adaptovat se na změnu podmínek. Není to však analýza samotného elementu, tj. informace, která nás dovádí k tomuto poznání, ale studium systému jako celku komplexním pohledem. Z něj pak

¹⁷² Viz Saxby, S. The Role of Government in National/International Internet Administration, in *The Internet, Law and Society*, ed. Akdeniz, Y., Walker, C., Wall, D., Harlow: Pearson Education Limited, 2000, str. 3.

můžeme vyčíst přirozené vlastnosti informace, které z informačních systémů libovolného charakteru vytvářejí místa, kde „život nachází svůj domov.“

Informaci jako nositelku života identifikovala v raném stadiu vývoje kybernetika. Její zakladatel Norbert Wiener k tomu uvádí¹⁷³: „Vesmír jako celek projevuje sklon k zániku, existují jisté lokální enklávy, jejichž vývojová tendence, jak se zdá, je protichůdná vývojovým tendencím celého vesmíru, a v nichž se projevuje omezená a dočasná tendence k růstu a organizovanosti. A právě v některé z těchto enkláv nachází život svůj domov.“

Nikoli teoreticky ale empiricky dospíváme k překvapivému závěru, že informační společnost není *per se* bezhodnotová. Bez ohledu na region či politické pozadí můžeme vidět, že tam, kde není vzájemné výměně informací bráněno, dochází prostřednictvím budování fyzické a logické informační infrastruktury a jejího následného naplnění obsahem k rozvoji přirozených základních společenských hodnot. Aniž by bylo třeba tyto hodnoty do informační společnosti aktivně vnášet, objevují se na pozadí běžné každodenní komunikace. Analýzou informační výměny, ať už se jedná o komunikaci informací o počasí, výměnu pozdravů, sdělení si novinek z rodinného života nebo rad ke zkouškám, tak dospíváme k závěru, že jako důsledek této partikulární komunikace nastávají komplexní tendence k rovnosti, slušnosti, pořádku, solidaritě¹⁷⁴ apod.

Z uvedeného vyplývá poněkud pompézní přesto však racionální závěr, že nechat jednotlivce volně komunikovat znamená mimo jiné dát prostor k rozvoji základním hodnotám lidské společnosti. Paradoxní je tento závěr v tom, že informační infrastruktura a wienerovská matematicko-logická metodika zpracování informací jsou samy o sobě bezhodnotové. Skutečnost, že má s jejich pomocí vytvořená informační společnost silně hodnotový charakter, pak vede k úvaze, že tyto hodnoty jsou komplexním projevem informace a zároveň jejím nevyjádřeným, přesto však přirozeným

¹⁷³ Viz Wiener, N. *Cybernetics: Or the Control and Communication in the Animal and the Machine*. Cambridge: MIT Press, 1961, str. 13.

¹⁷⁴ Skutečnost, že solidarita patří mezi přirozené hodnoty informační společnosti zdůrazňuje i řada publikací kritizujících restriktivní charakter práv duševního vlastnictví – srov. Drahoš, P., Braithwaite, J. *Information Feudalism – Who Owns the Knowledge Economy?* New York: New Press, 2007, str. 198 a násl.

obsahem¹⁷⁵. Stejně, jako jsme dali výše informaci do souvislosti se životem, můžeme ji tedy nyní dát do souvislosti se základními hodnotami lidské společnosti¹⁷⁶.

Výše naznačené přirozené souvislosti nejsou samozřejmě chtěné v politických systémech založených na autoritářské vládě a potlačování uvedených hodnot. Autoritářským režimům přitom netrvalo dlouho pochopit, že volná výměna informací znamená přímé ohrožení nesvobodného státního zřízení. Je tedy nasnadě, že se nyní v zemích s autoritářskou formou vlády setkáváme s maximálním omezováním jinde běžných možností vzájemné mezilidské komunikace, jakými jsou například nejruznější služby celosvětové sítě internet. Tam, kde z faktických důvodů nelze lidem zamezit v přístupu k informační infrastruktuře, se pak režim snaží alespoň vzájemnou informační výměnu monitorovat a zasahovat v situacích, kdy tato vede k explicitním projevům výše zmíněných komplexních efektů, tj. např. základních práv. Přirozenost informace je však i v těchto případech tak silná, že pokud je to alespoň trochu možné, jsou informační kanály udržovány a informace jimi v maximální možné míře proudí.

Příkladem může být fungování občanských informačních struktur v zemích, jako jsou Kuba nebo Čína. Sám, byť cíleně omezovaný, přístup veřejnosti k informačním technologiím způsobuje, že zde i přes restrikce dochází k vzájemnému informování a následnému rozvoji přirozených společenských hodnot. I přes silné informační embargo se tak například na jaře roku 2008 dostaly k západním médiím relativně konkrétní informace o nepokojích v Tibetu.

Za povšimnutí stojí v této souvislosti skutečnost, že přímá podpora rozvoje základních společenských hodnot nebývá při použití služeb informační společnosti příliš úspěšná. Účastníky informační výměny obvykle nezajímají diskuse vedené o svobodě projevu nebo pluralitě politických názorů.

¹⁷⁵ Jedním z důkazů komplexního charakteru základních společenských hodnot je i přirozená koherentnost různých implementačních aktivit včetně aplikačních procesů v právu – srov. Griffin, J. *Value Judgment – Improving Our Ethical Beliefs*. Oxford: Clarendon Press, 1997, str. 12 a násl.

¹⁷⁶ Uměle vytvořené informační prostředí (kyberprostor) může posloužit jako vynikající model informační společnosti – způsob organizace sociálních skupin v kyberprostoru prostřednictvím implicitních hodnot popisuje Pierre Lévy ve své *Kyberkultuře* – viz Lévy, P. *Cyberculture*. London: University of Minnesota Press, 2001, str. 165 a násl.

Namísto toho si spíše chtějí vyměňovat informace o módních výstřelcích, hudbě, sportu, sexu apod. Servery financované organizacemi podporujícími rozvoj informační společnosti, jejichž cílem je podpořit rozvoj základních společenských hodnot v nesvobodném světě, tedy obvykle zaznamenávají jen minimální zájem skutečných uživatelů¹⁷⁷.

Přestože je však odezva na přímou podporu základních hodnot v prostředí informační společnosti mizivá či uměle vytvářená, můžeme existenci a růst těchto hodnot prostě empiricky konstatovat jako komplexní efekt populárních služeb. Každý příspěvek do diskuse pod článkem o fotbalovém utkání či každý sdílený soubor s populární skladbou tedy přispívají k rozvoji komplexních efektů, jakými jsou například svoboda projevu nebo solidarita. Tím se právě v informační společnosti projevuje přirozenost informace jako základní jednotky organizace ale též jako nositelky života.

5.3 STRATEGIE BUDOVÁNÍ EVROPSKÉ INFORMAČNÍ SPOLEČNOSTI

Nutnost strategického přístupu vrcholných orgánů ES k problematice budování informační společnosti konstatovala a argumentovala takzvaná Bangemannova zpráva z června roku 1994¹⁷⁸. Touto správou byly prakticky založeny aktivity Společenství směřující k budování informační společnosti na nejvyšší úrovni.

V dokumentu se doslova uvádí (překlad autor): „(...) Technologický pokrok nám nyní otevírá možnost zpracovávat, ukládat, získávat a komunikovat informace v jakékoli formě – ústní, písemné nebo vizuální – bez omezení daného vzdáleností, časem či velikostí. Tato revoluce přináší velkolepé možnosti lidské inteligenci a zakládá zdroj,

¹⁷⁷ Za pozornost rovněž stojí i to, že takové služby informační společnosti zpravidla nevznikají spontánně ale pouze v případě předchozí finanční motivace. Naopak vznik a vývoj komunitních služeb, sítí pro sdílení multimedií apod. bývá často motivován spontánní potřebou spíše než ekonomickým efektem.

¹⁷⁸ Plný název dokumentu zní Recommendations to the European Council: Europe and the Global Information Society. Plný text je ke stažení např. na stránkách IDABC <http://ec.europa.eu/idabc>.

který mění způsob, jímž společně pracujeme a žijeme. Evropa se již na této revoluci podílí, ale přístupem, který je stále příliš roztržštěn a který by mohl omezit očekávané přínosy. Informační společnost je prostředkem k dosažení hned tolika z cílů Unie. Musíme jej užít správně a hned teď.“

V návaznosti na aktuálně populární myšlenkové směry se podpora budování evropské informační společnosti zaměřila především na její kvantitativní stránku, ekonomický potenciál a dále pak na vybrané partikulární aspekty společenského života, tj. především na zdravotnictví a veřejnou správu. Takové zaměření můžeme vyčíst z řady pozičních dokumentů Evropské Komise, z nichž nejdůležitějšími byly tzv. Lisabonská strategie¹⁷⁹ a na ni navazující strategické dokumenty eEurope 2002 a eEurope 2005. Základní směry podpory informační společnost byly shrnuty do první verze eEurope 2002 následovně:

- Dostupnější a bezpečnější internet (levnější a rychlejší připojení, rychlejší internet pro výzkumníky a studenty, výstavba zabezpečených sítí)
- Lidské zdroje (práce s mládeží, budování znalostní ekonomiky, zapojení občanů do znalostní ekonomiky)
- Podpora využití internetu (podpora e-commerce, e-governmentu, e-health, podpora tvorby evropského obsahu pro globální síť, inteligentní dopravní systémy)

Přestože se prioritní osy ve strategickém dokumentu eEurope 2005 mírně pozměnily, i nadále se strategie rozvoje informační společnosti soustředila především na její kvantitativní stránku. Aktuálním pozičním dokumentem k implementaci Lisabonské strategie se pak stalo Sdělení Komise Evropskému parlamentu č. KOM(2008) 594 týkající se budoucích sítí a internetu. V tomto dokumentu se Komise nadále hlásí ke kvantitativnímu přístupu, je zde však již patrný posun k důkladnějšímu zohlednění kvalitativních otázek a problémů. Za hlavní výzvy do budoucna byly označeny:

- Vysokorychlostní širokopásmové připojení
- Podpora tržního prostředí a soutěže na technologickém trhu

¹⁷⁹ Důraz na jednotlivé aspekty budování informační společnosti byl v Lisabonské strategii oproti původnímu znění z roku 2000 ještě posílen při revizi v roce 2005.

- Přehodnocení kvality absolutních práv k informacím¹⁸⁰
- Sémantický internet (podpora výstavby sítě nové generace založené na sémantických principech)
- Bezpečnost a ochrana soukromí¹⁸¹

Z výše uvedeného lze jasně vyčíst přenos důrazu od prostého budování komunikační infrastruktury ke komplexní podpoře rozvoje informační společnosti. Do středu zájmu se tak dostávají například sémantické aspekty informační výměny, jejichž podpora má přinést především snížení redundantních informačních toků, zvýšení efektivity informační výměny a tím i vyčištění informační společnosti od balastní informační zátěže.

O pár měsíců dříve, než bylo přijato výše zmíněné Sdělení, formuloval svoji strategickou pozici k rozvoji obsahu v informační společnosti ve formě usnesení i Evropský parlament. Toto usnesení se zabývá především otázkami souvisejícími s tvorbou a šířením kulturního obsahu, některé jeho momenty mají však mnohem širší dosah, a to dokonce i mimo obor informační společnosti.

Z jednotlivých ustanovení vybíráme:

Evropský parlament (...)

17. v souvislosti s rychlým technologickým vývojem a vývojem trhu a s cílem zajistit, aby měl kulturní průmysl a tvůrci obecně prospěch z vývoje digitálních platforem, naléhavě žádá Komisi, aby přezkoumala zásadní otázku duševního vlastnictví s ohledem na kulturní a hospodářské aspekty a aby v zájmu zachování rovnováhy mezi možnostmi přístupu ke kulturním aktivitám a obsahům a duševním vlastnictvím, která zaručí spravedlivou

¹⁸⁰ Tento kvalitativní moment nové strategie je třeba zvlášť zdůraznit, neboť se zde Komise hlásí k revizi autorského práva ve smyslu uvolnění bariér k šíření informací. Otázku legitimacy jednotlivých autorskoprávních restrikcí v prostředí informační společnosti řeší ve své monografii Lawrence Lessig - viz Lessig, L. *Freeculture*, New York: The Penguin Press, 2004, str. 273 a násl.

¹⁸¹ Aspekt soukromí genericky zahrnuje i ochranu osobních údajů. Pojem osobních údajů se však s postupem času stal na pojmu soukromí relativně nezávislým – k problému viz např. Polčák, R. *Some Notes on Current Paradoxes in the Law on Personal Data Protection*, *Information and Communications Technology and Law*, ročník 4, číslo 6, str. 52 a násl.

a účinnou odměnu všem kategoriím držitelů práv, skutečný výběr pro spotřebitele a kulturní rozmanitost, vyzvala všechny aktéry působící v tomto odvětví, zejména telekomunikační operátory a poskytovatele internetových služeb, ke společnému nalezení řešení, jež by byla spravedlivá pro velké i malé zúčastněné subjekty; v tomto ohledu upozorňuje na skutečnost, že kriminalizace spotřebitelů, kteří neusilují o zisk, za účelem boje proti počítačovému pirátství není vhodným řešením;

(...)

20. vyzývá Komisi, aby uznala, že internet zcela změnil tradiční způsoby užívání kulturních výrobků a služeb a že je zásadní zaručit bezproblémový přístup ke kulturnímu internetovému obsahu a rozmanitost kulturní tvorby přesahující pouhou průmyslovou a komerční logiku a kromě toho také zajistit spravedlivou odměnu pro všechny kategorie držitelů práv;

(...)

26. zdůrazňuje význam bezplatných informačních infrastruktur, jako je WorldWideWeb, které jsou založeny na modelech otevřené účasti a otevřených standardech, pro evropské kreativní odvětví a žádá Komisi, aby předložila strategii pro otevřenější a interoperabilnější informační infrastruktury;

Z výše uvedených pozičních a strategických iniciativ můžeme tedy formulovat základní otázky rozvoje evropské informační společnosti následovně:

Kvantitativní otázky:

- Dostupnost služeb informační společnosti, především širokopásmového připojení k internetu (s důrazem na rozvoj venkovských oblastí)
- Rozvoj stávajících a tvorba nových odvětví informačního průmyslu a znalostní ekonomiky
- Implementace ICT v komunikaci mezi státem a občanem resp. mezi občanem a službami, na jejichž poskytování je veřejný zájem (zdravotnictví, krizová intervence apod.)
- Ochrana komunikační infrastruktury

Kvalitativní otázky:

- Modifikace absolutních práv k informacím (především autorského práva)
- Ochrana informací (především ochrana soukromí a osobních údajů)
- Vzdělávání a motivace občanů k využívání ICT (formou přímých aktivit nebo zprostředkovaně formou zvýšené právní ochrany – např. u elektronických platebních prostředků, distanční spotřebitelské kontraktace apod.)
- Podpora kvalitativně nových forem komunikace s důrazem na sémanticky orientované služby

Vzhledem k tomu, že řešení kvalitativních otázek rozvoje informační společnosti představuje relativně novou agendu, dochází v této oblasti neustále k vyjasňování a změnám politických pozic. Problematické zkušenosti s aplikací práva duševního vlastnictví, ochrany osobních údajů nebo například právního rámce pro další využití informací veřejného sektoru tak vedou k postupnému přehodnocování právního řádu informační společnosti. Pro právo tato situace, kdy dochází v relativně rychlém sledu často i k zásadním změnám klíčových právních institutů,¹⁸² není příznivá. Jakékoli zásadní změny nebo doplnění právního řádu (nikoli jen legislativy) informační společnosti totiž vyžadují čas, který však často přesahuje životní cyklus příslušných změn. Otázkou pak je, zda je vůbec evropské právo se svým konzervatismem a pomalostí vůbec s to stačit technologickému vývoji informační společnosti. Někteří autoři v této souvislosti dokonce formulují tezi „příliš letargického práva“¹⁸³ jako důvodu legitimacy technicko-ekonomických opatření suplujících líný, nemohoucí či dýchavičný mechanismus právní regulace.

¹⁸² Takovým příkladem může být obecný institut civilní odpovědnosti, který byl v posledních několika letech zásadně měněn a doplňován o prvky odpovědnosti specifických subjektů tvořících fyzickou a logickou infrastrukturu informační společnosti, tj. ISP. K problematice viz Polčák, R. Právo na internetu – Spam a odpovědnost ISP, Brno: Computer Press, 2007, str. 28 a násl.

¹⁸³ Hned několik příkladů, kdy se právo kvůli své letargičnosti pohybuje na hranici vlastní legitimacy dává například Uta Kohl ve své monografii Kohl, U. Jurisdiction and the Internet, Cambridge: Cambridge University Press, 2007, str. 33 a násl.

Druhým problematickým momentem strategie evropského práva pro informační společnost je pak jeho častý proaktivní a regulační charakter¹⁸⁴. Lze v tomto směru vysledovat obecnou tendenci evropského právo tvůrce regulovat informační společnost namísto její motivace či cílené ochrany *a posteriori*. Evropské právo pro informační společnost je tedy často budováno na predikcích normativních potřeb a jejich preventivním ošetřování¹⁸⁵ namísto toho, aby právo tvůrce sledoval technologický a společenský vývoj a reagoval až následně na výskyt problematických (chaotizujících) elementů.

Nelze samozřejmě v této souvislosti formulovat a argumentovat jednoznačný názor na vhodnost spíše proaktivního nebo naopak protektivního přístupu právo tvůrce (viz výše). Řada praktických příkladů nás však vede k úvaze, že tam, kde je smyslem regulace docílit rozvoje systému služeb informační společnosti nebo zkvalitnit informační obsah, nebývá proaktivní státní regulace zrovna ideálním instrumentem.

5.4 STRATEGIE BUDOVÁNÍ INFORMAČNÍ SPOLEČNOSTI V ČR

Česká republika se ještě před vstupem do EU v otázkách souvisejících s informační společností bohatě inspirovala evropskými aktivitami. Organem, jemuž byla svěřena gesce nad politikou informační společnosti, se stalo Ministerstvo informatiky. Ani přes snahu představitelů tohoto v mno-

¹⁸⁴ Problému proaktivní regulace se věnují i některé základní učebnice práva informačních a komunikačních technologií, když na příkladech z praxe ilustrují problematickou ambici evropského právo tvůrce, obecně řečeno, rozlišovat mezi dobrými a špatnými informacemi – srov. Rowland, D., Macdonald, E. *Information Technology Law*, New York: Routledge Cavendish, 2005, str. 477 a násl.

¹⁸⁵ Význam evropského hospodářského a kulturního prostoru přitom často vede k tomu, že se negativní efekty proaktivní regulace rozšíří i mimo území EU. Příkladem může být ochrana osobních údajů, jejíž problematický správní charakter jakož i diskutabilní parametry nastavené evropským právo tvůrcem negativně ovlivňují právní prostředí v USA, Jižní Americe či Indii – srov. např. Cohen, J.E. *Examined Lives: Informational Privacy and the Subject as an Object*, *Stanford Law Review*, číslo 52, str. 1373 a násl.

ha směrech unikátního orgánu se však nepodařilo překročit stín evropských aktivit a tak tento úřad prakticky pouze doháněl vývoj ve starých státech EU. Na poli legislativy pak byla pak situace ještě o něco horší, když byl právní řád pro českou informační společnost vytvářen prakticky pouze překládáním evropských směrnic a jejich následného vydávání ve formě zákonů¹⁸⁶.

Jednotčím momentem podpory rozvoje informační společnosti v České republice je tradičně ekonomický přístup. Kvalita a efektivita informační společnosti tak bývá určována na základě ekonomických ukazatelů, jimiž jsou příkladně hrubý obrat služeb informační společnosti, podíl těchto služeb na HDP, nejrůznější ukazatele zaměstnanosti, apod. Pojem informační společnosti tak bývá v České republice ztotožňován s pojmem znalostní společnosti či znalostní ekonomiky¹⁸⁷.

Nejdůležitějšími strategickými dokumenty byly komplexní vládní program e-Česko 2006¹⁸⁸ a dále pak dřívější partikulární strategické dokumenty zpracované Ministerstvem informatiky, z nichž vybíráme především Bílou knihu o elektronickém obchodu¹⁸⁹. Tyto dokumenty však až na drobné výjimky¹⁹⁰ prakticky pouze transponovaly strategické priority EU, jejichž stručný nástin byl proveden výše.

Po zániku Ministerstva informatiky, jehož kompetence převzaly především Ministerstvo průmyslu a obchodu a Ministerstvo vnitra, byla řada dřívějších strategických iniciativ dokonce utlumena či ukončena, a to za časté z personálních důvodů¹⁹¹. Úlohu orgánu definujícího strategii pro rozvoj

¹⁸⁶ Tento osud postihl například oblast elektronických podpisů (ke zlepšení muselo dojít až následně velkou novelou), některých služeb informační společnosti nebo dalšího využití informací veřejného sektoru.

¹⁸⁷ K pojmu znalostní ekonomiky viz např. Chi-ang Lin, B. A New Vision of the Knowledge Economy, *Journal of Economic Surveys*, ročník 21, číslo 3, str. 553 a násl.

¹⁸⁸ Dokument byl schválen usnesením Vlády ČR č. 265 ze dne 24. března 2004.

¹⁸⁹ Tento dokument navázal na Zelenou knihu elektronického obchodu a byl schválen usnesením Vlády ČR č. 474 ze dne 19. května 2003.

¹⁹⁰ Jednou z výjimek byla například problematika daňových úlev – žádný komplexní program však nakonec nebyl implementován.

¹⁹¹ Strategie rozvoje informační společnosti patří v některých evropských státech k objektům zájmu centrálních státních orgánů zřízených k ochraně osobních údajů resp. k ochraně práva na informace. Přestože zde po zániku Ministerstva informatiky existoval solidní prostor

informační společnosti v ČR pak měla převzít Rada vlády pro informační společnost, jejíž činnost organizačně zajišťuje Ministerstvo vnitra.

Model strategického orgánu na úrovni vlády je nepochybně vhodný, neboť atributy informační společnosti jsou již dnes součástí řady veřejných agend a služeb a svěřit tuto problematiku do gesce jednoho z ministerstev či ústředních orgánů státní správy s sebou nutně nese konflikt pravomocí. Vládní koordinační orgán naopak může na jedné straně shromažďovat resortní podněty, na straně druhé může využít autoritu vlády k prosazení komplexních technických či legislativních řešení.

Přestože byla Rada vlády pro informační společnost ustavena a do její činnosti byly vkládány velké naděje, nepřinesla její existence doposud jediný použitelný výstup. Toto nepřijemné a na první pohled možná až příliš kategorické konstatování lze opřít i o oficiální informační stránky tohoto orgánu¹⁹², které kromě označení „Rada vlády pro informační společnost“ neobsahují žádné další informace.

Za neúspěchem tohoto potenciálně vysoce perspektivního orgánu můžeme hledat především personální důvody společně se skutečností, že téma strategického rozvoje informační společnosti není v České republice považováno za prioritní. Namísto strategické podpory, tvorby koncepčních řešení, definice standardů či unifikace technických kritérií pro jednotlivé informační systémy tak u nás dochází spíše k realizaci ojedinělých, izolovaných a krátkodobých aktivit partikulárního významu jednotlivými ministerstvy či ústředními orgány státní správy.

k prosazení Úřadu na ochranu osobních údajů, tento potenciál organizačních změn zůstal prakticky nevyužit.

¹⁹² Vzhledem k tomu, že činnost Rady zajišťuje Ministerstvo vnitra, jsou stránky Rady součástí jeho portálu na adrese www.mvcr.cz/informacni-servis-rada-vlady-pro-informacni-spolecnost.aspx.

5.5 STRATEGIE BUDOVÁNÍ INFORMAČNÍ SPOLEČNOSTI NA ÚROVNI MEZINÁRODNÍHO SPOLEČENSTVÍ

K roli mezinárodního společenství třeba předeslat, že aktivity vedoucí k rozvoji informační společnosti mají charakter rozvojový, nikoli záchranný či udržovací. V situaci, kdy je OSN zatížena řešením bezpečnostních konfliktů či elementárních otázek výživy a zdraví, nejeví se budování informační společnosti jako prioritní problém a nelze sem ani očekávat alokaci významných zdrojů. Přesto ustavila OSN agenturu UNGIS (United Nations Group on the Information Society), jejímž primárním cílem má být formulace světových politik v oblasti budování informační společnosti.

Skutečnost, že UNGIS nedisponuje prakticky žádnými významnými finančními ani politickými zdroji společně s faktem, že její existence a činnost jsou jen minimálně reflektovány médií i odborným tiskem, nedávají příliš nadějí na to, že by se tato skupina mohla stát tahounem dalšího rozvoje informační společnosti. Mezi její hlavní činnosti se tedy doposud řadily zejména politické konzultace a kontrola implementace závěrů Světových summitů o informační společnosti (WSIS – World Summit on the Information Society), a to především prostřednictvím tematicky zaměřených konferencí a zpracování analytických srovnávacích studií¹⁹³. Pokud už sama UNGIS vyvíjí nějakou faktickou činnost k rozvoji informační společnosti, jedná se pak pouze o koordinaci aktivit posilujících komunikační infrastrukturu v zemích třetího světa.

Významnou mezinárodní iniciativou na poli rozvoje informační společnosti se naopak stala Mezinárodní úmluva o kyberkriminalitě připravená Radou Evropy ve spolupráci s řadou zámořských zemí včetně USA. Rada Evropy v tomto případě prokázala obdivuhodný konsensuální potenciál,

¹⁹³ Poslední z publikovaných studií je zaměřena problematiku eGovernmentu s názvem UNDESA: The UN E-Government Survey 2008: From E-Government to Connected Governance. Její hlavní přínos je možné vidět v tom, že komparativní metodou a na společném podkladě prezentuje jednoduchá empirická zjištění z různých částí světa a vyzdvihuje zajímavá inovativní řešení.

když se touto úmluvou podařilo její signatáře zavázat k harmonizaci vnitrostátních trestních legislativ a vytvoření systému nepřetržité přeshraniční policejní spolupráce. Úmluva se zaměřuje především na kvantitativní bezpečnost informačních sítí a postihuje i situace mezinárodního významu. Nadto pak obsahuje i závazky harmonizovat národní trestní legislativu v otázkách kvalitativní ochrany informační společnosti, když zavádí povinnost upravit trestnost šíření a držení dětské pornografie a porušování práv duševního vlastnictví.

Skutečnost, že se podařilo na mezinárodním poli prosadit konkrétní závazky států k ochraně informační společnosti je o to významnější, že úmluva má potenciál k dalšímu rozšiřování prostřednictvím opčních protokolů. Tento mechanismus postupného doplňování úmluvy již byl využit pro zakotvení povinnosti stíhat projevy rasismu a xenofobie v informačních sítích¹⁹⁴ a v současné době probíhá debata nad dalšími typy konsensuálně akceptované obsahové kyberkriminality.

I přes dílčí úspěchy naznačené výše však platí, že informační společnost stále není dominantním tématem mezinárodního společenství. Jednotlivé globální kvantitativní i kvalitativní aspekty rozvoje informační společnosti jsou tedy buďto ponechány prakticky bez pozornosti nebo je jim věnována pozornost spíše okrajová. Iniciativu na mezinárodním poli tak v současné době mají především evropské mezivládní a americké nevládní organizace¹⁹⁵, jejichž úspěchy jsou často limitovány partikularitou jejich činností, omezeností jejich zdrojů nebo jejich rozdílnou politickou orientací. Platí přitom, že jakékoli veřejné globální projekty na podporu informační společnosti se nemohou obejít bez spolupráce s globálními dodavateli příslušných technologií, poskytovateli služeb a tvůrci technických standardů - i v tomto aspektu je pak možné vidět důvod stagnace současných mezinárodních aktivit.

¹⁹⁴ Tuto problematiku řeší Dodatkový protokol o trestním postihu rasistických a xenofobních činů spáchaných prostřednictvím počítačových systémů.

¹⁹⁵ V tomto případě se jedná především o nadace a nezisková sdružení podporovaná dodavateli informačních technologií a poskytovateli služeb informační společnosti.

5.6 ZÁVĚREČNÉ POZNÁMKY K POJMU INFORMAČNÍ SPOLEČNOSTI

Smyslem této kapitoly bylo především vymezit pojem informační společnosti z pozice teoretické právní vědy a zdůraznit jeho důležitost pro mechanismus právní regulace. Skutečnost, že právní věda, ale též etika či sociologie, se vlastní vinou stále vracejí k tradičním tématům a pomíjejí fenomén s kritickým významem pro další vývoj společnosti jako celku, způsobuje, že je informační společnost chápána téměř výlučně z ekonomických či technických pozic. Nezájem uvedených disciplin pak vede k tomu, že si kvantitativně orientované autority rozvíjející informační společnost musí často bez dostatečného odborného zázemí samy hledat prostředky k ochraně kvality informací a informačních struktur.

Příkladem mohou být současné práce na rekodifikaci českého občanského práva. Zátiemco je pozornost věnována tradičním avšak v praxi nepoužívaným institutům, jako jsou například koupě na zkoušku nebo výhrada lepšího kupce, právo tvůrce vůbec nezaznamenává například existenci institutu doménového jména a registrační smlouvy (připomeňme, že se podle nespécifických ustanovení českého občanského zákoníku v současné době trvale plní celkem okolo půl milionu takových smluv a tento počet stále stoupá). Řada ustanovení v těchto smlouvách, byť jejich organizační kvalita a obecná rozumnost je nepopíratelná, je však z důvodu absence specifické zákonné úpravy problematická nebo dokonce absolutně neplatná¹⁹⁶.

Vedle kvalitativního pojetí informační společnosti jsme se výše zabývali též otázkou strategie jejího budování. V tomto směru můžeme na jedné straně konstatovat postupný posun od čistě kvantitativního ke kvalitativnímu přístupu. Na straně druhé je však možné podrobit kritice a priori regulativní charakter této strategie, kdy je problém často předvídan a normativně řešen ještě před jeho hypotetickým výskytem. Ačkoli v některých oblastech může být preventivní regulace účinná a žádoucí, formulovali jsme výše názor, že pro informační společnost se tato metoda jeví jako

¹⁹⁶ Příkladem může být konstrukce mandatorního rozhodčího řízení, které je kvůli nezájmu právo tvůrce upraveno pouze nespécifickými soukromoprávními instrumenty. Taková úprava, byť pravděpodobně v nejlepší dosažitelné variantě, je však nanejvýš diskutabilní a je oprávněný důvod se domnívat, že takto založená pravomoc rozhodce je z podstaty vadná.

nevhodná, neboť namísto rozvoje přináší v této oblasti spíše restrikce a balastní právní zátěž.

Konečně jsme se pak stručně věnovali problematice hodnotové povahy informační společnosti. V tomto směru můžeme pracovat s tezí, že informační společnost není *per se* bezhodnotová, neboť základní její hodnoty nese v komplexním efektu její základní jednotka, tj. informace. Informační společnost je tedy možné chápat též jako ideál organizované společnosti, jejíž (nikoli nutně vyjádřenou) esencí jsou přirozené základní hodnoty.

6 PRÁVNÍ INFORMAČNÍ TOKY

6.1 PROMULGACE

Promulgace představuje jeden ze základních problémů platnosti pozitivního práva. Jedná se pozitivistickou optikou o komunikaci konstitutivních výpovědí o normách¹⁹⁷ směrem k jejich adresátům a skutečná existence takových výpovědí pak přímo podmiňuje nastoupení normativního tlaku. Objektivní vnímatelnost právních pravidel je tedy neoddělitelným znakem pozitivitu práva a tím i jeho platnosti¹⁹⁸.

Problému promulgace se důkladně věnoval už Jeremy Bentham. Jeho apel můžeme přitom použít nejen jako úvodní vymezení tohoto tématu, ale lze jej brát i za univerzální motto promulgace jako techniky a jako právního institutu. Bentham píše¹⁹⁹ (překlad autor): „*Má-li být právo dodržováno, je nutné, aby bylo známo. K tomu, aby bylo známo, je třeba jej promulgovat. Ovšem k promulgaci práva není třeba jen to, aby bylo vyhlášeno za zvuku trumpet na ulicích ani jen to, aby bylo čteno lidmi, dokonce ani to, aby bylo všechno vydáno tiskem. Všechny tyto nástroje mohou být dobré, ale jejich použití přesto nemusí vést k dosažení žádoucího účinku. Mohou totiž přinést spíš zdání než skutečnost promulgace. Promulgovat právo totiž znamená předložit jej vědomí těch, které zavazuje, a to tak, aby si jeho obsah mohli přirozeně zapamatovat a aby měli i pak po ruce veškeré dostupné prostředky k následnému řešení případných svých pochybností.*“

Přestože je otázka promulgace jako *conditionis sine quae non* platnosti pozitivního práva ve výše naznačeném smyslu stále aktuální, můžeme její rozsah mírně zrelativizovat. Fuller tak příkladně hovoří o promulgaci jako o nutné podmínce morality práva, jedním dechem však dodává, že je třeba řešit problém rozsahu pozitivního práva, tedy toho, co má být promulgo-

¹⁹⁷ K oddělení pojmu normy od její objektivně vnímatelné podoby, tj. výpovědi o normě viz Kelsen, H. Všeobecná teorie norem. Brno: Masarykova univerzita v Brně, 2000, str. 175.

¹⁹⁸ K tomu srov. tamtéž, str. 153.

¹⁹⁹ Citace byla převzata z digitalizované verze prvního svazku Benthamových esejí původně vydaných v roce 1843 a sestavených Sirem Johnem Bowringem. Digitalizaci Benthamových prací provedl tým University College London a je nyní dostupná na adrese www.ucl.ac.uk/Bentham-Project/.

váno²⁰⁰. Ať už však za rozsah pozitivního práva přijmeme libovolný obor (nabízí se v tomto případě opět řešení formou pozitivního jeho stanovení), musí se každopádně suverén potýkat s tradičním problémem, jak informovat subjekty pod svojí jurisdikcí o vytvoření nového nebo změně stávajícího právního pravidla. Není-li adresát o příslušném pravidle dostatečně informován, je následné nastoupení normativního tlaku velmi problematické, neboť v takovém případě očekává stát od subjektu, že bude realizovat právo, o jehož existenci však nebyl spraven.

Historicky byl problém informovanosti adresátů právních norem řešen různě. Pravidla byla šířena formou ústní tradice, nejrůznějších vyhlášek, právních knih apod. Institut promulgace právních pravidel však měl prakticky bez ohledu na specifika příslušné právní kultury odpradávná silně formální charakter²⁰¹. Adresát příslušného pravidla je *de iure* informován nikoli tehdy, pokud se o tomto pravidle skutečně dozví, ale pokud má formální možnost se s ním seznámit.

Důvodem tradičně hypotetické (nikoli faktické) informovanosti adresátů právních pravidel je především kombinace složitosti a značného rozsahu formálních pramenů práva ve spojení s nízkou úrovní informačních technologií. Prakticky tedy nebylo možné skutečně komunikovat všechny formálně platné prameny práva k jejich adresátům především z toho důvodu, že k takové informační aktivitě nedisponoval stát odpovídajícími komunikačními kanály. Typicky tedy byli adresáti nikoli přímo informováni o formálních pramenech práva, ale publikační povinnost byla splněna pouze formálním zpřístupněním příslušných informačních zdrojů.

Typickým příkladem takového postupu je Sbirka zákonů. Tento informační zdroj má sloužit k šíření informací o právních pravidlech mezi jejich adresáty. Vychází oficiálně ve formě tištěné publikace a veřejnost se s jejím obsahem může seznámit buďto přímo, tj. předplacením, nebo zprostředkovaně v nejrůznějších veřejných institucích, nově i formou neoficiální publi-

²⁰⁰ Srov. Fuller, L. L. *Morálka práva*. Praha: OIKOYMENH, 1998, str. 51 a násl.

²⁰¹ Promulgaci byla věnována pozornost především tam, kde byl právní systém založen na normativních právních aktech. Zweigert-Kötzovou systematikou tak můžeme hovořit především o románské, germánské a severské právní rodině – viz Zweigert, K., Kötz, H. *An Introduction to Comparative Law*. New York: Oxford University Press, 1998, str. 74 a násl., str. 132 a násl., str. 276 a násl.

kace na internetu. Prakticky však Sbírka zákonů svému *ex definitione* účelu informovat adresáty právních pravidel o jejich obsahu již dávno neslouží. Je to způsobeno především obrovskou inflací legislativy a následným zahlcením tohoto informačního zdroje a dále také skutečností, že se, poněkud paradoxně, pro účel informování adresátů právních pravidel kvůli své struktuře prostě nehodí. Namísto Sbírký zákonů tedy dnešní právník pracuje raději s komerčními publikacemi nabízejícími plná znění, komentovaná znění či ještě častěji s právními informačními systémy umožňujícími nejen práci s plným zněním příslušných předpisů, ale též sofistikované vyhledávání, vazby mezi různými typy formálních pramenů práva (typicky mezi legislativou a judikaturou) apod.

Na právě uvedeném příkladu můžeme vidět, že smyslem současných oficiálních komunikačních kanálů, jimiž stát informuje adresáty právních pravidel, ani zdaleka není organizovat společnost pod jurisdikcí příslušného suveréna. Naopak, a poněkud paradoxně, tyto kanály slouží *per se* pouze k legitimaci platnosti příslušného normativního obsahu. Princip *ignorantia legis neminem excusat* tedy zde nevede dokonce ani ke konstrukci domněnky, ale přímo fikce znalosti práva z oficiálního informačního zdroje. Fingování informovanosti odborné i laické veřejnosti o obsahu práva z oficiálních zdrojů je pak nejlépe patrné z komerčního úspěchu služeb a produktů přinášejících jejich adresátům prakticky jen obsah formálních pramenů práva a nahrazujících nedostatečně fungující oficiální informační systém.

ICT a především pak infrastruktura informační sítě přitom poskytují státům kvalitní zázemí pro vytvoření informačních technik, jež jsou způsobilé vrátit institutu promulgace jeho původní smysl a tím i legitimitu. Automatizované zpracování právních informací ve spojení s komunikačními kanály celosvětové informační sítě dávají státům možnost rychlejší, levnější a rozsáhlejší komunikace formálních pramenů práva. Nadto skýtají i prakticky neomezenou možnost nových forem publikace právních pravidel, které jsou v souvislosti se stávajícími formami dostupnější, srozumitelnější, méně náročné na předporozumění apod. Konečně pak využití ICT s prakticky neomezenou dostupností a kapacitou umožňuje vedle instantní informační funkce plnit i Benthamem zdůrazněnou úlohu permanentního zdroje k řešení pozdějších pochybností o obsahu platného práva.

V současné době můžeme z pozitivistického hlediska rozlišit tři způsoby promulgace práva, a to:

- Zákonnou promulgaci (povinná, založena zákonem)
- Oficiální promulgaci (nepovinná, jejím zdrojem je stát)
- Soukromou promulgaci (nepovinná, jejím zdrojem jsou subjekty soukromého práva)

Zákonná promulgace slouží bez výjimky ke komunikaci absolutně závazných pramenů práva a představuje současně podmínku jejich platnosti²⁰². Bývá svěřena státnímu orgánu, který ji pak provádí tiskem respektive prostředky dálkové komunikace. Tento typ promulgace je nejzávažnější, neboť má vzhledem k obsahu příslušných výpovědí konstitutivní charakter - normy komunikované prostřednictvím promulgovaných textů nabývají zákonnou promulgací platnosti.

Vzhledem k zásadnímu významu tohoto typu promulgace pro systém formálních pramenů práva lze očekávat, že jí bude věnována též největší pozornost. Ústředním aktuálním zájmem státu je v tomto směru kvantitativní institut dostupnosti, kdy je hlavní pozornost věnována tomu, aby byly promulgované formální prameny práva formálně dostupné občanům. Stát tedy zaměřuje svoji pozornost především na splnění formální povinnosti, Benthamovými slovy, vydat právní pravidla tiskem. Český i evropský právotvůrce však tuto svoji povinnost plní v mnoha případech doslova minimalisticky, když jsou do zákonné promulgace zahrnovány často jen novely platných právních předpisů. Adresát takto promulgovaného práva je tedy nucen složitě hledat jednotlivé fragmenty aktuálně platné právní úpravy a ty pak sám skládat do formy celistvého textu – tato činnost je přitom natolik svízelná a vyčerpávající, že se jen málokterý rozumně smýšlející člověk jme zjišťovat jejím prostřednictvím obsah platného práva.

Vedle paradoxu faktické nepoužitelnosti zákonné publikace můžeme konstatovat v některých případech i paradox její formální nedostatečnosti – to zejména tehdy, jsou-li texty platných normativních právních aktů pro-

²⁰² Zákonná promulgace argumentačně závazných pramenů práva jim *ex definitione* propůjčuje vyšší intenzitu závaznosti v porovnání s takovými, které jsou publikovány oficiálně nebo jen soukromně.

mulgovány, nikoli však jazykem jejich adresátů. Zvláštním případem pak jsou v tomto směru situace, kdy je jazykové vyjádření právních pravidel natolik chybové, že sám suverén připouští jejich nepoužitelnost resp. nutnost opatření jiné jazykové verze.

Řešením výše uvedených problémů zákonné promulgace souvisejících s dostupností plných znění příslušných normativních textů v jazyce jejich adresátů však často zapomínáme na skutečnost, že není smyslem promulgace přinést adresátu právního pravidla text (tj. výpověď o pravidle), ale dát mu informaci o tom, jaké normativní požadavky na něj klade suverén. Vyřešením kvantitativního problému promulgace tedy v tomto případě ještě ani zdaleka nedojde k naplnění její benthamovská definice – ta má totiž i kvalitativní aspekt měřený účinkem promulgace na vědomí adresáta. Ani v případě, je-li dostupný autentický text v plném znění, tedy nemusí dojít k naplnění smyslu promulgace, neboť i v takovém případě může publikovaný text být natolik složitý a nesrozumitelný, že ani jeho pozorné čtení nepřinese adresátům příslušné normativní informace²⁰³.

Na tuto situaci se hodí slova jednoho z významných představitelů české právní vědy, který na dotaz k praktickému právnímu problému prohlásil: „Do judikatury nekoukejte, to vás jen zmáte.“ Když pak tazatel rezignovaně doplnil, že zákon je ale v oně věci nejasný, dostalo se mu ještě rezolutnější odpovědi: „Do zákona taky nekoukejte, ten vás zmáte ještě víc!“

Oficiálními formami promulgace stát *de facto* přiznává nedostatky jejich zákonných forem a snaží se je s různou měrou úspěšnosti hojit. Dále jsou předmětem tohoto typu promulgace též právní prameny s argumentační závazností²⁰⁴, typicky judikatura vyšších soudů. Oficiální forma promulgace jim sice až na výjimky nepropůjčuje na rozdíl od zákonné promulgace vyšší intenzitu závaznosti, ale stát jejich faktickým zpřístupněním významně usnadňuje jejich používání.

Příkladem oficiální promulgace je v České republice správní portál na adrese portal.gov.cz, jehož součástí jsou i aktuální plná znění účinných právních předpisů. Nejedná se o formu zákonné promulgace (tj. Sbírkou zákonů), ale tím, že přináší alespoň plné texty pří-

²⁰³ K tomu srov. Fuller, L. L. *Morálka práva*. Praha: OIKOYMENH, 1998, str. 64 a násl.

²⁰⁴ K pojmu argumentační závaznosti viz Harvánek, J. a kol. *Teorie práva*. Plzeň: Aleš Čeněk, 2008, str. 250 a násl.

slušných právních předpisů, dalece předčí v použitelnosti zákonně promulgované informační zdroje. Můžeme v této souvislosti spekulovat o tom, co vede státní orgány k tomu, že tuto internetovou aplikaci neobohatí o více funkcionalit, které by například usnadnily vyhledávání v právních předpisech nebo v jejich vzájemných vazbách.

Soukromá promulgace mívá komerční charakter a soustředí se tak na plnění potřeb zákazníků. Snaha přinést adresátům právních pravidel relevantní informace v co nejlépe použitelné formě tak v tomto případě paradoxně není viditelná na straně státu, ale na straně podnikatelů snažících se nabídnout pro adresáty žádoucí službu, kterou však stát není schopen poskytnout ani garantovat. Fikce zakládající povinnost znát obsah publikovaného práva ve spojení s nedostatečnou vůlí a neschopností státu dostát své povinnosti právo skutečně, tj. benthamovsky, promulgovat, tak paradoxně vytváří mohutný trh dostupných a srozumitelných výpovědí o právních pravidlech.

6.2 DORUČOVÁNÍ INDIVIDUÁLNÍCH PRÁVNÍCH AKTŮ

Zvláštní problém pozitivitu a následně platnosti práva představují vedle absolutně či argumentačně závazných pramenů práva i adresované a tedy relativně závazné formy jeho aplikace. Na rozdíl od absolutní závaznosti, jejímiž atributy jsou znalost a respekt obecně vymezeného adresáta, totiž u individuálních právních aktů hovoříme o přímé jejich závaznosti formou vzniku, změny či zániku subjektivních práv nebo povinností²⁰⁵. Nutnost komunikovat takové přímo závazné sdělení státu jeho adresátovi je tedy v tomto případě ještě o něco intenzivnější než nutnost komunikovat obsah nově vytvořených absolutně závazných právních pravidel.

Právní systém na potřebu důkladnější komunikace imperativních informací v tomto případě pamatuje institutem doručení, přičemž platnost resp. právní moc a tím i autoritativní vymahatelnost příslušného individuálního právního aktu nemůže nastat dříve, než je tento svému adresátovi doručen. Doručení je tedy v porovnání s promulgací co do svého účinku fakticky

²⁰⁵ Dokonce i u deklaratorních individuálních právních aktů vznikají s jejich právní mocí práva a povinnosti – v tomto případě vyplývající z autoritativního přiznání nároku.

intenzivnější, avšak z hlediska požadavků na informační schopnosti státu též mnohem náročnější. Doručení tak do značné míry přesouvá těžiště informační aktivity a souvisejících nároků z občana na stát.

Podobně jako ve výše diskutovaném případě promulgate můžeme na institut doručení nahlížet z informační perspektivy, a to jako na prostý informační proces, jehož cílem je seznámit adresáta s obsahem individuálního právního aktu. Ideálně pak plní doručení v podstatě stejné funkce, které ve své úvaze popsal Bentham – v tomto případě však i formálně klademe důraz na to, aby se tento institut benthamovskému ideálu blížil v praxi více, než je tomu u promulgate.

Na rozdíl od promulgate normativních právních aktů neřešíme v případě doručování individuálních právních aktů otázku kompletnosti a dostupnosti příslušného normativního textu. Jednoznačnost a kompletnost je totiž *ex lege* podmínkou jeho bezvadnosti. Závažnější problém zde nepředstavuje ani balastní informační zátěž či složitost příslušných sdělení, neboť normativní obsah bývá zpravidla vyjádřen jednoduše a srozumitelně, to tak, aby mu byl schopen dokonale porozumět i adresát bez specifického předvedění. Problémem konečně není ani inflační výskyt takových sdělení, neboť adresáti individuálních právních aktů musejí informace v nich obsažené zpracovávat zpravidla jen ojedinele²⁰⁶.

Jediným závažným obecným problémem²⁰⁷ doručování individuálních právních aktů tedy z informační perspektivy zůstává technika samotného aktu doručení a jeho právní účinky. Otázkou tedy zůstává, jakou formu vyjádření příslušné informace zvolit a jakým prostředkem ji komunikovat k jejímu adresátovi, abychom mohli s praktickou jistotou konstatovat, že byla „předložena vědomí toho, kterého zavazuje.“

S rozvojem informační společnosti se státu nabízí využití nových komunikačních medií, z nichž ta nejzajímavější jsou vázána na síť internet. Inspi-

²⁰⁶ Připomeňme, že intenzita promulgate normativních právních aktů dosahuje nezřídka astronomických hodnot – v roce 2007 tak frekvence vydávání normativních právních aktů přesáhla jeden denně (včetně dní pracovního klidu a svátků).

²⁰⁷ Problematickou informační kvalitou, tj. např. nesrozumitelnost, nevyváženou strukturu odůvodnění apod. nepovažujeme za obecný problém individuálních právních aktů, ale za zhojitelné nedostatky v konkrétních případech.

raci může stát v tomto případě hledat v soukromé sféře, kde je doručování jedním z nejdůležitějších kontraktačních institutů²⁰⁸.

Když kontrahenti začali okamžitě s rozmachem služeb celosvětové informační sítě hledat mechanismy vzájemného doručování projevů vůle, narazili na technický problém neexistence věrohodného potvrzení o doručení adresátovi. Nejručnější mechanismy sloužící jako náhrada klasické poštovní doručeny totiž prokazují, navíc nikoli věrohodně, pouze skutečnost, že se zpráva dostala do určitého koncového zařízení, tj. do určitého počítače, mobilního telefonu apod. Je sice možné využít sítě nepřímých důkazů a koherenčním způsobem prokázat, že měl určitý adresát k takto doručené zprávě přístup, avšak takové prokazování bývá v praxi technicky poměrně náročné a žádá si (nikoli povinnou) součinnost dalších subjektů. Soudy se tak například při uplatnění námitky doručení u e-mailu zpravidla nespokojí s takzvanou doručenkou, kterou nabízí běžně dostupný poštovní software. Strana, která doručení tvrdí pak musí nabídnout ještě další nepřímé důkazy, jakými mohou být výpisy ze serverů, svědecké výpovědi apod. Typicky se doručení v těchto případech prokazuje snáze, pokud jej potvrdí nezávislý poskytovatel služeb informační společnosti, tj. příkladně poskytovatel připojení, webmailových služeb apod.

Soukromoprávní kontrahenti využívají obvykle k doručování kombinace dostupných technologií a speciálně sjednaných smluvních či předmluvních závazků, konkrétně například kombinace autentizačních nástrojů se závazkem neumožnit jeho použití třetím osobám a užívat jej výlučně k projevům vůle vůči druhé straně²⁰⁹. Často se také, a to i jako součást předmluvních ujednání²¹⁰, objevují závazky stran vzájemně oznamovat přijetí e-mailů formou potvrzovacího e-mailu se zaručeným elektronickým podpisem, jehož

²⁰⁸ Kontinentální právo je založeno na pravidle, podle kterého je smlouva uzavřena až doručení akceptace oferentovi (na rozdíl od angloamerického *mailbox rule* považujícího za okamžik doručení odeslání akceptace).

²⁰⁹ Tyto nástroje mohou na smluvním základě využívat například i šifrování implikující *per se* důvěrný charakter komunikace – podrobně k tomu viz např. Forder, J., Svantesson, D. *Internet and e-Commerce Law*. South Melbourne: Oxford University Press, 2008, str. 58 a násl.

²¹⁰ Taková ujednání bývají součástí předmluvních dohod o mlčenlivosti, jednacích exkluzivitě apod.

součástí je i kopie původní zprávy²¹¹. Další formou, běžně užívanou například aukčními servery, je zřízení kompletní kontraktační komunikační platformy s kontrolovaným a zaznamenávaným přístupem. Autentizace kontrahentů pak probíhá prostřednictvím hesel, která se tito zavazují držet pod vlastní kontrolou.

Má-li stát pracovat s elektronickou formou doručování svých projevů vůle, tj. individuálních právních aktů, je třeba rovněž kombinovat technická a právní řešení zajišťující faktické (technické) i formální předpoklady pro konstrukci právní skutečnosti doručení. Český právotvůrce se rozhodl řešit problematiku elektronického doručování centralizovaně, a to formou specifické služby informační společnosti nazvané Datové schránky. Jedná se v tomto případě o kombinaci technických elementů, tj. autentizace, platformy pro ukládání zpráv a důvěryhodného záznamu veškerých operací, s právní povinností držet přístupové prostředky pod výlučnou kontrolou a s institutem faktického a fingovaného doručení.

Datové schránky, jak jsou navrženy v českém právu, mají fungovat jako centralizovaný²¹² systém, jehož garantem je stát prostřednictvím Ministerstva vnitra. Plánovaná komplexnost celého systému společně s právní povinností zřizovat a používat datové schránky má ambice významně změnit dosavadní realizaci doručování a využít k tomu všech výhod elektronické komunikace, tj. především efektivity (vyšší rychlosti za nižších nákladů) a dále pak lepší kontroly a zabezpečení.

Aktuálně platná legislativa počítá s tím, že datové schránky budou povinně zřizovat orgány veřejné moci a právnické osoby. Ostatní subjekty včetně fyzických osob budou mít možnost zřídit datovou schránku na žádost, a to bezplatně. Celý projekt tedy ambiciózně počítá s tím, že se podstatná část agendy doručování přesune z dokumentární formy do formy elektronické. Vedle pasivní komunikace občana se státem mají navíc datové schránky umožnit i aktivní komunikaci, tj. mají fungovat i pro institut podání orgánu veřejné moci.

²¹¹ Tento mechanismus je používán i u elektronických podání, kdy má podatelna povinnost potvrdit přijetí e-mailového podání formou zvláštního e-mailu podepsaného zaručeným elektronickým podpisem.

²¹² Konkurence může v tomto případě přijít až s ukončením monopolu na poštovní služby – srov. § 14 odst. 2 zákona č. 300/2008 Sb.

Přes nesporně novátorský charakter a velké ambice je možné na českém řešení plné elektronizace institutu doručování vidět i řadu problematických momentů. Předně je třeba si uvědomit, že elektronická forma doručování v pravém smyslu toho slova virtualizuje dosavadní problémy tohoto institutu. To znamená, že řada problematických momentů odpadá, ale řada nových se okamžitě objevuje. Máme-li tedy doposud určité zkušenosti s vyrovnáváním se s úskalími dokumentární formy individuálních právních aktů a jejich následného (nejčastěji poštovního) doručování, je třeba se připravit na to, že přijdou jiná úskalí, která budou ovšem kvalitativně zcela odlišná a často i předem těžko předvídatelná.

Jedním z palčivých problémů, k jehož řešení datové schránky nesporně přispějí, je problém zneužití současné konstrukce institutu doručení k průtahům nebo jiným obstrukcím v řízení. Relativně nedávno se tak například známý pražský advokát poté, co v budově soudu spatřil pracovníka justiční stráže s písemností v ruce, dal před ním na útěk. Justiční strážník jej, zřejmě díky lepší kondici, sice záhy dostihl, advokát však i přes to nerezignoval a odmítl obsílku převzít. Doručení obsílky se pak stalo sporným bodem dalšího řízení.

Příkladem kvalitativně nového problému datových schránek může být skutečnost, že se jedná o komplexní systém, který je technicky zajišťován právníkou osobou a garantován orgánem veřejné správy. Přestože zákon přímo zakazuje správci, tj. Ministerstvu vnitra i provozovateli, tj. držitelé poštovní licence, přistupovat k datům ve schránkách²¹³, faktická možnost nepozorovaně a beze stop vytěžovat obsah datových schránek uvedenými institucemi nebo jejich pracovníky představuje reálný problém²¹⁴, a to jak ve vztahu k ochraně subjektivních práv jednotlivých subjektů, tak i co do ochrany principu dělby moci.

Obdobný problém představuje, především u fyzických osob, možnost udělení přístupových práv do datové schránky třetímu subjektu či dokonce možnost udělení práv třetí osobě podávat za osobu dokumenty ze schránky orgánům veřejné moci. Nejde přitom co do rozsahu o pouhou obdobu plné moci, ale kvůli faktické koncentraci informačního a komunikačního potenciálu o doslova totální prostředek v důsledku vedoucí k právnímu ovládnutí

²¹³ Srov. § 14 odst. 6 zákona č. 300/2008 Sb.

²¹⁴ Zde je třeba dodat, že zákonné řešení tohoto problému je u centralizovaného systému značně komplikované.

příslušného subjektu. Míra kvalifikované právní zneužitelnosti takto mocného institutu například proti dlužníkovi (v případě jeho použití jako quasi-zajištění dluhu) nebo nemohoucímu člověku je pak prakticky neomezená.

Ve vztahu k právníkům osobám je pak možné předpovídat například problematickou roli datové schránky v případech nejrozličnějších podílnických či manažerských soubojů o kontrolu nad korporacemi. Agenda datových schránek se tak jistě stane kolbištěm pro lité právní bitvy podobně, jako jsou jím nyní obchodní rejstříky. Otázkou, kterou *a priori* zřejmě nelze uspokojivě zodpovědět, v této souvislosti zůstává, zda je stávající právní úprava celého systému pro tento případ dostatečně robustní.

Výše uvedené však v žádném případě neznamená, že by snad služby informační společnosti nebyly s to pokrýt potřeby institutu doručování. Je-li však tento institut v porovnání s promulgací poměrně složitější a náročnější na vynaložené úsilí státu, je třeba rovněž očekávat více problémů a komplikací při jeho realizaci prostřednictvím kvalitativně nových technologií.

6.3 ELEKTRONICKÁ PODÁNÍ

Poslední z forem komunikace mezi státem a subjekty pod jeho jurisdikcí představují podání. Jedná se o procesní formu právního jednání užívanou subjekty k aktivní komunikaci se státem. Z informační perspektivy tak jde o opak individuálních právních aktů, kdy původcem sdělení je v tomto případě subjekt a jeho příjemcem je stát. Podání sice nemá normativní charakter, pro jeho odesilatele však může mít velký význam²¹⁵. Z hlediska státu je tedy žádoucí, aby bylo podávání pokud možná co nejjednodušší a jeho procesní efekt co nejbezprostřednější.

Jakékoli bezdůvodné bariéry pro podávání mohou vést k přímému popření základních práv, především pak práva na spravedlivý proces. Takovou bariérou, k jejíž akceptaci již tradičně došlo, je u řady podání podmínka jejich písemnosti. Technická obstrukce však v tomto případě není nikterak vážná a lze tedy konstatovat, že subjekty v jejich možnosti komu-

²¹⁵ Připomeňme, že prostřednictvím podání se nejen zahajují či modifikují řízení, ale že podání mohou mít i hmotněprávní účinky – typicky stavením lhůt.

nikovat se státem nijak zvlášť neomezuje. Jiné podmínky jsou k vidění výjimečně a mají spíše akcesorickou povahu k podmínce písemnosti. Můžeme se tedy setkat například s požadavkem na legalizaci dokumentu před jeho podáním, s podmínkou vytvoření dokumentu osobou se specifickou kvalifikací apod.

Vzhledem k tomu, že i podání je, podobně jako předchozí dva instituty, ve své podstatě informační instrument, mohou být k jeho komunikaci nasazeny moderní prostředky informační společnosti. Předpokladem toho, aby i tato forma komunikace lépe a efektivněji plnila svůj základní účel, tedy informačně spojit občana se státem, je opět nalezení a implementace odpovídající technologie a její následné adekvátní využití.

Základní problémy podávání za užití služeb informační společnosti jsou poněkud odlišné od těch, které jsme diskutovali výše. Nepředpokládáme například, že by se stát z nějakého důvodu bránil doručení určitého podání a, obrazně řečeno, prchal a schovával se před doručovatelem. Naopak ovšem musíme řešit problém fingovaného nebo jinak vadného podávání.

Tu a tam se v praxi objevují případy, kdy advokát, zavalen prací, s hrůzou zjistí, že je právě noc posledního dne běhu důležité lhůty. Aby uchránil klienta i sebe před katastrofou, vloží do faxu pár prázdných papírů a zašle je podatelně soudu. Během následujících tří dnů pak horečně napíše na stejný počet papírů text příslušného podání. Koncipient pak dostane nakázáno donést písemný originál teď už kompletního podání na soud, podívat se přitom, že před dvěma dny přišly jen prázdné listy a srdceryvně přísahat při svatém Yvonovi, že příslušný dokument sám uprostřed noci psal a odesílal.

Další obecný problém podávání prostřednictvím služeb informační společnosti spočívá v tom, že stát už nemůže ponechat pro tento typ komunikace relativně volná pravidla a požadovat jen zachování písemné formy, ale musí určit technologické standardy a případně i bližší podrobnosti formálního postupu. Splnění těchto požadavků pak samozřejmě omezuje odesílatele a do určité míry i ztěžuje podávání. Je proto třeba klást maximální důraz na omezení možnosti svévole jednotlivých státních orgánů a konkrétně pak důsledně dbát na dodržení principů technologické neutrality a zákazu diskriminace.

Stále bohužel nejsou výjimkou elektronické podatelny orgánů veřejné moci, které akceptují podání například jen ve vybraných proprietárních datových formátech nebo na podá-

ní aplikují jiná diskriminační omezení. Nedostatečnou ochotu a schopnosti státních orgánů pak musejí hojit výrobci a dodavatelé kancelářského a komunikačního software, jejichž produkty běžně umožňují formátové konverze i aplikaci dalších více či méně iracionálních omezujících podmínek.

V České republice je podávání za užití služeb informační společnosti řešeno dvěma základními způsoby, a to prostřednictvím elektronických podatelů a perspektivně pak za užití datových schránek. Oba způsoby jsou legislativně upraveny a orgánům veřejné moci je v tomto případě stanovena nikoli jen možnost ale přímo povinnost přijímat podání v elektronické formě.

Elektronické podatelny jsou starším řešením, které bylo sice zavedeno plošně, jeho technická realizace však probíhá decentralizovaně v režii jednotlivých orgánů veřejné moci. Legislativa v tomto případě stanoví základní podmínky pro provoz elektronických podatelů, přičemž jejich provedení, a to včetně úhrady nákladů, je již záležitostí jednotlivých orgánů veřejné moci. Nejčastější formou elektronické podatelny se tak stala e-mailová schránka, jejíž adresa je veřejně vyhlášena.

Problém prokazatelnosti doručení je u elektronických podatelů řešen povinností podatelny potvrdit přijaté podání. Takové potvrzení obsahuje v kopii původní zprávu a je podepsáno zaručeným elektronickým podpisem pracovníka podatelny. Tím jsou prokázány kromě skutečnosti doručení i obsah doručené zprávy, datum a čas doručení jakož i identita osoby, která podání přijala.

Přes skutečnost, že elektronická podání splňují požadavky na písemnou formu, nelze stále řadu podání, a to především v nejrůznějších správních procesech, tímto způsobem realizovat. Typickým důvodem uváděným orgány státní správy a samospráv pro nemožnost podávat elektronicky je nutnost zachování původní dokumentární formy příslušných formulářů, někde dokonce i s poukazem na to, že jsou tyto formuláře následně digitalizovány. Přestože je takový důvod zjevně mylný, nebyla samotná možnost elektronického podávání v takových případech doposud podrobena judiciálnímu testu zákonnosti ani ústavnosti.

Vedle orgánů státní správy a samospráv jsou elektronickými podatelny vybaveny samozřejmě i soudy. Přestože i v tomto případě splňuje elektronická forma podání požadavek písemnosti, dochází stále na řadě soudů k tomu, že podání jako takové je sice přijato, jeho přílohy však již soud

vcelku nepochopitelně vyžaduje v papírové formě²¹⁶. Ani v tomto případě však ještě nebyl postup, kdy je elektronický dokument bezdůvodně odmítnut jako irelevantní, ústavně testován.

Zvláštním typem podání jsou taková, jejichž realizaci usnadňují automatizované podatelny²¹⁷. Ty bývají zřizovány orgány veřejné moci, které zpracovávají velká množství podání. Díky tomu, že se takové podatelny například starají o automatizovanou strukturu podání, vkládají do nich standardní formulace apod. nejen usnadňují uživatelům sepsání příslušných podání, ale zároveň ulehčují přijímajícím orgánům následné jejich automatizované nebo poloautomatické zpracování. Jediný problém takových řešení představuje nastavení formalizačních kritérií, přičemž je třeba zvlášť dbát na to, aby příslušné elektronické formuláře a jejich soustavy²¹⁸ neomezovaly nebo dokonce neodrazovaly uživatele chtivě sepsat podání.

Obdobnou funkci jako v současnosti fungující elektronické podatelny bude plnit i podávání prostřednictvím datových schránek. Na rozdíl od podávání prostřednictvím e-mailu nebo specializovaných aplikací nebude nutné vyžadovat doručky²¹⁹ a uživatelé nebudou muset disponovat zaručenými elektronickými podpisy²²⁰. Vzhledem k tomu, že systém je v současné době teprve připravován a nejsou známy podrobnosti o jeho parametrech, není jasné, zda i datové schránky umožní nasazení asistenčních aplikací usnadňujících formulaci podání. Již nyní je však aktivní komunikace občanů ke státu formou podání nejvíce diskutovanou a technicky i právně nejproblematictější funkcionalitou systému datových schránek.

Ať už je podávání realizováno prostřednictvím e-mailu, specializovaných aplikací nebo uceleného systému datových schránek, je třeba si při

²¹⁶ Tato situace je obvyklá například u plných mocí, kde se soudy leckde nespokojí ani s elektronickým dokumentem podepsaným zaručeným elektronickým podpisem zmocnítele.

²¹⁷ Příkladem takového řešení může být univerzální justiční podatelna na adrese epodatelna.justice.cz.

²¹⁸ Běžné je řešení, kdy aplikace formou jednotlivých dotazů zjišťuje informace k vyplnění určitého podání. Odpovědi se zadávají do formulářových polí a uživatel postupuje od jednoho kroku ke druhému podobně, jako například při nákupu v on-line obchodě.

²¹⁹ Systém datových schránek díky své technické struktuře poskytne věrohodné a průkazné informace o doručení do příslušné schránky.

²²⁰ Autentizace bude vyžadována při přístupu do datové schránky – validaci obsahu jednotlivých podání pak již zajistí systém.

analýze jeho kritických momentů nejprve opět uvědomit základní rysy komunikace za užití služeb informační společnosti. Jakákoli komunikace prostřednictvím těchto služeb je v porovnání s jinými oficiálními formami komunikace (tj. osobně nebo prostřednictvím papírového doručování) nadměru rychlá, jednoduchá a dostupná. Vedle nesporných pozitivních efektů zahrnujících zvýšení efektivity, zlepšení dostupnosti (včetně nezanedbatelného momentu usnadnění přístupu k úřadům osobám se smyslovými handicapami), zvýšení rychlosti a zlevnění procesu podávání, však tyto základní rysy též zvyšují pravděpodobnost narušení a zneužití.

Narušením v tomto případě chápeme především vnitřní nebo vnější útok cílený z jakéhokoli důvodu na ochromení příslušné části státní komunikační infrastruktury. Jakkoli sofistikovaný systém nemůže pravděpodobnost takového útoku vyloučit a v sázce pak je nejen fungování státní agendy, ale především důvěra občanů ve stát²²¹. Nabízí se samozřejmě v takovém případě odstavit systém elektronického podávání a pracovat za užití standardních postupů – takové řešení však je možné pouze za situace, kdy lze tento postup fakticky zajistit. Tam, kde dojde k nasazení metod informační společnosti, však lze očekávat realokaci zdrojů nebo alespoň snížení standardních kapacit²²². To pak může mít v případě problémů elektronického systému za následek zhroucení nejen elektronického podávání, ale v případě výpadku i značné kapacitní problémy jeho klasické papírové alternativy.

Druhým kritickým momentem elektronického podávání je možnost zneužití jeho výhod. Jednoduchost a dostupnost tohoto typu podávání pak může vést, možná na první pohled paradoxně, k šikaně orgánů veřejné správy občany zneužívajícími výhodami jednoduché komunikace k zahlcení státu podáními různých typů. Zde je tedy třeba zvlášť upozornit na skutečnost, že oficiální kverulantství je přirozeným průvodním jevem demokracie

²²¹ Připomeňme, že právě důvěra je neuralgickým bodem, na nějž jsou mířeny nejrůznější typy násilných či propagandistických teroristických aktivit. Například Bobbitt formuluje v tomto směru zajímavou hypotézu, že vítězstvím terorismu už je i jen samotné vymizení důvěry v to, že jen státy mohou vést války – srov. Bobbitt, P. *Terror and Consent*. New York: Alfred A. Knopf, 2008, str. 126 a násl.

²²² Je-li například většina podání určité agendy realizována elektronicky, není důvod zaměstnávat desítky přepážkových úředníků, ať už státních, samosprávních nebo soudních.

a jedině, co je s to jej brzdit, jsou přirozené limity dané neefektivitou výkonu jednotlivých administrativních, policejních, soudních a jiných činností. Vysoce efektivní systém rychlého elektronického podávání se pak může v rukou technicky zdatného kverulanta stát doslova smrtícím nástrojem.

V uvedených souvislostech je tedy třeba ještě před skutečně masivním nástupem elektronických podání vést důkladnou diskusi proporcionality dvou ze základních právních principů, a to principu volného přístupu k veřejné moci a principu zákazu zneužití práva²²³ (zde procesního práva podávat a zakládat podáními procesní povinnosti orgánů veřejné moci).

Nejsou výjimkou případy, kdy nespokojený občan bombarduje nejrůznější orgány veřejné moci nesmyslnými nebo dokonce šikanózními podáními. Velmi oblíbeným je v tomto směru především výkon práva na svobodný přístup k informacím realizovaný dle zákona č. 106/1999 Sb. Orgány veřejné moci, které se octnou pod palbou žádostí o informace i jen průměrně zběhlého kverulanta, nemají v současné době prakticky žádné zákonné prostředky k obraně²²⁴. Ba co víc, ony nemohou ani před kverulantem prostě kapitulovat.

Zatímco problematice svévole státu věnují orgány soudní moci včetně Ústavního soudu pochopitelně velkou pozornost, nebyla problému svévolného nakládání se subjektivními právy na přístup k orgánům veřejné moci včetně práva na soudní ochranu věnována doposud prakticky žádná pozornost. Soudy v režimu správního soudnictví ani Ústavní soud tak doposud, zřejmě ze strachu o vstoupení na kluzký svah, neformulovaly čitelný právní názor na otázku, kdy jde ze strany účastníka řízení k prostému využití jeho zaručených práv podávat a dožadovat se aktivit státu²²⁵ a kdy jde naopak o zneužití těchto práv ke kverulantství.

²²³ Důsledkem zneužití je v tomto případě nejen plýtvání státních zdrojů, ale též snížení výkonnosti příslušných orgánů veřejné moci při uspokojování potřeb ostatních občanů.

²²⁴ Nabízelo by se řešení formou zpoplatnění příslušných úkonů – i to je však v naznačeném případě upraveno tak restriktivně, že poskytnutí šikanózně vyžadovaných informací lze kalkulovat maximálně v řádech desítek korun.

²²⁵ Připomeňme, že i v tomto případě nejde o nedotknutelná či svatá práva, ale o projev pouhých právních principů artikulovaných u nás Listinou základních práv a svobod.

6.4 ZÁVĚREČNÁ POZNÁMKA K PRÁVNÍM INFORMAČNÍM TOKŮM

V této části jsme se pokusili krátce popsat formy, jimiž služby informační společnosti modifikují základní způsoby komunikace občana a státu. Vzhledem k tomu, že nasazování nejrůznějších prostředků dálkové komunikace v čele s komunikací prostřednictvím služeb celosvětové sítě internet při výkonu státních agend je přirozené a vysoce žádoucí, je nutné, aby se právo důkladně zabývalo souvisejícími otázkami. Nejde přitom jen o vytváření parciálních řešení pro jednotlivé agendy, ale především o pochopení podstaty skutečné virtualizace jednotlivých informačních aktivit.

Problém právních informačních toků jsme zde rozdělili do struktury dle původce a adresáta příslušných právně relevantních informací. Promulgaci je v tomto směru možné vidět jako neadresovanou komunikaci normativních informací. Doručování pak jsme popsali *stricto sensu* jako proces, při němž jde opět o komunikaci informací, jejichž původce je stát, zde však k přesně určeným adresátům. Posledním typem komunikace, na který jsme se v této části zaměřili, pak bylo podávání, jehož informační podstata spočívá v komunikaci informací od občana či korporace ke státu.

Pro všechny typy informačních toků nabízejí současné a perspektivní informační a komunikační technologie řadu možností k zásadním kvantitativním i kvalitativním posunům. V některých případech, typicky u promulgace, můžeme konstatovat totální deficit ve využití (často i jen jednoduchých) dostupných technologií a je tedy na místě vyvíjet soustavný tlak na právotvůrce, aby příslušné informační procesy odpovídajícím způsobem upravil. V otázkách souvisejících s doručováním a podáváním je situace nepoměrně lepší, neboť zde již stát částečně reflektuje technologický vývoj²²⁶. V důsledku virtualizace těchto informačních agend je pak třeba řešit kvalitativně nové právní problémy, a to tak, aby nově zaváděné metody skutečně plnily svoje základní právně-informační funkce.

²²⁶ V porovnání se soukromým sektorem je to sice reflexe žalostně pomalá, stále však je lépe, pokud je nějaká spíše než žádná.

7 SLUŽBY INFORMAČNÍ SPOLEČNOSTI V JUSTICI - EJUSTICE

7.1 AUTORITATIVNÍ APLIKACE PRÁVA JAKO INFORMAČNÍ PROCES

Na procesy autoritativní aplikace práva lze z perspektivy právní informatiky pohlížet i jako na relativně prosté procedury tvorby, zpracování a následné distribuce informací. Orgán autoritativně aplikující právo, především soud, je touto optikou vnímám jako informační procesor, v němž dochází ke zpracování skutkových a právních informací vztahujících se k příslušnému případu. Výstupem pak je opět informace, tj. akt autoritativní aplikace práva, která ještě pro svou perfekci z formálního hlediska vyžaduje doručení (komunikaci) příslušným adresátům.

Toto kvantitativní pojetí práva není pro právníky příliš atraktivní a nejrůznější teorie, které se snaží popsat mechanismus právní regulace výše naznačeným způsobem, chápeme v lepším případě spíše jako zábavné extenze teoretické právní vědy. Pragmatický pohled na fungování procesů autoritativní aplikace práva však odhalí řadu po technické stránce kritických momentů, které mají sice ve své podstatě kvantitativní charakter, ve výsledku však zásadním způsobem ovlivňují kvalitu procesů. V tomto případě přitom nesrovnáváme banální informační toky při autoritativních aplikačních procesech s ničím menším, než je jeden ze základních kamenů legitimacy či morálky práva, tj. korespondence hmotného práva a výstupů z jeho procesů²²⁷.

S postupným rozvojem informačních a komunikačních technologií, především se zvyšováním jejich výkonu a kapacity, roste i potenciál těchto technologií v procesech autoritativní aplikace práva. Zřejmým cílem nasazení těchto technologií je pak především zvýšení efektivity (viz dále) a sní-

²²⁷ Srov. Fuller, I. Morálka práva, Praha, OIKOYMENH, 1998, str. 79 a násled.

žení míry rizika informačních defektů. Pro ilustraci informačních lapsů můžeme zmínit například situace, kdy soud:

- „zapomene“ aplikovat právo a dojde k průtahům v řízení
- čeká, až se k němu dostanou informace, na jejichž základě má rozhodnout nebo až procesní informace doputují stranám – opět jsou výsledkem průtahy
- ztratí ze spisu důležitý dokument
- nezjistí objektivní pravdu – nedostane se k adekvátním informacím o skutkovém stavu
- neodhalí kvantitativní chyby v předchozím řízení
- neoznámí (nedoručí) stranám některý z výstupů procesu apod.

Některé výše uvedené příklady problematické manipulace s informacemi vedoucí v důsledku k porušení práva na spravedlivý proces jsou samozřejmě sankcionovány, a to od úrovně disciplinární přes jednoduché právo až po ústavní rovinu. Nemůžeme však tyto problémy považovat za vyřešené jen proto, že na ně pamatují sankční ustanovení příslušných předpisů – dokud totiž tyto potíže objektivně existují, má justice povinnost hledat proti nim účinná protiopatření.

Jsou-li k dispozici přímé metody a dokonce technické (nikoli jen právní) prostředky k eliminaci uvedených problémů, jejich nasazení bývá nesrovnatelně efektivnější než *ex ante* hrozba sankce nebo *ex post* její uplatnění²²⁸. Takovými prostředky pak mohou být ve výše naznačeném směru právě informační a komunikační technologie, jejichž prostřednictvím lze zajistit procesům autoritativní aplikace práva přísun adekvátních informací, kontrolu jejich integrity, zvýšení ochrany, automatizovanou kontrolu dodržování procesních postupů, zefektivnění jednoduchých informačních operací apod.

²²⁸ Namísto normativity zde pak hovoříme o kauzalitě – k tomuto rozdílu v prostředí informačních sítí viz např. Polčák, R. In *Law, We Trust: Shortly to Bumblebees and the Normativity of Law in Cyberspace*, in *Cyberspace 2006*, Brno, Masarykova Univerzita, 2006, str. 3 a násl.

7.2 ELEKTRONIZACE A PROPORCIONALITA EFEKTIVITY

Nikoli přímo kvantifikovatelným, přesto však zásadně významným je obecný empirický aspekt autoritativní aplikace práva zjednodušeně ve výsledku označovaný jako vymahatelnost práva²²⁹. Podobným, nikoli však už tak populárním pojmem, je pak pojem efektivity²³⁰, kterou zjednodušeně ekonomicky vzato lze vymezit jako vztah mezi náklady a úspěšností ochrany základních hodnot sledovaných státem.

Snaha o zvýšení efektivity procesů autoritativní aplikace práva se přitom může dostat do přímého konfliktu s různými komponentami práva na spravedlivý proces nebo s jinými právními principy²³¹. Dojde-li tak příkladně ke stanovení lhůty k určitému rozhodnutí, může tím být negativně narušen princip rovnosti stran, princip zjištění materiální pravdy nebo třeba princip *iura novit curia*. Příkladem totální efektivity na úkor ostatních právních principů může být pak známé rčení „*pověste je všechny, on už si to Pánbů přebere*,“ nebo jeho aktuální justiční obdoba „*nějak to rozhodni, hlavně, ať už to odsud zmizí*.“

Proporcionalita mezi efektivitou autoritativní aplikace práva a dalšími právními principy²³² nemá, alespoň co se týče nasazení různých technických prostředků, ani zdaleka tak jasné kontury jako extrémní případy ohrožení spravedlivého procesu zmíněné v úvodu. Zatímco lze konstatovat, že opomenutí soudce aplikovat platné právo je frapantním zásahem do práva

²²⁹ Z popularizačních aplikací srov. např. Štraus, J. Vymahatelnost práva, právní rada. ihned.cz, 28. 6. 2006.

²³⁰ K pojmu efektivity z ekonomického hlediska viz především publikace z oboru law and economics. Specificky se problematice efektivity v justici věnuje i jedna ze základních monografií tohoto aktuálního směru v právním myšlení – viz Posner, R. A. *The Economics of Justice*. London: Harvard University Press, 1983, str. 13 a násl.

²³¹ Obecně se tomuto problému z liberální perspektivy věnuje Arnold, R. A. *Efficiency vs. Ethics: Which is the Proper Decision Criterion in Law Cases?*, *The Journal of Libertarian Studies*, ročník 6, číslo 1, str. 49 a násl.

²³² K problému aplikace právních principů a pojmu proporcionality viz Alexy, R. *On the Structure of Legal Principles*, *Ratio Iuris*, ročník 13, číslo 3, str. 1 a násl., z česky psané literatury pak Holländer, P. *Filosofie práva*, Plzeň, Aleš Čeněk, 2006, str. 158 a násl.

na spravedlivý proces, nelze vždy vyjádřit jednoznačné mínění ohledně toho, jaká míra neefektivit již má obecně být sankcionovatelná²³³. Obdobně pak, uložíme-li například soudci disciplinární sankci za nerespektování platného procesního předpisu, těžko se bude bránit poukazem na svou nezávislost. Má-li však být taková sankce uložena za neefektivní práci, je třeba důkladně zkoumat, zda je i sama možnost jejího uložení proporcionální a zda nejde spíše o šikanu soudce (tj. o nepřípustný zásah do jeho nezávislosti).

Hovoříme-li o zavádění nových technologií a uniformních postupů do justičních procesů, jedná se vždy o určitý zásah do soudcovské nezávislosti²³⁴. Je-li pak tento zásah veden ve snaze zvýšit efektivitu rozhodovací činnosti, je třeba vždy zkoumat standardním ústavním testem proporcionality²³⁵, zda je příslušné řešení:

- vhodné (zda splní svůj účel, tj. v tomto případě zvýší efektivitu procesů autoritativní aplikace práva)
- potřebné (tj. zda nelze stejného výsledku dosáhnout bez zásahu do jiného právního principu)
- poměrné (zda je důvod v tomto případě upřednostnit efektivitu před jiným principem)
- minimálně škodlivé (tj. zda je minimalizován zásah do ostatních principů, typicky do principu nezávislosti soudce)

Vyjdeme-li z předpokladu, že základy našeho právního systému (včetně základních práv) mají charakter právních principů²³⁶, docházíme k závěru, že výše uvedený test je třeba provádět vždy tam, kde by nasazení techniky

²³³ K tomu viz např. Cooter, R. D. Liberty, Efficiency and Law. Law and Contemporary Problems, ročník 50, číslo 4, str. 141 a násl.

²³⁴ K tomu ostatně dochází pokaždé, kdy je soudce direktivně usměřován ve své práci – banálním příkladem je rozpis jednacích místností, který omezuje soudce v možnosti nařídít jednání na určité místo.

²³⁵ Do našeho právního řádu byl tento test zaveden kontinuální řadou rozhodnutí Ústavního soudu, z nichž můžeme vybrat Pl. ÚS 4/94 ze dne 12. 10. 1994 nebo III. ÚS 256/01 ze dne 21. 3. 2002.

²³⁶ K tomu viz např. Dworkin, R. Non-Neutral Principles, The Journal of Philosophy, ročník 74, číslo 14, str. 491 a násl.

do procesů autoritativní aplikace práva mohlo přinést újmu dosavadnímu rozložení práv stran nebo kvalitě oprávnění soudů (soudců). Nejde tedy jen o nezávislost soudce, ale též například o rovnost stran, zákaz *denegationis iustitiae*, zásadu *audiatur et altera pars* apod.

Nelze s prostým poukazem na efektivitu bez dalšího (roz. bez argumentu proporcionalitou), a to ani zákonem, například direktivně přikázat soudci, aby pro určité typy své rozhodovací činnosti používal počítač a určitý software. Ani soudce však na druhou stranu nemůže dobře argumentovanou direktivu k užití nové technologie bez dalšího odmítnout, například jen jednoduchým poukazem na svou nezávislost (i ta je totiž ve své podstatě právním principem²³⁷) ale pouze tehdy, není-li direktivně aplikované technické řešení ve vztahu k jeho nezávislosti proporcionalní. K tomu může dojít například v případě, je-li soudce nucen k používání systému, který jej z definice omezuje ve formulaci výroku rozhodnutí. Můžeme ještě dodat, že struktura proporcionality zjevně nepočítá s individuálními preferencemi jednotlivých soudců. To znamená, že plošně zavádnou justiční technologii nelze poukazem na soudcovskou nezávislost odmítnout ani z důvodu individuální technické neobratnosti, špatného rozměru nebo třeba mentální rezervace.

Soudce se má z pohledu technologie soudní moci zabývat především autoritativním zpracováním informací a vytvářením nových informací pro účastníky. Dělá-li soudce cokoli jiného, tj. tráví-li čas zdlouhavým vyhledáváním informací²³⁸ (v normativních právních aktech, judikatuře, ...) nebo jejich komunikací (poučování, obesílání, ...), jedná se o neefektivní využití jeho času. Z pohledu soudce je tedy možné vnímat efektivitu jako jeho přiblížení základnímu pracovnímu úkolu, tj. souzení. Efektivní je pak v tomto směru takové řešení, které soudci v minimálním čase a s minimálními náklady přinese na základě jeho požadavků skutkové a právní infor-

²³⁷ K pojmu nezávislosti soudce a jejích limitů viz např. publikaci Wojciechowski, B. Dyskrecjonalność Sedziowska. Toruń: MADO, 2004, str. 197 a násled.

²³⁸ Volba informačních zdrojů a práce s nimi samozřejmě spadá pod rozsah činností soudce, nikoli však už vyhledávání po knihovnách a archivech.

mace, na jejichž základě bude moci pohodlně²³⁹ rozhodovat a o nic dalšího se nestarat.

Hledisko soudce však není co do efektivity samozřejmě jediným. Z pohledu účastníků řízení je efektivní takový proces, který jim s minimálními náklady (časovými, materiálními) umožní získat potřebné skutkové a právní informace, vést proces a dosáhnout ve věci perfektního rozhodnutí. Z pohledu státu je pak efektivní taková justice, která, jak bylo uvedeno výše, při minimálních nákladech plní funkce legitimující její existenci; ty zahrnují vedle výkonu samotné rozhodovací činnosti též například aktivity zajišťující její dostupnost, transparentnost, vážnost nebo plnění mezinárodních závazků.

Tlak na efektivitu je v justici ze zřejmých důvodů nesrovnatelně menší, než je tomu u komerčních právních činností²⁴⁰. Tam, kde je výkon právnických povolání motivován dosažením zisku, došlo již v minulosti k masivnímu nasazení informačních technologií zjednodušujících jednotlivé právníkové činnosti. Těžko tak dnes hledat advokátní kancelář, jejíž advokáti by nebyli vybaveni právními informačními systémy, přístupem na internet nebo mobilními telefony. Míra užívání informačních technologií v komerční právní službě však jde často ještě mnohem dál, to především u větších organizací, jakými jsou velké advokátní nebo poradenské kanceláře. Zde jsou zhusta k vidění komplexní centralizované systémy pro oběh elektronických dokumentů, kancelářský management, podpůrné nástroje pro automatizovanou tvorbu jednoduchých smluv nebo podání, aplikace pro permanentní dálkový kontakt s klienty apod.

Není samozřejmě smyslem tohoto článku srovnávat soudní praxi s výkonem advokacie. Jestliže však může být často i velice náročný klient

²³⁹ Kritérium pohodlí soudce si zaslouží zvláštní důraz, neboť pohodlí je v tomto případě určujícím faktorem kvality diskreční úvahy – srov. Vermuele, A. *The Judiciary is a They, not an It: Two Fallacies of Interpretive Theory*, The University of Chicago Public and Legal Theory Working Paper No. 49, 2003, str. 20 a násl.

²⁴⁰ Srovnatelný tlak můžeme v tomto směru pozorovat ze současné Evropy snad jen v Nizozemí, kde byl systém justice reformován takřka do podoby komerční služby. Jediný podstatný rozdíl mezi justicí a komerční právní praxí zde lze s nadsázkou vidět v tom, že soud nemůže skončit v úpadku. Reformou nizozemské justice v kontextu efektivity se zabývá publikace Hol, A., Loth, M. *Reshaping Justice- Judicial Reform and Adjudication in the Netherlands*. Maastricht: Shaker Publishing, 2004, str. 11 a násl.

uspokojen právní službou poskytovanou za užití moderních technologií (a řada klientů tento způsob dokonce přímo vyžaduje), není důvod se domnívat, že by obdobné technologie nebyly s to uspokojit za současného zvýšení efektivity systému i klienty justice, ať už za ně považujeme účastníky řízení nebo prchlivou a panovačnou Spravedlnost.

7.3 POJEM ELEKTRONICKÉHO SPISU

Centrálním momentem procesů autoritativní aplikace práva je spis. Jakkoli inovativní tedy má být řešení těchto procesů za užití informačních technologií, je třeba, aby roli spisu v podstatě zachovalo. Jakékoli technické řešení elektronizace, které by alespoň v dlouhodobém výhledu nepočítalo s elektronickým spisem, by přitom muselo čelit obtížím spojeným s udržetím vztahu elektronizovaných operací s papírovým spisem. Těžko si pak lze představit, že by technické řešení, které by bylo ve své podstatě postaveno na neustálé konverzi operací z papírové do elektronické podoby a zpět (ta by byla třeba vždy při komunikaci elektronické agendy s papírovým spisem), bylo dostatečně robustní, funkční, efektivní a ergonomické.

Přestože je elektronický spis jádrem celého systému elektronické justice, z hlediska technického nepředstavuje jeho architektura nikterak problematické zadání. Jedná se totiž pouze o elektronickou obdobu desek, do nichž jsou postupně vkládány jednotlivé dokumenty. Důležité je, aby elektronický spis nebyl omezen jen na určitý typ dokumentů, tj. aby zvládal práci s různými datovými formáty včetně audiovizuálních. Nelze totiž omezit strany v možnostech činit podání v libovolné formě²⁴¹. Takový spis pak není omezen ani co do dalšího vývoje, neboť je možné postupně zařazovat i nové datové formáty, k jejichž vytvoření teprve dojde. Je ale každopádně z technických důvodů vhodné, aby byly pro jednotlivé operace se

²⁴¹ Omezení stran v možnosti použití datových formátů by mohlo vedle *denegationis iustitiae* působit též jako konkurenční výhoda pro výrobce některých aplikací a bylo by tak v rozporu i s principem technologické neutrality – v souvislosti s elektronickými podatelny byl tento problém řešen v článku Polčák, R. Elektronické podatelny a jejich technologická neutralita, Veřejná správa, ročník 17, číslo 25, str. 10 a násl.

spisem a pro komunikaci spisu k soudu a účastníkům řízení zvoleny univerzální základní datové formáty, do nichž budou data vložená do spisu automaticky a bezstrátově konvertována.

Oproti papírovému spisu má ten elektronický řadu zásadních výhod. Pokud využívá technologii zaručeného elektronického podpisu ke vkládání jednotlivých dokumentů²⁴², je možné například zálohovat spis v jeho autentické podobě na více úložištích zaráz. Jestliže má pak některé z úložišť technické problémy (je například vyplaveno), lze spis obnovit z alternativního úložiště, a to v jeho původní autentické formě.

Automatizované šifrování dat uložených v elektronickém spisu společně s nastavením přístupového rozhraní zajistí, že se ke spisu nedostane nikdo nepovolaný. Zatímco k otevření papírového spisu nebo dokonce k jeho fyzické manipulaci může docházet prakticky bez omezení, může být elektronický spis zabezpečen do té míry, že jakékoli jeho otevření (pro pasivní nahlížení i aktivní operace s dokumenty) podléhá bezpečnostnímu režimu a je automaticky zaznamenáno. Spis si může navíc pamatovat i všechny své předchozí stavy, tj. dojde-li z jakéhokoli důvodu například k odebrání určitého dokumentu, je možné tuto operaci později lehce dohledat a obnovit ze zálohy předchozí stav. Takové řešení například vylučuje možnost nedovolené manipulace se spisem, „ztráty“ dokumentů apod.

Šifrování spisu jako celku a jednotlivých v něm obsažených dokumentů plní vedle běžné bezpečnostní funkce i důležitou ústavněprávní roli. Skutečnost, že dešifrovací klíče zůstávají pod kontrolou pouze těch osob, které jsou ze zákona oprávněny manipulovat se spisem nebo do něj nahlížet, zajišťuje, že se k datům obsaženým ve spise nedostane nikdo jiný, a to dokonce ani osoby dohlížející na technický chod celého systému. Je-li tedy provoz systému příkladně zajišťován (ať už z technického nebo bezpečnostního hlediska) orgány výkonné moci, je soudní moc tímto způsobem technicky chráněna před případnými pokusy o subverzi.

²⁴² Dokument, který je do spisu vkládán, je opařen zaručeným elektronickým podpisem soudce nebo soudního personálu, který provedl jeho uložení do spisu. Zaručený elektronický podpis pak nejen prokazuje identitu osoby, která data do spisu vložila, ale též zajišťuje jejich integritu (při jakékoli následné změně dokumentu lze tuto díky zaručenému elektronickému podpisu odhalit).

Vedle bezpečnostních aspektů je elektronická forma spisu samozřejmě výhodná, i co se týče provádění jednotlivých spisových operací. Soudce i strany mohou především ke spisu přistupovat dálkově, čímž odpadají transakční náklady²⁴³. Žádná z uvedených osob navíc není omezena aktuálním umístěním spisu, pracovní dobou soudu nebo náklady na opisy a výpisy. Mezi transakční náklady, k jejichž úspoře dochází, můžeme v tomto případě počítat i náklady na čas. Strany i soudce tak mohou být automaticky informováni o nových dokumentech ve spisu, o doběhnutí lhůt nebo o dalších skutečnostech, na něž mají pak možnost okamžitě reagovat.

Vedle zrychlení a usnadnění řady operací se spisem je možné vytvořit k obsluze systému i další aplikace, které budou provádět některé administrativní operace zcela automatizovaně. Obzvláště efektivní pak může být v tomto směru elektronický spis například ve spojení s elektronickým doručováním²⁴⁴ – celý proces obeslání účastníků, kontroly doručení a sledování lhůt pak může proběhnout plně automaticky bez nutnosti lidského vstupu²⁴⁵.

Možnosti automatizovaného provádění administrativních soudních operací se samozřejmě výše uvedeným nevyčerpávají – specializované aplikace tak mohou například počítat soudní poplatky a hlídat jejich úhradu, koordinovat nařízená jednání, doplňovat do spisu informace z rejstříků nebo jiných spisů, poučovat či aktivně vést účastníky řízení apod. Zvláštní kapitolou jsou i asistenční aplikace, jejichž prostřednictvím lze na spis navázat plně texty normativních právních aktů, judikatury nebo doktrinálních publikací. Na jednotlivé aplikace justičního systému pak je možné přes univerzální a veřejně dokumentovaná rozhraní napojit i další uživatelské informační systémy nezávislých dodavatelů podobně, jako to v současné

²⁴³ Na straně soudu odpadá například problém přenašení spisu mezi kanceláři, na straně účastníků pak zmizí, mezi některými advokátními kanceláři oblíbené, cestovatelství za spisem.

²⁴⁴ U nás má být elektronické doručování upraveno zákonem o elektronických úkonech a autorizované konverzi dokumentů – ten i přes některé nedostatky a mezery prošel PSP i Senátem a má nabýt účinnosti 1. 7. 2009.

²⁴⁵ Je-li například vydáno rozhodnutí, systém je automaticky odešle účastníkům do jejich elektronických schránek a pořídí o tom záznam. Po zákonném doručení pak systém automaticky zaznamená právní moc a případně o tom i uvědomí účastníky.

době například funguje u našeho insolvenčního rejstříku²⁴⁶. V důsledku pak může dojít ke kompletní informovanosti stran i soudu o aktuálním stavu řízení v reálném čase a, což je třeba obzvláště zdůraznit, k plné, okamžité, koncentrované a jednoduché kontrole soudce nad celým řízením.

7.4 KRITICKÉ MOMENTY ELEKTRONIZACE

Je třeba předně zdůraznit, že dostupnost adekvátních technologií nepředstavuje v současné době kritický element při budování systému elektronické justice. Aktuální stav vývoje informačních technologií tedy umožňuje plnou a nekompromisní elektronizaci justičních agend. Důkazem tohoto tvrzení mohou být již existující systémy elektronické justice, které nejenže plní veškeré požadované funkce, ale v mnoha směrech jdou dokonce za hranice naší kontinentálně-evropské právní představitosti. Nejdále je v tomto směru zřejmě vývoj singapurského soudnictví, kde je dlouhodobě fungující systém totální elektronické justice úspěšně vybaven funkcemi, jako jsou elektronické soudní jednání formou videokonference nebo jednání prostřednictvím videopřenosu z mobilního telefonu třetí generace²⁴⁷.

Kritickým momentem virtualizace administrativních procesů v justici²⁴⁸ tedy není sama technologie, ale spíše důsledky zásadní změny ve formě procesu na jeho vnímání účastníky. Jako nejproblématictější se tato změna jeví v otázce zabezpečení justice před vnějším nebo vnitřním narušením informačních toků. Zatímco současné zabezpečení je garantováno přede-

²⁴⁶ Především banky využívají možnost přistupovat k rejstříku prostřednictvím vlastních aplikací a automaticky přebírají informace do svých interních systémů. Podobně mohou fungovat ve vztahu k elektronickému spisu vnitřní kancelářské systémy advokátních kanceláří, notářů, exekutorů apod.

²⁴⁷ Informační materiály k systému včetně uživatelských návodů lze nalézt na adrese www.esf.com.sg.

²⁴⁸ Pojem virtualizace v tomto případě chápeme nikoli v jeho populární formě, ale v jeho pravém aristotelovském významu, tj., stručně řečeno, jako řešení problému přesunutím jeho těžiště - viz Lévy, P. *Becoming Virtual – Reality in the Digital Age*, New York, Plenum Trade, 2002, str. 6 a násl.

vším fyzickými parametry soudních budov, je ve stavu elektronické justice třeba vnímat zabezpečení mnohem více jako záležitost každého jednotlivce²⁴⁹. Nelze navíc spoléhat na stávající formy zabezpečení, ale je třeba se orientovat na jiné typy bezpečnostních prostředků. Zatímco si tedy dnes povolane osoby nedovolí ponechat bez dozoru klíče od trezoru, bude třeba v budoucnosti stejně bedlivě střežit například přístupová hesla k šifrovaným klíčům (ta se dnes dají často najít nalepená na žlutých lístečcích vedle počítačových monitorů – je to přitom z hlediska bezpečnosti stejný prohřešek, jako nechávat klíče od trezoru ležet přímo na něm).

S výše uvedeným samozřejmě souvisí i aspekt vzdělávání soudců a soudního personálu. Kritickou je především suma poznatků, které budou muset pracovníci v justici obsáhnout, aby byli schopní systém dobře využít (tj. nejen aby jej byli schopní základním způsobem používat, ale aby jeho užívání přinášelo kýžený pozitivní efekt). S tím samozřejmě souvisí i změna některých návyků a stereotypů, typicky při volném hodnocení důkazů předložených v elektronické formě nebo digitalizovaných do elektronického spisu. I zde je třeba především důkladného vzdělání soudců a soudního personálu v technických aspektech tvorby a používání elektronických dokumentů tak, aby byli adekvátně schopní hodnotit jejich *ad hoc* autenticitu a průkaznost²⁵⁰.

Jak je vidět, mají kritické momenty elektronizace spíše obecný sociálně-psychologický charakter. Z toho mimo jiné vyplývá, že je nelze řešit technicky a primárně ani legislativně. Zkušenosti ze zahraničí a koneckonců i naše zkušenosti se zaváděním partikulárních systémů elektronické justice přitom jednoznačně ukazují, že jedinou možností řešení je zde kvalitní vzájemná komunikace mezi soudy, orgánem technicky a legislativně zajišťujícím elektronizaci, politickou reprezentací a odbornou veřejností²⁵¹.

²⁴⁹ K problému srov. výklad k bezpečnosti informačních systémů veřejné správy in Mates, P., Smejkal, V. E-government v českém právu, Praha, Linde, 2006, str. 64 a násled.

²⁵⁰ Zde je třeba doplnit, že elektronické dokumenty jsou co do prokazování autenticity mnohem výhodnější než ty papírové – namísto znaleckého zkoumání papíru postačí ve většině případů ke zjištění autenticity jen automatická početní operace provedená speciálním softwarem.

²⁵¹ Kvalitně zachycených výstupů z takové komunikace není mnoho. Světlou výjimkou jsou například průběžné zprávy ze zavádění systému elektronické justice v Kalifornii – dokumenty k druhé generaci systému lze nalézt na adrese www.xmllegal.org/California2GEFS/

Pokud se tuto komunikaci podaří kvalitně založit, dochází pak dokonce k multiplikačnímu efektu, kdy účastníci dialogu nejen aktivně přispívají k vývoji systému, ale dokonce se k této aktivitě vzájemně motivují (například tak, že soudci vznášejí požadavky na nové aplikace a rozšiřování funkcionalit systému).

7.5 OBECNÉ OTÁZKY ELEKTRONIZACE

Přestože můžeme v mnoha oblastech čerpat ze zahraničních zkušeností, existuje řada aspektů elektronizace procesů autoritativní aplikace práva, jejichž diskuse a následné řešení musí nutně proběhnout výlučně v kontextu tuzemské právní kultury. Níže naznačené problémy se přitom zde nesnažíme řešit, ale předkládáme je pouze jako náměty k další odborné diskusi.

Jako první vybíráme problém organizace systému elektronické justice při jeho vytváření a následném nasazení. V tomto směru je především třeba odpovědět na otázku, kdo má navrhovat základní architekturu systému, kdo má systém vytvořit a kdo jej pak má provozovat a zajišťovat jeho bezpečnost. V zemích s centralizovanou samosprávou soudnictví (ať už pod vládou soudních rad nebo nejvyšších soudů) je tvorba a následná správa systému samozřejmě svěřena vrcholnému samosprávnému orgánu. V našem případě nelze tuto otázku vyřešit pouhým konstatováním, že elektronizace má organizační charakter a tudíž spadá pod správu soudnictví. Zčásti lze sice tomuto argumentu přisvědčit, ale proces elektronizace má i řadu materiálních aspektů (některé naznačené výše) a mimo jiné vyžaduje i provedení řady legislativních opatření. Nelze tedy dle našeho názoru opomenout při tvorbě systému zásadní význam soudů ani legitimované zákonodárné moci.

Dále je třeba řešit otázku, jaké úrovně plánování architektury systému, jeho tvorby a následného provozování mají být prováděny přímo státem a jaké se naopak hodí zadat komerčnímu sektoru. Zde máme důvod se domnívat, že veřejná zakázka na téma „vymyslete a vyrobte systém e-justice“ je v naší právní kultuře předem odsouzena k neúspěchu. Vedle složitosti a citlivosti celého procesu elektronizace vidíme důvod k takovému konstatování především ve výše naznačené nutnosti vzájemně komunikovat

a koordinovat aktivity justice, její správy a zákonodárné moci. Nejde přitom jen o zjišťování a zohledňování požadavků budoucích uživatelů (v tomto směru by případný dodavatel zcela jistě svoji roli zvládl), ale o koordinaci a aktivní vedení celého reformního procesu včetně organizačních a legislativních změn. Těžko si přitom lze představit takového podnikatele, který by byl něčeho podobného schopen²⁵² (a pokud by byl, není to dle našeho názoru rozhodně vhodný kandidát na architekta tak důležitého a citlivého systému).

Přestože lze, jak bylo naznačeno výše, od sebe oddělit technické fungování systému elektronické justice a jeho datovou základnu, představují jeho provoz a údržba rovněž citlivou kompetenční otázkou. Podobně je tomu i se zabezpečením, které bude třeba řešit nikoli jen pasivními prostředky, ale i jako monitoring a ochranu systému operátory v reálném čase. Tato otázka je o to problematičtější, že především ochrana tak rozsáhlého systému, navíc atraktivního pro útočníky²⁵³, představuje kvalitativně nový typ činnosti a v případě jejího zajištění ze strany ministerstva nebo justice bude jistě vyžadovat i politicky citlivé vytvoření nových pracovních míst.

S organizační strukturou systému elektronické justice souvisí i problém stanovení harmonogramu a míra zavádění metod elektronické justice do jednotlivých typů soudních řízení. Možností řešení, které se nabízejí, je celá řada, od postupného zavádění elektronického spisu a obslužných agend do jednotlivých podtypů řízení (případně ještě s překlenovacím obdobím stínového provozu²⁵⁴) až po metodu velkého třesku, kdy k určitému datu

²⁵² Zakázku jako takovou samozřejmě není problém zadat – nelze však poté očekávat a ani jako podmínku plnění stanovit konečnou spokojenost justice se systémem nebo prosazení legislativních změn. V konečném důsledku tedy může dojít k utracení peněz, jehož výsledkem bude systém, který justice oprávněně odmítne používat nebo který bude prakticky nepoužitelný kvůli chybějící legislativě.

²⁵³ Justiční systémy nepatří mezi útočníky k nejatraktivnějším, jejich atraktivita však poroste s jejich významem – k problému srov. např. Chandler, Jennifer A. Security in Cyberspace: Combatting Distributed Denial of Service Attacks, University of Ottawa Law & Technology Journal, číslo 1, str. 231 a násl.

²⁵⁴ Jedná se o nasazení elektronického systému současně s papírovou formou řízení, přičemž formálně je řízení stále vedeno nad papírovým spisem a elektronická forma po určitou dobu funguje jen jako neoficiální doplněk. Tento model byl úspěšně zvolen například u kalifornských soudů.

přechází na elektronickou formu celý typ řízení (například soudní řízení správní) nebo dokonce celá justice²⁵⁵.

V souvislosti s problémem harmonogramu je třeba též zdůraznit, že u nás nevycházíme z bodu nula, ale že řešení elektronické justice je třeba vybudovat v souvislosti s již nasazenými nebo nasazovanými systémy. V naší justici je v současné době funkční řada asistenčních aplikací, které izolovaně zajišťují některé administrativní činnosti – jedná se především o elektronické rejstříky, aplikace spisové služby, vnitřní evidenční systém judikatury nebo jednoduché portály pro kontakt s účastníky řízení nebo s veřejností (např. elektronické podatelny nebo aplikace Infosoud). Zásadní problém těchto aplikací a jejich použitelnosti pro systém elektronické justice spočívá v tom, že byly vyvíjeny nekoordinovaně, často doslova živelně a nejsou tedy postaveny na jednotící architektuře. To však z technického hlediska povětšinou nebrání tomu, aby byly (za cenu vytvoření nebo adaptace jejich rozhraní) zakomponovány do celkové architektury komplexního systému elektronické justice postaveného na elektronickém spisu – je však každopádně třeba rozhodnout, které z těchto aplikací a případně do jaké míry budou v komplexním systému zachovány.

7.6 VYBRANÉ KONKRÉTNÍ OTÁZKY ELEKTRONIZACE

Systém elektronické justice může bez větších obtíží produkovat rozhodnutí, jejichž autentická forma bude elektronická a která budou opatřena příslušnými bezpečnostními prvky, typicky zaručeným elektronickým podpisem soudce (členů senátu). Jsou-li taková rozhodnutí doručována adresátům elektronicky, není třeba hovořit o problému konverze. Nedisponují-li však účastníci řízení elektronickou schránkou způsobilou k zákonnému doručování²⁵⁶, je třeba rozhodnutí konvertovat do písemné podoby a následně doručit standardní cestou. K tomu lze samozřejmě využít institut

²⁵⁵ Tento typ zavedení elektronického spisu byl úspěšně aplikován v Singapuru – zde je však třeba vzít v potaz specifické charakteristiky zdejší společnosti a právního systému.

²⁵⁶ Zde je třeba zdůraznit, že e-mail není možné pro potřeby zákonného doručení využít, neboť nemožňuje prokázat doručení zprávy jejimu adresátovi.

opisu, přičemž je rozhodnutí prostě vytištěno a oprávněná osoba jej fyzicky podepíše. Takto konvertované rozhodnutí je pak odesláno adresátovi klasičnou poštou.

Aktuální trendy v poštovní službě však směřují k zavádění metod tzv. hybridní pošty, kdy je příslušný dokument zaslán poště elektronicky, ta jej přesune na provozovnu co nejbližší adresátovi, konvertuje jej do písemné podoby a poté s minimálními náklady fyzicky doručí (obdoba telegramu). Ke zvážení přitom zůstává, zda tuto konverzi, jejíž přesnost je pro adresáta i pro celý proces zásadně důležitá, opravdu svěřit subjektu mimo systém justice.

Přestože Česká republika není stížena kvantitativním nedostatkem internetové konektivity a počítačová gramotnost utěšeně stoupá²⁵⁷, je třeba řešit otázku, jakým způsobem vést řízení v případech, kdy účastníci nedisponují příslušnými technologiemi. Nejde přitom jen o výše zmíněný problém konverze a následného doručování rozhodnutí primárně vyhotoveného v elektronické formě ale především o otázku, kdo má nést náklady konverze papírových dokumentů podaných stranami resp. kdo má tuto konverzi provádět. Výsledné řešení by přitom nemělo nikoho bezdůvodně administrativně zatěžovat. Lze si například představit, že bude-li stranou řízení správní orgán, bude povinnost konvertovat papírové dokumenty (například správní spis) do elektronické formy přenesena na něj. Na druhou stranu by zřejmě nebylo vhodné vyžadovat konverzi dokumentů u všech osob zúčastněných na řízení (u nezastoupených stran, u osob pouze majících u sebe dokumenty apod.) – v takových případech může provést konverzi soud a originály dokumentů účastníkům obratem vrátit. Nastavení procesů konverze dokumentů k jejich zařazení do elektronického spisu je však i přes svou zřejmou banalitu jednou z otázek, kterou je každopádně třeba řešit konsensem mezi justicí, její správou, politickou reprezentací a odbornou veřejností (zde zřejmě především advokáty).

Další problém, opět s ústavněprávním dosahem, představuje nasazení automatizovaných mechanismů v rozhodovacím nebo quasirozhodovacím procesu. Tento problém už byl široce diskutován v souvislosti s elektronic-

²⁵⁷ Srov. statistiky informační společnosti publikované Českým statistickým úřadem, např. zápravy č. 9702-06, 9701-07 nebo 9703-07 dostupné na www.czso.cz.

kým platebním rozkazem, kde bylo původním záměrem architektů systému zcela vyloučit lidský element v rozkazním řízení (tj. systém přijme návrh, posoudí formální náležitosti a vydá příslušné rozhodnutí – zde platební rozkaz). Obdobně by mohl systém v případě elektronizovaného řízení rozhodovat například v případě nezaplacení soudního poplatku, marného uplynutí uložené lhůty apod. Odvážnou představu automatizace rozhodovacího procesu však v tomto případě nelze odbýt paušálním požadavkem na to, aby v každém případě rozhodoval člověk. Má-li určité procesní rozhodování čistě formálně sylogistický charakter a není-li ani dán prostor pro uvážení, je určitě vhodné se citlivou otázkou nahrazení člověka strojem v tomto případě přinejmenším zabývat²⁵⁸.

Vedle několika kritických momentů souvisejících se změnou formy spisu a virtualizací řízení (viz výše) odstraňuje elektronizace mnoho fyzických omezení, kvůli kterým v minulosti vznikla řada procesních institutů. Vydeme-li ze skutečnosti, že elektronický spis může být teoreticky zpřístupněn neomezenému počtu osob zaráz a přístup lze libovolně nastavit až do úrovně jednotlivých záznamů, je nasnadě diskuse například o smyslu zachování tzv. pomocných (sběrných) spisů. Podobně, uvážíme-li, že elektronický spis může obsahovat data v libovolné formě, můžeme do něj zařadit mimo jiné i plně audiovizuální záznamy z jednání a vyloučit tak například dnešní institut protokolu.

Podobně mohou být ke spisu prakticky bez omezení ukládány i další informace, které netvoří přímo součást spisu, ale souvisejí s řízením. Ty mohou být zpřístupněny například jen členům senátu (v úvahu připadá i online chat nad případem), soudnímu personálu případně i stranám nebo veřejnosti. Může se jednat o pokyny podřízeným, poznámky soudce v libovolné formě (včetně audiovizuálních), citace z podkladů nebo dokonce o dvoustrannou komunikaci soudu se stranami mimo jednání²⁵⁹. Komplexní

²⁵⁸ Na téma automatizovaného rozhodování byla publikována řada prací především v 80. letech minulého století. Nyní se zájem o automatizaci rozhodovacích procesů vrací, nikoli už však s cílem nahradit uvážení člověka ale maximálně mu asistovat – přehled aktuálních trendů a justičních realizací přináší publikace Oskamp, A. Lodder, A. R. Apistola, M (eds.) *IT Support of the Judiciary*. Den Haag: Asser Press, 2004.

²⁵⁹ Zahrnutí této komunikace výrazně zvýší transparentnost rozhodovacího procesu a posílí zásadu rovnosti stran. Obě strany tedy mají přehled o tom, na co se ta druhá soudce mimo jednání ptala a jak jí soudce odpověděl. Tato technologie funguje v současné například

dokumentace k případu vedená „nad spisem“ by pak mohla v případě potřeby posloužit nejen při řízení samotném, ale i v případě předání případu jinému soudci, zahájení kárného řízení apod. Přitom nehrozí, že by se vlivem opomenutí dostaly případné důvěrné poznámky nebo instrukce do nepovolanych rukou, neboť by přístup k nim byl zabezpečen na stejné úrovni jako přístup k samotnému spisu²⁶⁰. Otázkou však zůstává, jaké typy dat nad spisem by měl systém podporovat a zda na tuto funkcionalitu navázat i procesními povinnostmi, tj. zda například uložit soudci, aby dával pokyny podřízeným nebo aby komunikoval se stranami jen prostřednictvím systému.

Tradiční otázku konečně představuje i otevřenost justice veřejnosti²⁶¹. Se zavedením systému elektronické justice bude z technického hlediska představovat naprosto triviální funkcionalitu například zveřejňování plných textů rozhodnutí, statistických údajů o rozhodovací činnosti (i k osobám jednotlivých soudců) nebo případně i audiovizuálních záznamů z veřejných jednání. Není přitom, jak by se na první pohled mohlo zdát, možné konstatovat přímou úměru mezi mírou transparentnosti a mírou legitimacy soudnictví, a proto v této otázce očekáváme ještě bouřlivou diskusi²⁶².

u rozhodčího tribunálu ADR .eu fungujícího při RS OHKAK, kde je pro tzv. doménová řízení používán i systém kompletního elektronického spisu.

²⁶⁰ Nemohlo by tak dojít k situaci, že je například ve spise zapomenut žlutý nalepovací lísteček s telefonním číslem na zapisovatelku nebo tužkou psaná poznámka „to je vůl“ u protokolu o výslechu svědka.

²⁶¹ Zkoumáním míry transparentnosti v jednotlivých justičních systémech se zabývá Lasser, M. *Anticipating Three Models of Judicial Control, Debate and Legitimacy: The European Court of Justice, the Cour de cassation and the United States Supreme Court*, Jean Monet Working Paper 1/03, NYU School of Law, New York, 2003. Později byly teze této práce zahrnuty do monografie Lasser, M. *Judicial Deliberations: A Comparative Analysis of Transparency and Legitimacy*. Oxford: Oxford University Press, 2004.

²⁶² K tématu lze doporučit obecnou diskusi k otázkám publikace judikatury a transparentnosti justice, která je plynule vedena na serveru *Jiné Právo* – viz např. příspěvky Kühn, Z. *Jak zlepšit české právní informační systémy?*, 23. 2. 2008, Polčák, R. *Tučňáci a webkamery – pár poznámek k legitimní a nelegitimní transparentnosti soudnictví*, 20. 5. 2008 nebo dřívější příspěvek, nyní i otištěný: Molek, P. *Přežije nás anonymizace?*, *Jiné právo offline*, Praha, Auditorium, str. 227 a násl

7.7 ZÁVĚREČNÁ POZNÁMKA K EVROPSKÉMU ROZMĚRU ELEKTRONIZACE JUSTICE

Výše jsme stručně diskutovali některé základní otázky zavádění informačních a komunikačních technologií do procesů autoritativní aplikace práva a rovněž jsme se pokusili naznačit obecné a specifické problémy, jejichž postupné řešení považujeme za nevyhnutné. Závěrem namísto shrnutí ještě krátce připojíme poznámku k nadnárodnímu rozměru jednotlivých projektů elektronizace, které v současné době probíhají v Evropě. Řada států včetně České republiky totiž v nedávné minulosti zahájila nebo nyní připravuje ambiciózní projekty komplexní elektronizace soudního řízení a dalších procesů autoritativní aplikace práva. Zatímco v minulosti příliš nevadilo, že se jednotlivé partikulární justiční nebo správní elektronické systémy vyvíjely nekoordinovaně (a to ve vnitrostátním i mezinárodním měřítku), nyní začíná být jasné, že vývoj komplexních národních systémů elektronické justice s sebou nese obrovský potenciál rozvoje mezinárodní justiční spolupráce.

Ať už je to volný pohyb soudních rozhodnutí, dožadování procesních úkonů nebo třeba oficiální přístup do rejstříků, je zřejmé, že elektronizace a vzájemná kompatibilita jednotlivých národních řešení jsou nevyhnutným předpokladem dalšího budování evropského justičního prostoru. Není přitom nutné stanovit společné evropské standardy pro kdekou technickou finesu jednotlivých aplikací, ale je každopádně vhodné už od počátku budovat národní systémy tak, aby byly na nejvyšší úrovni vzájemně interoperabilní a aby byly schopné napojení na evropské agentury typu Eurojust. Komise ani Rada EU však v tomto směru žádnou aktivitu až donedávna nevyvíjely. Nynější iniciativa „eJustice“ Rady představená nedávno na bukurešťské konferenci EJTN pak sice vypadá ambiciózně, ale v mnoha směrech je postavená na vzdušných zámcích²⁶³ a koordinaci vývoje národních systémů dokonce vůbec nepovažuje za klíčovou prioritu. Tato situace

²⁶³ Projekt například předpokládá vznik systému pro automatizované překlady - takový systém však nejenže není k dispozici, ale jeho dostupnost již byla předpovídána mnohokrát a v dohledné době stále spíše do oblastí vědeckých fantazií.

samořejmě není pro evropský justiční prostor fatální, ale bude znamenat (tak typické) prodlevy, komplikace a především dodatečné náklady na adaptaci a koordinaci národních aktivit *ex post*. Zbývá tedy zřejmě jen doufat, že chybějící vzájemná komunikace států v rámci Rady bude v otázkách elektronizace co nejdříve doplněna alespoň mezinárodní výměnou informací na rezortní úrovni.

8 STRUKTURA INFORMAČNÍ SPOLEČNOSTI – DEFINIČNÍ NORMY

8.1 POJEM DEFINIČNÍCH NOREM

Mezi světovými válkami, v době, kdy se snad už naposled považovalo právo za exaktní vědní disciplínu²⁶⁴, vedli mezi sebou Engliš a Kelsen mimo jiné i debatu nad problémem účelů v právu. Stručně řečeno byla tato debata sporem o to, zda účel jako kategorie spadá v Humově systematice do světa bytí či mětí. Jednou z implikací Humovy teze je totiž postulát, že netautologické pravidlo (norma) nemůže být odvozeno ze skutečnosti²⁶⁵. Přírodní zákony jsou samozřejmě pravidly svého druhu a k jejich existenci se dobíráme pozorováním, jsou však v tomto směru právě pravidly tautologickými. Přírodní pravidlo (přírodní zákon) totiž zdůvodňuje výsledek kauzálního děje a zároveň je jím samo odůvodněno.

Byl-li by účel shledán v těchto intencích kategorií empirickou, patřil by do světa bytí a ryzí právo by s ním nijak nesouviselo. V opačném případě, tj. pokud by bylo lze argumentovat povahu účelu jako kategorii normativní, do práva by logicky patřil.

Výsledek tohoto sporu byl, rozumně vzato, nerozhodný. Kelsen tak zůstal stát na svém, tj. že účelem se právní věda zabývat nemá, a naopak Engliš, přesvědčen o váze svých argumentů, trval na existenci účelu a jeho významu v právu. Jádrem argumentace obou byla přitom odpověď na otázku, zda účel je pouze obrácenou kauzalitou, jak tvrdil Kelsen, nebo zda je konstruován na základě chtění, jak naopak tvrdil Engliš. Kelsen v tomto směru argumentoval, že účel je možné vidět jako obrácenou kauzalitu a k vysvětlení použil příklad s bitím srdce. Vyšel přitom z předpokladu, že účelem bití srdce je oběh krve. Na otázku, proč obíhá krev, můžeme pak

²⁶⁴ Srov. historizující komentář in Bix, B. Legal positivism (Working Paper). Minnesota: University of Minnesota Law School, 2000, str. 9 a násl.

²⁶⁵ K problému viz např. Holländer, P. (2006) Filosofie práva. Dobrá voda: Aleš Čeněk, str. 30 a násl.

kauzálně odpovědět, že je to z důvodu toho, že bije srdce. Tím se Kelsen pokoušel dokázat, že účel je tedy pouze otočením kauzality a jako takový má tedy povahu tautologického pravidla. Engliš v odpovědi na tento názor použil stejný příklad,²⁶⁶ přičemž však odmítl tezi, že účelem bití srdce je pouze prostý oběh krve, ale skutečnost, že tento oběh je chtěn. Prokázat chtění jako základní moment účelu zde tedy znamenalo prokázat jeho normativní povahu.

U přírodních zákonů, tj. u kauzálních pravidel, je otázka, zda bylo jejich základem chtění, otázkou spíše akademickou či přesněji teologickou. Nás však v tomto případě nebudou ani tak zajímat přírodní zákony fyzického prostředí ale základní kauzální pravidla vymezující prostředí informační sítě. Pokusíme se je tedy pro naše potřeby definovat, systematicky zařadit a odhalit alespoň něco z jejich podstaty tak důležité pro existenci a rozvoj nejen samotné komunikační infrastruktury ale, a to nás bude zajímat především, její společenské organizace.

Základní argument naznačené debaty o místo účelu ve světě měti můžeme použít i k zodpovězení otázky, zda pravidla definující informační síť, jsou tautologickými pravidly světa bytí nebo normami. Je sice pravda, že pozorovatel (uživatel) může jejich existenci dovozovat z empirické zkušenosti, tj. na základě poznání funguje/nefunguje. Toto však není jediná a ani ideální možnost, neboť se můžeme o jejich existenci mnohem pohodlněji než metodou pokus/omyl dozvědět i prostudováním manuálů či technických specifikací²⁶⁷. Navíc, a to je obzvláště důležité, je nesporné, že vznik takových pravidel byl otázkou něčího chtění.

Můžeme tedy konstatovat, že prokazatelný aspekt chtění společně s neoddiskutovatelnou existencí normotvorné autority nás vedou k poznání, že v případě technických pravidel vymezujících prostředí informačních sítí můžeme hovořit o normách *sui generis* a o jejich původcích jako o normotvorných autoritách. Tyto normy a jejich autority pak můžeme srovnávat s ostatními typy norem, jako jsou normy právní, sociální, etické nebo Boží.

²⁶⁶ Srov. Engliš, K. Kritika normativní teorie, in Brněnská škola právní teorie. Praha: Karolinum, 2003, str. 203 a násl.

²⁶⁷ Nabízí se zde dokonce i jakási paralela s Božími zákony vyjevenými ve svatých knihách. I Bible či Korán tak v tomto směru a s trochou nadsázky mohou být chápány jako uživatelské manuály – nikoli vždy však máme dostatečné schopnosti k jejich čtení a porozumění.

Vzhledem k tomu, že jsou tyto normy vytvářeny a implementovány subjekty s mocí definovat prostředí informační sítě, budeme jim nadále říkat normy definiční²⁶⁸ a jejich původce pak budeme, opět s akademickou licencí k nepřesnostem, nazývat definičními autoritami²⁶⁹.

Definiční normy je třeba, jak již bylo naznačeno, považovat za normy *sui genesis*. Důvodem jejich vzniku je, podobně jako u ostatních typů norem, chtění specifické definiční autority. Jejich charakter však způsobuje, že spíše než normativita je pro většinu jejich adresátů, tj. pro běžné uživatele, důsledkem jejich existence kauzalita. Rozhodnutí, zda se budou definičními normami řídit, tudíž přijímají pouze ti, jejichž technická zdatnost jim to umožňuje, tj. hackeři²⁷⁰. Definiční norma tak má ve standardním případě pro svého tvůrce charakter chtěného, pro adresáta však již má, podobně jako přírodní zákon, povahu nevyhnutelného nebo, chceme-li, nutného. Tím se definiční normy zásadně odlišují od všech ostatních, snad kromě norem Božích – v ostatních případech, tj. u norem právních, sociálních i etických, se ke kategorii normy váže atribut povinnosti. U norem definičních je, z hlediska teorie paradoxně, norma následována prostou kauzální nutností²⁷¹.

8.2 LESSIGŮV KÓD

Složitou otázkou s relativně jednoduchou odpovědí je otázka po tom, co jsou vlastně definiční normy zač a jak vypadají. Odpověď na ni nalézá

²⁶⁸ Srov. Polčák, R. Škop, M., Macek, J. Normativní systémy v kyberprostoru (úvod do studia). Brno: Masarykova univerzita v Brně, 2005, str. 81 a násl.

²⁶⁹ V tomto případě se však nejedná o naplnění Weibnergerovy resp. MacCormickovy představy instituce jako podmínky a zároveň záruky platnosti právních norem – definiční autority totiž vytvářejí systém vlastních kauzálních pravidel, který je až na výjimky popsané níže na systému právních pravidel nezávislý. K MacCormickovu pojetí instituce viz MacCormick, N. *Institutions of Law*. New York: Oxford University Press, 2008, str. 21 a násl.

²⁷⁰ Srov. Lessig, L. *Constitution and Code*. *Cumberland Law Review*, ročník 27, číslo 1, str. 3 a násl.

²⁷¹ Tato skutečnost činí definiční normu stoprocentně efektivním pravidlem – k tomu srov. např. Post, D. *Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace*. 1996, publ. on-line na adrese http://www.cli.org/DPost/X0023_ANARCHY.html.

americký konstitucionalista Lawrence Lessig ve své knize *Code and Other Laws of Cyberspace*, nyní čerstvě doplněné a vydané pod označením *Code 2.0* a označuje tyto normy prostým pojmem kód (angl. *code*). Lessig postavil svoji teorii na třech základních překážkách či regulativech lidského chování. Hovoří původně o právu, normách (zde ve smyslu sociálním) a konečně o kódu. Tuto základní klasifikaci pak Lessig později dále rozšířil, když pod pojem „normy“ podřadil i etické (individuální) regulativy a samoregulační, resp. samoorganizační mechanismy a celou klasifikaci ještě obohatil o čtvrtý faktor, tj. o pravidla ekonomiky²⁷².

Kód je u Lessiga předpisem, na jehož základě funguje informační infrastruktura – kód tedy kauzálně determinuje chování jednotlivých složek dohromady tvořících informační síť. Bylo by však až příliš zužující hovořit o kódu jen jako o počítačovém programu – ten je samozřejmě jako sled instrukcí také typem kódu. Pod pojem kód je však kromě programů možné podřadit i jiné formy kauzálních (technických) pravidel jakými jsou například omezení (kvóty), parametry prostředí, formáty dat, přenosové protokoly apod.

Ačkoli Lessig staví kód z hlediska klasifikace na stejnou úroveň s ostatními regulačními faktory, přiznává mu specifické postavení díky jeho značné efektivitě a přirovnává jej k přírodním zákonům. Přichází rovněž s přirovnáním k situacím, kdy využíváme přírodních zákonů k prosazení vlastních představ (vlastního chtění). Proto, jak říká, „můžu využít kódu reálného světa a zamknout si kolo, aby mi ho někdo neukradl.“²⁷³ Kolo, resp. vlastnické právo k němu je sice chráněno právem, zámek má však v porovnání s právní normou mnohem větší potenciál k tomu příslušné právo efektivně ochránit.

Využití definiční normy či kódu k regulaci chování je tedy možné srovnat s využitím přírodního zákona. Kód však, na rozdíl od přírodního zákona, není kauzálním pravidlem světa bytí, ale normou. Existuje zde tedy transparentní a v porovnání s Bohem i relativně dobře dosažitelná autorita,

²⁷² Viz Lessig, L. *Code V.2*. New York: Basic Books, 2006, str. 234. Publikace je též k dispozici on-line na adrese <http://pdf.codev2.cc/Lessig-Codev2.pdf> - komentář k této klasifikaci viz např. Greenleaf, G. *An Endnote on Regulating Cyberspace: Architecture vs. Law?* University of New South Wales Law Review, ročník 21, číslo 2, str. 603 a násl.

²⁷³ Viz Lessig, L. *Code V.2*. New York: Basic Books, 2006, str. 171.

kteřá kód vlastním chtěním vytváří a implementuje. Na rozdíl od přírodních zákonů tedy můžeme kód nejen využít, ale můžeme jím chování i přímo regulovat tak, aby odpovídalo chtění příslušné autority. Lessigův příklad využití „kódu reálného světa“ tak lze posunout ještě o úroveň výš, kde však již paralela s fyzickým světem není. Lze tak hovořit o kódu, který sám o sobě vynucuje, resp. určuje určité chování. Namísto toho, abychom využívali přírodních zákonů, máme tak v informačních sítích možnost je k obrazu našeho chtění přímo tvořit či přetvářet.

Kód či definiční normy informačních sítí vykazují kromě jiného charakteru i další odlišnost oproti přírodním zákonům. Vyskytují se totiž v nespočetných vrstvách, které na sobě vzájemně existenčně i funkčně závisí. Můžeme tedy vidět různé vrstvy základní fyzické informační a komunikační infrastruktury, operačních systémů, protokolů, aplikací, datových formátů apod. Definiční normy tak vytvářejí telekomunikační operátoři, producenti kancelářského software, ale i například tvůrci či provozovatelé on-line her nebo i každý, kdo si otevře vlastní blog nebo kdo má e-mailovou schránku²⁷⁴.

8.3 REGULACE PROSTŘEDNICTVÍM DEFINIČNÍCH NOREM

Normy nebo obecně pravidla všech normativních systémů působí na své adresáty především prostřednictvím sankcí. Nemusí to být samozřejmě v každém případě sankce pocházející z příslušného normativního systému - tak například k dodržování právních norem může jedince motivovat nejen právní ale též například společenský, etický či ekonomický motiv. Adresáti těchto pravidel mají však prakticky vždy²⁷⁵ na výběr, zda se jimi budou

²⁷⁴ Definiční normou vytvořenou uživatelem e-mailové schránky je například filtr, který automaticky provádí nastavenou operaci s doručenou poštou určité kvality. Je tak možné například nastavit automatické mazání e-mailů zaslaných z adresy neodbytného nápadníka.

²⁷⁵ Výjimku v tomto směru tvoří jen systém náboženských norem či lépe Božích zákonů. Pro velké množství jeho specifických rysů se jím však dále nebudeme zabývat.

řídít či nikoli – pokud pak odmítnou vyslyšet v příslušné životní situaci imperativ vyplývající z platného pravidla, legitimují tím aplikaci sankce.

Mezi základní znaky právního normativního systému patří též princip, podle kterého nenastupuje sankce automaticky, ale na základě předem stanovené procedury. Sankční postih za užití státního aparátu je tedy nejen otázkou porušení příslušných právních pravidel, ale též ochoty a schopnosti státu zakročit. Aktivita státu je přitom vyjádřena nejen konečným uplatněním postihu, ale zpravidla ještě jemu předcházejícím rozhodnutím. Můžeme se sice setkat i s přísně sylogistickým pojmáním procesů autoritativní aplikace práva, ani v takovém případě však nelze popřít existenci procedury, která nejprve konstatuje právní odpovědnost a následně stanoví odpovídající sankci.

Porovnáváme-li tedy definiční a právní normativitu, můžeme jejich mechanismus regulace rozlišit prostřednictvím následujících znaků:

- původ pravidel
- povaha regulačního (motivačního) faktoru – postih
- uplatnění postihu

Zatímco původcem právních pravidel bývá obvykle stát, je tvorba definičních norem svěřena nejrůznějším subjektům státní, polostátní, nejčastěji však soukromoprávní povahy. Legitimita ke tvorbě definičních norem se přitom neopírá o Boha, o doktrínu společenské smlouvy ani například o Grundnormu, ale o historicky založenou fakticitu. Definiční autority (viz dále) tak realizují svoji normotvornou kompetenci na základě zmocnění, které můžeme s nadsázkou označit za přirozené. Stejně přirozená je pak obvykle i změna v rozsahu a významu normotvorných kompetencí či dokonce zánik definičních autorit nebo vznik jiných.

Podstatnou roli při zakládání normotvorných kompetencí definičních autorit hrají sami uživatelé služeb informační sítě. Vzájemnou soutěží o jejich přízeň tak jednotlivé definiční autority získávají nejen kýžený ekonomický prospěch, ale (často rovněž ekonomicky motivovanou) též důležitou normotvornou legitimaci. V této souvislosti je často diskutována otázka, zda jsou uživatelé s to posoudit perspektivní význam svého jednání, a to především vzhledem k založení normotvorné kompetence příslušné

definiční autority, jejichž služeb se rozhodnou využívat. Nabízí se pak provokativní úvaha, zda jsou uživatelé služeb informační sítě vlastně vůbec způsobilí volit poskytovatele svých oblíbených služeb.

Jako příklad problematické situace s ohledem na založení normotvorné kompetence definiční autority můžeme jmenovat třeba značnou popularitu tzv. instant messengerů (např. ICQ, Skype) nebo tzv. komunitních serverů (např. LinkedIn nebo Facebook). Užíváním služeb těchto definičních autorit dávají jejich uživatelé, často nevědomky, všanc svou osobní integritu a potažmo i vlastní svobodu. Namísto přímého ekonomického prospěchu (uvedené služby jsou poskytovány zdarma) přitom příslušné definiční autority těží, a to nejen ekonomicky, právě ze skutečnosti, že jim jejich uživatelé vložili do rukou definiční normotvornou kompetenci.

Druhý rozdíl mezi právem a systémem definičních norem můžeme vidět v povaze postihu uplatňovaného při porušení normativní dispozice. Adresáti definičních norem totiž nemají možnost volit, zda se budou nebo nebudou podle těchto norem chovat. Namísto normativity tedy u definičních norem hovoříme o prosté kauzalitě, neboť naplněním jejich hypotéz dochází automaticky k realizaci dispozice. Jak bylo uvedeno výše, mají tedy tyto normy z hlediska jejich tvůrce charakter formalizovaného chtění, z hlediska adresáta mají však povahu přírodního zákona, o jehož dodržení jeho adresát nerozhoduje.

Definiční autority informačních sítí však na rozdíl od Boha (tj. definiční autority tzv. reálného světa) nesou veškeré atributy lidského chtění a jeho následné formalizace. Mohou tak být stíženy problémem nahodilosti, emocionality, ale především chybovosti. Po éře kouzelníků a šarlatánů snažících se, jak jinak než neúspěšně, ošálit přírodní zákony, tedy povstávají jedinci s ambicí uniknout definiční normativitě. Přírodní zákony informační sítě jsou však v porovnání s limity skutečné přírody nesrovnatelně snadnější výzvou. K jejich překonání postačí, pokud jsou technické schopnosti moderních kouzelníků lepší než u definičních autorit – narůstající složitost kódu přitom způsobuje, že možnosti k tomu dostat se mimo působnost definičních norem nejsou ani zdaleka nedosažitelné. Přestože dostalo pojmenování jedinců vyňatých díky jejich technickým schopnostem z působnosti definičních norem v poslední době vysoce negativní konotace, domníváme se, že je stále na místě používat pro jejich označení původního výrazu

hacker. Není přitom překvapením, že se sociální normativita klasické hackerské komunity blíží, a to včetně symboliky, sociální normativitě kouzelníků či šamanů.

Posledním z charakteristických znaků odlišujících od sebe právní a definiční normativní systém, je pak samozřejmě postup při uplatnění postihu za porušení příslušných norem. Zatímco proces autoritativní aplikace práva představuje jeden ze základních kamenů mechanismu právní regulace, jen marně bychom hledali jeho obdobu v systému definičních norem. Skutečnost, že definiční normy nedisponují sankčním aparátem ani soustavou orgánů autoritativně rozhodujících o uplatnění postihu, je samozřejmě důsledkem jejich výše popsaného kauzálního charakteru ve vztahu k jejich adresátům.

Skutečnost, že jsou však definiční normy stíženy chybovostí a je možné jejich aplikaci vyloučit, vede k zajímavému efektu zajištění těchto norem jiným normativním systémem, konkrétně právem. Namísto klasického modelu zajištění práva prostřednictvím definice kauzálních pravidel tedy dochází k situaci, kdy jsou kauzální pravidla informační sítě naopak zajišťována právem.

Na následujícím příkladu právního zajištění účinných technických prostředků ochrany autorských práv můžeme dokonce pozorovat zajímavou situaci, kdy je právní norma podpořena normou definiční. Vykonavatel autorských práv v tomto případě chrání své oprávněné zájmy za užití účinných technických prostředků (tj. definičních norem) označovaných jako DRM²⁷⁶. Sama tato technická ochrana je pak ještě chráněna právem, resp. možností postihu takového jednání, které by vedlo k jejímu odstranění. Stručně řečeno je tedy v tomto případě právo chráněno technickým prostředkem, který je sám chráněn právem. Pro ilustraci můžeme použít § 43 odst. 1 až 3 zákona č. 121/2000 Sb.:

(1) Do práva autorského neoprávněně zasahuje ten, kdo obchází účinné technické prostředky ochrany práv podle tohoto zákona.

²⁷⁶ Podrobně k pojmu DRM, jejich legitimitě a právní ochrany viz např. polemické články ve speciálním oddíle třetího čísla ročníku 2003 Berkeley Technology Law Journal, především pak Cohen, J. E. DRM an Privacy. Berkeley Technology Law Journal, roč. 18, číslo 3 respektive Sobel, L. S. DRM as Enabler of Business Models: ISPs as Digital Retailers, Berkeley Technology Law Journal, roč. 18, číslo 3. Problém DRM pak podrobně rozebírá i nová obsáhlá monografie Tarletona Gillespie – viz Gillespie, T. Wired Shut – Copyright and the Shape of Digital Culture. Cambridge: MIT Press, 2007.

(2) Do práva autorského neoprávněně zasahuje také ten, kdo vyrábí, dováží, přijímá, rozšiřuje, prodává, pronajímá, propaguje prodej nebo pronájem nebo drží k obchodnímu účelu zařízení, výrobky nebo součástky nebo poskytuje služby, které

jsou za účelem obcházení účinných technických prostředků nabízeny, propagovány nebo uváděny na trh,

mají vedle obcházení účinných technických prostředků jen omezený obchodně významný účel nebo jiné užití, nebo

jsou určeny, vyráběny, upravovány nebo prováděny především s cílem umožnit nebo usnadnit obcházení účinných technických prostředků.

(3) Účinnými technickými prostředky podle tohoto zákona se rozumí jakákoli technologie, zařízení nebo součástka, která je při své obvyklé funkci určena k tomu, aby zabraňovala nebo omezovala takové úkony ve vztahu k dílům, ke kterým autor neudělil oprávnění, jestliže užití díla může autor kontrolovat uplatněním kontroly přístupu nebo ochranného procesu jako je šifrování, kódování nebo jiná úprava díla nebo uplatněním kontrolního mechanismu rozmnožování.

Obrazně řečeno tedy v tomto případě právotvůrce nejen zakazuje činnost kouzelníkům ale též výrobu, distribuci či propagaci kouzelnických hůlek.

8.4 KÓDOVÁNÍ ZÁKLADNÍCH HODNOT

I přes to, že se můžeme, prozatím výjimečně, setkávat se situací, kdy právní pravidlo chrání definiční normu, zpravidla tomu bývá naopak. Definiční normy tedy zajišťují dodržování právních norem, to však nikoli díky sankcím ale pro svůj charakter kauzálního pravidla. S výjimkou hackerské komunity jsou tedy uživatelé služeb informační sítě nikoli jen přesvědčováni, ale přímo nuceni k dodržování těch právních pravidel, která jsou zajišťována definičními normami.

Jako příklad nám může posloužit diskusní server. Definiční normy zde, obecně vzato, chrání slušnost komunikace a předcházejí páčání civilních deliktů, přestupků i trestných činů. Často užívanou definiční normou je v tomto směru například automatický filtr zachycující vulgární výrazy – namísto povinnostního pravidla, tj. zákazu následovaného možností sankce, je v tomto případě uplatněna definiční norma, jejíž hypotézou je výskyt vulgárního výrazu a dispozicí je prosté smazání příslušného příspěvku. Filtr pochopitelně může být nastaven dle libovolného slovníku – namísto slov

„hovno“ nebo „negr“ může automaticky likvidovat třeba slova jako „svoboda“ nebo „demokracie.“

Nejen u diskusních serverů je filtrace velmi populární metodou používanou k eliminaci protiprávních aktivit uživatelů služeb informační společnosti. Velmi sofistikovanými filtry tak disponují například i populární služby umožňující uživatelům zveřejňovat multimediální obsah. Nejvýznamnější současná služba tohoto typu, americký YouTube, pro tento účel například používá referenční databázi videosekvencí chráněných autorským právem. Odpovídá-li pak uživatelská videosekvence referenčnímu vzorku uloženému v databázi, je automaticky odstraněna.

Definiční norma však může počítat i s lidským faktorem, kdy je do procesu filtrace například zapojen redaktor – ten má technickou kompetenci mazat uživatelský obsah, který se mu z nějakého důvodu jeví protiprávní nebo neslušný. V souvislosti s tím můžeme klást otázku, zda je z hlediska právních principů a ochrany základních práv přijatelnější, funguje-li příslušný filtr automaticky (a za případnou protiprávní filtraci plně odpovídá provozovatel) nebo počítá-li v reálném čase s rozhodující rolí člověka, tj. operátora, redaktora apod.²⁷⁷

V souvislosti se zajištěním právních pravidel prostřednictvím definičních norem, tj. lessigovského kódu, však vyvstává otázka po tom, zda je opravdu technicky možné a případně i nutné příslušná právní pravidla aktivně kódovat. Lessig sám je v tomto směru poměrně nekompromisní, když píše (překlad autor)²⁷⁸: „*Můžeme postavit nebo navrhnout nebo prostě nakódovat kyberprostor k tomu, vychránil hodnoty, o nichž jsme přesvědčení, že jsou fundamentální. Můžeme ale také kyberprostor postavit nebo navrhnout nebo nakódovat tak, aby nechal tyto hodnoty vymizet. Není žádná střední cesta.*“

V uvedeném citátu se Lessig hlásí k tezi, že kyberprostor je vždy vytvářen vůlí definičních autorit a právě jen jejich vůlí²⁷⁹. Cokoli tedy definiční autority do kyberprostoru vloží, včetně hodnot a principů civilizace, bude tam. Cokoli ale naopak opomenou, se v kyberprostoru prostě neobjeví.

²⁷⁷ Odpovědností definičních autorit za protiprávní aktivity uživatelů jakož i za protiprávní důsledky činnosti filtrů se zabýváme v následující kapitole.

²⁷⁸ Viz Lessig, L. Code V.2. New York: Basic Books, 2006, str. 6.

²⁷⁹ Viz též Bomse, A. L. The Dependence of Cyberspace. Duke Law Review, číslo 50, str. 1717 a násl.

S odkazem k dříve provedenému výkladu o pojmu a podstatě informační společnosti však můžeme uvedenou tezi zpochybnit, a to prostřednictvím dvou jednoduchých otázek:

- 1) Je možné aktivně kódovat základní hodnoty do kyberprostoru?
- 2) Je nutné aktivně kódovat základní hodnoty do kyberprostoru?

Odpověď na první otázku vychází ze základních rysů informační sítě jako uměle vytvořeného prostředí obsluhovaného službami a technologiemi informační společnosti. Jakékoli kódování má zde charakter vyjádření příslušných pravidel stoprocentně monotónní a kauzální sadou instrukcí typu „pokud se vyskytne situace A, tak proved' B,“ tj. například „pokud uživatel zadá do diskusního pole výraz 'hovno,' smaž diskusní příspěvek“. Chceme-li tedy vnést určité pravidlo do kyberprostoru, je třeba jej vyjádřit monotónně a relativně jednoduše tak, aby jej byl příslušný počítač, zjednodušeně řečeno, schopen pochopit.

Při vyjadřování pravidel legislativní formou narážíme na celou řadu obtíží – jazyk má své přirozené limity, lidské schopnosti aktivně či pasivně jazyka užívat jsou rovněž omezené a tato omezení se navíc mezi lidmi vzájemně liší. Tyto nedostatky pak u legislativy hojíme nejčastěji interpretací, kdy přirozené či nahodilé nedostatky právního předpisu nahrazujeme rozumem či zkušeností člověka fungujícího v postavení autoritativního státního orgánu. Zjednodušeně řečeno jsou tedy limity jazyka a schopností právotvůrce hojeny, tu s větším, jindy s menším úspěchem, díky schopnostem interpretů.

Adresátem definiční normy, tedy kódu, však primárně není člověk ale stroj. Počítač přitom není schopen ani na základní úrovni racionálně reflektovat příslušné instrukce - prostě je provádí. Požaduje přitom, aby tyto instrukce byly vyjádřeny jednoznačně, tj. monotónním jazykem. Počítač pak sice může být naprogramován dokonce i k určitému typu mechanické reflexe, její postup však opět musí být jednoznačný a kauzální.

Ptáme-li se tedy, zda je možné kódovat základní hodnoty lidské společnosti do kyberprostoru, naše otázka směřuje k našim schopnostem definovat tyto hodnoty jednoznačným, tedy monotónním, normativním jazykem,

a to tak, aby je byl schopen příslušný stroj automaticky zpracovat. Nemůžeme se přitom spolehnout na interpretační schopnosti stroje, jeho racionalitu či dokonce cit.

Po odpovědi na tuto otázku není třeba dlouho pátrat, neboť k ní elegantně dospěl už Kelsen, když provedl jednoduchou analýzu spravedlnostních postulátů. Prokázal přitom, že jednotlivé formule artikulující základy přirozeného práva jsou buďto obsahově prázdné nebo vnitřně rozporné. Není přitom pochyb o tom, že ideály jako jsou rovnost, svoboda, solidarita apod. objektivně existují. Nepřekonatelný problém jejich užití v právu však představuje subjektivní charakter jejich chápání a především pak, a to Kelsen prokázal především, nemožnost jejich, byť i jen trochu přesného, jazykového vyjádření.

Je-li nemožné objektivně vyjádřit základní hodnoty lidské společnosti, jejichž esencí jsou nesporně přirozená práva, nebude logicky možné ani zjednodušení takových vyjádření do monotónního jazyka srozumitelného strojům. Relativně jednoduše tedy dospíváme k závěru, že proaktivní kódování těchto hodnot do kyberprostoru není možné. Z tohoto závěru plyne i další poznatek, totiž že jakýkoli pokus o takové kódování skončí nutně nezdarem.

Snahu o ochranu základních hodnot jejich a priori nakódováním do kyberprostoru lze s trochou nadsázky přirovnat k práci slepého operátéra. Dotyčný se v nejlepším případě pouze netrefí do pacienta – mnohem pravděpodobnější však je, že skalpelem pořeže sebe, okolostojící personál nebo že pacientovi způsobí vážnější újmu, než je ta, kvůli které má být operován.

Zatímco odpověď na první otázku po naší schopnosti kódovat základní hodnoty vyznívá pesimisticky, můžeme na druhou otázku odpovědět naopak optimistickým poukazem na přirozenost informační společnosti. Je-li totiž kyberprostor alespoň z větší části tvořen informacemi splňujícími základní wienerovská definiční kritéria, můžeme se spolehnout i na skutečnost, že základní (přirozené) společenské hodnoty jsou v něm přítomné implicitně, a to jako přirozený avšak nevyjádřený obsah veškerých (skuteč-

ných) informací. Navenek se pak tyto hodnoty projevují opět nikoli explicitně ale v komplexních organizačních efektech²⁸⁰.

8.5 ZÁVĚREČNÁ POZNÁMKA K POMĚRU KÓDU A PRÁVNÍCH PRAVIDEL

Jak vyplývá z výše uvedeného, mají, technicky vzato, definiční normy v porovnání s právními pravidly řadu výhodných i nevýhodných rysů. Jejich výhody můžeme vidět především v důsledcích kauzálního jejich charakteru, kdy se účinkem blíží spíše přírodním zákonům. Výhoda právních pravidel naopak spočívá v tom, že se jejich tvůrce může spolehnout na znalosti, zkušenosti a především na rozumové a etické schopnosti interpretů. Definiční normy, tj. kód, tedy disponují vysokou mírou efektivity, avšak jejich tvorba je extrémně náročná, to především, mají-li limitovat svobodu lidského jednání.

Mají-li definiční normy fungovat jako opora právních pravidel, je třeba řešit často nepřekonatelný problém překladu z nemonotónního a na schopnosti interpreta spoléhajícího právního jazyka do monotónního strojového kódu. Pokud se však takový překlad vydaří a právo se může spolehnout na definiční zajištění, není již třeba se zvláště zabývat otázkou uplatnění právních sankcí – definiční normy jsou totiž způsobilé kauzálně uskutečňovat dispozice příslušných právních pravidel. Je-li tedy právní pravidlo zajištěno definiční normou, nemůže obecně dojít k jeho porušení. Subjekty, které mají technické kompetence k překonání definičních norem, tj. hackeři, pak v podstatě představují jedinou zbývající cílovou skupinu pro právní sankční aparát.

Ideální stav, kdy definiční norma materiálně odpovídá právnímu pravidlu, je však ve většině případů dosažitelný pouze hypoteticky. Dojde-li k pokusu přeložit právní jazyk do strojového kódu, je prakticky vždy výsledkem definiční norma s určitou mírou chybovosti. Lze pak formulovat

²⁸⁰ Otázky související s komplexitou základních hodnot jsou podrobněji rozebrány v druhé kapitole.

závěr, že chybovost takové definiční normy odpovídá složitosti resp. neurčitosti vyjádření příslušného právního pravidla. Kód vyjadřující takřka absolutně neurčitá právní pravidla, příkladně principy ochrany základních práv, tedy nutně musí být extrémně chybový. To ve spojitosti s vysokou mírou efektivity definičních norem nutně přinese výše naznačený efekt slepého chirurga.

Máme-li na základě právě uvedeného formulovat výslednou tezi stran použitelnosti definičních norem ke kauzálnímu kódování práva do kyberprostoru, je třeba předeslat, že nastavení pravidel tohoto procesu není úkolem pro právníky. K rozhodování o tom, jaká míra složitosti „automatizovaných“ právních pravidel a potažmo pak míra chybovosti jejich definičních forem je pro společnost přijatelná, nejsou právníci ani inforatici dostatečně kvalifikováni ani legitimováni. Politická reprezentace státu, jíž toto rozhodnutí přísluší, pak nutně musí vzít v potaz veškeré výše uvedené limity a rizika včetně institucionálních aspektů pojednaných dále.

9 STRUKTURA INFORMAČNÍ SPOLEČNOSTI - DEFINIČNÍ AUTORITY

9.1 POJEM DEFINIČNÍCH AUTORIT

Stručné pojednání o pojmu definičních autorit můžeme začít odkazem na Ovidiovy Proměny. Povahou totiž tyto definiční autority připomínají v mnoha směrech bohy antické mytologie. Jejich zrod líčí Ovidius následovně:

*Tvora však, který by světější byl a o velkých věcech
přemýšlet znal a vládnout ostatním, nebylo dosud:
povstal tudíž člověk – ať dal mu z božského vzniknout
semene strůjce jsoucna, ten původce lepšího světa,
či že snad čerstvá země, jež spojení s étherem právě
musela opustit, sourodých nebes si chránila símě,
tu pak Prométheus vzal, a smísiv ji s dešťovou vodou,
dal jí podobu bohů, těch správců celého světa.*

Bohové starého světa se od lidí lišili tím, že byli nadáni mocí vládnout přírodním silám. Stejně tak i definiční autority, jak bylo naznačeno v předchozí kapitole, se od ostatních subjektů liší technickou kompetencí ovládat tento prostor prostřednictvím svých definičních norem²⁸¹. Provozovatel online hry tedy například definuje formální a částečně i obsahové znaky herního prostředí a stanoví herní pravidla. Definiční autority sice, podobně jako Ovidiovi bohové, nemohou přímo definovat chování lidí. Mají však moc toto chování ovlivňovat na úrovni charakteristik prostředí. Ani bohové

²⁸¹ Fenomén definičních autorit se neobjevuje s příchodem internetu. Historii definiční kontroly nad společností stručně mapuje Lessig ve své starší monografii *The Future of Ideas – viz Lessig, L. The Future of Ideas – The Fate of the Commons in a Connected World. New York: Vintage Books, 2002, str. 143 a násl.*

tak člověku nemohli například zabránit v rouhání – pokud tak činil, mohli jej však zbavit řeči. Podobně provozovatel diskusního serveru nemůže přímo zabránit účastníkům debaty v tom, aby se vzájemně neuráželi – může však automaticky mazat diskusní příspěvky nebo dokonce vybraným diskutujícími zcela zablokovat aktivní přístup.

Dalším typickým znakem antického božství je omezení kompetencí. Svého boha tak měly různé lidské činnosti, božské patrony měla i města nebo pohoří. Dokonce kdejaká tuň či průsmyk měly své bůžky či jiné nadpřirozené správce. Kompetence všech možných nadpřirozených bytostí však nebyly rozděleny přesně a často se tedy stávalo, že si různí správci světa vzájemně zasahovali do objektů svého zájmu. Paralela s prostředím informačních sítí je i v tomto případě nasnadě. I zde jsou kompetence jednotlivých definičních autorit rozděleny v různých vrstvách a hranice působnosti jednotlivých definičních norem se tedy často prolínají. Hovořme-li například o již zmíněném diskusním serveru, jeho činnost samozřejmě bezprostředně řídí jeho provozovatel. Tento server však může být (a obvykle bývá) fyzicky umístěn na infrastruktuře jiného poskytovatele a prostřednictvím dalších „správců světa“ propojen s ostatními prvky celosvětové sítě. Není to tedy jen samotný provozovatel diskuse, kdo může ovlivňovat existenci a funkce tohoto diskusního serveru, ale do určité míry též majitel hostingového prostoru, provozovatel komunikačních linek, ba dokonce zprostředkovaně třeba i dodavatel energie nebo pronajímatel prostor k fyzickému umístění komunikační infrastruktury.

Definiční autority se Ovidiovým bohům vedle technických kompetencí dokonale podobají i lidskostí či lépe lidskou nedokonalostí. Božské akty jsou tedy často vedeny emocemi nebo i jen nahodilostí a jejich provedení je nedokonalé. Je tedy možné je za vynaložení odpovídajícího úsilí či za využití jiných vhodně zvolených nadpřirozených kompetencí zvrátit, změnit nebo se vyhnout jejich účinkům. Obdobně i definiční autority informačních sítí jednájí při realizaci svých definičních normotvorných kompetencí často iracionálně, krátkozrace, emocionálně apod. Definiční normy ustavené, tj. kódované, těmito autoritami pak jsou rovněž stíženy chybami, mezerovitostí či jinou technickou nedokonalostí.

Konečně pak nacházíme podobnost mezi Ovidiovými bohy a definičními autoritami i v posledním jejich společném charakteristickém znaku, kte-

rým je forma jejich existence. Bohové totiž vypadali na první pohled jako lidé – v mnoha případech dokonce ze své formální lidskosti i těžili, když s lidmi vstupovali do nejrůznějších vzájemných interakcí. Obdobně i forma definičních autorit je srovnatelná s formou subjektů, jimž tyto autority vytváří a spravují existenční prostor. Valná většina definičních autorit tak má standardní formu fyzických nebo právnických osob. V tomto bodě však dále paralela mezi bohy a definičními autoritami poněkud pokulhává, neboť bohové mohli svou formu měnit a především pak pro ně nebyla jejich lidská forma nikterak důležitou charakteristikou. Pro definiční autority informačních sítí je však jejich forma esencí jejich existence a skutečnost, že jde o standardní fyzické či častěji právnické osoby, má pro ně dalekosáhlé následky. Nejzávažnějším z nich je pak subjektivizace definičních autorit vůči právu. Jinými slovy činí jejich forma z definičních autorit před právem obyčejné smrtelníky.

Představa, že by byl některý z bohů souzen či by mu stát mohl jinak prostřednictvím práva přikazovat, jak má jednat, je sama o sobě absurdní. Bylo-li by to možné, měly by samozřejmě státy vykonávající jurisdikci nad bohy prakticky pod kontrolou jejich správcovské kompetence. Stát, který by například vykonával jurisdikci nad Poseidonem, by tedy *de facto* mohl kontrolovat všechna moře.

U definičních autorit je naopak absurdní představa, že by snad tyto měly být vyňaty z působnosti práva a tím i ze státní jurisdikce. Důvodem je skutečnost, že definiční autority neodvozují svůj původ od Prométhea, ale že se původně jedná o standardní subjekty práva a není zde dán důvod odlišovat je v jejich právním postavení od ostatních osob.

Výsadní postavení mezi „správci kyberprostoru“ má v současné době sdružení ICANN (Internet Corporation for Assigned Names and Numbers). Funguje totiž jako tzv. centrální doménová autorita a do její kompetence spadá stanovení pravidel pro provoz systému doménových jmen. Tuto kompetenci však nezískala ICANN na základě vůle státu vyjádřené zákonem nebo mezinárodní smlouvou ale fakticky²⁸². Přestože v tomto případě

²⁸² S tím souvisí i její poněkud problematické postavení jako subjektu, který nejen dominuje příslušnému „trhu doménových jmen“, ale který tento „trh“ fakticky vytváří – k tomu srov. např. Blue, L. Internet and Domain Name Governance: Antitrust Litigation and ICANN. Berkeley Technology Law Journal, roč. 19, číslo 1, str. 387 a násl.

nedošlo k jeho standardní legitimaci, má tento subjekt v době, kdy je prakticky veškerá masová komunikace na internetu adresována prostřednictvím doménových jmen, nesrovnatelně větší faktickou moc než řada státních orgánů. Aktuálně se tak ICANN stává institucí, kterou jako partnera přijímají nejen státy, ale dokonce i mezinárodní mezivládní organizace. Lze tedy konstatovat, že pro dění na internetu je v mnoha případech daleko důležitější rozhodnutí Rady ICANN než rozhodnutí české vlády nebo německého parlamentu. Přesto činnost toho „správce on-line světa“ stále zůstává pod státní jurisdikcí země, kde je usazen, tj. USA.

Faktická moc definičních autorit s sebou kromě zřejmých výhod (a definiční autority, jsou-li podnikatelskými subjekty, jich zhusta využívají) nese i aspekt velké společenské odpovědnosti. Nejen ICANN nebo sdružení typu NIX, ale i každý provozovatel diskusního serveru tak fakticky odpovídají za kvalitu komunikace, která se jejich přičiněním odehrává. Odpovědnost je to poněkud zvláštní, neboť možnosti jejího sankcionování, ať už právního, sociálního nebo jiného, jsou nevalné. Skutečností ale každopádně je, že řada definičních autorit, na prvním místě opět ICANN, bere tuto odpovědnost i bez hrozby sankce velmi vážně²⁸³.

9.2 EXKURS: HACKEŘI

Pojem hackera jsme již v předchozích kapitolách několikrát použili, a to v souvislosti s anomáliemi kauzálního působení definičních norem. Optikou definičních norem je tedy hackera možné brát jako subjekt, který těmito normami není vázán, to díky svým technickým schopnostem. Není možné jej považovat za definiční autoritu, neboť i on je adresátem definičních norem. Tyto normy však díky svým schopnostem není nucen²⁸⁴ dodržovat, naopak je může v míře dané svými schopnostmi obcházet či dokonce

²⁸³ Příkladem je vývoj hmotného a procesního soft law pro registraci generických doménových jmen včetně vytvoření systému alternativního řešení sporů – takzvané právo doménových jmen je tedy na generické úrovni v současné době tvořeno převážně nestátními prameny, ať už jsou to smluvní dokumenty nebo precedenty rozhodčích soudů.

²⁸⁴ Zde můžeme odkázat na výklad o nutnosti (nikoli povinnosti) dodržovat definiční normy informačních sítí provedený v předchozí kapitole.

měnit nebo rušit. Podle uznávaného lexikonu The Jargon File²⁸⁵ je hackera možné vymezit některou z následujících 7 definic (překlad autor):

- „1. člověk, kterého, na rozdíl od ostatních uživatelů chtivých učit se jen minimum nutných poznatků, baví objevovat detaily programovatelných systémů a rozšiřovat jejich možnosti*
- 2. člověk, který programuje zaujatě (až posedle) a víc jej baví programování než teoretizování o něm*
- 3. člověk schopný docenit hodnotu hacku (angl. hack value²⁸⁶)*
- 4. člověk, kterému jde rychlé programování*
- 5. odborník na určitý program nebo někdo, kdo s ním nebo na něm pracuje*
- 6. jakýkoli odborník nebo nadšenec – někdo může být například hackerem astronomie*
- 7. člověk, který se těší z intelektuální výzev spočívajících v kreativním překonávání nebo obcházení limitů“*

Jak sám Jargon File přiznává v přidané osmé definici, dostal především vlivem medializace některých problematických případů tzv. crackingu²⁸⁷ pojem hackera negativní konotace a je v současné době často používán pro označování pachatelů nejrůznějších škodlivých či dokonce protiprávních aktivit, jejichž objektem jsou fyzická nebo logická informační infrastruktura. Jako hackeri se totiž mají tendenci označovat i nejrůznější živly zneužívající svých technických schopností k dosažení zisku, šíření ideologií, teroru apod.

Esenci pojmu hacker však vedle technických schopností a vůle k jejich využití tvoří též třetí element, a to takzvaná hackerská etika. Ta je založena

²⁸⁵ Viz Raymond, E. S., Steele, G. L. (eds.) Jargon File. Project Gutenberg, 2000, dostupné on-line na www.gutenberg.org/dirs/etext02/jarg422.txt.

²⁸⁶ Jedná se o výraz pro uspokojení nad dosaženým technickým úspěchem – dle tvrzení hackerů se jeho podstata nedá vysvětlit, lze ji jen přímo zažít.

²⁸⁷ Jedná se, stručně řečeno, o označení aktivit spočívajících v průnicích do informačních systémů s cílem škodit.

na dvou základních maximách²⁸⁸ - na povinnosti sdílet své vědomosti a dále na zákazu škodit.

Můžeme konstatovat, že obě esenciální maximy hackerské etiky plně odpovídají ideovým základům kybernetiky. Požadavek na sdílení vlastních vědomostí odráží fakt, že hacker disponuje technologickými znalostmi, které mají informační hodnotu pro ostatní uživatele informační sítě. Šíření těchto vědomostí tedy snižuje entropii v systému. Tím, že hacker sdílí své vědomosti s ostatními, tj. že se vzdává kontroly na získanými či vytvořenými informacemi, přispívá tedy k organizaci celého systému informační sítě. Jedním z projevů této maximy je například i princip, podle kterého jakýkoli software vytvořený hackerem má mít povahu open source²⁸⁹.

Druhá maxima omezuje hackera v možnostech využití jeho technických schopností. Jak bylo uvedeno výše, není sice hacker vázán definičními normami, limitem je mu však právě účinek jeho jednání, který nesmí být škodlivý. Jinými slovy tedy nesmí hacker vnášet do systému informační sítě chaos.

Podobně, jako je tomu u definičních autorit, nejsou ani hackeři nikterak výjimeční co do své formy. Jedná se tedy z hlediska státu o běžné fyzické osoby nepožívající žádných zvláštních privilegií. Specifikum jejich právního postavení však plyne z povahy informační sítě a především pak z již diskutovaných problémů místní působnosti práva. Především je třeba si uvědomit, že libovolný kyberprostor je přímo tvořen definičními autoritami a veškeré dění je těmito autoritami zprostředkováváno. Má-li tedy dojít k výkonu individuálního právního aktu na on-line hodnotu nebo vztah, musí být takové rozhodnutí provedeno nikoli přímo, tedy například soudním vykonavatelem, ale příslušnou definiční autoritou. Pokud je například rozhodnuto o převodu doménového jména, je třeba, aby tento převod provedla příslušná doménová autorita (nikdo jiný včetně exekutorů, soudních vykonavatelů, policie apod. k tomu totiž nemá technickou kompetenci).

²⁸⁸ Viz Raymond, E. S., Steele, G. L. (eds.) Jargon File. Project Gutenberg, 2000, dostupné on-line na www.gutenberg.org/dirs/etext02/jarg422.txt - heslo „hacker ethics.“

²⁸⁹ Jedná se o typ tzv. volné licence, která umožňuje užívání takového software bez nutnosti platit licenční poplatky. Autor navíc dává veřejnosti k dispozici pro nevýdělečné účely i zdrojový kód.

Má-li však hacker schopnost obcházet nebo blokovat činnost příslušné definiční autority, je výkon rozhodnutí fakticky znemožněn.

Výše uvedené samozřejmě neznamená, že by byl hacker s odpovídající technickou kompetencí *de iure* nepostižitelný. Příslušný postih však musí být uplatněn přímo proti jeho osobě – v tom ovšem často brání faktické i formální limity působnosti práva diskutované v úvodních kapitolách.

Velmi vzdálenou přesto však případnou paralelu mezi hackery a prostředím informačních sítí můžeme nalézt i v právu. To je totiž aplikováno výlučně prostřednictvím k tomu určených státních orgánů. Právnické disponující dostatečnými znalostmi práva či jinými schopnostmi ovlivňovat činnost těchto orgánů, pak je *de facto* vyvázán z povinnosti dodržovat příslušné právní normy. Pokud tedy například takový právník ovládá techniku obrany před pokutami za špatné parkování, je jen na něm rozhodnout se, zda a kdy pokutu zaplatí. Míra imunity právníka a osob pod jeho ochranou vůči právním normám je pak přímo úměrná míře jeho znalostí práva a schopností ovlivňovat činnost autoritativních orgánů.

9.3 POJEM ISP

Jak bylo uvedeno výše, mají definiční autority v mnoha směrech *de facto* specifické postavení. Veškeré dění v informačních sítích probíhá prostřednictvím jejich infrastruktury či služeb a disponují tedy faktickým a výsoce efektivním regulačním potenciálem. Na druhou stranu však mají charakter běžných subjektů práva a státy nad nimi tedy mohou vykonávat svou jurisdikci.

Zvláštní postavení definičních autorit reflektuje právo především prostřednictvím institucionalizace a právní úpravy postavení vybraných jejich typů. Základním momentem specifické právní regulace definičních autorit je zavedení právního pojmu poskytovatele služeb informační společnosti (ISP – information service provider²⁹⁰). Ten, stručně řečeno, zahrnuje také definiční autority, jejichž prostřednictvím mohou ostatní vstupovat do

²⁹⁰ V angličtině se též používá kratší výrazu „information intermediary“ – tj. informační zprostředkovatel.

informační sítě, resp. jejichž prostřednictvím zde probíhá tvorba, zpracování nebo výměna informací.

Pojem ISP neobsahuje všechny definiční autority, ale jen takové, které poskytují své služby ostatním, typicky za úplatu. Pojem sám se v právu vyvíjel a v současné době je základem jeho definice v EU vymezení provedené směrnicí č. 98/34/ES o postupu při poskytování informací v oblasti norem a technických předpisů ve znění směrnice č. 98/48/ES. Tato směrnice nedefinuje pojem poskytovatele služeb informační společnosti ale jen pojem samotné služby informační společnosti a sama má spíše okrajový význam. Definice služeb informační společnosti je však z ní přebírána i do dalších oblastí evropského i národního práva. Směrnice tedy vymezuje pojem služby informační společnosti, a to v novelizovaném článku 1(2) následovně:

[Službou informační společnosti se rozumí] jakákoli služba informační společnosti, tj. každá služba poskytovaná zpravidla za úplatu, na dálku, elektronicky a na individuální žádost příjemce služeb.

Pro účely této definice se rozumí:

- "službou poskytovanou na dálku"; služba poskytovaná bez současné přítomnosti stran,
- "službou poskytovanou elektronicky"; služba odeslaná z výchozího místa a přijatá v místě jejího určení prostřednictvím elektronického zařízení pro zpracování a uchování dat (včetně digitální komprese) a jako celek odeslaná, přenesená nebo přijatá drátově, rádiově, opticky nebo jinými elektromagnetickými prostředky,
- "službou na individuální žádost příjemce služeb"; služba poskytovaná přenosem dat na individuální žádost.

Jak vyplývá z dikce ustanovení čl. 1(2) směrnice č. 98/34/ES, pokrývá pojem „služba informační společnosti“ takové služby, které jsou objednány uživatelem a jsou poskytovány na dálku a elektronicky. Výjimky uvedené v příloze č. 5 ke směrnici jsou pak následující:

1. Služby, které nejsou poskytovány "na dálku"

Služby poskytované za osobní přítomnosti poskytovatele a příjemce, a to i tehdy, použije-li se přítom elektronické zařízení:

- a) lékařská vyšetření nebo ošetření v lékařské ordinaci za použití elektronického zařízení a za osobní přítomnosti pacienta;
- b) prohlídka elektronického katalogu v prodejně za přítomnosti zákazníka;

- c) rezervace letenek pomocí počítačové sítě v cestovní kanceláři a za osobní přítomnosti zákazníka;
- d) zpřístupnění elektronických her v herně za osobní přítomnosti uživatele.

2. Služby, které nejsou poskytovány "elektronicky"

- Služby materiální povahy, ačkoli jsou poskytovány elektronickými přístroji:
 - a) přístroje pro automatický výdej peněz nebo lístků (bankovky, jízdenky);
 - b) vstup do silničních sítí, na parkoviště apod. podléhající poplatkům, a to i tehdy, jsou-li v místě vjezdu a výjezdu instalována elektronická zařízení kontrolující vstup a/nebo zajišťující řádné zaplacení,
- služby poskytované off-line: prodej kompaktních disků nebo programového vybavení na disketách,
- služby, které nejsou poskytovány elektronickými systémy pro zpracování/ukládání dat:
 - a) hlasové telefonní služby;
 - b) telefaxové/telexové služby;
 - c) služby poskytované hlasově po telefonu nebo faxem;
 - d) lékařské porady po telefonu/telefaxu;
 - e) právnícké porady po telefonu/telefaxu;
 - f) přímý prodej po telefonu/telefaxu.

Samotný pojem poskytovatele služeb informační společnosti, tj. právní definici ISP, zavedla do evropského práva až směrnice č. 2000/31/ES o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu ("směrnice o elektronickém obchodu") známá též pod anglickou zkratkou ECD ("*Electronic commerce directive*"). Definice je však v podstatě provedena jen odkazem na výše citovanou směrnici.

Podle výše uvedených definic je tak za poskytovatele služeb informační společnosti možné považovat subjekt, který, stručně řečeno, obstarává jiným možnost komunikovat v rámci informační sítě, případně který sám jako službu vytváří, zpracovává nebo šíří informace v elektronické formě. Definiční kritérium elektronické žádosti je přitom třeba vykládat extenzivně, když za takovou žádost je možné považovat prakticky jakoukoli aktivitu uživatele, na jejímž základě je služba poskytována (tj. například přihlášení se do sítě).

Stejně tak ani kritérium úplaty není nikterak rigorózní – výraz „zpravidla za úplatu“ je totiž třeba interpretovat tak, že je obvyklé za příslušnou

službu vybírat úplaty. Neznamená to však, že služba splňující výše uvedené podmínky, která je poskytována v konkrétním případě zdarma, této definici neodpovídá. Rovněž to neznamená, že úplata musí být nutně vybírána od toho, komu je příslušná služba poskytována (viz dále).

Obsah pojmu ISP, tj. poskytovatele služeb informační společnosti, můžeme dále demonstrovat na příkladech ze současné praxe. Následující klasifikace však vznikla pouze pro potřeby této kapitoly a zohledňuje aktuální nabídku služeb informační společnosti. V žádném případě si tak neklade za cíl vyčerpávajícím způsobem postihnout všechny možné typy služeb a ISP:

- Provozovatele síťové komunikační infrastruktury (fyzické, logické)
- Provozovatele síťové asistenční infrastruktury
- Provozovatele hostingových služeb, služeb pro bloggery, apod.
- Provozovatele e-mailových služeb
- Vyhledávače, portály
- Diskusní servery, diskusní služby
- Zpravodajské servery
- Doménové autority
- Provozovatelé instant messengerů
- Provozovatelé komunitních serverů

Budeme-li řešit v praxi otázku, zda je určitý subjekt možné považovat za poskytovatele služeb informační společnosti nebo nikoli, je třeba zaměřit se na tři základní kritéria:

- Služba musí být poskytována pro jiného (zde logicky odpadají například služby, které poskytuje zaměstnavatel zaměstnancům v rámci výkonu jejich pracovních činností, tj. na základě pracovní smlouvy),
- podstata služby je v elektronicky komunikované informaci (tam, kde podstatu služby tvoří cokoli jiného a informace jen umožňuje poskytnutí služby, nejedná se o službu informační společnosti – příkladem může být on-line obchod, kde elektronická komunikace jen usnadňuje uzavření smluv) a

- služba je poskytována individuálně (musí se jednat o službu, kterou uživatel konzumuje vlastní aktivitou a je tedy poskytována za jeho přímého přičinění – služby poskytované bez ohledu na uživatele jako například rozhlasové vysílání, do tohoto rámce nespádají).

Poněkud neobratně nám v pochopení pojmu služeb informační společnosti pomáhá i článek 18 preambule směrnice č. 2000/31/ES. Z legislativně-technického hlediska se sice nejedná o žádnou perlu, přesto nám může alespoň napovědět, že jsou to právě výše uvedená kritéria, která budou k *ad hoc* interpretaci pojmu ISP určující. Současně lze z tohoto ustanovení vyčíst i úmysl právotvůrce nestavět kvalifikaci pojmu ISP na kritériu přímé úplatnosti příslušné služby – tím došlo k zohlednění skutečnosti, že řada on-line obchodních modelů je založená na poskytování služeb zdarma a následném těžení ze sekundárních efektů spotřebitelského zájmu, resp. že řada služeb informační společnosti může být provozována zcela zdarma (což samo o sobě nepředstavuje důvod k vynětí jejich poskytovatelů z legální definice ISP). Článek 18 preambule nám tedy dává následující interpretační vodítko:

(18) Služby informační společnosti zahrnují širokou škálu hospodářských činností, které probíhají on-line. Tyto činnosti mohou spočívat zejména v on-line prodeji zboží. Činnosti, jako je dodávka zboží jako taková nebo poskytování služeb off-line, zde nejsou zahrnuty. Služby informační společnosti se neomezují výhradně na služby umožňující uzavírání smluv on-line, ale vztahují se rovněž, pokud jde o hospodářskou činnost, na služby, které nehradí ti, kdo je přijímají, jako např. služby poskytující informace on-line nebo obchodní sdělení nebo ty služby, které poskytují nástroje umožňující vyhledávání dat, přístup k datům a získávání dat. Služby informační společnosti zahrnují rovněž služby, které spočívají v předávání informací prostřednictvím komunikační sítě, v poskytování přístupu ke komunikační síti nebo v shromažďování informací poskytovaných příjemcem služby. Televizní vysílání ve smyslu směrnice 89/552/EHS ani rozhlasové vysílání nejsou službami informační společnosti, neboť nejsou poskytovány na individuální žádost. Naopak službami informační společnosti jsou služby, které jsou poskytovány z místa, jako je video na přání nebo poskytování obchodního sdělení elektronickou poštou. Používání elektronické pošty nebo jiných rovnocenných individuálních komunikačních prostředků fyzickými osobami mimo rámec jejich obchodní nebo profesní činnosti včetně jejich používání pro uzavírání smluv mezi těmito osobami není službou informační společnosti. Smluvní vztah mezi zaměstnancem a zaměstnavatelem není službou informační společnosti. Činnosti, které pro svou povahu nelze vykonávat na dálku a elektronickou cestou, jako povinná účetní kontrola společnosti nebo lékařská konzultace vyžadující fyzické vyšetření pacienta, nejsou službami informační společnosti.

Přestože je zřejmá snaha právotvůrce co nejpodrobněji specifikovat jednotlivé formy ISP, vyvstává v praxi celá řada problematických otázek nad konkrétními on-line službami či produkty. E-mailový newsletter tak sice směrnice za službu informační společnosti nepochybně považuje, zpravodajské www stránky však již mohou znamenat interpretační problém – jedná se sice o službu, k níž musí uživatel přistoupit vlastním přičiněním a kterou si stahuje a prohlíží na svém zařízení (minimálně musí zadat do vyhledávače příslušnou adresu a připojit se k www serveru), z hlediska efektu se však on-line zpravodajství v různých formách (např. i ve formě RSS feed) neliší od tištěných novin, televizního či rozhlasového vysílání, neboť není přílišného rozdílu mezi zadáním adresy do prohlížeče a zakoupením novin nebo naladěním televizního či rádiového kanálu. Podobný problém nastává například u klasických internetových rádií nebo televizních stanic, tj. u takových, kde uživatel příslušné vysílání jen sleduje a nemá možnost jej přímo ovlivnit (jiná je situace u služeb jako radio-on-demand nebo video-on-demand – zde uživatel přímo zadává svůj požadavek a poskytovatele služby tak lze nepochybně považovat za ISP ve smyslu legální definice).

Uvedená otázka nebyla ještě řešena národními soudy členských států ani Evropským soudním dvorem. Můžeme tedy jen opatrně předvídat, že bude zřejmě pro klasifikaci poskytovatele on-line služby jako ISP v takových případech nutné prokázat, že z jeho hlediska měl na kvantitu či kvalitu poskytované služby přímý vliv uživatel. Tímto interpretačním postupem tedy definice ISP nezahrne služby, s nimiž uživatelé komunikují pasivně, tj. ty, které lze zařadit do první skupiny takzvané škály Zippo (tj. pasivní webové stránky, internetová rádia, internetová TV, apod.). I v takovém případě však bude třeba *ad hoc* řešit jemné nuance různých variant – např. zpravodajský server, jehož vizáž mají možnost uživatelé individuálně konfigurovat.

Přestože může výše uvedený interpretační problém vypadat jako závažný, není dle našeho názoru třeba se jej v praxi nějak přehnaně obávat. Specifická legislativa upravující odpovědnost ISP by se totiž výše uvedených poskytovatelů služeb, jako jsou zpravodajské servery či on-line rádia, stejně nedotkla a otázka interpretace pojmu ISP tak ve většině shora nazna-

čených případů pasivní konzumace informací zůstane jen v rovině hypotetických úvah.

9.4 ODPOVĚDNOST ISP

Řada soukromoprávních deliktů založených na použití či zneužití informace má objektivní charakter. Ať už se jedná například o porušení osobní integrity, autorských práv, průmyslových práv duševního vlastnictví nebo o nekalosoutěžní jednání, nezkoumá se při uplatnění soukromoprávního postihu zavinění. Objem informací, jejichž tvorba, zpracování a přenos probíhá prostřednictvím nejrůznějších služeb informační společnosti, je přitom doslova obrovský a stejně obrovská je i pravděpodobnost, že tyto informace zasahují do něčích subjektivních práv. Je-li pak definována odpovědnost za takový zásah na objektivním principu, odpovídal by příslušný ISP i jen za to, že pomohl s provedením, respektive přímo provedl operaci spočívající v protiprávním vytvoření, zpracování nebo přenosu určité informace.

Snad nejznámějším on-line debatním společenstvím před vznikem internetových sociálních sítí se stala komunita Well²⁹¹. Jednalo se o komunitu, která se začala vyvíjet roku 1985 okolo počítače VAX a několika primitivních modemů a její existence *de facto* skončila až celých deset let poté, v březnu roku 1995. Již záhy se ukázalo, že ne všechny diskusní příspěvky musí být nutně všem po chuti (a po právu), proto komunita vypracovala vlastní pravidla odpovědnosti za obsah diskusních příspěvků²⁹² včetně výzvy „když někoho našteješ, nebudou žalovat nás ale Tebe.“ Tato pravidla byla samozřejmě motivována ekonomicky, neboť na jejich základě nemusela komunita vydávat prostředky na spory se subjekty, kterým zde publikované diskusní příspěvky zasáhly do jejich subjektivních práv.

²⁹¹ Vývojem této komunity se dlouhodobě zabývala Katie Hafner. Z jejích publikací viz např. Hafner, K. The Epic Saga of the Well. Wired, čís. 5.05, str. 98 a násl. Článek je rovněž k dispozici on-line na adrese http://www.wired.com/wired/archive/5.05/ff_well.html.

²⁹² Zde můžeme doplnit, že omezení odpovědnosti na bázi soukromoprávního ujednání či dokonce i jen ve formě jednostranného prohlášení je dle severoamerického práva možné. V kontinentálním evropském právu se s takovým omezením odpovědnosti můžeme setkat jen velmi zřídka a například čeština ani nezná ekvivalent anglického výrazu „disclaimer“, který by snad šel přeložit jako „prohlášení o omezení odpovědnosti“.

V naznačeném směru lze argumentovat, že poskytovatel služby informační společnosti nejen, že dává v takovém případě svoji komunikační infrastrukturu k dispozici k protiprávním aktivitám, ale že na tom dokonce sám vydělává. Zbavovat jej spoluodpovědnosti za protiprávní jednání (protiprávní kvalitu informací) by tedy v podstatě znamenalo přiznat mu postavení posvátné krávy, která může díky své nedotknutelnosti zastavovat dopravu na rušné křižovatce nebo spásat trávu v zakázaných chrámových zahradách. Proti zbavení ISP odpovědnosti za protiprávní kvalitu informace, k jejímuž vytvoření, zpracování nebo přenosu poskytl svoji infrastrukturu, hovoří i skutečnost, že se v případě postihu může ISP regresně zhojit na tom, kdo protiprávní informaci vytvořil nebo kdo nařídil její komunikaci.

Na druhou stranu však můžeme postavit argument, že ISP sice poskytuje infrastrukturu k protiprávnímu jednání, ale konkrétní informační spojení má pro něj veskrze bagatelní význam. Profit, který příkladně realizuje telekomunikační společnost z jednoho hovoru nebo který získá služba pro instant messaging z jedné odeslané zprávy, je totiž z ekonomického hlediska naprosto zanedbatelný. Vedle masovosti v poskytování služeb informační společnosti pak můžeme argumentovat i možností anonymity na straně uživatele příslušné služby – celá řada služeb informační společnosti je totiž poskytována na anonymní bázi a poskytovatel služby by pak ani při největší snaze nebyl schopen skutečného poruše práva dohledat a zhojit se na něm.

Z právě uvedeného pak vyplývá závěr, že případné ponechání možnosti k založení objektivní odpovědnosti ISP na standardní bázi by *de facto* znamenalo uložení povinnosti poskytovatelům služeb informační společnosti monitorovat kvalitu informací, k jejichž tvorbě, zpracování nebo komunikaci poskytují svoji fyzickou nebo logickou infrastrukturu²⁹³. Operátoři VoIP služeb by tak například museli sledovat obsah telefonních hovorů, freemaily by musely prohlížet obsahy poštovních schránek svých uživatelů a hostingové servery by byly nuceny prohlížet obsah prezentací, k jejichž provozu poskytují prostor. K tomu by pak navíc přistoupila nut-

²⁹³ Stručnou diskusi problému implicitně uložené povinnosti ISP sledovat kvalitu informací viz např. Harper, J. Against ISP Liability. Regulation, číslo 1/2005, str. 31 a násled.

nost bránit nejen vlastní infrastrukturu ale i její jednotlivé uživatele před útoky zvenčí, ať už by se jednalo o viry nebo řízené útoky hackerů²⁹⁴.

Často citovaným případem z americké soudní praxe je jeden z prvních sporů o odpovědnost hostingových providerů známý jako *John Doe v. Franco Productions*²⁹⁵. V tomto sporu se neznámým uživatelům podařilo získat záznam ze skrytých kamer umístěných v baseballové šatně. Na záběrech, které se následně objevily na internetu, byli hráči týmu vyobrazeni „v různém stadiu svlečenosti.“ Vzhledem k tomu, že video na hostingový server umístil anonymní uživatel, směřovali žalobci svůj nárok proti provozovateli serveru. Soudce si v tomto případě zřejmě nebyl zcela vědom významu sporu a dopadu rozhodnutí, proto je rozhodnutí relativně stručné a místy působí až primitivním dojmem. Jednoznačně z něj však vyplývá argument na obranu hostingového serveru před odpovědností za to, co na něj bez vědomí jeho provozovatele nahrají uživatelé. Soud doslova uvedl: „Žalobci prostě uvádějí, že žalovaní jako provozovatelé webhostingu poskytli médium jehož prostřednictvím bylo možné prodávat či nabízet k prodeji předmětné videonahrávky. Tím, že nabízejí hostingové služby k tvorbě webových stránek, se však žalovaní nemohou nějakým zázrakem považovat za jejich tvůrce.“

Kromě faktické nemožnosti kontrolovat obrovské množství informací (často anonymně) komunikovaných v informačních sítích pak můžeme vidět důvod k omezení objektivní odpovědnosti ISP za kvalitu informací i v právní nemožnosti provádět takovou kontrolu uživatelů dané především soukromoprávní i veřejnoprávní ochranou osobní integrity včetně ochrany osobnosti, soukromí, osobních údajů apod.

Shrneme-li argumenty pro a proti specifické regulaci, roz. omezení, objektivní (spolu)odpovědnosti ISP za protiprávní aktivity uživatelů služeb informační sítě, hovoří pro takové omezení především masovost a častá anonymita těchto služeb. K tomu se pak ještě pojí právem zaručená diskrece uživatelů. Pro odpovědnost ISP naopak hovoří zejména skutečnost, že profit realizovaný z protiprávních uživatelských komunikačních aktivit je nemravný a především pak fakt, že ISP je často jediným subjektem, na kterém lze efektivně uplatnit právní postih. Posledně zmíněný argument je

²⁹⁴ Z toho by pak logicky vyplynula absurdní povinnost každého ISP provozovat ty nejmodernější zabezpečovací systémy – k problému viz Smejkal, V., Švestka, J. *Odpovědnost za škodu při provozu informačního systému, aneb nemalujeme čerty na zeď. Právní rozhledy*, roč. 13, číslo 19, str. 719 a násl.

²⁹⁵ Viz rozhodnutí 2000 U.S. Dist. Lexis 8845 (N.D. Ill., June 21, 2000), jehož plné znění je k dispozici on-line například na adrese <http://pub.bna.com/eclr/997885.htm>.

pro konstrukci odpovědnosti ISP zásadní. Pokud by totiž nebylo možné dotčeného ISP právně postihnout (minimálně ve formě příkazu k blokování příslušné služby), mohlo by dojít k situaci, kdy nebude *de iure* možné uplatnit sistační nebo odstraňovací nárok. Objevil-li by se tedy například anonymní urážlivý post na diskusním serveru, neměl by poškozený legální možnost, jak donutit server k jeho smazání.

Výše uvedené regulační dilema bylo nejprve řešeno v USA, přičemž mediálně nejznámějšími byly případy takzvaných peer-to-peer sítí. Jejich provozovatelé dávali svým uživatelům možnost prostřednictvím těchto sítí vzájemně sdílet multimediální soubory a sítě se tak záhy staly fórem používaným k nezákonnému šíření autorských děl. Vzhledem k tomu, že bylo pro žalobce až příliš složité stopovat desítky tisíc jednotlivých uživatelů, žalovali z titulu objektivního deliktu spočívající v porušování autorských práv provozovatele sítí.

Prvním široce medializovaným případem tohoto typu byl spor mezi sdružením vydavatelských společností a provozovatelem P2P sítě Napster²⁹⁶. Zde kladl Napster k odražení žaloby všechny možné argumenty²⁹⁷, z nichž nejdůležitějším byl argument nedostatkem spoluodpovědnosti za zásah do autorských práv. Napster se zde odvolával na dřívější rozhodnutí ve věci Sony Corp. v. Universal City Studios, Inc.²⁹⁸, kde byla předmětem sporu odpovědnost výrobce videorekordérů za to, že se prostřednictvím těchto přístrojů porušují autorská práva. Soud zde konstatoval, že producenta technologie nelze postihnout za způsob, kterým je později jeho produkt zneužit.

V případě Napster ale soud tuto argumentaci odmítl s tím, že provozovatel P2P sítě měl věrohodné a mnohdy i detailní informace o tom, že jsou prostřednictvím jeho služby porušována autorská práva a nic proti tomu nepodniknul. Byl zde použit i zajímavý ekonomický argument, kdy soud doslova uvádí, že „lze vyjít z názoru okresního soudu, že Napster neosvědčil skutečnost, že jeho systém má nějaký ekonomický význam bez toho, aby se jeho

²⁹⁶ Viz rozhodnutí A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001), plný text lze nalézt například na adrese: <http://www.ce9.uscourts.gov/web/newopinions.nsf/0/c4f204f69c2538f6882569f100616b06?OpenDocument>

²⁹⁷ V tomto směru je možné pro poučení o pobavení doporučit studium plného textu cit. rozhodnutí, kde je provedena rekapitulace argumentů obou stran. Právní zástupci Napsteru zde kromě argumentů, jež budeme dále diskutovat, předložili například i zajímavou tezi, že uživatelé sdíleli hudební soubory proto, aby se mohli lépe rozhodnout, jaké CD si pak koupí a tím Napster *de facto* prováděl žalobcům reklamu jejich produktů.

²⁹⁸ Viz rozhodnutí Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417 (1984), plný text lze nalézt na adrese http://www.law.cornell.edu/copyright/cases/464_US_417.htm.

prostřednictvím porušovala autorská práva.“ Soud i na základě tohoto zjištění dospěl k závěru, že provozovatel P2P sítě o porušování autorských práv nejen věděl, ale že taková forma užívání jeho technologie třetími osobami byla přímo součástí jeho obchodního modelu. Z tohoto důvodu tedy soud konstatoval spoluodpovědnost provozovatele P2P sítě za porušování autorských práv a nařídil Napsteru nejen blokovat přenos informací ale též nahradit škodu především ve formě části ušlého zisku za licenční poplatky.

Evropské právo se, částečně pod vlivem amerických zkušeností, vydalo cestou legislativní úpravy odpovědnosti ISP, která byla provedena směrnicí číslo č. 2000/31/ES. Do českého práva pak byly limity objektivní odpovědnosti ISP vloženy formou zákona č. 480/2004 Sb. Právo tvůrce se zde rozdělil do tří základních skupin, a to na:

- 1) provozovatele služeb spočívajících v prostém přenosu informací (*mere conduit*)
- 2) provozovatele služeb spočívajících v automatickém meziukládání (*caching*)
- 3) provozovatele služeb spočívajících v ukládání informací (*hosting*)

Mezi služby prvního typu řadíme takové, jejichž podstatou je prostý přenos dat. Jejich poskytovatelé tedy dávají k dispozici uživatelům komunikační linky, aby mohli jejich prostřednictvím realizovat datová spojení²⁹⁹. Vedle poskytovatelů služeb spočívajících ve, zjednodušeně řešeno, připojování uživatelů k internetu, se tedy jedná o provozovatele veškerých datových linek včetně páteřních sítí apod. Mezi ISP prvního typu počítáme i subjekty, jejichž služby nespočívají jen v provozování fyzické komunikační infrastruktury, ale i logických služeb, jakými jsou například instant messaging nebo IP telefonie.

Pokud bychom měli shrnout nastavení limitů pro založení odpovědnosti ISP typu *mere conduit*, můžeme konstatovat, že ISP prvního typu jsou objektivní odpovědnosti zcela zbaveni. Nelze-li totiž takovému ISP příslušnou informaci přičíst (tj. prokázat, že je jejím původcem) nebo prokázat, že volil jejího adresáta, je jeho odpovědnost prakticky vyloučena. Provozovatelé linek se tedy prakticky vůbec nemusejí obávat toho, že by vůči

²⁹⁹ Zde je třeba připomenout, že definice ISP nezahrnuje poskytovatele služeb elektronických komunikací spočívajících v hlasové telefonii.

nim mohly být vznášeny soukromoprávní nároky z titulu porušování subjektivních práv uživateli jejich služeb.

Druhým typem ISP jsou subjekty, jejichž činnost spočívá v automatizovaném meziukládání informací. Těchto služeb je často využíváno tam, kde je třeba fyzicky přiblížit informace jejich uživatelům nebo rozšířit kapacitu příslušné informační infrastruktury. Je-li tedy například určitá americká WWW stránka často navštěvována uživateli z Evropy, je výhodné zřídit její pravidelně aktualizovaný obraz (ang. *mirror*) geograficky blíže jejím uživatelům. Takovým opatřením dochází ke snížení či rozložení komunikační zátěže a předchází se tak přetížení komunikačních linek.

Limity objektivní odpovědnosti jsou u provozovatelů služeb typu *caching* obdobné jako u ISP typu *mere conduit*. Jedinou výjimkou, kdy může příslušný ISP spoluodpovídat za kvalitu automaticky meziukládaných informací, je situace, kdy objektivně dojde k porušení technických standardů v meziúložišti. Taková situace může nastat například tehdy, pokud není meziúložiště (angl. *cache*) odpovídajícím způsobem a v patřičných intervalech aktualizováno.

Nejsložitější je situace s limity objektivní odpovědnosti u ISP třetího typu, tj. u provozovatelů služeb typu hosting. Tato kategorie totiž pokrývá velkou škálu služeb od hostování www prezentací přes komunitní portály, uživatelská úložiště dat nebo webmailové služby až po služby, spočívající uživatelském ukládání bagatelních informačních objemů, jakými jsou například diskusní servery nebo osobní blogovací stránky.

Omezení (spolu)odpovědnosti provozovatelů služeb třetího typu za soukromoprávní delikty spáchané jejich uživateli je vázáno na podmínku nevědomosti příslušného ISP o protiprávním charakteru uživatelské informace. Příslušný ISP tedy za protiprávnost uživatelské informace neodpovídá pouze tehdy, pokud neví o jejím protiprávním charakteru. *A contrario* pak platí, že ISP může za protiprávnost takové informace (spolu)odpovídat tehdy, pokud se o této protiprávnosti dozví³⁰⁰.

³⁰⁰ Česká právní úprava na rozdíl od většiny států EU nepoužívá v tomto případě koncept vědomé nedbalosti, ale stanoví jako minimální podmínku nevědomou nedbalost. ISP třetího typu tedy podle českého práva odpovídá i tehdy, pokud o protiprávnosti informace nevěděl, avšak vědět měl a mohl.

Směrnice č. 2000/31/ES obecně ponechala národním právním řádům relativně velký prostor ke konkrétní úpravě limitů odpovědnosti ISP. Ve většině případů však došlo pouze ke zkopírování příslušných formulací ze směrnice do národních legislativ, v důsledku čehož zůstává pro interpretační praxi řada problematických otázek. Vzhledem k tomu, že smyslem této publikace není detailně rozebírat pozitivně právní problematiku odpovědnosti ISP, zaměříme se v dalším výkladu pouze na dva vybrané typy esenciálně důležitých služeb informační společnosti, které však stojí mimo rozsah specifické legislativy. Konkrétně se budeme zabývat institucemi doménových autorit a vyhledávačů.

9.5 DOMÉNOVÉ AUTORITY

Jako doménové autority označujeme subjekty, pod jejichž kontrolou probíhá registrace doménových jmen. Jedná se tedy o specifické subjekty, jejichž prostřednictvím využíváme při komunikaci na internetu dobře zapamatovatelného alfanumerického adresování namísto složitých číselných IP adres. Podle typu jmen, jejichž registraci kontrolují, dělíme doménové autority na:

- Národní
- Generické a
- Centrální autoritu ICANN

Od doménových autorit kontrolujících databáze doménových jmen (tzv. DNS databáze) je potřeba ještě odlišit doménové registrátory, tj. subjekty zprostředkovávající registraci doménových jmen. Činnost a postavení registrátorů se u různých domén první úrovně liší, obecně lze však říci, že se většinou jedná o podnikatele, kteří jsou v přímém kontaktu se zájemci o doménová jména a zajišťují (zprostředkovávají) pro ně příslušné registrační úkony. Zatímco doménová autorita je pro určitou doménu první úrovně jen jedna (stejně jako je jedna databáze DNS), může být registrátorů více a mohou fungovat na klasické tržní bázi.

Z hlediska odpovědnosti nás subjekty registrátorů nemusejí příliš zajímat – jejich role je totiž pouze zprostředkovatelská. Naopak doménové autority udržující databáze DNS³⁰¹ nás co do své odpovědnosti za registrovaná jména zajímat budou, neboť se jedná z definice o poskytovatele služeb informační společnosti. Význam problematiky odpovědnosti doménových autorit je přitom přímo úměrný významu doménových jmen. Poslední vývoj pak ukazuje, že doménové autority nespravují jen velké hodnoty ekonomické, ale že jejich činnost může mít dokonce dalekosáhlý politický či obecně společenský dopad³⁰².

Pro obecné vyřešení otázky odpovědnosti doménové autority za kvalitu registrovaného doménového jména je klíčové zařazení registrace doménových jmen do tříd ISP. U doménových autorit se pak na základě aktuální judikatury nabízejí následující možnosti:

- Doménovou autoritu není možné považovat za ISP a ani neodpovídá za registraci a užívání protiprávního doménového jména
- Doménovou autoritu je možno považovat za ISP

K prvnímu názoru, tj. že doménová autorita je absolutně neodpovědná, se v současné době hlásí například italské soudy. Argumentují tím, že doménová autorita je v podstatě pouze technickým správcem rejstříku doménových jmen, jako taková nemá na registraci žádný vliv a není tedy spravedlivé činit ji odpovědnou za to, že jejich služeb někdo využije k zasahování do práv třetích osob.

V případě známém pod označením „altavista.it“, který rozhodnul Městský soud v Janově dne 17. července 1999, nebyl italský registrátor sice žalován, soud však v rámci obiter dictum vyslovil názor, že „doménová autorita je výkonným orgánem odpovědným pouze za technickou stránku registrace a údržby registrů.“

V pozdějším rozhodnutí známém jako „raccomandata.it“ se již Městský soud v Modeně v rozhodnutí ze dne 28. července 2000 přímo vyslovil k otázce odpovědnosti doménové

³⁰¹ U řady domén první úrovně je běžné, že příslušné doménové autority pověřují technickou správou registru DNS ještě další subjekt. Ten má pak, co se odpovědnosti za kvalitu registrovaných jmen týče, stejné postavení jako doménová autorita. Na úrovni centrální doménové autority je takovým subjektem Network Solutions, Inc.

³⁰² Získání vlastní národní domény představuje pro mnohé národy usilující o vlastní státnost významné politické vítězství.

autority. Na žalobu směřující proti porušiteli práv i doménové autoritě odpověděl výše uvedeným argumentem a vyloučil tak pasivní procesní legitimaci doménové autority k tomu být žalována.

Mimo tři základní kategorie ISP staví doménové autority i německé právo³⁰³. Stejně jako v italském případě je doménová autorita v podstatě neodpovědná za kvalitu registrovaných doménových jmen, nelze ji tedy žalovat ani po ní požadovat žádná plnění. Výjimku představují případy, kdy je protiprávnost doménového jména zjevná – v dostupné německé judikatuře však nelze nalézt případ, kdy by soud takovouto zjevnou protiprávnost konstatoval.

Precedenčním případem rozhodnutým Spolkovým soudem (BGH) byl případ známý pod označením „ambiente.de³⁰⁴“. Zde se vlastník ochranné známky „Ambiente“ domáhal na doménové autoritě DENIC zrušení protiprávní registrace doménového jména provedené dříve třetí osobou. Soud konstatoval, že DENIC neměl povinnost zjišťovat a prověřovat, zda registrací doménového jména nezasahuje třetí osoba do práv žalobce (a to ani poté, co mu žalobce porušení práv oznámil a doložil). Tímto rozhodnutím pak poskytnul soud pádný argument doménové autoritě ke zbavení se odpovědnosti i v dalších obdobných případech³⁰⁵.

Výše uvedené restriktivní možnosti řešení odpovědnosti doménových autorit samozřejmě nelze nemít za dostatečně argumentačně kvalitní. Je však třeba poukázat na to, že soudy v uvedených případech daly poněkud extenzivně přednost hledisku ochrany dobré víry doménové autority před ochranou subjektivních práv porušených protiprávní registrací doménového jména. Doménovou autoritu tak vnímaly nikoli jako soukromoprávní subjekt poskytující komerční službu, ale spíše jako veřejný rejstřík.

Doménová autorita sice nemá fakticky možnost kontrolovat právní kvalitu všech registrací, na druhou stranu je však právě a jen doménová auto-

³⁰³ Tento názor se objevil i v Národní zprávě k problematice odpovědnosti ISP, kterou za Německou v rámci projektu MARKT/2006/09/E zpracoval Gerald Spindler. Zpráva doposud nebyla publikována.

³⁰⁴ Případ rozhodnul BGH dne 17. 5. 2001 pod č.j. I ZR 251/99. Plný text rozhodnutí v němčině viz <http://www.jurpc.de/rechtspr/20010220.htm>.

³⁰⁵ Viz např. rozhodnutí BGH ze dne 19. 2. 2004 č.j. I ZR 82/01 (věc „kurt-biedenkopf.de“), OLG Hamburg ze dne 1. 7. 2004 č.j. 3 U 5/04 (věc „viagratip.de“) nebo OLG Frankfurt ze dne 13. 2. 2003 č.j. 6 U 132/01 (věc „viagratip.de“)

rita tím, kdo poskytuje technické zázemí pro fungování doménových jmen a jehož prostřednictvím se celý proces adresování odehrává. Vydělíme-li ji zcela z mezí právní odpovědnosti za kvalitu doménového jména, vystavujeme se nebezpečí problematické vymahatelnosti subjektivních práv v případech, kdy jejich porušitel je nedostižný.

Vyjdeme-li z pravidla, že povinnost lze soudním rozhodnutím uložit pouze účastníku řízení, docházíme k závěru, že doménové autoritě, nemá-li pasivní legitimaci k tomu být žalována, nelze v řízení žádné povinnosti ukládat. Verdikt tak musí směřovat pouze proti přímému porušiteli práv (tj. například proti cybersquatterovi) s tím, že mu je uloženo zrušit nebo převést registraci na žalobce. Žalovaný však tento úkon sám provést nemůže – technicky jej opět realizuje doménová autorita (žalobce se však za této situace nemůže domáhat přímého řešení na autoritě, ale poněkud paradoxně nepřímo prostřednictvím žalovaného).

Přístup, pro který se rozhodly německé a italské soudy, lze bez výhrad aplikovat v situaci, kdy je předmětem sporu například označení registrované v některém z rejstříků jako např. firma nebo ochranná známka. Nelze pak samozřejmě uvažovat o odpovědnosti příslušného rejstříku za to, že registroval právně vadné označení. Doménová jména však srovnání se zapsanými označeními v žádném případě nesnesou – doménová autorita je totiž soukromoprávní subjekt, registrace probíhá soukromoprávní smlouvou a z registrace nevyplývají subjektu žádná absolutní práva³⁰⁶. Máme tedy pádný důvod k tomu rozlišovat co do odpovědnosti mezi postavením veřejnoprávního rejstříku a doménové autority.

Z právního hlediska má tedy doménová autorita postavení subjektu, který na základě soukromoprávního závazku plní provozem DNS registru své smluvní povinnosti vůči držitelům³⁰⁷ doménových jmen. Z hlediska technického pak doménová autorita sama nebo zprostředkovaně poskytuje infrastrukturu třetím osobám k tomu, aby mohly realizovat informační

³⁰⁶ Uzavřením registrační smlouvy má držitel doménového jména pouze relativní právo vůči doménové autoritě na to, aby autorita zanesla jeho jméno do databáze DNS a tam jej udržovala – žádná práva vůči třetím osobám mu z registrace neplynou.

³⁰⁷ U doménových jmen nejde o držbu v pravém slova smyslu, neboť se nejedná o absolutní právo – subjekt, který si registroval doménové jméno, tedy označujeme za jeho držitele s vědomím, že toto označení je poněkud nepřesné a do určité míry i zavádějící.

výměnu v rámci informační sítě internet – tato služba pak spočívá v možnosti uložit do registru DNS informaci o doménovém jméně pod příslušnou doménou první úrovně a přiřadit jí určitou IP adresu. Ačkoli tedy lze do určité míry chápat výše citované názory německé respektive italské doktríny a justice, nelze, než konstatovat, že doménová autorita se na registraci doménového jména a jeho následném provozu technicky podílí. Z toho pak logicky vyplývá i její podíl na odpovědnosti za to, že je doménové jméno registrováno či užíváno protiprávně.

Přístup, který na rozdíl od německé respektive italské judikatury upřednostňuje ochranu práv třetích osob před protiprávní registrací doménových jmen, aplikovaly mimo jiné i české soudy. Doktrína i profesionální praxe tak nabádaly žalobce³⁰⁸, aby vedle samotného rušitele žalovali i doménovou autoritu a soudy následně uznávaly její pasivní procesní legitimaci. V české judikatuře se tak můžeme setkat s doménovými rozhodnutími, kde jsou vedle povinností ukládaných samotnému rušiteli uloženy i povinnosti druhému žalovanému, jímž je doménová autorita CZ.NIC. Je samozřejmě nadsadě, že doménová autorita nemohla v takových případech odpovídat za protiprávní registraci nebo užívání doménového jména v plném rozsahu – přiznané nároky se tak omezovaly prakticky jen na zrušení či převod registrace nebo nanejvýš na náhradu nákladů řízení.

Z tzv. doménových rozhodnutí českých soudů můžeme jmenovat například případ známý jako „ceskapojistovna.cz“³⁰⁹. Soud se zde vypořádával s argumenty doménové autority (druhého žalovaného) obdobnými těm, jímž ve shora citovaných případech přisvědčil německý BGH. Argumentaci doménové autority v řízení v prvním stupni shrnul soud následovně: „K žalobě podal své vyjádření druhý žalovaný, vyložil především své postavení při správě národní domény .cz a způsob registrace doménových jmen druhého stupně. Potvrdil tvrzení žalobce, že nekontroluje a ostatně, jak uvedl, není ani schopen kontrolovat přihlašovaná doménová jména (těch je nyní cca 190 tis. a každým dnem počet narůstá o další stovky) a prověřovat, zda neporušují práva třetích osob. Pokud by byl nucen je prověřovat, pak by také musel hodnotit - při jejich střetu s jinými právy k označení - kdo má "větší" právo k označení a právo na registraci doménového jména, to mu však zcela zjevně nepřísluší. Pak bylo třeba odpovědnost za přihlašovaná a registrovaná doménová jména ponechat

³⁰⁸ Srov. např. Polčák, R. Squatterů a jak na ně 10. PC World, ročník 2003, číslo 7-8, str. 98.

³⁰⁹ Viz rozhodnutí Vrchního soudu v Praze ze dne 10. srpna 2004 č.j. 2 Cm 290/2001-39, plný text byl zveřejněn na serveru itpravo.cz na adrese: <http://www.itpravo.cz/index.shtml?x=218427>.

na přihlašovatelích, na této zásadě jsou také založena jím vydávaná pravidla registrace doménových jmen.“

Soud již v prvním stupni této argumentaci sice částečně přisvědčil, odmítnul však žalovaného zcela zbavit odpovědnosti respektive konstatovat nedostatek jeho pasivní procesní legitimace. Odvolací soud tento závěr potvrdil a shrnul následovně: „Jiná situace je však ve vztahu k druhému žalovanému, jak soud uvedl, ten svým jednáním práva žalobce neporušil. Nebyl oprávněn – vázán vlastními pravidly registrace - odepřít prvnímu žalovanému registraci jím zvoleného doménového jména, jako soukromoprávní subjekt nemá postavení, jež by mu umožňovalo rozhodnout, zda právo registrace přihlašujícímu náleží či nikoli. Z pravidel registrace doménových jmen přitom plyne, že plnou odpovědnost za případné porušení práv třetích osob nese přihlašovatel a druhý žalovaný sám o své vůli změny ohledně držitele domény realizovat není oprávněn. Výjimkou je pouze případ upravený v pravidlech, že druhý žalovaný může zrušit registraci pro držitele na základě vykonatelného soudního rozhodnutí. Byť tedy druhý žalovaný ve vztahu k žalobci žádnou smluvní ani zákonnou povinnost neporušil, změnu registrace v osobě držitele lze dosáhnout - podle pravidel registrace - právě uložením povinnosti druhému žalovanému tuto změnu provést tak, aby jako držitel byl zapsán žalobce. Ve vztahu žalobce a druhého žalovaného proto soud uzavřel, že k odstranění protiprávního stavu - vzniklého jednáním prvního žalovaného- uvedenou povinnost realizovat změnu registrace tomuto druhému žalovanému uložil, jinak žaloba proti němu shledána jako důvodná nebyla.“

Verdikt soudu prvního stupně, který byl odvolacím soudem potvrzen, pak doménové autoritě založil povinnost převést registraci doménového jména na žalobce – doménová autorita byla tedy až do konce vzata jako účastník řízení na žalované straně a důsledkem její odpovědnosti byla povinnost změnit záznam v registru DNS³¹⁰. Soud tuto část výroku rozhodnutí odůvodnil následovně: „Žalobce měl volbu ve způsobech, jimiž bylo možno dosáhnout odstranění vzniklého závadného stavu. Bylo možno žádat uložení povinnosti prvnímu žalovanému, aby provedl příslušné úkony dle platných pravidel registrace, jež by vedly k následnému převodu doménového jména na žalobce. Za stavu, kdy účastníkem řízení vedle porušovatele práva byl i druhý žalovaný - tedy registrátor, bylo možno však i žádat, aby - podle daných smluvních podmínek - změnu v registraci učinil přímo druhý žalovaný, bez dalších úkonů (návrhu) ze strany prvního žalovaného. Pokud žalobce tento naposled zmíněný postup v žalobě navrhl a současně byla - a to je zcela nezbytný předpoklad - v řízení zjištěna odpovědnost stávajícího držitele doménového jména za vzniklý protiprávní stav, rozhodnutí soudu prvního stupně, jež tomuto návrhu vyhovělo, nelze vytknout pochybení.“

³¹⁰ Verdikt, jímž soud přikázal doménové autoritě „převést“ doménové jméno z prvního žalovaného na žalobce, vzbudil v právní doktríně bouřlivou diskusi. Z odmítavých názorů viz např. Aujezdský, J. Rozsudek ohledně domény ceskapojistovna.cz. Co je špatně? Ipravo.cz, 26. 1. 2005. Z kladných komentářů viz např. Polčák, R. Nekalosoutěžní agrese na internetu. Právní rozhledy, roč. 13, číslo 13, str. 475. Komentátoři se však ani v tomto případě nerozházeli v názoru na to, zda je správné pasivně legitimovat doménovou autoritu jako druhého žalovaného.

V četných debatách, které se u nás na téma odpovědnosti doménové autority vedly, zazníval opakovaně výše citovaný a dlužno dodat že i relevantní argument samotného CZ.NIC jeho dobrou vírou. Není totiž zřejmé spravedlivé³¹¹ činit doménovou autoritu odpovědnou (ukládat jí autoritativní povinnosti a nechat ji například hradit byť i jen vlastní náklady řízení) v situaci, kdy její činnost je masová, automatická a autonomně prakticky nekontrolovatelná. Tento argument je přitom v podstatě tentýž jako argumenty, které vedly nakonec k přijetí legislativy omezující obecně odpovědnost ISP (viz výše podkapitola o důvodech k omezení odpovědnosti ISP). Z toho pak vyplývá interpretační závěr, že legislativa omezující odpovědnost ISP by se měla vztahovat i na doménové autority a podobně jako u ostatních poskytovatelů služeb informační společnosti je do určité míry zbavovat odpovědnosti.

Opět odchylně od německé a italské praxe se tedy domníváme, že doménová autorita je poskytovatelem služeb informační společnosti ve smyslu čl. 1(2) směrnice č. 98/34/ES ve znění směrnice č. 98/48/ES. V této souvislosti pak zbývá ještě určit, o jaký typ ISP se v tomto případě jedná. Vzhledem k tomu, že činnost doménových autorit spočívá v ukládání uživatelských jmen do databází DNS, domníváme se, že je lze zařadit do kategorie ISP třetího typu ve smyslu čl. 14 směrnice č. 2000/31/ES. V českém právu to pak znamená, že můžeme národní doménovou autoritu CZ.NIC rovněž považovat za ISP třetího typu a vztahuje se na ni omezení odpovědnosti v rozsahu daném § 5 zákona č. 480/2004 Sb.

Můžeme tedy v této části uzavřít konstatováním, že doménová autorita je ze zákona zbavena objektivní odpovědnosti za kvalitu doménových jmen registrovaných třetími osobami. Její spoluodpovědnost lze pak založit podobně jako u ostatních ISP třetího typu až tím, že ji informujeme o protiprávním charakteru informace (doménového jména) uložené na její infrastruktuře (v registru DNS). K založení spoluodpovědnosti doménové autority za doménové jméno tedy dojde až splněním podmínek stanovených pro ISP třetího typu, nejčastěji tedy na základě oznámení o protiprávnosti informace (tzv. notice).

³¹¹ Tohoto termínu zde užíváme záměrně s odkazem na spravedlnostní cit – z hlediska pozitivního práva je spravedlnostní hodnocení objektivní odpovědnosti samozřejmě irelevantní.

9.6 VYHLEDÁVAČE

Existuje celá řada služeb informační společnosti, které přímo nespádají pod rozsah evropské ani národní úpravy omezující odpovědnost ISP³¹². Pro jejich provozovatele to znamená relativní nejistotu ohledně toho, do jaké míry mohou spoluodpovídat za protiprávní jednání, kterých se prostřednictvím jejich služeb mohou dopouštět třetí osoby. Vzhledem k tomu, že v takových případech prakticky nelze na základě zákona předvídat míru a formu založení spoluodpovědnosti, budeme se v následujícím výkladu držet prakticky pouze interpretačních závěrů učiněných soudy.

Jednou z nejvýznamnějších služeb spadajících mimo zákonnou definici ISP jsou internetové vyhledávače. Jejich důležitost je v současné době neoddiskutovatelná a slova jako ‘to google’ (česky něco jako ‘googlovat’ či dokonce ‘gūglovat’), která označující hledání v internetu za pomoci vyhledávače, se dokonce již stala součástí standardního jazyka. V mnoha případech je vyhledávač jediným způsobem, jak se dostat ke kýžené informaci. O to více pak překvapí, že se vyhledávače a jejich činnost nedostaly do hledáčku při přípravě evropské ani národních právních úprav³¹³.

Z hlediska důležitosti hrají vyhledávače významnou roli při veřejné prezentaci informací prostřednictvím www. Vedle umístění samotné informace na síť je totiž přinejmenším stejně důležité informovat o ní potenciální zájemce – v tom pak hrají vyhledávače nezastupitelnou roli³¹⁴. Kvůli jejich faktické důležitosti a nezastupitelnosti tedy můžeme logicky formu-

³¹² Vyhledávače sice spadají pod obecnou definici ISP, nelze je však již zařadit do žádné ze tří základních kategorií, a proto se na ně prakticky nevztahuje příslušná legislativa.

³¹³ V Německu se k této otázce vedla relativně bohatá diskuse. Přesto se nakonec právo tvůrce k myšlence legislativní úpravy postavení ISP nepřiklonil – viz stanovisko Spolkové vlády (Gegenäußerung der Bundesregierung), BT-Drucks, číslo 14/6098, str. 37, k dispozici on-line na adrese

http://www.gesetzesportal.de/jportal/docs/news_anlage/NLIT/pdf/1406098.pdf.

³¹⁴ Důležitost subjektů a služeb, které nám podle našeho zadání filtrují dostupné informace, bude s rostoucí informační nabídkou zřejmě dále stoupat. V této souvislosti se objevují první vize společnosti, kde ústřední roli hraje právě informační filtr (někdy se v této souvislosti používá termín postmoderní knihovnik) – viz např. Wigell-Ryyänen, B. Ensuring Citizenship, in the Knowledge Society, in KnowRight 2006. Wien: Österreichische Computer Gesellschaft, 2006, str. 139.

lovat hypotézu, že vyhledávače spoluodpovídají za zveřejnění příslušných informací prostřednictvím *www*. Postačí nám k tomu jednoduchý negativní test – nebýt jich, uživatelé by se k příslušným informacím často vůbec nedostali.

Argumentem proti odpovědnosti vyhledávačů by mohl být, jako už jsme si ukázali mnohokrát, poukaz na to, že jejich činnost je automatická a jejich provozovatelé nemohou technicky kontrolovat obsah cílových adres, na které vedou automaticky generované odkazy. Je tedy nespravedlivé činit vyhledávač odpovědným za to, že někdo využije jeho automatizovaných služeb k přilákání uživatelů na svůj nelegální informační obsah.

Jak bylo uvedeno výše, představují vyhledávače z hlediska klasifikace ISP interpretační problém. O jasném zařazení provozovatele vyhledávače do kategorie ISP tedy můžeme hovořit pouze v případě, kdy je příslušný odkaz kompletně, tj. včetně popisu, dodán třetí stranou (nejčastěji provozovatelem cílové *www* prezentace). V takovém případě funguje vyhledávač jako ISP třetího typu, neboť jsou prostřednictvím jeho služby ukládány a zpřístupňovány informace dodané uživateli. Problém však spočívá v tom, že pouze na takové bázi žádný z významnějších vyhledávačů nepracuje – jejich model je tak postaven na kombinaci komerčních odkazů dodaných třetí stranou (většinou zadavatelem reklamy) s odkazy generovanými vlastními sofistikovanými vyhledávacími algoritmy. I u odkazů dodaných třetí stranou se pak vyhledávání neděje jen na základě předem zadaných požadavků, ale automaticky dle vyhledávacího algoritmu. Z tohoto důvodu, jak bylo ostatně uvedeno výše, nemohou vyhledávače spoléhat na obecné zbavení odpovědnosti legislativou upravující postavení ostatních ISP.

Otázku toho, zda lze na vyhledávače uplatnit alespoň analogicky odpovědnostní režim ISP, řešil mezi jinými i Zemský soud v Berlíně³¹⁵. Výsledek jeho interpretace byl jednoznačný: činnost vyhledávačů se činnosti ostatních ISP zahrnutých do tří základních skupin

³¹⁵ Viz rozhodnutí LG Berlin ze dne 9.9.2004, č.j. 27 O 585/04. Podobně rozhodovaly i soudy v dalších případech, např. LG Berlin, 22.2.2005, 27 O 45/05, LG Berlin, 9.9.2004, 27 O 585/04, nebo LG Hamburg, 16.9.2004, 315 O 755/03. Přehled německé judikatury k problematice internetových vyhledávačů je možné nalézt na portále www.linksandlaw.de na adrese

<http://www.linksandlaw.de/Urteile-suchmaschinen-suchmaschinenoptimierung.htm>.

podobá jen částečně. Proto není možné na vyhledávače bez dalšího analogicky uplatnit režim zbavení odpovědnosti podle speciální legislativy.

Jiný, mediálně mnohem známější případ, se týkal on-line aukční platformy a vyhledávače provozované společností Yahoo! Inc. Tento portál zprostředkovával aukce předmětů s nacistickou tematikou a rovněž umožňoval vyhledávat na internetu nacistické www stránky. Spor řešený nejprve francouzskými³¹⁶ a posléze i americkými³¹⁷ soudy bývá komentován především v souvislosti s problematikou internetové jurisdikce nebo svobody projevu. Hodí se však velmi dobře i pro ilustraci konceptu odpovědnosti ISP. Francouzské soudy v tomto případě konstatovaly následující skutečnosti:

Na internetu dochází k obchodování s nacistickými artefakty a k propagaci nacismu formou www stránek

K nacistickým předmětům i stránkám je možné se jednoduše dostat prostřednictvím služeb Yahoo! Inc.

Yahoo! Inc. spoluodpovídá za to, že je prostřednictvím jeho služeb porušováno právo a má povinnost takovému jednání zabránit.

Skutečnost, že rozhodnutí Pařížského odvolacího soudu nebylo nikdy uznáno a vykonáno v USA přitom neznamená, že by na odpovědnost provozovatelů vyhledávačů měly americké soudy jiný názor. Je to jen výraz odlišných kulturně-právních tradic, přičemž v USA se propagace nacismu považuje za realizaci práva na svobodu projevu a prodej předmětů s nacistickou tematikou za realizaci práva na vlastnictví. Americký soud tedy neměl důvod uznat a vykonat rozhodnutí, kterým by zasáhl do výkonu (v porovnání s Evropou jinak pojímaných) základních práv na svém území³¹⁸.

Přestože vyhledávače nespádají pod „ochranu“ ustanovení speciální legislativy pro omezení odpovědnosti ISP, nelze rozhodně říci, že bychom v souvislosti s nimi mohli hovořit o plné spoluodpovědnosti nebo snad dokonce o výlučné odpovědnosti za obsah cílových www stránek. Přestože u nás v tomto směru neexistuje odpovídající judikatura, můžeme předpokládat, že i v našem právním prostředí se soudy vydají cestou interpretace příslušných ustanovení odpovědnostních předpisů, která zohlední jejich *ratio legis* (tj. smysl a účel). I bez aktivity právo tvůrce tedy můžeme oče-

³¹⁶ Viz rozhodnutí Tribunal de Grande Instance de Paris ze dne 20. 11. 2000, UEJF et Licra c/ Yahoo! Inc. et Yahoo France, plný text rozhodnutí ve francouzštině viz <http://www.juriscom.net/txt/jurisfr/cti/tgiparis20001106-rp.htm>.

³¹⁷ Viz rozhodnutí 145 F. Supp. 2d 1168 (N.D. Cal. 2001), kterým bylo vyhověno návrhu na odepření uznání a výkonu francouzského rozsudku v USA. Rozhodnutí je k dispozici on-line na adrese http://eric_goldman.tripod.com/caselaw/yahoovlicranov2001.htm.

³¹⁸ K případu a jeho ústavně-právním souvislostem viz např. Reindemberg, J. L. Yahoo and Democracy on the Internet. *Jurimetrics*, číslo 42, str. 261 a násl.

kávat, že se v otázce odpovědnosti vyhledávačů vyvine standard rozumné interpretace příslušných obecných předpisů, který zamezí tomu, aby se z vyhledávačů stali jacísi otloukánci či dojné krávy kohokoli, jehož práva jsou někde na internetu porušována³¹⁹.

Z dosavadních rozhodnutí různých soudů v evropských státech můžeme dovodit podobný přístup k vyhledávačům jako k ISP třetího typu. Vyhledávače tak byly jen zřídka shledány odpovědnými za zprostředkování informací o protiprávních *www* stránkách, pokud o protiprávním obsahu stránek neměly povědomí. Až na několik výjimečných případů se tak evropské soudy i v otázce tzv. objektivní odpovědnosti (např. v případě zásahu do autorských práv) kloní k takové interpretaci příslušných ustanovení obecných předpisů, která *de facto* omezuje odpovědnost vyhledávačů jen na situace, kdy jejich provozovatelé věděli o tom, že se lze jejich prostřednictvím dostat k protiprávnímu obsahu nebo to vzhledem k okolnostem vědět měli a mohli.

Můžeme tedy k otázce odpovědnosti internetových vyhledávačů uzavřít, že chybějící legislativa byla (a v České republice pravděpodobně ještě bude) doplněna racionální a teleologickou interpretací obecných právních norem, která i pro vyhledávače postupně zavádí stejný odpovědnostní režim, jaký mají ISP třetího typu. Budeme-li tedy chtít činit vyhledávač odpovědným za to, že nabízí přesměrování na *www* stránky s protiprávním obsahem, bude nejprve jeho provozovatele o protiprávním jednání náležitě informovat.

Vzhledem k tomu, že speciální legislativa na odpovědnost vyhledávačů nedopadá a česká judikatura zatím chybí, bude však každopádně třeba se alespoň v prvních případech připravit na obtížnou argumentaci a na procesy s relativně nejistým výsledkem. Tato dočasná obtíž je však běžná a tím i do značné míry omluvitelná vždy, když v obdobně skutkově specifických případech dochází k postupnému nalézání spravedlnosti.

³¹⁹ Jako odstrašující příklad může v tomto směru posloužit rozhodnutí Pekingského civilního soudu, který v rámci tažení proti internetovému hudebnímu pirátství přisoudil vydavatel-ským společnostem odškodné ve výši v přepočtu 27.000 USD za to, že vyhledávač Yahoo zprostředkoval linky na stránky s nelicencovanou hudbou. Rozhodnutí není dosud pravomočné (žalovaný se proti němu odvolal). O případu informoval zpravodajský server CNN na adrese http://english.people.com.cn/200704/25/eng20070425_369413.html.

LITERATURA

- Akehurst, M. Jurisdiction in International Law, in *British Yearbook of International Law*. London: Oxford University Press, 1972-1973, str. 179.
- Alexy, R. On the Structure of Legal Principles, *Ratio Iuris*, ročník 13, číslo 3, str. 1.
- Arnold, R. A. Efficiency vs. Ethics: Which is the Proper Decision Criterion in Law Cases?, *The Journal of Libertarian Studies*, ročník 6, číslo 1, str. 49.
- Asimov, I. I, Robot. Oxford: Oxford University Press, 2000.
- Asimov, I. Já, robot. Praha: Triton, 2004.
- Aujezdský, J. Rozsudek ohledně domény ceskapojistovna.cz. Co je špatně? *Itpravo.cz*, 26. 1. 2005.
- Awoyemi, B. Zippo is dying, should it be dead? The exercise of personal jurisdiction by U.S. federal courts over non-domiciliarily defendants in trademark infringement lawsuits arising out of cyberspace. *Marquette Intellectual Property Law Review*, ročník 9, číslo 1, str. 37.
- Berge, G. W. The Case of the S. S. Lotus. *Michigan Law Review*, roč. 26, číslo 4, str. 361.
- Bernam, P.S. The Globalization of Jurisdiction. *University of Pennsylvania Law Review*, číslo 151, str. 417.
- Bettinger, T., Thum, D. Territorial Trademark Rights in the Global Village - International Jurisdiction, Choice of Law and Substantive Law for Trademark Disputes on the Internet. *IIC*, číslo 31, str. 166.
- Bix, B. Legal positivism (Working Paper). Minnesota: University of Minnesota Law School, 2000.
- Blue, L. Internet and Domain Name Governance: Antitrust Litigation and ICANN. *Berkeley Technology Law Journal*, roč. 19, číslo 1, str. 387.
- Bobbitt, P. Terror and Consent. New York: Alfred A. Knopf, 2008.

- Bogdan, M. Internet and Private International Law. In Polčák R. a kol. Introduction to ICT Law (selected issues). Brno: Masarykova univerzita, 2007, str. 22.
- Bogdan, M. Torts in Cyberspace: The Impact of the New Regulation Rome „II,“ MUJLT, roč. 2, číslo 1, str. 2.
- Bomse, A. L. The Dependence of Cyberspace. Duke Law Review, číslo 50, str. 1717.
- Boura, F. K otázce výkladu zákonů. Právník, roč. 88, č. 7-8, str. 297.
- Boyle, J. Shamans, Software and Spleens. Cambridge: Harvard University Press, 1996.
- Brenner, S. W. Cybercrime Metrics: Old Wine, New Bottles? Virginia Journal of Law and Technology, roč. 9, číslo 13, str. 1.
- Brenner, S. W., Koops, B.-J. Approaches to Cybercrime Jurisdiction. Journal of High Technology Law, roč. 4, číslo 1, str. 19.
- Brunori, D. The Politics of State Taxation: Saving the Internet from the Taxman. State Tax Notes, roč. 29, číslo 6, str. 1.
- Bublávková, J. Automatizovaný systém pracovnoprávných informací a možnosti jeho využitia v právnej teórii a praxi. Právník, roč. 123, č. 5, str. 450.
- Bulín, H. Konstrukce pojmu „právních pramenů“ vůbec a pramenů římského práva zvláště z hlediska ryzí nauky právní, in Weinberger, O., Kubeš, V. (eds.) Brněnská škola právní teorie. Praha: Karolinum, 2003, str. 169.
- Burgin, M. Information Theory: a Multifaceted Model of Information, Entropy, číslo 5, 2003, str. 146.
- Cejpek, J. Automatizované vyhledávání informací z českých a slovenských textů právních dokumentů. Právník, roč. 120, č. 4, str. 360.
- Chandler, Jennifer A. Security in Cyberspace: Combatting Distributed Denial of Service Attacks, University of Ottawa Law & Technology Journal, číslo 1, str. 231.
- Chi-ang Lin, B. A New Vision of the Knowledge Economy, Journal of Economic Surveys, ročník 21, číslo 3, str. 553.
- Cohen, J. E. DRM an Privacy. Berkeley Technology Law Journal, roč. 18, číslo 3.

- Cohen, J.E. Examined Lives: Informational Privacy and the Subject as an Object, *Stanford Law Review*, číslo 52, str. 1373.
- Colotková, Z. Rozvoj automatizovanéj sústavy justičnej informatiky. Socialistické súdnictvo, roč. 37, č. 9, str. 1.
- Cooter, R. D. Liberty, Efficiency and Law. *Law and Contemporary Problems*, ročník 50, číslo 4, str. 141.
- Cosson, J.-B. Standard Private International Law Tested by the Networks. In *Internet International Law*, ed. Georges Chatillon. Bruxelles: Bruylant, 2005, str. 53.
- Coveney, P., Highfield, R. Mezi chaosem a řádem. Praha: Mladá Fronta, 2003.
- De Vel, G. The Convention on Cybercrime, in *Internet International Law*, ed. Georges Chatillon. Bruxelles: Bruylant, 2005, str. 225.
- Devillard, A. Zeturf.com contre PMU, les paris judiciaires sont ouverts. *01net.com*, 13. 7. 2005
- Dickstein, M. Pragmatism Then and Now, in *Revival of Pragmatism*, ed. Dickstein, M. London: Duke University Press, 1998, str. 1.
- Drahos, P., Braithwaite, J. *Information Feudalism – Who Owns the Knowledge Economy?* New York: New Press, 2007.
- Dworkin, R. *Law's Empire*. Oxford: Hart Publishing, 1998.
- Dworkin, R. M. Když se práva berou vážně. Praha: OIKOYMENH, 2001.
- Dworkin, R. Non-Neutral Principles, *The Journal of Philosophy*, ročník 74, číslo 14, str. 491.
- Engliš, K. Kritika normativní teorie, in *Brněnská škola právní teorie*. Praha: Karolinum, 2003, str. 203 a násl
- Forder, J., Svantesson, D. *Internet and e-Commerce Law*. South Melbourne: Oxford University Press, 2008.
- Fuller, L. L. *Morálka práva*. Praha: OIKOYMENH, 1998.
- Galindo, F. A. Code of Practice for the Globalisation of Electronic Commerce and Government. *Journal of Information, Law and Technology*, číslo 1.
- Gillespie, T. *Wired Shut – Copyright and the Shape of Digital Culture*. Cambridge: MIT Press, 2007.

- Goldsmith, J. L. Against Cyberanarchy. *Chicago Law Review*, číslo 65, str. 1250.
- Grand, S. *Creation – Life and How to Make it*. Cambridge: Harvard University Press, 2001.
- Greenleaf, G. An Endnote on Regulating Cyberspace: Architecture vs. Law? *University of New South Wales Law Review*, ročník 21, číslo 2, str. 603.
- Griffin, J. *Value Judgment – Improving Our Ethical Beliefs*. Oxford: Clarendon Press, 1997.
- Guadamuz, A. The Digital Divide: It's the Content, Stupid! *Computer and Telecommunications Law Review*, číslo 304, str. 73.
- Hafner, K. The Epic Saga of the Well. *Wired*, čís. 5.05, str. 98 a násl.
- Harper, J. Against ISP Liability. *Regulation*, číslo 1/2005, str. 31.
- Harvánek, J. a kol. *Teorie práva*. Plzeň: Aleš Čeněk, 2008.
- Hegel, G.W. *Základy filosofie práva*. Praha: Academia, 1992.
- Hobbes, T. *Leviathan*. Project Gutenberg, 2002.
- Hol, A., Loth, M. *Reshaping Justice- Judicial Reform and Adjudication in the Netherlands*. Maastricht: Shaker Publishing, 2004.
- Holländer, P. *Filosofie práva*. Plzeň: Aleš Čeněk, 2006.
- Hume, D. *A Treatise on Human Nature*. Project Gutenberg, 2003.
- Johnson, D. R., Post, D., G. *Law and Borders: The Rise of Law in Cyberspace*. *Stanford Law Review*, číslo 48, str. 1367.
- Katyal, K. Digital Architecture as Crime Control. *Yale Law Journal*, číslo 112, str. 2261.
- Katz, A. W. *Is electronic contracting different?* New York: Columbia University, 2004.
- Kelsen, H. *Všobecná teorie norem*. Brno: Masarykova univerzita v Brně, 2000.
- Kerr, O. S. Virtual Crime, Virtual Deterrence: A Skeptical View of Self-Help, Architecture, and Civil Liability', *Journal of Law, Economics & Policy*, roč. 1, číslo 1, str.1.

- Kleinwächter, W. From Self-Governance to Public-Private Partnership: The changing Role of governments in the Management of the Internet's Core Resources. *Loyola of Los Angeles Law Review*, číslo 36, str. 1103.
- Kleve, P. De Mulder, R. Cod is Murphy's Law. In *Cyberspace 2005*. Brno: Masarykova univerzita, 2006, str. 11.
- Knapp, V. O možnosti použití kybernetických metod v právu. Praha: Nakladatelství Československé akademie věd, 1963.
- Knapp, V. *Právo a informace*. Praha: Academia, 1988.
- Kohl, U. Eggs, Jurisdiction and the Internet. *International and Comparative Law Quarterly*, číslo 52, str. 577.
- Kohl, U. *Jurisdiction and the Internet*, Cambridge: Cambridge University Press, 2007.
- Kühn, Z. Jak Zlepšit české právní informační systémy? Jiné právo, jina-pravo.blogspot.com, 23. 2. 2008.
- Kühn, Z. Může absence publikace úplného znění zákona odůvodnit jeho protiústavnost? Jiné právo, on-line, jinepravo.blogspot.com, 25. 11. 2007.
- Kühn, Z., Bobek, M., Polčák, R. *Judikatura a právní argumentace*. Praha: Auditorium, 2006.
- Kur, A. Identical Marks Belonging to Different Owners in Different Countries. (How) Can They Coexist in Cyberspace? *The Journal of World Intellectual Property*, ročník 3, číslo 2, str. 307.
- Lasser, M. Anticipating Three Models of Judicial Control, Debate and Legitimacy: The European Court of Justice, the Cour de cassation and the United States Supreme Court, Jean Monet Working Paper 1/03, NYU School of Law, New York, 2003.
- Lasser, M. *Judicial Deliberations: A Comparative Analysis of Transparency and Legitimacy*. Oxford: Oxford University Press, 2004.
- Lessig, L. *Code V.2*. New York: Basic Books, 2006.
- Lessig, L. Constitution and Code. *Cumberland Law Review*, ročník 27, číslo 1, str. 3.
- Lessig, L. *Free Culture*. New York: The Penguin Press, 2004.

- Lessig, L. *The Future of Ideas – The Fate of the Commons in a Connected World*. New York: Vintage Books, 2002.
- Lévy, P. *Becoming Virtual – Reality in the Digital Age*, New York, Plenum Trade, 2002.
- Lévy, P. *Cyberculture*. London: University of Minnesota Press, 2001.
- Lindworsky, S. J. Příčinné myšlení u primitivního člověka. *Filosofická revue*, roč. 1929, č. 1, str. 13.
- MacCormick, N. *Institutions of Law*. New York: Oxford University Press, 2008.
- Mara, A. Norm Origin and development in Cyberspace: Model of Cybernorm Evolution, *Washington University Law Quarterly*, číslo 78, str.
- Marchand, M.-J. Quand Zeturf se moque des monopoles. *Droit-NTIC.com*, 3. 7. 2006.
- Mařík, V. Štěpánková, O. Lažanský, J. *Umělá inteligence*, 1. díl. Praha: Academia, 1993.
- Mates, P., Smejkal, V. *E-government v českém právu*. Praha: Linde, 2006.
- Molek, P. Přežije nás anonymizace? In *Jiné právo offline*, Praha: Auditorium, str. 227.
- Naso, P. O. *Proměny, přel. Ferdinand Stiebitz*. Praha: Státní nakladatelství krásné literatury, hudby a umění, 1958.
- Neff, V. *Filozofický slovník pro samouky*. Praha: Mladá fronta, 1993.
- Nöel, J.-W. Internet and Judicial Investigation. In *Internet International Law*, ed. Georges Chatillon. Bruxelles: Bruylant, 2005 str. 233.
- Oskamp, A. Lodder, A. R. Apistola, M (eds.) *IT Support of the Judiciary*. Den Haag: Asser Press, 2004.
- Paterson, M. Following the Right Lead: Gutnick and the Dance of Internet Jurisdiction. *Canadian Journal of Law and Technology*, roč. 4, číslo 1, str. 49.
- Plays, J. Internet and Judicial Investigation: Difficulties in Judicial Practice, in *Internet International Law*, ed. Georges Chatillon. Bruxelles: Bruylant, 2005, str. 245.
- Polčák, R. Elektronické podatelny a jejich technologická neutralita, *Veřejná správa*, ročník 17, číslo 25, str. 10.

- Polčák, R. In Law, We Trust: Shortly to Bumblebees and the Normativity of Law in Cyberspace, in *Cyberspace 2006*, Brno, Masarykova Univerzita, 2006, str. 3.
- Polčák, R. K elektronizaci justice. *Jurisprudence*, roč. 17, číslo 6, str. 3.
- Polčák, R. Nekalosoutěžní agrese na internetu. *Právní rozhledy*, roč. 13, číslo 13, str. 475.
- Polčák, R. *Právo na internetu – Spam a odpovědnost ISP*, Brno: Computer Press, 2007.
- Polčák, R. Škop, M., Macek, M. *Normativní systémy v kyberprostoru (úvod do studia)*, Brno: Masarykova univerzita v Brně, 2005.
- Polčák, R. Some Notes on Current Paradoxes in the Law on Personal Data Protection, *Information and Communications Technology and Law*, roč. 4, číslo 6, str. 52.
- Polčák, R. Squatterři a jak na ně 10. *PC World*, ročník 2003, číslo 7-8, str. 98.
- Polčák, R. Tučňáci a webkamery – pár poznámek k legitimní a nelegitimní transparentnosti soudnictví. *Jiné právo*, jinapravo.blogspot.com, 20. 5. 2008
- Posner, R. A. *The Economics of Justice*. London: Harvard University Press, 1983.
- Post, D. *Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace*. 1996, publ. on-line na adrese http://www.cli.org/DPost /X0023_ANARCHY.html.
- Post, D. G. *Governing Cyberspace*. *The Wayne Law Review*, číslo 43, str. 155.
- Post, D.G. *Against Against Cyberanarchy*. *Berkeley Technology Law Journal*, roč. 17, číslo 1, str. 23.
- Radbruch, G. *Statutory Lawlessness and Supra-Statutory Law (1946)*. *Oxford Journal of Legal Studies*, roč. 26, číslo 1, str. 1.
- Raymond, E. S., Steele, G. L. (eds.) *Jargon File*. Project Gutenberg, 2000.
- Reed, C. *Internet Law*. Cambridge: Cambridge University Press, 2004.
- Ridley, M. *Genom*. Praha: Portál, 2001.

- Robins, K. Kyberprostor a svět ve kterém žijeme. *Revue pro média*, roč. 2003, číslo 5, str. 17.
- Rowland, D., Macdonald, E. *Information Technology Law*, New York: Routledge Cavendish, 2005.
- Salomon, J.-J. *Technologický úděl*, Praha: Filosofia, 1997.
- Samuelson, P. Five Challenges for Regulating the Global Information Society, in *Regulating the Global Information Society*, ed. Chris Marsden. London: Routledge, 2000.
- Saxby, S. The Role of Government in National/International Internet Administration, in *The Internet, Law and Society*, ed. Akdeniz, Y., Walker, C., Wall, D., Harlow: Pearson Education Limited, 2000, str. 3.
- Schjolberg, S., Hubbard, A. M. *Harmonizing National Legal Approaches on Cybercrime*. Geneva: ITU (publikace č. CYB/04). 2005.
- Schrödinger, E. *What is Life*. Cambridge: Cambridge University Press, 1992.
- Sehnálek, D. *Mezinárodněprávní aspekty regulace e-commerce*. Disertační práce, Brno: Masarykova univerzita, 2006.
- Slováková, Z. Protection of trademarks and the Internet with respect to the Czech law. *Journal of International Commercial Law and Technology*, ročník 2, číslo 1, str. 73.
- Smejkal, V. a kol. *Právo informačních a telekomunikačních systémů*. Praha: C.H. Beck, 2004.
- Smejkal, V., Švestka, J. Odpovědnost za škodu při provozu informačního systému, aneb nemalujeme čerty na zeď. *Právní rozhledy*, roč. 13, číslo 19, str. 719.
- Sobel, L. S. DRM as Enabler of Business Models: ISPs as Digital Retailers, *Berkeley Technology Law Journal*, roč. 18, číslo 3.
- Solomon, J. J. *Technologický úděl*. Praha: Filosofia, 1997.
- Škop, M. Hranice práva a kyberprostoru - Subverzivita kyberprostoru. *Právník*, roč. 144, číslo 5, str. 1157.
- Štědroň, B., Hlaváč, L. New Cyberspace Managers in the Year 202, *MUJLT*, ročník 2, číslo 1, str. 119.

- Steiner, V. Logická formalizace právních norem a vztahů. *Právník*, ročník 124, 1985, číslo 11, str. 1008.
- Stoljarov, V., Kannegiesser, K. H. K niektorým filozofickým otázkam kybernetiky. *Otázky marxistickej filozofie*, roč. 18, č. 1, str. 57.
- Štraus, J. Vymahateľnosť práva. *pravnicaradce.ihned.cz*, 28. 6. 2006.
- Sullivan, J. W. N. *The Limitations of Science*. Clifton: Augustus M. Kelley Publishers, 1973.
- Svantesson, D. *Private International Law and the Internet*, Alpen aan den Rij: Kluwer Law International, 2007.
- Thomas, D. Criminality on the Electronic Frontier. In *Cybercrime*, ed. Thomas, D., Loader, B. D. London: Routledge, 2003, str. 17.
- Verheij, B. *Virtual Arguments*. The Hague: T.M.C. Asser Press, 2005.
- Vermuele, A. The Judiciary is a They, not an It: Two Fallacies of Interpretive Theory, *The University of Chicago Public and Legal Theory Working Paper No. 49*, 2003.
- Wiener, N. *Cybernetics: Or the Control and Communication in the Animal and the Machine*. Cambridge: MIT Press, 1961.
- Wigell-Ryyänen, B. Ensuring Citizenship, in the Knowledge Society, in *KnowRight 2006*. Wien: Österreichische Computer Gesellschaft, 2006, str. 139.
- Wilhelm, A. *Digital Nation – Towards an Inclusive Information Society*, Cambridge: The MIT Press, 2004.
- Wojciechowski, B. *Dyskrecjonalność Sedziowska*. Toruń: MADO, 2004.
- Yokoyama, D. T. You Can't Always Use the Zippo Code: The Fallacy of a Uniform Theory of Internet Personal Jurisdiction. *DePaul Law Review*, číslo 54, str. 1146.
- Zlatuška, J. *Informační společnost*. Zpravodaj ÚVT MU, ročník 8, číslo 4, str. 1.
- Zweigert, K., Kötz, H. *An Introduction to Comparative Law*. New York: Oxford University Press, 1998.

VĚCNÝ REJSTŘÍK

A

advokacie, 131
Ambiente.de (případ – Německo),
179
anarchie, 33
archiv, 22
Asimov, Isaac, 53
audiovizuální záznam, 141
autentizace, 117
automat, 29, 30, 90
autorita, 32, 33, 82, 89, 148, 160,
161, 164, 177, 178, 179, 180, 181,
182, 183
autorské právo, 101, 152, 153

B

banánová jurisdikce, 66
Bangemannova zpráva, 97
Barlow, John Perry, 36, 40
Bentham, Jeremy, 109, 111, 115
bezpečnost, 99, 105, 106, 137
Brokat.de (případ – Francie), 73

C

caching, 175, 176
celulární automat, 29, 30
ceskapojistovna.cz (případ – ČR),
181
cracker, 163
cybersquatter, 180
CZ.NIC, 181, 183

D

daň, 80, 103
datová schránka, 117, 118, 119, 122
definiční autorita, 150, 151, 154,
159, 160, 161, 162, 164, 165, 166
definiční norma, 147, 153, 154, 157
Deklarace nezávislosti
kyberprostoru, 36, 38
delikt, 70, 71, 153, 171, 174, 176
delimitace, 65, 66, 67, 68, 69, 80
delokalizace, 55, 56, 57, 60, 67, 71
dezorganizace, 15
diskusní server, 153, 154, 160, 162,
168, 174, 176
distanční kontrakt, 56
DNS, 177, 178, 180, 181, 182, 183
doménová autorita, 82, 161, 164,
177, 178, 179, 180, 181, 182, 183
domicil, 71, 83, 84, 85, 86, 87
doručování, 11, 114, 115, 116, 117,
118, 119, 123, 125, 134, 139, 140
DRM (digital rights management),
152
držitel doménového jména, 180, 182
důkaz, 22, 24, 54, 60, 62, 64, 65, 67,
75, 92, 116, 135, 136
duševní vlastnictví, 72, 99, 101, 106,
171

E

eEurope, 98
efektivita, 34, 103

eJustice, 126, 143
 Electronic Frontier Foudation, 36
 elektronický podpis, 116, 121, 122,
 133, 139
 elektronizace, 118, 128, 132, 135,
 136, 137, 139, 141, 143, 144
 e-mail, 57, 116, 121, 122, 149, 168,
 170
 Engliš, Karel, 145, 146
 entropie, 10, 11, 13, 14, 15, 16, 17,
 18, 27, 31, 33, 34, 89, 91, 92, 94,
 164
 Eurojust, 143

F

fikce, 111, 114
 filtr, 153, 154
 formalismus, 18, 20, 52, 79
 freemail, 172
 fuzzy logika, 23, 42
 fyzická osoba, 70, 117, 118, 161,
 164, 169

G

Game of Life, 30
 Google, 184
 Grundnorm, 150
 Gutnick (případ - Austrálie), 72, 73

H

hacker, 61, 152, 153, 162, 163, 165,
 173
 hosting, 160, 168, 172, 173, 175
 hraniční určovatel, 59, 60, 68, 69,
 71, 76, 78, 81, 83, 86
 Hume, David, 11, 16

Humova teze, 11, 16
 hybridní pošta, 140

Ch

chaos, 9, 11, 33, 164

I

ICANN (Internet Corporation for
 Assigned Names and Numbers),
 161, 162, 177
 individuální právní akt, 114, 115,
 117, 118, 119, 164
 informace, 9, 10, 13, 15, 16, 17, 18,
 19, 21, 22, 25, 26, 28, 29, 32, 33,
 34, 35, 42, 43, 44, 48, 49, 53, 57,
 71, 74, 75, 77, 82, 88, 89, 90, 91,
 92, 94, 95, 97, 104, 108, 113, 114,
 115, 124, 126, 131, 134, 141, 156,
 164, 167, 168, 169, 171, 174, 176,
 183, 184, 185
 informace veřejného sektoru, 101
 informační síť, 34, 38, 39, 41, 55,
 56, 59, 69, 71, 81, 84, 86, 90, 92,
 111, 116, 146, 147, 148, 150, 151,
 153, 155, 164, 166, 167, 173, 181
 informační společnost, 12, 55, 56,
 57, 66, 71, 77, 89, 90, 91, 92, 93,
 94, 95, 96, 97, 98, 99, 100, 101,
 102, 103, 104, 105, 106, 107, 108,
 115, 117, 119, 120, 121, 123, 125,
 126, 145, 154, 155, 156, 159, 165,
 166, 167, 168, 169, 171, 172, 177,
 178, 183, 184
 informační technologie, 47, 90, 93
 informační teorie práva, 23, 25, 42,
 45, 48, 50, 51, 53

informatika, 43, 45, 49, 50, 52, 53,
92
informovanost, 28, 29, 30, 33, 89,
91, 92, 110, 111, 135
Infosoud, 139
insolvenční rejstřík, 135
instant messaging, 172, 175
instant messenger, 55, 151, 168
internet, 11, 28, 30, 35, 36, 38, 39,
55, 60, 63, 70, 71, 72, 73, 74, 75,
76, 81, 82, 84, 85, 87, 88, 91, 96,
98, 100, 111, 115, 125, 131, 162,
173, 175, 177, 181, 184, 186, 187
IP adresa, 66, 177, 181
ISP (Information Service Provider),
165, 167, 168, 169, 170, 171, 172,
173, 175, 176, 178, 179, 183, 185,
186

J

Jargon File, 163
jiná provozovna, 78, 81
judikatura, 50, 77, 79, 111, 113, 134,
139, 178, 181, 186, 187
jurisdikce, 37, 38, 58, 60, 61, 62, 65,
66, 67, 74, 75, 77, 81, 83, 86, 87,
161, 186

K

kauzalita, 44, 145, 146, 147, 151
Kelsen, Hans, 25, 145, 146, 156
Knapp, Viktor, 9, 11, 45, 46, 47, 48,
49, 50, 51, 52
kód, 12, 43, 147, 148, 149, 151, 154,
155, 157
komplexita, 11, 29, 30, 34, 157

komunikační infrastruktura, 31, 56,
57, 63, 80, 99, 100, 105, 123, 146,
149, 160, 168, 172, 175
komunitní server, 151, 168
konektivita, 140
konverze, 121, 132, 139, 140
kverulant, 123, 124
kyberkriminalita, 63, 65, 67, 105,
106
kybernetika, 9, 10, 11, 12, 13, 22,
43, 45, 46, 47, 48, 49, 52, 53, 95,
164
kyberprostor, 11, 12, 35, 36, 37, 38,
57, 58, 59, 68, 80, 154, 155, 156,
158, 161, 164

L

legitimace, 11, 20, 111, 150, 162,
179, 180, 181, 182
legitimita, 18, 20, 27, 28, 32, 38, 40,
60, 83, 101, 111, 126, 142
Lessig, Lawrence, 40, 147, 148, 149,
154
locus delicti, 59, 71, 81
locus solutionis, 77, 78, 84, 86
logika, 10, 22, 23, 27, 42, 44, 46,
100
Lotus (případ - Stálý dvůr
mezinárodní spravedlnosti), 62

M

mere conduit, 175, 176
Ministerstvo informatiky, 102, 103
mirror, 176
místní působnost, 57, 58, 59, 60, 67,
68, 164

monotónnost, 23, 26, 43, 45, 155,
156, 157
morálka, 12, 16, 18, 37, 126

N

nahodilost, 35, 151, 160
Napster, 174
Naso. Publius Ovidius, 34
nekalá soutěž, 73
nekalosoutěžní jednání, 171
nezávislost soudů, 130
norma, 17, 18, 22, 24, 39, 112, 145,
146, 147, 148, 149, 151, 152, 153,
155, 157, 158, 160, 162, 165
normativita, 11, 16, 17, 18, 19, 20,
22, 24, 25, 32, 34, 43, 44, 52, 54,
58, 102, 107, 109, 110, 111, 112,
115, 119, 125, 130, 134, 145, 146,
147, 149, 150, 151, 152, 155
normotvorná kompetence, 150, 151,
160
notice, 183

O

obesílání, 130
objektivní odpovědnost, 172, 173,
175, 176, 183, 187
odpovědnost, 26, 53, 62, 63, 70, 72,
150, 162, 170, 171, 172, 173, 174,
175, 176, 178, 179, 180, 181, 182,
183, 184, 185, 186, 187
off-line, 35, 40, 57, 58, 167, 169
on-line, 56, 58, 70, 72, 80, 83, 85,
141, 149, 159, 162, 164, 168, 169,
170, 171, 186
open source, 164
organismus, 14, 15, 28

organizace, 15, 28, 29, 30, 31, 33,
35, 36, 39, 40, 43, 46, 79, 97, 106,
137, 146, 162

P

patria, 68, 81, 86
peer-to-peer síť, 174
penetrace, 91
perfekce, 126
pirát, 100, 187
platnost, 11, 17, 18, 23, 24, 27, 41,
85, 109, 111, 112, 114, 169
počítač, 42, 43, 45, 50, 64, 66, 72,
74, 78, 90, 116, 130, 155, 171
podání, 11, 117, 119, 120, 121, 122,
123, 131, 132
podatelna, 120, 121, 122, 139
portál, 63, 86, 113, 139, 168, 176,
186
pořádek, 43, 46
poskytovatel služeb informační
společnosti, 116
postih, 38, 73, 83, 150, 151, 152,
165, 171, 172, 173
pozitivní právo, 109
pragmatismus, 46, 50
pravda, 13, 21, 22, 23, 26, 39, 43,
127, 128
pravidlo, 11, 15, 17, 18, 19, 20, 21,
24, 25, 26, 30, 33, 37, 40, 44, 47,
55, 57, 65, 74, 92, 110, 112, 113,
120, 145, 146, 148, 149, 152, 153,
154, 157, 159, 171, 182
právní informační systém, 111, 134
právní informatika, 10, 11, 43, 45,
47, 49, 50, 51, 52, 53, 54, 126
právnícká osoba, 70, 117, 118, 119,
161

právník, 13, 27, 40, 41, 51, 53, 94,
111, 126, 158, 165
právotvůrce, 26, 56, 102, 107, 112,
117, 125, 153, 155, 169, 170, 186
primitivismus, 44
princip, 17, 20, 21, 24, 49, 57, 59,
60, 68, 83, 84, 86, 99, 118, 120,
124, 128, 129, 130, 150, 154, 158,
164, 171
promulgate, 109, 110, 111, 112,
113, 114, 115, 119, 125
proporcionalita, 124, 128, 129, 130
předporozumění, 111
přírodní zákon, 145, 146, 147, 148,
151, 157
přirozené právo, 156
publikace, 20, 25, 48, 50, 74, 110,
111, 112, 177
působnost práva, 38, 58, 60, 80, 81,
82, 87, 161, 165

R

Rada vlády pro informační
společnost, 104
ratio legis, 186
regulace, 11, 28, 31, 32, 33, 34, 36,
38, 39, 40, 46, 52, 58, 68, 84, 86,
101, 102, 107, 126, 149, 150, 152,
165, 195
reprodukce, 16, 41
rovnost, 95, 128, 130, 156
rozhodnutí, 11, 16, 24, 25, 60, 62,
69, 72, 73, 74, 75, 79, 85, 128,
130, 131, 139, 141, 142, 143, 147,
150, 158, 162, 164, 173, 174, 178,
179, 181, 182, 186, 187

S

samoorganizace, 34, 35
samoregulace, 34
samospráva, 121, 137
sázky, 84, 85
Sbirka zákonů, 110, 111
sdílení, 164
software, 60, 116, 121, 130, 149, 164
solidarita, 97, 156
soudnictví, 32, 47, 124, 135, 137,
142
soukromí, 99, 101, 173
spis, 11, 90, 127, 132, 133, 134, 136,
138, 139, 140, 141, 142
společenská smlouva, 37, 38, 82,
150
spotřebitel, 78, 100
spravedlivý proces, 119, 127, 128,
129
spravedlnost, 42, 44, 48, 60, 62, 132,
187
správní jurisdikce, 83, 86
správní soudnictví, 124
stát, 11, 18, 19, 21, 32, 36, 38, 41,
47, 48, 55, 57, 58, 59, 60, 61, 62,
63, 64, 65, 66, 67, 68, 69, 70, 71,
73, 74, 75, 76, 77, 80, 82, 83, 84,
86, 87, 91, 100, 103, 106, 110,
111, 112, 113, 114, 115, 117, 119,
120, 122, 123, 124, 125, 128, 131,
137, 143, 145, 150, 158, 161, 162,
164, 165, 170, 187
subjektivní právo, 70, 72, 74, 75, 76,
114, 118, 124, 171, 176, 179, 180
systém, 9, 10, 11, 12, 13, 16, 17, 18,
20, 23, 24, 25, 26, 28, 29, 30, 31,
32, 33, 34, 35, 44, 45, 48, 49, 50,
51, 52, 56, 64, 73, 77, 89, 94, 96,
98, 102, 104, 106, 111, 112, 114,

117, 118, 119, 122, 123, 124, 129,
131, 132, 133, 134, 135, 136, 137,
138, 139, 141, 142, 143, 149, 151,
152, 161, 163, 164, 167, 174

Š

šikana, 123, 129

T

technologický trh, 98
teritorialita, 55, 59, 87
teror, 163
text, 18, 26, 43, 60, 89, 93, 112, 113,
115, 120, 134, 142
transparentnost, 131, 142, 148
trestný čin, 60, 61, 62, 64, 65, 66

U

účel v právu, 145
Úmluva o kyberkriminalitě, 63, 65,
67, 105
United Nations Group on the
Information Society, 105
ústavní soudnictví, 85, 124
utopie, 52

V

videokonference, 55, 135
video-on-demand, 170
virtualizace, 55, 80, 118, 125, 135,
141

vyhledávač, 168, 170, 177, 184, 185,
186, 187
výpověď o normě, 25
výrok, 16, 17, 21, 23, 43, 130, 182

W

Well (internetová komunita), 171
Wiener, Norbert, 9, 12, 13, 15, 16,
22, 49, 95
World Summit on the Information
Society, 105

Y

Yahoo (případ Francie), 186

Z

základní práva, 96, 119, 129, 154,
158, 186
zákonnost, 24, 42, 44, 45, 46, 47, 50,
52, 121
závazek, 64, 66, 70, 71
závaznost, 20, 21, 24, 113, 114
Zippo (případ - USA), 75
znalostní ekonomika, 98, 100, 103
zneužití práva, 124

Ž

život, 13, 14, 17, 22, 23, 25, 42, 53,
62, 94, 95, 98

PRÁVO A EVROPSKÁ INFORMAČNÍ SPOLEČNOST

JUDr. Radim Polčák, Ph.D.

Vydala Masarykova univerzita roku 2009

Spisy PrF MU č. 344 (řada teoretická)

Ediční rada: J. Kotásek (předseda), J. Bejček, V. Kratochvíl,
N. Rozehnalová, P. Mrkývka, J. Hurdík, R. Polčák, J. Šabata

Tisk: TRIBUN EU, s.r.o., Gorkého 41, Brno

1. vydání, 2009

Počet výtisků: 201

Publikace PrF-7 /09-02/58

ISBN 978-80-210-4885-0 (brož.)

ISBN 978-80-210-4886-7 (CD-ROM)