Ján Matejka

Internet
jako objekt práva

Hledání rovnováhy autonomie a soukromí

Edice CZ.NIC

Ján Matejka

INTERNET JAKO OBJEKT PRÁVA:
hledání rovnováhy autonomie a soukromí

Vzor citace:
MATEJKA, J. Internet jako objekt práva: hledání rovnováhy autonomie a soukromí. 1. vydání. Praha: CZ.NIC, 2013.

Vydavatel:
CZ.NIC, z. s. p. o.
Americká 23, 120 00 Praha 2
Edice CZ.NIC
www.nic.cz

Recenzenti:
prof. JUDr. Martin Boháček, CSc.
doc. JUDr. Ing. Bohumír Štědroň, Ph.D., LL.M.

Technická a jazyková korektura:
Ing. Petr Aubrecht, Ph.D.
Petr Behún

© 2013 Ján Matejka
v licenci Creative Commons Attribution-ShareAlike (3.0),
s podporou RVO:68378122.

ISBN: 978-80-904248-7-6 (CZ.NIC, z. s. p. o.)

cz.nic

— Motto

„Takový vševládný stát (lhostejno jaké formy) roztáhne po zemi svou právní síť, a člověk bude běhat jako zajíc sem a tam, aby našel v této síti díru či větší oko, aby se dostal na místečko, kde by si oddechl a zašeptal: ‚Zaplať pánbů, tady jsem sám, tady si zaskotačím.' Pozorujte proto naše zákonodárství z tohoto hlediska a dávejte pozor, abychom na místě svobody netvořili nové formy nevolnictví."[1]

Emil Svoboda

1 SVOBODA, E. *O vývoji v právu.* Praha, 1926, s. 22. Podobný náhled lze však zaznamenat i jinde, viz např. výrok připisovaný W. Churchillovi: „Když budete mít deset tisíc nařízení, zničíte jakýkoliv respekt k právu." Případně výrok, jehož autorem je Lao-c: *„Čím více zákonů a nařízení, tím více je zlodějů a lupičů."* Nebo též Karel Havlíček Borovský: *„Byrokracie jest ten nepřirozený způsob vlády, při kterém se vlády do všeho občanského života míchají, všechno občanům předepisují, žádnou svobodnou vůli a samosprávu jim nenechávají… Něco jiného jest úřednictvo a něco zcela jiného byrokracie, úřednictvo musí býti v každém dobře zřízeném státu, byrokracie jest neštěstím každého…"*

— Ján Matejka

Internet
jako objekt práva:

hledání rovnováhy autonomie a soukromí

— Edice CZ.NIC

Obsah

— Obsah

Motto – 2
Seznam použitých zkratek – 9
Předmluva vydavatele – 13
Předmluva autora – 17

1. Úvodní úvahy: Internet a právo v (ne)klidu – 23
1.1 Internet a proměny axiomů — 25
1.2 Spekulace – právo internetové (koňské) a automobilové — 26
Klíčová slova — 31

2. Axiologie soukromí a jeho ochrany v prostředí informační společnosti – 33
2.1 Pojem soukromí a problém jeho vymezení — 35
2.2 Falešná dichotomie vztahu soukromí a práva na informace — 37
2.3 Informační společnost a metamorfózy ochrany soukromí,
zejména pak legitimního (přiměřeného, rozumného) očekávání — 38
2.4 „Lesk" a bída soukromí na dvou příkladech z prostředí informační společnosti — 43
Klíčová slova — 47

3 Některá metodologická východiska a kolize autonomie vůle s právem na soukromí – 49
3.1 Úvodní teze (metodologické) — 51
3.2 Specifický předmět ochrany soukromí — 52
3.3 Kolize soukromí s jinými hodnotami a způsoby jejich řešení — 53
Klíčová slova — 56

4. Právní regulace ochrany soukromí, její limity a možnosti – 17
4.1 Sedes materiae ochrany soukromí — 59
4.2 Evropský systém ochrany soukromí — 61
4.3 Přístup mezinárodní komunity k ochraně osobních údajů a dat — 72
4.4 Správněprávní úprava a její vybrané aspekty — 75
4.4.1 Koncepce právní úpravy a působnost národní autority ochrany dat — 75
4.4.2 Základní zásady v zákoně o ochraně osobních údajů — 78
4.4.3 Pojem osobní údaj jako jeden z klíčových pojmů určující věcnou působnost ZoOÚ — 84
4.4.4 IP adresa a další číselné identifikátory jako kontextuální osobní údaje — 89
4.4.5 MAC adresa, IMEI a IMSI jako kontextuální osobní údaje — 93
4.4.6 Zásada informovaného souhlasu v prostředí Internetu, zvláštní režim a zákonné licence — 95
4.4.7 Zpracování osobních údajů v prostředí Internetu se zřetelem k jejich zveřejňování — 102
4.4.8 Veřejné zasedání a zveřejňování souvisejících údajů na Internetu — 113
4.4.9 Sociální sítě – vybrané aspekty — 114
4.4.10 Veřejně přístupné internetové databáze a registry
(obchodní rejstřík, katastr nemovitostí a registr doménových jmen WHOIS) — 120
4.4.11 Registry dlužníků — 122

4.4.12 Zvláštní režimy zpracování osobních údajů s využitím cloud computingu — 123
4.4.13 Internet a právo být zapomenut — 124
4.5 Regulace soukromí a důvěrnosti komunikací v oblasti elektronických komunikací — 128
4.5.1 Procesněprávní aspekty ochrany provozních a lokalizačních údajů (data retention) se zřetelem k historických ústavněprávním souvislostem — 129
4.5.2 Data retention v současném českém právu — 133
4.6 Občanskoprávní úprava — 135
4.6.1 Obecné aspekty právní úpravy osobnostních práv fyzické osoby — 135
4.6.2 Rozsah a obsah práva na ochranu osobnosti — 137
4.6.3 Život a zdraví — 139
4.6.4 Občanská čest a lidská důstojnost — 140
4.6.5 Další rozsah a obsah práva na ochranu osobnosti — 141
4.6.5.1 Jméno — 142
4.6.5.2 Projevy osobní povahy — 142
4.6.5.3 Jiné statky občanským zákoníkem výslovně nevyjmenované — 143
4.6.6 Prostředky ochrany proti neoprávněným zásahům do práva na ochranu osobnosti — 145
4.6.7 Aktivní legitimace k uplatňování ochrany proti neoprávněným zásahům do práva na ochranu osobnosti — 146
4.6.8 Zákonné omezení práv osobnostních — 147
4.7 Pracovněprávní úprava — 147
4.7.1 Právo zaměstnance na soukromý a rodinný život — 149
4.7.2 Národní úprava — 150
4.7.3 Meze výkonu práva kontroly — 152
Klíčová slova — 156

5. Mezinárodní spolupráce jako conditio sine qua non efektivity práva – 157
5.1 Internet a existence právních problémů jeho globální povahy — 159
5.2 Ochrana osobních údajů a kolizní normy — 162
5.3 Ochrana osobních údajů v prostředí Internetu a základy určování soudní pravomoci — 169
5.4 Závěrem k problému (přeshraniční) působnosti práva — 174
Klíčová slova — 175

6. Exempla trahunt aneb k některým úkolům rozhodovací praxe – 177
Klíčová slova — 184

7. Závěr a další spekulace – 185

Resumé – 197
Zusammenfassung – 209
Seznam použitých pramenů a dalších zdrojů – 221
Rejstřík – 243

Seznam použitých zkratek

Níže uvedené právní předpisy jsou uváděny ve znění pozdějších předpisů, pokud není výslovně v textu uvedeno jinak.

- **Listina** – Usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku
- **ZoOÚ** – zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů
- **ZsPI** – zákon č. 106/2000 Sb., o svobodném přístupu k informacím
- **ZoZR** – zákon č. 111/2009 Sb., o základních registrech
- **AutZ** – zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon)
- **ZoEK** – zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)
- **ZoSIS** – zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti)
- **ObčZ** – zákon č. 40/1964 Sb., občanský zákoník
- **ObchZ** – zákon č. 513/1991 Sb., obchodní zákoník
- **NObčZ** – zákon 89/2012 Sb., občanský zákoník
- **ZoOchrZ** – zákon č. 441/2003 Sb., o ochranných známkách
- **ZoEP** – zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)
- **ZoEÚ** – zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů
- **ZoISVS** – zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů
- **zákoník práce** – zákon č. 262/2000 Sb., zákoník práce
- **zákon o evidenci obyvatel** – zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech
- **zákon o regulaci reklamy** – zákon č. 40/1995 Sb., o regulaci reklamy a o změně a doplnění zákona č. 468/1991 Sb., o provozování rozhlasového a televizního vysílání
- **zákon o občanských průkazech** – zákon č. 328/1999 Sb., o občanských průkazech
- **zákon o cestovních dokladech** – zákon č. 329/1999 Sb., o cestovních dokladech
- **zákon o zaměstnanosti** – zákon č. 435/2004 Sb., zákon o zaměstnanosti
- **zákon o advokacii** – zákon č. 85/1996 Sb., o advokacii
- **trestní zákoník** – zákon č. 40/2009 Sb., trestní zákoník
- **zákon o přestupcích** – zákon č. 200/1992 Sb., o přestupcích
- **trestní řád** – zákon č. 141/1961, o trestním řízení soudním (trestní řád)
- **správní řád** – zákon č. 500/2004 Sb., správní řád
- **tiskový zákon** – zákon č. 46/2000 Sb., o právech a povinnostech při vydávání periodického tisku a o změně některých dalších zákonů (tiskový zákon)
- **zákon o státní kontrole** – zákon č. 552/1991 Sb., o státní kontrole
- **zákon o krajích** – zákon č. 129/2000 Sb., o krajích (krajské zřízení)
- **zákon o obcích** – zákon č. 128/2000 Sb., o obcích

- **zákon o poštovních službách** – zákon č. 29/2000 Sb., o poštovních službách
- **zákon o bankách** – zákon č. 21/1992 Sb., o bankách
- **zákon o matrikách** – zákon č. 301/2000 Sb., o matrikách, jménu a příjmení a o změně některých souvisejících zákonů
- **zákon o zdravotních službách** – zákon č. 372/2001 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách)
- **Úmluva** – Úmluva o ochraně lidských práv a základních svobod Rady Evropy z roku 1950. Tato úmluva byla vyhlášena ve Sbírce zákonů ČR pod číslem 209/1992 Sb.
- **Úmluva č. 108** – Úmluva č. 108 Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat z roku 1981. Tato úmluva vyhlášena ve Sbírce mezinárodních smluv ČR pod číslem 115/2001 Sb. m. s.
- **Směrnice** – Směrnice Evropského parlamentu a Rady č. 95/46/ES o ochraně osobních údajů
- **Směrnice č. 58** – Směrnice Evropského parlamentu a Rady č. 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací,
- **Směrnice č. 24** – Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES.
- **Ústavní soud** – Ústavní soud České republiky
- **Úřad** – Úřad pro ochranu osobních údajů
- **ESLP** – Evropský soud pro lidská práva (European Court of Human Rights)
- **ESD** – Evropský soudní dvůr (European Court of Justice)
- **SDEU** – Soudní dvůr EU (Court of Justice of the European Union)
- **MSD** – Mezinárodní soudní dvůr (International Court of Justice)
- **Pracovní skupina 29** – Pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů zřízená podle článku 29 směrnice č. 95/46/ES o ochraně osobních údajů (Směrnice)

Předmluva vydavatele

Vážení čtenáři,

Zdá se to být neuvěřitelné, ale je to tak – Edice CZ.NIC, tedy vydavatelství, ve kterém se vám snažíme nabízet zajímavé knihy s tematikou Internetu, internetových technologií, software nebo programování, v letošním roce oslaví již 5 let své existence.

Kniha, kterou právě držíte v rukou, je však teprve první „netechnickou", která v Edici vychází. Jsem velmi ráda, že touto knihou je právě tato, která na svět Internetu nahlíží právní optikou. A ještě více, že se jedná o originální dílo, které je prostřednictvím naší Edice vydáváno poprvé. Jeho autor, JUDr. Ján Matejka, Ph.D., je respektovaný vysokoškolský pedagog, advokát a především také vědecký pracovník, který se právu informačních technologií věnuje již řadu let – je mj. jedním ze zakladatelů informačního serveru ITpravo.cz, který se touto oblastí práva zabývá bezmála jedno desetiletí.

Vztah Internetu a soukromí je vztahem velmi komplikovaným, na soukromí v něm čeká mnoho nástrah a pokušení. Internet je nástroj, bez kterého si již moderní komunikaci, bez ohledu na to, zda se jedná o soukromou či pracovní, neumíme představit. Poslední vývoj naznačuje, že bude stále běžnější situace, kdy uživatelé svá data více či méně dobrovolně a vědomě předávají dalším subjektům – sociální sítě jsou na vrcholu své popularity, podnikatelé ukládají svá data a data svých klientů do cloudů, e-mailem jsme schopni poslat informace, které bychom někdy neřekli ani svým nejbližším.

Problémy však obvykle tím, že se o nich mlčí, nemizí. Předkládaná publikace, která si, jak pevně věřím, své čtenáře najde nejen mezi odbornou právnickou veřejností, se srozumitelnou formou věnuje nejen fundamentálním aspektům právní ochrany soukromí, jako jednoho ze základních lidských práv, ale především speciálním otázkám, které by bez Internetu jen těžko vyvstaly. Knihu lze doporučit také širší veřejnosti, neboť problematika, jíž se věnuje, se dotýká téměř každého z nás. Jako studijní materiál jistě dobře poslouží také studentům především právnických fakult.

Přeji Vám příjemné čtení.

Zuzana Průchová
Praha, 15. července 2013

Předmluva autora

Předmluva autora

O vztahu Internetu a práva lze psát v nejrůznějších souvislostech. Ať již jde o otázky týkající se jeho právní či globální povahy, rozhodného práva nebo otázek tzv. kódování práva. Společným jmenovatelem potřebnosti řešení těchto otázek bude více či méně vzrůstající zájem všech, kteří Internet využívají, lhostejno, zda pro práci či zábavu. Jako autor jsem si dobře vědom toho, že psát knihu o vztahu práva a Internetu je obrovská troufalost. Jde o vztah v mnohém komplikovaný, ne vždy patrný, navíc se rodí a vyzrává jen velmi pomalu. Popsat tak průnik těchto dvou dynamických veličin je, domnívám se, práce na celý život. Nedělám si tak iluze, že se to v této knize podaří, není to ostatně ani mým cílem. Snad by to mohl být dobrý začátek. Právo i Internet se navíc až příliš rychle rozvíjejí a neustále se mění, než aby je bylo možné v klidu zachytit a popsat.

Kniha, kterou má čtenář v rukou, vznikala poměrně dlouhou dobu. Je to dáno jak časovými dispozicemi autora, tak i samotným tématem, které jakkoliv je podtitulem orientováno na otázky vztahu svobody a soukromí, stále představuje téma nesmírně dynamické, a to jak po stránce kvalitativní, tak i kvantitativní. Cílem této práce tak není podat či nabídnout vyčerpávající odpovědi na obecné otázky všech aktuálních proměn práva[2], ale věnovat se projevům aktuálního vztahu svobody a soukromí v prostředí Internetu. Navzdory takto zdánlivě úzkému zaměření práce si však jako autor nekladu za cíl poskytnout vyčerpávající odpověď na všechny související otázky. Celá řada podobných témat tak není v rámci této práce řešena, byť je zřejmé, že by si komplexní posouzení zasloužila také, u některých dílčích témat pak raději sahám po renomovaných zahraničních textech či stanoviscích správních orgánů, které již podstatu věci objasňují lépe, než bych to svedl sám.

Navzdory tomu, že téma publikace je stále v pohybu, panuje mezi odbornou veřejností nad jeho podobou zvláštní ticho. Absence jasných právních názorů (zejména v rovině argumentativní) pak nezřídka vede k tomu, že jsou zcela zásadní právní instituty vykládány účelově a nezřídka i chybně, což v kontextu dynamiky služeb Internetu bohužel mnohdy nevede ani k zahájení soudního řízení (a tedy ve své výsledné podobě ani k hledání argumentů), a to nejenom z důvodů jeho zdlouhavosti, ale především celkové absenci právní jistoty a nepřehlednosti celého portfolia této ochrany.

Práce představuje můj dílčí příspěvek k poznání tak rozmanité a rozsáhlé oblasti, jakou je okruh nových právních vztahů vznikajících v souvislosti s existencí Internetu[3] a jeho služeb či protokolů[4] ve vazbě na ochranu soukromí. Tato oblast bývá nezřídka označována za

2 Tomu už se dostatečně věnovali jiní, a navíc s výborným výsledkem, viz např. POLČÁK, Radim. *Internet a proměny práva.* 1. vyd. Praha: Auditorium, 2012

3 Autor této práce záměrně používá velké písmeno ve slově Internet, pokud jde o vlastní jméno (celosvětovou informační a komunikační síť), malé písmeno pak tam, kde hovoří o internetu ve smyslu propojených počítačových sítí. Je však nepochybné, že malé písmeno patří do trojice pojmů intranet – extranet – internet, užívané rovněž ve významu „komunikační médium", u nichž píšeme malé písmeno. Pokud jde o velké písmeno, mělo by vyznačovat samotný vlastní název jedinečného produktu, v tomto případě veřejně globálního Internetu.

4 Pro úplnost je nutné připomenout, že pojem „Internet" původně představoval po technologické stránce pouze jeden ze síťových protokolů.

nepředvídatelnou, případně nejistou. To, že tomu tak ve skutečnosti vůbec není, má racionálně dokázat tato kniha. Při volbě jejího názvu jsem se snažil upřednostnit především název obsahově výstižný před názvy jinými, byť mnohdy i výrazně cimrmanovsky[5] údernými. Samotné tematické zaměření obsahu na otázky soukromí však bylo zvoleno z několika důvodů.

Jde o téma povahy stále aktuální a praktické, navíc v mnohém odborně atraktivní, přičemž jsem se jimi již jako autor blíže zabýval, a to jak v rámci ryze pedagogické činnosti na Matematicko-fyzikální fakultě Univerzity Karlovy (MFF UK), případně v rámci činnosti svou povahou spíše právně-aplikační, resp. úřední, na Národním bezpečnostním úřadu a Úřadu pro ochranu osobních údajů v rámci jednání jejich rozkladových komisí, kde jsem působil a stále působím. Stranou těchto důvodů, v mnoha ohledech spíše partikulárních, mi v řadě věcí pomohla leccos osvětlit advokátní praxe, která mi k poznání přispěla více, než bych býval očekával.

Tam, kde je to účelné, jsem neváhal přistoupit k podrobnějším citacím judikatury, případně souvisejícím rozhodnutím a stanoviskům správní praxe některých autorit, a to jak českých, tak i zahraničních. Citována jsou především ta rozhodnutí, která mají dle mého soudu co říci i dnešní praxi nebo teorii, lhostejno zda nabyla právní moci či nikoliv. Naproti tomu nejsou citovány takové závěry některých rozhodnutí, jež jsou na první pohled sporná, ba zjevně chybná. Podobně jsem přistoupil i k citacím ostatních publikovaných textů, ať již monografií, případně článků. Místy jsem některé závěry v zájmu úspornosti zestručnil, nicméně vždy tak, abych smysl právního závěru neposunul nebo nezkreslil.

Práce je systematizována do sedmi částí, kde první část (Internet a právo v neklidu) představuje úvod do některých otázek obecné problematiky současných či budoucích metamorfóz práva, kde je v obecné rovině nastíněna hypotéza, že současné technologické změny a dynamizace naší globální společnosti v některých směrech zasahují do obsahu dosavadních právních vztahů a jejich existujících struktur natolik významně, že dochází k narušení samotné podstaty fungování některých tradičních právních postulátů, přičemž tyto změny generují normativně značně obtížně řešitelné právní problémy v celé řadě oblastí a institutů týkajících se soukromí (sdělnost a efektivita práva, jeho vynutitelnost, legitimního očekávání adresátů, ochrana subjektivních práv a řešení konfliktů mezi účely práva, atd.). V této části jsou uvedeny i některé dílčí spekulace a historické konotace, zmíněn je rovněž zcela zásadní význam práva koňského pro právo internetové. Druhá část (Axiologie soukromí a jeho ochrany v prostředí informační společnosti) se zabývá hodnocením a samotným významem soukromí jako základního hodnotového postulátu této ochrany. Nastíněna je problematika celkového právního a technologického kontextu, zmíněn je především interdisciplinární záběr, který se nezřídka nachází daleko za hranicí práva. Třetí část práce (Metodologická východiska a kolize autonomie vůle s právem na soukromí) se věnuje popisu metod použitých v této práci (analytických, logických, systematických, případně komparativních nebo syntézy), jakož i otázkám konfliktu hodnot, jež mohou být objektivně v rozporu s právem na soukromí. Zde je

5 Viz nejstarší z her v repertoáru Divadla Járy Cimrmana, hru Akt, kde v jednom z dialogů sděluje sexuolog dr. Josef Turnovský svůj záměr napsat knihu s názvem „Co se všechno schumelí mezi dvěma manželi", nicméně s ohledem na délku názvu je Bedřichem Sírou následně navrhován údernější název „Chumelenice".

nutné mít na zřeteli zejména ústavněprávní, případně lidskoprávní rozměr celého problému, zejména pak tu část, která se týká poměřování všech práv garantovaných ústavou, tedy práv na stejné úrovni.

Samotné jádro práce obsahuje čtvrtá část (Právní regulace ochrany soukromí, její limity a možnosti), kde se nejprve kriticky polemizuje o otázkách koncepce evropského systému ochrany osobních údajů a dat (včetně úpravy české) a dále je v ní analyzován současný model ochrany osobních údajů v prostředí Internetu, kde je důraz kladen zejména na zásady této úpravy a související práva a povinnosti v kontextu jejich významu pro internetovou praxi. V tomto ohledu jsou řešeny klíčové otázky aplikace současné právní praxe realizované na jednání v prostředí Internetu, jako je např. právní kvalifikace IP adresy, MAC adresy a ID datové schránky jako osobního údaje, režimu agendových informačních systémů (AIS), problematiky nevyžádaných obchodních sdělení (spamu) a sociálních sítí. Uveden je nezbytný kontext souvisejících právních režimů ochrany soukromí, jako jsou civilněprávní (občanskoprávní i pracovněprávní) a trestněprávní aspekty. Pátá část práce (Mezinárodní spolupráce jako conditio sine qua non efektivity práva v prostředí Internetu) rozebírá a popisuje jeden ze základních právních problémů Internetu – klíčovou otázku rozhodného práva a jurisdikce jako nepřímého důsledku skutečnosti, že Internet a jeho dosavadní služby fakticky vylučují fyzickou vazbu na většinu relevantních faktorů standardní mezilidské interakce. Tato základní podmínka efektivity práva je uvedena v historické souvislosti, tj. samotné skutečnosti, že Internet nikdy nebyl tvořen pro masové použití a nikdy také u jeho zrodu nebyly řešeny právní souvislosti jeho masového rozšíření. Předposlední šestá část (Význam a metody rozhodovací praxe) je orientována výlučně na praktické aspekty rozhodování, ať již jde o správní, či soudní rozhodování. Celkové shrnutí a závěry jsou obsaženy v části sedmé (Závěr a další spekulace), na kterou navazuje stručné resumé, seznam použité literatury, bibliografie pramenů a rejstřík.

Do knihy jsem zapracoval, ve více či méně přepracované podobě, některé své starší texty, podobně jsem použil některé fragmenty a myšlenky ze svých prvních prací, které jsem v letech 2000–2006 psal pro internetový server LUPA.cz[6] nebo ITpravo.cz[7]. Jakkoliv si jako autor za naprostou většinou svých starších názorů stojím, musím v tomto ohledu objektivně přiznat, že jsem v průběhu času řadu věcí dostudoval a (snad i lépe) promyslel, takže mnohé z toho, co jsem napsal dříve, bych dnes napsal buď úplně jinak, nebo bych to nenapsal vůbec. Za některé své dřívější názory se dokonce i stydím. Některá má starší tvrzení proto mohou být ve vzájemném rozporu – toto ať čtenář nebere jako protimluv, ale jako změnu názoru ovlivněnou zejména dosavadní praxí a zkušenostmi.

Kniha, kterou otvíráte, pak samozřejmě nereaguje na všechny otázky vztahující se k tématu práce, ale jen na některé, byť se vyskytují často. Bude-li to v mých časových možnostech, pokusím se v následujících letech k tomuto tématu vrátit, případně text tematicky doplnit, opravit či rozšířit o další aktuální otázky Internetu, a to tak, aby samotný název publikace zůstal stejný a rozšířen by byl jen podtitul.

6 Ačkoliv jde o texty mnohdy více než deset let staré, jsou stále dostupné na: www.lupa.cz/autori/jan-matejka/

7 Dostupné z: www.itpravo.cz/

Považuji za slušnost vyjádřit vděk těm, kdo se o výslednou podobu knihy zasloužili. Musím tedy poděkovat kolegům z Ústavu státu a práva AV ČR, v. v. i., zejména pak prof. JUDr. Monice Pauknerové, CSc., DSc., a mým studentům na Matematicko-fyzikální fakultě UK, kde působím, jakož i JUDr. Petru Hostašovi, Mgr. Zuzaně Průchové Durajové a Mgr. Jiřímu Průšovi, kteří byli seznámeni s rukopisem této knihy a opravili v něm nejeden nedostatek. Pokud je tedy tato práce něčím výjimečná, je to především jejich zásluha. Pokud v ní však některé nedostatky přetrvaly, jde to výlučně za jejím autorem.

Publikace je zpracována k právnímu stavu účinnému ke dni 1. prosince 2012.

Autor
Praha, prosinec 2012

1. Úvodní úvahy: Internet a právo v (ne)klidu

1. Úvodní úvahy: Internet a právo v (ne)klidu

1.1 Internet a proměny axiomů — 25

1.2 Spekulace – právo internetové (koňské) a automobilové — 26

Klíčová slova — 31

1. Úvodní úvahy: Internet a právo v (ne)klidu[8]

„Mír mezi lidmi žijícími vedle sebe není přirozený stav, tím je spíše stav válečný, tj. stav, který, ač není vždy vzplanutím projevů nepřátelství, je přece neustálým ohrožením míru. Stav míru musí být tedy zjednán; upuštěním od projevů nepřátelství není totiž ještě mír zajištěn, a není-li si člověk jist před svým sousedem, může se k tomuto sousedovi, kterého k takovému ujištění vyzval, chovat jako k nepříteli."[9]

Immanuel Kant

1.1 Internet a proměny axiomů

O vztahu práva a nových technologií, zejména pak Internetu, včetně jeho změn a transformací, toho bylo napsáno mnoho,[10] řada klíčových otázek však zůstává neřešena, řada dalších problémů se nachází pouze ve fázi jejich identifikace, případně analýzy, nicméně hledání rozumných řešení je v lepším případě na dobré cestě, v horším pak v nedohlednu. Internet je bezesporu fenomén *sui generis*, jako takový nestojí samostatně a je regulován zejména prostřednictvím regulace chování jeho uživatelů. Právo je tak jedním z jeho možných regulativů v podobě nedokonalých normativních konstrukcí, kde platí více než jinde, že mezi realitou, tedy tím, co je v prostředí Internetu skutečně realizováno, a normativitou, tedy tím, co má být (z vůle regulátora i naší), není shoda. Realita Internetu a jeho normativní regulace jsou tedy dvě relativně samostatné kategorie. Tento předpoklad nebude popírán ani v této publikaci, právě naopak, bude jedním z jejích nosných pilířů.

Většinu právních problémů týkajících se Internetu je nutné posuzovat v celkovém právním i technologickém kontextu, nikoliv pouze optikou zažitých vzorců či optikou jednotlivých právních oborů *per se*. Nejinak tomu bude i v této publikaci, která se primárně zabývá realizací ochrany soukromí v prostředí Internetu, ničím více, ničím méně. I takto zúžené téma však nutně vyžaduje celkový interdisciplinární záběr. V tomto ohledu bylo nezbytné si mnoho „vypůjčit" i z jiných právních oborů, ne vždy navíc zcela konzistentně s těmito obory, a to zejména u oborů, jež jsou daleko za hranicí soukromého práva,[11] kterým se autor této publikace dosud v převážné míře zabýval. Nezbývá než věřit, že to není na úkor kvality práce, ale právě naopak.

8 Zde si autor této publikace dovoluje parafrázovat úvodní kapitolu s názvem „Právo v klidu" publikace POLČÁK, Radim. *Internet a proměny práva*. 1. vyd. Praha: Auditorium, 2012, s. 11.

9 KANT, I. *K věčnému míru. Filosofický projekt O obecném rčení: Je-li něco správné v teorii, nemusí se to ještě hodit pro praxi*. Praha: OIKOYMENH, 1999. s. 13.

10 Viz např. POLČÁK, Radim. Kódování práva. *Právník,* Ústav státu a práva AV ČR, roč. 151, č. 1, od s. 52–80, 28 s. ISSN 0231-6625. 2012.; POLČÁK, Radim. *Internet a proměny práva.* 1. vyd. Praha: Auditorium, 2012. 388 s. ISBN 978-80-87284-22-3; POLČÁK, R., J. ČERMÁK, Z. LOEBL, T. GŘIVNA, J. MATEJKA, a M. PETR. *Cyber Law in the Czech Republic.* 1. vyd. Alpen aan den Rijn: Kluwer Law International, 2012. 228 s. Encyclopaedia of Laws/Cyberlaw. ISBN 978-90-411-4010-4.

11 Jistým vedlejším axiomem je zde nepochybně skutečnost, že každý (nejen právní) obor je omezen sám sebou, aniž to vypovídá cokoliv o jeho správnosti. V tomto ohledu se autor této publikace snaží spíše na jiné obory synergicky navazovat než je stavět proti sobě, a to zejména tam, kde dochází k jejich prolínání.

Vliv interdisciplinárních přístupů je v tomto ohledu významný hned z několika důvodů. Jednak tyto přístupy efektivně propojují právní vědu s dalšími lidskými obory, zejména pak informatikou, kybernetikou, psychologií, historií, případně s ekonomií apod. Dále pak proto, že právě zamýšlený záběr této publikace podléhá tomuto trendu velmi výrazně, což se silně projevuje jak v metodách, tak i v systematizaci samotné publikace.

Právo je opakovaně konfrontováno s rozvojem techniky a technologickým pokrokem, přičemž klíčovým faktorem zde má být zejména podpora rozvoje a ochrana jeho pozitivních stránek na jedné straně, a vytváření efektivních překážek a regulace souvisejících negativních důsledků na straně druhé. Úvahy se v tomto smyslu musejí ubírat zejména směrem k zachování minimálních standardů existující míry právní ochrany ve světle faktických důsledků možné budoucí aplikace konkrétní technologie v novém prostředí. Předmětem právních úvah tak není pouze technologie *per se*, ale především její aplikace v podmínkách dosavadních právních standardů a postulátů. Smyslem tedy není čelit zde souvisejícím technologickým proměnám, ale především se pokusit o jejich pochopení a zařazení do existujících podmínek právní regulace. Pouze tato cesta vede k poznání toho, jaké právní problémy a nové jevy v souvislosti s existující technologií vznikají. Proto nebudou úvahy v této publikaci vedeny se záměrem potvrdit, nebo naopak vyloučit právní rizika či nebezpečnost nějaké konkrétní technologie (či služby). Podstatou úvah bude naopak snaha o popis toho, jak právo na tyto technologie reaguje.

1.2 Spekulace – právo internetové (koňské) a automobilové

Ačkoliv se tato práce snaží nabídnout alternativu některých dosavadních řešení včetně těch doktrinárních či judikaturních, není jejím cílem informovat, zda jde o řešení špatná či dobrá. To nechť si posoudí čtenář sám. Publikace má jiný cíl, a to nabídnout nový či jiný úhel pohledu.

Onou pověstnou červenou nití většiny úvah je hypotéza, že některé současné technologické a společenské změny mohou vzhledem ke své globální povaze zasahovat do dosavadních právních vztahů natolik významně, že dochází k nemalému narušení samotné podstaty fungování některých právních postulátů. Svou povahou tak tyto změny generují normativně značně obtížně řešitelné právní problémy, které mohou vyústit v přeformulování právních institutů, jež jsou po staletí uznávány. Je samozřejmě otázkou, do jaké míry jde o jev, který dříve či později nastane, lhostejno z jakého důvodu.[12] V tomto ohledu však lze tvrdit, a nejinak tomu bude na řadě míst této publikace, že jde o jev v současné době natolik závažný, že je nutné jej zkoumat již nikoliv jako pouhou právní externalitu *sui generis*, ale především jako něco, co si zasluhuje hlubší zkoumání z důvodu své přítomné či budoucí důležitosti a významu pro samotnou podstatu práva.[13]

12 Viz jev zvaný normativní síla skutečnosti. K tomu více viz KNAPP, Viktor. Teorie práva. 1. vyd. Praha: C. H. Beck, 1995. 247 s. ISBN 80-7179-028-1, s. 54.

13 Je však nutné korektně poznamenat, že i autor této publikace byl přesvědčen, že některé výrazně starší technologické změny měly podstatu práva ovlivnit také, byť je v současné době zjevné, že se tak nestalo. Jako jeden

Hypotéza významu těchto technologickým změn pro podstatu práva však může být snadno zpochybněna, a to patrně s podobnými argumenty, které bývají postaveny proti přiznání existence samostatnosti právních oborů, jako je právě právo internetové, počítačové atd. Souvislost je sice volná, nicméně argumentace velmi podobná, a jak je známo, historie se opakuje. Již v roce 1996 publikoval známý americký soudce Frank Easterbrook vysoce zásadní článek,[14] kde ve vztahu k existenci kybernetického práva kriticky dovozuje, že tento obor nemá právo na existenci, že právní úpravu informační společnosti netřeba takto specificky řešit a že jediné, co je nutné v této věci učinit, je posílit ochranu soukromého vlastnictví. Easterbrook v tomto smyslu dále tvrdil, že tendence odborníků v oblasti kybernetického práva analyzovat dosavadní právní postuláty s novými technologiemi není nic více než jen omluva za neznalost a diletantismus.

Easterbrook kategoricky argumentoval, ať se technici soustředí na technologie a profesoři práva na primární právní postuláty. Dále byl toho názoru, že psát o právu kyberprostoru je, jakoby se psalo o koňském právu, a to s tím, že „koňské právo" samozřejmě neexistuje. Dle Easterbrooka je kůň jen zvíře, pro které platí stejné zákony jako pro cokoliv jiného. Právní zaměření na technologie nepomůže právo utvářet, uvedl. Technologie by měla prostě přijmout právo, které jsme pro ni vymysleli. Ukázalo se však, že se soudce Easterbrook, ostatně podobně jako jiní, mýlil. Proslavenou se poté stala velmi ostrá reakce,[15] kterou za tento text soudci Easterbrookovi uštědřil Lawrence Lessig, významný americký akademik v oboru internetového práva, který ve svém téměř padesátistránkovém textu Easterbrookova tvrzení důrazně odmítl, a to především s poukazem na samotný praktický význam tohoto nově vznikajícího právního odvětví, kde za klíčové nepovažoval ani tak argumenty vědecké či filozofické, jako především čistě pragmatické[16] (společenská důležitost nových technologií, související vznik specifického sociálního prostředí atd.).

V souvislosti s tímto ryze akademickým sporem, jakož i mírou „údernosti" Lessigovy odpovědi, se pojem „koňské právo" začal nezřídka používat jako přezdívka pro to, čemu dnes říkáme internetové právo, případně právo informačních a komunikačních technologií.[17] Existence nových technologií, v čele se samotným Internetem, vedla ve skutečnosti k tomu, že právo se již začalo vytvářet. První průkopníci v oblasti internetového práva, vůči nimž se právě Easterbrook ve svém článku vymezoval, nemohli ovšem ani tušit, nakolik budou v příštích letech

příklad za všechny lze uvést vlnu nadšení z nových možností poznání (včetně možností právní vědy), která se objevila již v šedesátých letech. K tomu více viz zcela ojedinělý titul v podobě monografie akademika Viktora Knappa (KNAPP, Viktor. *O možnosti použití kybernetických metod v právu.* 1. vyd. Praha: Nakladatelství ČSAV, 1963), jež tehdy otevřela zcela nový pohled na vliv technologie na právo, a která se na nějaký čas stala inspirací pro rozvoj oboru.

14 Viz EASTERBROOK, F. Cyberspace and the Law of the Horse. *The University of Chicago Legal Forum.* 1996, s. 207 a násl

15 LESSIG, L. The Law of the Horse: What Cyberlaw Might Teach Us. *Harvard Law Review.* 1999, roč. 113, č. 2, s. 501. Dostupné také z: http://digitallaw.info/cyberlaw/lessig.pdf

16 K tomu více viz LESSIG, ref. 15, s. 509. Dostupné také z: http://digitallaw.info/cyberlaw/lessig.pdf

17 V tomto ohledu je pro úplnost nutné konstatovat, že na kritiku Easterbrooka postupně ragovala celá řada dalších autorit, přičemž tento akademický spor o „koňské právo" slouží i dnes jako vyjádření důležitosti a životaschopnosti nové právní disciplíny, a to nikoliv pouze internetového práva.

právo a internetové technologie vzájemně propojeny. Tito průkopníci ale na něco přišli – viděli totiž, že tyto nové technologie jsou natolik významné, že související změny práva, kterými se řídí, už dávno probíhají.

Historie nás učí, že význam nových technologií není snadné předvídat. Mnohé zdánlivě zajímavé technologie po dlouhá časová období stagnovaly, a některé dokonce upadly a jejich stopy se časem ztratily. Není to ostatně tak dávno, kdy známý český autor ve svých starších textech[18] věnujících se Internetu a internetovému obchodování mimo jiné skepticky dovozoval, že „scestný je předpoklad obchodníků, že vydělají mnoho peněz, nabídnou-li svým zákazníkům tento způsob obchodování", přičemž v tomto duchu dále uváděl, že „… odmítám myšlenku uskutečňovat na Internetu transakce, které svým jednáním zakládají jakýkoliv právní vztah…". Celým textem se také jako červená nit táhla nedůvěra ohledně jistoty a pravdivosti informací z Internetu, včetně závěrečného předpokladu, že „… se celý slavný Internet nejspíš zahltí sám sebou". Dopad technologie a rozsah její interakce s vnějším světem nelze snadno prorokovat a ještě těžší je předvídat, jak na tyto technologie bude reagovat samotné právo. Ostatně budoucnost nelze také předvídat, jde ji však ovlivňovat, a to např. podobně, jak to výše učinil L. Lessig.

Internetové právo tedy ve své podstatě pojednává především o přizpůsobení neustále se měnících zákonů a postojů právní vědy vzhledem k nové a nové skutečnosti. V tomto ohledu je nezbytné technologie sledovat a hodnotit jejich význam a také budoucí potenciál. Bohužel ne vždy k takovému hodnocení dochází průběžně, ostatně nejinak je tomu v České republice, kde i v této specifické oblasti panovalo poměrně dlouhou dobu ticho, a to minimálně od dob profesora Viktora Knappa.[19] Jakkoliv lze najít některé zářivé výjimky,[20] které tuto dobu (ticha) důstojně překlenuly, je potřeba podívat se na současné technologické možnosti ve smyslu jejich právní kategorizace stále aktuálnější. Rovněž se ukazuje jako důležité na tyto práce obsahově navázat, a je lhostejné zda analyticky (kriticky) či zcela konzistentně. Důstojným příkladem takového přístupu jsou některé aktuální práce R. Polčáka, který nezřídka konzistentně navazuje na starší práce V. Knappa, a to včetně úzké vazby řešení technologických otázek (včetně kybernetiky a informatiky) s propojením excelentní znalosti práva s intelektuálním étosem a morálkou. Je totiž více než jasné, že naše „zasíťovaná" společnost potřebuje velmi dobré internetové právo a schopné průvodce tímto právem více než kdy dříve. Uživatelé těchto technologií si nepochybně

18 SMEJKAL, V. Internet po odložení růžových brýlí. *Magazín CHIP*. Únor 1997, č. 2, s. 18–20, případně SMEJKAL, V. Internet po odložení růžových brýlí (2). *Magazín CHIP*. Březen 1997, č. 3, s. 28–31.

19 Sluší se, myslím, připomenout, že dne 18. 12. 2013 by se Viktor Knapp dožil rovných sta let.

20 Viz např. starší působivé práce M. Boháčka (např. BOHÁČEK, Martin. Ochrana dat v českém právu. Praha: Kriminalistický ústav Policie ČR, 1993, případně BOHÁČEK, Martin a Jan DĚDIČ. Právo & software: I. sborník přednášek o právní úpravě ochrany a nakládání se softwarem. Praha: Dilia, 1990. ISBN 80-900120-5-1, případně BOHÁČEK, Martin a kol. Právo průmyslového a jiného duševního vlastnictví. 1. vyd. Praha: VŠE, 1994. 220 s. ISBN 80-7079-388-0, případně BOHÁČEK, Martin a Zbyněk LOEBL. Smluvní vztahy při tvorbě a šíření software. Mechanizace a automatizace administrativy. 1992, č. 9, s. 243–249), případně aktuální R. Polčáka (Viz např. POLČÁK, Radim. Kódování práva. Právník. Ústav státu a práva AV ČR, 2012, roč. 151, č. 1, s. 52–80. ISSN 0231-6625 nebo POLČÁK, Radim. Internet a proměny práva. 1. vyd. Praha: Auditorium, 2012. 388 s. ISBN 978-80-87284-22-3).

zaslouží takovou právní úpravu, která nejen respektuje, jak tyto technologie fungují, ale která je především efektivně chrání. Zpracování této oblasti práva hraje velice důležitou roli ve vzdělávání soudů, právníků i společnosti, roli, která zahrnuje budování mostů mezi právními doktrínami a komplexně se rozvíjejícími technologiemi a postupy. Pokud bychom v ideálním případě dokázali třeba jen nahlédnout do budoucnosti, mohli bychom se vyhnout chybám, které udělal soudce Easterbrook ve své kritice z roku 1996. Soudce Easterbrook tehdy neviděl budoucnost, která už přicházela. Možná ji však nevidíme jasně ani my dnes. Naše digitální technologie jsou nejen komplexní, ale vlastně jsou ve stavu permanentní evoluce. Právo je sice systém dynamický, nicméně obvykle reaguje se zpožděním. Toto zpoždění je však proměnlivé a jeho rozsah může být přímo úměrný tomu, do jaké míry se dokážeme ohlédnout zpět do minulosti a nechat se inspirovat. Historie, jak známo, se opakuje.

Zajímavý příklad možné podobnosti významu nových technologií a jejich způsobilosti změnit podstatu práva představuje Greg Lastowka,[21] který uvádí, že při úvahách o možném významu internetového práva se nabízí možná podobnost s právem automobilovým. Lastowka totiž dovozuje, že automobily[22] jako jedna z neoblíbenějších technologií dvacátého století změnily společnost tak, že vyvolaly vlny krveprolití. Ve 30. letech minulého století přišlo každoročně o život při automobilových haváriích desetitisíce lidí. Takové ztráty na životech překonaly veškeré předchozí živelné katastrofy.[23] Automobily rovněž v krátké době změnily fyzickou tvář krajiny, díky nim se zrodily nejen dálnice, ale také myriády nových obchodních i společenských sídel: restaurace, motely, předměstí, čerpací stanice a nákupní střediska. Auta změnila i podobu rodin, jejich členům dala větší svobodu a mobilitu, a tedy i větší možnosti trávení volného času, zaměstnání a bydlení.

Automobilové právo se také rodilo, jak dále Lastowka uvádí, velmi pomalu a postupně. Některé jeho části vznikly přímo formou předpisu, velice podobně jako přímé předpisy, které v současné době upravují Internet. Právě díky těmto předpisům (pozitivnímu právu) představují dopravní předpisy a předpisy v oblasti konstrukce a kontroly emisí, jeden ze základních pramenů tohoto odvětví. Jde svou povahou o výsledky pozitivního práva,[24] kde platí, že podobně jako automobilu se díky kyberprostoru zrodila celá řada nových forem kriminality a násilí, které prověřují kvalitu a kvantitu právních předpisů. Zajímavá je rovněž analogie ve vztahu k autu jako nástroji porušování práva, kde Lastowka zmiňuje tzv. „únikové auto", které sehrálo klíčovou roli v mnoha bankovních loupežích, což popohánělo orgány činné v trestním řízení k lepší koordinaci policejních jednotek jednotlivých států a v důsledku i k posílení pravomocí federální policie (analogie k on-line podvodům, informačním útokům z relativního bezpečí cizí jurisdikce). To nejdůležitější, jak uvádí Lastowka, je však to, co automobil udělal s právem

21 LASTOWKA, G. Foreword: Paving the Path of Cyberlaw. 38 *William Mitchell Law Review* 1. 2011.

22 V tomto ohledu rovněž vtipně dovozuje (ve stylu diskuse o „koňském právu"), že to byl právě automobil, který vrátil naše koně definitivně zpátky do stájí, čímž tak zcela změnil tvář světa.

23 Lastowka v tomto smyslu uvádí, že např. více než polovina pojišťovacího práva je v současné době právě právem automobilovým.

24 Ve Spojených státech však většina automobilového práva vznikla formou soudního výkladu, nikoliv prostřednictvím předpisů.

v podobě ovlivnění reálného života společnosti. To, jak naše kultura přijala automobily, nám přináší spoustu výhod, ale i celou řadu problémů: trvale vysoký počet smrtelných nehod, úpadek městských center, vyšší závislost států na fosilních palivech (a z toho plynoucí mezinárodní ozbrojené konflikty) a také přeměna životního prostředí na naší planetě. Technologie počítačů a Internetu nám přináší podobně smíšený balíček: mocné informační nástroje, ale rovněž velké hrozby (pojetí soukromí, autorského práva, důkazních materiálů, etiky, lidských práv a obchodu otočil kyberprostor vzhůru nohama).

Porovnávání cesty internetového práva s právem automobilovým by mělo odborníkům v oblasti kybernetického práva udělat jak vrásku na čele, tak je i povzbudit. Vrásku na čele proto, že to jen dokládá, jak malý vliv mělo nakonec právo a stát na obrovský sociální dopad automobilismu. Právo v oblasti automobilů sice zaoblilo mnoho ostrých hran, ale společnost se ve svém současném vztahu k automobilům dopustila spousty chyb. Tržní síla sehrála daleko větší roli než racionální myšlení. Z pohledu pesimistů je cesta k automobilovému právu příběhem technologie, která stát pořádně překvapila. Auto změnilo svět, ale především se náš právní systém ukázal jako bezmocný a nedovedl předpovědět obrovské změny, které tato technologie vyvolá. Na druhou stranu je automobilové právo rovněž povzbuzující, jelikož dokládá potenciál právního systému v některých ohledech uspět a přinést spravedlivé výsledky v soudních řízeních. Ponoříme-li se do automobilového práva, najdeme příběhy o úřednících a právních reformátorech, kteří dělali, co mohli, aby tuto technologii vylepšili co do bezpečnosti, efektivity, infrastruktury a spravedlnosti, a často při tom museli čelit velmi silnému odporu. Ne všechny příběhy o automobilovém právu vyprávějí o úspěších, ale v případě aut bylo odvedeno mnoho kvalitní právnické práce na podporu veřejného blaha.[25] Podobně jako v jiných případech, i zde tedy platí, že jednotlivosti v právu mají význam až po jejich propojení s okolním světem. Budiž ambicí této práce pokusit se pojmenovat existující problémy a izolovat je natolik, aby bylo možné dohledat určitá obecná pravidla, u kterých by v zásadě nezáleželo na tom, jaké jsou jejich konkrétní skutkové okolnosti.

Na právo je tak možné nahlížet z celé řady hledisek, ať již z pohledu externího nezúčastněného pozorovatele či přímého účastníka konkrétního právního problému, případně jakkoliv jinak. Ve všech případech by však mělo jít o nazírání rozumné a pokud možno i praktické. Vždyť obvyklým východiskem k celé řadě odpovědí je především snaha o praktické uchopení problému, v tomto ohledu rovněž podobně platí, že věda a praxe nemohou žít jeden bez druhého, byť zdánlivě existují nezávisle na sobě a nezřídka musejí slevovat ze svých ideálních představ o podmínkách pro vlastní existenci. Touto cestou se snaží kráčet i autor této publikace.

Existence Internetu bývá nezřídka přirovnávána k nástupu knihtisku. Není pochyb o tom, že z pohledu některých právních odvětví (např. autorského práva) může jít o pohled v mnohém více než přiléhavý. Tato paralela však nutně platit nemusí. Posouzení přiléhavosti takového srovnání je nutné posoudit až s odstupem, tím spíše, že ani takové hodnocení jedním právníkem by *per se* neobstálo před jakoukoliv solidní kritikou.[26] Navzdory výše uvedenému

25 K tomu srovnej též LASTOWKA, G., ref. 21.

26 Jakkoliv se tomu v této publikace autor opatrně brání, v minulosti se této paralely záměrně a opakovaně dopustil. Je však nutné na jeho obranu poznamenat, že se tak stalo vůči zcela jinému auditoriu, navíc ve snaze vyprovokovat diskusi mezi studenty.

je však nutné minimálně konstatovat, že mezi Internetem a knihtiskem zde existuje celá řada společných jmenovatelů, jež nemohou být ignorovány. Právě díky knihtisku se informace začaly šířit mnohem rychleji, efektivněji a především snadněji. Kombinace těchto skutečností pak vedla k dosud nevídanému rozkvětu vzdělanosti a tvořivosti lidstva. S Internetem to může být podobné, je však v současnosti těžké cokoliv v tomto ohledu kategoricky konstatovat, na to je příliš brzy. I zde ale platí ono známé alea iacte est.[27]

Klíčová slova

Internet, právní axiomy, hypotézy, spekulace, právo kyberprostoru, internetové právo, koňské právo, automobilové právo, technologické změny, existující problémy.

27 Případně též historia magistra vitae.

2. Axiologie soukromí a jeho ochrany v prostředí informační společnosti

2. Axiologie soukromí a jeho ochrany v prostředí informační společnosti

2.1 Pojem soukromí a problém jeho vymezení — 35
2.2 Falešná dichotomie vztahu soukromí a práva na informace — 37
2.3 Informační společnost a metamorfózy ochrany soukromí,
zejména pak legitimního (přiměřeného, rozumného) očekávání — 38
2.4 „Lesk" a bída soukromí na dvou příkladech z prostředí informační společnosti — 43
Klíčová slova — 47

2. Axiologie soukromí a jeho ochrany v prostředí informační společnosti

„Ti, kdo jsou ochotni se pro chvilkový pocit bezpečí vzdát svých základních práv a svobod, si nezaslouží ani bezpečí ani svobodu." [28]

Benjamin Franklin

2.1 Pojem soukromí a problém jeho vymezení

Pojem soukromí není jednoduché definovat. Jeho definici[29] tak zpravidla nenajdeme ani v aktuální judikatuře českých či zahraničních soudů ani v mezinárodních dokumentech nebo významných textech právní vědy (doktríny) či praxe. Jen výjimečně lze najít některé odpovědi v rozhodnutích Evropského soudu pro lidská práva, který obvykle váže tento pojem obecně na fyzickou i psychickou integritu osoby včetně sexuálního života.[30] Jde tak o pojem *per se* značně široký a flexibilní; ostatně podobně je tomu u řady jiných právních pojmů, které jsou velmi úzce navázány na další pomocné právo – vědní disciplíny (jako např. na právní sociologii apod.). Podobně jako je tomu u řady dalších pojmů (např. spravedlnost, důstojnost, svrchovanost, jistota atd.), ani v případě pojmu soukromí není taková definice patrně ani žádoucí, i zde totiž platí více než jinde stará římskoprávní regule *omnis definitio (in iure) periculosa es*.[31] Implicitní definice těchto pojmů pak lze dovodit prostřednictvím metod právní argumentace[32] (např. z rubriky právních předpisů, případně abstrakcí[33] atd.).

Z historické perspektivy je tento pojem postupně sémanticky vytvářen zejména ve Spojených státech, kde v roce 1890 vyšla na toto téma první obsáhlejší studie,[34] jejímž cílem bylo především odůvodnit, že pojem soukromí (privacy), jakkoliv jej Ústava USA či její dodatky nevymezují, představuje svého druhu obecné právo (general right to privacy), kterého by bylo možné se dovolat přímo, nikoliv tedy zprostředkovaně. V tomto ohledu autoři této studie (spo-

28 Nejde o autentický text B. Franklina, ale o jednu z celé řady parafrází textu z jeho časopisu, který vydával pod pseudonymem Richard Saunders s názvem P*oor Richard's Almanack,* který v Čechách překládal Josef Jungmann pod názvem Chudý Richard aneb Cesta k blahobytu.

29 Tedy máme-li na mysli definici explicitní reálnou. K tomu více viz KNAPP, V. *Vědecká propedeutika pro právníky.* Praha: Eurolex Bohemia, 2003, s. 178.

30 Viz např. rozsudek Evropského soudu pro lidská práva ze dne 11. 7. 2002, Goodwinová proti Spojenému království, stížnost č. 28957/95, kde bylo judikováno, že transsexuálové mají právo na svoji sexuální identitu a státy toto jejich právo musejí respektovat. Smluvní státy mají povinnost činit taková opatření, aby jednotlivcům byl umožněn přístup k informacím o jejich původu. Pokud osobě nejsou známy informace o rodičích nebo jí jsou utajovány na základě požadavku rodičů nebo na základě ochrany osobních údajů rodičů, můžeme se setkat se dvěma situacemi. Buď může stát jednotlivci informace poskytnout, nebo odmítnout.

31 Tedy že každá definice (v právu) je nebezpečná, mimo jiné už proto, že obvykle není zásady, aby z ní nebylo výjimky. Původ této zásady viz Iavolenaus. *Digesta* 50, 17, 202.

32 K tomu více viz SOBEK, T. O povaze právní argumentace. *Právník*. 7/2007, s. 713.

33 KNAPP, V., ref. 29, s. 183–185.

34 WARREN, S. a L. BRANDEIS. The Right to Privacy. 4 *HARV. L. REV.* 193 (1890).

lečného článku) dovozovali, že pojem soukromí obsahově spadá pod (tehdy) významnější právo na vlastní osobnost (the immunity of the person), přičemž deklarovali, že toto právo představuje *per se* jakýsi nový právní princip, který stojí relativně samostatně bez závislosti na jiných právech či svobodách. V Evropě došlo k utváření tohoto pojmu výrazně později, a to zejména na základě mezinárodních úmluv,[35] kde byl převážně používán pojem „soukromý a rodinný život".

Historická perspektiva se jeví jako významná, a to z mnoha důvodů. Předně proto, že především z této perspektivy lze sledovat velmi odlišný přístup různých autorit k chápání tohoto pojmu. Jiné pojetí lze vysledovat u J. S. Milla, který používal pojem osobní oblast lidského života, popř. svrchovanost nad sebou samým.[36] Dále pak proto, že jde o pojem svou povahou značně subjektivní (viz níže), který je podmíněn kulturními a historickými souvislostmi. Jak výstižně uvádí J. Filip,[37] zcela odlišně a logicky tak byl tento pojem chápán v dobách, kdy v jedné místnosti žila 12ti členná rodina, pro kterou by byly naše dnešní nároky na soukromí v oblasti bydlení něčím zcela nepředstavitelným. Jinak by také chápal soukromí francouzský král přijímající ráno šlechtu, před kterou vykonával všechny úkony ranní toalety. Pokud bychom pak pokračovali směrem do minulosti, zřejmě bychom dospěli až k poznání, které zpravidla překrývá jako prostředek ochrany onen pověstný fíkový list v souvislosti s uvědoměním si nahoty našich biblických předků Adama a Evy[38] ve Starém zákoně.[39] Pojem soukromí má v různých kontextech různý obsah a je chápáno a chráněno v různé šíři.[40]

Současné potíže s vymezením práva na soukromí však vyplývají především z jeho samotné podstaty, obvykle ze skutkových okolností určitého případu (typicky ve vazbě na tzv. informační sebeurčení). Soukromí je zakotveno v normách objektivního práva (soukromého i veřejného), zároveň však představuje významné subjektivní právo jednotlivce, který je tak chráněn i proti své vůli. V tomto ohledu se zde může střetnout závazek státu toto subjektivní právo chránit a respektovat svobodu jednotlivce. V této souvislosti je opakovaně diskutován rozsudek Spolkového správního soudu,[41] který se týkal možnosti vydání živnostenského povolení k provozování tzv. peep-show podle § 33a odst. 2 německého živnostenského řádu, kde soud konstatoval, že toto porušení lidské důstojnosti (člověk jako objekt, ne subjekt) nelze odstranit, ani oprávnit souhlasem dotyčných dam, neboť důstojnost člověka je objektivní nezcizitelná hodnota.

Problém s aplikací práva na soukromí pak obvykle vyplývá také ze skutečnosti, že zákaz porušování soukromí je obvykle nějak vázán na konkrétní rozsah, jaký si sama chráněná

35 Viz např. čl. 8 Úmluvy o ochraně lidských práv a základních svobod, 1950, případně čl. 17. Mezinárodního paktu o občanských a politických právech, případně čl. 12 Všeobecné deklarace lidských práv.

36 *The sovereignty of the individual over himself.*

37 FILIP, J. Úvodní poznámky k problematice práva na soukromí. In: V. ŠIMÍČEK, ed. *Právo na soukromí*. Brno: Masarykova univerzita, 2011, s. 13.

38 Viz Genesis 3:7 „Oběma se otevřely oči: poznali, že jsou nazí. Spletli tedy fíkové listy a přepásali se jimi."

39 Jak dále uvádí FILIP, J., ref. 37, s. 13.

40 CROWTHE, B. (Un)Reasonable Expectation of Digital Privacy. *Brigham Young University Law Review*. 2012, s. 343.

41 Sp. zn. 1C 232/79, z 15. února 1981 (celý rozsudek byl otištěn v Neue Juristische Wochenschrift, roč. 1982, č. 12).

osoba vymezí vůči veřejnosti a v jakém si vymezí hranice svého informačního sebeurčení, což ve svém důsledku objektivně snižuje tzv. právo nedostupnosti soukromí (např. dobrovolné zveřejnění intimní informace na sociálních sítích).

Objektivní právo nemůže pracovat pouze s filozofickými a etickými kategoriemi, musí je transformovat do právního jazyka. V tomto ohledu i naše Listina pojímá otázku práva na soukromí relativně komplexně. V článku 7 odst. 1 je zakotvena obecná garance nedotknutelnosti soukromí jako lex generalis, ze které poté vybíhá v Listině celá řada konkrétních záruk jednotlivých aspektů spojených se soukromím jedince. Stačí uvést hodnoty chráněné v článku 10 odst. 1 Listiny (lidská důstojnost, osobní čest, dobrá pověst, jméno). Všechny jsou spjaty se soukromím jedince. Totéž platí pro ochranu soukromého a rodinného života ve smyslu článku 10 odst. 2 (spojnice s mezinárodními lidskoprávními úmluvami) a ochranu před zneužíváním osobních údajů. Jiným projevem soukromí je tradiční pojetí nedotknutelnosti obydlí dle článku 12 Listiny, kde je soukromí vymezeno prostorově, stejně jako ochrana uchovávaných nebo přepravovaných písemností, záznamů a zpráv podle článku 13 Listiny. Bezprostředním výrazem ochrany soukromí je pak i článek 15 odst. 1 (svoboda myšlení, svědomí a náboženského vyznání či víry). Rovněž řada politických práv a svobod je spjata s problematikou ochrany soukromí. Zejména se jedná o aspekt negativní svobody, tedy o svobodu jedince rozhodovat o sobě tak, že určitý názor neprojeví, informaci nepřijme, postoj nesdělí apod.[42]

2.2 Falešná dichotomie vztahu soukromí a práva na informace

Lidská práva a svobody představují určité společenské hodnoty, které plní zastřešující funkcí úlohu indikátorů normativních očekávání subjektů práva. Představují tak určité druhově vymezené univerzální principy, prostřednictvím nichž se právo podílí na demarkaci veřejného prostoru svobody jednotlivce a jeho práv. Koncepce a celkové pojetí těchto principů pak významně ovlivňuje aplikaci samotného práva a ve svém důsledku i jeho postupnou transformaci. Svou povahou tak lze na lidská práva a svobody nahlížet jako na *sui generis* nástroj k hledání spravedlivé rovnováhy[43] mezi svobodou jednotlivce a jeho povinnostmi. Takto univerzálně pojaté právní principy (jako např. „Svoboda projevu a právo na informace jsou zaručeny."[44]) se nezřídka dostávají do konfliktu s jinými hodnotami a chráněnými zájmy. Uvedené však *per se* neznamená, že by tyto principy byly existencí konfliktů oslabeny, právě naopak, existence těchto konfliktů umožňuje, aby tyto nástroje splnily svůj účel a smysl.

Jazyk lidských práv je vstupní branou do společného světa argumentace. Tento společný svět však nepředchází vzniku konfliktu a jeho manifestaci v podobě argumentace u soudního sporu. Konflikt mezi dotčenými právy není abstraktním konfliktem mezi různými neutrálními principy s jasným významem, který je jaksi předem daný, a to buď proto, že koresponduje s jiným hodnotovým systémem objektivního charakteru (např. morálka), anebo proto, že existuje

42 FILIP, J., ref. 37, s. 13.
43 Resp. přesněji rozumné rovnováhy
44 Článek 17 Listiny.

možnost objektivně vyjádřit jejich pořadí. Snaha řešit tyto spory prostřednictvím argumentace, která směřuje k nalezení jednoho správného řešení, jež se opírá o objektivní významy, trivializuje závažnost konfliktu a jeho symbolický význam pro život.[45]

Prostředí informační společnosti je platformou, kde ke konfliktům mezi dotčenými právy a principy dochází stále častěji. Pokusíme-li se pojem informační společnosti analyzovat, dojdeme patrně k závěru, že jde o pojem možná až příliš obecný a tendenční, neboť každé společenství lze považovat za informační, protože jsou to právě informace, co je drží pohromadě a zajišťuje mu přežití a rozvoj. Pravý význam pojmu informační společnost, respektive význam, v němž se tento pojem aktuálně používá, však není obecným synonymem pro organizovanou nebo organizace chtivou společnost. Jedná se o pojem označující společnost, která si postupně uvědomuje důležitost informací a která ke zvýšení své informovanosti využívá možností daných moderními informačními a komunikačními technologiemi.[46] V jedné ze stěžejních publikací věnovaných pojmu a podstatě informační společnosti konstatuje anglický sociolog F. Webster, že informační společnost lze přesněji definovat prostřednictvím specifických rysů jednotlivých společenských funkcionalit.[47] Hovoří tak celkem o pěti podstatách,[48] z nichž pojem informační společnosti vychází. J. Herceg[49] vychází v tomto ohledu zejména z její technologické podstaty, když uvádí, že informační společnost je charakterizována podstatným využíváním digitálního zpracovávání, uchovávání a přenosu informací. Nejrůznější případy, kdy lidé mezi sebou na dálku vstupují do vztahů pomocí technických zařízení, s sebou automaticky přináší pokusy státu obsah vztahu a komunikace mezi nimi monitorovat; díky technickému prvku je pak tato ingerence státu technicky poměrně snadná a obvykle obtížně odhalitelná. S tím je spojena řada nových právních a etických otázek, a to včetně řešených konfliktů v této publikaci.

2.3 Informační společnost a metamorfózy ochrany soukromí, zejména pak legitimního (přiměřeného, rozumného) očekávání

Jedním z principů, který vyplývá z mezinárodních smluv (včetně lidskoprávních), je zásada ochrany oprávněných, případně legitimních očekávání subjektu práv a právo na jejich ústavní ochranu. Stát jakožto právní stát je omezený svými vlastními právními principy, z nichž vyplývá, že musí respektovat princip právní jistoty, princip ochrany legitimních očekávání a princip práv nabytých v dobré víře. Povaha informační společnosti přináší do aplikace těchto principů některé nové otázky, díky kterým tyto maximy mohou vyniknout více než v tradičních

45 CHRISTODOULIS, E. Constitutional Irresolution: Law and the Framing of the Civil Society. *European Law Journal.* 2003, roč. 9, č. 4, s. 401–432, případně též RADBRUCH, G. *O napětí mezi účely práva.* Wolters Kluwer ČR. 2012. s. 152

46 Vývojově se tomuto pojmu staví např. MAY, C. *The Information Society: A Sceptical View.* Malden: Blackwell Publishers, 2002, s. 19.

47 Viz WEBSTER, F. *Theories of the Information Society.* 3. vyd. New York: Routledge, 2006, s. 8 a násl.

48 Konkrétně jde o podstatu (alternativu) technologickou, ekonomickou, pracovní, teritoriální a kulturní.

49 HERCEG, J. Ústavněprávní limity monitoringu telekomunikačního provozu: konflikt mezi bezpečností a svobodou. *Bulletin advokacie.* 5/2010, s.

oblastech. Princip přiměřeného očekávání lze nepochybně vztáhnout na celou řadu práv, včetně práva vlastnického nebo ochrany dobré víry. Je poměrně všeobecně známo, jak je uplatňována realizace práva na soukromí v tradičním prostředí (viz např. zvláštní režim osobních či domovních prohlídek).

Výkon těchto práv tak lze v této oblasti označit za poměrně stabilizovaný, což je potvrzováno jak úřední praxí orgánů veřejné moci, tak i rozhodovací praxí soudů (včetně těch ústavních). Lze tak konstatovat, že ochrana soukromí v mnoha ohledech funguje v tradičním a známém prostředí, kde již byla definována a uplatněna. Realizace této ochrany v prostředí informační společnosti však vytvořila některá další specifika a limity, jež výkon tohoto práva obsahuje. Lze tak snadno souhlasit s výrokem soudce amerického Nejvyššího soudu A. Scalii, který prohlásil,[50] že „by bylo bláznovstvím tvrdit, že míra soukromí zůstala technickým pokrokem zcela nedotčena". Technologie tak vytvořily další problémy, které zpochybňují konzistenci aplikace práva na soukromí a ohrožují jeho aplikaci v prostředí informační společnosti. S nástupem digitálních technologií vyvstaly čtyři zásadní problémy, a to:

1. větší propast mezi mírou ochrany soukromí, kterou očekává jednotlivec v prostředí informační společnosti, a tím, co je „společnost" (tj. soud) ochotna uznat za přiměřené,
2. smluvní podmínky a povaha poskytování služeb v tomto prostředí, které podkopávají důležité dílčí principy práva soukromí,
3. nevídaný nárůst případů, jejichž předmětem je zejména rozsah možnosti vzdát se práva na ochranu soukromí (např. dobrovolné poskytnutí informací, limity autonomie člověka v oblasti vědomého se vystavení ztrátě soukromí atd. apod.),
4. nekompetentnost soudní i výkonné moci, která postrádá technické znalosti potřebné k tomu, aby mohla efektivně a přiměřeně vymezit ochranu soukromí v digitálním prostředí.

S nástupem nových technologií tak předně vzniká stále větší propast mezi tím, co je soud ochoten uznat jako soukromé, a tím, co za soukromé subjektivně považuje jednotlivec. Základní problém je, že vnitřní procesy technologického fungování informační společnosti za sebou nechávají daleko větší datovou (digitální) stopu, než si je většina lidí ochotna připustit, a části této datové stopy má k dispozici daleko větší množství lidí a subjektů, než lidé předpokládají. A jelikož soudy a jiné správní orgány poskytující ochranu soukromí obvykle při posuzování takovéhoto očekávání vycházejí z povahy výchozí technologie, lze vyslovit hypotézu, že tato propast se s dalším technickým vývojem bude ještě zvětšovat. Řečeno jinými slovy, soudy a příslušné správní orgány využívají přísnější normu ke změření očekávání ochrany soukromí jednotlivce, což obvykle vede k mylným závěrům, že společnost v mnoha případech v digitálním prostředí ochranu soukromí neočekává. Typickým příkladem, který vyvolal tento efekt v rozporu chápání přiměřeného očekávání ochrany soukromí je technologie Web 2.0.[51] Vedlejším účinkem nárůstu

50 *Kyllo proti Spojeným státům americkým,* 533 U.S. 27, 33–34 (2001).

51 Pojem Web 2.0 je ustálené označení pro etapu vývoje www, v níž byl pevný obsah webových stránek nahrazen prostorem pro sdílení a společnou tvorbu obsahu. Tato změna byla fakticky realizována postupně od roku 2004, nicméně tento termín použil cca o 5 let dříve DINUCCI, D. Fragmented Future, *Print.* Volume 53, issue 4, s. 32. Dostupné z: http://tothepoint.com/fragmented_future.pdf. DINUCCI v tomto svém článku mimo jiné uvedl, že: *„Web, jak ho známe teď, který se jako statický text načte do okna prohlížeče, je jen zárodek webu, který přijde. První záblesky*

využití on-line hlasových služeb a množství „záznamových zařízení" je shromažďování ještě většího objemu informací o uživatelích. Sdílení většího množství informací s různými zdroji ale nemusí nutně vést ke snížení úrovně ochrany soukromí, kterou si uživatelé zaslouží a kterou od těchto technologií očekávají. Ti, kdo vkládají své materiály na veřejné blogy, obvykle v nějaké formě akceptují, že se u těchto informací vzdávají svého práva na ochranu soukromí, je však otázkou, zda lze říci totéž o uživatelích mobilních telefonů, jejichž pohyb a základní atributy komunikace jsou neustále sledovány, kdykoli telefon vyhledá kvůli lepšímu fungování služeb nejbližší vysílač[52] či získá informace o přesné podobě uživatele za účelem geografické personalizace služeb (kolokační služby chytrých telefonů a používaných aplikací).

Tento objem digitálních informací bourá hranice mezi veřejnými a soukromými informacemi, a zákony na ochranu soukromí založené na zastaralých koncepcích. Pro uživatele technologií to znamená, že i když jejich subjektivní očekávání ochrany soukromí ve vztahu k informacím sdíleným v digitálním prostředí může být stále silné, skutečnost, že informace vznikají a jsou pravidelně sdíleny, naznačuje, že soudy jsou stále méně ochotné uznávat toto očekávání za přiměřené. To vede k tomu, že orgány činné v trestním řízení mohou tyto informace zcela volně shromažďovat a používat, aniž by musely nejprve žádat o vydání soudního příkazu.

Jak známo, jsou lidská práva nezadatelná a nezcizitelná, sotva by tak někdo namítal, že by nikdo neměl mít možnost podepsat smlouvu, kterou se vzdává svého práva na ochranu soukromí. Pravda je ale taková, že je v pracovních smlouvách,[53] smlouvách s mobilními operátory, smlouvách s poskytovateli služeb informační společnosti a smlouvách o užívání kreditních karet tento stav zcela běžným jevem.[54] V každém z těchto případů jednotlivec, který podepisuje smlouvu, uděluje druhé straně právo přístupu k údajům o své osobě, zdaleka nikoliv vždy v míře nezbytně nutné ve vztahu k plnění předmětu smlouvy druhou stranou. Pravdou je, že vzdávání se těchto práv je obvykle na dobrovolné bázi, vždyť smlouva je uzavřena svobodně, zároveň může rozsah poskytnutých údajů umožnit snadnější poskytování požadovaných služeb. Je však otázkou, zda je správné podobně argumentovat i v případě smluv uzavřených on-line (např. through-click). Zde totiž obvykle platí, že většina webových stránek a většina poskytovatelů online služeb má své podmínky spojené s danou stránkou nebo službou. Tyto podmínky bývají po-

Webu 2.0 se již začínají objevovat a my sledujeme, jak se toto embryo začíná vyvíjet. Web bude chápán ne jako obrazovky plné textu a grafiky, ale jako prostředí, jako éter, jehož prostřednictvím dochází k interaktivitě. Objeví se na obrazovce počítače, na televizním přijímači, na palubní desce, na mobilním telefonu, na herní konzoli, a možná, že i na vaší mikrovlnné troubě."

52 DEMPSEY, X. J. Digital Search & Seizure: Updating Privacy Protections to Keep Pace with Technology. 935. *INST PAT.* 2008, S. 543–548.

53 Viz např. *Spojené státy proti Simonsovi,* 206 F.3d 392, 398, Soud 4. okresku, kde bezpečnostní politika společnosti umožnila sledování všech přenosů souborů, navštívených webových stránek a všech e-mailových zpráv.

54 Viz např. VERIZON CUSTOMER AGREEMENT [online]. Dostupné z: http://www.verizonwireless.com, kde je v části věnované soukromí mj. uvedeno následující: „*Shromažďujeme o vás informace. Po dobu trvání našeho vztahu o vás sbíráme některé informace, např. informace o množství, technické konfiguraci, typu, destinaci a počtu použití našich telekomunikačních služeb…*" Během psaní tohoto textu však došlo k dílčí aktualizaci (update ze dne 29. listopadu 2012), kde je nově stručně popsán režim nakládání s osobními údaji, dostupné z: www.verizon.com/privacy. Smluvní (obchodní) podmínky evropských společností zůstávají velmi rámcové, viz např. www.upc.cz/o-upc/vseobecne-obchodni-podminky/.

jmenovány různě, někdy jako „licenční smlouvy s koncovým uživatelem", „lhůty a podmínky", „podmínky služby" nebo zjednodušeně „podmínky" a jejich význam spočívá v tom, že mají uživatele smluvně zavázat. Podmínky mohou být zobrazeny v podobě tzv. „*clickwrap*" smluv, tedy smluv odsouhlasených kliknutím na políčko „souhlasím", nebo jim podobných „*browsewrap*" smluv, které se považují za uzavřené pouhým procházením určitých stránek (objeví se oznámení ve spodní části stránky, které uživatele zaváže k dodržování podmínek a jeho souhlas se považuje za udělený, pokud stránku dále prochází), a případně i tzv. „*cookiewrap*" smluv, kdy se souhlas uživatele ukládá v podobě *cookies*[55] a použije se při další návštěvě stránek.[56] Tyto on-line uzavírané smlouvy se stávají tak běžné, že z pohledu průměrného jednotlivce je obvykle vysoce nepraktické (nikoliv však nemožné), aby četl vše, co „akceptuje". Ostatně i z provedených studií[57] vyplývá, že naprostá většina uživatelů se s obsahem těchto smluv odmítá seznámit a zcela tento právní rozměr závazku ignoruje. Navzdory této realitě, získávají si tyto formy on-line smluv stále větší uznání ze strany praxe, včetně té rozhodovací, čímž nepřímo podrývají tradiční teorie uzavírání smluv[58] a informovaného souhlasu.

Pro rozbor tradiční ochrany soukromí v tomto prostředí to znamená, že takovému očekávání, které je v rozporu s jasnými podmínkami takto uzavíraných on-line smluv, nemusí být poskytnuta přiměřená soudní či jiná ochrana soukromí. Je velmi pravděpodobné, že soud či jiný orgán ochrany bude respektovat autonomii vůle stran, a zcela upřednostní obsah takového závazku (smlouvy), přičemž otázce seznámení se s procesem uzavření smlouvy ve vztahu k vážnosti projevu vůle nebude vůbec věnovat pozornost. Soud tak jednoduše dojde k závěru, že se uživatel dobrovolně vzdal svých práv na ochranu soukromí. Lze tak s vysokou mírou pravděpodobnosti předpokládat, a to v naprosté většině jurisdikcí, že taková ochrana soukromí (legitimnímu očekávání), patrně nebude přiznána u naprosté většiny takto uzavíraných služeb,včetně standardních „podmínek služby" společnosti Google[59] nebo společnosti Facebook.[60]

---

55 Jako cookie (anglicky koláček, oplatka, sušenka) se v protokolu HTTP označuje malé množství dat, která WWW server pošle prohlížeči, který je uloží na počítači uživatele. Při každé další návštěvě téhož serveru pak prohlížeč tato data posílá zpět serveru. Cookies běžně slouží k rozlišování jednotlivých uživatelů, ukládá se do nich obsah „nákupního košíku" v elektronických obchodech, uživatelské předvolby apod. Myšlenku cookies navrhl v 90. letech Lou Montulli, pracující tehdy u firmy Netscape Communications. Název cookie – sušenka asociuje zvyklost ze Spojených států nebo Velké Británie nabídnout účastníkům určitého zájmového spolku nebo skupiny jejich oblíbenou sušenku pro vytvoření příjemnější atmosféry. K tomu více viz www.cs.wikipedia.org/wiki/HTTP_cookie

56 K otázce právní povahy cookies jako osobního údaje srovnej současný návrh nařízení o ochraně údajů v EU (viz část 4.4.13 této publikace), jakož i související publikace, např. KIM, Nancy S. Clicking and Cringing. Oregon Law Review. 2007 July 30, vol. 86, No. 3, 2007, s. 797, 799; OPPENHEIMER, Max Stul. Consent Revisited. 12 J. Internet L. 3, 3 (2010).

57 Viz KIM, Nancy S. Clicking and Cringing. 86 *OR. L. REV.* 797, 799 (2007); OPPENHEIMER, Max Stul. Consent Revisited. 12 J. *Internet L.* 3, 3 (2010), s. 800.

58 PRESTON, B. a T. CROWTHER. Infancy Doctrine Inquiries. *Santa Clara Law Review.* 2012, vol. 52, s. 47.

59 Tyto podmínky např. stanoví, že „Google si vyhrazuje právo (nikoli však povinnost) předem prověřit, zkontrolovat, označit, filtrovat, upravit, odm*ítnout nebo odstranit jakýkoli Obsah z jakékoli Služby.*" Viz Google Terms of Service 8.3. Dostupné z: www.google.com/accounts/TOS

60 Podmínky společnosti Facebook jsou v tomto ohledu o poznání jasnější, v zásadách ochrany soukromí Facebooku je uvedeno, že *„vaše informace můžeme poskytnout na základě zákonného požadavku (např. na základě příkazu k*

Obsah takto uzavíraných smluv může být kvalifikován jako poměrně nevyvážený, případně nerovný či nemravný, navíc vytváří evidentní prostor k případnému budoucímu zásahu do soukromí jednotlivců. V prostředí českého práva tak může být dovozována neplatnost takovýchto smluv, ať již částečná nebo úplná, přičemž potřebnou oporu pro takový závěr o neplatnosti pak lze najít jak z titulu zákonné správněprávní úpravy (viz např. problematická povaha a kvalita informovaného souhlasu), tak i základního občanskoprávního režimu ochrany dobrých mravů, podle kterého nesmí výkon práv a povinností vyplývajících z občanskoprávních vztahů bez právního důvodu zasahovat do práv a oprávněných zájmů jiných a nesmí být v rozporu s dobrými mravy (§ 3 odst. 1, § 39 a násl. ObčZ). Uvedený rozpor může být demonstrován na příkladu těch smluv, které podmiňují poskytování určitých služeb vyslovením neurčitého a rozsahově bezbřehého souhlasu s předáním osobních údajů třetím subjektům. Formu a kvalitu takovéhoto souhlasu nutno s ohledem na nezadatelnost těchto práv považovat za svého druhu podmínku platnosti, v tomto ohledu nelze připustit jakoukoliv jeho bezbřehost či neomezenost. Pokud je souhlas udělen (k předání osobních údajů třetímu subjektu), musí z něj jednoznačně vyplývat nejen identifikace tohoto subjektu, ale minimálně také účel, pro který bude osobní údaje zpracovávat. Neomezený souhlas, resp. vázaný toliko na další neurčité poskytování údajů za účelem reklamy či přímého marketingu, aniž by byl blíže určen či identifkován subjekt, kterému budou osobní údaje poskytnuty, nemůže požívat soudní či jiné obdobné ochrany.

Jde navíc o praxi natolik rozšířenou, že ji zcela jistě nelze označit za výjimečnou, naopak stoupá riziko, že právě tímto způsobem dochází k postupnému snižování určitého existujícího standardu v očekávání ochrany soukromí. Praxe tak nepochybně postupně mění standardy očekávání ochrany soukromí. Těžko pak lze argumentovat přiměřeným očekáváním této ochrany tam, kde poskytovatelé on-line služeb již od samotného počátku jejich poskytování výslovně popírají, že by taková ochrana byla dána a existovala, tím spíše, že naprostá většina uživatelů s takovými pravidly vyjádřila souhlas.

Takový přístup však zcela jistě nelze považovat za ideální, jakkoliv respektuje autonomii vůle stran, zejména ne tehdy, je-li aplikován bez předem daných zákonných limitů a omezení.[61] Bezbřehá aplikace tohoto přístupu vede např. k tomu, že uživatel, který uveřejní soukromou informaci na stránkách sociální sítě, automaticky může přicházet o jakoukoliv další kontrolu nad touto informací, a to zcela bez ohledu na to, jaká „pravidla" ochrany svého soukromí pro tuto informaci nastavil,[62] neboť dal vědomě svůj materiál k dispozici společnosti tuto sociální síť provozující jako třetí straně komunikace obsahu.[63] Důsledkem toho by prakticky veškerá

prohlídce, soudního příkazu nebo předvolání), budeme-li mít v dobré víře za to, že to po nás zákon požaduje." FACEBOOK DATA USE POLICY (verze ze dne 11. prosince 2012). Dostupné z: www. facebook.com/full_data_use_policy

61 Pro úplnost je nutné uvést, že v teritoriálním prostředí České republiky (případně EU) je situace zcela jiná, a to zejména s ohledem na poměrně přísnou veřejnoprávní regulaci v oblasti správně-právní (viz kapitola 4 této publikace), vzhledem ke globální povaze Internetu však nejde o řešení dostatečné.

62 Facebook umožňuje uživatelům kontrolovat, kdo má právo vidět vložený obsah, nastavením individuální ochrany soukromí, která sahá od sdílení „Jen s přáteli" až po sdílení s širokou veřejností. *FACEBOOK DATA USE POLICY* (verze ze dne 11. prosince 2012). Dostupné z: www. facebook.com/full_data_use_policy

63 V tomto ohledu se pro tento princip používá pojem doktrína třetí strany (third party doctrine). Více k tomu viz výše.

on-line aktivita přestala být chráněna režimem přiměřeného očekávání ochrany soukromí, jelikož většina webových stránek a on-line služeb vytváří záznam „běžné obchodní transakce", jako jsou návštěvy stránek, sdílený obsah a ostatní související údaje. Absence této ochrany má za následek, že celá řada subjektů může mít z vůle těchto poskytovatelů přístup k informacím soukromého charakteru bez nejmenší angažovanosti zákonem zmocněných orgánů k tomuto přístupu (např. formou příkazu k domovní prohlídce atd.). Soudní praxe[64] zatím nedává uspokojivé odpovědi na aplikaci těchto otázek v prostředí Internetu, nicméně některé soudy[65] se k této otázce stavějí poměrně jednoznačně.[66]

2.4 „Lesk" a bída soukromí na dvou příkladech z prostředí informační společnosti

Pozornost, která je obvykle věnována ochraně soukromí v prostředí Internetu, se zaměřuje zejména na velmi úzký okruh otázek počínaje zveřejňováním dlužníků (fyzických osob) jako formy sankce až po zpřístupnění materiálů různého typu a významu (např. intimní fotografie apod.). Právní literatura se tomuto tématu vyhýbá buď úplně, případně se věnuje širším otázkám ochrany soukromí u technologií využívanými orgány státu. Právo na soukromí se však uplatňuje i daleko nad rámec těchto oblastí, jež si zasluhují samostatnou analýzu. Pohlédneme-li na současnou judikaturu, je diskuse o právu na ochranu soukromí v osobních počítačích a osobní e-mailové korespondenci jen dokladem toho, že pevné body neexistují a vše je na pouhém začátku. Následující příklady ukazují, kde tradiční způsoby ochrany soukromí v prostředí informační společnosti selhávají a kde soudy a další orgány ochrany ještě musejí jasně definovat jejich hranice.[67]

V současné době ukládá většina uživatelů svá soukromá data na svém osobním počítači, tabletu či mobilním telefonu, jde-li o data vytvářená v prostředí sociálních sítí jsou pak automatizovaně ukládána v cloudovém úložišti (obvykle s přístupem uloženým v tomto zařízení ve formě HTTP cookies). V tomto ohledu soudy opakovaně konstatovaly, že *„v obecné rovině má jednotlivec ve vztahu ke svému osobnímu počítači objektivně přiměřené očekávání ochrany soukromí"*. [68]Toto přiměřené očekávání *„se však může snížit chováním dané osoby při práci s počítačem"*.[69] Soudy tak například došly k závěru, že sdílení těchto osobních souborů (na veřejné síti)

64 DITZION, Robert E. Note, Electronic Surveillance in the Internet Age: The Strange Case of Pen Registers. *Am. Crim. L. Rev.* 2004, vol. 41, s. 1321, 1334.

65 CROWTHE, B., ref. 40, s. 343.

66 Například Soud 9. okrsku v případu Spojené státy americké proti Forresterovi rozhodl, že *„uživatelé e-mailové komunikace a Internetu nemají žádná očekávání ochrany soukromí, pokud jde o adresy jejich zpráv nebo IP adresy webových stránek, které navštěvují, jelikož by měli vědět, že tyto informace předávají poskytovatelům internetových služeb, kteří je používají"*.

67 CROWTHE, B., ref. 40, s. 344.

68 *Spojené státy americké proti Ganoeovi,* 538 F.3d 1117, 1127 (9. okrsek 2008).

69 *Spojené státy americké proti Ahrndtovi,* č. 08-468-KI, 2010 WL 373994, s. *12–15 (D. Or. 28. ledna 2010); viz také Ganoe, 538 F.3d s. 1127 (konstatující, že očekávání ochrany soukromí žalovaného zaniklo zároveň s jeho

zakládá ztrátu práva na legitimní očekávání ochrany soukromí.[70] Soudy tedy vycházejí v tomto ohledu z kritéria chování konkrétního uživatele ve vztahu k ochraně svých soukromých dat, a podle toho pak dovozují míru poskytnuté ochrany soukromí v konkrétním případě. Zcela jasný a soudy dovoditelný zájem na ochraně soukromí svého počítače má například ten, kdo má počítač doma,[71] který je chráněn heslem[72] a není připojen na žádnou síť. Tato situace chrání i vymazané soubory, i když podle tradičního pojetí práva na ochranu soukromí k opuštěným věcem právo na ochranu soukromí neexistuje (taková analogie je však nepřiléhavá). Kromě toho uznaly soudy rovněž to, že „pouhé připojení se na síť ještě samo o sobě očekávání ochrany soukromí neruší".[73] V reálném prostředí Internetu by však měl jeho uživatel rozumně očekávat, že přichází minimálně o tu část svého soukromí, která se opírá o doprovodné údaje identifikující jeho počítač v této síti (viz problematika tzv. cookies řešena níže). Například jen tím, že zašle své informace poskytovateli internetových služeb nebo dokonce mobilnímu operátorovi, poskytuje přístup ke svým informacím, včetně své IP adresy, i státu.[74]

Např. soudy ve Spojených státech obvykle považují internetové identifikátory (nikoliv tedy jen IP adresu, ale další doprovodné údaje) za údaje, které jsou mimo sféru soukromých zájmů jednotlivce, jelikož jsou využívány elektronickými službami třetích stran.[75] Problematickým aspektem tohoto odůvodnění je, že mnoho uživatelů ani neví, že tyto identifikátory někomu sděluje. Většina uživatelů zcela jistě neudělala pro poskytnutí těchto identifikátorů úmyslně nic jiného, než si tyto webové stránky otevřela, což lze jistě jen těžko považovat za vyjádření souhlasu k zásahu do vlastního soukromí. Kromě toho, že jednotlivci pasivním způsobem poskytují informace na Internetu, se příslušným orgánům činným v trestním řízení dostalo obrovské volnosti v tom, že mohou libovolně shromažďovat informace o vybraných subjektech pomocí on-line nástrojů, aniž by si k tomu musely opatřovat soudní příkaz k prohlídce.[76] To se ukázalo jako extrémně praktické v případech, kdy zákon připouští, aby byl odpovědný uživatel určen zejména prostřednictvím IP adresy zjištěné na základě kvalifikovaného dotazu určené-

„rozhodnutím instalovat a používat software na sdílení souborů, a tudíž tím otevřel svůj počítač komukoli, kdo má stejně volně dostupný program").

70 Viz např. *Spojené státy americké proti Stultsovi,* 575 F.3d 834 (8. okrsek 2009).

71 *Viz Spojené státy americké proti Lifshitzovi,* 369 F.3d 173, 190 (2. okrsek 2004) („Jednotlivci obecně mají přiměřené očekávání ochrany soukromí ve svých doma instalovaných počítačích."); *Guest proti Leisovi,* 255 F.3d 325, 333 (6. okrsek 2001) („Vlastníci domů by samozřejmě měli přiměřené očekávání ochrany soukromí, pokud jde o jejich domovy a osobní věci —včetně počítačů—nacházejících se doma.").

72 Některé soudy uznaly, že ochrana heslem a zašifrování dává uživateli právo na větší míru ochrany soukromí. (*Spojené státy americké proti Andrusovi,* 483 F.3d 711, 718 (10. okrsek 2007).

73 *Spojené státy americké proti Heckenkampovi,* 482 F.3d 1142, 1146 (9. okrsek 2007).

74 *Spojené státy americké proti Perrinemu,* 518 F.3d 1196, 1204–05 (10. okrsek 2008).

75 K tomu srovnej evropský systém ochrany soukromí (viz část 4 této práce). Jinak *White proti Bakerovi,* 696 F. Supp. 2d 1289, 1303 n. 9 (N.D. Ga. 2010).

76 Viz *Spojené státy americké proti Ganoeovi,* 538 F.3d 1117, 1127 (9. okrsek 2008) (využívající software „peer--to-peer"); *Spojené státy americké proti Courtneymu,* č. 4:07CR261 ILH, 2008 U.S. Dist. LEXIS 109344, s. *5–6 (E.D. Ark. 22. září 2008) (zabývající se chatovými místnostmi, hledáním na Internetu a stránkami sociálních sítí); *Spojené státy americké proti Carterovi,* 549 F. Supp. 2d 1257, 1259 (D. Nev. 2008) (vkládání odkazů na „dummy" webové stránky s dětskou pornografií za účelem zaznamenávání IP adresy uživatelů).

mu poskytovateli připojení k internetu.[77] Tento postup se ukázal jako obzvláště efektivní při sledování a stíhání pachatelů trestné činnosti v oblasti dětské pornografie a ostatních deliktů realizovaných on-line.[78] Nicméně za tato bezpečnostní opatření lidé platí ztrátou soukromí v tomto prostředí. Nejbližší analogie tradičního prostředí k výše uvedenému opatření státu je shromažďování záznamů o telefonních hovorech od příslušných poskytovatelů služeb, jelikož obě opatření zahrnují předávání průběžných informací externí společnosti při používání jejích služeb. Množství informací, které lze shromáždit digitálně, je však daleko větší než objem dat, který měly orgány činné v trestním řízení běžně k dispozici ze záznamů o telefonních hovorech. Pokud si soudy těchto rozdílů všimnou a budou s nimi i tak zacházet, možná se jim podaří zformulovat právo, které bude poskytovat větší ochranu soukromí při činnostech, které se provádějí na soukromých počítačích, a to i tehdy, když jsou jejich uživatelé připojeni na Internet.[79]

Další typickou oblastí, kde se analýza přiměřeného očekávání ochrany soukromí hroutí, je ochrana soukromých e-mailů. Soudy obvykle docházejí k závěru, že zaměstnavatel může monitorovat (zachycovat a číst) e-maily svých zaměstnanců, zejména pak v těch případech, když má tuto možnost zakotvenou ve smluvních podmínkách (zejména v pracovní smlouvě či vnitřních předpisech zaměstnavatele).[80] To dává smysl, jelikož e-mailovou schránku (systém) poskytl zaměstnavatel a jeho zaměstnanci s tím souhlasili jako s podmínkou trvání svého pracovního poměru. Je však nutné zvážit, zda i zde nedochází k zásadním rozdílům od ochrany v běžném, tj. listinném světě přepravy a uchovávání listinných písemností. Tradičním pravidlem ochrany písemností (listinných) je skutečnost, že tyto listiny jsou zásadně chráněny především v průběhu jejich přepravy, tj. do okamžiku jejich doručení skutečnému adresátovi.[81] V tomto ohledu je také důsledně rozlišován samotný právní režim jejich ochrany. Relativně méně je tak např. chráněna vnější forma zásilky (např. údaj o odesílateli, adresátovi, hmotnosti apod.), samotný obsah zásilky je pak obvykle podřízen zvláštní ochraně formou veřejnoprávní (správněprávní, případně trestněprávní) regulace.[82] Ačkoliv analogie mezi listinnou (papírovou) a elektronickou podobou nezřídka[83] selhávají, v tomto případě je nutné uvést, že e-mail je s tradiční listinnou poštou zcela srovnatelný, byť nikoli ve všech aspektech.

77 Nutno však pro úplnost konstatovat, že samotná identifikace uživatele skrze IP adresy nestačí, jde pouze o nepřímý důkaz identifikující obvykle pouze příslušní počítač, nikoliv přímo osobu, která však může být identifikována prostřednictvím celé řady dalších nepřímých důkazů, včetně např. výsledků forenzní analýzy konkrétního počítače, atd. Viz např. *Spojené státy americké proti Stultsovi,* 575 F.3d 834, 838 (8. okrsek 2009).

78 Viz např. *Spojené státy americké proti Haffnerovi,* č. CR-337-J-34-TEM, 2010 WL 5296920, s. *2 (M.D. Fla. 31. srpna, 2010); *Spojené státy americké proti Ahrndtovi,* č. 08-468-KI, 2010 WL 373994, s. *2 (D. Or. 28. ledna 2010); *Spojené státy americké proti Christiemu,* 570 F. Supp. 2d 657, 690 (D.N.J. 2008).

79 CROWTHE, B., ref. 40, s. 323.

80 Viz např. *Spojené státy americké proti Simonsovi,* 206 F.3d 392, 398, Soud 4. okrsku, kde soud dovodil, že není dáno žádné legitimní očekávání ochrany soukromí při práci s Internetem, pokud strategie firmy umožňuje sledování „všech přenosů souborů, všech navštívených stránek a všech e-mailových zpráv.

81 Tento princip je v zásadě realizován celosvětově, k tomu více RAY, A. The Warrantless Interception of E-mail: Fourth Amendment Search or Free Rein for the Police? *Rutgers Computer & Tech. L. J.* 2010, vol. 36, s. 178, 200.

82 Např. v USA platí tato ochrana pouze pro ty případy, pokud je poštovní zásilka „zapečetěná", a tudíž například nechrání nezabalený časopis nebo noviny.

83 Viz příklad elektronického podepisování ve světle otázek jejich průkaznosti, otázek intertemporálních apod.

Základní rozdíl spočívá především ve skutečnosti, že e-maily jsou obvykle zasílány prostřednictvím třetí strany (poskytovatele služeb), nikoliv tedy přes státem garantovanou (licencovanou) autoritu, dále pak v tom, že e-mail je přenášen v nehmotné podobě, která přispívá trvalému uložení, které může být navíc realizováno na různých místech a v dispozici různých subjektů (např. v cloudu[84] apod.). Tyto rozdíly však z pohledu očekávání soukromí nejsou příliš významné, lze tak jen těžko argumentovat, že by se e-mailu mělo dostávat menší právní ochrany než běžné (papírové) poště. Problém však místy nastává u konkrétní aplikace, kdy nelze s dostatečnou mírou jistoty např. dovozovat rozsah práv jednotlivce ke konkrétním datům nacházejícím se mimo jeho přímou působnost (soukromí zpráv uložených na cizích serverech atd.).[85] Obecně tak bylo ve většině zemí[86] judikováno, že obsah e-mailů je chráněn v zásadě stejně jako obsah telefonických hovorů. Obsah e-mailu obvykle splňuje konvenční kritéria vztahující se na to, co se uživatel snaží chránit jako soukromé, ochrana by tedy měla být poskytována automaticky. Další otázkou související s mírou platnosti a respektem k soukromí je možný rozsah dispozice s obsahem uchovávaných zpráv u těchto poskytovatelů, kdy dochází k automatickému prohledávání tohoto obsahu ve quasi-veřejném zájmu (např. prověřování, zda zprávy neobsahují pornografický materiál, autorsky chráněný obsah nebo viry).

Analýza takovéhoto jednání a jeho právní kvalifikace je samozřejmě závislá na podobě konkrétní právní úpravy, která bude aplikována na základě zjištění rozhodného práva. Obvykle nebude činit zásadní problémy tam, kde existuje přímá úprava právním předpisem,[87] nicméně i v těchto případech není zcela jasný rozsah možné dispozice s tímto obsahem na základě výslovného zmocnění v konkrétní smlouvě mezi uživatelem a poskytovatelem (viz např. taková smluvní úprava, která zakládá odpovědnost poskytovatele za obsah, přičemž jej zároveň zavazuje k tomu, aby realizoval pravidelné audity, kontroly sledování obsahu). Právě otázka platnosti těchto smluv se dnes ukazuje jako obzvláště velký problém, jelikož velcí poskytovatelé služeb obsahu (Internetu) v mnoha ohledech zneužívají svého silného postavení a reálnou ochranu soukromí (přiměřeného očekávání) svými podmínkami služeb neposkytují, což může vést i k samotné neplatnosti těchto smluv (dle českého práva např. pro rozpor s dobrými mravy atd.). Rozhodování, zda je soukromý zájem ohledně obsahu dán, může v řadě případů záviset na celé řadě faktorů, bezpečnostními opatřeními (viz např. šifrování)[88] počínaje a konkrétními smluvními podmínkami

84 Viz např. pojem Cloud computing, tedy počítačovou technologii, kterou lze charakterizovat jako poskytování dat, služeb či programů uložených na serverech na Internetu s tím, že uživatelé k nim mohou přistupovat například pomocí webového prohlížeče nebo klienta dané aplikace a používat je prakticky odkudkoliv. Nabídka aplikací se pohybuje od kancelářských aplikací přes systémy pro distribuované výpočty až po operační systémy provozované v prohlížečích. Tato technologie bývá kritizována, a to např. z důvodů vzrůstajícího nebezpečí ztráty soukromí uživatelů. K tomu více viz např. STALLMAN, R. *Cloud computing is a trap, warns GNU founder Richard Stallman*. Dostupné z: www.guardian.co.uk/technology/2008/sep/29/cloud.computing.richard. stallman

85 CROWTHE, B., ref. 40, s. 341.

86 V USA viz např. případ *Warshak proti Spojeným státům americkým* z roku 2007. V případu *Warshak* potvrdil senát Soudu 6. okrsku předběžné opatření proti státu, který sledoval Warshakovu e-mailovou komunikaci prostřednictvím jeho poskytovatele e-mailových služeb (490 F.3d 455, Soud 6. okrsku).

87 Tak je tomu např. v rámci EU.

88 To by zároveň mohla být přijatelná analogie k „zalepení" listinné poštovní zásilky.

konče. Důsledkem této situace je právní nejistota, jakož i skutečnost, že ochrana soukromí, která je vlastní každému jednotlivci, je vystavena bezbřehým zásahům ze strany státu, poskytovatelů dotčených služeb i třetích stran. To ve svém důsledku oslabuje samotné lidské právo na soukromí, jež by mělo být jinak zaručeno ve všech procesních postupech těchto subjektů.[89]

Klíčová slova

Axiologie, přiměřené očekávání, autonomie vůle, rozumné očekávání, hranice, identifikátory, e-mail, počítač, historie soukromí, konflikt, ústavní záruky, nezadatelná a nezcizitelná práva.

89 CROWTHE, B., ref. 40, s. 343.

— Kapitola 2.

3 Některá metodologická východiska a kolize autonomie vůle s právem na soukromí

3 Některá metodologická východiska a kolize autonomie vůle s právem na soukromí

3.1 Úvodní teze (metodologické) — 51

3.2 Specifický předmět ochrany soukromí — 52

3.3 Kolize soukromí s jinými hodnotami a způsoby jejich řešení — 53

Klíčová slova — 56

3 Některá metodologická východiska a kolize autonomie vůle s právem na soukromí

„Nesmět říkat, co si myslím, je úděl otroků…"[90]
Eurípidés

3.1 Úvodní teze (metodologické)

Jednou ze základních otázek, která by měla mít své místo při výběru nezbytného metodologického východiska pro jakoukoliv práci s právem, je míra aplikace takovéhoto východiska na konkrétní skupinu či oblast právních norem. Takto lze buď hledat vhodné metody pro aplikaci práva (např. formou aplikace konkrétního právního institutu na skutkový děj), případně se zajímat o hodnocení práva[91] *per se* a jeho výstupů (např. řešení otázek týkajících se vhodnosti, úplnosti, rozsahu a rozumnosti právní úpravy). Tato východiska se obvykle více či méně opírají o určité argumentační hledisko, jehož charakter je v rovině argumentativní obvykle skládán z metod analytických, logických, systematických, případně komparativních anebo syntézy.

Samotná metodologická východiska pak musejí nutně obsahovat kromě deduktivních i induktivní aspekty právního myšlení. Takovouto charakteristiku právně teoretické orientace podává např. V. Knapp,[92] když dovozuje, že právní věda není axiomatická, ale argumentativní. To znamená, že poznání práva, právních institutů atd. a důsledně ani zjištění quid iuris v určitém případu nelze odvozovat od axiomů, nýbrž je zpravidla třeba se ho dobrat argumentací pro jednu z několika možností. Paralelně je pak problematika právní argumentace zkoumána v systematických pracích metodologických, jež utvářely[93] existující interpretační a aplikační přístupy. Samotná právní argumentace tak má být nejenom racionální, ale zároveň také etická. V. Knapp[94] v tomto ohledu uvádí, že jedním z nejdůležitějších etických postulátů vědecké práce je vědecká skromnost. Tato skromnost není přirozeně v rozporu s požadavkem vědecké odvahy. Odvahy je třeba při vyhledávání a řešení problémů, skromnosti je třeba při hodnocení a prezentování výsledků vlastní práce. Vědeckého sebevědomí je jistě zapotřebí, ale přemírné sebevědomí, ústící v přesvědčení, že vlastní názor je nevyvratitelně správný a moudrý, je v rozporu s vědeckou etikou, stejně jako přezírání názorů jiných, nedostatek sebekritické schopnosti revidovat svůj vlastní vědecký názor (a to ať na základě kritiky, nebo z vlastního podnětu), vědecká

90 Euripides ze Salaminy (480–406 př. n. l., starořecký dramatik, klasik tragédie, básník a filozof). Citace výroku Euripida ze Salamíny in HERCZEG, J. *Meze svobody projevu*. 1. vyd. Praha: Orac, 2004, s. 5.

91 K tomu srov. SOBEK, T. *Argumenty teorie práva.* Praha: Ústav státu a práva AV ČR; Plzeň: Aleš Čeněk, 2008. s. 268.

92 KNAPP, Viktor. *Teorie práva.* 1. vyd. Praha: C. H. Beck, 1995. 247 s. ISBN 80-7179-028-1, s. 54.

93 Viz např. ALEXY, R. *Theorie der juristischen Argumentation.* Frankfurt a. M., 1978; LARENZ, K. *Methodenlehre der Rechtswissenschaft.* Berlin-Heidelberg-New York, 1960; BYDLINSKI, F. *Juristische Methodenlehre und echtsbegriff.* Wien-New York, 1982; KOCH, H.-J. a H. RÜßMANN. *Juristische Begründungslehre.*

94 KNAPP, V. *Vědecká propedeutika.* Bratislava, 1993, s. 237.

svéhlavost a neochota přiznat vlastní omyl atd. I požadavek vědecké skromnosti tedy souvisí s požadavkem vědecké poctivosti.

3.2 Specifický předmět ochrany soukromí

Málokterá hodnota je právem natolik jasně konkretizována, že její předmět ochrany je vymezen natolik jasně a zřetelně a její hledání se omezuje toliko na přiřazení konkrétního skutkového děje ke konkrétní právní normě. Realizace práva na soukromí, a to zejména ve svém ústavněprávním, případně civilněprávním rozměru, tak patří k těm nejproblematičtějším aktům aplikace práva. Důvodem je zejména skutečnost, že nalézání konkrétního obsahu těchto hodnot (viz pojem soukromí výše) připomíná spíše složitý proces vyvažování více vzájemně proti sobě stojících hodnot či principů, který postrádá jasně vymezené mantinely a závisí spíše na konkrétním kontextu, skutkovém ději, jakož i konkrétním chování člověka a jeho očekávání. Tyto mantinely mohou být vysoce variabilní, mají svůj subjektivní základ, přičemž je lze jen velmi těžko předem jednoznačně vymezit či blíže strukturovat. Připustíme-li například, že oblast sexuálního života vždy spadá pod ochranu soukromí, musíme v konkrétních případech zohlednit také ty případy, kdy takováto ochrana bude samotným subjektem této ochrany vědomě odmítána, a to např. s odkazem na subjektivní potřebu sexuálního exhibicionismu. V takovém případě je nutné zvážit, zda určitá konkrétní oblast, která jinak pod ochranu soukromí (jeho sféry) spadá, nebude z této sféry vyňata, a to buď na základě důvodů objektivních (např. ochrana zdraví), případně subjektivních, tj. z vůle konkrétního subjektu ochrany, který konkrétní oblast své (např. sexuální) aktivity ze svého soukromí dobrovolně vyloučil.[95] Autonomie vůle člověka (jako subjektu ochrany soukromí) a jeho chování tak určuje rozsah a mantinely této ochrany. Problémem aplikace této právní úpravy tedy nebývá obvykle znalost či výklad práva (byť i to není výjimkou), ale zejména odpovědné posouzení konkrétního kontextu chování člověka ve všech jeho souvislostech.

Z pohledu všech skutečností spadajících pod ochranu soukromí je nutno pro úplnost konstatovat, že taxativní výčet těchto skutečností není a ani nemůže být rozumně definován. Více než jinde zde tedy platí, že každá definice je nebezpečná.[96] Soukromí je hodnota proměnlivá kulturně, historicky i subjektivně. Nelze ji tedy ani generalizovat na konkrétní kontury či tvary této ochrany,[97] když jde o ochranu natolik propojenou s životem člověka, jeho chováním, očekáváním, jakož i sociálním, kulturním a ve svém důsledku i technologickým prostředím.

95 K tomu více viz např. rozsudek Evropského soudu pro lidská práva ve věci *Laskey, Jaggard a Brown proti Spojenému království Velké Británie a Severního Irska,* ze dne 19. února 1997, kde se soud zabýval vyloučením určitých sexuálních aktivit z ochrany soukromého a intimního života. Meritem této věci byl rozsah skutečností chráněných právem na soukromí.

96 Viz výše uvedená zásada *omnis definitio (in iure) periculosa es.*

97 K tomu opačně viz RYŠKA, M. Ochrana vnitřního kruhu i jeho okolí v praxi práva na ochranu osobnosti. In: V. ŠIMÍČEK, ed. *Právo na soukromí.* Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2011, s. 79 a násl.

Nejistota proto nepanuje pouze ve vztahu k rozsahu takto subjektivně chráněných oblastí, ale také v rovině objektivního práva, kde nemusí být jednoznačně oddělitelná samotná soukromá sféra života člověka (tedy chráněná oblast) od sféry veřejné, kam tato ochrana nedopadá. Uvedené lze demonstrovat na příkladu vnitřních prostor běžného automobilu, kde je nutné připustit, že poskytnutí ochrany soukromí těmto prostorům může být v obecné rovině velmi nejisté (např. ve srovnání s ochranou obydlí), byť jistě nelze tuto ochranu zcela vyloučit. V tomto ohledu bude opět nutné zvážit všechny okolnosti, zejména pak skutečnost, že automobil může být svého druhu obydlí (např. pro bezdomovce), míra rozumného očekávání bude nepochybně jiná na zadních sedadlech a jiná na sedadle řidiče, jiná v nákladovém prostoru apod. Podobně bude významná povaha užití tohoto automobilu pro posouzení případných zásahů do soukromí realizovaných formou GPS přijímačů lokalizujících pohyb řidiče atd. apod.

Vzhledem k této povaze soukromí lze konstatovat, že právo na ochranu soukromí, zejména pak jeho civilněprávní část, bývá u nás tradičně chápáno jako právo silně dotvářené rozhodovací praxí s výraznou absencí pevných normativních základů, když zákonná právní úprava spíše naznačuje, než řeší. V tomto ohledu je pak nutné rozlišovat správněprávní oblast (u nás upravenou zvláštním zákonem), která vychází z evropského modelu ochrany, který je v tomto smyslu výrazně ochranářský, přičemž autonomie vůle člověka nepředstavuje zásadní prvek, na kterém tato ochrana spočívá (k tomu více viz podrobný rozbor v části 4).

Soukromí tak představuje jen velmi těžko popsatelnou hodnotu, jejíž hranice se mění, vytváří, mizí a přetváří v průběhu života člověka. Jde tedy o nikoliv nutně stálou a neproměnlivou sféru života, v níž může člověk žít svůj osobní život dle své aktuální vůle a představ, tj. s minimem možných zásahů z vnějšího (veřejného) světa.[98] Právo na soukromí tak implikuje svého druhu možnost seberealizace v reálném čase a nerušeného rozvoje své osobnosti, včetně širokého portfolia dílčích práv (např. právo na respektování soukromého a rodinného života, včetně souvisejícího práva vytvářet a rozvíjet vztahy s ostatními lidskými bytostmi atd.).[99]

3.3 Kolize soukromí s jinými hodnotami a způsoby jejich řešení

Každý jednotlivý zásah do práva na ochranu soukromí musí být posuzován individuálně se zřetelem ke všem okolnostem dané věci. V této souvislosti je zejména nutné uvést, že žádné právo nelze *per se* absolutizovat a nadřazovat nad jiná práva, která musejí být v dané věci aplikována současně. Takový stav obvykle nazýváme kolizí, kde je v rámci právní argumentace nutné zvažovat především existující účel a smysl každého jednotlivého zásahu. Takovým zásahem do práva na ochranu soukromí může být svoboda projevu, právo na informace, případně jiný veřejný zájem[100] či hodnota.

Při aplikaci konkrétního zákonného ustanovení je pak nutné mít na zřeteli zejména

98 K tomu srovnej KNAP, K., J. ŠVESTKA, O. JEHLIČKA, P. PAVLÍK, a V. PLECITÝ. *Ochrana osobnosti podle Občanského práva,* s. 130.

99 Viz např. rozsudek Evropského soudu pro lidská práva ze dne 16. 12. 1992 ve věci *Niemitz vs. Německo.*

100 Např. dosažení účelu trestního řízení apod.

ústavněprávní, případně lidskoprávní rozměr celého problému, zejména tu část, která se týká poměřování všech ústavou garantovaných práv, tedy práv na stejné úrovni. Poměřování práv je relativně běžnou agendou většiny ústavních soudů, byť tato úvaha bývá nezřídka aplikována i na úrovni soudů obecných. Ústavní soud se v jednom ze svých aktuálních rozhodnutí[101] (byť argumentačně nikoliv nově)[102] vyjádřil k otázce svobody projevu a právem svobodně vyjadřovat své názory. Ústavní soud při posuzování této otázky vycházel především z toho, že toto právo a svoboda je obsahově omezeno právy jiných, přičemž tato práva mohou vyplývat jako ústavně zaručená z ústavního pořádku republiky či z jiných zábran daných zákonem chránících celospolečenské zájmy či hodnoty. Přitom právo vyjadřovat názory mohou zbavit ústavní ochrany nejen obsahová omezení, neboť i forma, jíž se názory navenek vyjadřují, je úzce spjata s ústavně zaručeným právem, k němuž se upíná. Vybočí-li publikovaný názor z mezí pravidel slušnosti obecně uznávaných v demokratické společnosti, ztrácí charakter korektního úsudku (zprávy, komentáře) a jako takový se zpravidla ocitá již mimo meze ústavní ochrany.[103] Ústavní soud dále výslovně judikoval, že „základní právo podle čl. 17 Listiny je zásadně rovno základnímu právu podle čl. 10 Listiny,[104] přičemž je především věcí obecných soudů, aby s přihlédnutím k okolnostem každého případu zvážily, zda jednomu právu nebyla bezdůvodně dána přednost před právem druhým".[105] Že toto právo není absolutní, lze demonstrovat na tom, že ve vztahu k osobám veřejně známým či politicky činným vychází náš Ústavní soud z přesvědčení, že právo kritiky, zakotvené v čl. 17 odst. 2 Listiny a čl. 10 Úmluvy, které je neoddělitelnou součástí svobody projevu a práva na informace, musí respektovat rovnováhu mezi tímto právem a osobnostními právy konkrétního subjektu a nemůže překračovat určité hranice spojené s atributy demokratické společnosti. Takto vymezené mantinely ve vztahu k fyzické osobě, která jedná či vystupuje jako „veřejná osobnost", jsou širší než ve vztahu k osobě soukromé.

V konkrétním případě je proto vždy nezbytné zkoumat míru (intenzitu) tvrzeného porušení základního práva na ochranu osobnosti (osobní cti a dobré pověsti), a to právě v kontextu se svobodou projevu a s právem na informace a také se zřetelem na požadavek proporcionality uplatňování těchto práv (a jejich ochrany). Zároveň je nutné, aby příslušný zásah bezprostředně souvisel s porušením chráněného základního práva, tj. aby zde existovala příčinná souvislost mezi nimi. V dané věci obecné soudy shledaly, že publikací článků v periodikách a na webových stránkách stěžovatele dotýkajících se soukromé a intimní sféry došlo ke zvlášť závažnému zásahu do osobnostních práv žalobce, a to i přesto, že žalobce je veřejně známou osobu, takže musí snášet vyšší míru kritiky.[106] Ústavněprávní konformní interpretace tohoto ustanovení vede

101 Usnesení sp.zn. II. ÚS 1879/11 ze dne 25. ledna 2012.

102 Ústavní soud se k této problematice vyjadřuje opakovaně ve svých rozhodnutích, materie je poměrně kvalitně shrnuta v rozhodnutí sp. zn. I. ÚS 156/99.

103 K tomu srov. nález sp. zn. III. ÚS 359/96, Ústavní soud: Sbírka nálezů a usnesení. Sv. 8. C. H. Beck, 1998, s. 367.

104 Viz nález sp. zn. II. ÚS 357/96, Ústavní soud: Sbírka nálezů a usnesení. Sv. 9, C. H. Beck, 1998, s. 355.

105 Viz nález sp. zn. IV. ÚS 154/96, Ústavní soud: Sbírka nálezů a usnesení. Sv. 10, C. H. Beck, 1998, s. 113.

106 Z § 13 ObčZ vyplývá, že je možné fyzické osobě, do jejíhož práva na ochranu osobnosti bylo zasaženo, poskytnout morální (odst. 1) nebo i finanční (odst. 2) zadostiučinění. Přitom § 13 odst. 2 ObčZ pro přiznání relutární náhrady předpokládá značnou míru dotčení osobnosti fyzické osoby (samo toto ustanovení uvádí případy, kdy lze

k závěru, že při poskytnutí ochrany osobnosti dotčené fyzické osoby je nezbytné přihlížet i k možné satisfakční roli samotného rozsudku (příp. jiného rozhodnutí) konstatujícího neoprávněnost zásahu. Proti výše uvedenému závěru obecných soudů, opřenému o výklad § 13 ObčZ, který představuje zákonný limit pro ústavně zaručenou svobodu projevu, nemá Ústavní soud z ústavněprávního hlediska žádné výhrady. V této souvislosti naopak ještě zdůrazňuje, že právo na osobní čest a dobrou pověst vyplývající z čl. 10 Listiny je v situaci, kdy se jedná o zásah do soukromé až intimní sféry dotčené osoby, rozhodně hodno ochrany v intenzivnějším měřítku než při běžných hodnotících úsudcích. Výše uvedený postup Ústavního soudu představuje svého druhu aplikaci tzv. testu proporcionality, který se podle stávající judikatury (srov. např. nález Ústavního soudu Pl. ÚS 4/94) sestává ze tří kroků,[107] resp. posouzení (hodnocení) zásahu dle kritéria:

1. **vhodnosti,** jehož obsahem je zvažování zásahu z pohledu možného naplnění sledovaného účelu, který musí být legitimní (není-li daný zásah způsobilý sledovaného účelu dosáhnout, jde o projev svévole, jenž se považuje za rozporný s principem právního státu),
2. **potřebnosti,** jež sleduje analýzu plurality možných prostředků ve vztahu k zamýšlenému účelu a jejich subsidiaritu z hlediska omezení ústavou chráněné hodnoty – základního práva nebo veřejného statku (lze-li sledovaného účelu dosáhnout alternativními prostředky, je pak ústavně konformní ten, jenž danou ústavně chráněnou hodnotu omezuje v míře nejmenší,
3. **proporcionality** ve smyslu vážení proti sobě stojících ústavních hodnot (jde tak o metodologii svého druhu, jejíž aplikační podmínkou je skutečnost, že prověřovaný zásah směřuje k ochraně ústavně chráněné hodnoty a zároveň jinou takovou hodnotu omezuje).

Výše uvedený test proporcionality pramení spíše z právní filozofie než z pozitivistické právní argumentace. Jde o svého druhu navázání na Dworkinovu[108] teorii právních principů, zformulovanou jako argumentační instrumentárium Hartovy právně-pozitivistické koncepce, na kterou navázal Alexy,[109] který tuto teorii propojil se zásadou proporcionality. Jak výstižně uvádí P. Holländer,[110] má tento test řadu oponentů, přičemž hlavními argumenty proti jeho

s ohledem na intenzitu zásahu proti osobnosti fyzické osoby přiznat náhradu nemajetkové újmy v penězích pouze demonstrativně), a to za situace, kdy by se tak nejevilo postačujícím morální zadostiučinění podle § 13 odst. 1 ObčZ. NObčZ na tuto problematiku hledí v zásadě obdobně, byť zákon zde vychází z principu, že k zachycení, rozšiřování a použití podoby člověka nebo údajů týkajícího se člověka nebo jeho projevů osobní povahy je nutno jeho svolení (§ 84–87), přičemž zde výslovně uvádí, že tohoto svolení není třeba, pokud se podobizna nebo zvukový či obrazový záznam pořídí nebo použijí k výkonu nebo ochraně jiných práv nebo právem chráněných zájmů jiných osob (§ 88 odst. 1), svolení pak není třeba ani v případě, když se podobizna, písemnost osobní povahy nebo zvukový či obrazový záznam pořídí nebo použijí na základě zákona k úřednímu účelu nebo v případě, že někdo veřejně vystoupí v záležitosti veřejného zájmu (§ 88 odst. 2).

107 Pro úplnost nutno podotknout, že některé teorie proporcionality rozlišují čtyři stupně testu, přičemž prvním je určení legitimního cíle ochrany.

108 DWORKIN, R. *Když se práva berou vážně.* Praha: OIKOYMENH, 200

109 ALEXY, R. *Theorie der Grundrechte.* 3. vyd., Frankfurt am Main: Suhrkamp, 1996. K teorii Alexyho a Dworkina více např. AGHA, P. *Herkulovo dilema,* Právník č. 2, 2013, s. 1104-1121.

110 HOLLÄNDER, P. Zásada proporcionality: jednosměrná ulice nebo hermeneutický kruh? In: V. ŠIMÍČEK, ed. *Právo na soukromí.* Brno: Masarykova univerzita, 2011, s. 26.

uplatňování jsou námitky svévole takového testu (poměřování), ztráta právní jistoty a negativní vývoj směrem k soudcovskému státu spjatý s omezováním prostoru pro tvorbu práva mocí zákonodárnou, případně mocí výkonnou. Česká právní teorie se podrobné analýze tohoto testu, resp. uplatňování této zásady, věnuje velmi okrajově, případně vůbec. Ojedinělou výjimkou je studie D. Kosaře,[111] v níž je tato zásada kriticky posuzována a zejména je v ní negativně hodnocena nejednotnost při uplatňování této zásady v rozhodovací praxi Ústavního soudu.

Celkově je tedy nutné zcela souhlasit s P. Holländerem,[112] že řešení kolize principů, resp. výše uvedených hodnot, lze skutečně spatřovat v axiologickém rozlišování mezi dobrem a zlem, přičemž v tomto ohledu je pak tím nejdůležitějším předpokladem použití testu proporcionality morální diskurs.

Klíčová slova

Autonomie, dobrá pověst, absolutní práva, relativní práva, právo na osobní čest, ochrana osobnosti, právo na informace, zásada proporcionality, test proporcionality, svoboda projevu, lidská práva

111 K tomu více viz KOSAŘ. D. Kolize základních práv v judikatuře Ústavního soudu ČR. *Jurisprudence*. 1/2008, s. 8.

112 HOLLÄNDER, P., ref. 110, s. 26.

4. Právní regulace ochrany soukromí, její limity a možnosti

4. Právní regulace ochrany soukromí, její limity a možnosti

4.1 Sedes materiae ochrany soukromí — 59
4.2 Evropský systém ochrany soukromí — 61
4.3 Přístup mezinárodní komunity k ochraně osobních údajů a dat — 72
4.4 Správněprávní úprava a její vybrané aspekty — 75
4.4.1 Koncepce právní úpravy a působnost národní autority ochrany dat — 75
4.4.2 Základní zásady v zákoně o ochraně osobních údajů — 78
4.4.3 Pojem osobní údaj jako jeden z klíčových pojmů určující věcnou působnost ZoOÚ — 84
4.4.4 IP adresa a další číselné identifikátory jako kontextuální osobní údaje — 89
4.4.5 MAC adresa, IMEI a IMSI jako kontextuální osobní údaje — 93
4.4.6 Zásada informovaného souhlasu v prostředí Internetu, zvláštní režim a zákonné licence — 95
4.4.7 Zpracování osobních údajů v prostředí Internetu se zřetelem k jejich zveřejňování — 102
4.4.8 Veřejné zasedání a zveřejňování souvisejících údajů na Internetu — 113
4.4.9 Sociální sítě – vybrané aspekty — 114
4.4.10 Veřejně přístupné internetové databáze a registry (obchodní rejstřík, katastr nemovitostí a registr doménových jmen WHOIS) — 120
4.4.11 Registry dlužníků — 122
4.4.12 Zvláštní režimy zpracování osobních údajů s využitím cloud computingu — 123
4.4.13 Internet a právo být zapomenut — 124
4.5 Regulace soukromí a důvěrnosti komunikací v oblasti elektronických komunikací — 128
4.5.1 Procesněprávní aspekty ochrany provozních a lokalizačních údajů (data retention) se zřetelem k historických ústavněprávním souvislostem — 129
4.5.2 Data retention v současném českém právu — 133
4.6 Občanskoprávní úprava — 135
4.6.1 Obecné aspekty právní úpravy osobnostních práv fyzické osoby — 135
4.6.2 Rozsah a obsah práva na ochranu osobnosti — 137
4.6.3 Život a zdraví — 139
4.6.4 Občanská čest a lidská důstojnost — 140
4.6.5 Další rozsah a obsah práva na ochranu osobnosti — 141
4.6.5.1 Jméno — 142
4.6.5.2 Projevy osobní povahy — 142
4.6.5.3 Jiné statky občanským zákoníkem výslovně nevyjmenované — 143
4.6.6 Prostředky ochrany proti neoprávněným zásahům do práva na ochranu osobnosti — 145
4.6.7 Aktivní legitimace k uplatňování ochrany proti neoprávněným zásahům do práva na ochranu osobnosti — 146
4.6.8 Zákonné omezení práv osobnostních — 147
4.7 Pracovněprávní úprava — 147
4.7.1 Právo zaměstnance na soukromý a rodinný život — 149
4.7.2 Národní úprava — 150
4.7.3 Meze výkonu práva kontroly — 152
Klíčová slova — 156

4. Právní regulace ochrany soukromí, její limity a možnosti

„Dnes si už nikdo nepamatuje dohody, kterými silnější strana zcela vylučovala svou odpovědnost. Tyto dohody byly tištěny malým písmem na zadních stranách lístků, objednávek, katalogů a faktur. Byly závazné pro každou osobu, která je akceptovala bez výhrady. Nikdo se proti tomu neohrazoval. Nikdo je nikdy nečetl, ani nevěděl, co v nich stojí. Bez ohledu na to, jak byla nepřiměřená, byla závazná. Toto vše se dělo ve jménu ‚smluvní volnosti'."[113]

Lord Denning

„Je třeba dávat přednost obecným zájmům před soukromými, trvalým před pomíjejícími."[114]

Plinius

4.1 Sedes materiae ochrany soukromí

Navzdory celkové orientaci této publikace se sluší také podívat na to, co stanoví česká právní úprava, zejména pak ta zákonná, jakož i související rámec práva EU (komunitárního práva), se kterým je vznik naší, zejména pak té veřejnoprávní, úpravy v mnoha ohledech nerozdílně spjat. Zajímá nás tedy obzvlášť právo komunitární (zejména příslušné směrnice a související rozhodovací praxe) mezinárodní a ústavní, dále pak právo národní – české, a to nejenom soukromé, ale i veřejné. Konkrétně proto připadají v úvahu zejména ObčZ (§ 11 a násl.) a zákoník práce na straně práva soukromého, dále pak trestní zákoník a ZoOÚ na straně práva veřejného.

Z pohledu práva ústavního lze samotné základy práva na soukromí nalézt v řadě mezinárodních dokumentů, a to zejména v Úmluvě, která ve svém článku 8 mimo jiné stanoví, že *„každý má právo na respektování svého soukromého života, obydlí a korespondence, přičemž státní orgán nemůže do výkonu tohoto práva zasahovat, kromě zákonem stanovených případů, a i to pouze v nezbytném rozsahu a okruhu případů"* (např. zájem národní či veřejné bezpečnosti apod.). Podle čl. 12 Všeobecné deklarace lidských práv[115] nesmí být nikdo vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence, ani útokům na svou čest a pověst. Každý má rovněž právo na zákonnou ochranu proti takovým zásahům nebo útokům.

Podobnou ochranu rovněž poskytuje i Listina, a to zejména v čl. 7, 10 a 13. Článek 7 stanoví obecné pravidlo, že *„nedotknutelnost osoby a jejího soukromí je zaručena, omezena může být jen v případech stanovených zákonem"*. O poznání komplexnější úpravu stanoví čl. 10, který praví, že: *„Každý občan má právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno."* Stejně tak se zde uvádí, že *„každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života a na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě"*. Listina dále v tomto ohledu rovněž ve

113 Rozhodnutí soudce Denninga ve věci *George Mitchell (Chesterhall) Ltd vs. Finney Lock Seeds Ltd* z roku 1982, které se týkalo otázek prodeje zboží a limitace odpovědnosti. Dostupné z: http://en.wikipedia.org/wiki/George_Mitchell_%28Chesterhall%29_Ltd_v_Finney_Lock_Seeds_Ltd

114 PLINIUS, ml. Antická knihovna sv. 58: Dopisy. Praha: Nakl. Svoboda, 1988.

115 Všeobecná deklarace lidských práv Valného shromáždění OSN ze dne 10. 12. 1948.

svém čl. 13 uvádí, *„že nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon*".

Z pohledu další aplikace těchto ústavních základů musí být součástí všech těchto úvah pohled komparativní, kritický a v neposlední řadě také analytický.

Komparativní pohled je významný hned z několika důvodů, jednak proto, že řešeny jsou zde otázky zcela nové, přičemž není důvod předpokládat, že evropský koncept této ochrany, případně odvozený koncept český, je zcela ideální. Dále pak proto, že ve světě existuje celá řada mnohdy velmi odlišných a fungujících přístupů k ochraně soukromí. Typické srovnání se nabízí se zeměmi v systému *common law*, zejména pak se Spojenými státy americkými, kde regulační systém ochrany soukromí prakticky neexistuje, neexistuje zde ani systém veřejnoprávních prostředků ochrany osobních údajů obdobný tomu, jenž je postaven na komunitárněprávním základě.[116]

V tomto ohledu se zdá být zajímavé srovnání samotné EU, která má velmi rozsáhlou právní regulaci a zřetelně nejrozsáhlejší právní prostředky ochrany soukromí na světě, se Spojenými státy, kde tento systém ochrany soukromí jednotlivce neexistuje. Ve Spojených státech není ochrana soukromí přímo zakotvena ani v ústavě či jejich dodatcích, nepřímo však vyplývá, resp. přesněji je precedentně dovozována z ochrany před nepřiměřenou prohlídkou a konfiskací (*unreasonable searches and seizures*) ve smyslu čtvrtého dodatku[117] Ústavy Spojených států. Tato ochrana je však pojata formou zakotvení ochrany před zásahy ze strany státu,[118] kde takto zakotvené právo na ochranu soukromí může být uplatňováno toliko proti jednotlivým státům (ve smyslu čtrnáctého dodatku Ústavy, který upravuje řádný proces).[119] Klíčovým pojmem této úpravy je pojem přiměřeného očekávání ochrany soukromí k prohledávané (či prohledané) věci nebo místu.[120] Aby očekávání bylo shledáno za dostatečně přiměřené, musí být přiměřené subjektivně i objektivně. Jde tak o test přiměřenosti *sui generis* (podobně orientovaný jako níže zmíněný test proporcionality), který fungoval v kontextu původních podmínek,[121] nicméně aplikace tohoto testu pro potřeby ochrany soukromí v digitálním kontextu vyvolává některé nové otázky. S nástupem informační společnosti totiž musí nutně docházet k stále většímu vyvažování soukromých zájmů proti zájmům státu. Vzhledem k existujícím technologiím, smluvním podmínkám dominantních poskytovatelů služeb Internetu, se totiž stále více zmenšuje prostor, kde lze prokazatelně koncept přiměřeného očekávání ochrany soukromí reálně aplikovat,[122]

116 Viz LIPTON, J. Mapping Online Privacy. *Nw. U. L. REV.* 2010, vol. 104, s. 477, 484.

117 Ke čtvrtému dodatku Ústavy spojených států viz http://en.wikipedia.org/wiki/Fourth_Amendment_to_the_ United_States_Constitution#Computers_and_privacy

118 Ústava USA, 4. dodatek IV; viz *Katz proti Spojeným státům americkým.* 389 U.S. 347, s. 350–51 (1967); viz také *Berger proti New Yorku.* 388 U.S. 41, 53 (1967).

119 *Mapp proti státu Ohio,* 367 U.S. 643, 655 (1961).

120 *Katz.* 389 U.S. na s. 360 (Harlan, J., souhlasné stanovisko).

121 Například Katz vznesl otázku, zda odposlouchávací zařízení na vnější straně telefonní budky porušuje právo na soukromí obžalovaného pachatele trestného činu. *Katz.* 389 U.S. na s. 348.

122 SMITH, J. Threatsense Technology: Sniffing Technology and the Threat to Tour Fourth Amendment Rights. *TEX. Tech L. REV.* 2011, vol. 43, s. 615, 628.

tj. zejména se ho dovolat. Posuzování přiměřenosti takového očekávání je totiž touto doktrínou posuzováno mimo jiné tak, že je rozebírána povaha samotné technologie, smluvních podmínek jejich použití, jakož i skutečnost, že jde o služby, které jsou více či méně poskytovány v prostředí veřejné sítě. Tato doktrína tak ve Spojených státech způsobuje, že soudy dokážou jen s velkými obtížemi vymezit hranice soukromí při provádění prosazování práva.[123]

V České republice se Internet stal rovněž neodmyslitelnou součástí společnosti, a tak vyvstávají otázky spojené s ochranou práv jeho uživatelů, zejména práv spojených s ochranou osobnosti a soukromí. Je nepochybné, že osobní údaje a jiné informace publikované v prostředí Internetu (bez ohledu na jejich pravdivost) mají obrovský potenciál zasáhnout dotčenou osobu v mnoha sférách jejího života, tedy jak v rodinném, tak i v pracovním či veřejném životě. Je proto na místě klást si otázku, zda a jakými prostředky lze ochranu soukromí v prostředí Internetu chránit. Ochrana osobnosti a soukromí je v České republice ústavně zakotvenou hodnotou (viz čl. 10 Listiny). Historicky spadá především do soukromoprávní kategorie práv, tedy do oblasti, kde jsou práva osob chráněna soudy v občanském soudním řízení v návaznosti na konkrétní žalobu. Nicméně pro určité oblasti, v nichž by zásah do práv představoval zvýšené riziko pro celospolečenské hodnoty, zákonodárce (obvykle pod vlivem společenského vývoje a mezinárodních dokumentů) rozhodl, že je důvodné poskytovat ochranu veřejnoprávní cestou, tj. formou státního zásahu. Zákonné provedení zmíněného čl. 10 Listiny tak lze nalézt jak v občanském zákoníku (ochrana osobnosti podle § 11 až 16), tak v trestním zákoníku (trestný čin neoprávněného nakládání s osobními údaji podle § 180) a v neposlední řadě i v ZoOÚ. Otázka zveřejňování osobních údajů na Internetu může v některých případech podléhat i dalším právním předpisům, např. zákonu o regulaci reklamy, zákonu o provozování rozhlasového a televizního vysílání nebo zákonu o některých službách informační společnosti. Žádný z uvedených právních předpisů a priori nevylučuje ze své působnosti oblast Internetu – je tedy nutné vycházet z toho, že i přes svobodu a volnost, které jsou základními atributy tohoto média, není ani zde právní vakuum umožňující zcela libovolné jednání.[124]

4.2 Evropský systém ochrany soukromí

Informační stopa člověka se během dvou posledních desetiletí rozrostla v míře dosud v historii naší společnosti nevídané. Lidstvo o sobě generuje neuvěřitelné množství dat, mnohdy navíc zcela bez jakékoliv přímé aktivity dotčených osob. Jedinec je často automaticky omezen v možnosti ovlivňovat okruh informací, které jsou o něm zpracovávány, mnohdy ani nemá šanci zjistit jejich rozsah či strukturu, ztrácí reálnou možnost ovlivnit další nakládání s těmito údaji, jakož i rozhodovat o jejich dalším osudu. Na tento stav reagovala relativně dynamicky a nekompromisně Evropská unie vytvořením veřejnoprávního institutu ochrany osobních údajů. Tento institut byl koncipován v polovině devadesátých let na základě Směrnice. Tato Směrnice

123 CROWTHE, B., ref. 40, s. 343.

124 Viz např. Stanovisko Úřadu č. 13/2012 z března 2012 (původně K problémům z praxe č. 4/2010) zabývající se zveřejňováním osobních údajů na Internetu.

stanovila členským státům EU lhůtu pro její provedení do 24. října 1998, přičemž do současné doby představuje základní referenční normu v oblasti ochrany osobních údajů. Směrnice tak zavedla základní právní rámec, jehož cílem bylo ustavení rovnováhy mezi vysokou úrovní ochrany soukromí jednotlivců a volným pohybem osobních údajů v rámci EU. Za tímto účelem stanovila tato Směrnice velmi přísná pravidla a omezení pro shromažďování a využívání osobních údajů a zároveň stanovila povinnost všem členským státům vytvořit nezávislý vnitrostátní orgán pověřený ochranou těchto údajů. Toto pojetí (evropské) ochrany pramení do značné míry z průkopnického rozsudku[125] vydaného v roce 1983 německým Federálním ústavním soudem, který uznal základní lidské právo na „informační sebeurčení". Zákon na ochranu osobních údajů byl začleněn do práva všech dvaceti sedmi členských států EU, jakož i některých nečlenských zemí EU (jako je Island, Lichtenštejnsko a Norsko) a měl výrazný vliv na formování zákonů na ochranu osobních údajů v právních systémech, jako je Argentina, Kanada, dubajská zóna volného obchodu Dubai International Financial Centre (DIFC), Hongkong nebo Rusko.[126]

Význam Směrnice však spočívá především v jejím konečném dopadu ve formě veřejnoprávního zásahu do dosud typicky soukromoprávních vztahů, a to zejména s ohledem na svou osobní i věcnou působnost. Směrnice dopadá na všechny údaje zpracovávané automaticky (např. databáze zákazníků), jakož i na údaje, které jsou obsaženy v neautomatizovaném rejstříku nebo do něj mají být zařazeny (tradiční lístkové rejstříky či kartotéky), a je lhostejné, jakým způsobem či v jaké formě je samotné zpracovávání prováděno. Z věcné působnosti této Směrnice je vyjmuto pouze zpracování prováděné fyzickou osobou pro výkon výlučně osobních či domácích činností a zpracování prováděné pro výkon činností, které nespadají do oblasti působnosti práva Unie (např. veřejná bezpečnost, obrana či bezpečnost státu). Samotným cílem Směrnice je přirozeně ochrana práv a svobod osob v souvislosti se zpracováním osobních údajů, přičemž za účelem naplnění tohoto cíle stanoví Směrnice některé hlavní zásady[127] zpracování těchto údajů, a to zejména:

- **zásada kvality údajů** (osobní údaje musí být zejména zpracovány korektně a zákonným způsobem a shromažďovány pro stanovené účely, výslovně deklarované a legitimní, dále musejí být přesné, a je-li to nezbytné, i aktualizované),
- **zásada legitimity zpracování údajů** (zpracování osobních údajů může být provedeno pouze, pokud subjekt údajů nezpochybnitelně udělil souhlas nebo je zpracování nezbytné),[128]
- **zásada proporcionality a finality zpracování údajů** (zpracování osobních údajů může být realizováno pouze za účelem dosažení stanoveného účelu a jen v míře nezbytné k jeho dosažení),

125 Bundesverfassungsgericht, Judgment of 15 December 1983, 65 BVerfGE 1.

126 K tomu více viz KUNER, Ch. *The 'Internal Morality' of European Data Protection Law.* November 24, 2008. Dostupné z: http://ssrn.com/abstract=1443797 nebo http://dx.doi.org/10.2139/ssrn.1443797

127 Viz http://europa.eu/legislation_summaries/information_society/data_protection/l14012_cs.htm

128 Směrnice taxativně stanoví několik důvodů takové nezbytnosti, např. pro splnění smlouvy, kde je subjekt údajů jednou ze stran; nebo pro splnění právní povinnosti, které podléhá správce; nebo pro zachování životně důležitých zájmů subjektu údajů; nebo pro vykonání úkolu ve veřejném zájmu; nebo pro uskutečnění oprávněných zájmů správce.

- **zásada informování osob,** kterých se týká zpracování údajů (správce musí poskytnout osobě, od které získává údaje, které se jí týkají, některé informace [totožnost správce, účely zpracování, příjemce údajů atd.]),
- **zásada oznamovací** (správce musí zaslat oznámení vnitrostátnímu orgánu dozoru, a to před zahájením zpracování, orgány dozoru po obdržení oznámení provedou předběžná šetření o případných rizicích z hlediska práv a svobod subjektů údajů, musí být zajištěno zveřejnění zpracování a orgány dozoru musí vést rejstřík oznámených zpracování.)
- **zásada zákazu zpracování některých kategorií údajů** (je zakázáno zpracování osobních údajů, které odhalují rasový či etnický původ, názory na veřejné otázky, náboženské nebo filozofické přesvědčení, odborovou příslušnost, jakož i zpracování údajů týkajících se zdraví a sexuálního života; toto ustanovení platí s výhradou případů, kdy je zpracování nezbytné např. k obraně životně důležitých zájmů subjektu údajů nebo pro účely zdravotní prevence či lékařských diagnóz.)
- **zásada důvěrnosti a bezpečnosti zpracování** (jakákoli osoba, která jedná z pověření správce nebo zpracovatele, jakož i samotný zpracovatel, který má přístup k osobním údajům, je může zpracovávat pouze podle pokynů správce. Správce musí mimo to přijmout vhodná opatření na ochranu osobních údajů proti náhodnému nebo nedovolenému zničení, náhodné ztrátě, úpravám a neoprávněnému sdělování nebo přístupu).[129]

Směrnice dále za účelem naplnění těchto zásad zakládá široké portfolio práv dotčené osoby, které se uplatní na dotčené zpracování, přičemž v případě porušení těchto práv musí mít každá dotčená osoba garantované právo předložit věc soudu. Kdokoli, kdo byl poškozen neoprávněným zpracováním svých osobních údajů, může se, kromě souvisejících nároků na náhradu způsobené škody domáhat také práva přístupu k údajům[130] a práva výhrady proti zpracování údajů,[131] jakož i řady dílčích práv. K předávání osobních údajů z členského státu do třetí země může dojít tehdy, pokud dotyčná třetí země zajistí odpovídající úroveň ochrany. Naopak k předávání osobních údajů z členského státu do třetí země, která takový stupeň ochrany nemá, s limitativně vyjmenovanými výjimkami, dojít nesmí. Jakýmsi vedlejším cílem Směrnice je též podpora vypracování vnitrostátních kodexů chování a kodexů chování platných na úrovni Unie, které mají přispět k řádnému uplatňování vnitrostátních právních předpisů a právních předpisů Unie. Směrnice proto stanovila povinnost zřídit pracovní skupinu pro ochranu fyzických osob

129 Je nutné zmínit, že předmětná Směrnice také obsahuje celou řadu výjimek a omezení, a to zejména co do rozsahu povinností a práv týkajících se kvality údajů, informování subjektu údajů, práva na přístup k údajům, bezpečnost státu, obranu, veřejnou bezpečnost, stíhání trestných činů, významný hospodářský nebo finanční zájem členského státu nebo EU.

130 Každý subjekt údajů musí mít právo získat od správce (1) potvrzení, že údaje, které se ho týkají, jsou, či nejsou zpracovávány, a sdělení o údajích, které jsou předmětem zpracování, a (2) opravu, výmaz nebo blokování údajů, jejichž zpracování není v souladu s touto směrnicí – zejména z důvodů neúplné nebo nepřesné povahy údajů –, a oznámení třetí osobě, které údaje byly sděleny.

131 Subjekt údajů musí mít právo vznést z legitimních důvodů námitku proti zpracování osobních údajů, které se ho týkají. Musí mít také možnost podat návrh a bezplatně vznést výhradu proti zpracování osobních údajů připravovanému pro účely přímého marketingu a konečně musí být informován dříve, než jsou osobní údaje sděleny třetí osobě pro účely přímého marketingu, a musí mu být výslovně poskytnuta možnost námitky proti tomuto sdělení.

v souvislosti se zpracováním osobních údajů (dále jen Pracovní skupina 29), která je složena ze zástupců vnitrostátních orgánů dozoru, zástupců orgánů dozoru, vytvořených pro orgány a instituce Společenství, a ze zástupce Komise.

Evropská unie tak na výše zmíněný dramatický nárůst informační stopy člověka a možnosti jejího zneužití reagovala vytvořením velmi specifického systému práv, povinností a systematizovaných postupů, na jejichž dodržování dohlíží specifický dozorový orgán (případně více orgánů s rozloženou působností). Jde tak o poměrně unikátní způsob realizace ochrany jinak výhradně subjektivních práv ve veřejném zájmu, jehož rozsah i dopad na právní vztahy v celé EU je nevídaný. Není sporu o tom, zda měla Evropská unie na výše popsaný stav reagovat, je však zcela legitimní otázkou, zda monumentalita tohoto způsobu řešení obstojí a obhájí svou budoucnost v širší perspektivě. Kritické ohlasy na tento specifický systém však zaznívají spíše výjimečně. Jedním z takových kritiků je Ch. Kuner,[132] který se v jedné ze svých starších studií zabývá hlediskem vnitřní morálky tohoto systému, kde vychází z argumentů právní filozofie, konkrétně pak aplikačně navazuje na starší diskusi mezi H. L. A. Hartem a L. Fullerem o přednostech právního pozitivismu (jehož zastáncem byl Hart) oproti přednostem teorie přirozeného práva (kterou naopak prosazoval Fuller).[133] Předmětná diskuse pojmenovala základní otázky o povaze práva a zásadních vlastnostech jeho efektivity, včetně otázek vymáhání. Obecně vzato lze říci, že Fuller s Hartem zde diskutovali netriviální otázku obecné podoby práva, aby fungovalo tak, jak má. Podobné otázky si na konkrétním příkladu systému ochrany osobních údajů v Unii pokládá i Kuner, když uvádí, že evropský systém ochrany osobních údajů je příliš obsáhlý, složitý, byrokratický i administrativně náročný a nepříliš jasný co do jeho cílů, navíc v mnoha směrech zastaralý ve srovnání s moderními trendy regulatorní praxe.

Kuner úvodem argumentuje[134] tím, že ochrana dat představuje téma zcela zásadního vědeckého i společenského významu, a to jak pro vlády, tak i soukromý sektor. Nicméně navzdory této důležitosti panuje rozsáhlé ticho o celkové koherenci a účinnosti tohoto systému ve smyslu argumentů právní vědy. Evropský systém ochrany osobních údajů si vydobyl natolik vysokou míru důležitosti, že si zaslouží, aby se s ním nakládalo s úctou přiznávanou jiným oblastem práva, což znamená posuzovat jej ve světle těchto kritérií. Takové posouzení je pro tento systém významné především proto, že samotný systém počítá, že bude dále přehodnocován, a proto je nutné zjistit zejména jeho klady i zápory a vyznačit problematická místa, nad nimiž by se měli zákonodárci ještě zamyslet. Úvodní Kunerova kritika směřuje zejména k nepřehlednosti jednotlivých zdrojů tohoto systému (ve smyslu pramenů práva) a dále pak ke způsobu vymáhání souvisejících předpisů. Kuner tvrdí, že systém evropské ochrany se skládá z mnoha různých zdrojů, které bývají v praxi používány, k nimž patří zejména:

132 KUNER, Ch., ref. 126.

133 HART, H. L. A. Positivism and the Separation of Law and Morals, *Harvard Law Review.* 1958, vol. 71, s. 593 a FULLER, Lon L. Positivism and Fidelity to Law — A Reply to Professor Hart. *Harvard Law Review.* 1958, vol. 71, s. 630. Citace z díla KUNER, Ch. *European Data Protection Law: Corporate Compliance and Regulation.* 2nd edition. Oxford University Press, 2007.

134 K tomu více KUNER, Ch. *European Data Protection Law: Corporate Compliance and Regulation*. 2nd edition. Oxford University Press, 2007.

- Směrnice a Směrnice č. 58, národní zákony na ochranu osobních údajů,
- stanoviska úřadů pro ochranu osobních údajů členských států,
- Pracovní skupina 29,
- technické normy přijaté normalizačními úřady a odvětvovými sdruženími,
- články a komentáře předních odborníků a další zdroje.

Tyto prameny evropského práva ochrany osobních údajů mají diametrálně odlišnou povahu, a to zejména co do své závaznosti a vynutitelnosti (národní právní předpisy a evropské směrnice mají vysokou míru závaznosti, byť směrnice zavazují jen členské státy, na rozdíl od národních předpisů, které zavazují jednotlivce). Technické normy vyhlášené normalizačními úřady mohou být závazné v určitém prostředí (například pokud je na ně uveden odkaz ve směrnici nebo v zákoně anebo v rámci členství v určité skupině nebo sdružení). Články a komentáře předních odborníků nejsou sice závazným pramenem práva, nicméně mnohdy působí silou své argumentace, přičemž nezřídka z nich soudy a regulatorní orgány vycházejí. Další rozdíl se týká způsobu, kterým jsou tyto zdroje navrhovány nebo schvalovány. Směrnice a zákony se přijímají v rámci zákonodárného procesu, stanoviska příslušných úřadů vypracovávají zaměstnanci těchto úřadů, technické normy schvalují příslušné úřady atd. Kuner považuje tuto rozmanitost zdrojů evropských právních norem na ochranu osobních údajů za neslučitelnou s výše uvedenou Fullerovou definicí práva, jež vyjadřuje *„ochotu lidí podřídit své jednání normativnímu režimu*“,[135] a naopak uvádí slavnou větu L. Lessiga vyjadřující, že *„kód je právo*“, tedy že *„software a hardware, které společně vytváří kyberprostor tím, čím je, regulují kyberprostor takový, jaký je*“.[136] Kuner v tomto ohledu dále dovozuje, že mezi právní silou výše uvedených zdrojů evropského systému ochrany osobních údajů a jejich skutečným aplikačním významem neexistuje v praxi příliš velká spojitost. Některým akademickým komentářům, které nejsou právně závazné, tedy může být v určitých právních systémech přikládána velká váha. Totéž platí i v případě stanovisek úřadů na ochranu osobních údajů nebo Pracovní skupiny 29, které sice po formální stránce právně závazné nejsou, ale soudy je mohou citovat jako precedent, na který je třeba brát zřetel. Samostatnou kapitolou jsou pak technické normy, které rovněž nejsou obecně závazné, nicméně z jejich porušení mohou vyplývat relativně závazné sankce, byť mnohdy i nepřímo. Mnoho takových norem se týká zabezpečení údajů, což je obvyklý klíčový prvek národních zákonů o ochranu osobních údajů, včetně toho českého. Příkladem je norma Payment Card Industry Data Security Standard (v2.0),[137] která byla přijata sdružením provozovatelů systémů platebních karet v roce 2006 a aktualizována v roce 2010. Jelikož nedodržení této normy může v konečném důsledku vést k zákazu zpracovávat platby platební kartou, je porušení této technické normy nutné považovat za mnohdy významnější, než je tomu v případě porušení národních předpisů. Kuner tak z různorodé povahy zdrojů evropského systému ochrany osobních údajů a chybějícího vztahu mezi jejich formální právní silou a účinností usuzuje, že jak správci, kteří chtějí právo

135 KUNER, Ch., ref. 133.

136 K tomu více viz LESSIG, Lawrence. *Code and other laws of cyberspace.* Basic Books, 1999, s. 6.

137 Dostupné [online] z: www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

dodržovat, tak i subjekty údajů, které chtějí zjistit, jaká mají práva, čelí obtížnému úkolu hledat v rozsáhlém archivu různých zdrojů a snažit se najít, který z nich je vlastně pro ně směrodatný.[138]

Další důležitý problém se týká úrovně dodržování evropského systému ochrany osobních údajů a způsobu, jakým je vymáhán.[139] V tomto může být zajímavé si připomenout jednu z prvních zpráv Evropské komise z roku 2003 o provádění směrnice o ochraně osobních údajů (95/46/ES),[140] která v tomto ohledu uvádí, že neoficiální důkazy, kombinované s různými prvky „tvrdých" faktů, které má Komise k dispozici, však naznačují existenci tří vzájemně propojených fenoménů – (1) úsilí vynaloženému při vymáhání práva, které vychází z nedostatečných zdrojů, a dozorovým orgánům s širokým spektrem úkolů, k nimž patří i vymáhání, se přikládá nízká priorita, (2) velice nejednotné dodržování související zákonné úpravy ze strany správců údajů, kteří evidentně nejsou nijak zvlášť ochotni měnit své zavedené postupy, aby začali dodržovat něco, co vypadá příliš složitě a náročně, když riziko, že je při tom někdo chytí, je poměrně nízké, (3) zjevně nízká úroveň povědomí o právech mezi subjekty údajů, která právě může být příčinou předchozího fenoménu. Kunerova kritika dále pokračuje na příkladech těch ustanovení, která ačkoliv jsou nezpochybnitelně závazná, bývají v praxi obvykle porušována a příslušné úřady pak dodržování těchto ustanovení nevymáhají. Kuner tento závěr opírá o článek 4 odst. 2 Směrnice, který stanoví, že v případě uvedeném v odst. 1 písm. c) článku 4 musí správce usazený mimo EU určit zástupce usazeného na území zmíněného členského státu. Tito zástupci ale ve skutečnosti určováni nejsou a příslušné úřady dodržování tohoto ustanovení obvykle ani nevymáhají.

Míra efektivity a vynucování dodržování evropského systému ochrany osobních údajů se zdá být v poměru k objemu osobních údajů, které se v současné době zpracovávají, skutečně relativně nízká. Pro takto rozšířené nedodržování právních norem však existuje celá řada vysvětlení, z nichž to nejjednodušší se týká dvou zásadních změn způsobu, jakým se data zpracovávají. Jde především o to, že zpracování údajů nyní probíhá po síti a globálně, což je fenomén, který se projevuje od doby, kdy se na konci 90. let minulého století masově rozšířilo používání Internetu a elektronického obchodování. Zpracování údajů po síti znamená, že se údaje stále více zpracovávají přes počítačové sítě, takže zpracovatelské úlohy se obvykle rozdělí mezi velký počet počítačů, které se mohou klidně nacházet v různých zemích a oblastech. Možnost rozdělování úloh při zpracování údajů nesmírně komplikuje schopnost správců zjistit, jaké jsou jejich povinnosti při dodržování souvisejících národních zákonů, jelikož rozdělením se násobí počet norem, které se mohou na jednotlivé zpracovatelské operace vztahovat, a taková situace může být aplikačně velmi problematická i pro samotné úřady, které vykonávají dohled. Je nutné podotknout, že výrazně roste také počet subjektů, které údaje zpracovávají, což statisticky značně snižuje reálnou možnost kontroly. Totéž platí i o expanzi Internetu, díky němuž se ze zpracování dat stává stále více mezinárodní aktivita, kdy se údaje často zadávají nebo zpracovávají bez ohledu na státní hranice. Stále rozšířenější globální zpracování dat komplikuje jak dodržování,

138 KUNER, Ch., ref. 126.

139 Hart (viz výše) se domnívá, že značně rozšířené nedodržování tohoto zákona a obecně nedostatečná úroveň jeho vymáhání by mohly zpochybnit status normativního systému jako „práva", a tento názor sdílí i H. Kelsen.

140 KUNER, Ch., ref. 126.

tak i vymáhání právních norem, jelikož správci musejí stále obtížněji zjišťovat, které právo se na jejich zpracovatelské operace zrovna vztahuje, a to vede k tomu, že se mnoho zpracovatelských úloh odehrává mimo sféru pravomoci dohledových úřadů. Úřady se tak soustředí na namátkové kontroly, případně kontroly na základě podnětu, což je patrně jediná efektivní možnost, jelikož medializované opatření přijaté proti důležitému správci údajů obvykle motivuje ostatní k tomu, aby začali více dodržovat zákony (národní úpravy). Namátkově prováděné akce je však třeba vždy pečlivě nastavit a zvážit, aby se uplatňovaly důsledně a spravedlivě a tak, aby někteří správci nezačali mít pocit, že si je někdo nespravedlivě vybírá jako terč.[141]

Navzdory rostoucímu počtu donucovacích opatření je šance, že bude uplatněno opatření za konkrétní porušení příslušného zákona na ochranu osobních údajů, ve většině případů stále poměrně nízká. Nedostatečně rozšířené a nedůsledné vymáhání práva v případech porušování zákona na ochranu osobních údajů se negativně projevuje na ochotě správců dodržovat v této oblasti národní a evropské předpisy. Mezi složitostí norem, které upravují zpracování údajů, a poměrně nízkým rizikem uplatnění donucovacího opatření zeje široká propast. Výsledkem toho je, že správci často přikládají větší význam oblastem práva, kde jsou sankce přísnější (jako jsou daně, praní špinavých peněz, zákony o cenných papírech atd.) než ochraně osobních údajů.[142] Kromě „ze zákona vycházejících" donucovacích metod, jako jsou pokuty a předběžná opatření, jsou důležitým motivem k dodržování práva na ochranu osobních údajů i tzv. „měkké" sankce, jako je například negativní publicita, jelikož újma na dobré pověsti může firmě v konečném důsledku přivodit daleko větší škodu na trhu než pokuta samotná. Zákazníci navíc stále více očekávají od svých dodavatelů i poskytovatelů elektronických služeb dobrou úroveň ochrany údajů a i tento tlak může být efektivnějším způsobem motivování správců k dodržování zákona než tradiční, zákonem stanovené donucovací metody.[143]

Kritiku systému evropské ochrany osobních údajů završuje Kuner tím, že apeluje na Fullerův koncept vnitřní morálky práva, který vychází z osmi klíčových selhání práva.[144] Fullerova „vnitřní morálka" nemá nic společného s náboženstvím, ale spíše s logickou a vnitřní sou-

141 KUNER, Christopher. *The 'Internal Morality' of European Data Protection Law.* (November 24, 2008). Dostupné z: http://ssrn.com/abstract=1443797

142 V globální ekonomice platí pro všechny faktory, které mají vliv na náklady (včetně zátěže spojené s dodržováním právních předpisů), postupy uplatňované v rámci řízení rizik, přičemž dodržování zákona je pravděpodobnější tehdy, když jsou rizika a náklady spojené s jeho nedodržováním vyšší než v případě opačném. V mnoha případech mohou tedy správci pohlížet na právní normy na ochranu osobních údajů spíše jako na jistou formu byrokratického obtěžování než jako na „právo", které patří do téže kategorie jako daně a ostatní právní oblasti, a to zejména díky relativně nedostatečné míře vymáhání a mírnosti případných pokut.

143 KUNER, Ch., ref. 141.

144 První a nejvíce očividná chyba spočívá v neschopnosti dospět k pravidlům, takže se o každém problému musí rozhodovat ad hoc. Další chyby jsou tyto: (2) neschopnost zveřejnit nebo vůbec zpřístupnit dotyčným subjektům pravidla, která mají dodržovat; (3) zneužití retroaktivního zákonodárství, které nejen nemůže být vodítkem jednání, nýbrž podkopává i integritu pravidel působících do budoucna, protože se vystavují hrozbě, že bude retroaktivně změněna; (4) neschopnost vytvořit srozumitelná pravidla; (5) schvalování pravidel, která si odporují, nebo (6) pravidel vyžadujících chování, jehož ten, na koho se vztahují, není schopen; (7) tak časté změny pravidel, že se podle nich nelze orientovat; a nakonec (8) neshoda mezi vyhlášenými pravidly a jejich uplatňováním v praxi. K tomu více viz FULLER, Lon L. *The Morality of Law,* s. 39.

držností. Fuller to popisuje jako „přirozená pravidla tesařské práce nebo přinejmenším jako pravidla, kterými se tesař řídí, chce-li, aby dům, jenž staví, zůstal stát a sloužil těm, kteří v něm žijí".[145] V tomto ohledu pak Kuner rozvádí pět základních problémů evropského systému ochrany osobních údajů:

1. Chybějící pravidla, která by upravovala běžné situace. Evropská legislativa na ochranu osobních údajů nestanoví pravidla pro některé situace, k nimž při zpracování údajů v praxi běžně dochází. Například články 25 a 26 Směrnice neobsahují žádná ustanovení o několikanásobných předáváních údajů, která jsou dnes velice běžná. Přitom údaje se často převádějí od správce v EU zpracovateli mimo EU a potom je zpracovatel posílá ještě dalšímu zpracovateli. Tato situace vzniká například tehdy, když správce v EU zašle osobní údaje zpracovateli údajů mimo EU, který si najme dalšího zpracovatele v jiné zemi, aby provedl rutinní údržbu IT pomocí svých databází. Jelikož původní předání údajů firmě na zpracování údajů se považuje za mezinárodní předání údajů a umožnění přístupu firmě zabývající se údržbou IT do serverů externí firmy se považuje za „další předání" údajů, jedná se o počáteční mezinárodní předání údajů zpracovateli, po němž následuje další předání údajů jedním zpracovatelem dalšímu. Nicméně právo většiny členských států EU evidentně s předáváním údajů mezi zpracovateli nepočítá, takže zpracování údajů visí v právním vzduchoprázdnu a dotyčné strany převodu dat ani nevědí, co mají dělat, aby dodržovaly zákony.
2. Nedostatečná publicita a sdělnost pravidel. Jak prokázaly studie uveřejněné v roce 2004 Evropskou komisí, panuje mezi evropskými správci a občany o zákonu na ochranu osobních údajů velice nízké povědomí. Tento nedostatek povědomí je patrně do značné míry způsoben tím, že členské státy EU nepřikládají ochraně údajů příliš velký význam, a tak ho ani veřejnosti nijak zvlášť nepředstavily, což se projevuje například tím, že v mnoha případech není úřadům na ochranu osobních údajů přiznána odpovídající nezávislost ani finanční zdroje na provozní činnost. Správci mají například celkem zmatečné představy o problematice, jako jsou právní požadavky členských států na používání vzorových smluvních ustanovení schválených EU o předávání údajů a formality, které jsou v členských státech nezbytné při schvalování závazných korporátních norem. A přitom by stačilo pár jednoduchých opatření, například kdyby Pracovní skupina 29 vydala několik přehledů a tabulek, v nichž by byly požadavky a formality jednotlivých členských států na ochranu údajů vypsány.
3. Nejasná pravidla. Evropský systém ochrany osobních údajů je koncipován normativně natolik nedůsledně, že zakládá obzvláště vysokou míru zmatečnosti a komplikovanosti, což se projevuje zejména v následujících oblastech:
    - Vzhledem k pochopitelné absenci použitelné judikatury dochází k příliš velkému spoléhání se na nezávazné právní zdroje. V oblasti ochrany údajů existuje citelný nedostatek právně závazných rozhodnutí soudů a regulatorních orgánů,[146] a tudíž je příliš

145 FULLER, Lon L., s. 96.

146 Viz BYGRAVE, L. Where have all the judges gone? Reflections on judicial involvement in developing data protection law. *Privacy Law & Policy Reporter.* 2000. 7, s. 11.

často nutné spoléhat se na nezávazné zdroje, jako jsou neformální stanoviska úřadů na ochranu osobních údajů a články či komentáře akademiků. Tyto zdroje mohou být jistě velmi cenné, nemají ale právní moc závazných zdrojů a mohou být ve vzájemném rozporu, což jen vede k dalším zmatkům.

- Spoléhání se na obecné právní zásady, které nejsou výslovně zakotvené v příslušných právních předpisech. Zákon na ochranu osobních údajů staví velice silně na obecných právních zásadách, které často nejsou v příslušných právních předpisech výslovně zakotveny, a tudíž nemusí být snadno rozpoznatelné. Příkladem je zásada proporcionality, která je v textu Směrnice zmiňována pouze na několika místech, a tudíž může budit mylné zdání, že jí není přikládán velký význam. Ve skutečnosti ale ESLP zásadu proporcionality běžně uplatňuje jako kritérium při rozhodování, zda zpracování údajů proběhlo v souladu se zákonem, a tuto zásadu ve vztahu ke zpracování údajů uplatňuje i ESD. Jelikož ale zásada proporcionality není ve většině právních předpisů na ochranu osobních údajů výslovně uvedena a mnoho správců je navyklých chápat dodržování zákonů na ochranu osobních údajů jako plnění dobře vymezeného souboru zákonem stanovených požadavků, může se stát, že budou při výkladu této zásady tápat.

4. Vzájemně si odporující zásady. Mezi soudy a příslušnými úřady pro ochranu osobních údajů nezřídka dochází k neshodám ohledně některých nejdůležitějších konceptů evropského zákona na ochranu osobních údajů, a to leckdy dokonce i v téže zemi. Pro dotyčné subjekty je velice obtížné určit svá práva a povinnosti, když se musí ve své zemi potýkat se spory mezi soudy a regulatorními orgány ohledně vymezení jednoho z nejzákladnějších právních konceptů.[147]
5. Neshoda mezi pravidly a jejich uplatňováním v praxi. Tato zásada odkazuje na existující propast mezi pravidly a způsobem, jakým se ve skutečnosti uplatňují v praxi. Jak již bylo naznačeno výše, míra dodržování a vymáhání zákonů na ochranu osobních údajů není příliš vysoká, což svědčí o tom, že mezi uveřejněnými normativními pravidly a způsobem, jakým se uplatňují, existuje propast. Navíc v působnosti Směrnice existují velké výjimky, a to zejména pokud jde o zpracování údajů v záležitostech národní obrany, bezpečnosti a v trestních věcech. Ačkoli má toto odlišné zacházení určitě své zákonné důvody, z pohledu běžného občana je těžké pochopit, proč by právní normy na ochranu osobních údajů neměly platit i na zpracování dat donucovacími orgány, když tato činnost může představovat přinejmenším stejně vysoké riziko jako zpracování údajů v soukromém sektoru. Výjimky z působnosti zákona rovněž podkopává respekt k evropskému rámci na ochranu osobních údajů mezi běžnými občany a správci údajů.[148]

Navzdory svému kritickému pohledu na dosavadní úpravu evropského systému ochrany dovozuje dále Kuner, že příslušná Směrnice položila široké základní schéma zásad zpracování osobních údajů a měla velký vliv na zákony v ostatních zeměpisných oblastech. Tento systém tak dosáhl celé řady úspěchů. Navzdory těmto kladům však stále přetrvávají jeho problémy, a to

147 Obdobně je v těchto věcech přistupováno i v ČR. K právní povaze IP adresy, MAC adresy a ID datové schránky v českém právu viz následující kapitolu 4.4 této publikace.

148 KUNER, Ch., ref. 141 nebo http://dx.doi.org/10.2139/ssrn.1443797

jak v oblasti hmotněprávní a programové (politics), tak i celkového povědomí ve smyslu dostatečné sdělnosti celého tohoto systému.

Podstata hmotněprávních problémů ochrany osobních údajů by měla být revidována v několika oblastech. Příkladem je požadavek odst. 1 článku 25 Směrnice stanovující, že osobní údaje mohou být předávány do třetích zemí, které zajistí „dostatečnou úroveň ochrany". Účel této povinnosti – především zajistit, aby osobní údaje nebyly zbavovány veškeré ochrany, když se převádějí mimo EU – je patřičný a pochopitelný. Je však otázkou, zda to, že bude omezováno předávání údajů do třetích zemí, o nichž bylo rozhodnuto, že poskytují „dostatečnou" úroveň ochrany,[149] je opravdu tou nejúčinnější uskutečnitelnou cestou k dosažení tohoto účelu. Ve skutečnosti vydala Evropská komise za posledních deset let od nabytí účinnosti této Směrnice jen několik rozhodnutí o dostatečnosti a žádné z nich se netýkalo dynamickým států v rozvojových částech světa, do kterých se údaje stále častěji převádějí (jako je Čína a Indie). Je tudíž evidentní, že pravidla o vydávání rozhodnutí o dostatečnosti nefungují a je třeba je revidovat.

Podstata programových problémů je zapříčiněna zejména politickými faktory. Uvedené lze demonstrovat na neochotě příslušných národních úřadů pro ochranu osobních údajů sjednotit národní požadavky v oblastech, jako je oznamovací povinnost, formality týkající se registrace vzorových smluvních ustanovení v rámci EU a schvalování stanovisek a doporučení. Ačkoli smyslem Směrnice není stoprocentní harmonizace práva a nechává členským státům při implementaci těchto norem jistý prostor k volnému uvážení, jejím cílem je přesto vysoká míra harmonizace a členské státy by měly při implementaci věnovat znění a účelu příslušných ustanovení Směrnice velkou pozornost. Členské státy ale zatím přistupují k harmonizaci svého národního práva v oblasti ochrany osobních údajů relativně váhavě, což ve většině případů pramení z jejich neochoty zříci se dlouhodobě zastávaného národního přístupu k této problematice. [150]Orgány ochrany osobních údajů tak nezřídka zastávají odlišné názory na implementaci rozhodnutí vydaných Evropskou komisí ohledně mezinárodního předávání údajů (jako je například rozhodnutí Komise 2000/520/ES o zásadách ochrany dat ve formě tzv. „bezpečného přístavu", rozhodnutí o vzorových smluvních ustanoveních atd.) a ukládání řady dalších požadavků.[151] Tento „bezpečný přístav" je koncipován tak, aby dával americkým organizacím prostředky pro splnění právního požadavku EU umožnit „odpovídající" ochranu dat informacím, podle kterých lze identifikovat osoby, jejichž osobní údaje se převádějí z EU do Spojených států,

149 A formal finding of adequacy is carried out by the Member States and the European Commission following the procedure set out in Article 30(1) of the EU Data Protection Directive, with the advice of the Article 29 Working Party.

150 K tomu více viz MATEJKA, J. a L. VOSTRÁ. Harmonizace práva v České republice – volný pohyb služeb na příkladu práva autorského. J. SUCHOŽA a J. HUSÁR, ed. *Obchodné právo a jeho širšie kontexty.* Košice: Univerzita Pavla Josefa Šafárika v Košiciach, 2010, s. 10–31.

151 V tomto ohledu je rovněž zarážející, že se vlády členských států do značné míry zbavily jakékoli odpovědnosti za formování efektivnějšího a proveditelnějšího právního rámce ochrany osobních údajů. Vlády členských států se například obecně neúčastní workshopů o mezinárodním předávání údajů, které v Bruselu pořádá Evropská komise, nepředkládají žádné návrhy Pracovní skupině 29 v rámci jejích otevřených připomínkových řízení ani nejsou ochotny vést otevřený dialog s občany a správci o důležitých problémech v oblasti ochrany osobních údajů. To svědčí o tom, že většina vlád nechápe výhody, které přináší globální proudění dat jejich ekonomikám.

jelikož právní ochrana v USA se v tomto ohledu nepovažuje za dostatečnou.[152] Bez ohledu na rozdílnosti jednotlivých systémů a přístupů, lze z povahy tohoto „bezpečného přístavu" vysledovat některé zásady. Pokud jde o správu osobních údajů, měl by mít subjekt dat možnost ve vztahu k údajům, které jsou o něm vedeny, zkontrolovat a případně je včas a transparentním způsobem opravit. Samotný subjekt dat tak nesmí být z režimu nakládání se svými údaji vyloučen.

Vývoj v oblasti harmonizace práva na ochranu osobních údajů v Evropě lze dosáhnout pouze tehdy, pokud členské státy přijmou jasný politický i právní závazek řešit existující problémy této úpravy. Dále je nutné reflektovat problém absence povědomí ve smyslu sdělnosti celého tohoto systému. Navzdory úsilí, které příslušné úřady pro ochranu osobních údajů, jakož i orgány EU v posledních letech věnovaly tomu, aby se zvýšilo povědomí o zákonu na ochranu osobních údajů, mezi občany i správci panuje o tomto zákonu a jeho požadavcích stále velká nevědomost. Většina správců svým povinnostem, které tento zákon stanoví, nerozumí a úřady na ochranu osobních údajů mají zmatené představy o tom, jak v současné době firmy údaje zpracovávají, a také občané nemají plnou představu o svých právech a povinnostech. Úroveň povědomí by se zvýšila, kdyby tvorba koncepce ochrany osobních údajů byla transparentnější. To například znamená, že iniciativy Pracovní skupiny 29 by měly před schválením projít veřejným připomínkováním, v Bruselu a v hlavních městech členských států by se měla konat pravidelná jednání o nejdůležitějších legislativních iniciativách v této právní oblasti a vlády členských států by se měly více zapojovat do tvorby koncepce ochrany osobních údajů.[153] V ideálním případě by EU měla přijmout ucelenější a jednodušší přístup k ochraně osobních údajů, než existuje nyní. To by například znamenalo sloučení Směrnice se Směrnicí č. 58 do jednoho právního nástroje, aby se dal snáze pochopit jejich vzájemný vztah. Pracovní skupina 29 by měla uveřejňovat případové studie nebo postupy na základě konzultací s občany, úřady na ochranu osobních údajů a správci údajů, které by sloužily jako vodítko při uplatňování právního rámce na skutečné situace vznikající při zpracování údajů. Pravidla ochrany osobních údajů by se co nejvíce sjednotila tak, aby z nich vznikl jednotný soubor norem platných pro zpracování osobních údajů jak ve veřejnoprávním, tak i v soukromém sektoru. Evropská komise by si lépe ohlídala, kde se členské státy odchylují od Směrnice, a členské státy a příslušné úřady by společně projednávaly důležité změny legislativy v oblasti práva na ochranu osobních údajů a společné postupy předtím, než je zavedou. Šance, že by se některé z těchto změn uskutečnily v blízké budoucnosti, je bohužel nepatrná.

Evropský systém ochrany osobních údajů lze považovat za úspěšný a v mnoha směrech efektivní, je však nutné podotknout, že příslušná Směrnice byla schválena ještě předtím, než vypukla internetová revoluce a než se zpracování dat začalo globalizovat, a tudíž je třeba ji revi-

152 SATOLA, D. a H. JUDY. Towards a Dynamic Approach to Enhancing International Cooperation and Collaboration in Cybersecurity Legal Frameworks: Reflections on the Proceedings of the Workshop on Cybersecurity Legal Issues at the 2010 United Nations Internet Governance Forum. 37 *William Mitchell Law Review.* 1745, 2011. s. 1763.

153 V tomto směru by se dalo souhlasit s Fullerovou kritikou, že na právo by se nemělo nahlížet jako na „jednosměrný projev moci" vlád, ale jako na společný podnik, v němž je nezbytná akceptace právního řádu a účast ze strany těch, kteří jsou řízeni, a jen tak může vzniknout efektivní a účinný systém regulace.

dovat a přizpůsobit tak, aby si zachovala ve vztahu k úřadům, správcům a jednotlivcům vnitřní soudržnost, a tedy i účinnost.[154] Uvedené ostatně konstatovala sama Evropská komise v rámci provádění veřejného připomínkování stávajícího právního rámce práva na ochranu osobních údajů v roce 2009, kde bylo v související zprávě uvedeno, že směrnice byla vypracována v době před plnou komercializací Internetu, kdy byla většina technologií, pomocí kterých dnes probíhá zpracování dat, stále ještě ve stadiu experimentu."[155]

4.3 Přístup mezinárodní komunity k ochraně osobních údajů a dat

Jedním z důležitých předpokladů efektivního fungování mezinárodní spolupráce, je ochrana důvěrných informací, zejména pak osobních údajů a dalších důvěrných dat, včetně těch osobních. Odhaduje se, že více než polovina hodnoty obchodů ve Spojených státech amerických je uložena právě v obchodním tajemství a ostatních právech duševního vlastnictví a že tato hodnota každým rokem klesá v řádu miliard dolarů.[156] Soukromé firmy a ostatní společnosti, které jsou vázané závazky mlčenlivosti nebo obdobnými závazky (např. advokáti, daňoví poradci atd.),[157] potřebují pro výkon své profese garance důvěrné komunikace.

Základní zásadou managementu znalostí je, že pomocí odpovídajícího sdílení informací mohou organizace přijímat správná rozhodnutí, a být tak ve své činnosti úspěšnější. Nevhodné sdílení informací, případně nesprávné zákazy s tím spojené, mají za následek větší riziko vzniku negativních důsledků, a to včetně přijímání strategicky méně vhodných rozhodnutí. Uvedené lze částečně demonstrovat na známém případě WikiLeaks z roku 2010, kde se zveřejňované zprávy orientovaly především na odhalení konspirační povahy vlád,[158] přičemž se ukázalo, že státy, instituce a další organizace jsou svého druhu stroji na výrobu a zpracování dat, a tato data pak představují vysoce účinný prostředek možného nátlaku zcela univerzálního významu. Těžko však předjímat konečný dopad tohoto konkrétního případu na tvorbu vnitřních procesů a postupů při zajišťování bezpečnosti informací. Tento incident rovněž upozornil na to, jak je obtížné určit, jaké formy sdílení, restrikcí a tudíž bezpečnostních postupů jsou vhodné pro různé typy organizací a informací. Otázkám důvěrnosti osobních údajů a dat v informační společnosti je tak nezbytné věnovat dostatečnou pozornost.

Nezbytnou součástí vytváření informační společnosti a jejího kvalitního právního

154 KUNER, Christopher. The 'Internal Morality' of European Data Protection Law (November 24, 2008). Dostupné z: dx.doi.org/10.2139/ssrn.1443797

155 SATOLA, D. a H. JUDY. Towards a Dynamic Approach to Enhancing International Cooperation and Collaboration. In: Cybersecurity Legal Frameworks: Reflections on the Proceedings of the Workshop on Cybersecurity Legal Issues at the 2010 United Nations Internet Governance Forum. 37 *William Mitchell Law Review* 1745, 2011. s. 1763.

156 Viz LAWRENCE M. SALINGER, ed. *Encyclopeadie ef White Collar & Corporate Crime*. 273. 2005.

157 Případy jako je Wikileaks demonstrují jak citlivou povahu, tak i odpovídající potřebu ochrany dat v informační společnosti.

158 ASSANGE, Julian. *State and Terrorist Conspiracies,* IQ (10. listopad 2006). Dostupné z: http://iq.org/conspiracies.pdf

prostředí je ochrana osobních údajů, a to hned vedle dalších témat jako např. svoboda projevu, právo na informace, vyjadřování politických názorů, cenzura, filtrování obsahu a nakládání s informacemi ze strany třetích stran. Subjekty osobních údajů jsou skuteční lidé a nikoli právnické osoby nebo jiné „morální osoby". Celosvětovým trendem v mezinárodních otázkách ochrany osobních údajů je přijímání přístupu založeného na výslovném zakotvení práv subjektu těchto údajů, případně přístupu výlučně ústavního (tj. v podobě judikovaných zásad vyvažování[159] soukromých zájmů jednotlivce a zájmů státu v oblasti bezpečnosti a ostatních politik nebo jiných zájmů). Tento ústavní přístup ostatně vyplývá ze Směrnice, Směrnice č. 58 a Úmluvy č. 108.[160] Jakkoliv jsou v této oblasti realizovány jisté mezinárodní aktivity,[161] chybí v této oblasti jakákoliv výrazná unifikace či jednotný přístup, byť dochází ke shodě, že hlavním problémem spojeným s ochranou osobních údajů a dalších dat je především ochrana proti druhotnému použití a zakotvení zvláštního režimu ohlašování v případě ohrožení důvěrnosti těchto dat v prostředí Internetu. Univerzální mezinárodní přístup k těmto aspektům ochrany osobních údajů však neexistuje, byť řada zemí (nikoliv pouze Evropská unie, viz níže) jde cestou vytvoření zvláštních orgánů dozoru, případně komisařů pro ochranu dat nebo soukromí. S výjimkou dopadů komunitárního práva na členské země EU tak nelze hovořit o jakékoliv formě unifikace či mezinárodní spolupráce v této oblasti, naopak existují zcela zásadní rozdíly v rozsahu poskytování této ochrany.[162] Rozdíly spočívají jak v rozsahu této ochrany (včetně toho jak intenzivně je poskytována ochrana veřejným právem), tak irozsahu oblasti oznamování zásahů do práva na ochranu osobních údajů. Průběžně je však reagováno rozšiřující se ochranou poskytovanou na základě interních pravidel dotčených autorit ve formě vývoje řady technických norem o bezpečnosti dat, zejména pak pokud jde o postupy v bankovnictví a v sektoru kreditních karet, případně o normy zavedené Mezinárodní organizací pro normalizaci (ISO), ISO 17799.[163]

Zcela zásadním faktorem, který pohání trend sbližování právních systémů USA a EU v oblasti ochrany osobních údajů, je vysoká míra integrace ekonomik USA a EU, která se proje-

159 K tomu srovnej princip proporcionality, více viz předchozí kapitola č. 3 této publikace.

160 K tomu více viz D. SATOLA a H. JUDY, ref. 155.

161 Pro úplnost je nutné zmínit existenci tzv. Fóra OSN pro správu Internetu (IGF), kde jedním z hlavních výsledků bylo založení tzv. Koalice pro ochranu soukromí, a to v roce 2009 na schůzi tohoto Fóra v Sharm el Sheik. Tato koalice společně s občanskými sdruženími a ostatními odborníky v oblasti ochrany soukromí vyhlásila tzv. „Madridskou deklaraci o soukromí", která potvrdila, že ochrana soukromí je základním lidským právem. Zatímco deklarace řeší poměrně obšírně otázky spojené s ochranou soukromí v digitálním věku, naléhá zároveň na státy, které ještě nezformulovaly komplexní rámec ochrany soukromí a nezřídily nezávislý úřad na ochranu dat, aby tak učinily co možná nejdříve. Naléhá rovněž na země, které tak doposud neučinily, aby přijaly Úmluvu č. 108. Tato úmluva byla vyhlášena k ratifikaci v roce 1981 a Rada Evropy v současné době projednává její modernizaci.

162 Obecně vzato, se ve Spojených státech právo na ochranu soukromí uplatňuje minimálně a závisí spíše na hospodářském a obchodním sektoru a na typu osobních údajů (např. data v oblasti zdravotnictví, autorskoprávní ochrana apod.). Jiné právo tak platí pro osobní údaje vedené finančními institucemi a poskytovateli zdravotní péče a jiné zase na údaje o řidičských průkazech, informace z videopůjčoven atd. V Evropě platí pro osobní údaje obecné normy podle směrnic, a to bez ohledu na jejich různorodou povahu. Právo v USA je výrazně liberálnější ohledně míry a lhůt pro udělování souhlasu ze strany subjektu dat se shromažďováním a sdílením jeho osobních údajů.

163 SATOLA, D. a H. JUDY, ref. 155.

vuje jednak silnou komerční aktivitou, jednak objemným tokem osobních dat mezi těmito ekonomikami. Mimořádně významným nástrojem je dále Doporučení o ochraně soukromí z roku 2010,[164] které se v současné době zabývá ochranou osobních údajů a dat. Jedná se především o evropský právní nástroj, ale mohou k němu přistoupit i mimoevropské země. Jedním z klíčových rysů tohoto doporučení je skutečnost, že není účinné bez dalšího, tj. země, které k němu přistoupí, musí nejprve začlenit (implementovat) jeho zásady do své vnitrostátní legislativy. Toto doporučení stanoví, že údaje se smějí *„shromažďovat pro stanovené účely, výslovně vyjádřené a legitimní, a nesmějí být dále zpracovávány způsobem neslučitelným s těmito účely*".

Dalším příkladem ilustrujícím odlišný přístup ostatních zemí, je Ekonomické seskupení Asie a Tichomoří (APEC, Asia-Pacific Economic Cooperation), které představuje organizaci sdružující 21 zemí. Cílem tohoto seskupení, které bylo založeno v roce 1989, je zlepšit ekonomické a politické vztahy mezi členskými státy. Populace členských ekonomik APEC čítá více než 2,7 miliardy obyvatel a členské ekonomiky představují přibližně padesát jedna procent světového HDP a čtyřicet jedna procent objemu světového obchodu. APEC zaměřuje svou činnost na tři klíčové oblasti: liberalizace obchodu a investic, pomoc podnikání a hospodářská a technická spolupráce. Na podporu těchto cílů zformulovala APEC svůj Rámec ochrany soukromí (dále jen Rámec). Přestože Rámec řeší úpravu ochrany soukromí v členských ekonomikách, zaměřuje se na sdílení informací mezi ekonomikami, a formou vzájemné spolupráce tak vytváří systém norem na ochranu soukromí napříč jednotlivými státy, který může rovněž sloužit obchodním korporacím. Rámec řeší ochranu soukromí spíše jako problematiku ochrany spotřebitelů a správy majetku než z hlediska lidských práv a občanských svobod a velmi silně se spoléhá na samoregulaci. Tomu ostatně odpovídá i rozsah veřejnoprávní regulace.[165] APEC v tomto ohledu zformuloval iniciativu nazvanou Cross-Border Privacy Enforcement Arrangement (CPEA),[166] která usnadňuje sdílení informací a spolupráci mezi jednotlivými orgány, které mají na starost ochranu údajů a spotřebitelů v oblasti APEC. Iniciativa CPEA, kterou ministři APEC posvětili v listopadu 2009, zahájila svou činnost 16. července 2010. Prvními signatáři byli Komisaři pro ochranu soukromí z Austrálie, Nového Zélandu, Kanady, Hongkongu a Federální obchodní komise USA, tedy orgány, které mají na starost vymáhání práva na ochranu soukromí. Iniciativy APEC znamenají podstatný krok směrem k ochraně soukromí, a to zejména v celé řadě méně rozvinutých zemí v této oblasti, a mohou položit velice cenný základ pro další vývoj tohoto právního rámce, a to včetně mezinárodní spolupráce.[167]

Dalším historickým zdrojem zásad ochrany osobních údajů je rovněž Doporučení Organizace pro hospodářskou spolupráci a rozvoj (OECD) pro ochranu soukromí a toky osobních

164 Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling.

165 APEC vznikla původně jako diskusní fórum zemí, které chtěly řešit ekonomické problémy regionu, nicméně význam a oblast působnosti se během posledního desetiletí výrazně rozrostl. K tomu více viz www.apec.org

166 Dostupné z: www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx

167 K tomu srovnej SATOLA, D. a H. JUDY, ref. 155.

údajů přes hranice ze dne 1. října 1980,[168] kde jsou stanoveny obecné zásady, kterými se ochrana soukromí a přeshraniční toky osobních údajů mají řídit. Toto Doporučení představovalo svého druhu první pokus o vytvoření komplexních a sjednocujících standardizačních pravidel na ochranu osobních dat.

4.4 Správněprávní úprava a její vybrané aspekty

4.4.1 Koncepce právní úpravy a působnost národní autority ochrany dat

Jak již bylo uvedeno výše, jsou v České republice otázky realizace práva na soukromí upraveny relativně roztříštěně a nekonzistentně. To však neplatí ohledně správněprávní regulace práva na soukromí, tj. specifické veřejnoprávní regulace ve formě úpravy ZoOÚ, který patří jednoznačně k aplikačně nejvýznamnějším právním předpisům v této oblasti, o čemž svědčí jak pestrá rozhodovací správní praxe, tak o poznání méně barvitá judikatura. Základními východisky pro zpracování nové právní úpravy ochrany osobních údajů se staly Listina, tak i předchozí a již zrušený zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech,[169] jakož i Směrnice a Úmluva č. 108. Nová koncepce je jako důsledek implementace evropského systému této ochrany postavena především na silné veřejnoprávní regulaci, jejímž praktickým důsledkem má být výrazná minimalizace rozsahu shromažďovaných osobních údajů, zejména s ohledem na přiměřenost ve vztahu k účelu, pro který jsou zpracovávány. Za účelem dosažení tohoto cíle stanoví tato regulace řadu výrazně omezujících zásad, které limitují možnosti tyto údaje zpracovávat a dále s nimi nakládat. Dohled nad aplikací zákona byl jako kontrolnímu orgánu svěřen Úřadu pro ochranu osobních údajů (dále jen Úřad), který je ze zákona nezávislým správním orgánem pro provádění dozoru nad zpracováním osobních údajů.[170] Úřad řídí jeho předseda,[171] kterého jmenuje a odvolává prezident republiky na návrh Senátu Parlamentu České republiky. Samotná nezávislost Úřadu má několik aspektů, které navazují na organizační uspořádání celé soustavy orgánů veřejné správy, zejména pak jde o funkční nezávislost na ostat-

168 Toto doporučení však z hlediska právní závaznosti a okruhu působnosti nelze počítat k významným. Nicméně zajímavé jsou právě principy, které byly na této úrovni poprvé stanoveny. Doporučení je dostupné (online) z: www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

169 Uvedený zákon upravoval ochranu osobních údajů, zejména povinnosti související s ochranou informací, pouze při provozování informačních systémů nakládajících s osobními údaji. V případě manuálního nakládání s osobními údaji bylo nutné zákon přiměřeně aplikovat. Dále stanovil odpovědnost provozovatelů takových informačních systémů a dalších fyzických a právnických osob účastnících se provádění činností souvisejících s provozováním informačních systémů. Neupravil či upravil pouze částečně řadu dalších oblastí, např. dostatečnou ochranu osobních údajů vypovídajících o osobnosti a soukromí, povinnost toho, kdo shromažďuje osobní údaje, informovat občana o jeho právech a o jiných pro něj významných skutečnostech, oznamovací povinnost nakládání s osobními údaji u kontrolního orgánu subjektem, který hodlá nakládat s osobními údaji, možnost zásahu kontrolního orgánu před zahájením takového nakládání s osobními údaji, které by z hlediska ochrany osobníc h údajů mohlo představovat určitá rizika, sankce za porušování zákona a předávání údajů do jiných zemí.

170 K tomu více viz důvodová zpráva k ZoOÚ.

171 Předseda Úřadu je jmenován na dobu 5 let. Může být jmenován maximálně na 2 po sobě jdoucí období.

ních orgánech výkonné moci, jejíž nezbytnou součástí musí být dostatečná nezávislost v rovině personální i materiální. Podmínka materiální nezávislosti tohoto orgánu však není absolutní, a to zejména s ohledem na existující praxi při tvorbě rozpočtové kapitoly Úřadu a souvisejících otázek, kde je nutné vycházet z nezávislého postavení ve vztahu k efektivitě působnosti Úřadu ve vztahu ke skutečnosti, že Úřad vykonává svěřené kompetence i vůči všem ostatním orgánům veřejné moci.[172] Samotná věcná i osobní působnost zákona není a v minulosti ani nebyla vázána toliko na otázky ochrany osobních údajů. Původní znění předmětného zákona svěřilo Úřadu kompetence pro oblast elektronického podpisu (v rozsahu ZoEP). Tato kompetence byla však ze ZoOÚ opět vypuštěna, a to zákonem č. 517/2002 Sb. s účinností dnem 1. ledna 2003, kdy byla celá problematika elektronického podpisu přesunuta do působnosti nyní již zrušeného Ministerstva informatiky ČR, která pak přešla na Ministerstvo vnitra ČR. Později pak došlo prostřednictvím zákona o některých službách informační společnosti (ZoSIS) k rozšíření kompetencí Úřadu na agendu dozoru nad dodržováním povinností při šíření obchodních sdělení a postih za nesplnění těchto povinností. V současné době je působnost Úřadu relativně široká, týká se jak působnosti věcné, tak i osobní, přičemž její vymezení lze kromě ZoOÚ hledat v celé řadě souvisejících zákonných předpisů.

Dalším z důležitějších předpisů je zákon č. 111/2009 Sb., o základních registrech, v platném znění (dále jen ZoZR) který vymezuje obsah všech základních registrů, informačního systému základních registrů a informačního systému územní identifikace a stanoví práva a povinnosti, které souvisejí s jejich vytvářením, užíváním a provozem, přičemž zároveň zřizuje Správu základních registrů, tedy správní úřad, který je podřízen Ministerstvu vnitra ČR. Základními registry ve smyslu § 3 předmětného zákona jsou:

- základní registr obyvatel (dále jen „registr obyvatel", případně „ROB"),
- základní registr právnických osob, podnikajících fyzických osob a orgánů veřejné moci (dále jen „registr osob", případně „ROS"),
- základní registr územní identifikace, adres a nemovitostí (dále jen „registr územní identifikace", případně „RUIAN"),
- základní registr agend orgánů veřejné moci a některých práv a povinností (dále jen „registr práv a povinností", případně „RPP").

Působnost Úřadu vyplývá zejména z ustanovení § 11 zákona o základních registrech, podle kterého Úřad vytváří zdrojové identifikátory fyzických osob (ZIFO) a agendové identifikátory[173] fyzických osob a vede jejich seznamy, a zároveň zajišťuje převod agendového identifikátoru fyzické osoby v agendě na agendový identifikátor této fyzické osoby v jiné agendě, a to na základě zákonného požadavku. Samotná bezpečnost osobních údajů je v základních

172 Úřad je tak standardním příkladem nezávislého regulačního orgánu, jež v sobě koncentruje pravomoci tradičně náležející orgánům moci zákonodárné, výkonné a soudní (čímž se vymykají tradiční dělbě moci) v oblasti zvláštních agend, v jejichž rámci je požadována zesílená ochrana práv a oprávněných zájmů zainteresovaných subjektů. K tomu více viz HANDRLICA, J. Ke koncepci tzv. „nezávislých regulačních orgánů" a k problematice jejich „nezávislosti". *Správní právo*. 2005, č. 4.

173 Ve smyslu ustanovení § 11 odst. 2 zákona o základních registrech, v platném znění, používá zdrojový identifikátor fyzické osoby výhradně jen Úřad pro vytváření agendových identifikátorů fyzických osob.

registrech založena na zdrojovém identifikátoru fyzické osoby a agendových identifikátorech fyzických osob, které jsou neveřejné.[174] Zdrojový identifikátor generuje Úřad a je veden pouze v evidenci zdrojových identifikátorů fyzických osob. Orgány veřejné moci mají přiděleny pouze agendové identifikátory, nikoliv tedy zdrojové. Na základě ustanovení § 14 odst. 4 ZoZR zasílá do datové schránky bezplatně Správa základních registrů tzv. záznam o využívání údajů v základním registru osobě, o které jsou tyto údaje vedeny, a to za předpokladu, že tato osoba má zřízenu a zpřístupněnu datovou schránku. Tento záznam se vždy zasílá za uplynulý kalendářní rok.

Pro úplnost je nutné uvést, že na základě § 7 zákona o základních registrech je dána generální povinnost Správy základních registrů informovat Úřad o jakékoliv důvodné pochybnosti o neoprávněném přístupu orgánu veřejné moci k osobním údajům.

Dalším zákonným předpisem určujícím působnost Úřadu je zákon č. 341/2011 Sb., o Generální inspekci bezpečnostních sborů, v platném znění, kde na základě ustanovení § 45 písm. b) je dána povinnost této inspekce neprodleně ohlásit Úřadu zřízení každé evidence obsahující osobní údaje (součástí tohoto ohlášení je název organizační části odpovědné za zpracovávání osobních údajů, účel evidence, kategorie subjektů údajů a osobních údajů, které se těchto subjektů týkají, a popis opatření k zajištění požadované ochrany osobních údajů). Dále pak v ustanovení § 52 odst. 2 písm. b) téhož zákona je dána kompetence Úřadu, podle něhož je inspekce povinna na písemnou žádost soudu nebo Úřadu provést neprodleně a bezplatně označení údajů vztahujících se k osobě žadatele, jestliže žadatel popírá jejich přesnost a nelze zjistit, zda jsou přesné, nebo nikoli.[175] Podobná povinnost jako v předchozím případě je pak zakotvena v ustanovení § 83 zákona č. 273/2008 Sb., o Policii České republiky, kde je dána působnost Úřadu odstranit označení údajů, které bylo provedeno policejním prezídiem na základě žádosti subjektu údajů, jestliže tento popírá jejich přesnost a nelze zjistit, zda jsou přesné, nebo nikoli. Obdobně, jak je tomu výše, byla ve smyslu ustanovení § 86 stanovena povinnost policie neprodleně ohlásit Úřadu zřízení každé evidence obsahující tyto osobní údaje.[176] Podobně je založena povinnost Vojenské policie informovat v předepsaném rozsahu Úřad o zřízení evidence osobních údajů na základě § 35e zákona č. 124/1992 Sb., o Vojenské policii, v platném znění.

Pro oblast elektronických komunikací je významným zákonem vymezujícím působnost Úřadu především zákon o elektronických komunikacích, kde je v ustanoveních § 87 a násl. upravena ochrana osobních, provozních a lokalizačních údajů a důvěrnost komunikací v oblasti služeb a sítí elektronických komunikací. Výkon dozoru ve smyslu § 87 tohoto zákona pak vykonává Úřad podle ZoOÚ, přičemž práva a povinnosti související s ochranou osobních

174 Agendový identifikátor fyzické osoby (AIFO) je neveřejným identifikátorem, který je jednoznačně přiřazen záznamu o fyzické osobě v příslušném agendovém informačním systému nebo základním registru, je odvozen ze zdrojového identifikátoru fyzické osoby a kódu agendy a je užíván výlučně k jednoznačnému určení fyzické osoby pro účely výkonu agendy, pro kterou byl přidělen.

175 Takové označení se odstraní pouze se souhlasem žadatele nebo na základě rozhodnutí příslušného soudu anebo Úřadu.

176 Součástí tohoto ohlášení je název útvaru odpovědného za zpracovávání osobních údajů, účel evidence, kategorie subjektů údajů a osobních údajů, které se těchto subjektů týkají, a popis opatření k zajištění požadované ochrany osobních údajů.

údajů, jež tento zákon neupravuje, se řídí zákonem o ochraně osobních údajů (§ 87 odst. 2). Specifická oblast zabezpečení ochrany osobních, provozních a lokalizačních údajů a důvěrnosti komunikací je upravena v § 88 zákona, kde je dána široká působnost Úřadu na postupy v případech porušení ochrany osobních údajů u podnikatelů poskytujících veřejně dostupnou službu elektronických komunikací. Pro úplnost je nutné zmínit také ustanovení § 130 odst. 3 zákona, které stanoví povinnost Českého telekomunikačního úřadu konzultovat otázky ochrany osobních údajů s Úřadem, případně zmocňovací ustanovení § 150, jež zmocňuje Úřad vydat vyhlášku k provedení § 88 odst. 7 zákona, kde může stanovit podrobnější podmínky, za nichž je podnikatel poskytující veřejně dostupnou službu elektronických komunikací povinen oznámit porušení ochrany osobních údajů.[177]

V oblasti služeb informační společnosti je nutné zmínit ZoSIS, kde je na základě ustanovení § 10 tohoto zákona Úřad příslušným orgánem k výkonu dozoru nad dodržováním tohoto zákona pro šíření obchodních sdělení, přičemž mu přísluší projednávání souvisejících správních deliktů a přestupků. Uvedená působnost však nedopadá na šíření obchodních sdělení prostřednictvím ISDS, které podle § 26c ZoEÚ spadá do působnosti Ministerstvo vnitra ČR. Duplicitně s touto působností je v souvislosti s tím Úřadu svěřen také dozor nad nevyžádanou reklamou šířenou elektronickými prostředky ve smyslu zákona o regulaci reklamy.

Neméně významnou je pak zvláštní kompetence Úřadu v oblasti evidence obyvatel a identifikačních dokladů. Na základě ustanovení § 17e zákona o evidenci obyvatel, je Úřadu svěřena působnost pro projednávání správních deliktů spočívajících v neoprávněném nakládání, resp. v neoprávněném využívání rodných čísel. Obdobně je na základě ustanovení § 34a až 34c zákona o cestovních dokladech svěřena působnost k Úřadu k projednávání správních deliktů a přestupků spočívajících v neoprávněném zpracování údajů v nosiči dat s biometrickými údaji, případně působnost k projednávání správních deliktů a přestupků spočívajících v neoprávněném zpracování strojově čitelných údajů vedených v občanských průkazech a údajů vedených v kontaktním elektronickém čipu na základě § 16a a násl. zákona o občanských průkazech.[178]

4.4.2 Základní zásady v zákoně o ochraně osobních údajů

Předmětem ZoOÚ je především úprava práv a povinností při zpracování osobních údajů a stanovení podmínek, za nichž se uskutečňuje předání osobních údajů do jiných států,

177 Uvedené zmocňovací ustanovení bylo do zákona o elektronických komunikacích začleněno s účinností dnem 1. 1. 2012, a to zákonem č. 468/2011 Sb., ze dne 6. prosince 2011, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a některé další zákony.

178 Nejde však o výčet vyčerpávající. Z dalších předpisů upravujících působnost Úřadu lze uvést např. zákon o zaměstnanosti, jehož § 17 upravuje povolování předání osobních údajů fyzických osob, kterým je zprostředkováváno zaměstnání, mimo členské státy EU, případně zákon č. 159/2006 Sb., o střetu zájmů, v platném znění, jehož § 23 a násl. upravuje projednávání přestupků, které se týkají používání osobních údajů obsažených v registrech vedených podle tohoto zákona.

a to k naplnění práva každého na ochranu před neoprávněným zasahováním do soukromí (§ 1 zákona). Zákon se vztahuje na všechny osobní údaje, které zpracovávají státní orgány, orgány územní samosprávy, jiné orgány veřejné moci, jakož i fyzické a právnické osoby.[179]

Za účelem zajištění efektivity a sdělnosti těchto práv, povinností a podmínek, pracuje platná právní úprava s celou řadou zásad, které mají svůj nezpochybnitelný normativní, ale vzhledem ke své povaze také interpretační význam. Za zásady tak lze považovat obecné právní myšlenky, které vyjadřují poslání, cíle a úkoly systému ochrany soukromí (osobních údajů), kde se tyto právní myšlenky musejí projevovat v konkrétních normách této ochrany, byť nemusejí být projeveny výslovně a zpravidla ani nemusejí být zcela totožné s normami právními. Lze tak vycházet z určitého (nad)pozitivního charakteru[180] těchto principů jako nositelů hodnot, případně jsou tyto principy identifikovány dle jejich dlouhodobosti působení a prostorové rozšířenosti v rámci celého systému ochrany.[181] Tyto zásady (právní principy) tak mají povahu určité extrakce či druhového souhrnu základních práv, povinností a axiomatiky úpravy, jež vyjadřuje charakter, případně dílčí úkoly samotného systému ochrany a vyznačují se vysokou mírou obecnosti, čímž udávají obecné mantinely zvláštního režimu práv a povinností, v jakých by měla ochrana soukromí probíhat.

Klíčovou je zde zásada nezávislosti dozorového orgánu, která představuje conditio sine qua non efektivního fungování systému ochrany osobních údajů. Zakotvení nezávislé veřejnoprávní instituce dozorující na dodržování zákonného rámce ochrany osobních údajů představuje zásadní požadavek vyplývající z evropského systému ochrany osobních údajů.

Jednou ze základních zásad je především zásada legitimity, která reflektuje skutečnost, že zpracovat lze pouze takové osobní údaje, které byly získány poctivě a v souladu se zákonem. Při nakládání s osobními údaji musí být respektována základní práva a svobody jednotlivců, kterých se zpracování týká, zejména pak musí být naplněno právo každého na ochranu před neoprávněným zasahováním do soukromí.

Další zásadou je zásada informovaného souhlasu, podle které mohou být zpracovávány pouze ty osobní údaje, s jejichž zpracováváním vyslovil subjekt údajů svůj souhlas. Tento souhlas musí představovat svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů. Vědomost souhlasu implikuje skutečnou informovanost subjektu o jeho povaze (viz pojem informovaný souhlas řešený níže).[182] Tato zásada však neplatí absolutně, zákon stanoví, že i bez tohoto souhlasu lze osobní údaje zpracovávat v taxativně vymezených případech (jako např. k ochraně životně důležitých zájmů subjektu údajů, v případě oprávněném zveřejnění osobní údajů, případně je-li to nezbytné pro ochranu

179 Zákon se však nevztahuje na zpracování osobních údajů, které provádí fyzická osoba výlučně pro osobní potřebu nebo na nahodilé shromažďování osobních údajů, pokud tyto údaje nejsou dále zpracovávány.

180 Srov. KUHN, Z. *Aplikace práva ve složitých případech: K úloze právních principů v judikatuře.* Praha: Karolinum, 2002, s. 283.

181 K tomu více viz GALVAS, M. O některých pracovněprávních důsledcích Nálezu Ústavního soudu č. 116/2008 Sb. In: *Spisy právnické fakulty Masarykovy univerzity v Brně.* Sv. 341. Brno: Masarykova univerzita, 2008, s. 74.

182 K tomu více viz např. NONNEMAN, F. Náležitosti souhlasu se zpracováním osobních údajů. *Právní rozhledy.* 2011, č. 9.

práv a právem chráněných zájmů správce – např. ochrana majetku, atd.).[183] Zajímavé je, že v mezinárodních dokumentech nemá tato zásada zásadní právní zakotvení, kterého by si zasluhovala, naopak v souvislosti s ochranou soukromí nebývá obvykle otázka informovaného souhlasu subjektu řešena. [184]

Samotná právní povaha souhlasu se zpracováním osobních údajů, ostatně podobně jak tomu bude i u jeho odvolání, je poměrně jednoznačná.[185] Jde bezesporu o právní úkon, který musí splňovat všechny náležitosti vyžadované občanským právem (viz § 34 a násl. ObčZ). Jakkoliv jde zdánlivě o jednostranný souhlas subjektu údajů, je nutné podotknout, že se spíše blíží smlouvě, tj. dvoustrannému úkonu, jde totiž o vztah synallagmatický, tedy vzájemně podmíněný, kde plnění jednoho (projev směřující k udělení souhlasu) je ke vzniku právních účinků podmíněno plněním druhého (přijetí takového souhlasu a zahájení zpracovávání osobních údajů na základě tohoto souhlasu).[186] Takovýto souhlas musí být svobodný a vážný a musí být učiněn ve srozumitelné formě, určitým způsobem a k tomu oprávněnou osobou. Rovněž odvolání souhlasu musí splňovat všechny tyto náležitosti. Pokud je však právní vztah ukončen dříve, než bylo jeho oběma stranami dojednáno nebo předpokládáno, je teoreticky možné posuzovat i otázku souladu takového jednání s dobrými mravy.[187] Tento souhlas pak musí být správce (zpracovatel) schopen prokázat po celou dobu zpracování (§ 5 odst. 4 zákona).

Zásada finality[188] reprezentuje skutečnost, že osobní údaje lze shromažďovat pouze pro konkrétní a legitimní účel, jenž musí být určen ještě před samotným zpracováváním osobních údajů. Do okamžiku stanovení (určení) takovéhoto účelu nelze s osobními údaji jakkoliv nakládat. Údaje rovněž nesmí být zpracovávány k účelům, které by odporovaly tomuto určenému původnímu zamýšlenému účelu. Zpracovávat osobní údaje k jinému účelu lze pouze v mezích výjimek uvedených v ustanovení § 3 odst. 6 zákona, nebo pokud k tomu dal subjekt údajů předem souhlas.

Se zásadou finality úzce souvisí zásada proporcionality,[189] zpracování osobních údajů totiž může být realizováno pouze za účelem dosažení stanoveného účelu a jen v míře nezbytně nutné k jeho dosažení. Uvedená zásada se tak přímo vztahuje na podmínku doby zpracovávání (např. uchovávání datového záznamu), rozsah a kvalitu osobních údajů. Zásada tak mimo jiné

183 K taxativnímu vymezení těchto výjimek viz § 5 odst. 2 písm. a) až g) zákona o ochraně osobních údajů.

184 Tato otázka např. není ani řešena ve výše uvedené Úmluvě č. 108, lze ji však nepřímo dovodit interpretací. Stanoví totiž požadavek, podle kterého osobní údaje musejí být získávány poctivě a v souladu se zákony. Je-li tedy tato povinnost stanovena, je třeba ji plnit

185 K tomu srovnej DOLEŽAL, T. Problematické aspekty vztahu lékaře a pacienta zejména s ohledem na institut tzv. informovaného souhlasu. Časopis zdravotnického práva a bioetiky. Rok 2011, roč. 1, č. 1, s. 25.

186 Podobně lze přistupovat např. ke kvalifikaci plné moci jako jednostranného prohlášení zmocnitele směřující k třetím osobám o tom, že zmocněnec je oprávněn zastupovat zmocnitele, a o rozsahu, v jakém mu toto oprávnění náleží. Od tohoto jednostranného prohlášení je však nutné odlišovat dvoustranný právní úkon, na jehož základě je zmocněnec oprávněn (případně i povinen) zmocnitele zastupovat. Zákon označuje takový úkon jako „dohodu o plné moci". Tou bývá obvykle příkazní či mandátní smlouva. Plná moc jako jednostranné prohlášení může tvořit rovněž součást smlouvy, zakládající právní vztah mezi zmocnitelem a zmocněncem.

187 K tomu více viz § 3 odst. 1 ObčZ, případně rozsudek NS, sp. zn. 29 Cdo 1583/2000.

188 Lze se setkat s označením této zásady jako zásadou účelovosti, resp. určenosti cílem.

189 Tato zásada se někdy nepřesně nazývá zásadou minimalizace.

určuje povinnost likvidace těchto údajů v případě, že se stanou již nepotřebnými vzhledem k dosažení stanoveného účelu. Osobní údaje, které jsou předmětem zpracování je proto nutné uchovávat pouze po dobu, která je nutná k naplnění předem stanoveného účelu. V tomto ohledu nepřipouští tato zásada žádnou bezbřehou archivaci údajů.[190] Zásada zákazu sdružování osobních údajů (zásada spojování databází) je dalším projevem zásady proporcionality. Tato zásada zakazuje sdružovat údaje získané k rozdílným účelům. Je tedy nepřípustné propojovat jednotlivé databáze těch osobních údajů, které byly získány za různým účelem využití.

Zásada transparentnosti (informovanosti a oznamovací) reflektuje požadavek směřující k získání úplných, srozumitelných a pravdivých informací o zpracovávaných údajích, jakož i souvisejících skutečností. Jde tak o zakotvení široké povinnosti informovat dotčené osoby, kterých se týká zpracování údajů (správce musí poskytnout osobě, od které získává údaje, které se jí týkají, některé informace (totožnost správce, účely zpracování, příjemci údajů atd.), jakož i povinnost oznámit zpracovávání osobních údajů úřadu před zahájením zpracování.

Další zásadou je zásada kvality údajů, která vyjadřuje skutečnost, že osobní údaje musí být zejména zpracovány přesně, a je-li to nezbytné, musí být aktualizovány. Zásada tak zakládá právo dotčené osoby na opravu nepřesných a nepravdivých či zastaralých údajů nebo právo na jejich úplný výmaz v případě, pokud byly zpracovány v rozporu se zákonem. Zjistí-li správce, že jím zpracované osobní údaje nejsou s ohledem na stanovený účel přesné, provede bez zbytečného odkladu přiměřená opatření, zejména zpracování blokuje a osobní údaje opraví nebo doplní, jinak osobní údaje zlikviduje.

Významnou je rovněž zásada důvěrnosti a bezpečnosti zpracování, která stanoví, že jakákoli osoba, která jedná z pověření správce nebo zpracovatele, jakož i samotný zpracovatel, který má přístup k osobním údajům, je může zpracovávat pouze podle pokynů správce. Přímým důsledkem této zásady je povinnost správce a zpracovatele osobních údajů přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů.[191] Správce i zpracovatel je povinen dále zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů. Tato povinnost je ve smyslu § 13 odst. 3 zákona posílena pro oblast automatizovaného zpracování, kde je správce nebo zpracovatel v rámci opatření povinen také:

- zajistit, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze oprávněné osoby,
- zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby,
- pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány,
- zabránit neoprávněnému přístupu k datovým nosičům.

190 Výjimky jsou připuštěny v případech dlouhodobého uchovávání údajů například pro vědecké, statistické či archivní účely.

191 Tato povinnost platí i po ukončení zpracování osobních údajů.

Zvýšený důraz na aplikaci zásady důvěrnosti a bezpečnost zpracování osobních údajů klade zejména neustálý vývoj v oblasti prostředků elektronického zpracování dat i možností jejich ochrany. Z toho vychází i výše uvedený § 13 zákona, který však neobsahuje taxativní výčet opatření potřebných k zajištění bezpečnosti zpracovávaných dat. Splnění povinnosti stanovené § 13 odst. 1 zákona závisí na mnoha faktorech, které se u jednotlivých správců, případně i u jednotlivých zpracování osobních údajů mohou velice lišit, nezřídka pak bývá konkrétní rozsah a způsob ochrany dat předmětem obchodního tajemství. V takových případech je však nutno individuálně posuzovat a zohlednit odlišný rozsah existujících rizik, včetně eliminace těchto rizik při zpracování osobních údajů ve veřejnoprávních informačních systémech (jako je např. evidence obyvatel, rejstřík trestů atd.).[192] Samotné posouzení rizik souvisejících se zpracováním osobních údajů je otázkou vyhodnocení konkrétní situace daného správce či zpracovatele, zejména pak zvolených či stanovených prostředků a způsobu zpracování osobních údajů, druhu a rozsahu těchto údajů, ale také třeba specifik lokality či budovy, v níž ke zpracování dochází.[193] Při hledání základního přístupu pro určení adekvátních bezpečnostních opatření je možné se inspirovat již zmíněným recitálem 46 Směrnice, kde je vyjádřen požadavek na přijetí odpovídajících technických a organizačních opatření, a to jak při přípravě zpracování osobních údajů, tak i v jeho samotném průběhu, s cílem zajistit bezpečnost dat a zabránit jakémukoli neoprávněnému zpracování. Přijatá opatření přitom musejí vykazovat náležitou odbornou úroveň odrážející rizika spojená s konkrétními operacemi s osobními údaji a s povahou zpracovávaných údajů. Důležité je také zdůraznit, že jak Směrnice, tak § 13 zákona předpokládají, že správci a zpracovatelé osobních údajů budou muset na přijetí vhodných opatření vynaložit vysoké náklady. Správce je osobou, která o zpracování osobních údajů rozhodla, a proto je povinen nést i související náklady na tato opatření.[194]

Aplikace zásady důvěrnosti a bezpečnosti zpracování osobních údajů obsahově vychází z realizace řady opatření, jimiž správce osobních údajů plní svou zákonnou povinnost ve smyslu § 13 odst. 1 zákona. Rozsah této povinnosti lze vymezit několika oblastmi. První oblast představuje objektové zabezpečení (jako např. zámky, mříže či bezpečnostní fólie na oknech, zabezpečovací systémy atd.),[195] tedy opatření ve vztahu k ochraně prostor a objektů, kde jsou osobní údaje uchovávány, před náhodným i úmyslným neoprávněným vstupem a odcizením

192 MATOUŠOVÁ, M. a L. HEJLÍK. *Osobní údaje a jejich ochrana.* Praha: ASPI, Wolters Kluwer, 2008.

193 KUČEROVÁ, A., V. BÁRTÍK, J. PECA, K. NEUWIRT, a J. NEJEDLÝ. *Zákon o ochraně osobních údajů: Komentář.* 1. vydání. Praha: C. H. Beck, 2003.

194 KUČEROVÁ, A., L. NOVÁKOVÁ, V. FOLDOVÁ, F. NONNEMAN, a D. POSPÍŠIL. *Zákon o ochraně osobních údajů: Komentář.* 1. vydání. Praha : C. H. Beck, 2012, s. 17.

195 Jsou-li osobní údaje zpracovávány manuálně, což v současné době znamená zejména uchování nejrůznějších dokumentů, např. životopisů uchazečů o zaměstnání nebo kopií vysvědčení, které sloužily k ověření požadované kvalifikace, podkladů pro uzavření smluv anebo formulářů, jejichž prostřednictvím byly shromažďovány potřebné osobní údaje, je nezbytné zajistit, aby kartotéky či skříně, v nichž jsou tyto listiny uloženy, byly uzamykatelné, umístěné na vhodném místě, tedy nikoli ve volně přístupných místnostech apod. Nutno rovněž realizovat související organizační opatření, včetně zakotvení zvláštního režimu vstupu do prostor, kde jsou tyto písemné dokumenty uchovávány, jakož i stanovení dalších pravidel nakládání s těmito dokumenty (obvykle inkorporací těchto pravidel do pracovněprávních úkonů či směrnic).

dat. Do druhé oblasti patří zabezpečení týkající se zpracování osobních údajů prostřednictvím výpočetní techniky, kde je třeba chránit počítače alespoň vstupním heslem, popř. i dalšími přístupovými právy. Současně tak lze z uvedeného dovozovat § 13 odst. 3 písm. d), že není přípustné, aby jednu sadu přístupových hesel (oprávnění) sdílelo více osob, neboť tím se významně snižuje možnost vyvození odpovědnosti za jednání konkrétní osoby, a vzniká tak prostor mj. i pro neoprávněné zpracování osobních údajů. Je třeba zabezpečit také vlastní servery, resp. datové nosiče.[196] Mezi další oblast patří opatření organizační povahy ve smyslu zakotvení jasných pravidel promítnutých do obsahu souvisejících smluvních ujednání, případně opatření směřujících do pracovněprávních vztahů správce.

Význam ustanovení § 13 odst. 1 ZoOÚ narůstá zejména v případech, kdy je nutno přistoupit k likvidaci nosičů osobních údajů (tj. listin nebo CD, DVD či jiných záznamových zařízení). Za souladný postup dle ZoOÚ nutno považovat pouze důslednou skartaci těchto nosičů či jinou obdobnou forma jejich bezpečné fyzické či spolehlivé datové likvidace. Rizika pro bezpečnost osobních údajů vznikají také v souvislosti s využíváním elektronické pošty, kdy je třeba dbát na to, aby předmětné sdělení či dokument obsahující osobní údaje odešel skutečně výhradně na adresu oprávněné osoby (např. v důsledku využití funkce „odpovědět všem" může být zpráva zaslána i příjemcům, kteří nejsou oprávněni se s konkrétními osobními údaji seznámit). V oblasti elektronické komunikace je ostatně v souladu s § 13 zákonem nutné trvat na zabezpečení např. formou šifrování zpráv a ověřování totožnosti uživatele a serveru například v souvislosti s používáním zaručeného elektronického podpisu; odesílání osobních údajů elektronickou poštou bez jakéhokoli zabezpečení je s ohledem na zvýšené riziko spojené s „překlepnutím" či omylem v osobě adresáta anebo s útokem hackera nutné považovat za rizikové jednání, které v případě většího rozsahu dat, případně jsou-li takto zasílány citlivé údaje, vede k porušení § 13 odst. 1 zákona.[197]

Samotný přístup k informacím (osobním údajům) zpracovávaným v informačním systému je tak nutné chránit formou fyzické ochrany datových nosičů a datových úložišť před neoprávněnými osobami, tedy např. před krádeží či okopírováním. Také ve vztahu k datovým nosičům je na místě přijmout vhodná organizační i technická opatření, tj. zejména určit, jak je nutné datové nosiče uchovávat a jakým způsobem lze s datovými nosiči na daném pracovišti nakládat, např. jakou cestou je lze předávat zpracovatelům osobních údajů nebo zda a za jakých okolností lze datové nosiče odnášet mimo místo výkonu práce. V tomto ohledu již bylo judikováno,[198] že existují určité standardy bezpečnostních opatření, které lze při ochraně osobních údajů realizovat, aniž by musely být výslovně stanoveny zákonem.

196 Vodítkem může být i demonstrativní výčet opatření uvedený na formuláři Úřadu „Oznámení o zpracování osobních údajů" (dostupné z www.uoou.cz), kde jsou uvedena základní bezpečnostní opatření (z hlediska zabezpečení budov a místností se jedná o zámky, mříže apod., centrální pult ochrany, elektronické zabezpečení či bezpečnostní směrnice, v oblasti automatizovaného zpracování se potom jedná o přístupová práva, bezpečnostní zálohy, antivirovou ochranu nebo šifrování). Návod při zvažování vhodných bezpečnostních opatření lze hledat i v mezinárodních (ISO) či českých technických normách (ČSN).

197 KUČEROVÁ, A., L. NOVÁKOVÁ, V. FOLDOVÁ, F. NONNEMAN, a D. POSPÍŠIL, ref. 194, s. 50.

198 Rozsudek NSS, čj. 3 As 21/2005-105, kde Nejvyšší správní soud posuzoval incident s odcizením zálohovacího zařízení, na základě kterého přijala stěžovatelka množství opatření, kterými se snažila zabránit možnému opakování podobných událostí (zavedení kontroly režimu vstupu do budov společnosti; evidence přidělování klíčů; evidence

Výkladem § 13 zákona se zabýval i Nejvyšší správní soud České republiky,[199] který k otázce tvrzené protiústavnosti názoru Městského soudu v Praze ve vztahu k argumentaci, že existují určité standardy bezpečnostních opatření při ochraně osobních údajů, uvádí, že právní názor Městského soudu v Praze sdílí, přičemž na podporu tohoto názoru odkazuje na výše citovanou důvodovou zprávu k ustanovení § 13 zákona, kde se mimo jiné říká, že opatřeními, která je správce povinen učinit, se rozumí opatření technická, organizační, právní a jiná. Zákonodárce tak do textu důvodové zprávy v podstatě zahrnul část znění čl. 17 Směrnice (rovněž viz výše), kterou zřejmě neshledal nezbytnou při formulaci ustanovení § 13 zákona, a tuto ještě doplnil o opatření právní a jiná. I Nejvyšší správní soud připouští, že užitá dikce klade na správce a zpracovatele v jistém smyslu vyšší nároky, když způsob a prostředky zabezpečení osobních údajů ponechává na jednu stranu jejich vlastní úvaze, na druhou stranu za nesplnění předmětné povinnosti hrozí poměrně vysokými sankcemi. Nelze však akceptovat směr, kterým se ubírá argumentace stěžovatelky, neboť tento by v konečném důsledku vedl k nepoužitelnosti ustanovení § 13 zákona jako celku. Nejvyšší správní soud tak uzavírá, že výklad Městského soudu v Praze je zcela legitimní, neboť obecná formulace ustanovení § 13 zákona nutně předpokládá přijetí naprosto konkrétních opatření organizačních a technických, kdy by měl „standard" představovat jakési nutné minimum. Nejvyšší správní soud považuje v této souvislosti rovněž za významné, že po incidentu s odcizením zálohovacího zařízení přijala stěžovatelka množství opatření, kterými se snažila zabránit možnému opakování podobných událostí (zavedení kontroly režimu vstupu do budov společnosti; evidence přidělování klíčů; evidence vstupu osob do serveroven etc.), a výše naříkaná skromnost formulace ustanovení § 13 zákona jí v tom nijak nebránila.

4.4.3 Pojem osobní údaj jako jeden z klíčových pojmů určující věcnou působnost ZoOÚ

Podstatným pojmem celé úpravy ochrany osobních údajů je pojem osobní údaj. Na tomto pojmu je založena jak samotná koncepce ochrany, tak i vymezení její věcné působnosti, tj. samotné určení okruhu společenských vztahů, na které dopadají ustanovení této právní úpravy. Zákon upravuje práva a povinnosti při zpracování osobních údajů (viz § 1 zákona), a tak existence osobních údajů představuje svého druhu conditio sine qua non jakékoliv aplikace této právní úpravy na společenské vztahy. Nejsou-li splněny zákonem předpokládané definiční znaky pojmu osobní údaj, nelze předmětnou úpravu, byť i jen zčásti, aplikovat. Naopak předmětnou právní úpravu lze aplikovat pouze tehdy, pokud objektivně existuje informace, která je osobním údajem (objektivní podmínka), přičemž je způsobilá neoprávněně zasáhnout do soukromí člověka (subjektivní podmínka). Pojem osobní údaj je tak pojmem specifickým pro

vstupu osob přistupujících k serveru atd.). Předmětné rozhodnutí je dostupné z: ispis.cz/judikatura/3As21/2005

199 Rozsudek NSS, čj. 3 As 21/2005-105. Dostupné z: ispis.cz/judikatura/3As21/2005

veřejnoprávní rozměr úpravy ochrany soukromí, přičemž nepostihuje všechny způsoby, kterými lze zasáhnout do soukromí člověka.

Svým způsobem tak jde o úpravu komplementární, jejímž smyslem je jak preventivní působení, tak i následné prostřednictvím sankce, to vše zcela automaticky, navíc zásadně nezávisle na aktivitě konkrétní fyzické osoby, jejíž soukromí je předmětem ochrany. Paralelně s touto ochranou může být ochrana soukromí realizována řadou dalších opatření, zejména pak žalobou na ochranu osobnosti podle příslušných ustanovení ObčZ. Jak vyplývá z předchozích částí této publikace, je pojem soukromí pojmem značně neostrým a flexibilním,[200] přičemž nesporně pokrývá celou řadu chráněných hodnot, jež jsou spjaty se soukromím jedince a představují hodnoty lidskoprávní, jako např. lidská důstojnost, osobní čest, dobrá pověst nebo jméno.[201] Samotná veřejnoprávní ochrana směřující proti neoprávněnému nakládání s osobními údaji tak představuje pouze jeden z mnoha právních prostředků ochrany soukromí, přičemž ani zdaleka neposkytuje ochranu soukromí jako celku, navíc vyčerpávajícím způsobem. Naopak ochrana osobních údajů stanoví zvláštní režim pouze pro relativně omezenou část soukromí, jde tak spíše o fragment ochrany soukromí v podobě zákonných podmínek nakládání s osobními údaji, jejímž definičním základem je pojem osobní údaj.

Veřejnoprávní režim ochrany osobních údajů a soukromoprávní prostředky ochrany se tedy mohou překrývat, což je patrné např. u pojmu projev osobní povahy, uvedeného v § 11 ObčZ.[202] Právo na ochranu osobních údajů, stejně jako právo na respektování projevů osobní povahy, je složkou práva na ochranu osobnosti, a proto vždy dochází k jejich prolínání (např. obrazový či zvukový záznam anebo dopis velmi často obsahují nejrůznější informace o konkrétní fyzické osobě, tj. osobní údaje). Ač se jedná o dva odlišné pojmy, mohou být svým obsahem identické. Lze říci, že každý projev osobní povahy, který můžeme přiřadit ke konkrétní osobě, je osobním údajem, nicméně osobním údajem mohou být i informace odlišného charakteru, nezávislé na osobnosti jedince, např. rodné číslo nebo číslo bankovního účtu.[203]

Současná[204] definice pojmu osobní údaj je vymezena v ustanovení § 4 ZoOÚ, přičemž se osobním údajem rozumí *„jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo*

200 Podobně je tomu u řady jiných právních pojmů, které jsou proměnlivé a jsou velmi úzce navázány na další pomocné právo – vědní disciplíny (jako např. na právní sociologii apod.) a na kulturní prostředí.

201 Totéž platí pro ochranu soukromého a rodinného života. Viz výše.

202 K tomu srovnej velmi podobnou úpravu promítnutou do NObčZ.

203 Pro posouzení toho, zda má dotčená osoba v konkrétním případě svá osobnostní práva a právo na soukromí hájit prostřednictvím veřejnoprávní úpravy provedené v ZoOÚ nebo žalobou na ochranu osobnosti u obecného soudu, bude klíčový zejména charakter zásahu do soukromí, resp. míra a způsob využití informací, které se k této osobě vztahují, a jejich charakter. K tomu více viz KUČEROVÁ, A., L. NOVÁKOVÁ, V. FOLDOVÁ, F. NONNEMAN, a D. POSPÍŠIL, ref. 194, s. 50.

204 K tomu srovnej definici uvedenou v ustanovení § 4 písm. a) původního znění zákona č. 101/2000 Sb., o ochraně osobních údajů, kde se osobním údajem rozumí *„jakýkoliv údaj týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze na základě jednoho či více osobních údajů přímo či nepřímo zjistit jeho identitu. O osobní údaj se nejedná, pokud je třeba ke zjištění identity subjektu údajů nepřiměřené množství času, úsilí či materiálních prostředků.“*

identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu". Z uvedené definice vyplývá, že jde o pojem kontextuální, který je normativně vázán na určitelnost člověka (jako subjektu osobních údajů) v kontextu způsobilosti jeho individuální (osobní) identifikace. Způsobilost informace, lhostejno v jakém kontextu, k osobní identifikaci konkrétního člověka, tak představuje základní kriteriální znak pojmu osobní údaj.

Předmětná zákonná definice osobního údaje vychází z téměř identické definice uvedené ve Směrnici, která uvádí, že „*Pro účely této směrnice se rozumí osobními údaji veškeré informace o identifikované nebo identifikovatelné osobě (dotčená osoba); identifikovatelnou osobou se rozumí osoba, která může být identifikovaná, přímo či nepřímo, zejména s odkazem na identifikační číslo nebo na jeden či více zvláštních prvků její fyzické, fyziologické,*[205] *psychické,*[206] *ekonomické,*[207] *kulturní*[208] *nebo sociální*[209] *identity*". Zákonná definice je tedy téměř shodná s definicí uvedenou ve Směrnici, nepříliš významný rozdíl spočívá pouze v tom, že český zákon v rámci demonstrativního výčtu způsobů identifikace osoby uvádí navíc některé identifikační faktory jako je číslo, kód, prvek apod.[210]

Jak vyplývá z výše uvedeného, pod pojmem osobní údaj ve smyslu § 4 písm. a) zákona je nutné chápat pouze takovou informaci, která je ve svém celkovém kontextu navázána na určitelnost člověka ve smyslu jeho způsobilosti k identifikaci. Uvedené tedy představuje svého druhu základní kriteriální a definiční znak. Předmětné ustanovení bylo od nabytí účinnosti ZoOÚ novelizováno pouze jednou, avšak poměrně výrazně, a to zákonem č. 439/2004 Sb. Tato změna spočívala v tom, že byla jednak odstraněna část definice obsahující slovní spojení kruhem („osobním údajem je jakýkoli údaj"), dále byl doplněn demonstrativní výčet informací, které obvykle vedou ke zjištění identity osoby, a byla vypuštěna část definice obsahující negativní vymezení pojmu osobní údaj. Před touto novelizací se totiž za osobní údaj nepovažovala taková informace, kterou sice bylo možné vztáhnout k určité nebo určitelné fyzické osobě, ale k identifikaci bylo zapotřebí nepřiměřeného množství času, úsilí nebo materiálních prostředků. S ohledem na rozvoj informačních technologií a jejich širokou dostupnost, kdy je zjištění identity fyzické osoby možné bez výjimečného úsilí či vynaložení nepřiměřených prostředků (myšleno zejména finančních či lidských) v naprosté většině případů, a také vzhledem k problémům při aplikaci tohoto negativního vymezení pojmu osobní údaj, byla daná část negativní definice

205 Jde např. o vzhled dané osoby, tvar jejího obličeje, hlavy i celého těla, výšku, váhu, barvu vlasů a očí atd. apod.

206 Např. informace o chování či reakcích dané osoby v určitých situacích, případně o motivaci takového chování.

207 Ekonomickou identitu fyzické osoby určují především informace o jejím majetku, pohledávkách i závazcích, o výši a zdroji jejích příjmů.

208 Např. zájmy, záliby a schopnosti jedince.

209 Např. identita člověka ve společnosti, zařazení do sociální struktury skupin, například rodinný stav, sociální původ, vzdělání, zaměstnání či jiné aktivity, z nichž lze odvodit další informace, které napomáhají k bližší identifikaci této osoby.

210 Definice uvedená ve Směrnici byla patrně přejata z mezinárodních dokumentů, konkrétně Úmluvy č. 108, kde je pojem osobního údaje vymezen tak, že se jedná o každou informaci týkající se identifikované nebo identifikovatelné fyzické osoby.

ze zákona vypuštěna.[211] Obdobný názor na snižující se náročnost možností přímé nebo nepřímé identifikace osoby vzhledem k současnému rozvoji informačních a komunikačních technologií zastává i Nejvyšší správní soud, který v jednom ze svých rozhodnutí[212] uvedl: *„Plná identita fyzické osoby v současných podmínkách technologicky vyspělé společnosti, tj. za vysokého stupně rozvoje elektronických a jiných médií, která jsou většině populace snadno dostupná, ve své podstatě neznamená nic jiného než možnost tuto osobu určitým způsobem kontaktovat, aniž by bylo nutno znát místo jejího aktuálního pobytu. Proto se výklad pojmu osobní údaj nemůže omezit striktně jen na znalost např. rodného čísla, adresy či pracoviště subjektu údajů. Z tohoto pohledu je za osobní údaj třeba považovat i číslo mobilního telefonu určité osoby, jakkoli může být takové číslo používáno příslušnou osobou jen dočasně, a zároveň nijak nespecifikuje jeho fyzickou, psychickou, ekonomickou, kulturní nebo sociální identitu (viz shora). Prostřednictvím tohoto čísla je však možno daný subjekt v určitém časovém úseku přímo kontaktovat (což se ostatně stalo i v posuzovaném případě), a tento subjekt je tak dosažitelný a jistým způsobem určitelný, a to případně i bez znalosti jeho jména a dalších údajů, které již vazbu na jeho fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu mají.*“[213]

Pojem osobní údaj je právním pojmem relativně interdisciplinárním, je používán v celé řadě právních předpisů,[214] přičemž jeho normativní obsah nemusí být vždy identický s normativním významem ve smyslu ZoOÚ. Uvedené je dáno především odlišnou působností těchto souvisejících právní předpisů, jakož i jejich účelem a konkrétními prostředky ochrany. Odpovědné posouzení obsahu tohoto pojmu ve smyslu zákonného režimu ochrany osobních údajů je nutno vycházet z konvenčních kritérií stanovených v ZoOÚ, nutno tedy zejména přihlédnout k tomu, zda se jedná o informaci týkající se konkrétního člověka (subjektu údajů).

Zbylá část definice pojmu osobní údaj odpovídá záměru evropského i českého zákonodárce uchopit pojem osobní údaj co nejšířeji, aby tato definice zahrnovala veškeré informace o určitém či určitelném jednotlivci. Nejedná se tedy pouze o identifikační údaje, tedy údaje, na jejichž základě můžeme danou osobu odlišit od osob jiných, jak je někdy nesprávně vykládáno, ale skutečně o všechny, byť zdánlivě banální či nekonkrétní skutečnosti a informace, které se týkají přímo či nepřímo určené nebo určitelné fyzické osoby. Jinými slovy pokud je osoba, která informací disponuje, schopna ji přiřadit ke konkrétnímu člověku,[215] potom se o osobní údaj jedná. Na druhé straně je však nutné dodat, že osoby, které jsou z hlediska jednoho správce na základě dat, kterými disponuje, jednoznačně identifikovatelné, jsou pro jiné správce určitelné jen za některých okolností a pro některé nebudou identifikovatelné vůbec.

Typickým příkladem, kdy dochází k přímé identifikaci člověka, je provozování internetového obchodu, kde údaje o zákazníkovi, resp. údaje o osobách, které se u konkrétní-

211 Jak ostatně uvádí samotná důvodová zpráva k zákonu č. 439/2004 Sb., kterým se mění ZoOÚ, k odstranění negativního vymezení pojmu osobní údaj bylo nutné přistoupit zejména z důvodů plné slučitelnosti zákona se Směrnicí, jakož i proto, že ze zkušeností a poznatků souvisejících s nástupem a rozvojem informačních technologií, kdy dosažení a zjištění identity subjektu údajů v dnešní době již nevyžaduje nijak výjimečné úsilí ani materiální prostředky.

212 Viz rozsudek č. j. 9 As 34/2008 ze dne 12. února 2009. Dostupný na kraken.slv.cz/9As34/2008

213 KUČEROVÁ, A., L. NOVÁKOVÁ, V. FOLDOVÁ, F. NONNEMAN, a D. POSPÍŠIL, ref. 194, s. 52.

214 Viz např. zákon o ZsPI, trestní zákoník, zákoník práce, zákon o zdravotních službách atd.

215 Na informace o právnických osobách se právní úprava ochrany osobních údajů logicky nevztahuje.

ho provozovatele jako zákazníci registrovaly, představují osobní údaje, které přímo identifikují konkrétního zákazníka (fyzickou osobu), nicméně samotné přihlašovací jméno či login (řetězec znaků vybraný zákazníkem), pod kterým tento zákazník vystupuje v diskusních fórech tohoto obchodu, již osobním údajem být nemusí.[216] Možnost přímého určení konkrétní fyzické osoby znamená jednoznačné a relativně jednoduché ztotožnění osoby na základě údajů, které daný subjekt má přímo k dispozici. Za příklad nejčastějšího použití takovéhoto způsobu spojení informací s konkrétní fyzickou osobou ve veřejné sféře slouží vyhledávací činnost Policie ČR, která disponuje řadou oprávnění zpracovávat přímé identifikátory, neboli osobní údaje umožňující přímou a jednoznačnou identifikaci fyzických osob, pro účely evidencí a rejstříků a dále disponuje přístupovými oprávněními pro ověřování a aktualizaci těchto informací. Určitelný bude pro správce také ten subjekt, kterého může přímo ztotožnit, byť ne pouze na základě informací, kterými sám disponuje. Pro jeho určení tak bude správce muset vyvinout větší úsilí než v prvním případě, bude muset např. získat či využít další osobní údaje z veřejného zdroje nebo zpracovávané jiným správcem. Za nepřímé identifikování osoby pak bude nutné považovat takový proces, který rovněž povede k určení konkrétní osoby, ale až po vynaložení většího úsilí (času, materiálních prostředků), neboť správce disponuje např. pouze jejím popisem či fotografií, ale ne identifikačními údaji. Při posuzování, zda je možné identitu fyzické osoby v konkrétním případě určit, ať už přímo nebo nepřímo, je nutné přihlížet ke všem objektivním možnostem, které konkrétní správce či další osoba, jež má k osobním údajům přístup, v daném případě reálně má. Toto interpretační pravidlo vychází z recitálu 26 Směrnice, dle kterého *„pro určení, zda je osoba identifikovatelná, je třeba přihlédnout ke všem prostředkům, které mohou být rozumně použity jak správcem, tak jakoukoli jinou osobou pro identifikaci dané osoby*". Definice osobního údaje je doplněna demonstrativním výčtem typů informací a sfér lidské osobnosti a života, jejichž projevy mohou přispět k identifikaci konkrétní osoby. Lze je však využít i jako názorný výčet příkladů informací, které mohou být osobními údaji. Před bližším rozborem této části komentovaného ustanovení je rovněž vhodné podotknout, že za osobní údaj je nutné považovat jak objektivní, pravdivé, prokázané nebo ověřené skutečnosti, tak i subjektivní a nepravdivá sdělení, pokud jsou zpracovávána v rámci stejné databáze s ostatními údaji, a ne odděleně, a dále i různá více či méně formální hodnocení a posudky. Opačný výklad, tedy že osobními údaji mohou být toliko objektivní informace, by z ochrany poskytované pravidly pro ochranu osobních údajů nedůvodně vylučoval celou řadu v praxi zcela obvyklých situací, v nichž je tato ochrana jednoznačně žádoucí (například hodnocení prováděná bankami či pojišťovnami ve vztahu k bonitě klienta, posouzení zájemce o pracovní pozici zaměstnavatelem anebo nemalá část operací prováděných s osobními údaji v rámci činnosti policie, resp. všech orgánů činných v trestním řízení).[217]

Osobním údajem tedy může být prakticky jakákoliv informace identifikující konkrétní osobu, ať již stojí relativně samostatně (např. jméno a příjmení, fotografie, daktyloskopický otisk, biometrický údaj osoby, případně jakýkoliv záznam vztahující se ke konkrétní osobě, ať již

216 Uvedené však platí pouze za předpokladu, že předmětný řetězec znaků (login) neumožňuje s přihlédnutím k celkovému kontextu z pohledu třetích stran (tj. osob odlišných od správce) identifikovat osobu zákazníka. Z pohledu provozovatele obchodu však o osobní údaje jde.

217 KUČEROVÁ, A., L. NOVÁKOVÁ, V. FOLDOVÁ, F. NONNEMAN, a D. POSPÍŠIL, ref. 194, s. 54.

jde o videozáznam, zvukový záznam, záznam chůze nebo např. dynamiky psaní na klávesnici), případně zasazena v kontextu jiných informací (např. pseudonym používaný fyzickou osobou pro komunikaci v diskusních fórech na Internetu, cookies,[218] atd.). V obecné rovině tak platí, že jakékoliv označení, byť jen ve formě náhodného řetězce znaků či číselného údaje) týkající se určeného nebo určitelného subjektu údajů, je osobním údajem ve smyslu § 4 písm. a) ZoOÚ. Jak je výše uvedeno, za osobní údaje je třeba považovat i každou jednotlivou informaci, která se vztahuje k určité či určitelné fyzické osobě, tedy nejen údaje identifikační (jako jsou její jméno, příjmení a adresa bydliště), ale také např. i pouhý údaj o věku či vzdělání navázaný na jiný konkrétní údaj (např. příjmení), ze kterého je fyzická osoba určitelná.

4.4.4 IP adresa a další číselné identifikátory jako kontextuální osobní údaje

Jedním z číselných identifikátorů, který je za určitých podmínek (tj. v rozhodném kontextu) způsobilý identifikovat člověka ve smyslu § 4 písm. a) zákona, je IP adresa,[219] rodné číslo,[220] číslo bankovního účtu, datum narození, případně jakýkoliv další identifikátor člověka[221] (např. číselné označení studenta nebo číslo přidělované zaměstnanci zaměstnavatelem). V této souvislosti je třeba připomenout, že tyto identifikátory nemusejí vést přímo k identifikaci konkrétní osoby, postačí totiž, že tuto identifikaci umožňují nepřímo, a to například na základě dalších provedených zjištění. Zatímco samotné telefonní číslo nebo ENUM záznam[222] umožňují obvykle přímo kontaktovat konkrétní osobu bezodkladně a přímo,[223] v případě IP adresy, MAC adresy a podobných identifikátorů tomu tak obvykle nebude, k identifikaci je třeba provést další kroky, na základě kterých bude osoba ztotožněna. Z pohledu druhových definičních znaků pojmu osobní údaj je nevýznamné, zda je osoba identifikovatelná přímo či nepřímo,

218 V tomto ohledu je zcela zásadní samotný kontext v podobě existujících informací, které jsou o uživateli dále sbírány a sledovány, včetně míry jejich průběžné anonymizace a zvolené formy užití (viz např. behaviorální reklama, apod.). K tomu srovnej Cookies jako osobní údaj? Neumím si představit, jak to bude v praxi fungovat. Právní rádce 12/2012, str. 68

219 IP adresa slouží k rozlišení síťových rozhraní připojených k počítačové síti. Síťovým rozhraním může být síťová karta (Ethernet, Wi-Fi), IrDA port, ale může se jednat i o virtuální zařízení (loopback, rozhraní pro virtuální počítač a podobně). Zkratka IP znamená Internet Protocol, což je protokol, pomocí kterého spolu komunikují všechna zařízení v Internetu. Dnes je nejčastěji používaná jeho čtvrtá verze (IPv4), průběžně se však přechází na novější verzi 6 (IPv6). V jiných protokolech se adresování jednotlivých zařízení může provádět jinak (viz např. MAC adresa). Více viz http://cs.wikipedia.org/wiki/IP_adresa

220 Nakládání s rodnými čísly je předmětem samostatné úpravy v zákoně o evidenci obyvatel, byť konvenční znaky osobního údaje splňuje.

221 Např. zdrojový identifikátor fyzické osoby i agendové identifikátory fyzické osoby ve smyslu zákona o základních registrech, neboť i tyto číselné identifikátory se budou vztahovat k jediné a jedinečné fyzické osobě.

222 Tato technologie umožnuje zveřejnit k telefonnímu číslu informaci, jak se na něj lze dovolat přes internet. K tomu více viz http://enum.nic.cz/page/270/co-je-enum/

223 Byť i v těchto případech lze jistě vysledovat dílčí rozdíl mezi jistotou kontaktovat osobu na základě (osobního) mobilního telefonního čísla a domácí pevné linky, případně telefonního čísla na pracoviště konkrétní osoby apod.

nicméně z pohledu posouzení míry intenzity zásahu a možných následků do soukromí člověka může být tato skutečnost velmi významná.

U samostatně stojících číselných identifikátorů může být schopnost identifikace člověka výrazně oslabena, případně nemusí být vůbec dána, a to zejména na základě skutečnosti, že identifikátor sám o sobě nemusí vést k identifikaci konkrétní osoby, ale např. počítače (např. IP adresa identifikující webový nebo aplikační server), případně osobu sice identifikuje, nicméně půjde o osobu právnickou (např. číslo bankovního účtu identifikující obchodní společnost). V takových případech zde není dána zákonem požadovaná vazba na člověka (jako na subjekt osobních údajů), nejedná se o osobní údaj ve smyslu § 4 písm. a) zákona a takový identifikátor je ze zákonné ochrany zcela vyloučen. Takto lze nahlížet v zásadě na všechny číselné identifikátory, případně i na některé další údaje, jejichž identifikační způsobilost je omezena (viz např. fotografie či portrét neexistujícího člověka, který byl fiktivně vytvořen).

U těchto identifikátorů je pak zcela zásadní jejich celkový kontext, který ačkoliv sám o sobě nesplňuje konvenční kritéria, který klade zákon na osobní údaje, představují významný prvek (informaci) umožňující identifikaci člověka jako subjektu osobních údajů. Uvedené je typické právě např. u IP adresy, která, jak známo, jednoznačně identifikuje síťové rozhraní v počítačové síti, nikoliv přímo konkrétní osobu. V tomto ohledu lze hovořit o tom, že IP adresa sama o sobě představuje neperfektní identifikátor směřující pouze k místu připojení, případně k síti více počítačů či jednomu konkrétnímu počítači. Samotná IP adresa tak z principu neslouží k identifikaci konkrétní osoby, ale směřuje toliko k místu, kde je realizována nějaká činnost, přičemž není samo o sobě známo, zda jde o činnost strojovou (tj. počítače) nebo činnost konkrétní osoby. Nemusí být totiž na první pohled zjevné, zda vůbec u počítače nějaká osoba seděla, a pokud ano, tak IP adresa není způsobilá tuto osobu identifikovat – v daném okamžiku mohla u počítače sedět jakákoliv osoba, přičemž IP adresa může směřovat např. k pouhému neurčitelnému okruhu těchto osob, nikoliv tedy ke konkrétní osobě. Uvedené je však problém prokazatelnosti (významné např. pro trestní řízení), nikoliv skutečnosti, že IP adresa identifikuje konkrétní prostředek používaný konkrétní fyzickou osobou.

Uvedené lze demonstrovat i na činnosti Policie ČR, která při dokazování trestného činu spáchaného z prostředí Internetu potřebuje disponovat prokazatelnou a spolehlivě zjištěnou vazbou (vztahem) konkrétní IP adresy ke konkrétní osobě. Jakkoliv lze konstatovat, že zajišťování a provádění takového důkazu může být obtížné,[224] nemůže to být samo o sobě důvodem pro vyloučení identifikátoru v podobě IP adresy z ochrany, kterou zákon poskytuje osobním údajům. Jakkoliv může jít o náročnou expertní činnost, lze takový důkaz úspěšně provést, a to právě na základě samotného kontextu v podobě dalších záznamů síťového provozu, případně na základě dalších důkazů, ze kterých vyplývá, že konkrétní fyzická osoba v předmětném čase pracovala s počítačem majícím tuto IP adresu. Ke zmíněné IP adrese a otázce toho, zda se i v jejím případě může jednat o osobní údaj, se vyjádřil i Nejvyšší správní

224 Zpráva o workshopu konaném dne 26. ledna 2011 na Právnické fakultě Masarykovy univerzity s názvem Dokazování elektronickými prostředky, pořádaný v rámci projektu OPVK Právo a technologie. K tomu více viz KINCL, Libor. IP adresa identifikuje místo připojení, nikoli osobu. *Revue pro právo a technologie*. 2011, roč. 2, č. 3. Brno: Masarykova univerzita, s. 5. Dostupné také z: www.law.muni.cz/dokumenty/12793

soud, který v jednom ze svých rozsudků[225] i s odvoláním na SDEU mj. uvedl: „Při posuzování povahy IP adresy je možno podpůrně odkázat rovněž na judikaturu SDEU. Ten ve svém rozhodnutí ze dne 29. 1. 2008, sp. zn. C-275/06, Productores de Música de España (Promusicae) vs. Telefónica de España SAU (rozhodnutí je dostupné z http://curia.europa.eu), považoval IP adresu v kontextu daného případu (Promusicae požadovala po Telefonice odhalení identit osob, kterým poskytovala připojení k Internetu a u nichž byla známá jejich IP adresa a datum a čas připojení) za osobní údaj ve smyslu předpisů na ochranu osobních údajů. Pro účely nyní posuzované věci lze z uvedeného závěru vyvodit, že jestliže může IP adresa za určitých okolností představovat osobní údaj, tedy údaj, na jehož základě lze identifikovat (přímo či nepřímo) nějakou konkrétní osobu, pak může sloužit také jako důkaz v přestupkovém řízení, byť jako důkaz nepřímého charakteru."[226]

K charakteru IP adresy se vyjádřila také Pracovní skupina 29, která mj. uvedla, že zejména v případech, kdy se zpracování IP adres provádí za účelem identifikace uživatelů počítače (například ze strany majitelů autorských práv, kteří chtějí stíhat uživatele počítačů za porušování práv duševního vlastnictví), správce údajů předjímá, že prostředky, které mohou být rozumně použity k identifikaci těchto osob, budou k dispozici např. prostřednictvím soudů, na něž se obrátí (jinak by sběr informací neměl smysl), a tyto informace by se proto měly považovat za osobní údaje. V tomto ohledu je třeba zohlednit také článek 26 Směrnice, který stanoví, že je nutné přihlédnout ke všem prostředkům, které mohou být rozumně použity jak správcem, tak jakoukoli jinou osobou pro identifikaci dané osoby. Požadavek rozumnosti (ve vztahu k prostředkům) je zapotřebí posuzovat a především důkladně vážit jak ve smyslu přiměřenosti očekávání ochrany soukromí člověka (viz výše), tak i ve vztahu ke konkrétnímu účelu zpracování. Uvedený důraz na rozumnost je třeba akcentovat zejména z toho důvodu, že česká právní úprava s tímto pojmem bohužel nepracuje, což je vzhledem k legální definici pojmu osobní údaj problematické. V tomto ohledu lze však problém, tam kde je to nezbytné, řešit za pomoci euro-konformního výkladu.

Internetové zdroje a poskytovatelé jejich obsahu totiž obvykle s IP adresou konkrétního uživatele (tj. jeho veřejnou IP adresou) dále pracují, zpracovávají ji, nezřídka ji pak zveřejňují, a to např. v rámci diskusního příspěvku umístěného na diskusní fórum či web uživatelem, případně na stránku s jeho vlastním osobním profilem.[227] V tomto ohledu zanechává takovýto uživatel za sebou jakousi elektronickou stopu, která však již zdaleka nestojí samostatně, nýbrž je ve svém souhrnu doplněna o celou řadu dalších osobních údajů, nezřídka pak obsahuje pravé jméno (případně pseudonym či nick) a funkční e-mail, vlastní (autorský) text a v některých případech i fotografii. Záznamy o takové konkrétní veřejné IP adrese vztahující se ke konkrét-

225 Sp. zn. 1 As 90/2008 – 189, ze dne 4. února 2009.

226 KUČEROVÁ, A., L. NOVÁKOVÁ, V. FOLDOVÁ, F. NONNEMAN, a D. POSPÍŠIL, ref. 194, s. 54.

227 Pro úplnost je třeba dodat, že v některých případech může být zveřejněna pouze část IP adresy (např. bez uvedení prvního či posledního trojčíslí apod.), případně neúplné značení domény (viz např. zveřejňování IP adresy u diskusních příspěvků na www.lupa.cz/). Takovýto postup lze doporučit zejména tam, kde má zveřejnění IP adresy plnit zcela jiný účel než identifikaci konkrétní osoby (např. identifikace příspěvků zdánlivě pocházejících z různých účtů, jež ve skutečnosti patří k jedné osobě apod.).

nímu uživateli pak ve svém celkovém kontextu způsobují, že takováto osoba je poměrně snadno určitelná, a to nikoliv na základě použití nákladných prostředků, ale na základě několika velmi jednoduchých dotazů a práce s internetovými vyhledávači. Právě stále se zlepšující možnosti internetových vyhledávačů umožňují pracovat s podobnými záznamy velmi snadno a vysoce efektivně. V tomto ohledu tak ve svém důsledku umožňují vytvořit osobnostní profil konkrétní osoby, jež byla na počátku nejistě identifikovatelná pouze jakousi IP adresou, přičemž výsledkem několikasekundové operace může být nalezení skutečného jména a příjmení, e-mailu, fotografie a dílčích projevů osoby v prostředí Internetu za posledních několik let (včetně např. informace o stažených či sdílených aplikacích, chování v prostředí Internetu atd.). Moderní vyhledávače jsou navíc schopné pracovat v tomto kontextu vysoce efektivně, a to byť i jen na základě zdánlivě nevýznamného fragmentu takovéto informace (např. části fotografie jakési osoby na ulici),[228] kterou lze díky těmto prostředkům následně ztotožnit s řadou dalších fotografií a záznamů vztahujících se k této osobě, přičemž stále půjde o rozumné použití prostředků ve výše uvedeném smyslu.

Zvláštním případem by pak nepochybně byl druh IP adres, které za určitých okolností z různých technických a organizačních důvodů skutečně neumožňují identifikaci uživatele. Příkladem mohou být IP adresy přidělované počítači v internetové kavárně, kde se nevyžaduje prokázání totožnosti zákazníků. Zde by se dalo tvrdit, že údaje o používání konkrétního počítače shromážděné za určité časové období neumožňují identifikaci uživatele, a tedy nejsou osobními údaji. Je ovšem třeba poznamenat, že poskytovatelé internetových služeb s největší pravděpodobností nebudou vědět, zda daná IP adresa umožňuje nebo neumožňuje identifikaci, a že údaje spojené s touto adresou budou zpracovávat stejným způsobem jako informace spojené s IP adresami řádně zaregistrovaných uživatelů, kteří jsou identifikovatelní. Pokud tedy poskytovatel internetových služeb není schopen s naprostou jistotou odlišit údaje odpovídající uživatelům, kteří nemohou být identifikováni, bude muset nakládat se všemi informacemi o IP adresách jako s osobními údaji.

Podřazení specifickému režimu nakládání ve smyslu dalšího zpracovávání a uchovávání konkrétních IP adres ze strany poskytovatelů o fyzických osobách lze považovat za zcela zásadní požadavek platné právní úpravy. Je nutné reflektovat zejména skutečnost, že takovéto nakládání s IP adresami ve specifickém kontextu, např. vyhledávaných výrazů na Internetu z konkrétní IP adresy v časových souvislostech, má svůj ekonomický i psychologický aspekt, který je zcela reálně způsobilý zasáhnout do soukromí člověka, a to poměrně s vysokou mírou intenzity. V tomto ohledu si lze připomenout ne až tak vzdálený případ, kdy na základě chybného postupu společnosti AOL došlo ke zveřejnění údajů o cca statisících internetových operací svých uživatelů, a to včetně kontextu informací o konkrétních vyhledávaných slovech a frázích. V tomto případě došlo ke zveřejnění zdánlivě anonymních údajů (AOL ve zveřejněných datech nepoužívala uživatelská či reálná jména svých zákazníků, ale pouze specifické zákaznické číslo), nicméně je evidentní, že z pohledu společnosti AOL byly tyto údaje způsobilé přímo iden-

228 K tomu opačně OTEVŘEL, Richard. Soumrak užitečného internetu. (Díl. I) [online]. *JINÉ PRÁVO*. (vid. 18. 10. 2010). Dostupné z: http://jinepravo.blogspot.cz/2010/10/soumrak-uzitecneho-internetu-dil-i.html

tifikovat konkrétního zákazníka – fyzickou osobu. Na základě triviální analýzy bylo z takto zveřejněných dat možné dohledat vysoce citlivé informace a údaje vztahující se ke konkrétním osobám.[229] Některá média (např. New York Times) tak odhalila jméno a příjmení řady konkrétních osob, a to zcela bez součinnosti se společností AOL.[230]

Lze tedy třeba dospět k závěru, že se zpracovávání IP adres musí podřadit pod zvláštní zákonný režim systému ochrany, a to zcela bez ohledu na omezenou schopnost výkonu teritoriální působnosti českého i evropského systému ochrany dat, případně komplikovaného určení, zda jde či nejde o osobní údaj v konkrétním případě. Opačný přístup by vedl ke vzniku celé řady dílčích rizik a nevyváženosti ochrany soukromí ve formě veřejnoprávních nástrojů ochrany osobních údajů, včetně zcela zásadní a v tomto kontextu často opomíjené problematiky dataminingu,[231] představující analytickou metodologii získávání netriviálních skrytých a potenciálně užitečných soukromých informací z dostupných dat.

4.4.5 MAC adresa, IMEI a IMSI jako kontextuální osobní údaje

Jak ostatně vyplývá z výše uvedeného, za osobní údaj je nutné považovat v zásadě jakoukoliv informaci týkající se určené nebo určitelné fyzické osoby, k níž se osobní údaje vztahují. Osobním údajem tak může být informace zdánlivě zcela nevýznamná (např. přezdívka nebo váha osoby), případně jakákoliv jiná informace, která se k fyzické osobě na první pohled přímo nevztahuje, nicméně s přihlédnutím ke všem souvislostem týkajících se určitelnosti osoby lze dokázat, že je spojena s konkrétní fyzickou osobou. Nemusí být tedy nutně splněna podmínka, že na základě či prostřednictvím této informace lze osobu identifikovat, postačí totiž, že je osoba identifikovatelná prostřednictvím jiné informace (kontextu), kde tyto informace ve svém souhrnu tvoří osobní údaje o konkrétní fyzické osobě.

Typickým příkladem číselného identifikátoru, který ačkoliv sám o sobě nemusí splňovat pojmové znaky osobního údaje, nicméně podobně jako (veřejná) IP adresa (viz výše) slouží jako relativně[232] jedinečný identifikátor síťového zařízení počítače, je MAC adresa.[233] MAC ad-

229 Např. uživatel skrývající se pod svým konkrétním zákaznickým číslem vyhledával nejprve slova o *„jsi těhotná a dítě nechceš“*, poté *„jak se stravovat v těhotenství“*, a následně *„potratové kliniky v NYC“*, později pokračoval vyhledáváním slov *„může křesťan získat odpuštění za potrat“*. Podobně jiný uživatel vyhledával slova *„jak zabít vlastní ženu“* atd. apod.

230 Viz WIEHL, L. Be Careful What You Search For. *New York Times.* January 16, 2008

231 Data mining se používá v komerční sféře (například v marketingu při rozhodování, které klienty oslovit dopisem s nabídkou produktu), ve vědeckém výzkumu (například při analýze genetické informace) i v jiných oblastech (například při monitorování aktivit na internetu s cílem odhalit činnost potenciálních škůdců a teroristů).

232 Moderní síťová zařízení mají možnost MAC adresu změnit, a tak není zcela zaručena jednoznačná identifikace zařízení v lokální počítačové síti LAN.

233 MAC adresa (z anglického „Media Access Control“) je jedinečný identifikátor síťového zařízení, který používají různé protokoly druhé (spojové) vrstvy OSI. Ethernetová MAC adresa se skládá ze 48 bitů a podle standardu by se měla zapisovat jako tři skupiny čtyř hexadecimálních čísel (např. 0123.4567.89ab), mnohem častěji se ale píše jako šestice dvojciferných hexadecimálních čísel oddělených pomlčkami nebo dvojtečkami. K tomu více viz http://cs.wikipedia.org/wiki/MAC_adresa

resa totiž může představovat další identifikátor fyzické osoby, je totiž přiřazována síťové kartě každého počítače (včetně mobilního telefonu), čímž reprezentuje číselný identifikátor, který je relativně neměnný a který navíc může mimo jiné ve svém důsledku (kontextu) vést k lokalizaci pohybu konkrétní osoby. MAC adresa je totiž přiřazována síťově kartě již při výrobě tohoto síťového zařízení, proto představuje poměrně neměnný prvek síťové komunikace. Z tohoto důvodu se mnohdy namísto MAC adresy používá pojem fyzická adresa.

Způsobilost MAC adresy identifikovat konkrétní osobu je však ve srovnání s (veřejnou) IP adresou omezena. Zatímco veřejná IP adresa identifikuje konkrétní počítač (router) v rámci celého Internetu, MAC adresa se bude měnit podle toho, za jakým routerem se nachází cílový počítač. Rozdíl spočívá mimo jiné v tom, že veřejná IP adresa může „cestovat" s osobou, čímž identifikuje počítač (router), zatímco MAC adresa „cestuje" pouze k nejbližšímu síťovému zařízení na druhé straně (např. router u poskytovatele připojení k Internetu). IP adresa tedy identifikuje chování uživatele „po celou dobu", MAC adresa je určena k identifikaci počítačů pouze v jednom segmentu sítě (např. ve vztahu router–router atd.). K zalogování MAC adresy na cílovém serveru tedy nedochází, logována je pouze v rámci původní lokální sítě, informace o MAC adrese tak dále neputuje. Ve vztahu k omezené identifikaci MAC adresy je však třeba konstatovat, že v případě použití internetového protokolu verze 6 (IPv6[234]) namísto verze 4 (IPv4) se tyto adresy skládají ze dvou logických částí, tj. 64bitového (pod)síťového prefixu a 64bitové části hosta, buď automaticky vytvářené na základě MAC adresy, případně přiřazené následně. V tomto ohledu je v případech použití IPv6 zesílena způsobilost identifikace konkrétní fyzické osoby. S ohledem na dosavadní zvyklosti byl vyvinut nový standard (RFC 3041),[235] a to s cílem snížit šanci trvalého svázání identity uživatele a IPv6 adresy, což obnovuje některé z možností anonymity existující u IPv4.

Podobně jako na MAC adresu lze nahlížet také na identifikátor IMEI mobilního telefonu,[236] který představuje druhově velmi podobné a rovněž unikátní číslo přidělené výrobcem mobilnímu telefonu. Podobná bude rovněž kvalifikace v případě identifikátoru IMSI,[237] který představuje jedinečné identifikační číslo SIM karty mobilního telefonu přidělené mobilním operátorem pro SIM kartu v mobilní síti (GSM, UMTS, CDMA atd.). Oba tyto identifikátory (IMEI, IMSI) jsou v průběhu komunikace odesílány mobilnímu operátoru a v interních systé-

234 K tomu více viz např. www.ripe.net/lir-services/resource-management/faq/faq-ipv6 případně www.ipv6.cz/Přechod_od_IPv4_k_IPv6 .

235 K tomu více viz dokument Privacy Extensions for Stateless Address Autoconfiguration in IPv6, dostupný z: http://tools.ietf.org/html/rfc3041

236 IMEI je zkratka z anglického termínu International Mobile Equipment Identity, jež představuje patnáctimístné číslo, které lze zapsat ve formátu ZZnnnn-MM-nnnnnn-X. První skupina je tzv. type approval code (TAC) uvozený dvěma číslicemi kódu země (ZZ). Druhá skupina (MM) je kód výrobce (viz níže), třetí skupina je sériové číslo telefonu. Poslední cifra (X) je využívána pro kontrolní součet (Luhn algorithm / modulo 10). K tomu více viz http://en.wikipedia.org/wiki/International_Mobile_Station_Equipment_Identity

237 IMSI je zkratka z anglického termínu International Mobile Subscriber Identity (někdy také mylně International Mobile Station Identity). K tomu více http://en.wikipedia.org/wiki/International_Mobile_ Subscriber_ Identity

mech operátora obvykle slouží k dohledání detailů o konkrétním uživateli.[238] Podobně jako je tomu u předchozích číselných identifikátorů, i tyto lze za určitých podmínek změnit.

Na rozdíl od výše uvedených číselných identifikátorů (IP adresa, MAC adresa, IMEI, IMSI atd.), které lze samy o sobě (tj. bez kontextu) považovat za identifikačně neperfektní, nepanují ohledně identifikátoru datové schránky, je-li jím fyzická osoba, jakékoliv pochybnosti. Identifikátor datové schránky slouží ve smyslu ustanovení § 21 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, v platném znění, k identifikaci datové schránky. Podobně jako ostatní identifikátory je i tento zcela unikátní, není tedy zaměnitelný s žádným jiným identifikátorem využívaným orgány veřejné moci.[239] Ověření skutečnosti, zda jde o identifikátor člověka, případně jiné osoby (obchodní společnosti, orgánu veřejné moci atd.) je poměrně snadné. Zákon[240] totiž stanoví povinnost Ministerstva vnitra ČR vést specifický seznam fyzických osob, podnikajících fyzických osob, právnických osob a orgánů veřejné moci, které mají zřízenu a zpřístupněnu datovou schránku.

4.4.6 Zásada informovaného souhlasu v prostředí Internetu, zvláštní režim a zákonné licence

Klíčovou zásadou každého zpracovávání[241] osobních údajů, včetně jejich zveřejnění, je zásada informovaného souhlasu. Zpracovávány tak mohou být pouze takové osobní údaje, s jejichž zpracováváním vyslovil subjekt údajů svůj souhlas.[242] Bez tohoto souhlasu mohou být tyto údaje zpracovávány pouze v případě, byla-li naplněna některá ze sedmi výjimek uvedených v ustanovení § 5 odst. 2 písm. a) až g) zákona, tedy:

238 Kvůli zvýšení bezpečnosti a možnostem odposlechu na úrovni rádiových vln je IMSI zasíláno co nejméně a často je nahrazeno náhodně generovaným TMSI. IMSI není volatelné číslo.

239 Ve smyslu ustanovení § 21 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, v platném znění, stanoví způsob tvorby identifikátoru Ministerstvo vnitra ČR vyhláškou.

240 Seznam držitelů datových schránek je ve smyslu zákonného zmocnění uvedeného v § 14b zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů ve znění pozdějších předpisů a je součástí informačního systému datových schránek. Zahrnuje v sobě funkčnost původního Seznamu orgánů veřejné moci, který byl zřízen a provozován na základě ustanovení § 14b zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění platném do 28. 11. 2011. V seznamu držitelů datových schránek lze vedle orgánů veřejné moci, právnických osob nalézt rovněž fyzické osoby, podnikající fyzické osoby, soudní exekutory, notáře, advokáty, insolvenční správce či daňové poradce, které mají zřízenou a zpřístupněnou datovou schránku. Vyhledávat lze prostřednictvím http://seznam.gov.cz/ovm/welcome.do

241 Zpracováním osobních údajů se rozumí jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace (§ 4 písm. e) zákona).

242 Tento souhlas musí být svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů. K tomu více viz např. NONNEMANN, F. Náležitosti souhlasu se zpracováním osobních údajů. *Právní rozhledy.* 2011, č. 9.

a) jestliže provádí zpracování nezbytné pro dodržení právní povinnosti správce,[243]
b) jestliže je zpracování nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro jednání o uzavření nebo změně smlouvy uskutečněné na návrh subjektu údajů,
c) pokud je to nezbytně třeba k ochraně životně důležitých zájmů subjektu údajů. V tomto případě je třeba bez zbytečného odkladu získat jeho souhlas. Pokud souhlas není dán, musí správce ukončit zpracování a údaje zlikvidovat,
d) jedná-li se o oprávněně zveřejněné osobní údaje v souladu se zvláštním právním předpisem.[244] *Tím však není dotčeno právo na ochranu soukromého a osobního života subjektu údajů,*
e) pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby; takové zpracování osobních údajů však nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života,
f) pokud poskytuje osobní údaje o veřejně činné osobě, funkcionáři či zaměstnanci veřejné správy, které vypovídají o jeho veřejné anebo úřední činnosti, o jeho funkčním nebo pracovním zařazení, nebo,
g) jedná-li se o zpracování výlučně pro účely archivnictví podle zvláštního zákona.

Výše uvedené výjimky představují zákonné licence[245] správce umožňující zpracovávat osobní údaje bez souhlasu subjektů těchto osobních údajů. Jde tak o zásadní výjimku z režimu ochrany stanovené ve formě základních práv a povinností správce osobních údajů. Základním právním titulem pro zpracovávání však stále zůstává především (informovaný) souhlas subjektu údajů, který má být aplikován přednostně, přičemž zákonné licence pro správce by měly být použity až sekundárně, tj. poté, kdy právo jednotlivce na ochranu soukromí je převáženo jiným legitimním právním či veřejným zájmem (viz důvody výše). V tomto ohledu je nezbytné zvážit, zda namísto doslovné aplikace těchto výjimek, nelze primárně postupovat cestou obstarání si souhlasu a zpracovávání osobních údajů na tomto základě, čemuž je právní úprava zcela jistě nakloněna. Zákonné licence zpracovávání osobních údajů ze strany správce je tak nutné považovat za svého druhu výjimky, které lze aplikovat pouze ve zvláštních skutkových případech stanovených v tomto zákoně (§ 5 odst. 2) a zásadně také pouze tehdy, pokud je dán objektivně existujícím legitimním právním či veřejným zájmem, přičemž je třeba dbát na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů.

Z pohledu specifického prostředí Internetu lze za aplikovatelnou licenci považovat zejména ustanovení § 5 odst. 2 písm. a),[246] které umožňuje nahradit souhlas subjektů osobních údajů v případě, že jde o zpracování nezbytné pro dodržení právní povinnosti správce. Zákono-

243 Například zákon č. 111/1998 Sb., o vysokých školách, v platném znění; zákon č. 564/1990 Sb., o státní správě a samosprávě ve školství, v platném znění; zákon č. 153/1994 Sb., o zpravodajských službách České republiky, v platném znění; zákon č. 154/2000 Sb., o šlechtění, plemenitbě a evidenci hospodářských zvířat, v platném znění; zákon č. 166/1999 Sb., o veterinární péči, v platném znění; zákon č. 246/1992 Sb., na ochranu zvířat proti týrání, v platném znění; zákon č. 147/1996 Sb., o rostlinolékařské péči, v platném znění, a zákon č. 219/2003 Sb., o uvádění do oběhu osiva a sadby pěstovaných rostlin, v platném znění.

244 Zákon č. 81/1966 Sb., o periodickém tisku, ve znění pozdějších předpisů.

245 Z latinského licet (dovolení).

246 Jde patrně o nejčastěji užívanou zákonnou licenci pro zpracovávání osobních údajů bez souhlasu jejich nositele, zejména v oblasti veřejné správy.

dárce zde měl na mysli především takovou povinnost, která byla založena na základě zvláštního předpisu ve vztahu k nakládání s osobními údaji, zejména pak s jejich sběrem, případně jakékoliv další operací s těmito údaji včetně jejich shromažďování, třídění, ukládání, využívání až po jejich archivaci, skartaci nebo likvidaci informace či jejího nosiče. Typickou právní povinností ve smyslu § 5 odst. 2 písm. a) zákona představuje povinnost vyplývající z ustanovení § 3 odst. 1 zákona č 133/2000 Sb., o evidenci obyvatel a rodných číslech, v platném znění, které stanoví povinnost Ministerstva vnitra ČR spravovat informační systém evidence obyvatel jako agendového informačního systému veřejné správy ve smyslu ZoISVS.[247] V rámci této zákonné licence pro zpracování osobních údajů je realizována zejména právní úprava podmínek pro výměnu informací v rámci integrace základních registrů podle ZoZR.

Dalším příkladem právní povinnosti ve smyslu ustanovení § 5 odst. 2 písm. a) zákona je povinnost zaměstnavatele vést evidenci pracovní doby. Jde o povinnost rámcovou, zákon neobsahuje konkrétní způsob vedení této evidence. Takže je nutné vycházet z toho, že způsob musí být legitimní neboli musí odpovídat účelu vedení evidence pracovní doby. Proto by z ní mělo být patrné, kolik hodin za den, za týden, za měsíc, za vyrovnávací období zaměstnanec odpracoval, kolik z toho připadlo na práci přesčas, případně noční práci, a kolik z této množiny činí hodiny pracovní pohotovosti, která součástí pracovní doby není. Současně musí být samozřejmě dodržena i ostatní pravidla, která ZoOÚ stanoví (zejména týkající se rozsahu shromažďovaných údajů a způsobů jejich následného využití). Aby zaměstnavatelé ze svého pohledu vyhověli požadavkům zákoníku práce týkajícím se průkaznosti používané evidence pracovní doby, volí často metody, které jsou sice velmi průkazné, ale jejich informační schopnost vypovídá i o dalších skutečnostech, které již s evidencí pracovní doby nesouvisejí nebo souvisejí jen velmi okrajově. Jde zejména o nejrůznější docházkové systémy, které prostřednictvím zabezpečení na vstupech do budovy zaznamenávají v kombinaci s dalšími sledovacími systémy každý pohyb zaměstnance v prostorách jeho zaměstnavatele, například přímými záběry kamer; zaměstnanec, respektive jeho chování je však sledováno také nepřímo, a to zejména pomocí vnitřních objektových zabezpečovacích systémů. Dalším trendem je nasazování sledovacího softwaru do informačních systémů, kam se zaměstnanci každodenně připojují, a v neposlední řadě jde i o užívání technologie GPS pro sledování vozidel nebo samotných zaměstnanců. Ve všech uvedených případech je nezbytné pečlivě hodnotit zejména vyváženost použitých technických prostředků a míru zásahu do soukromí zaměstnanců. V této souvislosti však lze odkázat na Rozsudek Evropského soudu pro lidská práva ve věci Niemietz,[248] podle něhož je nutné pod pojmem právo na soukromí rozumět nejen osobní soukromí člověka, ale i právo každého člověka na vytváření a rozvíjení vztahu s dalšími lidskými bytostmi, a to i na pracovišti. Každý zaměstnavatel proto musí nejprve důsledně analyzovat, zda má pro takovéto zpracování osobních údajů zákonnou licenci neboli zda plní právem uloženou nebo očekávanou povinnost, nebo zda se jedná jen o jeho vlastní záměr. Zatímco v prvém případě může využít právní titul pro

247 Zákon č. 365/2000 Sb., o informačních systémech veřejné správy, v platném znění.

248 Rozsudek ESLP ze dne 16. 12. 1992, ve věci *Niemietz v. Spolková republika Německo* (stížnost č. 13710/88).

zpracování osobních údajů upravený v tomto ustanovení zákona, v případě druhém tak může činit jen za předpokladu existence jiného právního titulu.[249]

V některých případech je formulace právní povinnosti ve smyslu § 5 odst. 2 písm. a) zákona nejednoznačná,[250] případně sice může být jasně stanovena, ale v praxi může být překročen její rozsah[251] (ve vztahu ke sledovanému účelu). V těchto případech může být sporné, do jaké míry lze související zákonnou licenci aplikovat. V takovém případě je třeba přihlédnout ke konkrétní odpovědnosti správce, k významu zákonné povinnosti ve vztahu k účelu, který předmětná povinnost sleduje, a to v poměru k míře případného zásahu do soukromí a osobního života člověka.

Dalším příkladem, kdy lze navzdory absenci souhlasu využít zákonnou licenci, je takové zpracování osobních údajů, které je nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro jednání o uzavření nebo změně smlouvy uskutečněné na návrh subjektu údajů ve smyslu § 5 odst. 2 písm. b) zákona. Tato zákonná licence se normativně opírá o existenci smluvního vztahu mezi správcem a subjektem údajů, případně o existenci jednání o podobě tohoto vztahu. Jde tak o situaci, ve které dochází ke sjednávání nové smlouvy, k plnění smlouvy již uzavřené nebo ke změně uzavřené smlouvy (včetně jejího zániku). Ve všech těchto případech je pro aplikaci § 5 odst. 2, písm. b) zákona nezbytné, aby smluvní stranou nebo stranou, která iniciuje takové jednání, byl sám subjekt údajů. Tato zákonná licence tak postihuje ty případy, kdy ačkoliv není dán výslovný souhlas subjektu osobních údajů s jejich zpracováváním, je takové zpracování nezbytné pro plnění předmětu smlouvy, jejímž je subjekt osobních údajů smluvní stranou. V řadě případů by sice bylo možné dovodit souhlas subjektu osobních údajů s takovým zpracováním konkludentně (např. z povahy plnění stran, předmětu smlouvy apod.), nicméně v případech, kdy by se zpracovávání opíralo pouze o konkludentně dovozený souhlas (např. na základě zvláštní smlouvy), bylo by nutné počítat s tím, že může být souhlas stejně tak odvolán, jako byl udělen – uvedené by pak mohlo mít zásadní vliv na možnost plnění jedné či druhé strany, včetně výkonu práva od smlouvy odstoupit nebo smlouvu vypovědět.

249 KUČEROVÁ, A., L. NOVÁKOVÁ, V. FOLDOVÁ, F. NONNEMAN, a D. POSPÍŠIL., ref. 194, s. 152.

250 Tak je tomu např. v ustanovení § 62 zákona č. 273/2008 Sb., o Policii ČR, v platném znění, jež stanoví, že: „*Policie může, je-li to nezbytné pro plnění jejích úkolů, pořizovat zvukové, obrazové nebo jiné záznamy osob a věcí nacházejících se na místech veřejně přístupných a zvukové, obrazové nebo jiné záznamy o průběhu úkonu.*" V tomto ohledu tak není zřejmý ani rozsah či způsob výkonu této licence ve vztahu k provozování kamerových systémů Policií ČR. Je však nutné dovodit, že musí jít o plnění nezbytné právní povinnosti, což bezbřehou aplikaci této licence omezuje.

251 Výroční zpráva Úřadu za rok 2004 v tomto ohledu zmiňuje případ banky, která nutila své zaměstnance dodávat zaměstnavateli kontakty a podrobnější informace o svých příbuzných a známých, kteří pak byli interně vyhodnocováni a kontaktováni obchodníky s nabídkou produktů této banky. Minimální rozsah shromážděných osobních údajů u jednotlivých subjektů údajů zahrnoval příjmení a telefonní číslo, u jiných kontaktů byly ovšem vedeny osobní údaje zahrnující všechny bankou požadované položky, tedy především jméno, příjmení, lokalitu, odhadovaný věk, telefon, a v některých případech i další nepovinné položky, jako například titul, firmu, počet dětí, případně i údaje o tom, kde má dotyčný účet nebo zda má hypotéku. Kontrola provedená Úřadem odhalila, že ve svých interních pokynech banka zcela ignorovala zákonnou povinnost vyžádání souhlasu. Na základě těchto zjištění bylo vydáno rozhodnutí, jímž byla této bance za porušení povinností stanovených v § 5 odst. 2 a 5, § 11 odst. 1, 2 a 3 zákona, tedy za správní delikt podle § 46 odst. 1 citovaného zákona, uložena pokuta ve výši 485 000 Kč.

Ve vztahu k zajištění fáze sjednávání smlouvy je nutné postupovat ve smyslu ustanovení § 43 ObčZ, které stanoví, že účastníci jsou povinni dbát, aby při úpravě smluvních vztahů bylo odstraněno vše, co by mohlo vést ke vzniku rozporů. Tento normativ je zcela zásadní pro posuzování rozsahu nezbytných osobních údajů, které správce zpracovává v souvislosti s plněním smlouvy, uzavřené se subjektem údajů v mezích právního titulu obsaženého v komentovaném § 5 odst. 2 písm. b) zákona. Jde zejména o identifikační údaje smluvních stran, popis předmětu plnění a rozsah závazků s plněním souvisejících, ale také platné podpisové smluvní doložky nebo vzory smluvních stran. Pokud jde o základní identifikátory subjektu údajů nezbytné pro uzavření smlouvy, lze je rozdělit do tří skupin: jmenné (jméno, příjmení, titul), adresní (adresa bydliště; případně místa podnikání, sídla firmy) a číselné (datum narození nebo rodné číslo). Zejména ve vztahu k rodnému číslu je třeba odkázat na zvláštní právní úpravu podmínek pro nakládání s tímto údajem, obsaženou v zákoně o evidenci obyvatelstva.[252] Tento zákon chápe rodné číslo (srov. § 13 odst. 1 a 9 zákona o evidenci obyvatel) jako identifikátor fyzické osoby, se kterým je oprávněna nakládat (užívat nebo rozhodovat o jeho využívání v mezích stanovených zákonem) výlučně fyzická osoba, které bylo rodné číslo přiděleno; jinak lze rodné číslo využívat jen v případech stanovených v § 13c tohoto zákona. Nezřídka jsou při sjednávání smluvních vztahů vyžadovány také jiné informace, které sice zdánlivě do soukromí subjektu údajů nezasahují, ale ve svém důsledku může být jejich zpracování diskriminačním. Těmito otázkami se zabýval v poslední době úřad veřejného ochránce práv,[253] když posuzoval postupy subjektů při sjednávání smluvních vztahů v nejrůznějších oblastech a konstatoval existenci diskriminačních praktik.

Z pohledu výkonu práv v prostředí Internetu lze za velmi významnou zákonnou licenci považovat zejména ustanovení § 5 odst. 2 písm. d) ZoOÚ, které umožňuje zpracovávat osobní údaje bez souhlasu subjektu osobních údajů, jedná-li se o oprávněně zveřejněné osobní údaje v souladu se zvláštním právním předpisem. Možnost zpracovávat oprávněně zveřejněné osobní údaje bez souhlasu subjektu údajů upravená v zákoně není zcela souladná s příslušnou Směrnicí, jejíž článek 7 písm. f) stanoví, že „*zpracování osobních údajů bez souhlasu subjektu údajů je možné výlučně v případech, kdy je to nezbytné pro uskutečnění oprávněných zájmů správce nebo třetí osoby či osob, kterým jsou údaje sdělovány, za podmínky, že nepřevyšují zájem nebo základní práva a svobody subjektu údajů*“. Směrnice tedy obsahuje zcela jinou úpravu než český ZoOÚ,

252 KUČEROVÁ, A., L. NOVÁKOVÁ, V. FOLDOVÁ, F. NONNEMAN, a D. POSPÍŠIL, ref. 194, s. 153.

253 K praxi vyžadování předložení výpisu z rejstříků trestů se vyjadřuje veřejný ochránce práv ve svém publikovaném doporučení (www.ochrance.cz) sp. zn. 30/2011/DIS/LO zcela jednoznačně, když uvádí, že: „Požadavek doložení bezúhonnosti před uzavřením pracovního poměru může být porušením povinnosti zaměstnavatele podle zákoníku práce. Také po vzniku pracovního poměru je zaměstnavatel oprávněn vyžadovat uvedenou informaci jen tehdy, souvisí-li bezprostředně s výkonem práce.“ V souladu s obsahem doporučení lze dospět k závěru, že pokud budoucí zaměstnavatel neodůvodní svou potřebu znát údaje o bezúhonnosti uchazeče o zaměstnání, jedná se o porušení ustanovení § 5 odst. 1 písm. a), popř. písm. d) zákona. V takovém případě se jedná o správní delikt, za nějž může Úřad uložit pokutu. Velmi podobně se veřejný ochránce práv vyjádřil k praktikám obcí při sjednávání pronájmu obecních bytů, když prostřednictvím svého doporučení sp. zn. 22/2010/DIS/AHŘ označil jako diskriminační požadavky na státní občanství, pohlaví, rasu a etnickou příslušnost žadatele o obecní byt a označil je jako diskriminační kritéria porušující zásadu rovného zacházení při přístupu k bydlení.

která nezbavuje oprávněně zveřejněné osobní údaje ochrany před dalším zpracováváním, což vzhledem k dosavadní judikatuře[254] může přinášet aplikační problémy.

Jak vyplývá z předmětného ustanovení, tato výjimka je vázána na současné splnění dvou podmínek, a to, že musí jít o osobní údaj zveřejněný v souladu s právním předpisem (tj. oprávněně), a zveřejněním nesmí být dotčeno právo na ochranu soukromého a osobního života subjektu těchto údajů. Za zveřejněný údaj považuje ZoOÚ „údaj zpřístupněný zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením n*ebo jako součást veřejného seznamu*" (§ 4 písm. l) ZoOÚ).

Při analýze podmínek této licence si musíme nejprve zodpovědět otázku, co ZoOÚ rozumí slovy „*zveřejněný v souladu s právním předpisem*". V tomto ohledu je zřejmé, že tuto podmínku nesplňuje takové zveřejnění, které bylo realizováno v rozporu se zákonem, tj. zveřejnění *contra legem*. Je však otázkou, zda má zákon na mysli toliko zveřejnění ve smyslu *secundum et intra legem,* tzn. na základě (podle) zákona a v souladu s ním, případně zveřejnění ve smyslu *preater legem,* tzn. ne přesně podle zákona, ale neporušuje ho a v souladu s jeho účelem. Dle názoru autora jsou správným výkladem obě tyto varianty, tj. jak výklad zveřejnění ve smyslu *intra legem* (na základě právního předpisu), tak i *preater legem* (v mezích). Zejména je třeba přihlédnout k tomu, že zákon hovoří výlučně o zveřejnění „v souladu s právním předpisem", nikoliv o zveřejnění toliko „na základě právního předpisu", tedy na základě existujícího zmocnění, případně stanovené právní povinnosti.

ZoOÚ tak stanoví jako základní kritérium oprávněnost takového zveřejnění ve smyslu jeho nerozpornosti s platnou právní úpravou a je lhostejné, zda se tak stalo na základě zákona (např. přímo zákonem) nebo v jeho mezích (např. na základě existujícího souhlasu subjektu osobních údajů). Za oprávněně zveřejněné osobní údaje je možné považovat jak ty údaje, jejichž zveřejnění stanoví ZoOÚ jako povinnost,[255] tak i takové údaje, které byly zveřejněny na základě zpravodajské licence v médiích, případně údaje, které o sobě zveřejnily samy subjekty těchto údajů. Za oprávněně zveřejněné osobní údaje lze považovat také ty osobní údaje, které jsou oprávněně veřejně přístupné komukoliv. Takovým příkladem je sbírka listin katastru nemovitostí, do které může nahlížet kdokoliv.[256] V některých případech jsou sice údaje veřejně přístupné, nicméně jejich použití je vázáno na nějaký konkrétní účel,[257] případně musí osoba, která k těmto údajům přistupuje, prokázat svůj právní zájem. V takovém případě již nelze hovořit o tom, že by šlo o oprávněně zveřejněné údaje v souladu s právním předpisem (viz výše),

254 Viz rozsudek Evropského Soudního dvora ve spojených věcech č. C-468/10 a C-469/10.

255 Jde o tzv. veřejné seznamy, jako např. katastr nemovitostí, obchodní rejstřík, živnostenský rejstřík (pouze veřejná část), on-line databáze ochranných známek, veřejný registr kandidátních listin pro volby, rejstřík veřejných výzkumných institucí (veřejná část týkající se statutárních orgánů) atd.

256 V těchto případech je ovšem právo přístupu vázáno na skutečnost, že seznamování se s jejím obsahem je spojeno s aktivitou zájemce, který se musí dostavit na katastrální úřad (neboť listiny uložené ve sbírce listin nejsou na Internetu zpřístupněny), znakem toho, že další použití zde získaných osobních údajů může představovat zásah do soukromí subjektu údajů.

257 Např. ochranu práv k nemovitostem, daňové a poplatkové účely, ochrana životního prostředí, zemědělského půdního fondu, pozemků určených k plnění funkcí lesa, nerostného bohatství, kulturních památek, pro rozvoj území, k oceňování nemovitostí, na účely vědecké, hospodářské a statistické.

protože zákon přístup k těmto údajům dále omezuje. Svou povahou tak nejde o údaje veřejně zcela přístupné, ale o údaje, které byly zpřístupněny za určitým účelem. Tento účel je nutné respektovat.[258] Ne každé zpracování oprávněně zveřejněných osobních údajů bude tedy možné bez souhlasu subjektu údajů, ale jen to, které nebude zasahovat do jeho soukromí. Pro posouzení, zda je zásah do soukromí nepřiměřený, bude vždy nezbytné provést test proporcionality (viz výše). Zásadním hlediskem bude přitom účel dalšího zpracování již zveřejněných údajů, a to zejména posouzení, zda je zpracování pro uskutečnění oprávněných zájmů správce nebo třetí osoby nezbytné.[259]

Sporným pak mohou být některé případy zveřejnění osobních údajů v obsahu veřejně vyhlašovaných rozsudků soudu, ačkoliv jde o oprávněně zveřejněné osobní údaje, nicméně mohou vzhledem ke své povaze obsahovat celou řadu osobních údajů účastníků i dalších osob, jejichž další šíření může být způsobilé zasahovat do jejich soukromého života. Jasné je to u těch soudních agend, kde je další šíření promítnuto formou zákazu přímo v zákonném předpise, jako je tomu např. v zákoně č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže, v platném znění (zveřejňování informace o řízení vedeném proti mladistvým), případně zvláštní ochrana poškozených v trestním řízení atd.[260]

Další zákonnou licencí pro zpracovávání osobních údajů bez souhlasu subjektu je skutečnost, že jde o zpracovávání nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby (ve smyslu § 5 odst. 2 písm. e) ZoOÚ). Takové zpracování osobních údajů však nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života.[261] Jak vyplývá ze samotné dikce tohoto ustanovení, musí být tato zákonná licence opřena o objektivně existující zájem, resp. subjektivní právo (např. vlastnické právo, právo na život a zdraví). Typickým příkladem bude stav, kdy např. zaměstnavatel poskytne kontaktní údaje svého zaměstnance osobě, která prokáže, že tyto kontaktní údaje potřebuje pro ochranu svých vlastních práv, resp. právem chráněných zájmů. Předání těchto osobních (kontaktních) údajů jiné osobě (příjemci) tak správce učiní bez souhlasu subjektu údajů, a to z důvodu ochrany práv příjemce, tedy zcela v intencích této zákonné licence. V praxi se lze nejčastěji s aplikací výjimky dle § 5 odst. 2 písm. e) ZoOÚ setkat při zpracování osobních údajů prostřednictvím

258 Obdobně je upraveno použití osobních údajů vedených z registru oznámení ve smyslu zákona č. 159/2006 Sb., o střetu zájmů, byť je tento registr ze zákona veřejně přístupný každému zájemci, informace z něj lze až na výjimky (např. ústavní činitele) použít pouze za účelem zjištění případného střetu zájmů. Informace tak lze dále užít či zpracovávat pouze za tímto účelem, nikoliv za účelem jiným.

259 K tomu srovnej KUČEROVÁ, A., L. NOVÁKOVÁ, V. FOLDOVÁ, F. NONNEMAN, a D. POSPÍŠIL, ref. 194, s. 155.

260 Nejvyšší správní soud v rozsudku NSS sp. zn. 2 As 21/2011, bod 41 uvádí, že „Čl. 96 odst. 2 Ústavy upravující veřejné vyhlašování rozsudku stanoví něco kvalitativně jiného než další veřejné šíření informací, v tomto rozsudku obsažených. Jestliže totiž smyslem a plně legitimním důvodem veřejnosti vyhlašování rozsudků je transparentnost justice a preventivní působení práva, nelze z toho fakticky dovozovat, že by tyto rozsudky měly sloužit současně i třeba jako prostředky ke skandalizaci či dehonestaci dotčených osob."

261 K tomu srovnej Směrnici, a to v různých jazykových mutacích, viz např. anglická verze, jež praví: „*Member States shall provide that personal data may be processed only if processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1.*"

záznamů z kamerových systémů. Je tomu tak proto, že zpracování na základě souhlasu subjektu údajů (tj. všech zaznamenaných osob) je v naprosté většině případu nerealizovatelné. Současně slouží kamerové nebo jiné monitorovací systémy k ochraně práv správců, zejména k ochraně jejich majetku, tedy vlastnického práva. V těchto případech je přitom třeba pečlivě posuzovat především charakter sledovaného prostoru, a to jak z hlediska četnosti výskytu osob (sklad nebo veřejná ulice), tak z hlediska jeho využití (vchod do budovy nebo šatna či sociální zařízení), vlastní předmět ochrany (umělecká sbírka nebo čistota ve výtahu), přesný záběr kamery (široký záběr na restauraci nebo cílený záběr na pokladnu), režim pořizování záznamu (nepřetržitě nebo pouze v odpoledních a nočních hodinách jako doplněk zabezpečovacího systému v uzavřeném a prázdném areálu) a také jiné možnosti zabezpečení ochrany konkrétních práv či zájmů (tj. nezbytnost zpracování). Až na základě vyhodnocení (zejména) těchto kritérií lze poté učinit závěr, zda je možné zpracování realizovat na základě § 5 odst. 2 písm. e) zákona, nebo nikoliv.[262]

Významná zákonná licence je pak zejména ustanovení § 5 odst. 2 písm. f) ZoOÚ, kde je zpracovávání osobních údajů bez souhlasu dotčeného subjektu vázáno na skutečnost, že zpracovatel poskytuje osobní údaje o veřejně činné osobě, funkcionáři či zaměstnanci veřejné správy, které vypovídají o jeho veřejné anebo úřední činnosti, o jeho funkčním nebo pracovním zařazení. Předmětná zákonná licence nebyla součástí původního vládního návrhu ZoOÚ, byla do zákona vložena na základě novely č. 439/2004 Sb. jako pozměňovací návrh, který byl předložen petičním výborem, a to jako reakce veřejnosti na zpřístupňování informací podle ZsPI.

4.4.7 Zpracování osobních údajů v prostředí Internetu se zřetelem k jejich zveřejňování

Internet se stal zcela neodmyslitelnou součástí naší společnosti, je zcela zásadním komunikačním prostředkem. Zcela legitimně tak vyvstávají otázky spojené s ochranou práv jeho uživatelů, zejména práv spojených s ochranou osobnosti a soukromí. Je nepochybné, že osobní informace zveřejněné prostřednictvím Internetu (bez ohledu na jejich pravdivost) mají obrovský potenciál zasáhnout dotčenou osobu v mnoha sférách jejího života, tedy jak v rodinném, tak i v pracovním či veřejném životě. Je proto na místě klást si otázku, zda a jakými prostředky lze ochranu soukromí v prostředí Internetu chránit. Ochrana osobnosti a soukromí je v České republice ústavně zakotvenou hodnotou (viz čl. 10 Listiny základních práv a svobod). Historicky spadá především do soukromoprávní kategorie práv, tedy do oblasti, kde jsou práva osob chráněna soudy v občanském soudním řízení v návaznosti na konkrétní žalobu. Nicméně pro určité oblasti, v nichž by zásah do práv představoval zvýšené riziko pro celospolečenské hodnoty, zákonodárce (obvykle pod vlivem společenského vývoje a mezinárodních dokumentů) rozhodl,

262 Se zpracováním osobních údajů na základě této výjimky je spojen i specifický způsob plnění informační povinnosti, neboť podle § 11 odst. 5 zákona je při zpracování osobních údajů podle § 5 odst. 2 písm. e) a § 9 písm. h) zákona správce povinen informovat subjekt údajů o zpracování jeho osobních údajů bez zbytečného odkladu, a nikoliv přímo při shromažďování osobních údajů (srov. komentář k § 11 odst. 5 zákona). K tomu více KUČEROVÁ, A., L. NOVÁKOVÁ, V. FOLDOVÁ, F. NONNEMAN, a D. POSPÍŠIL., ref. 200, s. 155.

že je důvodné poskytovat ochranu veřejnoprávní cestou, tj. formou státního zásahu. Zákonné provedení zmíněného čl. 10 Listiny základních práv a svobod tak lze nalézt jak v Občanském zákoníku (ochrana osobnosti podle § 11 až § 16), tak v trestním zákoníku a v neposlední řadě i v ZoOÚ.[263] Žádný z uvedených právních předpisů a priori nevylučuje ze své působnosti oblast Internetu – je tedy nutné vycházet z toho, že i přes svobodu a volnost, které jsou obecně deklarovanými atributy tohoto média, ani zde není právní vakuum umožňující zcela libovolné jednání.[264] Zákon o ochraně osobních údajů představuje svého druhu veřejnoprávní regulaci realizovanou formou pevného zakotvení autoritativního orgánu ochrany dat v podobě Úřadu zřízeného za tímto účelem. Tato regulace je odůvodněna zásadním zájmem na ochraně osob před riziky spojenými se zneužitím shromážděných osobních údajů v informačním prostředí Internetu. Hranice působnosti ZoOÚ jsou vymezeny v jeho § 3, dle kterého je státní zásah opodstatněný v situaci, kdy dochází k určitému systematickému (cílenému) využívání osobních údajů, které neslouží výhradně pro osobní potřeby fyzických osob.

Při aplikaci veřejnoprávní regulace ochrany soukromí je třeba normativně vycházet zejména ze ZoOÚ, předpisů komunitárního práva, konkrétně Směrnice, kterou ZoOÚ provádí, a také ze související judikatury ESD. Směrnice, s ohledem na dobu vzniku, neupravuje výslovně otázku zpracování (zveřejňování) osobních údajů na Internetu, nicméně konstatuje, že do působnosti Směrnice spadá především automatizované zpracování dat – tj. zpracování s pomocí výpočetní techniky. Tento fakt je třeba vnímat jako základní východisko k závěru, že ani oblast Internetu není a priori z působnosti Směrnice (a tedy i ZoOÚ) vyloučena.

Další vodítko poskytuje judikatura ESD, ze které lze především zmínit rozhodnutí zn. C-101/01, ze dne 6. listopadu 2003 (tzv. případ Lindqvist). Podle tohoto rozhodnutí se Směrnice, a tedy pravidla v ní stanovená pro zpracování osobních údajů, uplatní v případě, kdy jsou prostřednictvím webových stránek zveřejňovány informace týkající se určité skupiny osob.[265] Dalším vodítkem při aplikaci ZoOÚ je judikatura Ústavního soudu České republiky týkající se principu tzv. *ultima ratio* trestní represe, kterou je nutné zohlednit nejen v oblasti trestního práva, ale i při správním trestání (tedy při trestání za správní delikty definované v ZoOÚ). Ústavní soud ve svých nálezech opakovaně[266] zdůrazňuje, že prostředky trestního práva (a analogicky tedy i správního trestání) lze využít pouze tehdy, pokud užití jiných (soukromoprávních) prostředků ochrany nepřichází v úvahu nebo by bylo jejich využití zjevně neúčelné. Dle názoru Ústavního soudu lze trestněprávní kvalifikaci určitého jednání považovat až za krajní právní prostředek, který má své opodstatnění pouze v případě ochrany základních společenských hodnot.

Z uvedených východisek je zřejmé, že aplikace ZoOÚ na prostředí Internetu, které

263 Otázka zveřejňování osobních údajů na Internetu může v některých případech podléhat i dalším právním předpisům, např. zákonu o regulaci reklamy, zákonu č. 231/2001 Sb., o provozování rozhlasového a televizního vysílání nebo ZoSIS.

264 Viz Stanovisko Úřadu č. 13/2012, z března 2012 (původně K problémům z praxe č. 4/2010) zabývající se zveřejňováním osobních údajů na Internetu.

265 V uvedeném případě byly zveřejněny informace o osobách působících na farnosti, včetně jejich jména (úplného či jen křestního), popisu jejich funkce a zálib. V několika případech byl zmíněn i rodinný stav těchto osob, telefonní číslo a další informace (rozsudek viz: http://curia.europa.eu).

266 Viz např. nálezy Ústavního soudu sp. zn. IV. ÚS 469/02, I. ÚS 4/04 nebo I ÚS 541/10.

slouží obvykle k realizaci soukromoprávních aktivit, je omezená, nikoli však vyloučená. Při naplnění podmínek uvedených v § 3 tohoto zákona a zachování uvedeného principu ultima ratio, je i zveřejňování osobních údajů na Internetu postižitelné prostřednictvím ZoOÚ. Jinými slovy pro zpracování (tedy zejména zveřejňování) osobních údajů na Internetu neplatí a priori žádná výjimka a Úřad je kompetentní posoudit každý případ a rozhodnout, zda došlo k jednání, které zákon o ochraně osobních údajů reguluje či nikoli. Skutečnost, že se ne vždy bude jednat o zpracování osobních údajů podléhající uvedenému zákonu, anebo že nebude vždy možné dohledat odpovědnou osobu (tj. z hlediska ZoOÚ správce či zpracovatele osobních údajů), neznamená, že zde není dána působnost Úřadu, anebo že lze na aplikaci ZoOÚ v této oblasti rezignovat.

Jak již bylo uvedeno v předchozí kapitole, zpracování osobních údajů tak musí být realizováno buď na základě prokazatelného (informovaného) souhlasu subjektů osobních údajů, jichž se údaje týkají, případně na základě alespoň jedné z výše uvedených zákonných licencí (§ 5 odst. 2 zákona). Je-li tedy dán jeden z těchto právních titulů zpracovávání, musí ten, kdo hodlá jako správce zpracovávat osobní údaje, oznámit tuto skutečnost písemně Úřadu, a to ještě před samotným zpracováváním osobních údajů[267] (§ 16 zákona). Tato oznamovací povinnost je základní administrativní povinností správce, jejímž cílem je, s ohledem na skutečnost, že registr oznámených zpracování je veřejně přístupný prostřednictvím webových stránek Úřadu (www.uoou.cz), informovat zejména dotčené subjekty údajů (čímž je doplňována informační povinnost podle § 11 a 12 zákona), ale i další subjekty, pro které mohou být tyto informace relevantní (například předpokládané zpracovatele či smluvní partnery správce). Jak vyplývá z obsahu tohoto ustanovení, zákon v souladu s komunitárním právem výslovně stanoví obsah takového oznámení, ale neurčuje jeho formu.[268] Úřad na svých webových stránkách zpřístupňuje vzorový formulář, který může každý, kdo hodlá tuto povinnost realizovat, využít, a to včetně komentářů a doporučení zde uvedených.[269]

Další zcela zásadní podmínkou zpracování je důsledný postup ve smyslu ustanovení § 13 ZoOÚ, který upravuje základní povinnosti správce a zpracovatelem osobních údajů ve vztahu k zabezpečení ochrany těchto údajů. Toto klíčové ustanovení ukládá dvěma hlavním subjektům, tj. správci[270] (jako hlavnímu odpovědnému subjektu) a zpracovateli (tedy vedlejšímu subjektu, který koná obvykle na základě pověření správcem) povinnost přijmout taková opatření, aby nemohlo dojít:

- k neoprávněnému nebo nahodilému přístupu k osobním údajům,

267 S výjimkou zpracovávání osobních údajů uvedených v § 18 zákona.

268 BARTÍK, V. a E. JANEČKOVÁ. Oznamovací povinnost zaměstnavatele podle zákona o ochraně osobních údajů. *Práce a mzda*. 2011, č. 2, s. 23.

269 Viz Stanovisko Úřadu č. 13/2012 z března 2012 (původně K problémům z praxe č. 4/2010) zabývající se zveřejňováním osobních údajů na Internetu

270 Vztah mezi správcem a zpracovatelem vyplývá z ustanovení § 2 písm. j) a k), podle kterého je správcem každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak. Zpracovatelem je pak tedy každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona.

- k jejich změně, zničení či ztrátě, neoprávněným přenosům,
- k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů.

Jde tedy o klíčovou povinnost, která platí jak po celou dobu zpracování osobních údajů, tak i po ukončení tohoto zpracování (viz kapitola 4.4.3 této publikace).

Ve vztahu k výše uvedenému je mimořádně významný také požadavek § 6 zákona, jakož i článku 17 odst. 3 výše uvedené Směrnice, který stanoví další požadavky na náležitosti smlouvy o zpracování osobních údajů, jejíž uzavření je tedy nutné považovat za nedílnou součást zabezpečení osobních údajů. Správce osobních údajů uzavřením takové smlouvy zajišťuje, že také zpracování prováděné zpracovatelem osobních údajů bude probíhat v souladu s požadavky na bezpečnost zpracovávaných dat. V ZoOÚ je smlouva o zpracování osobních údajů upravena odděleně (viz § 6 zákona). Důraz na existenci této smlouvy je však třeba s odkazem na Směrnici posuzovat jako součást bezpečnostních opatření i při aplikaci ZoOÚ. Tento fakt je významný také proto, že absence smlouvy o zpracování osobních údajů sama o sobě nezakládá odpovědnost za správní delikt nebo přestupek podle ZoOÚ. Také Úmluva č. 108 obsahuje ve svém čl. 7 povinnost učinit vhodná bezpečnostní opatření na ochranu osobních údajů zpracovávaných v režimu této smlouvy proti náhodnému nebo neoprávněnému zničení nebo náhodné ztrátě, jakož i proti neoprávněnému přístupu, změnám nebo šíření.

Správce i zpracovatel osobních údajů tak má zákonem uloženou povinnost chránit osobní údaje nejen před následky lidského jednání, a to jak úmyslného, tak nedbalostního (tedy např. před ztrátou jakéhokoliv nosiče osobních údajů), ale i před živelními událostmi anebo selháním techniky, v jejichž důsledku by mohlo ke ztrátě, poškození, zničení či zneužití údajů dojít. S ohledem na pestrost praxe při zpracování osobních údajů a neustálý vývoj v oblasti prostředků zpracování dat i možností jejich ochrany (zejména v oblasti výpočetní techniky) je logické, že § 13 zákona nemůže obsahovat detailní nebo přímo taxativní výčet opatření potřebných k zajištění bezpečnosti zpracovávaných dat. Splnění povinnosti stanovené § 13 odst. 1 zákona závisí na mnoha faktorech, které se u jednotlivých správců, případně i u jednotlivých zpracování osobních údajů mohou velice lišit. Opatření, která postačí u podnikatele, který zaměstnává deset osob a osobní údaje potřebné pro plnění povinností zaměstnavatele shromažďuje a uchovává pouze v listinné podobě v kartotéce, neobstojí tam, kde je zaměstnanců deset tisíc, některé jejich údaje jsou dostupné na interní počítačové síti a jsou předávány jiným společnostem, případně i do zahraničí. Opatření jiného charakteru je samozřejmě nutné přijmout pro ty evidence, kde jsou zpracovávány „obyčejné" údaje, a tam, kde jsou zpracovávány také údaje citlivé ve smyslu § 4 písm. b) zákona. A jiný rozsah rizik je třeba zohlednit a eliminovat při zpracování osobních údajů v existujících veřejnoprávních informačních systémech. Je tedy zřejmé, že posouzení rizik souvisejících se zpracováním osobních údajů je otázkou vyhodnocení konkrétní situace daného správce či zpracovatele, zejména pak zvolených či stanovených prostředků a způsobu zpracování osobních údajů, druhu a rozsahu těchto údajů, ale také třeba specifik lokality či budovy, v níž ke zpracování dochází.[271]

271 KUČEROVÁ, A., L. NOVÁKOVÁ, V. FOLDOVÁ, F. NONNEMAN, a D. POSPÍŠIL, ref. 194, s. 231.

Povinnost uvedená v § 13 není časově omezena, je tedy třeba postupovat ve smyslu tohoto ustanovení i po ukončení zpracovávání osobních údajů. V tomto ohledu je samozřejmě otázkou, kdy vůbec takový okamžik ukončení zpracování nastává. Zákon v tomto ohledu bližší vodítko neposkytuje, je tedy nutné vycházet spíše ze skutečnosti, že předmětné ustanovení zde z opatrnosti pokrývá situaci, kdy osobní údaje sice nadále existují, nicméně nedochází a nebude již docházet k jejich systematickému nakládání (tj. například situace, kdy došlo k rozhodnutí podnikatele o tom, že osobní údaje zákazníků, které byly poskytnuty za účelem zasílání obchodních sdělení, již nadále nebudou takto používány). V takovém případě tak pominul účel zpracování (shromažďování), přičemž je nezbytné postupovat ve smyslu ustanovení § 20 zákona upravující likvidaci osobních údajů. Pro úplnost je třeba konstatovat, že i samotná likvidace osobních údajů je ze zákona považována za zpracování osobních údajů.[272] Dochází-li tedy k likvidaci nosičů osobních údajů (tj. HDD, SDD, CD, DVD, flash disků či jiných záznamových zařízení), tedy stále ještě ke zpracování osobních údajů, je nutné postupovat rovněž ve smyslu ustanovení § 13, tzn. zajistit bezpečnou likvidaci (skartaci) těchto nosičů záznamu, a to primárně formou specializovaného programu, který trvale a bezpečně tato data odstraní, případně rovněž formou bezpečné fyzické likvidace těchto nosičů.[273] Tato otázka zůstává vysoce aktuální, jak uvedeno výše, zejména v případě ukončení podnikatelské činnosti, případně při pravidelné archivaci dat nebo běžné komunikaci.[274]

Správce nebo zpracovatel je povinen zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy (§ 13 odst. 2). Pro splnění této povinnosti je nezbytné zohlednit veškeré okolnosti daného zpracování (personální, lokální, objektové a technologické), přičemž se tato povinnost vztahuje na dokumentaci vzhledem ke všem opatřením, která správce či zpracovatel ve vztahu k rozhodným činnostem přijal. V rámci těchto opatření pak správce nebo zpracovatel posuzuje rizika týkající se:

a) plnění pokynů pro zpracování osobních údajů osobami, které mají bezprostřední přístup k osobním údajům,
b) zabránění neoprávněným osobám přistupovat k osobním údajům a k prostředkům pro jejich zpracování,
c) zabránění neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahujících osobní údaje,
d) opatření, která umožní určit a ověřit, komu byly osobní údaje předány.

272 K tomu srovnej ustanovení § 4 písm. e), podle kterého se zpracováním osobních údajů rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace.

273 Za bezpečnou likvidaci však nelze považovat přeformátování tohoto nosiče, případně jednoduché vymazání příslušných nosičů. V tomto případě totiž příslušné údaje na nosiči dále existují, ale jsou obtížněji přístupné. Za bezpečné se v tomto ohledu považuje několikanásobné přemazání příslušného nosiče samými náhodnými znaky (nikoliv např. pouhými nulami), což dostatečně garantuje nemožnost data obnovit.

274 K tomu více viz KUČEROVÁ, A., L. NOVÁKOVÁ, V. FOLDOVÁ, F. NONNEMAN, a D. POSPÍŠIL, ref. 194, s. 231.

Povinnost posuzovat výše uvedená rizika musí být realizována ještě před zahájením zpracování osobních údajů. Jde o požadavek na provedení analýzy rizik, tj. komplexní popsání existujících a reálných rizik plynoucích z možného ohrožení osobních údajů. Porušení některé z povinností uvedených v ustanovení § 13 odst. 3 zákona představuje skutkovou podstatu přestupku nebo jiného správního deliktu ve smyslu ustanovení § 44 odst. 2 písm. h) zákona (tj. nepřijetí nebo neprovedení opatření pro zajištění bezpečnosti zpracování osobních údajů).

Pro zpracování osobních údajů v prostředí Internetu je zcela zásadní ustanovení § 13 odst. 4 zákona, které upravuje tzv. automatizované zpracování osobních údajů, tj. takové zpracování, které je realizováno prostřednictvím automatizovaného prostředku (zejména elektronicky prostřednictvím počítače). Důvodem této specifické úpravy jsou zejména požadavky Schengenské prováděcí úmluvy ve vztahu ke zpracování osobních údajů v rámci Schengenského informačního systému, konkrétně čl. 118 této Úmluvy.[275] V tomto ohledu je zde upraven výčet povinností při zabezpečení automatizovaně zpracovávaných osobních údajů, a tím do určité míry upřesňuje obsah povinnosti uvedené v § 13 odst. 1 zákona. Současně stanovuje minimální standard opatření, které je správce nebo zpracovatel povinen přijmout vždy. Tato rizika je povinen vyhodnotit každý správce a zpracovatel, který zpracovává data automatizovaně, aniž by však byla jakkoli dotčena jeho obecná povinnost ve smyslu § 13 odst. 1 zákona. Porušení některé z povinností uvedených v ustanovení § 13 odst. 3 zákona představuje skutkovou podstatu přestupku nebo jiného správního deliktu ve smyslu ustanovení § 44 odst. 2 písm. h) zákona (tj. nepřijetí nebo neprovedení opatření pro zajištění bezpečnosti zpracování osobních údajů). Základní povinností správce nebo zpracovatele, který zpracovává osobní údaje tímto způsobem (tj. automatizovaně) je také:

a) zajistit, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze oprávněné osoby,
b) zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby,
c) pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány,
d) zabránit neoprávněnému přístupu k datovým nosičům.

Tyto specifické povinnosti uvedené v ustanovení § 13 zákona tak dopadají na všechny správce (zpracovatele), kteří zpracovávají osobní údaje v prostředí Internetu (tj. automatizovaně v elektronické podobě). Do této kategorie spadají v zásadě všichni provozovatele e-shopů, zaměstnavatelé umožňující zaměstnancům pracovat s osobními údaji prostřednictvím Internetu (homeworking), provozovatelé veřejných i neveřejných seznamů, jakož i řada dalších subjektů, včetně poskytovatelů obsahu v prostředí Internetu. Je tedy základní povinností těchto subjektů, aby nastavily podrobné parametry ochrany a zabezpečení souvisejících informačních systémů,

275 Úmluva k provedení Schengenské dohody ze dne 14. června 1985 mezi vládami států Hospodářské unie Beneluxu, Spolkové republiky Německo a Francouzské republiky o postupném odstraňování kontrol na společných hranicích [online]. (Úř. věst. L 239, 22. 9. 2000, s. 19). Dostupné z: http://eur-lex.europa.eu/ LexUriServ/LexUriServ.do?uri=CELEX:42000A0922%2802%29:CS:NOT

a to ve všech výše uvedených oblastech, nikoliv pouze po stránce technologické, ale také objektové, personální a právní (obchodněprávní, pracovněprávní, autorskoprávní atd.). V tomto ohledu je nezbytné nastavit tyto systémy důsledně na zákonná kritéria ve smyslu ustanovení § 13 odst. 4 zákona, a to zejména ve vztahu k zajištění logování přístupů k těmto údajům, jakož i požadavkům na dostatečnou kryptografickou či jinou obdobnou ochranu před neoprávněným přístupem.

V oblasti zajištění systémů pro přístup pouze oprávněných osob (§ 13 odst. 4 písm. a), je tedy třeba nastavit v souvislosti se zpracováním osobních údajů vhodný systém přístupových oprávnění (minimálně formou individuálních přihlašovacích jmen a hesel), případně jinou formu autentizace). Tímto způsobem je přitom nutné chránit jak využívanou techniku (typicky osobní počítače), tak i jednotlivé informační systémy, v nichž jsou osobní údaje zpracovávány.[276] Samotné zajištění systémů pro přístup pouze k údajům odpovídajícím oprávnění těchto osob (tj. ve smyslu konkrétního omezeného rozsahu uživatelských oprávnění zřízených výlučně pro specifickou – oprávněnou – kategorii) uživatelů (§ 13 odst. 4 písm. b), je nutné zajistit přístup pouze k těm osobním údajům, které odpovídají oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby (tj. individuální přístupové účty). Splnění této povinnosti spočívá ve vyhodnocení okolností daného zpracování a záměrů správce či zpracovatele osobních údajů a nastavení vhodného rozsahu oprávnění pro každého pracovníka, resp. pracovní pozici. V souladu s principy ZoOÚ je nezbytné, aby každý, kdo se na zpracování osobních dat podílí, měl přístup jen k takovému rozsahu osobních údajů, který nezbytně potřebuje pro výkon své činnosti. Je tedy nutné diferencovat přístupová oprávnění jednak vertikálně (nadřízení mají přístup k většímu rozsahu dat než běžní zaměstnanci, kteří mají z principu přístup výhradně k údajům, které osobně zpracovávají v souvislosti s výkonem práce), jednak horizontálně (pracovníci v různých úsecích či odborech mohou nahlížet pouze do dat souvisejících s jejich agendou). Dále je vyloučeno, aby správce či zpracovatel zřídil hromadná přístupová oprávnění (sdílená více osobami) ke všem osobním údajům nebo k jejich některým kategoriím, aniž by zohlednil pracovní náplň jednotlivých zaměstnanců. Takový postup nedůvodně rozmělňuje odpovědnost konkrétních osob za zpracování osobních údajů, a tím zvyšuje riziko jejich ztráty či zneužití.[277]

Ve vztahu k realizaci povinnosti zajistit zákonný požadavek systémů pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány (§ 13 odst. 4 písm. d), je povinností každého správce a zpracovatele osobních údajů pořizovat při automatizovaném zpracování elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány (např. změněny, smazány, ale i jen zobrazeny). Tato povinnost znamená, že v rámci předmětného informačního systému je kromě samotného obsahu (osobních údajů) uchováván

276 Nároky na systém přístupových oprávnění je třeba posuzovat s ohledem na charakter zpracovávaných údajů a další okolnosti zpracování u daného správce či zpracovatele, jako je fyzické umístění využívané techniky nebo standardní provoz na daném pracovišti. Jiné nároky budou jistě kladeny na zpracování personální agendy středně velké firmy a jiné na vedení rozsáhlého informačního systému veřejné správy (např. Informační systém evidence obyvatel) anebo policejní informační systémy.

277 KUČEROVÁ, A., L. NOVÁKOVÁ, V. FOLDOVÁ, F. NONNEMAN, a D. POSPÍŠIL, ref. 194, s. 239.

také záznam vypovídající o každé operaci, která byla s osobními daty provedena. Tyto záznamy (logy) slouží jako historie zpracování osobních údajů, přičemž v souladu s § 13 odst. 4 písm. c) zákona musí být z těchto logů zjistitelná doba zpracování, identita osoby, která data zpracovávala, a také důvod takového zpracování. Záznamy slouží samotnému správci či zpracovateli osobních údajů ke kontrole plnění povinností jeho zaměstnanců a dalších osob spolupracujících na zpracování osobních údajů – logy lze využít k namátkové (preventivní) kontrole, anebo ke kontrole následné, v případě, kdy má správce nebo zpracovatel podezření na zneužití osobních údajů konkrétní osobou. Jak bylo již několikrát uvedeno, pravidelná a důsledná kontrola plnění pokynů a povinností udělených zaměstnancům, příp. ostatním pracovníkům, je nedílnou součástí zajištění bezpečnosti osobních dat. Využití logů ke kontrole je tak de facto další povinností správců a zpracovatelů osobních údajů.

Záznamy pořízené v souladu s ustanovením § 13 odst. 4 písm. c) zákona může využít také Úřad v případě, kdy je předmětem jím vedené kontroly zpracování osobních údajů prostřednictvím informačního systému kontrolovaného subjektu, příp. jako důkaz v rámci vedeného správního řízení. U rozsáhlých informačních systémů je dále na místě zajištění pravidelného vyhledávání anomálií při zpracování osobních údajů, tj. automatizovaná nebo i manuální kontrola záznamů (logů) za účelem odhalení případného chybného postupu nebo zneužívání dat. V této souvislosti lze dále odkázat na povinnost podle § 5 odst. 1 písm. e) zákona, tedy povinnost uchovávat osobní údaje pouze po nezbytnou dobu, neboť tento princip je nutné vztáhnout také k záznamům pořízeným podle § 13 odst. 4 písm. c) zákona. Obvykle je doba uchování těchto záznamů vázána na existenci údajů, k nimž se záznamy vztahují (logy mohou být likvidovány současně s korespondujícími daty anebo s krátkým odstupem, umožňujícím kontrolu zpracování dat ještě určitou dobu po odstranění samotných osobních údajů). V případě rozsáhlých evidencí, které jsou vedeny de facto stále (tedy zejména veřejné registry typu evidence obyvatel), lze však, s ohledem na dobu zpracování osobních údajů a s tím spojenou technologickou náročnost uchovávání všech logů, akceptovat určitý časový limit, např. tří let, kdy jsou korespondující logy mazány.[278]

Zcela zásadní povinností je zabránit neoprávněnému přístupu k datovým nosičům (§ 13 odst. 4 písm. d). Je totiž logické, že stejně jako je chráněn přístup k informacím (osobním údajům) zpracovávaným v informačním systému, je nutné chránit i přístup k nosičům, na nichž jsou tato data zaznamenána. V tomto ohledu lze na jedné straně hovořit o zabezpečení dálkového přístupu, a o ochraně konkrétního nosiče záznamu na straně druhé. Zatímco v prvním případě půjde obvykle o softwarové zabezpečení systému proti neoprávněnému přístupu, ve druhém případě jde o fyzickou ochranu datových nosičů a datových úložišť před neoprávněnými osobami, tedy např. před krádeží či okopírováním. Také ve vztahu k datovým nosičům je na místě přijmout vhodná organizační i technická opatření, tj. určit, jak je nutné datové nosiče uchovávat a jakým způsobem lze s datovými nosiči na daném pracovišti nakládat, např. jakou cestou je lze předávat zpracovatelům osobních údajů nebo zda a za jakých okolností lze datové nosiče odnášet mimo místo výkonu práce.[279]

278 KUČEROVÁ, A., L. NOVÁKOVÁ, V. FOLDOVÁ, F. NONNEMAN, a D. POSPÍŠIL, ref. 194, s. 240.
279 KUČEROVÁ, A., L. NOVÁKOVÁ, V. FOLDOVÁ, F. NONNEMAN, a D. POSPÍŠIL, ref. 194, s. 242.

Z praktického hlediska patří problematika zpracování osobních údajů v prostředí Internetu k nejčastěji řešené agendě správněprávní oblasti ochrany osobních údajů. Samotné zpracování osobních údajů v prostředí Internetu, zejména otázky spojené se zveřejňováním a zajištěním bezpečnosti těchto údajů, patří k nejčastěji řešené agendě Úřadu. V tomto ohledu se Úřad zabývá zejména případy, kdy dochází ke zveřejnění seznamu dlužníků (tzv. černé listiny neboli blacklisty, podrobněji řešeno v části 4.4.11) na webových stránkách obchodních společností, podnikajících osob či obcí (podrobněji řešeno v části 4.4.8). Dále Úřad posuzoval případy zveřejnění osobních údajů zaměstnanců, ať již v souvislosti s pracovněprávním sporem nebo vyhlášením konkurzního řízení (podrobněji řešeno v části 4.7). Úřad se také velmi často zabývá zveřejněním osobních údajů v rámci dokumentů pocházejících z činnosti obcí či měst, případně dalších subjektů (viz níže). Ve všech výše uvedených případech dospěl Úřad k závěru, že podmínky pro aplikaci ZoOÚ jsou naplněny a posuzoval tedy zjištěný stav z hlediska plnění povinností tímto zákonem stanovených, zejména povinnosti zpracovávat osobní údaje pouze na základě zákonem předvídaného právního titulu dle § 5 odst. 2 ZoOÚ a základních povinností vyjádřených v § 5 odst. 1 tohoto zákona (např. povinnosti zpracovávat osobní údaje pouze v souladu s původním účelem). Naopak mimo působnost ZoOÚ budou obvykle jednotlivé informace publikované v rámci blogů, zájmových webových stránek, nejrůznějších diskusí anebo sociálních sítí. Uvedené neznamená, že by zveřejněním nějaké osobní informace touto cestou nemohlo dojít k zásahu do osobnostních práv, nicméně s ohledem na výše uvedená východiska nebude ve většině takových případů opodstatněný veřejnoprávní zásah ze strany Úřadu. Dotčené osoby se nicméně mohou svých práv domoci cestou občanského soudního řízení.[280]

Pro úplnost je třeba dodat, že nezřídka dochází k situacím, že jsou prostřednictvím Internetu zveřejňovány osobní údaje jako důsledek specifického výkladu zákonné povinnosti orgánu veřejné správy zveřejnit různé údaje a informace způsobem umožňujícím dálkový přístup. Nejčastěji jde o specifický a právními normami stanovený způsob doručování písemností sloužící k zachování práv účastníků řízení, případně pak obecně o umožnění veřejnosti jednoduchým způsobem získat informace o činnosti (úkonu) konkrétního orgánu veřejné správy. Nikoli výjimečně přitom dochází k situaci, kdy listiny zveřejněné prostřednictvím elektronické úřední desky (např. podle správního řádu) obsahují osobní údaje, které zůstávají za použití internetových vyhledávačů přístupné i určitou dobu po tom, co jsou z elektronické desky po uplynutí zákonem stanovené doby listiny technicky odstraněny. K tomu, aby byla i v prostředí webových stránek dodržena pravidla pro ochranu osobních údajů, je třeba použít některého z běžně do-

280 Samotné zveřejnění jména a příjmení jedné osoby nepředstavuje systematickou operaci prováděnou s osobními údaji ve smyslu režimu zákona o ochraně osobních údajů. V takovém případě rovněž není nutný souhlas dotčené osoby ke zveřejnění jejího jména a příjmení na internetu. Nicméně zejména v případech, kdy je jméno a příjmení zveřejňováno sice jednotlivě, avšak v souvislostech dotýkajících se občanské cti a lidské důstojnosti, soukromí, dobrého jména nebo projevů osobní povahy, může dotčená osoba postupovat proti takovému zveřejnění žalobou na ochranu osobnosti podle § 11–16 ObčZ, pokud je jí ovšem známo, kdo její jméno a příjmení v těchto souvislostech na internetu zveřejnil. K tomu viz více část 4.6 této publikace.

stupných nástrojů,[281] který zamezí indexování[282] příslušných webových stránek, respektive jejich ukládání do cache[283] internetového vyhledávače. V tomto ohledu lze doporučit vycházet z publikovaného stanoviska[284] Úřadu, které stanoví možný přístup k úpravě webových stránek či webového portálu do stavu souladného s ochranou osobních údajů, přičemž se tato problematika týká zejména institucí, které budují komplexní nástroje pro výkon elektronizované veřejné správy a dostupnost jejich služeb pro občany na Internetu. Jednou z podmínek zadávání a tvorby těchto systémů musí být i dále uvedené požadavky na standardizované zpracování osobních údajů.[285] V případě indexování stránek je softwarový nástroj (program–robot),[286] který indexaci a cachování stránek provádí, schopen po určité době odstranit záznam o stránce či souboru (včetně otisku z cache), které již na předchozím umístění nenalezne. Webové dokumenty tak zůstávají dohledatelné a přístupné prostřednictvím vyhledávače ještě po dobu, než robot vyhledávače provede jejich reindexaci. Při zobrazení z cache jsou přitom přístupné i stránky či soubory, které již byly odstraněny, pokud je jejich otisk uložen na serveru vyhledávače. V případě webových archivů, které uchovávají webové stránky trvale, lze nadbytečnému ukládání stránek obsahujících osobní údaje zamezit, resp. přesněji výrazně omezit pravděpodobnost takového ukládání, vhodným nastavením práv pro přístup výše zmiňovaných robotů. V tomto ohledu zde platí, že takový stav, kdy osobní údaje, jejichž zákonem stanovená doba pro zveřejnění uplynula (viz princip proporcionality) a které zůstávají nadále přístupné (relativně) neomezenému okruhu osob, musí být považován za porušení povinnosti stanovené v § 13 odst. 1 ZoOÚ.[287] Úřad v tomto ohledu

281 Nástroje či návody k zákazu indexování lze najít prostřednictvím obvyklých internetových vyhledávačů, např. po zadání klíčových slov „zákaz indexování" nebo „zákaz přístupu vyhledávačů".

282 Indexování probíhá tak, že vyhledávač prochází stránky skrze náhodné odkazy a každou novou nebo aktualizovanou stránku odešle do své databáze, a pokračuje dalším (i náhodným) odkazem ze stránky. K tomu více viz ZICHA O. Princip vyhledávačů [online]. Dostupné z: www.biolib.cz/cz/help/id154/

283 Označení pro vyrovnávací paměť používanou ve výpočetní technice. Internetové vyhledávače často ukládají indexované webové stránky do své cache a mohou ji i zpřístupnit. (Cache.[vid. 1. června 2011]. Dostupné z: http://cs.wikipedia.org/wiki/Cache) Cachování tedy znamená ukládání webových stránek do vyrovnávací paměti internetového vyhledávače.

284 K tomu srovnej související stanovisko č. 1/2011 (srpen 2011) Úřadu k problematice zveřejňování listin s osobními údaji prostřednictvím Internetu. Dostupné z: www.uoou.cz/files/stanovisko_2011_1.pdf

285 Lze připomenout, že podle § 5b ZoISVS, orgány veřejné správy uplatňují opatření odpovídající bezpečnostním požadavkům na zajištění důvěrnosti, integrity a dostupnosti informací zpracovávaných v informačních systémech veřejné správy.

286 Internetový robot je počítačový program, který pro svého majitele opakovaně vykonává nějakou rutinní činnost na internetu – obvykle sbírá data, odesílá a zpracovává požadavky na služby vzdálených serverů. Častým příkladem robota jsou vyhledávací roboty internetových vyhledávačů. Tento typ robotů prochází jednotlivé webové stránky, hledá na nich odkazy na nové stránky, indexuje obsah zpracovávaných stránek a umožňuje jejich následné prohledávání. Podobným příkladem může být robot na kontrolu odkazů. Prochází zadanou množinu stránek (opět následuje odkazy) a hledá na nich odkazy na již neexistující stránky. Více k internetovému robotu viz http://cs.wikipedia.org/wiki/Internetový_robot

287 Tedy porušení povinnosti přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i jinému zneužití osobních údajů.

ve svém stanovisku[288] dovozuje, že správným postupem z hlediska ochrany osobních údajů je až obecný zákaz indexování listin s osobními údaji, které jsou umisťovány na elektronické úřední desky, což současně znamená i zákaz jejich cachování. Účelem zpřístupnění osobních údajů, respektive konkrétních dokumentů, uvedeným způsobem totiž není „automatické" umožnění předávání a sdružování údajů zveřejněných na jednotlivých úředních deskách do úložišť mimo působnost orgánů veřejné správy, ani trvalé uchovávání, prohledávání nebo profilování těch dokumentů s osobními údaji, u nichž zákon přesně stanovil některé způsoby zpracování, a to včetně doby tohoto zpracování. Tento úřadem deklarovaný postup směřující k zákazu cachování je však nutné interpretovat především ve vztahu ke konkrétnímu zákonem předpokládanému účelu takovéhoto zveřejnění, přičemž v těch případech, kdy je zřejmým účelem zveřejnění široká veřejná kontrola, je třeba dovodit, že tento zákaz neplatí, zájem na takto širokém zveřejnění totiž může být silnější než omezení vyplývající z poměřování principem proporcionality. Tyto hodnoty je však nutné vážit s ohledem na skutečnost, že zákaz indexování a prohledávání předmětných dokumentů podstatně omezuje možnost kontroly (např. obecní a veřejné správy), neboť kontrolující veřejnost má k informacím tohoto typu zhoršený přístup. Střetává se zde tedy právo na ochranu osobních údajů a principy transparentnosti obecní samosprávy či veřejné správy, včetně práva na jejich kontrolu.[289]

Úřad ve vztahu k výše uvedenému zákazu autoritativně doporučuje,[290] aby byl příslušný dokument odstraněn z příslušného webového serveru, případně kvalifikovaně přesunout do jeho zabezpečené (HTTPS)[291] části webu. Je tedy nezbytné vycházet v tomto ohledu ze skutečnosti, že zákaz indexování webových stránek, resp. dokumentů s osobními údaji, je svého druhu standardní opatření na straně správce osobních údajů, které má zamezit neoprávněným přístupům a přenosům osobních údajů tak, jak vyžaduje § 13 odst. 1 ZoOÚ. Za účelem naplnění tohoto ustanovení a pro případ takto zveřejněných dokumentů, jakož i jejich republikace na jiném místě či prostředí, doporučuje Úřad dodržovat v prostředí webových stránek realizování níže uvedených pravidel ochrany osobních údajů:

- pro celé webové stránky zakázat prostřednictvím souboru robots.txt přístup robotů,
- zakázat přístup robotů pro každou stránku zvlášť pomocí meta tagu obsaženého v hlavičce stránky, případně pro vlastní odkazy použít atribut rel="nofollow", rel="noindex" a rel="noarchive", v důsledku čehož je odkaz s tímto parametrem pro robota neviditelný, neprovede indexaci stránky nebo její uložení do cache. Použití těchto atributů přitom většina vyhledávačů respektuje,
- problematické stránky (tj. ty, jež obsahují osobní údaje) zařadit na druhou, lépe třetí a další úroveň struktury webových stránek,
- minimalizovat (dle možnosti) počet odkazů na uvedenou stránku,

288 K tomu srovnej související stanovisko č. 1/2011, ref. 294.

289 Viz např. povinnost obcí zveřejňovat prostřednictvím úřední desky ve smyslu zákona o obcích, kde je nutné poměřovat povahu a účel takovéhoto zveřejnění ve vztahu k ochraně soukromí konkrétních osob.

290 K tomu srovnej související stanovisko č. 1/2011, ref. 294.

291 Viz síťový protokol HTTPS (Hypertext Transfer Protocol Secure), jenž umožňuje zabezpečit spojení mezi webovým prohlížečem a webovým serverem před neoprávněným přístupem a umožňuje též ověřit identitu protistrany.

- webové stránky obsahující osobní údaje vždy opatřit označením správce těchto údajů a dobou, kdy byly tyto stránky vytvořeny.[292]

4.4.8 Veřejné zasedání a zveřejňování souvisejících údajů na Internetu

Při posuzování uvedeného problému je třeba v prvé řadě vycházet z ustanovení § 42 zákona o krajích a z ustanovení § 93 odst. 2 zákona o obcích (obecní zřízení), ve znění pozdějších předpisů, podle nichž je zasedání zastupitelstva veřejné. Diskuse na těchto zasedáních, i když jsou v jejich průběhu osobní údaje používány, nenaplňuje pojmové znaky zpracování osobních údajů ve smyslu ustanovení § 4 písm. e) ZoOÚ. Uskutečnění přímého televizního přenosu z jednání zastupitelstev na Internetu tak není možné podřizovat zákonu o ochraně osobních údajů a jakkoliv je z hlediska tohoto zákona omezovat.

Okruh možných příjemců informací se přenosem prostřednictvím televize nebo internetu rozšiřuje, což je jistě obecně pozitivním jevem. Z pohledu ochrany osobních údajů to však může mít i negativní důsledky, neboť jsou šířeny i k těm příjemcům, kteří by o ně přímou účastí na jednání zájem neprojevili, což může zvyšovat riziko zneužití osobních údajů.

V průběhu zasedání mohou nebo i musí zastupitelé používat osobní údaje, které jsou v některých případech výstupem ze zpracování osobních údajů prováděných krajem či obcí, jako správcem osobních údajů, stejně jako údaje později uvedené v zápisu ze zasedání. Je ale třeba činit rozdíl mezi zápisem ze zasedání, za který je odpovědný správce osobních údajů a který má být, podle § 12 odst. 2 písm. c), § 12 odst. 3 a § 13 zákona o krajích či podle § 16 odst. 2 písm. e), § 16 odst. 3 a § 17 zákona o obcích, zpřístupňován vymezenému okruhu příjemců a veřejnou diskusí na zasedání. Zastupitelé se s osobními údaji, které jsou výstupem ze zpracování, seznámili jako osoby, které v rámci plnění zákonem stanovených oprávnění a povinností přicházejí u správce do styku s osobními údaji a jsou povinni zachovávat o nich mlčenlivost podle § 15 ZoOÚ. Bude-li však použití osobních údajů pro projednání určité kauzy nezbytné, nelze je posuzovat jako porušení povinnosti mlčenlivosti.

Je však třeba připomenout rovněž § 10 ZoOÚ, podle kterého má správce při zpracování osobních údajů dbát, aby subjekt údajů neutrpěl újmu na svých právech, zejména na právu na zachování lidské důstojnosti a také dbát na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů. Správce by tedy měl pamatovat na to, aby při veřejném zasedání byly v souvislosti s projednávanou kauzou používány osobní údaje pouze v nezbytně nutném rozsahu. Pokud jde o citlivé údaje vypovídající např. o zdravotním stavu subjektu údajů, které jsou případně v evidencích vedených orgány samosprávy zpracovávány, podléhají podle § 9 ZoOÚ přísnějšímu režimu ochrany. Na úrovni veřejného zasedání zastupitelstva však není k jejich použití žádný důvod. Při veřejném zasedání přesto nelze vyloučit, že mohou být zastupiteli i jinými účastníky proneseny výroky, které osoba, jíž se týkají, může

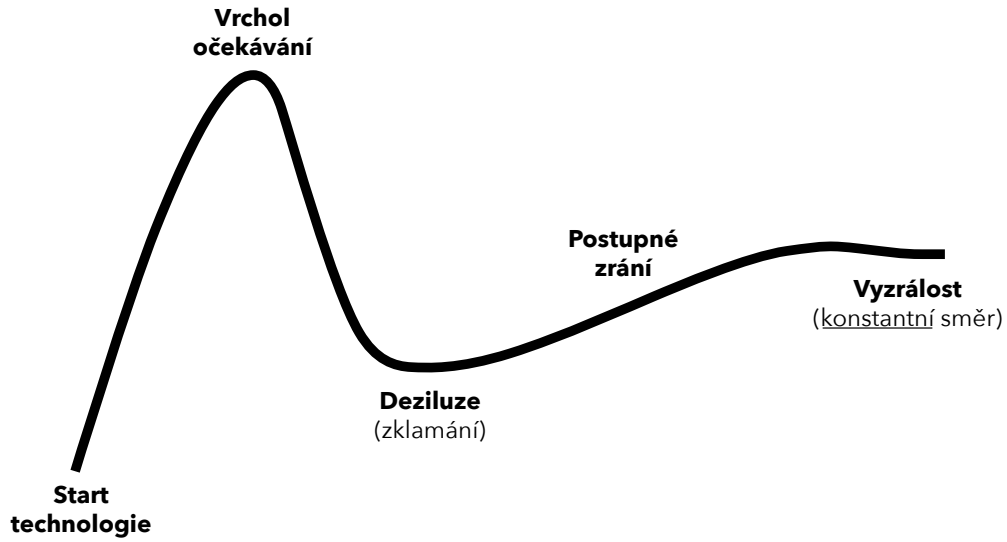
292 K tomu srovnej související stanovisko č. 1/2011 (srpen 2011) Úřadu k problematice zveřejňování listin s osobními údaji prostřednictvím internetu. Dostupné z: www.uoou.cz/files/stanovisko_2011_1.pdf

považovat za neoprávněné zveřejňování osobních, případně i citlivých údajů. Právo na ochranu před neoprávněným zveřejňováním osobních údajů obecně, tedy i v případě, že nejde o jejich zpracování podle ZoOÚ, stanoví článek 10 odst. 3 Listiny základních práv a svobod. V tom případě se však tohoto práva a případného zadostiučinění lze domáhat pouze soudní žalobou na ochranu osobnosti podle § 11–16 ObčZ.

Pro úplnost je třeba dodat, že na rozdíl od přímého přenosu z jednání zastupitelstva považuje[293] Úřad za nepřípustné zveřejňování neanonymizovaných záznamů z jednání zastupitelstva na webových stránkách obce, při kterém dochází k uchovávání osobních údajů v záznamech obsažených, tedy jejich zpracování ve smyslu definice ZoOÚ se zpřístupňováním neomezenému okruhu příjemců. Případné zpřístupňování videozáznamu jednání je podle názoru Úřadu ve stejném režimu jako zpřístupňování zápisu stanoveného zákonem o obcích.

4.4.9 Sociální sítě – vybrané aspekty

Nezpochybnitelným fenoménem současnosti jsou sociální sítě. Jak to už u takovýchto fenoménů bývá, platí i zde tzv. Gartnerova křivka (*gartner hype cycle*),[294] která vyjadřuje vyspělost a aktuální stav IT technologií a jejich připravenost na další rozvoj. Křivka má pět základních fází (start technologie a nárůst počátečního zájmu, vrchol očekávání, deziluze, postupné zrání a výslednou vyzrálost v podobě přijetí samotné technologie).



293 K tomu více viz příslušný názor Úřadu (rubrika: Otázky kladené v souvislosti se zákonem o ochraně osobních údajů. Dostupné z: http://uoou.cz/uoou.aspx?menu=14&loc=331#a75).

294 K tomu více viz http://en.wikipedia.org/wiki/Hype_cycle

Výše uvedenou křivku lze vztáhnout také na sociální sítě, zejména pak co se týče vzájemného vztahu očekávání a související deziluze. Podobně jako byla všeobecně deklarována výhoda transparentnosti a veřejnosti těchto sítí ve světle jejich efektivity, začínají se objevovat vážné obavy o zachování určitého přiměřeného (rozumného, příp. legitimního) očekávání soukromí v prostředí těchto sítí. Uvedené představuje dílem problém samotné koncepce této technologie, včetně přehlednosti uživatelského nastavení,[295] jakož i bezdůvodné důvěřivosti jejich uživatelů. Právní režim sociálních sítí je do jisté míry závislý na otázce rozhodného práva a jurisdikce, v tomto ohledu je třeba jinak přistupovat k ochraně soukromí na sítích, jako je např. facebook.com, twitter.com nebo linkedin.com, jejichž provozovatelé sídlí mimo evropský systém ochrany soukromí, a sítí v ČR jako např. lide.cz, spoluzaci.cz nebo sousede.cz. Geografická vzdálenost obvykle není faktorem, který významně ovlivňuje potřebu prezentovat, nebo naopak získat určité informace na Internetu, nicméně z pohledu efektivního uplatňování práv jde o zásadní otázku určující rozhodné právo samotné ochrany (k tomu více viz kapitola 5 této práce).

Sociální sítě nicméně disponují celou řadou nesporných výhod. Zatímco tradiční média se obvykle snaží vyvažovat existující soukromé zájmy s právem veřejnosti na informace, ve světě neomezeného šíření informací takovéto vyvažování nehraje tak zásadní roli. Pro případné blogery či jiné podobné tvůrce obsahu tak nemusí být vůbec důležité, co veřejnost vlastně potřebuje vědět, naopak zásadní je především to, co chce osobně sdělit. Prostředí služeb Internetu umožňuje přímou komunikaci s veřejností, přičemž rozhodnutí o tom, zda vůbec a pokud ano, tak jaký typ informací zveřejnit, je na konkrétních uživatelích. Uvedené má však i svá rizika, kterých si nemusí být uživatelé vědomi. Prostředí sociálních sítí může totiž být v celé řadě aspektů velmi zrádné.

Jak ostatně uvádí Gelman,[296] v okamžiku, kdy je prostor pro uveřejňování informací neomezený a je na rozhodnutí konkrétního uživatele, jaký obsah sdělí veřejnosti, začíná dosavadní systém selhávat. Gelman v tomto ohledu zmiňuje případ Megan Meierové, třináctileté uživatelky sítě MySpace.[297] Poté, co se pohádala s kamarádkou, vytvořily matka a chůva zhrzené kamarádky falešný profil mladíka jménem Josh, který předstíral, že je do Megan zamilovaný. Poté, co si vyměnili nesčetně zpráv, „Josh" Megan napsal: „Tento svět by byl bez tebe lepší." Druhého dne spáchala Megan sebevraždu. Rok se o tomto případu nikde nemluvilo, jelikož zločin vyšetřovala policie. Poté, co teta Megan vyprávěla tento příběh deníku St. Louis Dispatch, nastalo mediální šílenství. Noviny se rozhodly, že jméno matky kamarádky Megan Meierové (Lori Drewové, která byla v té době vyšetřována, nezveřejní, aby ochránily soukromí její dcery. Netrvalo ale ani pár hodin a blogeři vložili na různé webové stránky fotografie,

295 V tomto ohledu je nutné zmínit, že technologie jako je facebook.com nebo twitter.com ve svém základním nastavení zpřístupní (tj. automaticky zveřejnují) některé informace uvedené v rámci soukromého účtu. K nastavení soukromí na facebook.com viz www.justit.cz/wordpress/2011/09/08/navod-jak-si-nastavit-lepsi-soukromi-na-facebooku/

296 GELMAN, L. Privacy, free speech, and „blurryedged" social networks. Boston College Law Review. Vol. 50:1315. 2009, s. 1337.

297 Síť MySpace (myspace.com) vznikla v roce 2003 a slouží jako sociální síť pro internetové profily lidí a pro ukládání a sdílení multimédií. Je považována za druhou nejpoužívanější sociální síť na světě, patří společnosti Specific Media. K tomu více viz http://en.wikipedia.org/wiki/Myspace

telefonní čísla, e-mailové adresy a poštovní adresy Drewových. V tomto případě se blogeři a klasická vydavatelství rozhodli ohledně ochrany soukromí nezletilé osoby jinak. Zda bylo z normativního hlediska rozhodnuto správně, je těžké říci. Definice toho, co je zajímavé pro média (angl. „newsworthiness"), je ale v tomto případě stěží k užitku. Lze si představit, že se jak noviny, tak i bloger rozhodli s přesvědčením. Sarah Wellsová, blogerka, která jako první odtajnila jméno a příjmení Lori Drewové, v e-mailu uvedla: „Toho, že jsem Drewovou jmenovala, nelituji." Zajímavé ale je podívat se na institucionální způsobilost těch, kteří rozhodovali. Reportér v novinách byl v událostech třetí osobou a udělal to, co by se dalo nazvat nezaujatým rozhodnutím přijatým na základě historické zkušenosti s řešením obdobných věcí v minulosti. Na druhé straně byla paní Wellsová matka středního věku z Virginie, kterou článek v novinách rozčílil, a tak spustila vlastní vyšetřování za účelem zjištění kontaktních údajů Lori Drewové, přičemž tuto informaci umístila na svém blogu. Jakmile se jméno dostalo ven, byl účinek okamžitý. Další vložené informace odhalily adresu paní Drewové, telefonní číslo a údaje o podnikání. Její dcera musela odejít ze školy, ale díky internetové paměti jí budou záznamy o těchto skutečnostech pronásledovat navěky. Ale i to může být patřičný výsledek. Rozhodnutí, zda mají být osobní údaje Lori Drewové uveřejněny či nikoli, však pochopily noviny a paní Wellsová rozdílně. Pokud by chtěla Lori Drewová nebo její dcera podat proti paní Wellsové žalobu na ochranu osobnosti (soukromí), ptala by se patrně platná právní doktrína, zda byly tyto informace pravdivé a mediálně zajímavé.

Právní doktrína hledání rovnováhy mezi právem na soukromí a svobodou projevu počítá s duálním zveřejněním. Předpokládá se, že prostředníci, tj. zejména institucionalizovaní (tradiční) poskytovatelé obsahu (vydavatelé novin), mají celosvětové auditorium a vytvářejí záznamy trvalého charakteru. Jejich rozhodnutí informaci zveřejnit propůjčuje předmětu zveřejnění určitou hodnotu i ochranu zároveň, což následně představuje důvod, proč se má stát taková informace součástí veřejného záznamu. Tato doktrína předpokládá, že se tato rozhodnutí přijímají proto, aby se některé věci udržely v tajnosti, a to pro svobodu slova znamená akceptovatelnou zátěž. Rozhodnutí o zveřejnění či nezveřejnění určité informace se přijímá za účelem prosazení hodnot svobody slova a projevu, kterých si ceníme.[298] Rozhodnutí paní Wellsové zveřejnit soukromé údaje možná přišlo po hluboké vnitřní debatě o tom, zda jsou tyto informace pro média zajímavé. Ve světě milionů potenciálních novinářů a blogerů ale stačí k tomu, aby se nějaká informace stala veřejnou, i jen jediný méně pečlivě uvažující řečník, který zveřejní soukromé údaje z jakéhokoli důvodu, který bude on sám považovat za patřičný. A to platí jak pro osobní informace o něm samém, tak i o jiných. Pokud je tato informace zajímavá pro média, nemá soukromí na žádnou ochranu nárok.[299]

Zajímavou otázku si v tomto ohledu položil L. Strahilevitz,[300] který řešil, zda principy fungování sociálních sítí mohou soudům poskytnout empirické výsledky, které pro ně budou

298 Viz *Cohen proti Cowles Media Co.,* 501 U.S. 663, 670. 1991, kde bylo mimo jiné rozhodnuto, že tisk není imunní vůči obecně platnému přestupkovému právu, které může být porušeno při shromažďování informací.

299 GELMAN, L., ref. 296.

300 STRAHILEVITZ, L. A. Social Networks Theory of Privacy, 72 *U. Chicago Law Review* 919, 943–46. 2005. Dostupné z: www.law.uchicago.edu/faculty/strahilevitz

mít praktický význam při rozhodování, zda by se určitá skutečnost stala veřejnou informací, pokud by byla sdělena jednomu členovi komunity. Jeho práce vychází z předpokladu, že právo by nemělo zacházet se sdělováním informací jako s duální volbou. Nikdo by se neměl vzdávat své právní ochrany na základě jednorázového poskytnutí informace, pokud by se dalo empiricky prokázat, že by tímto způsobem pravděpodobně nedošlo k rozšíření předané informace mezi obecnou veřejností. Nicméně se řeší stále stejná otázka, zda stojí zato některé poskytování informací podněcovat neboli, jinak řečeno, zda blaho společnosti plynoucí z podporování lidí, aby zveřejňovali své příběhy, převáží újmu, která může být napáchána svobodě projevu v případě, že někomu jinému bude bráněno, aby tytéž příběhy uveřejnil podruhé. Pokud stojí zato zachytit společenskou hodnotu, kterou má poskytování informací, jež vymezuje rozostřenou hranici našich sociálních sítí, pak se právo musí změnit tak, aby chránilo soukromou povahu osobních údajů poté, co budou poskytnuty, a to i nad rámec toho, co navrhuje Strahilevitz.

V roce 2009 se kalifornský odvolací soud v případu Moreno proti společnosti Hanford *Sentinel, Inc.*[301] potýkal s problémem, zda zveřejnění informací na veřejné síti dostupné na celém světě může být považováno za soukromé, pokud původním úmyslem bylo sdělení informace pouze omezenému okruhu osob. Cynthia Morenoová napsala negativní článek o svém rodném městě nazvaný „Óda na Coalingu" a zveřejnila jej na své webové stránce na MySpace. Jeden z čtenářů předal ódu místním novinám – The Coalinga Record, které článek zveřejnily v sekci Dopisy redakci. Autorství bylo přisouzeno Cynthii, a to s uvedením celého jejího jména. Následovala bouřlivá reakce, kdy rodina Morenů začala dostávat dopisy s výhrůžkami smrti a musela zavřít i rodinný obchod. Cynthia a její rodina žalovali noviny, mimo jiné za porušení zákona v případě zveřejnění soukromých údajů. Soud rozhodl, že se o žádné soukromé údaje nejednalo, jelikož „věc, která je již veřejná nebo se veřejnou stala, soukromou není". Soud podotkl, že osoba, která uveřejní informace na Internetu, nemůže mít přiměřené očekávání, že zůstanou soukromé, a rozhodl, že „fakt, že Cynthia očekávala omezený okruh čtenářů, na tomto právním rozboru nic nemění. Vložením článku na MySpace zpřístupnila Cynthia tento text veřejnosti bez jakýchkoli omezení. Velikost jejího potenciálního publika byla obrovská." Lze si jistě představit, že záměrem Cynthie bylo oslovit jiné publikum než městské noviny, ale neměla jak to svým čtenářům naznačit. A i poté, co se rozhodla vložený obsah odstranit ze své stránky na MySpace, už dávno ztratila nad Ódou kontrolu, jelikož si ji někdo jiný stačil zkopírovat. MySpace a ostatní sociální sítě budí zdání publikace s obsahem pro omezený okruh osob a kontroly nad ním, ale ve skutečnosti nemají uživatelé žádné technické prostředky, aby tuto kontrolu mohli uskutečnit, ani právo, které by jejich rozhodnutí potvrdilo.[302]

Je smutnou skutečností, že uživatelé služeb sociálních sítí často uveřejňují neuvěřitelné množství osobních údajů, přičemž obvykle nemají k dispozici prostředky, kterými by sdělili své preference ohledně ochrany soukromí, případně efektivně omezili použití takovýchto údajů ze strany třetích osob. Režim smluvních podmínek jednotlivých sociálních sítí sice nějaká pravidla nastavení soukromí stanoví (viz níže), nicméně lze v tomto ohledu sotva mluvit o (informo-

301 Viz *Moreno v. Hanford Sentinel, Inc.,* 172 Cal. App. 4th 1125. [online] Dostupné z: www.lawlink. com/research/caselevel3/86629

302 GELMAN, L., ref. 296.

vaném) souhlasu uživatelů s jejich obsahem. Zajímavé řešení tohoto problému navrhuje opět Gelman,[303] když uvádí, že bez větších prostředků kontroly mohou být uživatelé vystavováni negativním důsledkům nechtěného pozorování a zkoumání, což může v důsledku vést k tomu, že přestanou být ochotní vytvářet a sdílet obsah. Technické řešení, které umožní uživatelům vyjádřit své preference ohledně ochrany soukromí, pokud jde o obsah, který sdílejí, by bylo cenným prostředkem ochrany soukromí, přičemž by byl zároveň ochráněn zájem spojený se svobodou projevu. Jednou z možností by byl nástroj, který by umožňoval uživatelům u nahraného obsahu vyjádřit a uplatnit své preference ohledně ochrany soukromí. Pomocí tohoto nástroje by uživatelé mohli vyjádřit své úmysly označením nahraného obsahu ikonou, která by s těmito referencemi okamžitě seznámila třetí osoby. Na základě licence Creative Commons[304] by tento nástroj poskytoval třetím osobám okamžitou vizuální odezvu o preferencích majitele obsahu a odkaz na webovou stránku, která by obsahovala podrobnosti o způsobu, jakým lze tento obsah použít nebo sdílet. Zároveň by umožňovala třetím osobám požádat osobu, která tento obsah uveřejnila, aby odstranila to, co nechtějí, aby bylo zveřejněno.

Existující společenské normy v on-line prostředí a související obecné právní zásady tak nepřímo dotvářejí určité preference člověka ve vztahu k jeho požadavkům zachovávat soukromí. Webové stránky také disponují vlastností realizované prostřednictvím tzv. metadat,[305] jež mohou vyhledávačům poskytnout informaci, že by příslušný obsah neměl být dále šířen, což umožňuje kvalitativně vyšší předpoklad garance soukromí (viz výše). Pokud je tedy příslušná webová stránka označena konkrétním metatagem[306] jako svého druhu soukromá, vyhledávače tuto stránku samy obvykle dobrovolně přeskočí a nezahrnou ji do svých databází.[307] Určení takovéto povahy webové stránky tak může být velmi významné z pohledu rozsahu právní ochrany. Podobné systémy založené na principu metadat zaměřené na individuální vložené obsahy nebo obrázky by

303 GELMAN, L., ref. 296, s. 1338.

304 Asociace Creative Commons dává uživatelům Internetu jednoduchý prostředek na „označení" obsahu, který nahrávají on-line, různými preferencemi ohledně autorského práva. Takže namísto standardních pravidel, kterými se automaticky označují autorská a původní díla, uživatelé „označí" svůj obsah tak, že například povolí jeho sdílení, ale pouze s uvedením svého autorství a pouze nekomerčním uživatelům. Tyto „značky" obsahují jednak text, který je viditelný pro ostatní uživatele Internetu, jednak kód, který dokážou přečíst technologie, jako jsou vyhledávače. Asociace Creative Commons v současné době nabízí šest různých licencí, které umožňují uživatelům vyjádřit různé preference ohledně použití svých děl.

305 Metadata jsou strukturovaná data o datech. Příkladem je katalogizační lístek v knihovně, obsahující data o původu a umístění knihy: jsou to data o datech v knize uložená na lístku. Metadata mohou sloužit např. k snadnému vyhledávání. K tomu více viz http://en.wikipedia.org/wiki/Metadata

306 Metatagy jsou zvláštní formy metadat, které se píšou do hlavičky webové stránky, a to např. za účelem jejich bližšího popisu či konkretizace obsahu. Např. Google akceptuje metatag googlebot. Vyhledávači je tím poskytnuta informace o tom, že u konkrétní webové stránky je požadován zákaz další archivace a výpisu úryvků, např. takto: <meta name="googlebot" content="nosnippet,noarchive">

307 Obdobou metatagů je např. protokol (soubor) „robots.txt", který vyhledávače hledají na indexovaných webových stránkách. Tento protokol poskytuje informaci pro zakázání přístupu robotům. Používá se v případech, kdy je potřeba procházení určité stránky či části webu robotům zakázat (např. placené články ve zpravodajských archivech, soukromá či interní diskusní fóra, výsledky vyhledávání položek v e-shopu apod.). K syntaxi i využití tohoto standardu více na http://napoveda.seznam.cz/cz/robots.txt.html

mohly vytvořit obecně přijímanou společenskou normu v případě preferencí ochrany soukromí. Jak komerční, tak i soukromí uživatelé si jistě více rozmyslí porušování preferencí ochrany soukromí, když se tyto preference objeví hned vedle příslušného obsahu. Posílení ochrany soukromí pravděpodobně podpoří dobrovolné sdílení obsahu, protože právě o to jde. Tento model je třeba uskutečnit tak, aby neomezoval uživatele pouze u určitých webových stránek nebo prostředí. Spousta obsahu vytvořeného uživateli je již dostupná, aniž by se uživatelé, kteří si chtějí tento obsah prohlédnout, museli přihlašovat, a opatření v rámci *„gate-keepingu"*, neboli procesu výběru informací vpuštěných do médií, dokážou jen těžko zarazit neomezeně proudící tok obsahu mezi komunitami a počítači.[308] Aby tento nástroj pro ochranu soukromí mohl být účinný, měl by být stejně mobilní. A současně platí, že má-li být tento nástroj přijat v široké míře a využíván v plném rozsahu, měl by být všem spotřebitelům uživatelsky vytvořeného obsahu k dispozici pouhým kliknutím, a to bez ohledu na to, zda jsou, či nejsou členy nebo ověřenými uživateli určitého prostředí, v němž je tento nástroj zaveden. Stejně tak by preference ochrany soukromí vyjádřené pomocí značky (tagu) neměly spustit jejich povinné vynucování technickými prostředky. Takové smrtelné tlačítko *„kill switch"* u obsahu by podkopalo základní cíl podpory sdílení obsahu a závažným způsobem by zmrazilo vyjadřování názorů po síti. Předpokladem prosté přátelské úcty je ctít preference ochrany soukromí druhých, dokud se tyto preference nedostanou do konfliktu se silnějšími zájmy nebo neohrozí hodnoty svobody projevu. Pokud taková situace nastane, mělo by být možné preference druhého uživatele „přebít". Automatické vynucování vyjádřených preferencí ochrany soukromí by tuto křehkou rovnováhu narušilo. Nástroj umožňující uživatelům vyjádřit své preference ohledně obsahu, který vkládají na Internet, by mohl vést i k dalším změnám práva na ochranu osobních údajů. Při řešení zásahů do soukromí se v tomto smyslu ve Spojených státech používá svého druhu test směřující ke zjištění, zda by rozumná osoba považovala konkrétní poskytnutí informací za urážlivé.[309] Lze jistě souhlasit, že předmětný postup je v mnoha směrech vhodný, testování má smysl zejména tam, kde by bylo příliš obtížné požadovat, aby si uživatelé před zveřejněním informace vypočítali konkrétní míru citlivosti určité osoby. Kdyby ale uživatelé měli možnost označit obsah značkou své preference nebo získali prostředky jak dát ostatním vědět, že určitý obsah, který tito lidé zveřejnili, dle jejich názoru narušuje soukromí, bylo by možné si představit, že by se při řízení o zásazích do soukromí začalo přihlížet k očekávání jednotlivců ohledně ochrany jejich soukromí.

Pro úplnost je třeba konstatovat, že zásadním problémem realizace práv uživatelů (fyzických osob) v rámci sociálních sítí je skutečnost, že jejich provozovatelé jsou mimo faktický (teritoriální) dosah českého či evropského systému ochrany osobních údajů, včetně reálné možnosti postihu těchto provozovatelů formou autoritativního rozhodnutí orgánů veřejnoprávní ochrany. V tomto ohledu lze mimo jiné zmínit skutečnost, že se evropské sídlo Facebooku (viz požadavek Směrnice i českého zákona na správce, který je usazen mimo území EU) nachází v Dublinu, a působnost (pravomoc) v oblasti ochrany dat tak vykonává irský úřad pro ochranu osobních údajů (nad uživateli sítě mimo Spojené státy a Kanadu). V souvislosti s touto působ-

308 5. září 2007 vyhlásil Facebook, že profily, které mají volbu pro ochranu osobních údajů nastavenou na „veřejné", mohou největší vyhledávače indexovat a prohledávat.

309 GELMAN, L., ref. 296, s. 1337.

nosti byla společnosti Facebook adresována řada žádosti o zpřístupnění osobních údajů vložených uživateli na základě evropského práva, spor o vyhodnocení těchto žádosti v současné době probíhá (viz iniciativa Europe v. Facebook),[310] podobně jako diskuse nad povahou a závazností pravidel používání obsahu.[311]

4.4.10 Veřejně přístupné internetové databáze a registry (obchodní rejstřík, katastr nemovitostí a registr doménových jmen WHOIS)

Spolu s rostoucí důležitostí Internetu nabývá na významu také celá řada specifických internetových databází a registrů, které lze definovat prostřednictvím celé řady kritérií.[312] Za nejdůležitější lze patrně považovat definiční kritérium konkrétní povahy právní ochrany jejich obsahu, resp. chráněnosti,[313] kde je právními předpisy vyžadováno určité omezení přístupu a dalšího nakládání s těmito údaji, případně jde o databáze svou povahou nechráněné, které zpravidla obsahují takové informace, kde je dán veřejný zájem na jejich přístupnosti a s tím související ničím neomezená možnost jejich dalšího šíření.[314]

Zvláštním, byť zároveň také zcela typickým, příkladem chráněných databází jsou ty, jež obsahují osobní údaje. Vzhledem k jejich silné veřejnoprávní ochraně je z pohledu existence obvykle lhostejné, zda jde o databáze provozované ve veřejném zájmu, na principu publicity, tj. obvykle ze zákona, případně zda jde o databáze soukromé, tj. realizované obvykle na základě jedné ze zákonných výjimek, zejména pak smlouvy.

Za účelem transparentnosti a publicity jsou např. zveřejňovány údaje o podnikatelích (fyzických osobách) v obchodním rejstříku, rejstříku živnostenského podnikání nebo insolvenčním rejstříku, kde se obecně vychází z toho, že je požadavek ochrany osobních údajů do jisté míry oslaben z důvodu upřednostnění kritéria transparentnosti obchodního styku a s tím spojené nezbytnosti jeho publicity. Podnikatel jako fyzická osoba (statutární orgán, společník atd.), byť stále zůstává subjektem ochrany osobních údajů, si tak má být vědom skutečnosti, že zápis jeho osobních údajů je obligatorní náležitostí vzniku jeho dalších práv, přičemž musí počítat s tím, že tyto údaje budou za tímto účelem poskytnuty veřejnosti, a to na základě principu transparentnosti. Přístupnost těchto databází tak vyplývá přímo z právního předpisu.[315] Po-

310 Dostupné z: http://europe-v-facebook.org/EN/en.html

311 K aktuálnímu vývoji ve smluvních podmínkách facebook.com srovnej www.lupa.cz/clanky/facebook-meni-pravidla-soukromi-cokoli-udelate-muze-pouzit-k-zobrazeni-reklam/, případně k dalšímu užití obsahu news.cnet.com/8301-13578_3-57559710-38/instagram-says-it-now-has-the-right-to-sell-your-photos/

312 Např. dle formy jejich nosiče, povahy subjektu spravujícího databázi (veřejný, soukromý, komerční, nekomerční atd.), dle struktury a složitosti vyhledávání (abecední, jazykové, encyklopedické, vědecké atd.).

313 Tj. např. databáze obsahující díla chráněná právem duševního vlastnictví, obchodní tajemství, státem utajované informace, případně osobní údaje atd.

314 Tj. např. databáze obsahující právní předpisy, statistické údaje, metodické či úřední pokyny, soudní či správní rozhodnutí atd.

315 Viz např. § 28 obchodního zákoníku. Ministerstvo spravedlnosti ČR za tímto účelem zřídilo aplikaci umožňující přístup k informacím v obchodního rejstříku. Účelem této aplikace je poskytnout rychlé a obecně dostup-

dobným způsobem jsou zveřejňovány osobní údaje v dalších obdobných databázích, jako např. v katastru nemovitostí, který byl zřízen za účelem ochrany práv k nemovitostem, případně k daňovým a poplatkovým účelům, k ochraně životního prostředí, ochraně kulturních památek.[316] Konkrétní účel nemá ve vztahu k ochraně osobních údajů fyzických osob deklaratorní povahu, naopak je zcela zásadním a důležitým kritériem pro stanovení dalšího režimu zpracovánítěchto zveřejněných osobní údajů ve smyslu správněprávní ochrany osobních údajů, případně civilněprávní agendy ochrany osobnosti. Skutečnost, že jsou tyto údaje zveřejněny na základě právního předpisu, totiž sama o sobě neznamená, že jsou takto zveřejněné osobní údaje zcela vyjmuty z ochrany ve smyslu zákona. Zákon o ochraně osobních údajů výslovně počítá s tím, že zveřejněné osobní údaje[317] podléhají nadále jeho ochraně, v tomto ohledu pouze stanoví právní titul k dalšímu zpracování (§ 5 odst. 2 písm. d), a to za podmínky, že tím nebude dotčeno právo na ochranu soukromého a osobního života subjektu údajů (viz kapitola 4.4.7).

Stranou režimu ochrany osobních údajů tak nestojí ani zvláštní evidence údajů o držitelích internetových domén a dalších osobách (databáze WHOIS). Tuto databázi vede v zásadě každý správce národních i generických domén nejvyššího řádu, a to obvykle za účelem zajištění transparentnosti stavu registrace doménových jmen, včetně údajů o subjektech odpovědných za provozování služeb nebo poskytování obsahu pod touto doménou. Databáze WHOIS je obvykle spravována na základě smlouvy o registraci doménových jmen, resp. pravidel registrace konkrétního správce.

Z pohledu správněprávní úpravy ochrany osobních údajů, jakož i souvisejícího civilněprávního pojetí této ochrany je tedy zveřejňování osobních údajů opíráno především o právní titul uvedený v ustanovení § 5 odst. 2 písm. b) ZoOÚ. Jde totiž o zpracování, které je nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů.[318] V rámci existujícího vícestranného právního vztahu realizovaného zejména mezi správcem tohoto registru (v České republice sdružení CZ.NIC), držitelem doménového jména, registrátorem a případně dalšími osobami (např. administrativním kontaktem), jsou za účelem transparentnosti těchto vztahů a zajištění technické funkčnosti zveřejňovány osobní údaje v rozsahu jméno a příjmení, e-mailová adresa a adresa trvalého bydliště. Sdružení CZ.NIC je tak správcem těchto osobních údajů centrálního registru, registrátor pak jejich zpracovatelem. Pravidla registrace pak obvykle umožňují, aby některé osobní údaje byly označeny jako skryté (viz např. jméno, e-mail, telefon, fax, daňový identifikátor, případně za splnění předchozí podmínky validace službou mojeID také adresu, apod.), takové údaje nejsou zveřejňovány, byť v samotném registru WHOIS zůstávají nadále vedeny a mohou být v určitých případech poskytnuty třetím osobám na základě jejich žádosti. V souvislosti s touto formou ochrany osobních údajů ve formě omezení jejich dalšího šíření

né základní informace o jednotlivých subjektech zapsaných v obchodním rejstříku. K tomu více viz www. justice.cz/xqw/xervlet/insl/index?sysinf.@typ=staticPages&sysinf.@strana=operationTerms

316 K tomu srovnej § 1 odst. 2 zákona č. 344/1992 Sb., o katastru nemovitostí České republiky, v platném znění.

317 Za zveřejněný osobní údaj se považuje osobní údaj zpřístupněný zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu (§ 4 písm. l) zákona o ochraně osobních údajů).

318 K tomu viz Pravidla registrace doménových jmen v ccTLD .cz (v platnosti od 1. 12. 2012). [online] Dostupné z: www.nic.cz/files/nic/doc/Pravidla_registrace_CZ_DSDng_20121201.pdf

je třeba zmínit, že někteří registrátoři domén z těchto důvodů umožňují službu maskování databáze WHOIS, kde je jako držitel uveden subjekt odlišný od skutečného držitele (obvykle právnická osoba), který pak vystupuje jako držitel domény.[319]

Z pohledu existence zákonných právních titulů nezbytných pro zpracování osobních údajů lze rovněž uplatnit titul uvedený v ustanovení § 5 odst. 2 písm. e), tedy nezbytnost takovéhoto zpracování (zveřejňování) pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby, kde je nutné respektovat požadavek bezrozpornosti takového zveřejňování s právem subjektu údajů na ochranu jeho soukromého a osobního života.

4.4.11 Registry dlužníků

Za poměrně praktické a aktuální téma lze např. považovat zveřejňování dlužníků v prostředí Internetu, které je poměrně často postihováno pro rozpor se zákonem o ochraně osobních údajů. Zatímco ze soukromoprávní povahy pohledávky vyplývá, že s ní je možné dále různě nakládat, tj. zejména ji prodat, tento prodej inzerovat, což jistě není možné úspěšně realizovat bez zveřejnění údajů tuto pohledávku specifikujících (jako např. jméno a příjmení dlužníka, výši této pohledávky, její splatnost apod.), zásady ochrany osobních údajů zveřejňovat takovéto údaje bez souhlasu jejich subjektu to nedovolují. Existuje zde tedy možný rozpor mezi soukromoprávní úpravou obsahující výkon práva věřitele s pohledávkou dále nakládat (typicky ji prodat) a úpravou veřejnoprávní, která pod sankci chrání zveřejňování osobních údajů bez souhlasu subjektu těchto údajů. Jde však o rozpor řešitelný výkladem, a to zejména formou sledování a poznání skutečného a pravého účelu zveřejnění těchto údajů, resp. zkoumání míry nadbytečnosti rozsahu zveřejňovaných údajů, denunciační povahy takovéhoto zveřejnění, zastřenost skutečného účelu apod.

Obecně lze uvést, že Úřad konzistentně považuje ve své správní praxi zveřejnění nebo zpřístupnění osobních údajů dlužníků za nátlakové jednání, kterým jsou porušována ustanovení článku 10 Listiny základních práv a svobod. Jakkoliv jde o poměrně silné tvrzení, opírá se patrně o denunciační povahu takovéhoto jednání, což je v mnoha směrech častá praxe. Samotné zveřejňování nebo zpřístupňování osobních údajů v souvislosti s nesplněním závazku (typicky pohledávky), považuje Úřad za nepřípustné zasahování do soukromí osob, neboť zpřístupněním takového údaje, který byl získán na základě soukromoprávního vztahu, může dojít k poškození dobrého jména dlužníka (je nutné podotknout, že může probíhat spor o platnost pohledávky věřitele, zápis může mít šikanózní povahu, vzhledem k tomu, že provozovatelé těchto registrů neověřují podklady, na základě kterých byla fyzická osoba do seznamu zapsána atd.) v mnoha dalších vztazích, jak soukromoprávních, tak i veřejnoprávních. Zpřístupnit osobní údaje bez souhlasu subjektu údajů (dlužníka) lze v tomto případě pouze oprávněným osobám. V ostatních případech může správce osobní údaje zveřejnit nebo zpřístupnit jen na základě informovaného

319 Součástí této služby pak obvykle bývá přidělená e-mailová adresa, která slouží ke kontaktování původního majitele domény.

souhlasu (viz výše) subjektu údajů (dlužníka).[320] Lze tak konstatovat, že pokud nebyl dán souhlas těchto dlužníků s jejich zveřejněním v takovýchto seznamech, jde o zveřejnění v rozporu se zákonem o ochraně osobních údajů. Před případným kontaktováním Úřadu je žádoucí, aby dotčená osoba požádala provozovatele o vysvětlení a zároveň o provedení výmazu svých osobních údajů, a to s odkazem na rozpor takového uveřejnění v seznamu s platnou legislativou. Pokud nebude žádosti vyhověno, může se osoba, jejíž osobní údaje jsou neoprávněně zveřejňovány v seznamu dlužníků, obrátit na Úřad se stížností, přičemž pro efektivní vyřízení věci, je spolu se stížností či podnětem vhodné zaslat veškeré možné relevantní dokumenty k posouzení (screen webu, uvedení odkazu apod.), včetně doložení výzvy na odstranění osobních údajů vůči provozovateli seznamu dlužníků.[321]

4.4.12 Zvláštní režimy zpracování osobních údajů s využitím cloud computingu

Na ochranu osobních údajů v rámci využití *cloud computingu*[322] při jejich zpracování je třeba nahlížet zcela konvenčními kritérii, tj. optikou standardních požadavků, které na ochranu těchto údajů stanoví zákon. Při aplikaci této úpravy je nutné klást zvýšený důraz především na smluvní zajištění, kvalitativní záruky ve vztahu k zajištění těchto údajů, jakož i samotnou transparentnost procesu zpracování (z pohledu odpovědnosti). Z pohledu správce osobních údajů, tedy z pozice subjektu, který s údaji primárně nakládá a rozhoduje o druzích prostředků, které budou pro zpracování osobních údajů použity, tak nutno nahlížet na řešení správy pomocí cloud computingu jako na svého druhu pronájem výpočetního výkonu či úložného prostoru poskytovatele.

Ve většině případů bude poskytovatel cloud computingu zpracovatelem ve smyslu § 4 písm. k) ZoOÚ, ve znění pozdějších předpisů. To však nezbavuje správce osobních údajů (tedy subjekt, který si služby v rámci cloud computing najímá) povinností, které jsou na něj kladeny zákonem o ochraně osobních údajů, a v této souvislosti je nutné zmínit zejména povinnost stanovenou v § 13 zákona, která se týká zabezpečení osobních údajů. Je tak na správci, aby analyzoval dopady řešení využití cloud computingu (analýza rizik), zajistil adekvátní opatření na své straně (např. šifrování dat) a aby si uzavřením smluvních vztahů s případným poskytovatelem služeb cloud computingu ošetřil veškeré podmínky zpracování (zajištění odpovídající úrovně zabezpečení, odpovědnost poskytovatele služeb a zpracovatele za jeho případná selhání v oblasti ochrany osobních údajů atd. apod.).[323]

S ohledem na uvedené výše je nezbytné klást zvýšené nároky na kvalitativní stránku zajištění všech právních i organizačních otázek souvisejících s realizací služeb v rámci cloud computingu, zejména pak formální a obsahovou kvalitu příslušné smlouvy, kde lze minimálně

320 K tomu srovnej související stanovisko č. 1/2011, ref. 294.

321 K tomu více viz příslušný názor Úřadu (rubrika: Otázky kladené v souvislosti se zákonem o ochraně osobních údajů. Dostupné z: http://uoou.cz/uoou.aspx?menu=14&loc=331#a60).

322 K tomu více viz http://en.wikipedia.org/wiki/Cloud_computing

323 K tomu více viz příslušný názor Úřadu (rubrika: Otázky kladené v souvislosti se zákonem o ochraně osobních údajů. Dostupné z http://uoou.cz/uoou.aspx?menu=14&loc=331#a71).

doporučit důsledné zakotvení povinnosti uchování zpracovávaných osobních údajů v zemích EU (viz výše).

4.4.13 Internet a právo být zapomenut

O vztahu práva na soukromí a Internetu toho lze napsat mnoho, obvykle však nepůjde o pohled optimistický, ale spíše pesimistický a kritický. Tento zjevně negativní dopad Internetu do intimní oblasti člověka nelze zcela přehlížet, naopak je nutné se zamyslet nad dalším vývojem v této oblasti. Lidstvo v posledním období své historie o sobě shromažďuje dosud nevídané množství dat, navíc v mnoha směrech až příliš snadno dostupných, a to i tam, kde se dostupnost jeví jako zcela nevhodná nebo minimálně neúčelná. Důsledkem těchto technologických změn vzniká masivní redundance údajů, která je netypická nejenom ve smyslu hledisek kvantitativních (rozsahem) a kvalitativních (snadno zaznamenatelná, šiřitelná a dostupná formou elektronického záznamu), ale především také ve vztahu k jejich časovému působení.

Z tohoto důvodu lze považovat za nezbytnou takovou ochranu práv, která bude dopad těchto technologických změn ve formě negativního působení[324] na soukromí člověka efektivně regulovat. Touto cestou se v nedávné době vydala i Evropská unie, která dne 25. ledna 2012 představila návrh nařízení[325] o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů). Důvodem pro tento návrh je především snaha reagovat na rychlý technologický rozvoj, který staví ochranu osobních údajů před nové výzvy. Objem sdílených a shromažďovaných údajů dramaticky roste. Technologie umožňují jak soukromým společnostem, tak orgánům veřejné moci využívat při provádění jejich činnosti osobní údaje v nebývalém rozsahu. Jednotlivé osoby stále častěji zveřejňují své osobní údaje i v globálním měřítku. Technologie tak mění jak ekonomiku, tak i společenský život člověka. V tomto ohledu je jistě významné budovat důvěryhodné prostředí Internetu. Nedostatek důvěry vede k tomu, že se spotřebitelé zdráhají nakupovat on-line a využívat nové služby. Opačný přístup by patrně vedl k zpomalení rozvoje inovativního využívání nových technologií. Ochrana osobních údajů proto hraje důležitou roli v Digitální agendě pro Evropu[326] a ještě obec-

324 Podle nedávného průzkumu z června 2011 (Eurobarometru č. 359, Attitudes on Data Protection and Electronic Identity in the European Union) považuje 74 % Evropanů odhalování osobních informací ve stále větší míře za součást moderního života. Hlavním důvodem k odhalení informací je přístup k internetové službě. To se týká jak uživatelů sociálních sítí a stránek pro sdílení dat (61 %), tak lidí, kteří na internetu nakupují (79 %). Při registraci na sociální síti nebo registraci za účelem využití internetové služby zná více než polovina uživatelů internetu (54 %) podmínky sběru údajů a ví, k čemu budou jejich údaje dále využívány. Jen o něco více než čtvrtina uživatelů sociálních sítí (26 %) a dokonce ještě méně lidí, kteří nakupují na internetu (18 %), má pocit, že mají své údaje zcela pod kontrolou.

325 Za nejvhodnější právní nástroj pro definování rámce pro ochranu osobních údajů v Unii se považuje nařízení. Na základě přímé použitelnosti nařízení podle článku 288 Smlouvy o fungování Evropské unie (SFEU), se omezí právní nejednotnost a zvýší právní jistota tím, že se zavede harmonizovaný soubor základních pravidel, zlepší ochrana základních práv jednotlivců a přispěje k fungování vnitřního trhu.

326 Dostupná [online] z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?ur=iCOM:2010:0245:FIN:CS:PDF

něji ve strategii[327] EU pojmenované „Evropa 2020".[328] Tato strategie, pokud jde o její část týkající se ochrany osobních údajů, má své základy ve zprávě Evropského parlamentu ze dne 6. července 2011, která podpořila přístup Komise k reformě rámce pro ochranu údajů.[329] Rada EU přijala dne 24. února 2011 závěry, v nichž v široké míře podporuje úmysl Komise reformovat rámec pro ochranu údajů a souhlasí s mnoha prvky jejího přístupu. Evropský hospodářský a sociální výbor obdobně podpořil cíl Komise zajistit jednotnější uplatňování pravidel EU pro ochranu údajů ve všech členských státech a odpovídající přezkum Směrnice.[330]

Předmětný návrh respektuje dosavadní obecné zásady, nicméně stávající systém ochrany upravuje tak, aby lépe reagoval na výzvy, které s sebou nese rychlý vývoj nových (on-line) technologií a rostoucí globalizace. Jedním z hlavních důvodů pro vytvoření nového právního rámce byla především existující nejednotnost ochrany osobních údajů v EU, která ve svém důsledku v řadě případů vedla k právní nejistotě a celkové nedůvěře v on-line prostředí, jakož i obavě z rizik spojených se sdílením osobních údajů. Zpracovávání a sdílení osobních údajů je přitom pro současnou ekonomiku nezbytným předpokladem pro uskutečňování obchodních transakcí nejrůznějšího charakteru. Účelem nového nařízení je tedy vytvořit takové právní prostředí, které by zajišťovalo maximální právní jistotu jednotlivcům využívajícím elektronických služeb. Dalším důvodem byla složitá pravidla týkající se mezinárodního předávání osobních údajů, která tvoří významnou překážku při provádění některých činností.

Samotná právní stránka návrhu spočívá na několika pilířích, klíčový je zejména rozšířený katalog práv subjektu údajů, včetně navazujících povinností správce (zpracovatele) údajů včetně zvláštních požadavků na organizační strukturu jednotlivých kategorií správců a zpracovatelů. Návrh nařízení dále zavádí speciální pravidla pro zpracovávání údajů v konkrétních kategoriích (osobní údaje dětí, zaměstnanců apod.). V souvislosti s tím pak tento návrh zavádí nový institut, kterým je inspektor ochrany osobních údajů.

Z rozsáhlého katalogu práv zakotvených v návrhu tohoto nařízení lze považovat za dominantní především právo být zapomenut (right to be forgotten),[331] případně právo na výmaz,[332] jakožto svého druhu určité součásti lidské i právní[333] podstaty. Návrh v tomto ohledu

327 Viz http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:CS:PDF

328 V čl. 16 odst. 1 SFEU, který byl zaveden Lisabonskou smlouvou, je zakotvena zásada, že každý má právo na ochranu osobních údajů, které se jej týkají. Kromě toho Lisabonská smlouva zavedla s čl. 16 odst. 2 SFEU zvláštní právní základ pro přijetí pravidel ochrany osobních údajů. V článku 8 Listiny základních práv EU je ochrana osobních údajů zakotvena jako základní právo.

329 Usnesení EP ze dne 6. července 2011, o komplexním přístupu k ochraně osobních údajů v EU (2011/2025).

330 Viz příslušný návrh nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů). K návrhu předmětného nařízení jsou k dispozici konzultační dokumenty dostupné z: http://ec.europa.eu/justice/ newsroom/data-protection/news/120125_en.htm a řada dalších dostupných podkladů: http://ec.europa.eu/justice/data-protection/index_en.htm

331 V tomto ohledu vřele doporučuji velmi výstižnou prezentaci doc. JUDr. Radima Polčáka, Ph.D., na téma informačního fetišismu a práva být zapomenut (Information fetishism and the art of forgiving) přednesenou v rámci TEDxBrno. Dostupné [online] z: www.youtube.com/watch?v=zS4deaFRBKI

332 Z angl. „right to be forgotten and to erasure".

333 I v právních institutech je patrný, byť v mnoha ohledech zcela jinak orientovaný, režim „zapomínání", viz

stanoví právo na opravu osobních údajů, a „právo být zapomenut“, pokud uchovávání těchto údajů není v souladu s tímto nařízením (návrhem). Subjekty údajů by především měly mít právo na to, aby jejich osobní údaje byly vymazány a nebyly dále zpracovávány, pokud tyto údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány, pokud subjekty údajů odvolaly svůj souhlas se zpracováním nebo pokud vznesly námitku proti zpracování osobních údajů, které se jich týkají, nebo pokud zpracování jejich osobních údajů není slučitelné s tímto nařízením z jiných důvodů. Toto právo je obzvláště důležité v případech, kdy subjekt údajů dal svůj souhlas v dětském věku, aniž by si byl v plném rozsahu vědom rizik spojených se zpracováním údajů, a později chce tyto osobní údaje zejména na Internetu odstranit.[334] Za účelem posílení „práva být zapomenut“, počítá návrh s rozšířením práva na výmaz takovým způsobem, aby správce, který zveřejnil osobní údaje, měl povinnost informovat třetí strany, které tyto údaje zpracovávají, že subjekt údajů požaduje vymazání veškerých odkazů na své osobní údaje či veškerých kopií nebo replikací těchto osobních údajů. Podle této úpravy by měl správce a zpracovatel ve vztahu k údajům, za jejichž zveřejnění je zodpovědný, přijmout veškerá rozumná opatření, včetně technických, aby toto informování třetích stran zajistil. V souvislosti se zveřejněním osobních údajů třetí stranou by měl odpovědnost nést správce, pokud třetí straně zveřejnění povolil.

Další požadavky klade návrh na organizační strukturu správce a zpracovatele, zejména pak ve vztahu k základní povinnosti jmenovat inspektora ochrany údajů, a to v těch případech, kdy zpracování provádí orgán veřejné moci či veřejnoprávní subjekt nebo zpracování provádí podnik zaměstnávající 250 či více osob (v tomto případě může skupina takovýchto subjektů jmenovat jediného inspektora) nebo hlavní činnost správce nebo zpracovatele spočívá ve zpracovávání údajů, které kvůli své povaze, rozsahu nebo účelu vyžadují pravidelné a systematické sledování subjektů údajů. Postavení inspektora vyplývá z článku 36 návrhu, který stanoví, že inspektor musí být náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů. Správce nebo zpracovatel zajistí, aby inspektor ochrany údajů plnil své povinnosti a úkoly nezávisle a nepřijímal žádné pokyny k výkonu své funkce. Inspektor ochrany údajů je přímo podřízen vedení správce nebo zpracovatele. Správce nebo zpracovatel jsou inspektorovi ochrany údajů při plnění jeho úkolů nápomocni a poskytují mu dostatečné personální a objektové zajištění a jakékoliv další zdroje potřebné k výkonu jeho povinností a úkolů. Mezi hlavní úkoly inspektora patří:

a) informovat správce nebo zpracovatele a udílet jim rady, pokud jde o jejich povinnosti plynoucí z tohoto nařízení, a vést dokumentaci o této činnosti a obdržených odpovědích,
b) sledovat provádění a uplatňování politik správce nebo zpracovatele souvisejících s ochranou osobních údajů včetně svěřování odpovědnosti a školení pracovníků zapojených do zpracovávání a souvisejících auditů,

---

např. význam a koncepce promlčení v soukromém právu, případně promlčení a zahlazení odsouzení v právu trestním, prekluze atd. apod.

334 Další uchovávání údajů by však mělo být přípustné, pokud je to nezbytné pro účely historiografického, statistického a vědeckého výzkumu, z důvodů veřejného zájmu v oblasti veřejného zdraví, pro výkon práva na svobodu projevu, pokud to vyžaduje zákon nebo pokud existuje důvod pro omezení zpracování údajů namísto jejich výmazu.

c) sledovat provádění a uplatňování tohoto nařízení, zejména požadavků týkajících se ochrany údajů již od návrhu, standardního nastavení ochrany údajů a bezpečnosti údajů a požadavků týkajících se informovanosti subjektů údajů a jejich žádostí o výkon jejich práv podle tohoto nařízení,
d) zajišťovat vedení dokumentace,[335]
e) sledovat dokumentaci a ohlašování a oznamování případů narušení bezpečnosti osobních údajů,[336]
f) sledovat, zda správce nebo zpracovatel vypracovávají posouzení dopadu na ochranu údajů a žádají o předchozí povolení nebo předchozí konzultaci, jsou-li těmito úkony povinováni,[337]
g) sledovat reakce na žádosti orgánu dozoru a v mezích svých pravomocí inspektora ochrany údajů spolupracovat s orgánem dozoru, pokud o to požádá, nebo pokud k tomu dá podnět inspektor ochrany údajů,
h) působit jako kontaktní osoba pro orgán dozoru v záležitostech souvisejících se zpracováváním, a je-li záhodno, vést s orgánem dozoru konzultace z vlastní iniciativy.[338]

Za významnou změnu oprati dosavadní úpravě je třeba označit samotnou územní působnost[339] předmětného návrhu nařízení, která se vztahuje na zpracování osobních údajů těch subjektů údajů, které mají bydliště v EU, ze strany správce, který není usazen v EU, pokud zpracování údajů souvisí buď s nabídkou zboží nebo služeb těmto subjektům údajů v EU nebo s monitorováním jejich chování (čl. 3, odst. 2). Tito správci mají v určitých případech podle čl. 25 povinnost jmenovat svého zástupce se sídlem v jednom z členských států, v němž trvale žijí subjekty, jejichž údaje jsou zpracovávány pro výše uvedené účely.

Celkově lze shrnout, že navrhované nařízení je v mnoha směrech revolučním počinem, byť naráží na celou řadu aplikačně zcela zásadních otázek, a to včetně samotné aplikovatelnosti (např. vzhledem k technicistní povaze šíření dat ve vztahu k důsledné realizaci práva být zapomenut). Navíc není v mnoha směrech zcela jasné, proč je dosavadní relativně komplexní a stálé efektivněji fungující úprava nahrazována úpravou novou. Existující počiny Evropské komise (viz výše) se nezdají být v tomto ohledu přesvědčivé. Jisté dílčí změny jsou jistě důsledkem rozvoje nových technologií, ty však mohly být dostatečně promítnuty do dosavadní Směrnice. V tomto ohledu je nezbytné reflektovat skutečnost, že formou nařízení navrhovaná právní úprava nezakládá nijak zásadní změnu či posílení postavení subjektu ochrany osobních údajů, naopak, v některých směrech zavádí celou řadu nových institutů, které svou povahou povedou spíše ke snížení právní jistoty účastníků souvisejících právních vztahů, včetně zvýšení nákladů na důslednou aplikaci právní úpravy a souvisejících administrativních nákladů.

335 Viz článek 28 návrhu upravující povinnost správce a zpracovatele vést podrobnou dokumentaci o všech zpracováních.
336 Viz článek 31 a 32 návrhu.
337 Viz článek 33 a 34 návrhu.
338 Viz článek 37 návrhu.
339 Toto nařízení se vztahuje na zpracování osobních údajů správcem, který není usazen v EU, ale na místě, kde se vnitrostátní právní předpisy členského státu uplatňují na základě mezinárodního práva veřejného.

4.5 Regulace soukromí a důvěrnosti komunikací v oblasti elektronických komunikací

Jak již bylo zmíněno výše, jedním z nejvýznamnějších právních předpisů, který poskytuje obecnou ochranu soukromí člověka, je Listina, která ve svém článku 13 uvádí, že nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením. Rovněž ustanovení čl. 10 odst. 2 Listiny uvádí, že každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života. Tato ustanovení jsou však poměrně obecná, nemusí být vždy zřejmé, jak velkému okruhu údajů, resp. písemností a záznamů, je tato ochrana poskytována. V tomto ohledu lze ale vycházet z dosavadní soudní praxe, zejména pak souvisejících nálezů Ústavního soudu,[340] podle které toto ustanovení chrání nejenom vlastní obsah zpráv a záznamů (ať již jde o zprávy či záznamy telefonické, elektronické či jiné), ale také veškeré související údaje (např. údaje o volaných číslech, datu a čase hovoru, době jeho trvání, informace o základových stanicích zajišťujících hovor apod.), které lze považovat za nedílnou součást tohoto obsahu. Nejde však o práva absolutní, právní řád tak výslovně dovoluje zákonné výjimky z této ochrany, a to především z důvodu zájmu demokratické společnosti, případně zájmu ústavně zaručených základních práv a svobod jiných, a to zejména zájmem na ochraně společnosti před trestnými činy a na tom, aby takové činy byly náležitě zjištěny a potrestány.

Přípustný je tedy pouze zásah do základního práva nebo svobody člověka ze strany veřejné moci, jestliže jde o zásah nezbytný v uvedeném smyslu. K tomu, aby nebyly překročeny meze této nezbytnosti, musí existovat systém účinných záruk, jejichž účelem je efektivní kontrola jejich dodržování. Za tímto účelem byl do klíčového zákona č. 127/2005 Sb., o elektronických komunikacích, v platném znění, zařazen také zvláštní institut ochrany důvěrnosti komunikací.[341] Na základě této úpravy jsou všichni podnikatelé zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupné služby elektronických komunikací povinni zajistit technicky a organizačně důvěrnost zpráv a s nimi spojených provozních a lokalizačních údajů, které se přenášejí prostřednictvím jejich veřejné komunikační sítě a veřejně dostupných služeb elektronických komunikací. Zejména nepřipustí odposlech, ukládání zpráv nebo jiné druhy zachycení nebo sledování zpráv a s nimi spojených údajů osobami jinými, než jsou uživatelé, bez souhlasu dotčených uživatelů, pokud zákon nestanoví jinak.[342] To nebrání technickému ukládání údajů, které je nezbytné pro přenos zpráv,[343] aniž by byla dotčena zásada důvěrnosti.

340 ŠÁMAL, K., V. KRÁL, J. BAXA, a F. PŮRY. *Trestní řád: komentář*, I. díl. Praha: C. H. Beck, 2001, s. 463

341 Viz § 89 a násl. zákona o elektronických komunikacích, v platném znění.

342 Viz např. § 88 trestního řádu.

343 Zprávou se rozumí jakákoli informace, která se vyměňuje nebo přenáší mezi konečným počtem účastníků nebo uživatelů prostřednictvím veřejně dostupné služby elektronických komunikací, s výjimkou informace přenášené jako součást veřejného rozhlasového nebo televizního vysílání sítí elektronických komunikací, nelze-li ji přiřadit k určitelnému účastníkovi nebo uživateli, který tuto informaci přijímá.

V tomto ohledu zákon stanoví, že každý, kdo hodlá používat nebo používá sítě elektronických komunikací k ukládání údajů nebo k získávání přístupu k údajům uloženým v koncových zařízeních účastníků nebo uživatelů, je povinen tyto účastníky nebo uživatele předem prokazatelně informovat o rozsahu a účelu jejich zpracování a je povinen nabídnout jim možnost takové zpracování odmítnout. Tato povinnost neplatí pro technické ukládání nebo přístup výhradně pro potřeby přenosu zprávy prostřednictvím sítě elektronických komunikací nebo, je-li to nezbytné, pro potřeby poskytování služby informační společnosti, která je výslovně vyžádána účastníkem nebo uživatelem.

4.5.1 Procesněprávní aspekty ochrany provozních a lokalizačních údajů (data retention) se zřetelem k historických ústavněprávním souvislostem

S účinností od 1. září 2008 byla přijata významná novela[344] zákona č. 127/2005 Sb., o elektronických komunikacích, a o změně některých souvisejících zákonů, ve znění pozdějších předpisů (dále jen zákon o elektronických komunikacích).[345] Tento zákon ve svém ustanovení § 97 odst. 3 a 4 stanovil zcela zásadní povinnost vybraných subjektů (operátorů, poskytovatelů připojení apod.) uchovávat provozní a lokalizační údaje, které jsou vytvářeny nebo zpracovávány při zajišťování jejich veřejných komunikačních sítí a při poskytování jejich veřejně dostupných služeb elektronických komunikací. Tyto údaje se týkají jak neúspěšných pokusů, tak i těch realizovaných, a to za předpokladu, že jsou tyto údaje vytvářeny nebo zpracovávány a zároveň uchovávány nebo zaznamenávány). Subjekty, které tyto provozní a lokalizační údaje uchovávají, jsou povinny je na požádání bezodkladně poskytnout orgánům oprávněným k jejich vyžádání podle zvláštního právního předpisu. Současně jsou tyto subjekty povinny zajistit, aby s těmito údaji nebyl uchováván obsah zpráv. Doba pro uchovávání těchto údajů nesmí být kratší než 6 měsíců a delší než 12 měsíců (§ 97 odst. 3 zákona o elektronických komunikacích ve znění tehdejších předpisů). Po uplynutí této doby je osoba, která údaje podle věty první a druhé uchovává, povinna tyto údaje zlikvidovat, pokud nebyly poskytnuty orgánům oprávněným k jejich vyžádání podle zvláštního předpisu nebo pokud zákon o elektronických komunikacích nestanoví jinak.[346] Za účelem provedení výše uvedených ustanovení, jakož i na základě zvláštního zákonného zmocnění[347] zákona o elektronických komunikacích byla přijata vyhláška č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání. Vyhláška tak

344 Viz zákon č. 247/2008 Sb. ze dne 5. června 2008, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

345 Příslušná novela byla vyhlášena dne 4. 7. 2008 ve Sbírce zákonů v částce 78 pod č. 247/2008 Sb.

346 Viz např. § 90 zákona o elektronických komunikacích.

347 Tímto zmocněním bylo právě ustanovení § 97 odst. 4 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích). Vyhláška byla podepsána ministryní pro informatiku a byla publikována v částce 169 pod č. 485/2005 Sbírky zákonů s účinností dnem jejího vyhlášení, tj. 15. 12. 2005.

podrobně vymezovala ve struktuře dle jednotlivého druhu služeb elektronických komunikací ve své původní podobě nejen samotný rozsah takto uchovávaných provozních a lokalizačních údajů (např. IP adresu počítače, IMEI mobilního telefonu atd. apod.), dobu jejich uchovávání, jakož i formu a způsob jejich předávání orgánům oprávněným k jejich využívání a způsob likvidace údajů, které byly poskytnuty orgánům oprávněným k jejich vyžádání podle zvláštního právního předpisu.[348]

Především je třeba zdůraznit, že hlavním deklarovaným účelem výše uvedené právní úpravy data retention bylo zejména čelit zvyšujícím se bezpečnostním rizikům a zajištění bezpečnosti a obrany České republiky. Samotná důvodová zpráva k předmětným ustanovením však tento účel jakkoliv blíže nerozváděla, pouze spíše heslovitě hovořila o zpřesnění povinnosti uchovávat provozní a lokalizační údaje a tyto údaje bezodkladně poskytovat orgánům oprávněným k jejich vyžádání, pouze mimo jiné stručně odkázala na příslušnou Směrnici č. 24, která vztahuje povinnost uchovávat tyto údaje pouze na ty údaje, které jsou vytvářeny nebo zpracovávány, a to s tím, že takto uchovávané údaje pak mají být orgánům oprávněným k jejich vyžádání poskytnuty bezodkladně. Jakékoliv bližší zdůvodnění účelu či cílů této úpravy však bylo absentováno (viz důvodová zpráva k tomuto zákonu). Vzhledem k plošnosti této právní úpravy jako celku, jakož i k jejímu dopadu na jednotlivce, došlo v České republice k poměrně široké mediální a částečně i odborné diskusi, které převážně dominovala problematika absence zvláštního důvodu pro plošné uchovávání předmětných údajů. Navzdory skutečnosti, že zákon poměrně důsledně vycházel z principu, že je zakázáno uchovávat samotný obsah komunikace (viz výše), stala se tato úprava předmětem silné kritiky převážně z řad nevládních organizací, které se zabývaly ochranou lidských práv, zejména pak práva na soukromí. Podobný postup bylo možné sledovat i v řadě dalších zemí EU, kde v některých případech došlo k napadení podobných úprav data retention před národními ústavními soudy.[349] Podobný osud spočívající v ústavním přezkumu této úpravy pak logicky následoval úpravu i v České republice.[350]

Dne 26. března 2010 byl Ústavnímu soudu České republiky doručen návrh skupiny 51 poslanců na zrušení ustanovení § 97 odst. 3 a 4 zákona o elektronických komunikacích a na zrušení jej provádějící vyhlášky č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich vyu-

348 Viz Směrnice č. 24.

349 Např. v Německu byl takovýto přezkum u Spolkového ústavního soudu realizován již 31. prosince 2007. Napadána zde byla příslušná ustanovení německého telekomunikačního zákona a německého trestního řádu, stanovující poskytovatelům veřejně dostupných telekomunikačních služeb povinnost plošně uchovávat údaje o telekomunikačním provozu po dobu 6 měsíců. Soud v tomto ohledu konstatoval, že uchovávání údajů samo o sobě nelze považovat protiústavní, a to přesto, že se jedná o obzvláště závažný zásah s dopadem, jaký německý právní řád doposud nepoznal. Rozhodujícím pro tento výrok byl především fakt, že data retention je časově omezené na dobu šesti měsíců, občan se tak může spolehnout na to, že uchovaná data budou smazána, data nejsou uchovávána přímo státem, ale za pomoci soukromých subjektů, poskytovatelů služeb elektronických komunikací, stát tak nemá přístup ke všem potřebným datům najednou, a tedy nevzniká jakési univerzální úložiště, ke kterému by měl stát neomezený přístup.

350 K tomuto tématu více viz např. MYŠKA, Matěj. Aktuální otázky data retention. *Revue pro právo a technologie*. Brno: Masarykova univerzita, 2010, č. 1. ISSN 1804-5383.

žívání, tedy návrh na zrušení výše uvedené úpravy data retention. Základním argumentem ve prospěch zrušení těchto ustanovení byl konflikt v podobě nepřiměřeného zásahu do ústavou garantovaného práva na soukromí. Na uvedené nedostatky upozorňovali nejen odborníci na akademické půdě, ale zejména nevládní organizace.[351] Podle navrhovatelů představuje shromažďování a využívání provozních a lokalizačních údajů v takovém rozsahu, v jakém jej vymezují napadená ustanovení zákona o elektronických komunikacích a jej provádějící vyhlášky č. 485/2005 Sb., neproporcionální zásah do základních práv uvedených v Listině a Úmluvě. Poukazovali přitom jak na související judikaturu Ústavního soudu, tak i Evropského soudu pro lidská práva, jakož i na skutečnost, že k jakémukoliv zásahu do základních práv je nezbytné, aby byl objektivně odůvodněn naléhavou společenskou potřebou a byl zároveň proporcionální vzhledem ke společenské potřebnosti a sledovanému legitimnímu cíli.

O rok později, dne 31. března 2011, po podání výše uvedeného návrhu, zrušil Ústavní soud napadenou právní úpravu data retention svým nálezem č. 94/2011 Sb. ze dne 22. března 2011. Ústavní soud v úvodu svého nálezu zdůraznil význam respektu k soukromému životu a právo na informační sebeurčení v právním státu, tedy možnost osoby samostatně rozhodovat o tom, jaké informace o sobě poskytne, komu a v jakém rozsahu, přičemž dále uvedl (a to i s odkazem na judikaturu ESLP),[352] Spolkového ústavního soudu a dalších ústavních soudů, které v této otázce již rozhodovaly, a přičemž dovodily, že povinnost uchovávat předmětné údaje se sice nevztahuje na obsahy jednotlivých sdělení, avšak z daných údajů o uživatelích, adresátech, časech, datech, místech a formátech komunikace, pokud budou sledovány po delší časový úsek, lze v jejich kombinaci sestavit velmi detailní informace o jednotlivých osobách. Připomněl také, že při zásazích do základních práv a svobod jednotlivce musejí být respektovány ústavněprávní limity a veřejná moc tak může do osobní integrity a soukromí osob zasáhnout jen zcela výjimečně, pokud je to v demokratické společnosti nezbytné a pokud nelze sledovaného účelu dosáhnout jinak. Ústavní soud rovněž zmínil skutečnost, že úprava byla přijata v souvislosti s bojem proti závažné trestné činnosti (viz argument zmíněný důvodovou zprávou výše), nicméně zákon umožňoval uchovávání a poskytování údajů bez předchozího podezření, tedy zcela plošně a bez rozlišení míry závažnosti konkrétního deliktu, který je vyšetřován. V tomto ohledu tak úprava data retention představuje významný zásah do základního práva jednotlivce na ochranu soukromí v podobě informačního sebeurčení, a to bez ohledu na skutečnost, že nejsou uchovávány obsahy[353] těchto sdělení. Důvodem pro zrušení této úpravy tak

351 Zejména pak organizace Iuridicum Remedium, která byla hlavním iniciátorem českého návrhu, kterým skupina poslanců toto ustanovení napadla.

352 ESLP ve své judikatuře stanovil požadavky na právní úpravu umožňující zásah do práva na soukromý život veřejnou mocí v podobě užití odposlechu telefonních hovorů apod. – zdůraznil, že je třeba vymezit jasná pravidla upravující rozsah a použití takových opatření, stanovit minimální požadavky na délku, způsob uložení získaných informací, jejich použití, přístup třetích osob k nim a zakotvit procedury k ochraně důvěrnosti údajů a též k jejich zničení (Z odůvodnění nálezu ÚS sp. zn. Pl. ÚS 24/10).

353 Samotné provozní a lokalizační údaje sbírané po delší časový úsek umožňují vytváření tzv. komunikačních profilů, z nichž lze získat údaje nejen o minulých aktivitách jedince, ale s vysokou mírou pravděpodobnosti i předvídat jeho aktivity budoucí. Názorně to demonstroval německý poslanec Malte Spitz, který poskytl provozní a lokalizační údaje uchovávané o jeho mobilním telefonu německému týdeníku Die Zeit.

lze vysledovat zejména ze samotné nejasnosti a neurčitosti této úpravy, a to jak v oblasti zákonem zmocněného okruhu orgánů oprávněných k vyžádání si těchto údajů, tak i v oblasti absence vymezeného účelu, pro který mohou být tyto údaje oprávněným orgánům poskytovány.[354] Velmi podobný argument se objevil i v rozhodnutí Spolkového ústavního soudu v Německu, neboť i tam šli národní legislativci nad rámec požadavků EU, protože Směrnice č. 24 výslovně uvádí, že uchovávané údaje mají být dostupné pro účely vyšetřování, odhalování a stíhání závažných trestných činů. Ústavní soud v tomto ohledu rovněž připomněl, že pro oprávněné orgány, které navíc nebyly zákonnou úpravou ani přesně vymezeny, je vyžádání provozních a lokalizačních údajů velmi pohodlným usnadněním práce.

K zásadním pochybnostem český Ústavní soud dospěl i při zkoumání toho, zda nástroj plošného a preventivního uchovávání provozních a lokalizačních údajů je z pohledu jeho původního účelu (ochrana před bezpečnostními hrozbami a prevence před páchání zvlášť závažné trestné činnosti) nástrojem efektivním, a to zejména při existenci tzv. anonymních SIM karet, které se vymykají z napadené právní úpravy předvídaného rozsahu uchovávaných provozních a lokalizačních údajů a které jsou dle vyjádření Policie České republiky až ze 70 % využívány ke komunikaci při páchání trestné činnosti.[355] V této souvislosti lze odkázat na analýzu Spolkového úřadu vyšetřování SRN (Bundeskriminalamt) ze dne 26. 1. 2011, který na základě porovnání statistických údajů o spáchané závažné trestné činnosti na území SRN za období před přijetím předmětné právní úpravy k data retention a po něm, dospěl k závěru, že použití nástroje plošného a preventivního uchovávání provozních a lokalizačních údajů nemělo téměř žádný vliv na snížení počtu spáchaných závažných trestných činů ani na míru jejich objasňování.[356] Obdobné závěry lze přitom učinit i při zběžném pohledu na statistické přehledy kriminality na území České republiky zveřejňované Policií České republiky, např. srovnání statistických údajů za období let 2008 až 2010.[357] V neposlední řadě považoval český Ústavní soud za nutné vyjádřit pochybnosti i nad tím, zda je vůbec žádoucí, aby soukromé osoby (poskytovatelé služeb v oblasti Internetu a telefonní a mobilní komunikace, zejm. mobilní operátoři a obchodní společnosti zajišťující připojení k Internetu) byly nadány oprávněním uchovávat veškeré údaje o jimi poskytované komunikaci i o zákaznících, jimž jsou jejich služby poskytovány (tzn. údaje jdoucí i nad rozsah údajů, jež jsou dle napadené právní úpravy povinny uchovávat), a volně s nimi za účelem vymáhání pohledávek, rozvoje obchodní činnosti a marketingu disponovaly. Tato skutečnost se Ústavnímu soudu ČR jeví jako nežádoucí zejména z toho důvodu, že v zákoně o elektronických komunikacích ani v jiných právních předpisech není toto oprávnění a jeho účel blíže a podrobněji regulován, nejsou striktně vymezena práva a povinnosti, rozsah uchovávaných údajů, doba

354 Zákon v tomto ohledu obsahuje jen obecnou formulaci, že se shromážděná data smějí využívat za účelem objasnění skutečností důležitých pro trestní řízení (viz např. ustanovení § 88a trestního řádu), což je v rozporu s principem předvídatelnosti a legitimního očekávání.

355 K tomu srovnej článek: Česká policie chce zakázat anonymní předplacené karty, operátoři se brání. iDNES.cz, 18. 3. 2010.

356 Samotná analýza, jakož i konkrétní statistické údaje jsou dostupné z: www.vorratsdaten speicherung.de/content/view/426/79/lang,de/

357 Dostupné z: www.policie.cz/clanek/statisticke-prehledy-kriminality-650295.aspx

a způsob uchovávání, stejně jako nejsou blíže konkretizovány požadavky na jejich zabezpečení a kontrolní mechanismy.

Kromě rozhodnutí, že úprava není v souladu s ústavněprávními limity, protože porušuje požadavky plynoucí z principu předvídatelnosti rozhodování a legitimního očekávání a koliduje s požadavky na omezení práva na soukromí, vyjádřil také Ústavní soud jasnou pochybnost nad samotnou nezbytností a přiměřeností plošného a preventivního uchovávání těchto údajů.

V tomto ohledu lze zakončit, že Ústavní soud potvrdil celkový trend a existující rozhodovací praxi evropských orgánů ochrany ústavnosti o neústavnosti úpravy data retention, a to navzdory skutečnosti, že dosavadní praxe komunitárních orgánů tuto praxi navzdory silné kritice[358] důsledně obhajuje.[359] Povinnosti transponovat předmětnou Směrnici však nadále trvá, budoucnost data retention tak bude předmětem diskuse i nadále, a to jak v oblasti národních států, tak i na úrovni celoevropské. Výše uvedený nález tak rozhodně nelze považovat za konec úpravy data retention v České republice.

4.5.2 Data retention v současném českém právu

Pro úplnost je nutné konstatovat, že dne 1. října 2012 vstoupila v účinnost novela zákona o elektronických komunikacích č. 273/2012 Sb., kterou reagoval český zákonodárce na ústavněprávní problémy řešené v předchozí kapitole této části, zejména pak na nález Ústavního soudu Pl. ÚS 24/10 ze dne 22. března 2011,[360] jakož i související nález Ústavního soudu Pl. ÚS 42/11 ze dne 20. prosince 2011.[361] Obsahem zrušených ustanovení zákona o elektronických komunikacích bylo uložení povinnosti právnickým a fyzickým osobám zajišťujícím veřejnou komunikační síť nebo poskytujícím veřejně dostupnou službu elektronických komunikací (zejména telefonní operátoři a poskytovatelé internetového připojení – dále jen „operátoři") po dobu 6 až 12 měsíců uchovávat provozní a lokalizační údaje, které jsou vytvářeny nebo zpracovávány při zajišťování jejich veřejných komunikačních sítí a při poskytování jejich veřejně dostupných služeb elektronických komunikací, a povinnosti tyto údaje v daném rozsahu a daným způsobem poskytnout orgánům oprávněným k jejich vyžádání. Vyhláška č. 485/2005 Sb. pak stanovila rozsah uchovávaných provozních a lokalizačních údajů, dobu jejich uchovávání a způsob předávání těchto údajů oprávněným orgánům.

358 Kritikou nešetřila zejména nevládní organizace EDRi (European Digital Rights) ve své Stínové zprávě dostupné v angličtině z: www.edri.org/files/shadow_drd_report_110417.pdf

359 Evropská komise. Hodnotící zpráva o směrnici o uchovávání údajů [online]. [vid. 28. června 2011]. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:CS:PDF

360 Vyhlášený pod č. 94/2011 Sb., kterým byla zrušena ustanovení § 97 odst. 3 a 4 zákona o elektronických komunikacích a vyhláška č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání.

361 Vyhlášený pod č. 43/2012 Sb., kterým se ustanovení § 88a trestního řádu uplynutím dne 30. září 2012 zrušuje.

Provozní a lokalizační údaje[362] operátoři poskytují v souladu s ustanovením § 88a trestního řádu soudci (předsedovi senátu) a v přípravném řízení státnímu zástupci nebo policejnímu orgánu. Policejními orgány se podle § 12 odst. 2 trestního řádu rozumějí:

- útvary Policie České republiky (dále jen „policie"), a to i pro případy, kdy policie získává provozní a lokalizační údaje mimo trestní řízení podle zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů. Jedná se o případy, kdy je zahájeno pátrání po konkrétní hledané nebo pohřešované osobě nebo je policie oprávněna tyto údaje získávat za účelem zjištění totožnosti osoby neznámé totožnosti nebo totožnosti nalezené mrtvoly.[363]
- Generální inspekce bezpečnostních sborů v řízení o trestných činech příslušníků Policie České republiky, příslušníků Vězeňské služby České republiky, celníků anebo zaměstnanců České republiky zařazených k výkonu práce v Policii České republiky nebo o trestných činech zaměstnanců České republiky zařazených k výkonu práce ve Vězeňské službě České republiky anebo v Celní správě České republiky, spáchaných v souvislosti s plněním jejich pracovních úkolů,
- pověřené orgány Vězeňské služby České republiky v řízení o trestných činech osob ve výkonu vazby, trestu odnětí svobody a zabezpečovací detence, spáchaných ve vazební věznici, věznici nebo v ústavu pro výkon zabezpečovací detence,
- pověřené celní orgány v řízení o trestných činech spáchaných porušením celních předpisů a předpisů o dovozu, vývozu nebo průvozu zboží, a to i v případech, kdy se jedná o trestné činy příslušníků ozbrojených sil nebo bezpečnostních sborů, a dále porušením právních předpisů při umístění a pořízení zboží v členských státech Evropských společenství, je-li toto zboží dopravováno přes státní hranice České republiky, a v případech porušení předpisů daňových, jsou-li celní orgány správcem daně podle zvláštních právních předpisů,
- pověřené orgány Vojenské policie v řízení o trestných činech příslušníků ozbrojených sil a osob, které páchají trestnou činnost proti příslušníkům ozbrojených sil ve vojenských objektech, proti vojenským objektům, vojenskému materiálu nebo ostatnímu majetku státu, s nímž je příslušné hospodařit Ministerstvo obrany ČR,

362 Provozními údaji se podle zákona o elektronických komunikacích rozumí jakékoli údaje zpracovávané pro potřeby přenosu zprávy sítí elektronických komunikací nebo pro její účtování. Lokalizačními údaji se rozumí jakékoli údaje zpracovávané v síti elektronických komunikací, které určují zeměpisnou polohu koncového zařízení uživatele veřejně dostupné služby elektronických komunikací. Jedná se například o datum a čas zahájení komunikace, telefonní čísla volajícího a volaného, délka komunikace, IP adresy, množství přenesených dat při datové komunikaci. Laicky řečeno se jedná o údaje, ze kterých je patrno kdo, odkud, s kým a po jakou dobu komunikoval. Zrušenými ustanoveními § 97 odst. 3 a 4 zákona o elektronických komunikacích byla do českého právního řádu implementována některá ustanovení Směrnice č. 24.

363 Provozní a lokalizační údaje v nezbytném rozsahu dále může získávat útvar policie, jehož úkolem je boj s terorismem, a to za účelem předcházení a odhalování konkrétních hrozeb v oblasti terorismu. Policie je podle zákona o zvláštní ochraně svědka oprávněna získávat v nutném rozsahu údaje o uskutečněném telekomunikačním provozu, je-li dáno podezření, že chráněná osoba nedodržuje povinnosti uvedené v § 6 zákona o zvláštní ochraně svědka (tzn. dodržovat podmínky poskytování zvláštní ochrany a pomoci, řídit se pokyny příslušníků policie a příslušníků vězeňské služby, informovat bezodkladně policisty a příslušníky vězeňské služby o všech nových skutečnostech a změnách, které mohou být významné pro postup policie a vězeňské služby) a nelze-li podezření prověřit jiným způsobem.

- pověřené orgány Bezpečnostní informační služby v řízení o trestných činech příslušníků Bezpečnostní informační služby,
- pověřené orgány Úřadu pro zahraniční styky a informace v řízení o trestných činech příslušníků Úřadu pro zahraniční styky a informace,
- pověřené orgány Vojenského zpravodajství v řízení o trestných činech příslušníků Vojenského zpravodajství,
- pověřené orgány Generální inspekce bezpečnostních sborů v řízení o trestných činech příslušníků Generální inspekce bezpečnostních sborů nebo o trestných činech zaměstnanců České republiky, zařazených k výkonu práce v Generální inspekci bezpečnostních sborů.[364]

Oprávnění získávat provozní a lokalizační údaje má na základě ustanovení § 8 odst. 1 písm. d) zákona č. 15/1998 Sb., o dohledu v oblasti kapitálového trhu v platném znění, Česká národní banka, a to pro účely výkonu dohledu nad kapitálovým trhem. Provozní a lokalizační údaje ve smyslu zákona o elektronických komunikacích představují osobní údaje, spadají tedy do režimu ZoOÚ, a to zejména co do podmínek jejich zpracování v podobě zabezpečení ve smyslu § 13. Z těchto důvodů byla Úřadu svěřena působnost v podobě dozoru nad dodržováním povinností při zpracování osobních údajů podle zákona o elektronických komunikacích (§ 87 odst. 3 zákona o elektronických komunikacích).

Samotná existence zákonné povinnosti uchovávat provozní a lokalizační údaje představuje *sui generis* zásah do soukromí uživatelů služeb elektronických komunikací. Zaznamenávají se informace o každém telefonickém spojení, textové zprávě či odeslaném emailu. Je zřejmé, že uchovávání podrobných dat o veškeré komunikaci, lokalizaci komunikujícího, internetových službách a stránkách lze hodnotit jako zásah do soukromého života člověka,[365] případně jako porušení práva na nerušený soukromý život osoby. V tomto ohledu je třeba klást enormní důraz na kvalitu a rozsah procesních záruk při aplikaci výše uvedené veřejnoprávní úpravy.

4.6 Občanskoprávní úprava

4.6.1 Obecné aspekty právní úpravy osobnostních práv fyzické osoby

Základ soukromoprávní ochrany osobnosti fyzické osoby vyplývá z ustanovení § 11 až 16 ObčZ. Samotná podstata této úpravy je pak tvořena tzv. generální klauzulí uvedenou v § 11 ObčZ, jež obsahuje (demonstrativní) pozitivně vymezený výčet chráněných ideálních statků, které tak tvoří dílčí složky jednotného práva osobnostního. Tato ochrana je pojata tak, že je řazena pod tzv. všeobecná osobnostní práva,[366] která příslušejí každé fyzické osobě jako subjektu

364 Viz důvodová zpráva k zákonu č.. 273/2012 Sb.

365 K tomu např. HORÁK, J. Právo na soukromí versus bezpečnost ve sjednocené Evropě: zamyšlení nad problematikou „data retention". *Acta Universitatis Carolinae, Iuridica.* 2006, č. 1, s. 81.

366 K tomu srovnej pojetí tzv. zvláštních osobních práv, která naopak příslušejí pouze vybraným subjektům, jež splňují zákonem stanovená kritéria (jako např. tvůrci autorských děl, výkonní umělci, původci nebo přihlašovatelé patentů na vynálezy apod.).

práva.[367] Generální klauzule je dále rozváděna a konkretizována v § 12. Prostředky, jimiž se lze této ochrany domáhat, jakož i samotný rozsah možných nároků, jsou pak vymezeny v ustanovení § 13 až 16 ObčZ. Je rovněž třeba zmínit, že ochrana osobnosti se týká výlučně osob fyzických, právnická osoba nemá z povahy věci právo na ochranu osobnosti jako fyzická osoba. Má však práva obdobná,[368] jako např. právo na ochranu svého názvu, jakož i právo na ochranu své dobré pověsti, reputace, image apod. (§ 19b odst. 2 a 3 ObčZ).

Jakkoliv lze úpravu ObčZ považovat za úpravu relativně samostatnou a možná i tradiční,[369] nejde o úpravu komplexní. Nezřídka lze totiž předpokládat, že ochrana osobnosti poskytovaná ObčZ bude často realizována v souběhu s jinými způsoby ochrany, a to jak předpisy práva soukromého (např. zákoníkem práce), tak i veřejného (např. trestním zákonem, zákonem o přestupcích). Problematika integrity fyzické osoby totiž není spojena jen se samotným občanským právem, ale velmi úzce souvisí s celou řadou dalších právních odvětví napříč právním řádem, zejména pak s právem ústavním, správním, tiskovým, trestním apod.

Význam naprosto zásadní má pak úprava práv osobnostních v rovině ústavněprávní, která vyplývá mimo jiné z čl. 7 a čl. 10 Listiny základních práv a svobod upravující zejména právo na soukromí, osobní čest, dobrou pověst, jakož i právo na jméno. Tato ochrana je pak rovněž dotvářena řadou vyhlášených mezinárodních smluv, resp. úmluv,[370] které mají ve vztahu k zákonné úpravě aplikační přednost podle čl. 10 Ústavy ČR. Tato ústavněprávní, resp. mezinárodněprávní rovina tak obsahuje zcela zásadní principy, které dotvářejí úpravu uvedenou v občanském zákoníku. V souladu s těmito principy musí být soukromoprávní úprava ochrany osobnosti fyzické osoby zejména vykládána ústavně-konformním způsobem, jakož i používána a doplňována (např. rozšířením demonstrativního výčtu v generální klauzuli apod.).

Vyjma řady právních předpisů, které na úpravu v občanském zákoníku přímo navazují a o kterých bude pojednáno v další části, lze považovat za významnou zejména ochranu poskytovanou trestním zákoníkem, který mimo jiné upravuje skutkovou podstatu pomluvy (§ 184), neoprávněného nakládání s osobními údaji (§ 180), porušení tajemství dopravovaných zpráv (§ 182) nebo porušení tajemství listin a jiných dokumentů uchovávaných v soukromí (§ 183), jakož i řady dalších trestných činů, které sledují zájem na ochraně osobnostních práv.

367 ObčZ se však vyhýbá výrazu „člověk", ačkoliv by to jistě bylo u ochrany lidské osobnosti namístě, navíc by tak došlo k provázání této problematiky s právem ústavním a mezinárodním, kde je výraz člověk (stejně tak jako výraz lidská důstojnost apod.) hojně používán. ObčZ tak patrně činí z důvodů historických, resp. ideologických. V minulosti byl v kontextu ochrany osobnosti používán také soukromoprávně zcela nevhodný výraz „občan", který byl nahrazen výrazem „fyzická osoba" až o téměř 28 let později, a to novelou ObčZ zákonem č. 509/1991. Sb.

368 Uvedené vyplývá rovněž z názorů Ústavního soudu ČR, který právnickým osobám přiznává rovněž pouze tato práva, jakož i práva vyplývající z ochrany hospodářské soutěže či obchodního tajemství. K tomu srov. sp. zn. III. US 35/01, sv. 22, usn. č. 18, s. 369.

369 Odlišně, byť s některými obdobnými rysy, byla ochrana osobnosti upravena již v obecném zákoníku občanském, a to v dílu prvním, v rámci úpravy práv o právu osobním, kde bylo v ustanoveních § 15 a násl. Hlavy prvé pojednáno o právech, která se týkají osobních vlastností a poměrů. Podlé této úpravy se osobní práva týkala jak osobních vlastností a poměrů, tak i poměrů rodinných.

370 Zejména pak Úmluvou o ochraně lidských práv a základních svobod vyhlášenou ve Sbírce zákonů ČR pod číslem 209/1992 Sb., Úmluvou na ochranu lidských práv a důstojnosti lidské bytosti v souvislosti s aplikací biologie a medicíny vyhlášenou ve Sbírce zákonů ČR pod číslem 96/2001 Sb. apod.

Dalším významným předpisem správního práva je zákon č. 200/1990 Sb., o přestupcích, v platném znění, který v ustanovení § 49 a násl. stanoví sankce za přestupky proti občanskému soužití, kterých se dopustí mimo jiné ten, kdo působí jinému újmu pro jeho příslušnost k národnostní menšině nebo pro jeho etnický původ, pro jeho rasu, barvu pleti, pohlaví, sexuální orientaci, jazyk, víru nebo náboženství, pro jeho politické nebo jiné smýšlení, členství nebo činnost v politických stranách nebo politických hnutích, odborových organizacích nebo jiných sdruženích, pro jeho sociální původ, majetek, rod, zdravotní stav anebo pro jeho stav manželský nebo rodinný.

Určité aspekty ochrany osobnostních práv lze rovněž nalézt i v řadě dalších předpisů, byť předmětem jejich úpravy není ochrana osobnosti fyzické osoby, ale spíše jejích některých dílčích a souvisejících složek. Jde zejména o předpisy nepřímo upravující nebo omezující obsah aplikace osobnostních práv, např. zákon č. 361/2003 Sb., o služebním poměru příslušníků bezpečnostních sborů, v platném znění, upravující povinnosti při kontrole a prohlídce osob, zákon č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže, v platném znění, zákon č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání, v platném znění, ZsPI, zákon o poštovních službách, jakož i některé další.

Jak vyplývá z výše uvedeného, osobnost fyzické osoby je chráněna celým právním řádem, nejen tedy ObčZ. Ochrana dle ObčZ tak bude často realizována v souběhu s jinými způsoby ochrany, které upravují další právní předpisy, a to jak předpisy práva soukromého, tak i veřejného. Není tedy vyloučeno, aby spolu s nároky fyzické osoby vyplývající z ObčZ uplatňovanými žalobou na ochranu osobnosti podle občanského soudního řádu byla spojena i žádost o uveřejnění odpovědi a dodatečného sdělení jak podle tiskového zákona, tak i zákona o provozování rozhlasového a televizního vysílání, jakož i následné uplatnění těchto práv na uveřejnění u soudu. Souběžně s těmito nároky pak může být rovněž podáno (trestní) oznámení o skutečnostech nasvědčujících tomu, že byl spáchán trestný čin podvodu podle § 206 trestního zákona, případně trestný čin neoprávněného nakládání s osobními údaji dle § 178 trestního zákona. V některých případech však může být souběh více způsobů ochrany vyloučen, a to zejména vzhledem ke speciální povaze těchto nároků.[371]

4.6.2 Rozsah a obsah práva na ochranu osobnosti

Obsah práva na ochranu osobnosti vyplývá zejména z generální klauzule § 11 ObčZ, která tak zakotvuje jednotlivé složky, resp. ideální statky jednotného práva osobnostního, které jsou chráněny normami občanského práva. Výčet statků (složek) chráněných tímto ustanovením je demonstrativní, jejich význam pak vyplývá mimo jiné z použití výkladu ústavně-konformního, jakož i pořadí, v jakém jsou tyto jednotlivé složky řazeny. Z generální klauzule, jakož i z jednotné povahy práva osobnostního tak vyplývá, že fyzická osoba má právo na ochranu své osobnosti, zejména

371 DOLEŽÍLEK, J. *Přehled judikatury ve věcech ochrany osobnosti.* ASPI, 2002.

- *života a zdraví,*
- *občanské cti a lidské důstojnosti,*
- *soukromí,*
- *svého jména,*
- *projevů osobní povahy,*
- *jiných ideálních statků ObčZ výslovně nepojmenovaných.*[372]

Vzhledem k tomu, že toto ustanovení chrání rozsáhlý pojem osobnosti člověka, tj. jako obecně uznávanou hodnotu, včetně všech jeho jednotlivých statků (složek), lze jej bez dalšího aplikovat na všechna související jednání realizovaná v prostředí Internetu. Zveřejnění některých důvěrných informací týkajících se osobního života člověka, lhostejno, zda pravdivých či nikoliv, může mít své dopady ve všech těchto složkách, včetně dopadů na (psychické) zdraví, čest, důstojnost, včetně logické vazby na jméno člověka. Technologické možnosti Internetu, včetně uchovávání a zcela bezbřehého šíření (sdílení) takové informace, jež se stává svou povahou nezastavitelné, pak umocňuje povahu takovéhoto zásahu jak z pohledu hledisek kvalitativních, tak i kvantitativních. Zároveň je třeba zdůraznit, že standardní instituty ochrany, jako je zejména efektivní odstranění těchto následků, omluva, přiměřené zadostiučinění, upuštění od dalších zásahů, nejsou v tomto prostředí realizovatelné. Poškození tak musí hledat prostředky především v rovině důsledného uplatňování práva na náhradu nemajetkové újmy v penězích (viz níže).

Samotná generální klauzule je dále rozváděna a konkretizována v § 12, a to tak, že pod tuto ochranu spadají všechny písemnosti osobní povahy, podobizny, obrazové snímky a obrazové a zvukové záznamy týkající se fyzické osoby nebo jejích projevů osobní povahy, mohou být pořízeny nebo použity jen se svolením (souhlasem) fyzické osoby, které se týkají.

Výše uvedené složky ochrany osobnosti nemohou být považovány za samostatně stojící, obsah práv vyplývající z těchto složek se mnohdy překrývá, uplatňování jedné z nich je totiž mnohdy podmíněna aplikací druhé a naopak, v tomto ohledu mluvíme o tzv. nedělitelnosti osobnostních práv. Rozsah ochrany všeobecných osobnostních práv pak může mít v některých případech kolizní povahu s jinými chráněnými hodnotami a statky, a to zejména se svobodou projevu (např. výkon práva kritiky napadající čestnost fyzické osoby), právem na soukromí a ochranu jména (např. zveřejňování dlužníků bez jejich souhlasu), právem na informace, případně také s právem na samosprávnost některých institucí.[373] Tyto rozpory pak musí být řešeny výkladem, a to obvykle výkladem ústavně-konformním (viz výše).[374]

372 Poslední z bodů uvedených pod písm. e) však není v generální klauzuli uveden. Ochranu těchto dalších statků je ale nutné připustit s ohledem na povahu jednotného osobnostního práva, skutečnosti, že generální klauzule obsahuje pouze demonstrativní výčet těchto ideálních statků, jakož i z použití ústavně-konformního výkladu.

373 K problematice vybraných hmotněprávních aspektů ochrany osobnosti ve vztahu k působení církevních a mysliveckých soudů srovnej BÁRTA, J. Otázky ochrany osobnosti s ohledem na soudy myslivecké a soudy církevní. *Právník.* 2001, č. 3; případně HRDINA, A. Soud nad církevním soudcem. *Právník.* 2000, č. 4, s. 421.

374 K tomu srovnej DOLEŽAL T. Nahlížení do zdravotnické dokumentace pacienta a sdělování informací. *Právní rozhledy.* 2007, roč. 15, č. 15, s. 572.

4.6.3 Život a zdraví

Jak vyplývá z příkladmého výčtu generální klauzule § 11, na prvním místě je jako chráněný statek, resp. složka ochrany osobnosti fyzické osoby uveden právě život a zdraví (tj. zejména tělesná a duševní nedotknutelnost – integrita fyzické osoby jako celku). Z povahy tohoto statku vyplývá, že subjektivní a přirozené právo na život je neoddělitelné od práva na zdraví, a opačně. Právo na tělesnou a duševní nedotknutelnost tak zahrnuje celou řadu dílčích práv osobnostních, a to zejména včetně práva

a) na ochranu života, a to již před narozením,
b) na život ve zdravém životním prostředí,
c) na respektování svého života,
d) na důstojný život,
e) k vlastnímu tělu a jeho částem,
f) na informace o vlastním zdraví.

Obsah nedělitelného práva na život a zdraví je tedy velmi široký, přičemž jeho počátky sahají již k prenatálnímu vývoji, resp. k početí života jako takového (viz čl. 6 odst. 1 Listiny), přičemž trvají po celý život člověka (např. právo na informace) a nezanikají mnohdy ani po jeho smrti (např. při vyslovení nesouhlasu s posmrtným odběrem tkání nebo orgánů).[375] V platné právní úpravě se tak tato ochrana projevuje jednak v obecných preventivních ustanoveních,[376] v obecných ustanoveních upravujících náhradu škody, veřejnoprávní ochraně spotřebitele,[377] dále v právních předpisech upravujících poskytování zdravotní péče,[378] umělé přerušení těhotenství,[379] jakož i nakládání s částmi lidského těla.[380]

Ochrana ve smyslu tohoto statku tak není omezena pouze na tělesnou integritu fyzické osoby, ale také na její vnitřní psychické složky, se kterými je nedílně spojena. Každý takový zákrok tak vyžaduje její svobodný a informovaný souhlas, a to po poučení o konkrétním realizovaném jednání, o jeho důsledcích, včetně možných alternativ a rizicích.[381] Zatímco do tělesné integrity lze zasáhnout především lékařským či jiným zákrokem, přičemž je zde nezbytná existence určitého fyzického kontaktu, psychická složka může být narušena, byť i pouhým umístěním důvěrné informace na diskusním fóru,[382] případně blogu. Takovýto zásah může být

375 K důsledkům aplikace některých práv osobnostních, zejména pak práva na život a zdraví, jakož i k dalším chráněným statkům osobnostním více viz TELEC, I. Chráněné statky osobnostní. Právní rozhledy. 2007, č. 8, s. 271.

376 K tomu srovnej např. ustanovení § 415 ObčZ.

377 K tomu více např. Kolektiv autorů, In: Pocta Martě Knappové k 80. narozeninám; KANDA, A. a J. MATEJKA. *Spotřebitelské smlouvy a jejich význam v informační společnosti.* Praha: ASPI, 2005, s. 159–204.

378 Např. zákon o zdravotnických službách.

379 Např. zákon č. 66/1986 Sb., o umělém přerušení těhotenství, v platném znění.

380 Např. zákon č. 285/2002 Sb., o darování, odběrech a transplantacích tkání a orgánů, v platném znění, zákon č. 256/2001 Sb., o pohřebnictví, v platném znění, apod.

381 K tomu obdobně DOLEŽAL, T., Problematické aspekty vztahu lékaře a pacienta zejména s ohledem na institut tzv. informovaného souhlasu. *Časopis zdravotnického práva a bioetiky.* 2011, roč. 1, č. 1, s. 27.

382 K tomu srovnej rozsudek Nejvyššího soudu ČR 7 Tdo 254/2003 k otázce spáchání trestného činu pomluvy na internetovém diskusním fóru, dostupné z: http://itpravo.cz/index.shtml?AA_SL_Session=6c5f31ee

realizován např. ve formě opakovaného vkládání vysoce agresívních a útočných komentářů (v diskusi), příspěvků na diskusním fóru či blogu s šikanujícími či hrubě poškozujícím obsahem (tzv. cyberbullying).

Velmi závažným deliktem je vytváření (falešných) profilů, blogů a jiných účelově zkreslených prostředí ve vazbě na zneužití či krádež identity. Podobně významný dopad může mít narušení tajemství dopravovaných či uchovávaných zpráv, jakož i neoprávněné zmocnění se a zneužití přístupu k cizímu emailů či jinému podobnému komunikačnímu prostředků. Takové jednání je obvykle výrazně za hranicí civilněprávní (občanskoprávní) či správněprávní úpravy, a s ohledem na kvalitu a intenzitu takovéhoto zásahu do osobnostních práv, bude na místě použití prostředků trestního práva, zejména trestního zákoníku, konkrétně pak ustanovení § 180 – 184 stanovícím trestné činy proti právům na ochranu osobnosti, soukromí a listovního tajemství. Je zde tak poskytována trestněprávní ochrana celkové rozvoji osobnosti člověka proti různým typům zásahů, a to ať již jde o ochranu osobních údajů (§ 180 trestního zákoníku), poškozování cizích práv (§ 181 trestního zákoníku), porušování tajemství dopravovaných zpráv i tajemství listin a dalších osobních dokumentů uchovávaných v soukromí (§ 182 a § 183 trestního zákoníku) a útoky proti cti a dobré pověsti formou pomluvy (§ 184 trestního zákoníku). Zákon u těchto trestných činů požaduje úmyslné zavinění, avšak s logickou výjimkou trestného činu neoprávněného nakládání s osobními údaji podle § 180 odst. 1, 2, kde postačí i nedbalost. Tyto instituty trestněprávní ochrany však nejsou vyčerpávající, je totiž zřejmé, že svoboda, ochrana života a soukromí, představují natolik významné a vzájemně propojené společenské hodnoty s širokým společenský základem, že ochranu soukromí lze hledat i v celé řadě dalších institutů trestního práva, a to nejenom hmotného, ale také procesního (viz např. ustanovení o nebezpečném pronásledování upravené v § 354 trestního zákoníku, apod.)

4.6.4 Občanská čest a lidská důstojnost

V pořadí druhým statkem, resp. skupinou práv vyplývajících z generální klauzule, je ochrana občanské cti a lidské důstojnosti. Tato ochrana tak navazuje na čl. 10 Listiny základních práv a svobod, který ale hovoří o lidské důstojnosti, osobní cti a dobré pověsti,[383] jehož cílem je ochrana psychické, resp. duševní součásti komplexní integrity fyzické osoby, jež se dotýká jeho cti či důstojnosti. Jak pojem důstojnost, tak i pojem čest představují svého druhu etickou a vysoce subjektivní kategorii, jež však není oborově omezena pouze na etiku, ale také na filozofii, náboženství a kulturu, netýká se tedy pouze oblasti vědomí (ve smyslu uvědomová-

9308ee4bb22d1759b04f9a2c&sh_itm=62b5ef2bb3ddb3670e96b2a30c1b9028&all_ids=1#disc, případně též rozsudek Městského soudu v Praze ze dne 17. 3. 2010, č.j. 10 Cm 47/2009-39, a na něj navazující druhostupňový rozsudek Vrchního soudu v Praze ze dne 2. 3. 2011, č. j. 3 Cmo 197/2010-82 (popsán na www.epravo.cz/top/clanky/odpovednost-poskytovatelu-sluzeb-informacni-spolecnosti-nekolik-postrehu-k-zaverum-vrchniho-soudu-v-praze-v-kauze-prolux-88471.html)

383 Nikoliv tedy cti občanské, jak je tomu u ObčZ

ní si), ale zejména svědomí (ve smyslu individuálního pociťování).[384]

Důsledky zásahu do lidské důstojnosti, cti či dobré pověsti nebo jména fyzické osoby se projevují zpravidla v rodině, v obchodních, podnikatelských či dalších společenských vztazích, tedy jak veřejných, tak i soukromých. K zásahu do těchto práv může dojít např. sdělením nepravdivých údajů o konkrétní osobě, o její rodině či o jejím rodinném a soukromém životě, přičemž taková nepravda je objektivně způsobilá značnou měrou ohrozit dobrou pověst, čest, vážnost, jméno a důstojnost ve společnosti, nebo narušením soukromého a rodinného života[385] (např. uveřejněním okolností z intimní či rodinné sféry jedince, odejmutí dítěte z péče rodiče, aniž by k tomu byly faktické a zákonné důvody apod.). V tomto ohledu lze usuzovat, že aplikace této části ochrany může být v prostředí Internetu velmi široká, vždyť v zásadě jakékoliv nedovolené šíření soukromých či nepravdivých informací s vysokou intenzitou může efektivně směřovat k zásahu tohoto typu, lhostejno, zda je tímto způsobem šířena listina, fotografie, případně jakákoliv jiná informace.[386]

4.6.5 Další rozsah a obsah práva na ochranu osobnosti

Úpravu ochrany osobnostních, resp. osobních práv, obsahuje celá řada právních předpisů, jež budou aplikovány současně, ať již jde o úpravu zákonem č. 262/2006 Sb., zákoník práce, v platném znění, který v ustanovení § 316.[387] Ochrana osobních práv zaměstnanců, resp. zejména právo na soukromí v rámci pracovněprávních vztahů je zde propojeno s ochranou majetkových vztahů, čemuž pak odpovídá i formulace těchto práv. Úprava ochrany osobních práv provedená zákoníkem práce tak vychází z principu delegace na ObčZ, a je tedy jako taková aplikovatelná souběžně[388] (viz dále). Jisté aspekty ochrany soukromí člověka, konkrétně pak listovní, telekomunikační a bankovní tajemství, upravuje poměrně podrobně zákon o poštovních službách,[389] zákon o elektronických komunikacích, zákon o bankách atd.

384 TELEC, I. Rozum a cit. *Právní rozhledy.* 2003, č. 7, s. 317.

385 K tomu srovnej VOSTRÁ, L. Maďarská kodifikace soukromého práva se zřetelem k právu rodinnému. *Právník.* 2010, roč. 149, č. 12, s. 1263–1273. ISSN 0231-6625.

386 Lze tak např. dovozovat, že i samotná existence údajů ve veřejně přístupné databázi s výsledným efektem denunciace, může vést k významnému zásahu do lidské důstojnosti těchto osob (viz např. neoprávněné zveřejnění databáze dlužníků, odsouzených osob atd.).

387 K tomu více BĚLINA, M., L. Drápal a kol. *Zákoník práce: komentář.* Praha: C. H. Beck, 2012. Autorem příslušné části komentáře § 316 je M. Štefko.

388 K tomu srovnej úpravu provedenou v předchozím zákoně č. 65/1965 Sb., zákoníku práce, kde bylo rovněž, byť poněkud komplikovaně, dovozováno, že v těch případech, které nejsou ošetřeny výslovnou právní úpravou zákoníku práce ani speciálních předpisů, je namístě využití analogie iuris, a tedy aplikace ustanovení ObčZ §11 a násl. o ochraně osobnosti, a to za podmínky, že to vyžaduje integrita obecných zásad právních a pracovněprávních. Takové řešení se však stále více ukazovalo jako poměrně komplikované, navíc v praxi zřídka kdy docházelo k jeho uplatnění

389 K provedení některých ustanovení tohoto zákona (§6 odst. 6 a § 22 odst. 4) pak byla přijata vyhláška Ministerstva informatiky ČR č. 286/2004 Sb.

4.6.5.1 Jméno

Ochrana jména, resp. právo na jméno je upraveno značně roztříštěně, napříč řadou právních předpisů. Jménem se obvykle rozumí individualizační a identifikační znak fyzické osoby, pod kterým tato osoba působí, jedná a činí právní úkony. Tato ochrana je poskytována jak samotnému jménu vlastnímu a jménu rodovému, tedy jménu a příjmení, včetně dalšího nebo změněného příjmení, rodného příjmení, jménu krycímu (pseudonymu, případně nickname), přezdívce, iniciále jména či monogramu. Subjektem práva na ochranu osobnosti, resp. této jeho dílčí složky (právu na ochranu jména) může být jen fyzická osoba. Veřejnoprávní ochrana jména vyplývá zejména u ustanovení § 61 a násl. zákona o matrikách, který mimo jiné uvádí, že občan má právo i povinnost užívat při jednání před orgány veřejné moci jméno, popřípadě jména, která jsou uvedena v jeho rodném listu vydaném matričním úřadem. Do matriční knihy nelze zapsat jména zkomolená, zdrobnělá a domácká. Fyzické osobě mužského pohlaví nelze zapsat jméno ženské a naopak. Matriční úřad dále nezapíše jméno, pokud je mu známo, že toto jméno užívá žijící sourozenec, mají-li sourozenci společné rodiče. Vzniknou-li pochybnosti o správné pravopisné podobě jména, je žadatel povinen předložit doklad vydaný znalcem. Občan je povinen užívat v úředním styku dvě jména, jsou-li zapsána v matriční knize vedené matričním úřadem.

Jak již bylo uvedeno výše, soukromoprávní úprava je značně roztříštěna, přičemž základem je právě úprava v ustanovení § 11 ObčZ. Určité aspekty ochrany těchto práv lze nalézt v řadě dalších předpisů, byť předmětem jejich úpravy není ochrana osobnosti fyzické osoby, ale spíše některých dílčích a souvisejících složek. Jde zejména o předpisy upravující zejména duševní vlastnictví, konkrétně pak o autorský zákon, který v ustanovení § 7, 74 a § 70 odst. 2 a 3) upravuje tzv. krycí jméno umělecké (pseudonym). Dalším významným předpisem je ObchZ, který v ustanoveních §8 a násl. upravuje institut obchodního firmy,[390] apod. Dalším velmi významným předpisem je ZoOchrZ, který umožňuje v určitých případech chránit jméno a příjmení člověka jako ochrannou známku.

Obdobně jak je tomu v případě většiny výše uvedených osobnostních statků, resp. dílčích složek práva osobnostního, i v případě ochrany jména není vyloučen souběh ochrany mezi osobnostním právem ke jménu ve smyslu ObčZ, obchodní firmou a ochrannou známkou. Takovýto souběh pak rozšiřuje meze ochrany práva na jméno, a to jak ve smyslu hmotněprávním, tak i procesním.

4.6.5.2 Projevy osobní povahy

Za projevy osobní povahy lze považovat v zásadě jakékoliv vyjádření vztahující se k fyzické osobě, a to s tím, že je lhostejné, zda je toto vyjádření provedeno ústně (např. ústním pro-

390 Jde typicky o ochranu poskytovanou jménům užívaným při výkonů nezávislých soukromých profesí, jako např. advokát, notář, daňový poradce, lékař nebo živnostník, jakož i u obchodní firmy člověka, který je podnikatelem zapsaným v obchodním rejstříku.

jevem), písmem, zvukem či obrazem, případně audiovizuálním snímkem. Rozhodná je zejména souvislost s integritou fyzické osoby, resp. její osobní povahou, nikoliv forma tohoto vyjádření. Ochrana je tak poskytována všem nosičům těchto vyjádření, ať již tradičním listinným či elektronickým, a to zcela bez ohledu na to, kde a jakým způsobem jsou tyto nosiče dále uloženy. Typickým příkladem projevů osobní povahy bude obsah příloh e-mailů, včetně e-mailů samotných, jakož i osobních fotografií, statusových změn a dalších osobních vyjádření umístěných v prostředí sociálních sítí. S těmito projevy je nutné nakládat v režimu ochrany statků chráněných § 11 ObčZ.

Osobní povaha projevu se posoudí konkrétně podle okolností případů. U písemností (osobní povahy) může jít zejména o osobní (soukromou) korespondenci (např. osobní elektronická pošta), deník fyzické osoby, případně i stenografický záznam slovního projevu fyzické osoby. Zvukovým záznamem se rozumí nahrávka hlasového projevu (např. na diktafon) nebo jiný nosič záznamu. Za obrazový projev osobní povahy je třeba považovat zejména fotografie, obrazy a další podobizny fyzických osob, ze kterých je fyzická osoba, ať již přímo nebo nepřímo, identifikovatelná. Osobní povaha těchto obrazových projevů spočívá zejména v tom, že je tato osoba identifikovatelná podle svých charakteristických rysů, které umožňují zobrazit její individuální tělesný vzhled nebo jeho identifikovatelnou část (např. tvář). Neoprávněný zásah do projevu osobní povahy spočívá zejména v jakékoliv neoprávněné dispozici s tímto, byť jedním jediným, projevem, a to počínaje jeho pořízením přes další nakládání (např. čtení, poslech apod.) až po jeho zničení (znehodnocení, likvidaci či skartaci).[391]

Za projevy osobní povahy je rovněž nutné považovat i takové projevy, které byť nepocházejí od osoby, které se týkají, se svou povahou k této osobě vztahují, tj. včetně textů, které jsou těmto osobám z nějakého důvodu připisovány (viz např. falešný profil na sociální síti, otevřený dopis s podpisem konkrétní osoby falešně uvedené jako autor atd.).

4.6.5.3 Jiné statky občanským zákoníkem výslovně nevyjmenované

Jak již bylo uvedeno výše, je osobnost fyzické osoby chráněna celým právním řádem, nejen tedy ObčZ, který navíc upravuje obsah a rozsah osobnostních práv značně obecně, přičemž pomocí příkladmého výčtu v generální klauzuli § 11 ponechává prostor k dalšímu rozšíření této ochrany o další statky práva osobnostního, které si vzhledem ke své povaze nebo argumentům ústavně-konformním, ochranu občanským právem rovněž zasluhují. Mezi tyto statky tak bezesporu patří např. osobní svoboda (projevu, pobytu, pohybu apod.), právo na výchovu a vzdělání, právo na informace, právo na osobní tajemství, dobrou pověst apod. Existence těchto dalších chráněných osobnostních statků tak může být závislá na řadě faktorů, které mohou být povahou nepředvídatelné (např. právní úprava, technologický či společenský rozvoj apod.).

391 K tomu srovnej Rozhodnutí ESLP č. 34315/96, ve věci *Krone Verlag proti Rakousku,* kde soud dovodil, že portréty politiků, jejichž tváře se běžně vyskytují na oficiálních internetových stránkách, mohou být svobodně zveřejňovány i v novinách, pokud nejde o snímky ze soukromého života.

Je tedy zajisté dobře, že výčet uvedený v generální klauzuli není enumerativní (taxativní), ale zůstává výčtem demonstrativním.

V některých případech tak jsou v rámci úpravy osobnostních práv stanoveny i konkrétní postupy (hodnoty), jejichž účelem je zvýšená hmotněprávní či procesní ochrana osobnostních práv (např. právo na pravdivá skutková tvrzení). Významný je pak také tiskový zákon, který upravuje některá práva a povinnosti vydavatelů a dalších fyzických a právnických osob v souvislosti s vydáváním periodického tisku. Jakkoliv nelze automaticky vyloučit analogickou aplikaci tiskového zákona na vydavatele (provozovatele) internetového zpravodajství (obsahově obdobného), tak lze trvat na závěru, že věcná působnost tiskového zákona na tyto vztahy nedopadá.[392] Ostatně tento záměr neměl ani sám zákonodárce, § 2 tohoto zákona však praví, že se zákon vztahuje na tisk vydávaný (pojem vydávání je definován v § 3) nebo šířený, což je v mnoha ohledech nepříliš vhodná formulace, která připouští vícerý výklad. Vzhledem k dalším ustanovením tohoto zákona však měl pojem šířený zahrnovat periodický tisk, který je vydávaný zahraničním vydavatelem a veřejně šířený na území České republiky, za předpokladu že zahraniční vydavatel má na území České republiky umístěnu organizační složku, nikoliv tedy elektronická periodika. Podstatné, a to i pro případnou možnost uplatnění analogie, jsou zejména ta ustanovení tohoto zákona, která upravují právo na uveřejnění odpovědi (§ 10) a právo na uveřejnění dodatečného sdělení (§ 11). Jestliže bylo v periodickém tisku uveřejněno sdělení obsahující skutkové tvrzení, které se dotýká cti, důstojnosti nebo soukromí určité fyzické osoby, anebo jména nebo dobré pověsti určité právnické osoby, má tato osoba právo požadovat na vydavateli uveřejnění odpovědi. Vydavatel je povinen na žádost této osoby odpověď uveřejnit.[393] Jestliže bylo v periodickém tisku uveřejněno sdělení o trestním řízení nebo o řízení ve věcech přestupků vedeném proti fyzické osobě anebo o řízení ve věcech správních deliktů vedeném proti fyzické nebo právnické osobě, kterou lze podle tohoto sdělení ztotožnit, a toto řízení nebylo ukončeno pravomocným rozhodnutím, má tato osoba právo požadovat na vydavateli uveřejnění informace o konečném výsledku řízení jako dodatečného sdělení. Vydavatel je povinen na žádost této osoby informaci o pravomocném rozhodnutí jako dodatečné sdělení uveřejnit. Podle ustanovení § 13 tohoto zákona je vydavatel povinen odpověď nebo dodatečné sdělení uveřejnit do 8 dnů ode dne doručení žádosti o uveřejnění odpovědi nebo dodatečného sdělení, a to:

a) *ve stejném periodickém tisku, v němž bylo uveřejněno napadené sdělení, a to takovým způsobem, aby nové sdělení bylo umístěním a formou rovnocenné a rozsahem přiměřené napadenému sdělení, a je-li napadena pouze jeho část, této jeho části,*
b) s výslovným označením „odpověď" nebo „dodatečné sdělení",
c) na vlastní náklady,
d) v témže jazyce, ve kterém bylo uveřejněno napadené sdělení,

392 K tomu opačně viz HRÁDEK, J. *Tiskový zákon pro Internet?* [online]. Server ITpravo.cz. Dostupné z: www.itpravo.cz/index.shtml?x=89570

393 Tato odpověď se však musí omezit pouze na skutkové tvrzení, kterým se napadené tvrzení uvádí na pravou míru nebo neúplné či jinak pravdu zkreslující tvrzení se doplňuje nebo zpřesňuje. Odpověď musí být přiměřená rozsahu napadeného sdělení, a je-li napadána jen jeho část, pak této části.

e) s uvedením jména a příjmení nebo názvu osoby, která o uveřejnění odpovědi nebo dodatečného sdělení žádá.

Neuveřejní-li vydavatel odpověď nebo dodatečné sdělení anebo nedodrží-li podmínky pro uveřejnění odpovědi nebo dodatečného sdělení, rozhodne o povinnosti uveřejnit odpověď nebo dodatečné sdělení na návrh osoby, která o jejich uveřejnění žádala, soud. Návrh musí být podán soudu do 15 dnů po uplynutí lhůty stanovené pro uveřejnění odpovědi nebo dodatečného sdělení, jinak právo domáhat se uveřejnění odpovědi nebo dodatečného sdělení u soudu zaniká. Efektivita uplatnění tohoto práva je pak obvykle podmíněna samotnou kvalitou souvisejících žádosti a dalších procesních kroků. Zákon totiž stanoví velmi obecné předpoklady, včetně zásady uvedené v § 10 odst. 2 zákona, že odpověď musí být přiměřená rozsahu napadeného sdělení a zároveň formou rovnocenná. Je otázkou, co má zákon na mysli, když požaduje, aby odpověď byla přiměřená rozsahu napadeného sdělení, bylo již zmíněno v komentáři u § 10. Odpověď má být uveřejněna tak, aby umístěním a formou bylo nové sdělení rovnocenné. Pojem byl použit se záměrem, aby se odpovědi dostalo pokud možno stejného slyšení, a to i pokud jde o umístění na příslušné straně z hlediska rozsahu textu, ale i formy podání. I když lze přisvědčit, že tyto požadavky je možné v zásadě akceptovat, tak nelze vyloučit, že v jednotlivostech nebude způsob uveřejnění s původním sdělením identický. Požadavek, aby nové sdělení bylo umístěním rovnocenné, neznamená, jak to vyžadoval předchozí tiskový zákon, uveřejnění na stejném místě, ale na místě, které je stejně hodnotné jako místo původního sdělení. Bylo-li sdělení uveřejněno na první straně, měla by i odpověď být uveřejněna na této straně, neboť z hlediska významu by uveřejnění na jiné straně zřejmě nebylo rovnocenné.[394]

Ochrana osob dotčených obsahem rozhlasového nebo televizního vysílání je upravena v hlavě druhé zákona č. 231/2001 Sb., o provozování rozhlasového a televizního vysílání, v platném znění, který ve svých ustanoveních § 35 a násl. obsahuje v zásadě identickou úpravu práva na uveřejnění odpovědi a právo na uveřejnění dodatečného sdělení, jak je tomu ve výše uvedeném tiskovém zákoně.

4.6.6 Prostředky ochrany proti neoprávněným zásahům do práva na ochranu osobnosti

Konkrétní (specifické) prostředky, jimiž se lze domáhat ochrany osobnosti, jakož i samotný rozsah konkrétních nároků, jsou pak vymezeny v ustanoveních § 13 ObčZ. Podle těchto ustanovení má fyzická osoba právo se zejména domáhat:

a) aby bylo upuštěno od neoprávněných zásahů do práva na ochranu její osobnosti,
b) aby byly odstraněny následky těchto zásahů,
c) aby jí bylo dáno přiměřené zadostiučinění.

394 CHALOUPKOVÁ, H. *Zákon o právech a povinnostech při vydávání periodického tisku (tiskový zákon) a předpisy související.* 2. vydání, 2006, s. 41–42.

Jak ostatně vyplývá z výše uvedených nároků (bod a), jakož i z jejich povahy, upuštění od neoprávněných zásahů do práva na ochranu její osobnosti se může fyzická osoba domáhat pouze v tom případě, kdy jde o zásah trvající (pokračující) povahy. Dotčená osoba se pak může domáhat zdržení se takovýchto neoprávněných zákroků, a to žalobou zdržovací.[395] Domáhat se odstranění následků již skončeného zásahu (bod b) do ochrany osobnosti (např. zničení neoprávněně pořízených projevů osobní povahy) se může dotčená osoba žalobou odstraňovací. Právo na přiměřené zadostiučinění (tzv. satisfakci) může být dotčené osobě přiznáno pouze v morální podobě (tzv. materiální satisfakce), a to např. v podobě stanovení povinnosti k veřejné omluvě. V odůvodněných případech však ObčZ připouští, že i satisfakci materiální (náhradu nemajetkové újmy v penězích), a to v případě, kdy by se morální satisfakce nejevila jako dostačující, a to zejména proto, že byla ve značné míře snížena důstojnost fyzické osoby nebo její vážnost ve společnosti. Výši této majetkové náhrady určí soud, a to s přihlédnutím k závažnosti vzniklé újmy a k okolnostem za nichž k porušení práva došlo.

Tyto prostředky ochrany osobnosti jsou uvedeny pouze demonstrativně, a lze tedy dovozovat, že občanskoprávní úprava ochrany osobnosti nevylučuje, aby dotčená fyzická osoba využila i jiných občanskoprávních prostředků určených k jejich ochraně. Soud tedy musí připustit i takové žaloby, které se ve svém petitu budou domáhat pouhého výroku soudu, resp. konstatování soudu o nepravdivosti určitých konkrétních výroků. Obecným (generálním) prostředkem proti neoprávněnému zásahu do práva na ochranu osobnosti pak je možnost fyzické osoby domáhat se náhrady způsobené škody. Ustanovení § 16 ObčZ uvádí, že ten, kdo neoprávněným zásahem do práva na ochranu osobnosti způsobil škodu, odpovídá za ni podle ustanovení ObčZ o odpovědnosti za škodu.

4.6.7 Aktivní legitimace k uplatňování ochrany proti neoprávněným zásahům do práva na ochranu osobnosti

K uplatnění ochrany proti neoprávněným zásahům do práva na ochranu osobnosti je primárně aktivně legitimována pouze dotčená fyzická osoba, jejíž práva, resp. dílčí složky ochrany osobnosti byly dotčeny konkrétním neoprávněným zásahem.

Ustanovení § 15 ObčZ však obsahuje tzv. posmrtnou (postmortální) ochranu osobnosti fyzické osoby. Zákon totiž vychází z předpokladu, že osobnost fyzické osoby by měla být chráněna i po její smrti, kdy se již nemůže zásahům do svých práv bránit. Zejména z tohoto důvodu přiznává ObčZ z titulu zvláštního právního nástupnictví (sukcese)[396] určitým taxativně vymezeným osobám zvláštní původní osobnostní právo na uplatnění ochrany osobnosti zemřelé fyzické osoby. Občanský zákoník (§ 15) tato práva přiznává výlučně manželovi, partnerovi[397] a dětem (osvojencům) zemřelé fyzické osoby, a není-li jich, jejím rodičům (osvojitelům). Man-

395 Tzv. negatorní žaloba.

396 Nejde tedy o dědění ve smyslu § 460 ObčZ, ale o zvláštní právní nástupnictví založené § 15 ObčZ.

397 Nejde toliko o druha, resp. o družku, ale pouze o registrovaného partnera ve smyslu zákona č. 115/2006 Sb., o registrovaném partnerství, v platném znění.

žel, partner a děti zemřelé osoby mohou toto právo uplatnit každý sám a samostatně, přičemž k uplatnění tohoto práva jednou z těchto osob není zapotřebí souhlasu ostatních. Právo na postmortální ochranu může být uplatněno pouze po smrti dotčené fyzické osoby bez zřetele k tomu, byl-li neoprávněný zásah učiněn ještě za jejího života či nikoliv.[398]

4.6.8 Zákonné omezení práv osobnostních

Navzdory výše uvedeným obecným principům úpravy ochrany osobnosti v občanském právu připouští ObčZ určité zásahy do osobnostních práv, a to z důvodů úředních, vědeckých, uměleckých a reportážních. Občanský zákoník tyto důvody, resp. výjimky z ochrany osobnosti, výslovně uvádí v ustanovení § 12, který ve svém prvním odstavci nejprve stanoví, že písemnosti osobní povahy, podobizny, obrazové snímky a obrazové a zvukové záznamy týkající se fyzické osoby nebo jejích projevů osobní povahy smějí být pořízeny nebo použity jen se svolením příslušné fyzické osoby. Zákon však z tohoto principu připouští hned několik výjimek, a to v ustanovení § 12 odst. 2 a 3 ObčZ.

První výjimka je tvořena tzv. úřední licencí, která spočívá v tom, že souhlasu dotčené fyzické osoby není třeba, použijí-li se písemnosti osobní povahy, podobizny, obrazové snímky nebo obrazové a zvukové záznamy k účelům úředním na základě zákona. Druhou výjimkou, resp. skupinou výjimek, jsou licence vědecká, umělecká a reportážní. Podle ustanovení § 12 odst. 3 mohou být bez svolení fyzické osoby pořízeny nebo použity přiměřeným způsobem podobizny, obrazové snímky a obrazové a zvukové záznamy pro vědecké a umělecké účely a pro tiskové, filmové, rozhlasové a televizní zpravodajství. Ani takové použití však nesmí být v rozporu s oprávněnými zájmy fyzické osoby.

4.7 Pracovněprávní úprava

V řadě právních oborů se stává, že technický pokrok jakoby „předbíhá" platnou právní úpravu. Nejinak je tomu i v případě úpravy pracovněprávní. Kupodivu tomu tak není vždy z důvodu nedbalosti či neznalosti zákonodárce, ale zejména proto, že technika a věda vůbec jsou fenoménem, který sám o sobě musí být vždy dynamičtější. Jednou z oblastí, která je, v důsledku dosud zcela nevídaného rozvoje odposlouchávacích, kamerových a jiných podobných zařízení, stále častěji veřejností v tomto smyslu přetřásána, je vyjma obecné problematiky ochrany osobnostních statků člověka, také ochrana těchto statků při výkonu práce zaměstnance pro zaměstnavatele. Zatímco stávající právní úprava ochrany osobnostních práv člověka (viz předchozí kapitola) se nedočkala za posledních padesát let žádných výrazných změn, informační a komunikační technologie,

398 K tomu více JEHLIČKA, O., J. ŠVESTKA, a M. ŠKÁROVÁ. *Občanský zákoník: komentář.* 7. vydání. Praha: C. H. Beck, 2002, s. 103.

které umožňují do tohoto práva velmi efektivně zasáhnout, naopak prošly změnami zcela zásadními, a to včetně jejich (zejména cenové) dostupnosti. Je tedy zcela zřejmé, že řada právních odvětví se nutně musí potýkat s otázkou, zda vybrané právní předpisy stále více nezaostávají za reálným ekonomickým životem a praktickými potřebami ekonomických subjektů. Jedním z odvětví, které v minulých letech šlo touto cestou, bylo pochopitelně pracovní právo.[399] Nová pracovněprávní úprava k problematice absence řešení ochrany osobnostních práv zaměstnance v pracovněprávních vztazích přistoupila odlišně, a to začleněním zvláštní úpravy částečné ochrany těchto práv ve formě normativních ustanovení § 316 zákoníku práce, a to právě z důvodu absence[400] dosavadní úpravy, kde se ochrana zaměstnance v těchto vztazích musela „dohánět" výkladem za použití obecných ústavních východisek vyplývajících z Listiny základních práv a svobod a za použití § 7 odst. 2 dosavadního zákoníku práce o postupu podle zásady dobrých mravů.[401]

Úmluva se sociálních práv dotýká pouze okrajově,[402] a její význam pro obor pracovního práva se tak projevuje spíše ve specifických, nikoliv však významově marginálních oblastech.[403] Jednou z nich je právo zaměstnance na ochranu soukromí. V Úmluvě je toto základní lidské právo chráněno především čl. 8 jako právo na respektování soukromého a rodinného života. Dílčí prvky ochrany jsou obsaženy v čl. 6 Úmluvy v podobě „práva na soud"[404] a čl. 10 v právu na svobodu projevu. Práva dle čl. 8 Úmluvy jsou svou povahou speciální vůči právu dle čl. 10 Úmluvy.[405] Mezinárodní úprava má pro zlepšení pracovních podmínek zaměstnanců zcela zásadní význam, a to nejen v České republice. Po vstupním pojednání o povaze práva zaměstnance na soukromí, resp. práva na respektování soukromého a rodinného života (čl. 8 odst. 1 Úmluvy), nutno tak další výklad zaměřit na logiku čl. 8 odst. 2 Úmluvy. Právo každého na respektování soukromého a rodinného života, obydlí a korespondence míří především vůči státu, kterému ukládá být pasivní,

399 V tomto ohledu je nutné podotknout, že předchozí úprava zákonem č. 65/1965 Sb., zákoník práce, ve znění pozdějších novel, (tj. úprava účinná až do konce roku 2006) byla problematická hned v několika ohledech, kde především na úpravu osobnostních práv vůbec nepamatovala. Klíčovým problémem zde byla zejména skutečnost, že tehdejší pracovněprávní předpisy ochranu osobnostních práv zaměstnanců neřešily buď vůbec, anebo pouze zcela okrajově. Předchozí zákoník práce se totiž těchto práv dotýkal pouze výjimečně (jde zejména o ustanovení § 7 odst. 2, jež poskytuje ochranu před ponižováním lidské důstojnosti účastníka pracovněprávního vztahu, dále pak § 22 odst. 2. Poněkud krkolomně a obtížně se tedy dovozovalo, že v těch případech, které nejsou ošetřeny výslovnou právní úpravou zákoníku práce ani speciálních předpisů, je namístě využití analogie iuris, a tedy aplikace ustanovení ObčZ § 11 a násl. o ochraně osobnosti, a to za podmínky, že to vyžaduje integrita obecných zásad právních a pracovněprávních. Takové řešení se však stále více ukazovalo jako poměrně komplikované, navíc v praxi zřídka kdy dochází k jeho uplatnění.

400 K tomu srovnej MATEJKA, J. K oprávnění zaměstnavatele kontrolovat práci zaměstnance pomocí moderních technologií. *Právo a zaměstnání.* 2003, č. 5, s. 7–16.

401 Viz důvodová zpráva k zákonu č. 262/2006 Sb., zákoníku práce.

402 Jde především o zákaz nucené práce (čl. 4), zákaz diskriminace (čl. 14), koaliční svobody (čl. 11) a práva na spravedlivý proces (čl. 6) jako procesní záruky při omezování sociálních práv.

403 Informace získané zaměstnavatelem ze soukromí zaměstnance, resp. navzdory ochraně soukromí zaměstnance mohou sloužit ke skončení pracovního poměru s tímto zaměstnancem či k založení odpovědnosti zaměstnance za škodu způsobenou zaměstnavateli. Srov. *Financial Times Ltd a další v. Spojené království,* stížnost č. 821/03. Z vnitrostátní judikatury lze zmínit recentní rozsudek NS sp. zn. 21 Cdo 4928/2010.

404 ESLP rozsudek *McMichael v. Spojené království* 1995, A-307-B, s. 57, § 91.

405 ESLP rozsudek Silver 1983, A-61, § 106–107.

nezasahovat. Jedná se především o povinnost zákonodárce respektovat při tvorbě národní legislativy omezení plynoucí z čl. 8 Úmluvy. I my, proto podrobíme národní úpravu testu souladnosti zákona s čl. 8 Úmluvy. Omezena je též výkonná moc. Ta může do soukromého života zaměstnance zasáhnout pouze v souladu s platnou právní úpravou. ESLP však v některých případech tento výklad překročil a založil jednak aktivní povinnost státu něco činit k ochraně narušeného práva,[406] jednak povinnost zaměstnavatele určitého jednání se zdržet.[407]

4.7.1 Právo zaměstnance na soukromý a rodinný život

ESLP neshledal možným (ale ani nutným) podat vyčerpávající definici pojmu „soukromý život". Toto právo má též zaměstnanec, a to přestože jeho základní povinností je během pracovní doby pracovat pro zaměstnavatele. Jak dovodil též ESLP nelze odepřít ochranu dle čl. 8 odst. 1 Úmluvy jen z toho důvodu, že napadené opatření se vztahuje pouze na profesní činnost. Jak bylo judikováno, při současném odposlouchávání obchodních i soukromých hovorů došlo k zásahu do soukromého života.[408] Zmínit pak je nutné především rozsudek *Halfordová v. Spojené království*, kde ESLP založil legitimnost očekávání zaměstnankyně, že uskutečněné hovory jsou soukromé na tom, že zaměstnankyně ve své funkci generálního kontrolora měla k dispozici vlastní místnost vybavenou dvěma telefonními aparáty (z nichž jeden byl určen k soukromým hovorům) a dále na absenci předchozího poučení o odposlouchávání telefonních hovorů. Soud z tohoto důvodů dospěl k závěru, že hovory uskutečněné stěžovatelkou z pracoviště spadají pod pojmy "soukromý život" a "korespondence" a čl. 8 Úmluvy je na ně aplikovatelný. Pojmy soukromý život a obydlí dle čl. 8 odst. 1 Úmluvy je proto v této souvislosti třeba interpretovat jako zahrnující též místa profesní či komerční aktivity.[409] Na základě judikatury ESLP[410] a později též českého Ústavního soudu lze shrnout, že soukromým životem dle čl. 8 Úmluvy, resp. soukromím dle čl. 7 Listiny základních práv a svobod, je třeba rozumět jednak osobní soukromí člověka (osobní sféra jednotlivce, tedy např. údaje týkající se identifikace pohlaví, jména, sexuální orientace a sexuálního života), jednak právo každého člověka na vytváření a rozvíjení vztahů s dalšími lidskými bytostmi (soukromé i profesní povahy, jakási zóna interakce zaměstnance s jinými jednotlivci). Dle čl. 8 Úmluvy požívá ochrany též korespondence, a to v písemné i elektronické podobě.[411] Součástí tohoto práva naopak není např. právo vybrat si zaměstnání[412] či právo na informace o členství soudce v KSČ ke dni 17. 11. 1989.[413]

406 ESLP rozsudek *Marckx v. Belgie* 1979, A-31, § 31.
407 ČAPEK, J. *Evropská úmluva o ochraně lidských práv a základních svobod: I část: Úmluva.* Praha: Linde, 2010, s. 286.
408 ESLP rozsudek *Huvig v. Francie* 1990, A-176-B, § 8 a 25.
409 ČAPEK, J., ref. 407, s. 283.
410 ESLP rozsudek Niemitz 1992, A-251-B, *Klass a ostatní v. Německo,* 1978, A-28 nebo Malone v. UK, 1984, A-82.
411 ESLP rozsudek *Klass a ostatní,* § 48–49.
412 ESLP rozsudky *Glasenapp a Kosiek v. Německo,* 1986, A-104, § 49, a A-105,§ 35; dále též *Vogt v. Německo,* 1995, A-323, § 43-44) nebo *Thlimmenos v. Řecko,* 2001, stížnost č. 34369/97, § 41, ECHR 2000-IV.
413 US nález sp. zn. I. ÚS 517/10.

Míra ochrany soukromí je u zaměstnance určována charakterem prostor, ve kterých se nachází,[414] dobou, kdy se v nich nachází, jeho vztahem k danému místu a legitimnímu očekávání vzhledem k těmto faktorům. Pokud např. zaměstnanec vede rozhovor se soukromou osobou, oprávněně očekává, že hovoří pouze s touto osobou a nikoliv se svým zaměstnavatelem, resp. oddělením pro vnitřní záležitosti.[415] V této souvislosti je nutné dále zohlednit, že přestože pracovněprávní vztah vytváří velmi osobní dlouhodobé pouto mezi zaměstnavatelem a zaměstnancem, i na pracovišti v pracovní době musí zůstat výkon práva zaměstnance na soukromý a rodinný život praktický a účinný.[416]

4.7.2 Národní úprava

Zasahování do soukromého a rodinného života a korespondence se stává porušením čl. 8 Úmluvy, pokud není v souladu se zákonem, pokud nesleduje legitimní cíl či cíle dle čl. 8 odst. 2 Úmluvy a pokud není nezbytné pro dosažení těchto cílů.[417] Zákon musí být přiměřený, dosažitelný a předvídatelný.[418] Zákon dále musí vykazovat kvalitu odpovídající principům právního státu, zejména musí být dostatečně přesný. Nezbytnost zásahu předpokládá jeho celkovou přiměřenost vzhledem ke sledovanému cíli, nezbytnost pak v demokratické společnosti zahrnuje určitou naléhavou sociální potřebu.[419] Musí být zachována kontrola nezávislým soudem proti svévolnému zasahování do práva na soukromý a rodinný život.[420]

Základem české ochrany soukromí člověka je úprava v čl. 7 Listiny[421] a ustanovení § 11 a násl. ObčZ. Obecná úprava ochrany osobních údajů obsažena v ZoOÚ a zákoník práce stejně jako zákon o zaměstnanosti představují speciální úpravu ochrany osobních údajů zaměstnance. Občanskoprávní úprava působí vůči obecné a speciální úpravě podpůrně.[422] V zákoníku práce

414 Srov. rozsudek ESLP *Uzun v. Německo,* stížnost č. 35623/05, kde soud přirovnal očekávání osob monitorovaných ve veřejném prostoru s pomocí technologických prostředků (zaměstnanci ostrahy sledující prostor skrze kamery v uzavřeném televizním okruhu) k očekáváním osoby kráčející po ulici.

415 ESLP rozsudek von *Vondel v. Nizozemsko,* 2007, ke stížnosti č. 38258/03.

416 ESLP rozsudek *K. H. a ostatní v. Slovensko,* § 46 a násl. Dále též *M. G. v. Spojené království* 202, stížnost č. 39393/98, § 31.

417 Např. ESLP rozsudek Krusslin 1990, A-176, § 26.

418 ESLP rozsudek Sunday Times 1979, A-30, § 47-49.

419 ČAPEK, J., ref. 407, s. 281.

420 ESLP rozsudek Niemietz 1993, A-251-B, § 69.

421 Též ochrana soukromí dle čl. 7 Listiny je doplněna ochranou poskytovanou dalšími ustanoveními Listiny. Tak čl. 10 odst. 3 Listiny upravuje právo každého na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě a čl. 13 Listiny stanoví, že nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon; stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením.

422 MATEJKA, J. a J. ZACHARIÁŠ. Ochrana osobních práv v pracovněprávních vztazích. *Karlovarská právní revue.* 2007, č. 1, s. 60 a násl. Dále především MORÁVEK, J. *Předávání osobních údajů do zahraničí: česká a evropská právní úprava, otázky a odpovědi.* Praha: Linde, 2012, s. 33.

se soukromí zaměstnance zvlášť intenzivně dotýkají ustanovení § 30 a 316. V ustanovení § 316 odst. 1, 2, 3 zákoníku práce je upraven výkon práva kontroly (tato ustanovení je nutné vykládat společně), resp. právo zavést sledovací opatření a v § 316 odst. 4 obecný rámec pro získávání informací týkajících se zaměstnance.[423] Zaměstnanec je dle této úpravy, zřejmě ve shodě s judikaturou ESLP,[424] povinen sdělovat, resp. umožnit sběr informací týkajících se jeho osoby, pokud se tyto informace týkají vykonávané práce nebo je zaměstnavatel potřebuje ke splnění svých povinností stanovených obecně závaznými právními předpisy. Otázkou tedy dle české úpravy není, zda zaměstnavatel může provádět zpracovávání údajů týkajících se osoby zaměstnavatele, ale v jakém rozsahu tak může činit. Zaměstnavatelovo právo kontrolovat zaměstnance totiž naráží na právo každé lidské bytosti na ochranu její lidské důstojnosti a ve smyslu čl. 8 Úmluvy též práva na respektování soukromého a rodinného života.[425]

V České republice tedy existuje explicitní zákonná úprava, na jejímž základě je zaměstnavatel oprávněn zasahovat do soukromého a rodinného života zaměstnance. K rozsahu tohoto oprávnění zaměstnavatele se vyjádřil i Nejvyšší soud, který v jednom ze svých posledních rozhodnutí[426] zaujal výklad ustanovení § 316 zákoníku práce, které dovoluje zaměstnavateli přiměřeným způsobem kontrolovat zákaz využívat výrobní a pracovní prostředky zaměstnavatele včetně výpočetní techniky zaměstnancem pro osobní potřebu. Soud v tomto ohledu mimo jiné uvedl, že z dosavadní právní úpravy vyplývá, že není vyloučeno, aby zaměstnanec využíval výrobní a pracovní prostředky zaměstnavatele včetně výpočetní techniky, případně jeho telekomunikační zařízení i pro svou osobní potřebu, ale toliko se souhlasem zaměstnavatele. Tak může zaměstnavatel souhlasit s tím, aby jeho počítač (podobně jako přidělený psací stroj) byl použit i pro napsání soukromého dopisu, aby služební telefon byl používán i k soukromým telefonátům nebo aby přidělená výpočetní technika byla používána i pro soukromé potřeby zaměstnance. Protože zákonem stanovený zákaz používat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele je absolutní, může zaměstnavatel souhlas k jejich použití stanovit v libovolném rozsahu (od úplného souhlasu bez jakéhokoli omezení přes souhlas jen v určitém rozsahu časovém nebo věcném až třeba po souhlas jen k jednorázovému použití). Stanovení rozsahu souhlasu k použití výrobních a pracovních prostředků zaměstnavatele pro osobní potřebu zaměstnance (zaměstnanců) je zcela na vůli zaměstnavatele. Samotná zákonná úprava je veřejně dostupná, zásahy zaměstnavatele podléhají jak správnímu dozoru ze strany inspekce práce, resp. Úřadu, tak se může zaměstnanec domáhat ochrany u nezávislého soudu. V souladu s mezinárodními závazky a unijním právem je též zaměstnavatel omezen ve svém jednání. Je-li možné něco národní úpravě něco obecně vytknout, pak je to extrémně rychlý roz-

423 Úprava v § 316 odst. 1, 2 a 3 je kogentní, od odst. 1 se lze odchýlit ku prospěchu zaměstnance, jedná se tedy o úpravu polonutkavou (při použití terminologie prvorepublikové terminologie).

424 K tomu srov. ESLP rozsudek *Copland vs. Spojené království*, 2007, ke stížnosti č. 62617/00. Soud zde akceptoval, že někdy může být pro zaměstnavatele legitimní monitorovat či kontrolovat užívání telefonu a internetu zaměstnancem.

425 MATEJKA, J. a M. ŠTEFKO. Osobní povaha pracovněprávních vztahů. *Právník*. 2012, č. 8, s. 872–891, ISSN 0231-6625.

426 Rozhodnutí Nejvyššího soudu č. 21 Cdo 1771/2011, jehož předmětem byla kontrola dodržování zákazu uvedeného v ustanovení § 316 odst. 1 zák. práce, jejíž výkon zaměstnavateli umožňuje zákon, a nikoli o sledování soukromí zaměstnance.

voj veřejnoprávních předpisů chránících či naopak zasahujících do soukromí jednotlivce. S tím souvisejí četné nejasnosti při aplikaci pracovněprávní úpravy ochrany soukromí zaměstnance. Tak např. ustanovení § 316 zákoníku práce představuje tzv. fakultativní důvod pro zpracovávání osobních údajů, což znamená, že zaměstnavatel je povinen vždy svůj záměr sledovat zaměstnance oznámit Úřadu.[427] Lze jistě i argumentovat opačně, tedy obligatorností tohoto důvodu. V takovém případě by ovšem zaměstnavatel nebyl povinen splnit registrační povinnost. Striktní výklad o fakultativnosti je v každém případě zastáván u sledovacího kamerového systému.

4.7.3 Meze výkonu práva kontroly

Zaměstnavatel je oprávněn provádět kontrolu zaměstnance za účelem předejití možným škodám (obdobně § 248 odst. 2 zákoníku práce), ustanovení § 316 odst. 2, 3 zákoníku práce omezují zaměstnavatele pouze ve zvlášť intenzivním, soustavném a systematickém kontrolování zaměstnance,[428] ať už se děje otevřeně či skrytě.[429] Zákoník práce stanoví dodatečné (k podmínkám vyplývajícím z obecné úpravy v zákonu o ochraně osobních údajů, jako je např. stanovení účelu zpracovávání osobních údajů, rozsahu jejich zpracovávání, testu proporcionality, zabezpečení ochrany zpracovávaných osobních údajů, zpracovávání pouze pravdivých a přesných údajů atd.) podmínky, které zaměstnavatel musí naplnit, před zavedením sledovacích opatření. Ve shodě s judikaturou ESLP je zaměstnavatel oprávněn provádět kontrolu zaměstnance formou otevřeného a nikoliv tajného sledování.[430] Konkrétní způsob provádění sledování zákoník práce neomezuje, stanoví však, že zavedení kontrolních mechanismů musí být odůvodněno závažným důvodem. Kontrola musí být provedena přiměřeným způsobem. Další podmínkou je předchozí písemná informace všech dotčených zaměstnanců o rozsahu kontroly a o způsobech jejího provádění. Prováděním sledovacích opatření nesmí dojít k nepřiměřenému zásahu do soukromí zaměstnance. Jako takové by bylo hodnoceno ve shodě s judikaturou ESLP jednání zaměstnavatele, který např. prohledá v nepřítomnosti zaměstnance jeho psací stůl a skříň na spisy. Zaměstnanec totiž v takovém případě může oprávněně předpokládat, že jeho psací stůl i skříň na spisy budou pokládány za soukromý majetek, protože zde má uloženy i své vlastní potřeby.[431]

Úprava v zákoníku práce je však pouze částí relevantní právní úpravy, další omezení vyplývají z obecné úpravy obsažené v ZoOÚ. Povinnosti vyplývající ze ZoOÚ se budou na zaměstnavatele vztahovat tehdy, pokud bude provozovat sledovací systém, který uchovává záznam

427 Obligatorním důvodem ke zpracovávání osobních údajů povinnost evidovat pracovní dobu v rozsahu § 96 zákoníku práce.

428 K tomu srovnej BĚLINA, M., L. Drápal a kol. *Zákoník práce: komentář.* Praha: C. H. Beck, 2012. Autorem příslušné části komentáře k § 316 je M. ŠTEFKO.

429 Srov. rozsudek ESLP *Uzun v. Německo,* stížnost č. 35623/05, kde soud konstatoval, že otázky týkající se práva na soukromí mohou vyvstat v okamžiku, kdy vznikne jakýkoliv systematický či stálý záznam takového materiálu pořízeného z veřejného prostoru. Dále *P. G. a J. H. v. Spojené království,* § 57; *Peck v. Spojené království,* § 58–59 a *Perry v. Spojené království,* § 38.

430 ESLP rozsudek Leander 1987, A-116, § 48, Klass a ostatní 1978, A-28 a rozsudek Malone 1984, A-82.

431 ESLP rozsudek *Peev v. Bulharsko,* 2007, ke stížnosti 64209/01

pořizovaných záběrů či informací, a zároveň účelem pořizovaných záznamů (informací) je jejich využití k identifikaci fyzických osob v souvislosti s určitým jednáním. Takovým systémem je např. kamerový systém, různé systémy sledující práci na počítači (sledování, které internetové stránky zaměstnanec navštívil a jak dlouho je prohlížel, jakož i sledování využívání aplikací na přiděleném osobním počítači), monitorující listovní a e-mailovou korespondenci či telefonní komunikaci (odposlech, příposlech a záznam zaměstnancových telefonických hovorů).[432]

Důvodem může být ochrana života a zdraví zaměstnavatele, zaměstnance, spoluzaměstnanců a jiných osob, které se v kontrolovaném prostoru zdržují. Dalšími legitimními důvody jsou ochrana majetku zaměstnavatele, spoluzaměstnanců a jiných osob a kontrola pracovní výkonnosti zaměstnance. Nelze tedy souhlasit s názory, které právo kontrolovat přiznávají pouze zaměstnavateli vykonávajícímu činnost zvlášť nebezpečnou či mimořádně ohrožující (např. jaderná elektrárna atd.). Na základě stanoviska č. 8/2001 (č. j. 5062/EN/Final), zpracovaného speciálním kolegiem expertů ustavených dle čl. 29 Směrnice, lze kontrolní právo přiznat při splnění dále uvedených podmínek každému zaměstnavateli. Důvod, pro který zaměstnavatel zahájí sledovací opatření, určuje a do značné míry limituje způsob provedení kontroly. Tomuto důvodu musí být přizpůsobeny organizační a technické parametry použitých sledovacích zařízení. Nejvíce omezujícím je v tomto směru sledování pracovní výkonnosti zaměstnance. V odborné literatuře se profilují názory na tzv. činnost v širším a užším smyslu. Praktické návody obecně aplikovatelné však zatím k tomuto podány nebyly.[433]

Ve světle názorů Komise a judikatury ESLP lze tyto důvody označit za interní důvody zaměstnavatele. Vedle těchto důvodů lze rozlišovat též důvody externí, jako např. národní bezpečnost. Tak např. bezpečnostní kontrola uchazečů o zaměstnání sama o sobě do práva na respektování soukromého a rodinného života nezasahuje, pokud též nedojde ke zpracovávání údajů o soukromém životě uchazeče.[434] Rozsah sledovaných a zaznamenávaných informací je ovlivněn důvodem, pro který se sledovací opatření zavádějí. Vedle tohoto omezení je třeba zmínit, že některé údaje jsou z povahy věci z kontroly vyloučeny. Příkladem relevantním z hlediska existence pracovně-lékařských služeb a úpravy jejich komunikace se zaměstnavatelem pacienta je ochrana zdravotních údajů. Respektování důvěrnosti zdravotních údajů je důležitým principem v právních systémech všech smluvních států Úmluvy, a to jednak pro respektování pocitu soukromí pacienta, jednak z důvodu zachování pacientovy důvěry v lékařskou profesi a zdravotnické služby vůbec. Bez takové ochrany by se lidé potřebující lékařskou pomoc obávali odhalovat informace o osobním a intimním životě nebo by se vůbec mohli obávat vyhledat lékařskou pomoc.[435] Dalším příkladem je „úřední" pohlaví u transsexuála.[436]

---

432 V případě kamerového systému je nutné zdůraznit, že musí jít o systém, který bude sledovat uzavřené prostory, kde se předpokládá pohyb osob. Sledovací systém, který pouze zprostředkuje aktuální snímek sledovaného děje bez následné archivace, nezpracovává osobní údaje. K tomu více viz MATEJKA J. a M. ŠTEFKO. Osobní povaha pracovněprávních vztahů. *Právník*. 2012, č. 8, s. 872–891, ISSN 0231-6625.

433 BĚLINA, M., L. Drápal, a kol., ref. 428

434 Komise rozhodnutí *Hilton v. Spojené království* 1988, stížnost 12015/86, D.R. č. 57, s. 108–130.

435 ESLP rozsudek *Szuluk v. Spojené království,* § 48; dále *Hurtado v. Švýcarsko* 1994, A-280-A, názor Komise, § 79 a rozsudek *Mouisel v. Francie,* stížnost č. 67263/01, § 40, ECHR 2002-IX.

436 *B. v. Francie* 1992, A-232-C).

Ze stávající judikatury evropských a českých soudů a rozhodnutí Úřadu vyplývá, že zaměstnavatel nesmí sledovat, monitorovat ani zpracovávat obsah telefonické, e-mailové a listinné korespondence svých zaměstnanců. Bez dalšího lze sledovat počet došlých a odeslaných e-mailových zpráv, a to včetně adresy odesílatele. Pokud jde o telefonický hovor, pak je podstatně snížena nebezpečnost jednání včasným upozorněním dotčených osob o zavedení sledovacích opatření.[437] V případě sledování pohybu zaměstnance na Internetu je přípustné monitorovat (nahodile) datum, hodinu a čas strávený prohlížením určité webové stránky.[438] Vhodná, velmi efektivní a právně bezvadná je předchozí blokace určitých webových stránek či domén, které jsou pro výkon práce nepoužitelné.[439]

Zaměstnavatel je oprávněn provádět pouze otevřené sledování. Část odborné literatury, která připouští též skryté sledování, pro oprávněnost tohoto typu sledování zatím nenabídla žádné podporující soudní rozhodnutí. ESLP v této souvislosti hovoří o „oprávněném nebo přiměřeném očekávání na soukromí" nebo o „předvídatelnosti" zaměstnance, že jeho jednání má povahu soukromou.[440] Zaměstnavatel je proto povinen předem informovat zaměstnance o rozsahu kontroly (jaké údaje budou shromažďovány) a o způsobech jejího provádění (kde a po jakou dobu budou shromážděné údaje uschovány, kdo k nim má přístup, kdo bude provádět kontrolu, které údaje se budou dlouhodobě archivovat, jaká jsou bezpečnostní opatření na zabránění neoprávněného přístupu atd.). Měl by tak učinit rozmístěním informativních cedulí a dále podrobnou úpravou ve vnitřním předpise (či kolektivní smlouvě). Půjde-li o zavedení sledovacího systému, který bude uchovávat informace sloužící k identifikaci osob, pak lze z rozhodnutí a stanovisek úřadu dovodit následující obecná doporučení.[441] Před zavedením sledovacích opatření je nutné oznámit úmysl zpracovávat osobních údaje úřadu. Sledování je možné provádět pouze namátkově, zaměstnanec musí mít šanci „uniknout" (tzv. princip „fair play"). Sledovat lze prostory, kde došlo k protiprávnímu jednání (např. opakované krádeže) nebo jde o plnění povinností stanovených obecně závaznými právními předpisy (např. zajištění bezpečnosti a ochrany zdraví při práci). Nelze použít jiný méně soukromý zasahující prostředek. K tomuto kritériu tzv. invazivnosti sledovacích opatření je možné uvést, že sledování výkonnosti zaměstnanců je povinností vedoucího zaměstnance. Především tento zaměstnanec by měl být přítomen na pracovišti a soustavně sledovat výkonnost podřízených zaměstnanců. Kontrolu pořízených záznamů bude provádět komise, jejímž členem bude také zástupce zaměstnanců; kontrolu je třeba provést zpravidla druhý den po pořízení záznamu, nejpozději však do tří dnů. Ihned po zjištění protiprávního jednání musí zaměstnavatel učinit oznámení na policii, případně jiných příslušných orgánech. Dlouhodobě lze archivovat pouze pozitivní záznamy (důkaz o protiprávním jednání, dochází ke změně důchodu evidence a archivace těchto osobních údajů).

437 Srov. rozhodnutí NS sp. zn. 21 Cdo 1009/98.

438 MORÁVEK, J. *Průvodce ochranou osobních údajů v pracovněprávní agendě.* Praha: BMSS-Start, 2010, s. 4 a násl.

439 K tomu více viz MATEJKA, J. a M. ŠTEFKO. Osobní povaha pracovněprávních vztahů. *Právník.* Rok 2012, č. 8, str. 872–891, ISSN 0231-6625.

440 ESLP rozsudek *Halfordová v. Spojené království,* Příloha časopisu *Soudní Judikatura.* 2000, č. III, Přehled judikatury ve věcech ochrany osobnosti, s. 33.

441 Zejména Stanoviska č. 6/2002, 1/2003, 4/2004, 1/2006, 1/2007 a 2/2009.

Pokud je předmětem kontroly výkonnost zaměstnance či na záznamu mohou být obsaženy záznamy zaměstnance, je vhodné takovému zaměstnanci umožnit zhlédnutí pořízeného záznamu (princip transparence). Zaměstnavatel je povinen vytvořit organizační a technické zábrany neoprávněnému přístupu k archivovaným záznamům (např. přístup k elektronickým datům je umožněn po zadání hesla, jsou archivovány údaje o osobě prohlížející údaje, uschovávají se záznamy o učiněných změnách, kódování dat v případě přenosu dat jinému subjektu, sjednání zpracovatelské smlouvy atd.). V písemné zpracovatelské smlouvě je nutné vymezit v jakém rozsahu, za jakým účelem a na jakou dobu se sjednává a záruky zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů.[442]

Vedle obecných doporučení lze učinit několik poznatků k monitorování listinné a e-mailové korespondence, a to právě se zřetelem na výslovnou úpravu dle čl. 8 Úmluvy. Zvlášť intenzivně je chráněna korespondence s advokátem, tu lze pouze otevřít, nikoliv však číst. Dle ESLP musejí být vytvořeny dostatečné záruky pro zabránění čtení této korespondence, jako je např. otevření listovní zásilky v přítomnosti vězně, existence racionálního důvodu pro uskutečnění kontroly a výjimečnost otevírání tohoto privilegovaného typu korespondence.[443] Ještě intenzivnější ochrana se uplatní při kontrole dopisu vězně adresovaného advokátovi. Ten lze číst jen opravdu za výjimečných okolností.[444]

K čl. 8 Úmluvy se váže rozsáhlá judikatura ESLP, která zůstává cenným inspiračním zdrojem pro českého zákonodárce, vnitrostátní soudy i aplikační praxi. Pokud jde o ústavodárce lze např. zmínit, že čl. 8 Listiny ve své původní podobě v tisku č. 330 i 331[445] neobsahoval explicitně pojem soukromí. K jeho doplnění došlo až po jednání na ústavněprávních výborech.[446] Podobně lze argumentovat též u prostého práva, kdy zákonodárce reagoval v zákoníku práce teprve v roce 2007, a to spíše problematickým způsobem. Je tak stále pravdou, že též vůči zákonodárci si navzdory své obecnosti a zčásti též specifičnosti čl. 8 Úmluvy a k němu vztahující se judikatura ESLP zachovává významnou regulativní funkci. Právě na úrovni obyčejného práva jsme totiž v posledních letech svědky hypertrofie veřejného práva. Díky čl. 8 Úmluvy je stále živou otázkou, zda i dnes odpovídá česká roztříštěná úprava požadavku dostatečné přesnosti zákona. Protože, jak formuloval ESLP, tato přesnost musí občanovi umožňovat orientovat se v této úpravě a reagovat na její porušení.[447] Zmínili jsme především zásadní spor o povahu ustanovení § 316 zákoníku práce, o jeho obligatornost či fakultativnost. Národní úprava tak přesně neodpovídá na jednoznačnou otázku, zda je zaměstnavatel oprávněn sledovat zaměstnance ex lege či zda musí splnit další požadavky stanovené zákonem o ochraně osobních údajů.

442 BĚLINA, M., L. DRÁPAL a kol., ref. 428.

443 Např. ESLP rozsudek Fox, Cambell a Hartley 1990, A-182, § 32 a rozsudek Campbell 1992, A-233, § 48.

444 MATEJKA, J. ŠTEFKO, M. Osobní povaha pracovněprávních vztahů. *Právník.* 2012, č. 8, s. 872–891, ISSN 0231-6625.

445 Srov. www.psp.cz/eknih/1990fs/tisky/t0330_01.htm (vid. 13. června 2012).

446 Tisk č. 392 FS ČSFR.

447 Zpráva Komise k případu *Hewitt a Haman v. Spojené království* 1989, D.R. č. 67, s. 88–122. Zpráva Komise k případu Hewitt a Haman v. Spojené království 1989, D.R. č. 67, s. 88–122.

Rychlý rozvoj techniky umožňuje zaměstnavateli kontrolovat své zaměstnance neustále sofistikovanějšími metodami a přístroji. Stejně tak na základě společenské poptávky dochází zákonem k umožnění stále intenzivnějších zásahů do soukromí nejen zaměstnanců. Český zákonodárce přitom stále není schopen uživatelům práva nabídnout srozumitelnější obecné kritérium legitimnosti pocitu soukromí, než jaké v podobě legitimnosti očekávání dovodila rozhodovací praxe ESLP. Míra ochrany soukromí je u zaměstnance určována charakterem prostor, ve kterých se nachází, dobou, kdy se v nich nachází, jeho vztahem k danému místu a legitimnímu očekávání vzhledem k těmto faktorům. Není proto divu, že kontrolní orgány se k tomuto zdroji poznání práva na respektování soukromého a rodinného života znovu vracejí.[448]

Přestože tedy čl. 8 Úmluvy svým věcným rozsahem právo na respektování soukromého a rodinného života významně přesahuje, tak obsahuje zcela zásadní postuláty aplikované v oblasti pracovního práva, čímž pomáhá podstatným způsobem zlepšovat jak pracovní podmínky, tak i humanizuje samotný výkon práce.[449] Jakkoliv lze oblast ochrany osobnostních práv považovat za relativně roztříštěnou a nesourodou, lze ji přesto z pohledu obecné ochrany zaměstnance jako slabšího subjektu pracovněprávního vztahu hodnotit pozitivně. Zaměstnanec je chráněn proti nerovnému zacházení, resp. většině druhů diskriminačního jednání, před zásahem do své tělesné i duševní integrity, svého soukromí, cti a lidské důstojnosti atd. apod. V případě zásahu do jeho osobnostních práv mu zákon poskytuje celou řadu efektivních prostředků ochrany, ať již jde o výzvu zaměstnavateli směřující k upuštění od porušování práv, případně k odstranění následků či zajištění nápravy až po řešení sporu v občanském soudním řízení. V každém případě i zde platí stará *maxima vigilantibus iura scripta sunt*,[450] a tak i zde platí více než kde jinde, že kdo nezná svá práva, nebude se jich nikdy dovolávat.

Klíčová slova

Bezpečnost osobních údajů, cache, cloud computing, Cross-Border Privacy Enforcement Arrangement, data retention, elektronická úřední deska, elektronické komunikace, Evropský systém ochrany osobních údajů, Fullerův koncept vnitřní morálky, Gartnerova křivka, generální klauzule, ideální statky, IMEI, IMSI, inspektor ochrany údajů, invazivnost sledovacích opatření, IP adresa, ISDS, logování (protokolové soubory), MAC adresa, Moreno vs. Hanford, občanská čest a lidská důstojnost, ochrana osobnosti fyzické osoby, osobní údaj, Payment Card Industry Data Security Standard, právo být zapomenut, projevy osobní povahy, prostředky ochrany, provozní a lokalizační údaje, přiměřené očekávání, rozumné očekávání, příposlech, registry, satisfakce, služby informační společnosti, technicko-organizační opatření, základní registry, zákonné licence, zákonná omezení práv osobnostních, zásady bezpečnosti, důvěrnosti, finality, informovaného souhlasu, zásada kvality údajů, zásada legitimity, zásada oznamovací, zásada zákazu zpracování některých kategorií údajů.

448 Stanoviska Úřadu č. 1/2003 a 3/2003 a v neposlední řadě č. 2/2009.
449 BĚLINA, M., L. DRÁPAL a kol., ref. 428.
450 Pouze bdělým náležejí práva.

5. Mezinárodní spolupráce jako conditio sine qua non efektivity práva

5. Mezinárodní spolupráce jako conditio sine qua non efektivity práva

5.1 Internet a existence právních problémů jeho globální povahy — 159
5.2 Ochrana osobních údajů a kolizní normy — 162
5.3 Ochrana osobních údajů v prostředí Internetu a základy určování soudní pravomoci — 169
5.4 Závěrem k problému (přeshraniční) působnosti práva — 174
Klíčová slova — 175

5. Mezinárodní spolupráce jako conditio sine qua non efektivity práva

„Chceš-li postavit loď, nesmíš poslat muže, aby sehnali dřevo a připravovali nástroje, ale nejprve musíš ve svých mužích vzbudit touhu po nekonečných dálkách otevřeného moře.“[451]

Antoine de Saint-Exupéry

5.1 Internet a existence právních problémů jeho globální povahy

Zásadním právním problémem Internetu není ani tak skutečnost, že umožňuje překonat velikou vzdálenost, to se ostatně povedlo před více než sto lety[452] už i telegrafu, ale především fakt, že Internet a jeho dosavadní služby fakticky vylučují fyzickou vazbu na většinu hmotných a relevantních faktorů mezilidské komunikace.[453] V tomto ohledu tak Internet představuje vysoce specifické prostředí, které nezná teritoriálních hranic, jež jsou obvyklým definičním kritériem pro uplatňování práva. Zvláštnost tohoto prostředí vyplývá především ze samotné historie vzniku a původního účelu tohoto fenoménu, jakož i technologických principů jeho fungování.

Již v okamžiku svého zrodu byl totiž Internet obdařen takovou vnitřní stavbou a koncepcí, že žádné státy či orgány nad ním nemohly získat úplnou kontrolu.[454] Důraz byl naopak kladen na nedůvěru k jakékoliv centralizované kontrole, což, jak bývá uváděno,[455] bylo způsobeno vlnou idealismu z 60. let minulého století a souvisejícími hodnotami americké libertariánské ideologie. Tento koncept formoval vznik Arpanetu, předchůdce Internetu,[456] jako decentralizované sítě, která se pak stala základem struktury dnešního Internetu. Tento koncept ve svém důsledku vedl k vytvoření sítě, která kromě toho, že není postavena na centrální kontrole, postrádá základní respekt k teritoriální působnosti práva, jež by umožňovala efektivní kontrolu na území jednotlivých států (byť lze konstatovat, že některé státy jako např. Čína a Irán se této efektivní kontrole poměrně silně přiblížily). V tomto smyslu se obvykle hovoří[457] o bezhraničnosti[458] Internetu jako o jednom z jeho klíčových znaků. Důvodem tohoto atypického vnitřního charakteru

451 Tato slova bývají připisována stejnému autorovi, byť nezřídka různým jeho publikacím, prokazatelně však jde o velmi volnou parafrázi básně Dessine-moi un bateau publikované v knize Antoine de Saint-Exupéryho, *Citadelle,* tedy knihy, kterou její autor nikdy nedokončil (byla vydána posmrtně v roce 1948), knihy, která je plná myšlenek, jež není lehké interpretovat.

452 Patrně i dříve, a to minimálně v rovině optického telegrafu. Jak známo, tak v roce 1184 př. n. l. bylo dobytí Tróje oznámeno do Mykén ohňovými signály řetězcem ohnišť.

453 Srov. ŠKOP, M. Hranice práva a kyberprostoru – Subverzivita kyberprostoru. *Právník.* 144, číslo 5, s. 1157.

454 Viz GOLDSMITH, J. a T. WU. *Who Controls the Internet? Illusions of a Borderless World.* Oxford University Press, 2006, s. 22.

455 BARAN, P. *On Distributed Communications: I. Introduction to Distributed Communications Networks* [online]. RAND CORP. 1964. Dostupné z: www.rand.org/pubs/research_memoranda/2006/RM3420.pdf

456 K otázce vzniku a počátků Internetu více viz obecně ABBATE, J. *Inventing The Internet.* MIT Press, 2000.

457 SVANTESSON, B. „Imagine There's No Countries…“: Geo-Identification, the Law, and the Not-So--Borderless Internet. 10 *J. Internet L. I.* I, 20. 2007.

458 K tomu viíce SVANTESSON B. How Does the Accuracy of Geo-Location Technologies Affect the Law. *Masaryk University Journal of Law and Technology.* 2008, č. 1.

Internetu byla především skutečnost, že byl budován primárně jako vojenská technologie, která musí odolat útoku nepřátel. Rozložená architektura sítě nebyla tedy věcí náhody, ani její zrod nediktovala technická nutnost, šlo naopak o důvody strategické a politické.

Internet původně nebyl tvořen pro masové použití, proto také u jeho zrodu nebyly řešeny právní souvislosti jeho masového či civilního rozšíření. Nebylo tak pamatováno na otázky efektivity práva v jeho prostoru, jakož i zcela zásadního dopadu na působnost a pravomoc státních orgánů, včetně možnosti ukládat nové povinnosti a vynucovat jejich dodržování.

Jak známo, jedním z pojmových znaků státu je veřejná moc, tedy svého druhu forma efektivní kontroly (suverénní moc) v rámci svého území.[459] Aby mohla vláda efektivně regulovat, musí mít možnost uplatnit svou veřejnou moc, případně nějakou formou pověřit jinou vládu, aby tuto moc vykonávala za ni. Ochota nebo naopak neochota cizích vlád propůjčit se k vynucování předpisů jiné vlády vymezuje meze regulační možnosti této vlády. Reálná možnost a způsobilost jedné vlády vynutit svou vůli na svém území (například proto, že jsou zde umístěny příslušné servery),[460] tak ve svém důsledku představuje formu celosvětové regulace, byť tento rozměr nelze přeceňovat, a to zejména s ohledem na nové technologie, pro které je umístění serveru podružné (cloud computing, mirroring, poskytování služeb geograficky diverzifikovaných do více lokalit atd.). Ostatní vlády nemohou takovou moc efektivně vyloučit[461] a regulační rámec (a vynucování) jedné země se tak automaticky rozšiřuje na celý světový internetový prostor.[462]

Poté, co se Internet stal celosvětově rozšířeným, nahradilo původní potřebu jeho neutrality a nezávislosti poznání, že nulová regulace kyberprostoru může nakonec přinést větší problémy, než evidentní společenská přínosnost. Je samozřejmě otázkou, zda se dá Internet vůbec reálně regulovat. Jednou z prvních osobností, která na nevýhody chybějící regulace Internetu veřejně upozornila, byl L. Lessig,[463] který uvedl, že Internet je nutné nějak řídit, nicméně taková regulace by měla vycházet především z tzv. „kódu", tj. vnitřní stavby Internetu jako technologického konceptu, který již svým způsobem chování na Internetu reguluje (k tomu viz více v předchozích částech této práce).[464] Touto vnitřní stavbou by se do velké míry řídila i působnost práva, takže by se stala nejen „kódem" v technickém slova smyslu, ale do určité míry rovněž

459 Mezi první autory tohoto konceptu patří Georg Jellinek, více viz JELLINEK, G. *Algemeine Staatslehre.* 1900. Citace dle českého překladu JELLINEK, G. Všeobecná státověda. Praha, 1906, s. 410.

460 Fyzická přítomnost provozovatele webových stránek nebo jeho majetku nemusí být ve státě, kde se právo vymáhá, místem vymáhání, ale může být země, kde jsou umístěny servery. GOLDSMITH, J. Against Cyberanarchy. 65 U. *Chicago Law Review.* 1199, 1217. 1998.

461 Vlády se mohou snažit vybudovat na Internetu virtuální zdi, které omezí přístup k určitému obsahu mimo jejich území; filtrování obsahu je však spojené s celou řadou problémů a v zásadě neexistuje dokonalé řešení. K tomu více viz SVANTESSON, B., ref. 457.

462 CHANDER, A. Trade 2.0. 34 *YALE J. INT'l L.* 281, 285 (2009) („Ponecháme-li síť zcela volnou, bez jakéhokoli dohledu, může tím dojít k ohrožení tuzemského práva. Místní právo může být nahrazeno úpravou domovského státu poskytovatele služeb v dané síti… Předpokladem dovozu služeb by neměl být dovoz cizího práva.").

463 LESSIG, L. *Code and Other Laws of Cyberspace.* Basic Books, 1999, ISBN 0-465-03913-8. [online] Dostupné z: code-is-law.org/

464 GEIST, M. Cyberlaw 2.0. 44 *B.C. L. Rev.* 323, 357 (2003) („Třemi zásadami kyberpráva 1.0 … se ve skutečnosti prolíná jedna nejdůležitější zásada, že vláda by na Internet neuplatnila, nemohla ani neměla uplatňovat tradiční regulatorní mechanismus.").

„kodexem" ve smyslu právním. Pokud by vlády chtěly Internet regulovat, musely by využít jeho vnitřní stavbu, tedy „kód" v technickém smyslu slova, zároveň by však tato architektura chránila Internet před právními zásahy ze strany státu, které by neodpovídaly struktuře sítě.[465] Řešení problému úpravy (regulace) Internetu by tedy muselo vycházet z jeho vnitřní stavby.[466] Patrně lze přistoupit na tezi, že chování v prostředí sítě Internet by mělo být regulováno. Otázkou však je, kdo by jej měl regulovat a jakou formou či způsobem. Lessigova teorie je v tomto ohledu velmi zajímavá, nicméně klade požadavky zejména na související autority (svou povahou spíše soukromoprávní), jako např. správce doménových jmen, poskytovatele služeb, výrobce hardwaru, tvůrce softwaru atd. (k tomu viz níže).

Zajímavá analýza tohoto problému byla realizována ve známém textu[467] autorů D. Satoly a H. Judy, kteří uvádějí, že od počátku vědomí o existenci tohoto problému se objevila řada myšlenkovým směrů, kde jeden prohlašoval, že Internet by neměl být kýmkoliv regulován, přičemž se objevilo několik významných deklarací (viz níže) tohoto směru, včetně příslušných argumentů. Je však třeba uvést, že ani tyto úvahy nevylučovaly regulaci Internetu absolutně.[468] Nejznámější hnutí, na jehož počátku stála zásadní deklarace tohoto typu, byla organizace Electronic Frontier Foundation, jejímž zakladatelem je americký básník, textař a esejista John Perry Barlow. Tato organizace se již od počátku svého vzniku významně angažovala v celé řadě protestů a osvěty proti omezování svobody jedince na Internetu. Jejím základním dokumentem je takzvaná Deklarace nezávislosti kyberprostoru,[469] jejímž ústředním motivem je problém právní regulace a činnost států a jejich orgánů. Deklarace mimo jiné říká *„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. Nemáme vládu ani po žádné netoužíme. Mluvím k Vám tedy z pozice autority ne větší, než jakou má sama Svoboda. Vyhlašuji, 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 dík našemu společnému úsilí. Dovoláváte se problémů okolo nás a říkáte, 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 vypořádáme se s nimi vlastními prostředky. Máme novou společenskou smlouvu. Takové vládnutí se nezakládá na podmínkách Vašeho světa, ale toho našeho a náš svět*

465 Nejde ani tak o požadavek na absenci celkové regulace kyberprostoru ze strany států, ale především o to, aby státy Kyberprostor regulovat ani nemohly. K tomu více viz LESSIG, L. Code 2.0. Basic Books, 2006, ISBN 10:0-465-03914-6, ISBN 13: 978-0-465-03914-2. [online] Dostupné z: http://codev2.cc/

466 TRIMBLE, M. The Future of Cybertravel: Legal Implications of the Evasion of Geolocation (April 12, 2012). *Fordham Intellectual Property, Media & Entertainment Law Journal.* 2012, Vol. 22, s. 579

467 SATOLA, D. a H. JUDY, ref. 152.

468 K tomu srovnej MALÍŘ, J. Mezinárodní právo a jak je (ne)používáme. *Právník*. 2011, roč. 150, č. 5, s. 417.

469 V původní podobě je tato deklarace dostupná [online] z: http://stalkr.k47.cz/clanek/255

je jiný. Pojmy Vašeho práva, jako vlastnictví, vyjadřování, subjektivita, pohyb nebo okolnosti, se na nás nevztahují… "[470]

Řešení otázky regulace kyberprostoru se tak postupně dostala do dvou extrémních poloh. Jedna skupina horující pro výjimečnou povahu Internetu vyzývá ke zřízení nových orgánů, které by měly řídit kyberprostor.[471] Druhá skupina, která nepovažuje Internet za nic výjimečného, pouze za svého druhu jinou komunikační infrastrukturu a platformu, považovala za zbytečné diskutovat o tom, kdo má regulovat Internet, protože právo již na něj dopadá. Postupem času se však natolik rozšířilo spektrum činností, které se na Internetu uskutečňují, že právo začalo tyto činnosti automaticky regulovat a vymáhat alespoň tam, kde to bylo možné. Státy se tak začaly podílet na de facto globálním vynucování práva na Internetu. Absence hranic vyplývající z povahy Internetu se najednou v mnoha aspektech nezdála tak výhodná a potřebnost efektivity práva se začala znovu výrazně legislativně prosazovat. Tento vývoj lze vnímat jako logický důsledek toho, že Internet přestal být vnímán jako něco zcela nedotknutelného, výjimečného a především fakticky nekontrolovatelného. Zájem států na zakotvení efektivity práva v prostředí Internetu se tak stal nejenom pochopitelný, ale zejména legitimní. Vytváření právních hranic tak zcela jistě začíná, byť pomalu, ale začíná. Otázka, jaké tyto hranice budou, tak zůstává stále otevřena.

5.2 Ochrana osobních údajů a kolizní normy

Důsledkem globální povahy Internetu je tedy skutečnost, že vzhledem k rozdílným teritoriálním umístěním subjektů jako účastníků nepřeberné řady právních vztahů v tomto prostředí, jakož i jejich prostředků (serverů, datových úložišť apod.), které tyto subjekty používají za účelem realizace těchto vztahů, dochází k tomu, že je v řadě případů zcela nezbytné použití zahraničního práva, což je oblast, která patří ke klasickým tématům mezinárodního práva soukromého. Soudy tak nezřídka musejí aplikovat cizí právo, a to obvykle tehdy, když je dán tzv. vztah s mezinárodním prvkem, což je případ, kdy má např. jeden ze subjektů sídlo nebo bydliště v zahraničí, případně má jinou než českou státní příslušnost, nebo se v zahraničí nachází místo plnění smlouvy (umístění serverů), v zahraničí došlo ke vzniku škody atd. apod.[472]

Z hlediska rozhodujícího subjektu – ať již jde o soudce, nebo o rozhodce – je po vyřešení pravomoci a příslušnosti další otázkou nikoli vlastní hmotněprávní úprava, ale otázka, které právo, právo kterého státu, se použije. Do hry tak vstupují kolizní normy, které teprve určí

470 Citace českého překladu z pera POLČÁKA, R. Autoritativní regulace kyberprostoru a legitimita trestního práva. In: T. GŘIVNA a R. POLČÁK, eds. *Kyberkriminalita* a právo. Praha: Auditorium, 2008, s. 19. Původní text je dostupný z: www.eff.org

471 JOHNSON, T. a D. POST. Law and Borders-The Rise of Law in Cyberspace, 48 *STAN. L. REV.* 1367, 1367 (1996).

472 Vztah k zahraničí – „mezinárodní prvek" určitého soukromoprávního poměru – musí být dostatečně relevantní, tedy nikoli zanedbatelný. A je třeba přiznat, že existují i hraniční případy, které vyžadují specifické posouzení. Pokud je v soukromoprávním vztahu obsažen mezinárodní prvek, mění se i mechanismus aplikace právních předpisů.

rozhodné hmotné právo. Spíše výjimečně se přímo použijí tzv. přímé normy, obsahující hmotněprávní úpravu, které jsou většinou obsaženy v mezinárodních smlouvách. Kolizní normy jsou způsobilé překlenovat rozdíly mezi právními řády různých států, aniž zasahují do vlastních hmotněprávních řešení, takže státy unifikované kolizní normy snáze akceptují než unifikované normy hmotného práva. Kolizní normy nacházíme ve vnitrostátním právu jednotlivých států, v České republice především v zákoně o mezinárodním právu soukromém a procesním č. 97/1963 Sb., v platném znění, který bude s účinností od 1. 1. 2014 nahrazen zákonem č. 91/2012 Sb., i v četných mezinárodních smlouvách.

Obrovský úspěch unifikace kolizního práva dokumentují některá nařízení přijatá v rámci EU, zejména nařízení Řím I,[473] o právu rozhodném pro smluvní závazkové vztahy, které navázalo na Římskou úmluvu o právu rozhodném pro smluvní závazkové vztahy, a nařízení Řím II,[474] o právu rozhodném pro mimosmluvní závazkové vztahy. Tyto instrumenty obsahují kolizní normy, které jsou univerzálně použitelné, což znamená, že se použije kteréhokoli právního řádu, na který takové kolizní normy odkážou, bez ohledu na to, zda se jedná o právo členského státu EU, či nikoli. Kolizní normy mohou určit jako rozhodný právní řád i zahraniční právo. Pokud kolizní norma odkáže na zahraniční právo, vznikají otázky, zda je soudce či rozhodce povinen toto právo aplikovat, zda je povinen sám zjistit jeho obsah, jak ho bude aplikovat, kdo bude hradit náklady spojené se zjištěním cizího práva, jak se lze bránit proti nesprávné aplikaci cizího práva, jak postupovat, když se cizí právo nepodaří zjistit atd. Na zodpovězení těchto otázek závisí vlastní efektivita kolizních norem: tedy zda se lze spolehnout na to, že kolizní norma, která určuje jako rozhodné právo zahraniční právní řád, bude naplněna a soudce nebo rozhodce bude skutečně cizí právo aplikovat. Odpověď na otázky spojené s používáním zahraničního práva není vždy jednoznačná, a výsledek sporu, v němž přichází v úvahu použití cizího práva, tak často bývá obtížně předvídatelný.[475] Nejinak tomu bude i v případě kolizních norem týkajících se ochrany osobních údajů.

Výše zmíněná Pracovní skupina 29 potvrdila, že pravomoc (působnost) dle práva na ochranu osobních údajů by měla být posuzována mimo jiné také dle mezinárodního práva veřejného.[476] Závaznost norem mezinárodního práva je významná zejména s ohledem na globální povahu Internetu, jakož i skutečnost, že státy jsou schopny harmonizovat kolizní i procesní normy, nicméně obvykle nikoliv hmotné právo.

Z pohledu evropského standardu ochrany práv osobních údajů lze za zásadní dokument považovat nařízení Evropského parlamentu a Rady č. 593/2008 ze dne 17. června 2008, o právu rozhodném pro smluvní závazkové vztahy (Řím I), které se vztahuje na smluvní zá-

473 Nařízení Evropského parlamentu a Rady č. 593/2008 ze dne 17. června 2008, o právu rozhodném pro smluvní závazkové vztahy (Řím I).

474 Nařízení Evropského parlamentu a Rady (ES) č. 864/2007 ze dne 11. července 2007, o právu rozhodném pro mimosmluvní závazkové vztahy (Řím II).

475 PAUKNEROVÁ, M., Aktuální otázky používání zahraničního práva v soudním a v rozhodčím řízení. *Právník*. 2009, ročník CLI, č. 12, s. 1265.

476 Viz stanovisko Pracovní skupiny 29, WP 56 (s. 13) 2, která uvádí, že „*otázka, zda se vnitrostátní právo (na ochranu osobních údajů) použije na situace s vazbami na několik států je rovněž obecnou otázkou mezinárodního práva*".

vazkové vztahy podle občanského a obchodního práva v případě kolize právních řádů, čímž přijímá vymezení své věcné působnosti z původního nařízení Brusel I,[477] pokud se týká pojmu občanské a obchodní věci a současně doplňuje vymezení věcné působnosti nařízení Řím II,[478] které upravuje mimosmluvní závazkové vztahy občanského a obchodního práva v případě kolize právních řádů. Nařízení Řím I a Řím II tak dopadá na všechny závazkové právní vztahy občanského a obchodního práva, které nejsou z jejich věcné působnosti výslovně vyloučeny. Otázkou samozřejmě zůstává, jaký bude aplikační rozsah občanských a obchodních věcí u jednotlivých států, a to zejména vzhledem k analogického výkladu pojmů obsažených a shodných s pojmy v nařízení Brusel I, které bylo přijato prakticky o osm let dříve.[479] Použití judikatury k nařízení Brusel I pro interpretaci pojmů v nařízení Řím I, především pojmu věci obchodní a občanské a pojmu „smlouva", předpokládala již Zelená kniha,[480] kterou byl zahájen proces transformace Římské úmluvy do Nařízení a současně preambule obou zmíněných nařízení.[481]

Z pohledu ochrany osobních údajů v prostředí služeb Internetu se jeví jako významná úprava článku 6 nařízení Řím I, které definuje spotřebitelské smlouvy. Podle tohoto ustanovení jde o smlouvy uzavřené fyzickou osobou za účelem, který se netýká její profesionální nebo podnikatelské činnosti (dále jen „spotřebitel"), s jinou osobou, která jedná v rámci výkonu své profesionální nebo podnikatelské činnosti (dále jen „obchodník"), se řídí právem země, v níž má spotřebitel obvyklé bydliště, pokud: a) obchodník provozuje svou profesionální nebo podnikatelskou činnost v zemi, kde má spotřebitel své obvyklé bydliště, nebo b) se jakýmkoli způsobem taková činnost na tuto zemi nebo na několik zemí včetně této země zaměřuje a smlouva spadá do rozsahu této činnosti.

Strany si rovněž mohou zvolit právo rozhodné pro smlouvu, která splňuje podmínky tohoto článku (čl. 6 odst. 1). V důsledku této volby však nesmí být spotřebitel zbaven ochrany, kterou mu poskytují ustanovení právního řádu, od nichž se nelze smluvně odchýlit, a jež by se v případě neexistence volby práva na základě odstavce 1 jinak použila.[482] Podle tohoto nařízení se tak tyto spotřebitelské smlouvy řídí právem státu obvyklého bydliště spotřebitele, je-li splněna alespoň jedna ze dvou podmínek, tj. (1) obchodník provozuje své profesionální nebo podnikatelské činnosti ve státě, kde má spotřebitel své obvyklé bydliště, nebo (2) Pokud se jakýmkoli způsobem taková činnost obchodníka na zemi obvyklého bydliště spotřebitele

477 Nařízení Rady (ES) č. 44/2001 ze dne 22. prosince 2000, o příslušnosti a uznávání a výkonu soudních rozhodnutí v občanských a obchodních věcech (Brusel I).

478 Nařízení Evropského parlamentu a Rady (ES) č. 864/2007 ze dne 31. července 2007, o právu rozhodném pro mimosmluvní závazkové vztahy (Řím II).

479 BĚLOHLÁVEK, A. J. *Římská úmluva a Nařízení Řím: Ikomentář v širších souvislostech evropského a mezinárodního práva soukromého,* I. díl. 1. vyd. Praha: C. H. Beck, 2009. s. 10.

480 COM (2002) 654 final Green Paper on the conversion of the Rome Convention of 1980 on the law applicable to contractual obligations into a Community instrument and its modernization.

481 Z nejvýznamnějších judikátů lze v tomto ohledu uvést rozhodnutí ESD ve věci Lufttransportunternehmen GmbH & Co. KG vs. Eurocontrol. Rozsudek ESD ze dne 14. 10. 1976, C-29/76, věc LTU Lufttransportunternehmen GmbH & Co. KG vs. Eurocontrol.

482 KUČERA, Z. *Mezinárodní právo soukromé a procesní.* Brno: Aleš Čeněk, 2009. s. 322.

nebo na několik zemí včetně této zaměřuje.[483] Právě toto ustanovení má být řešením pro problematickou úpravu smluv uzavíraných přes Internet, včetně otázek ochrany dat, sociálních sítí apod. Existence datového obsahu na Internetu, resp. jeho umístění na konkrétním serveru v konkrétní zemi, však není a ani nemůže být rozhodujícím prvkem. V tomto ohledu je nezbytné analyzovat samotnou povahu tohoto obsahu, možnost uzavřít smlouvu, případně další otázky. Pokud není splněna ani jedna z předcházejících podmínek pro použití práva státu obvyklého bydliště spotřebitele, určí se rozhodné právo pro smlouvy mezi spotřebitelem a obchodníkem podle čl. 3 a 4 nařízení, tzn. jako pro smlouvy obecně (tj. volba práva a kolizní kritéria).

Jak uvádí Kuner,[484] působnost (pravomoc) těchto norem mezinárodního práva se do značné míry překrývá, přičemž ji v obecné rovině můžeme členit na tři kategorie, a to legislativně-nařizovací, posuzovací a výkonnou. *Legislativně-nařizovací pravomoc* (Legislative or prescriptive jurisdiction) je pravomoc státu uplatňovat své právní normy na případy zahrnující cizí (mezinárodní) prvek.[485] Legislativní pravomoc bývá spíše souběžná než výlučná. Příkladem legislativní pravomoci v kontextu práva na ochranu osobních údajů by mohlo být například uplatnění práva EU na ochranu osobních údajů na webové stránky zřízené mimo EU, které využívají cookies ke zpracování osobních údajů jednotlivců se sídlem (bydlištěm) v EU. *Posuzovací pravomoc* (Adjudicative jurisdiction) je pravomoc soudů určitého státu soudit případy zahrnující cizí (mezinárodní) prvek. Příkladem uplatnění této pravomoci může být například úřad pro ochranu osobních údajů zřízený v rámci EU, který rozhoduje o stížnosti předložené soukromou osobou s bydlištěm v EU na základě zpracování jeho osobních údajů subjektem usazeným mimo EU. Tam, kde se právo na ochranu osobních údajů považuje za „právo veřejné", znamená zákonná pravomoc totéž co pravomoc legislativní. V právu na ochranu osobních údajů vlastně vede ke stejnému výsledku celá řada důležitých otázek týkajících se pravomoci a působnosti (jako je například dosah článku 4 odst. 1 písm. c) Směrnice. Výkonná pravomoc (Enforcement jurisdiction) je pravomoc jednoho státu vykonávat právní úkony na území státu jiného.[486] Zde by se mohlo jednat o případ, kdy se úřad pro ochranu osobních údajů zřízený v rámci EU bude snažit provést kontrolu subjektu usazeného mimo EU. Zákonnost výkonné pravomoci je úzce spjata se zákonností pravomoci legislativní a soudní a omezení u jednoho druhu pravomoci se mohou dotýkat rozsahu ostatních pravomocí.

Otázka, zda existují meze působnosti (jurisdikce) v rámci mezinárodního práva, a to zejména pokud jde o jednání v prostředí Internetu, je sporná. Lze vycházet z případu Lotus,[487] kde Mezinárodní soudní dvůr (MSD) rozhodoval, zda je dána trestní jurisdikce tureckých sou-

483 RAGNO, F. The Law applicable to a Consumer Contract under the Rome I Regulation. In: FERRARI, F. a S. LEIBLE, eds. *Rome I Regulation. The Law Applicable to Contractual Obligations in Europe.* Munich: Sellier – European Law Publisher, 2009. s. 155.

484 KUNER, Ch. Data Protection Law and International Jurisdiction on the Internet (Part 1) [online]. 18(3) *International Journal of Law and Information Technology.* 2010. Dostupné z: http://ssrn.com/abstract=1496847

485 AKEHURST, M. ‚Jurisdiction in International Law' (1972-73). 46 *British Yearbook of International Law* 145.

486 AKEHURST, M., ref. 485.

487 PCIJ, SS Lotus (*Francie proti Turecku*), Zprávy PCIJ, série A, č. 10, s. 19.

dů nad důstojníkem francouzské lodi, která se na volném moři srazila s tureckou lodí. V tomto případě soud prohlásil: *„Tímto se v žádném případě nekonstatuje obecný zákaz v tom smyslu, že by státy nesměly rozšiřovat působnost svých normativních aktů a soudů na osoby, majetek a jednání mimo svá území, v tomto smyslu je jim ponechána široká diskreční pravomoc, která je omezena pouze v některých případech zakazujícími právními normami. Pokud jde o ostatní případy, má každý stát právo přijmout zásady, které sám považuje za nejlepší a nevhodnější.“* Tento rozsudek byl v mnoha ohledech kritizován,[488] ale i nadále má velký význam jako patrně nejznámější případ řešící působnost (jurisdikci) v mezinárodním právu. Jádro tohoto rozhodnutí patrně spočívá v konstatování, že stát nemůže vymáhat své právo za svými hranicemi přímo, ale uplatňování práva určitého státu na jednání, k němuž došlo za jeho hranicemi, se považuje do značné míry za přípustné, pokud k tomu existují uznané právní důvody. Od případu Lotus se omezení výkonné pravomoci stalo všeobecně přijímaným faktem.[489] Většina veřejnoprávních orgánů rovněž zjistila, že existují[490] i jistá omezení mezinárodní legislativní pravomoci. Taková omezení jsou patrně nezbytná v případě základních principů, jako je suverenita státu a zásada nevměšování se.[491] Nicméně míra konsenzu, v čem tato omezení spočívají, je velice nízká, a to zejména vzhledem k tomu, že státy, využívajíce celé řady právních důvodů, jsou při hledání ospravedlnění pro uplatnění své legislativní pravomoci velice kreativní.[492]

V rámci mezinárodního práva veřejného neexistuje žádný nástroj pro celosvětovou aplikaci práva, který by obsahoval pravidla jurisdikce v rámci práva na ochranu osobních údajů.[493] Důvody této situace jsou vysvětleny v důvodové zprávě ke směrnicím OECD o ochraně soukromí z roku 1981, kde se mimo jiné praví, že: *„Expertní skupina věnovala nemalou pozornost problematice kolizních norem, a to zejména otázkám volby sudiště a volby práva. Diskuze o různých strategiích a navrhovaných zásadách potvrdila názor, že v této fázi – s nástupem tak rychlých technologických změn a vzhledem k nezávazné povaze těchto směrnic není vhodné prosazovat konkrétní podrobná řešení.“*[494] V roce 1999 Haagská konference soukromého mezinárodního práva posuzovala otázku soudní pravomoci a rozhodného práva v oblasti ochrany osobních údajů v rámci svého

488 Např. RYNGAERT, C. *Jurisdiction in International Law.* Oxford University Press, 2008, s. 26, který v tomto ohledu uvádí, že rozhodnutí v případu Lotus bývá co do doktríny vehementně kritizováno. Dnes se již považuje za přežité a dokonce se má za to, že nikdy nebylo rozhodnutím precedentním.

489 Viz BROWNLIE. I. *Principles of Public International Law.* 7th ed. Oxford University Press, 2008, s. 37, který uvádí, že hlavní zásada je, že stát nemůže přijímat opatření formou výkonu svého vnitrostátního práva na území jiného státu bez jeho souhlasu.

490 Viz např. případ týkající se společnosti *Barcelona Traction, Light and Power Co Ltd (Belgie) proti Španělsku,* 1970.

491 Z odkazu na nadřazenost mezinárodního práva vyplývá to, co lze nazývat povinností nevměšování se do záležitostí cizích států. Konkrétně tato důležitá podmínka stanoví, že právní akty, které by měly za následek regulaci jednání cizinců v cizích zemích, by byly nezákonné.

492 KUNER, Ch., ref. 484.

493 Ustanovení Směrnice představují první a jediný soubor norem obsažených v mezinárodním právním dokumentu o ochraně osobních údajů, který řeší konkrétně určování rozhodného práva.

494 Organizace pro hospodářskou spolupráci a rozvoj (OECD), Pravidla ochrany soukromí a přeshraničních toků osobních údajů (1981) 35.

„Ženevského kulatého stolu o elektronických obchodech a mezinárodním právu soukromém". Tyto diskuse však vedly pouze k vyjádření stanoviska, že dané téma je třeba dále prostudovat.[495]

V roce 2009 začala skupina složená ze zástupců úřadů pro ochranu osobních údajů z celého světa, které předsedal španělský úřad pro ochranu osobních údajů, koncipovat návrh celosvětového právního nástroje o ochraně osobních údajů s odhodláním předložit jej OSN (Organizaci spojených národů). Rané návrhy obsahovaly i ustanovení, které se nakonec objevilo ve finální verzi, konkrétně pak v článku 25, upravujícím rozhodné právo a soudní pravomoc, který stanoví, že zpracování osobních údajů se bude řídit rozhodným právem a bude o něm rozhodovat soud státu, na jehož území je usazena osoba, v rámci jejíž činnosti se zpracování uskutečnilo, tj. (1) v případech, kde tato osoba není ve státě usazena, ale svou činnost odesílá výhradně na území daného státu, bude zpracování osobních údajů prováděné v rámci této činnosti spadat pod pravomoc soudů právě tohoto státu a řídit se jeho právem, případně (2) pro účely tohoto odstavce se pod pojmem usazení rozumí jakékoli stálé zařízení, které umožňuje skutečné a efektivní provádění dané činnosti, a to bez ohledu na jeho právní formu.

Úprava teritoriální působnosti je rovněž zapracována do ustanovení § 3 odst. 5 ZoOÚ, a to na základě požadavku článku 4 Směrnice, který požaduje zajištění aplikace pravidel přijatých členskými státy EU pro oblast ochrany dat i na zpracování s mezinárodními prvky. Tato úprava vychází z požadavku na zajištění stejné míry ochrany všem údajům zpracovávaným na území EU anebo dat odsud pocházejících bez ohledu na faktickou lokalizaci správce,[496] jejím účelem je tedy zajištění odpovídající ochrany osobních údajů a umožnění řádného výkonu práv subjektů údajů i vůči správcům dat sídlícím mimo území EU.[497]

V opačném případě – při absenci obdobných institutů – by mohlo v důsledku působení správců osobních dat ze třetích zemí nebo přesidlování správců do lokalit s žádnou nebo jen fragmentární úpravou ochrany osobních údajů docházet k citelnému snížení úrovně této ochrany v rámci evropského prostoru, kde je úprava této oblasti plně rozvinutá a patří k nejpřísnějším (včetně ochrany poskytované právům subjektu údajů). Současně se jedná o vyjádření jednoho ze základních principů evropské spolupráce, a to volného pohybu osobních údajů v rámci EU. Správce osobních údajů usazený v členském státě EU tak může provádět zpracování i v jiné členské zemi, aniž by byl jakkoliv administrativně omezován nebo měl povinnost zajistit zpracování v této zemi prostřednictvím zde usazeného zpracovatele. Reálné možnosti příslušných národních autorit (a zřejmě kteréhokoli obdobného orgánu v rámci EU) skutečně vykonávat dozor nad dodržováním pravidel stanovených zákonem o ochraně osobních údajů ve vztahu k subjektům sídlícím mimo území EU jsou značně omezené. Vyšší míra vymahatelnosti práva na ochranu osobních údajů ve vztahu k členským státům EU je dána také tím, že v rámci evropského právního prostoru působí jako sjednocující prvek při aplikaci principů pro ochranu osobních údajů Evropský inspektor ochrany údajů (zřízený na základě nařízení Evropského parlamentu a Rady č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvis-

495 Viz Tisková zpráva, Geneva Round Table on Electronic Commerce and Private International Law. Dostupné z: cuiwww.unige.ch/~billard/ipilec/pressre.html

496 Viz recitál 20 Směrnice.

497 K tomu viz MALÍŘ, J., ref. 468, s. 419.

losti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů). Evropský inspektor vede aktivní komunikaci směrem k jednotlivým evropským institucím, které se na prosazování principů ochrany osobních údajů podílejí, a přispívá tak k jisté vyváženosti názorů a k lepší vymahatelnosti práv subjektů údajů. S možností praktického vymáhání ZoOÚ v případech s mezinárodním prvkem je spojena i otázka možné efektivní spolupráce s příslušným dozorovým orgánem pro ochranu osobních údajů v dané třetí zemi. V případě, kdy správce osobních údajů sídlí v zemi, která ratifikovala Úmluvu č. 108 (jedná se o 43 ze 47 členských států Rady Evropy), je na místě uplatnit ustanovení článku 13 Úmluvy č. 108, který obsahuje závazek smluvních stran zřídit dozorový orgán a jeho prostřednictvím spolupracovat s ostatními signatáři na zajištění požadované úrovně ochrany osobních údajů. Citovaná Úmluva č. 108 obsahuje také (v článku 14) povinnost smluvních stran poskytnout pomoc kterékoli osobě, která má bydliště v zahraničí (tedy i na území států, které k Úmluvě č. 108 nepřistoupily). Tato povinnost poskytnout pomoc se týká zejména těch případů, kdy se tato (zahraniční) osoba obrátí na určitý dozorový orgán přímo nebo prostřednictvím svého „domácího" dozorového orgánu. V zemích, které nejsou členy Rady Evropy, resp. nejsou signatáři Úmluvy č. 108, je však možnost spolupráce a tedy i případného vymáhání pravidel pro ochranu osobních údajů výrazně snížena.[498] Závěrem této obecné části je vhodné zmínit chystanou novou právní úpravu ochrany osobních údajů na komunitární úrovni, která bude mít formu obecného nařízení pro ochranu dat (General Data Protection Regulation). V oblasti teritoriální působnosti dojde s přijetím tohoto nařízení ke změně spočívající v tom, že se bude aplikovat na činnost správců či zpracovatelů sídlících v některé členské zemi EU a dále na zpracování osobních údajů realizované správci sídlícími mimo území EU, pokud se bude jednat o osobní údaje subjektů údajů, kteří žijí ve společném evropském prostoru, a pokud bude současně účelem zpracování nabízení zboží či služeb anebo sledování chování osob. Na správce sídlící mimo členské státy EU se bude obecné nařízení dále vztahovat za předpokladu, že sídlí v zemi, kde se na základě mezinárodního práva veřejného uplatní národní právní úprava některého členského státu.[499] S aplikací zahraničního práva je spojena celá řada principů procesního povahy, jedním z nejdůležitějších je pak ten, že se zahraniční právo používá podobně jako právo národní, a nikoli jako skutečnost, kterou by bylo potřeba dokazovat.[500] V řadě dalších států tomu tak však není, existují základní rozdíly mezi evropským kontinentálním (románsko-germánským) přístupem k cizímu právu a přístupem států common law.[501] V rámci těchto velkých skupin se vyskytuje řada rozdílů v postoji jednotlivých právních řádů, které mohou základní akademické členění – tedy členění, zda se s cizím právem zachází jako s právem, či jako se skutečností, a zda

498 Výkladu článku 4 Směrnice se věnuje také Pracovní skupina 29, viz stanovisko č. 8/2010 k použitelnému právu.

499 KUČEROVÁ, A., L. NOVÁKOVÁ, V. FOLDOVÁ, F. NONNEMANN, a D. POSPÍŠIL. *Zákon o ochraně osobních údajů: Komentář.* 1. vydání. Praha: C. H. Beck, 2012, s. 12.

500 Zásada iura novit curia se v tomto případě neaplikuje bezpodmínečně. I když se s cizím právem stále zachází jako s právem, soud je pouze povinen toto právo ex officio zjistit, nikoli již předem znát.

501 PAUKNEROVÁ, M., Aktuální otázky používání zahraničního práva v soudním a v rozhodčím řízení. *Právník.* 2009, ročník CLI, č. 12, s. 1265.

soudy aplikují cizí právo *ex officio,* nebo zda musí být cizí právo navrhováno a prokazováno stranami, dost podstatně relativizovat.[502] Jak výstižně uvádí Pauknerová,[503] ačkoliv k tomuto tématu existuje bohatá literatura, právní teorie a právní praxe nemusejí být a často ani nemohou být identické, přičemž za tímto účelem uvádí případ v USA známý jako *„Oklahoma against Foreign and International Law"* („Oklahoma proti zahraničnímu a mezinárodnímu právu",[504] kdy voliči státu Oklahoma poměrem 70 % schválili Dodatek ke státní ústavě, tzv. *„Sharia Amendment"* („Dodatek šaría"), jehož smyslem a účelem byl zákaz použití zahraničního práva. Tzv. *„Save Our State Amendment"* („Dodatek k záchraně našeho státu") stanoví, že soudy státu Oklahoma: (1) nebudou přihlížet k právním pravidlům jiných národů nebo kultur; (2) nebudou brát v úvahu mezinárodní právo nebo právo šaría; a (3) budou používat právo jiného státu USA pouze tehdy, pokud je to „nezbytné", a za předpokladu, že takové právo neobsahuje právo šaría. Dodatek Oklahoma byl napaden u Federálního apelačního soudu. Dne 12. ledna 2012 Federální soud tento Dodatek zrušil s tím, že Dodatek porušuje Ústavu USA.

5.3 Ochrana osobních údajů v prostředí Internetu a základy určování soudní pravomoci

Jakkoliv může být právo na ochranu osobních údajů realizováno v prostředí Internetu, je vždy do jisté míry postaveno na principu teritoriality. Jak uvádí Kuner,[505] podle principu teritoriality se soudní pravomoc určuje podle jednání, k němuž došlo na území dotčeného státu, určitou variantou tohoto principu je však zásada objektivní teritoriality, což je případ, kdy jednání bylo započato v zahraničí, ale dokončeno na území daného státu, případně tam, kde se základní prvek takového jednání uskutečnil na území jiného státu. Jde tak o princip, z něhož především vycházel MSD v případu Lotus (viz výše). Prostředí Internetu však uplatňování tohoto principu komplikuje, jelikož jednání uskutečněné on-line je prakticky nemožné lokalizovat jako úkon uskutečněný v nějakém konkrétním státě.

Princip teritoriality v oblasti ochrany osobních údajů však zůstává významný i nadále, např. článek 4 odst. 1 písm. c) Směrnice lze považovat za svého druhu vyjádření principu objektivní teritoriality, jelikož přinejmenším částečně vychází ze spáchání určitého činu (s využitím vybavení nacházejícího se na území EU). Dalším významným principem je zde zásada personality, podle které uplatňuje svou pravomoc ten stát, jehož občanem je pachatel (princip aktivní personality)[506] nebo oběť (princip pasivní personality). Zatímco se princip personality využívá

502 K tomu více viz ROZEHNALOVÁ, N., V. TÝČ, a R. ZÁLESKÝ. *Vybrané problémy mezinárodního práva soukromého v praxi.* 2. vydání. Brno: Masarykova Universita, 1997, s. 12.

503 PAUKNEROVÁ, M.,ref. 501, s. 1267.

504 SYMEONIDES, S. Choice of Law in the American Courts [online]. In 2010: Twenty-Fourth Annual Survey. *American Journal of Comparative Law.* 2011, vol. 58 [vid. 30. srpna 2012]. Dostupné také z: ssrn.com/ abstract=1737558

505 KUNER, Ch., ref. 484

506 RYNGAERT, C. *Jurisdiction in International Law.* Oxford University Press, 2008, s. 96.

především v trestním právu, existují i příklady, kdy byl uplatněn v právu civilním. Princip pasivní personality bývá kritizován, ale princip personality jako takový se stále využívá jako základní doktrína pro určování soudní pravomoci v celé řadě oblastí, jako je daňové právo, hlasovací práva a diplomatická ochrana. Příklad principu personality v právu na ochranu osobních údajů najdeme v řeckém právu, které rozšířilo soudní pravomoc řeckého úřadu pro ochranu osobních údajů i na správce dat působící mimo Řecko, kteří zpracovávají údaje o řeckých obyvatelích. Dle řeckého práva mají totiž správci dat povinnost jmenovat zástupce v Řecku, který bude za zpracování dat odpovědný.[507] Patrně nejkontroverznější zásada určování soudní pravomoci je „doktrína účinku", podle které se soudní pravomoc určuje na základě toho, že jednání uskutečněné mimo daný stát má v tomto státě účinky.[508] Tato doktrína se rozšířila právě na případy uplatňování soudní pravomoci na jednání v prostředí Internetu. Základní problém této doktríny účinku je její neurčitost. Další problém je, že rozšíření dosahu účinku založeného pravidly o určování soudní pravomoci vede k rozšíření propasti mezi přiměřenými důvody pro uplatnění nároků na určení soudní pravomoci a aplikaci práva na straně jedné a přiměřenými důvody pro uznání a výkon cizích soudních rozhodnutí na straně druhé. Ačkoli výše uvedený článek 4 odst. 1 písm. c) Směrnice zdánlivě využívá principu objektivní teritoriality, ve skutečnosti se nezaměřuje na použití vybavení jako takového, ale spíše se snaží zabránit správcům dat, aby obcházeli právní normy EU tím, že přestěhují své sídlo mimo její území.

Pracovní skupina 29 tak jasně deklarovala, že jedním z hlavních účelů článku 4 odst. 1 písm. c)[509] je ochrana jednotlivců v EU. Zdá se tedy, že účelem tohoto ustanovení je především chránit jednotlivce v EU, a to i přesto, že nesplňuje tradiční kritéria principu ochrany, jehož účelem je chránit stát před jednáním, které se uskutečnilo v zahraničí a které ohrožuje jeho suverenitu. Takto určená soudní pravomoc se obvykle omezuje na trestní právo a závažné přečiny, které ohrožují bezpečnost státu, a za běžných okolností by se to nemělo týkat přestupků proti právu na ochranu osobních údajů. Dle principu ochrany je navíc hlavním cílem ochrana státu, nikoli ochrana jednotlivce (jako je tomu v případě práva na ochranu osobních údajů). Členské státy EU si však zjevně princip ochrany vykládají velice zeširoka, vybočujíce tak z kontextu bezpečnostních otázek, takže jeho uplatňování pak připomíná uplatňování principu objektivní teritoriality nebo doktríny účinku (viz výše).[510] V každém případě platí, že výše uvedený článek 4 odst. 1 písm. c) Směrnice stanoví, že právo EU se použije na zpracování osobních údajů, které se uskutečňuje v rámci činností provozovny správce dat v EU. Přesný výklad tohoto ustanovení je však věcí národního práva členských států a mezi těmito výklady jednotlivých členských států existují podstatné rozdíly, z nichž některé rozšiřují dosah své soudní pravomoci a práva ještě

507 Viz Evropská komise. *Analysis and impact study on the implementation of Directive EC 95/46 in Member States* (2003), která uvádí, že „Ustanovení ve Směrnici, podle kterého jsou správci povinni jmenovat zástupce v případě, že takové prostředky použijí, řecké právo tento požadavek rozšířilo nad rámec toho, co zamýšlela Směrnice, když uložilo povinnost, aby všichni správci působící mimo Řecko jmenovali zástupce, pokud zpracovávají údaje o řeckých občanech". Dostupné z: ec.europa.eu/justice_home/fsj/privacy/docs/ lawreport/consultation/technical-annex_en.pdf

508 SVANTESSON, B., ref. 457.

509 Viz stanovisko Pracovní skupiny 29, WP 56 (s. 13) 7, kde se uvádí, že cílem tohoto ustanovení je, *„že jednotlivec by neměl být bez ochrany, pokud jde o zpracování, které se uskutečňuje v jeho zemi"*.

510 KUNER, Ch., ref. 484.

dále, než činí samotná Směrnice.[511] Článek 4 odst. 1 písm. c) Směrnice má navíc za následek, že se právo členského státu uplatňuje v případě, kdy „správce není usazen na území EU a používá za účelem zpracování osobních údajů prostředků, automatizovaných či nikoli, umístěných na území zmíněného členského státu, ledaže jsou tyto prostředky použity pouze pro účely tranzitu přes území EU", čímž dochází k rozšíření působnosti práva EU i za územní hranice členských států EU. Jak již bylo uvedeno výše, soudní pravomoc v případě stížností předložených národnímu úřadu pro ochranu osobních údajů se určuje podle článku 28 odst. 6 Směrnice, která zakotvuje pravidlo teritoriality, takže každý národní úřad pro ochranu osobních údajů (DPA z angl. Data Protection Authority) má pravomoc rozhodovat o zpracování dat, k němuž došlo na jeho území.[512]

Ve Směrnici č. 58[513] chybí kolizní normy (ustanovení o střetu práva), jako je článek 4 Směrnice. Evropská komise a národní úřady pro ochranu osobních údajů obecně považují územní působnost Směrnice č. 58 za obdobnou působnosti směrnic na ochranu spotřebitele, jako je například Směrnice o smlouvách uzavřených na dálku,[514] která se v důsledku použije na jakékoli komerční vztahy s jednotlivcem ve členském státě EU.[515] Tento názor vychází z článku 3 odst. 1 Směrnice č. 58, který stanoví, že *„tato směrnice se vztahuje na zpracování osobních údajů ve spojení s poskytováním veřejně dostupných služeb elektronických komunikací ve veřejných komunikačních sítích v rámci Společenství"*. Panuje všeobecný názor, že k tomu, aby se mohla uplatnit směrnice o soukromí a elektronických komunikacích, musí být poskytována veřejně dostupná služba elektronických komunikací ve veřejných komunikačních sítích v EU, což ve svém důsledku znamená, že jakékoli využití sítí, které se fyzicky nacházejí v EU, této směrnici podléhá a tudíž jakýkoli jednotlivec v EU, který takovou síť použije, požívá ochrany, jež tato směrnice poskytuje. Evropská komise je v tomto toho názoru, že tato směrnice platí i pro nevyžádané komerční e-maily ze zemí mimo EU zasílané jednotlivcům v EU, a to navzdory skutečnosti, že vymahatelnost takovéhoto přístupu je z pohledu jakéhokoliv následného správního postupu v mnoha směrech problematická.[516]

Extrateritoriální dopad může mít i právo na ochranu soukromí platné v severoamerických zemích. Zákon USA o ochraně mládeže na Internetu (Children's Online Privacy Protecti-

511 Například německý federální zákon o ochraně osobních údajů (§ 1 odst. 5 uvádí, že zákon se vztahuje na správce dat mimo EU, pokud shromažďují, zpracovávají nebo používají osobní údaje v Německu).

512 KUNER, Ch., ref. 484.

513 Směrnice č. 58.

514 Směrnice Evropského Parlamentu a Rady 1997/7/ES ze dne 20. května 1997, o ochraně spotřebitele v případě smluv uzavřených na dálku, [1997] Úř. věst. L144/19.

515 Viz stanovisko Pracovní skupiny 29, WP 56 (str. 13) argumentující, že *„směrnice o smlouvách uzavíraných na dálku se vztahuje i na subjekty usazené mimo EU, které prodávají zboží občanům EU např. mailem, po Internetu atd.!"*

516 Viz Evropská komise, Generální ředitelství pro informační společnost a média, Pracovní dokument „Practical follow-up to the opt-in approach regarding unsolicited electronic mail for direct marketing as included in Directive 2002/58/EC" na s. 6, kde se uvádí, že tato směrnice se vztahuje na zpracování osobních údajů v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací ve veřejných komunikačních sítích ve Společenství. Článek 13, který zavádí pravidlo „výslovného projevu vůle", se tedy vztahuje na veškerou nevyžádanou komerční komunikaci přijatou nebo odeslanou ze sítí ve Společenství. To znamená, že tyto zprávy pocházející ze třetích zemí musí splňovat normy ES stejně jako zprávy původem z ES odeslané na adresy ve třetích zemích.

on Act – COPPA[517]) platí na všechny webové stránky kdekoli na světě, které shromažďují osobní údaje od dětí v USA, a zejména na webové stránky, které jsou provozovány mimo USA, ale *„jsou zaměřeny na děti ve Spojených státech nebo vědomě shromažďují informace od dětí ve Spojených státech"*. Také nařízení o prodejním telemarketingu vydané Federální obchodní komisí v USA (Telemarketing Sales Rule – TSR) se vztahuje na prodejce a obchodníky ze zemí mimo USA prodávající zboží formou telemarketingu, kteří se obracejí na spotřebitele v USA. V Kanadě v roce 2007 Federální soud rozhodl, že ačkoli zákon o ochraně osobních údajů a elektronických dokumentech (Personal Information Protection and Electronic Documents Act - PIPEDA[518]) nemá extrateritoriální účinky, má kanadský Federální komisař pro ochranu osobních údajů pravomoc vyšetřovat nelegální shromažďování dat v Kanadě organizacemi, které mají sídlo mimo kanadské území. I v Austrálii může mít právo na ochranu osobních údajů extrateritoriální účinky. Například australský zákon o spamech z roku 2003 zakazuje nevyžádané komerční emaily s vazbou na Austrálii, a to dokonce i v případech, kdy má zpráva původ mimo Austrálii, ale byla na jejím území otevřena. A § 5B australského zákona na ochranu osobních údajů z roku 1988 stanoví, že se zákon může za jistých omezených okolností uplatnit i na činy nebo jednání, k nimž došlo mimo Austrálii, pokud se takový čin nebo jednání týká osobních údajů o australském občanovi nebo osobě, která má v Austrálii bydliště.[519]

Ponecháme-li stranou otázku vhodnosti samotné regulace hranic, lze nepochybně soudit, že teritoriálně zcela neomezená regulace a vymáhání práva v prostředí Internetu mohou být v mnoha směrech dvousečné, přičemž nezřídka záleží na značně subjektivním úhlu konkrétního pozorovatele, ať již je takovým pozorovatelem konkrétní stát nebo člověk. V tomto ohledu lze považovat za zcela přirozené, že v případě vzájemné realizace či vynucování těchto „svých" práv či hodnot, která jsou mnohdy navíc v přímém konfliktu, se začínají vyhledávat způsoby, jak upřednostnit vlastní systém hodnot, případně alespoň na tento systém navazující práva. Internet s hranicemi by měl jednu velkou výhodu, umožnil by lidem s různými systémy hodnot koexistovat v rámci veřejného prostoru této sítě.

M. Trimble[520] uvádí, že existují v zásadě tři způsoby, jak na Internetu vybudovat hranice: první dvě metody vycházejí z filtrování obsahu a třetí staví na jednání provozovatelů webových stránek. Filtry obsahu lze instalovat přímo na hardware uživatelů nebo použít na úrovni poskytovatelů internetových služeb, tedy těch, kteří připojují uživatele na Internet, jako jsou kabelové společnosti, telefonické společnosti a poskytovatelé bezdrátového připojení. První způsob filtrování, tedy filtry instalované na hardwarovém vybavení, považuje M. Trimble za velice kontroverzní,[521] druhý způsob, tedy filtrování obsahu u poskytovatelů služeb, má

517 Dostupné [online] z: www.coppa.org/coppa.htm

518 Dostupné [online] z: http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf

519 KUNER, Ch., ref. 498.

520 TRIMBLE, M. The Future of Cybertravel: Legal Implications of the Evasion of Geolocation (April 12, 2012). Fordham Intellectual Property. *Media & Entertainment Law Journal.* Vol. 22, 2012, s. 580.

521 S tím lze dle autora tohoto textu zcela souhlasit, jakékoliv filtrování obsahu představuje svého druhu specifické nakládání s obsahem (daty), což může mít zásadní dopad do soukromí, případně vliv na použitelnost služeb, případně jejich dílčí provázanost.

jistě své opodstatnění, zejména pak tehdy, používá-li se v rámci výkonu rozsudků či správních rozhodnutí. [522]Pokud však nevychází z rozhodnutí o konkrétním individuálním obsahu, není patrně žádný typ filtrace obsahu přijatelným prostředkem, jak dosáhnout běžného dodržování místních právních předpisů. Na tyto metody filtrace veřejnost obvykle nahlíží se značnou dávkou skepticismu, ne-li pobouření. Akademici namítají, že tyto dva typy filtrování by měly být zakázány, jelikož jsou v rozporu se svobodou projevu, a ESD nedávno rozhodl, že soudem uložené, časově neomezené, obecné filtrování porušuje Listinu základních práv EU a ostatní legislativu EU.[523] Třetí metoda vytyčování hranic na Internetu ponechává břemeno na příslušných provozovatelích webových stránek a vyžaduje, aby právě oni přijímali opatření nezbytná k dodržování místně definovaných povinností. Tato metoda má několik výhod. Za prvé předchází veřejnému pobouření spojenému se zasahováním státu do provozu na Internetu a vzniku případných problémů s porušováním ústavních a lidských práv, které by mohly vyvstat z důvodu zásahů mající povahu cenzury. Za druhé tato metoda staví na osobách, které vždy skutečně znají obsah webových stránek, a tudíž by měly být s to posoudit své právní závazky v různých územních kontextech.[524] Za třetí tato metoda nezpochybňuje postavení poskytovatelů internetových služeb jako běžných dopravců, kteří mají nárok na bezpečné přístavy, které je chrání před druhotnou odpovědností.[525] Zásada bezpečného přístavu vychází z teorie, že běžní dopravci neznají obsah nákladu, který přepravují, a nemají technické možnosti, které by jim umožnily efektivně sledovat obsah, a zabránit tak přímému porušování zákonů. Pokud to stát nařídí a poskytovatelé služeb začnou filtrovat některé obsahy, bude postavení běžného přepravce ohroženo.[526]

Třetí metoda vytyčování hranic na Internetu prostřednictvím provozovatelů webových stránek je pravděpodobně lepší než druhá metoda, která vychází z filtrování obsahu prováděného poskytovateli internetových služeb. Provozovatelé těchto služeb zde mají lepší pozici k tomu, aby omezovali nebo blokovali přístup na ke svým službám uživatelům z některých vybraných zemí. K dosažení tohoto cíle využívají provozovatelé webových stránek nástroje pro geolokaci.[527] Co se týče ochrany soukromí, existuje bezpočet příkladů, které dokládají široké

522 Soud může například poskytovatelům internetových služeb nařídit, aby zablokovali přístup na webové stránky, které se neřídí rozhodnutím soudu vydaným dle místních předpisů proti pornografii. Je problematičtější, pokud vláda požádá, aby poskytovatelé služeb filtrovali obsah webových stránek kvůli pornografii a blokovali ho bez jakýchkoli formálních řízení, které by rozhodly o jeho nezákonnosti.

523 Viz případ C-70/10, *Scarlet Extended SA proti Societe Beige des Auteurs,* Compositeurs et Editeurs SCRL (SABAM).

524 Situace je o to komplikovanější, když provozovatelé, jako je eBay nebo YouTube, poskytují prostor uživatelům, kteří zde mohou vkládat svůj vlastní obsah; o míře, do jaké jsou tyto provozovatelé sto sledovat obsah nahrávaný uživateli, se dá jen diskutovat. Např. *Content ID,* YouTube, viz www.youtube.com/t/contentid

525 Poskytovatelé internetových služeb nebo provozovatelé webových stránek provozující vyhledávače nebo veřejná fóra s obsahem, který vkládají uživatelé, by neměli nést odpovědnost, pokud je jejich odpovědnost omezena ustanovením o bezpečném přístavu. Viz např. Digital Millennium Copyright Act, 17 U.S.C. § 512(g)(2) (2010); Communications Decency Act, 47 U.S.C. § 230(c) (2006); směrnice Evropského parlamentu a Rady 2001/31/ES z 8. června 2000, o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu na vnitřním trhu, čl. 12–15, ÚV 2000 (L 178) I, 3.

526 SATOLA, D. a H. JUDY, ref. 152.

527 TRIMBLE, M. The Future of Cybertravel: Legal Implications of the Evasion of Geolocation (April 12,

prosazování institucionálních obranných prostředků v praxi.[528] Pro úplnost je však nutné dodat, že v rámci EU je otázka přístupu k zahraničnímu právu kladena zejména v návaznosti na poměrně širokou a nadále se rozšiřující unifikaci kolizního práva, kdy je třeba zajistit, aby kolizní normy sjednocené na evropské úrovni byly efektivně využívány. Uvedeným se výslovně zabývá Prohlášení Komise k přístupu k zahraničnímu právu (článek 30 Řím II), kde se praví, že *„Komise, vědoma si rozdílné praxe v jednotlivých členských státech, pokud jde o přístup k zahraničnímu právu, zveřejní s přihlédnutím k cílům Haagského programu nejpozději čtyři roky po vstupu nařízení Řím II v platnost a v každém případě, jakmile bude k dispozici, horizontální studii o používání zahraničního práva v občanských a obchodních věcech soudy členských států. Je rovněž připravena přijmout v případě potřeby odpovídající opatření.*"[529]

5.4 Závěrem k problému (přeshraniční) působnosti práva

Výše uvedené skutečnosti prakticky a v mnoha směrech výrazně omezují vynutitelnost práva v prostředí Internetu. Je nutné vycházet ze skutečnosti, že domáhání se efektivní ochrany svých práv v tomto prostředí znamená často soudní řízení konané buď v jednotlivých státech, případně v domovském státě podle cizího práva. Z pohledu běžného uživatele, nikoliv však nutně např. poskytovatele služeb či investora, jde o řízení poměrně nákladné a v případě úspěchu takovéhoto postupu pak navíc dochází k problémům při uznání a výkonu těchto rozhodnutí, ať již u nás nebo v zahraničí, nemluvě o specifických problémech zejména v rovině důkazní spolehlivosti a relativní anonymity tohoto prostředí.[530]

Pro konkrétního uživatele to obvykle znamená, že na ochranu svých práv rezignuje. V horším případě rezignuje i konkrétní orgán veřejnoprávní ochrany, a to buď s odůvodněním na absenci spolehlivých důkazů z důvodů anonymity tohoto prostředí, případně z důvodů nedostatku místní působnosti.[531] Za zmínku stojí v tomto ohledu i rozsudek[532] Nejvyššího soudu ČR týkající se obvinění z trestného činu pomluvy prostřednictvím za tímto účelem patrně i založené internetové diskuse o zaměstnancích Záchranné služby hl. m. Prahy. V tomto ohledu bylo předmětem kritické posouzení postupu vyšetřovatele Policie ČR, který zastavil trestní

2012). Fordham Intellectual Property, *Media & Entertainment Law Journal,* Vol. 22, 2012, s. 582.

528 SATOLA, D., JUDY, H. Towards a Dynamic Approach to Enhancing International Cooperation and Collaboration in Cybersecurity Legal Frameworks: Reflections on the Proceedings of the Workshop on Cybersecurity Legal Issues at the 2010 United Nations Internet Governance Forum. 37 William Mitchell Law Review 1745, 2011. s. 1763

529 PAUKNEROVÁ, M., ref. 475, s. 1276.

530 K tomu doporučuji KOMÁREK, J. Tentýž čin v Prostoru svobody, bezpečnosti a práva – komentář rozsudku Soudního dvora ve věci C-436/04 Van Esbroeck, *Jurisprudence* č. 3/200.

531 Tacitním důvodem jsou pak obvykle důvody spočívající v osobní kvalifikaci, případně jazykové vybavenosti.

532 Viz rozhodnutí Nejvyššího soudu sp. zn. 4 Tz 265/2000 ze dne 6. ledna 2001. Dostupné [online] z: www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/B82A96F8E1B60D3AC1257A4E00694707?openDocument&Highlight=0

stíhání z důvodů skutečnosti, že se skutek stal v prostředí Internetu.[533] Problém přeshraniční vymahatelnosti v podobě absence efektivního vynucení ze strany státu je tak nutné považovat za velmi významný. Právo zde zcela jistě působí a platí, nicméně prostřednictvím svých tradičních nástrojů není způsobilé jednání v tomto prostředí fakticky a efektivně regulovat. V tomto ohledu je třeba hledat pomoc buď v samotné spolupráci s existujícími autoritami (poskytovateli služeb, doménovými autoritami, provozovateli a poskytovateli příslušného obsahu atd.), případně v užší mezinárodní spolupráci ve výše uvedeném smyslu.

Klíčová slova

Kolizní normy, určení rozhodného práva, přeshraniční působnost práva, globální povaha Internetu, nařízení Řím I., nařízení Řím II., spotřebitelské smlouvy

533 Nejvyšší soud v tomto ohledu mimo jiné dovodil, že: „*Podstata porušení zákona v daném případě spočívá v tom, že vyšetřovatel učinil rozhodnutí o zastavení trestního stíhání, aniž náležitě zjistil skutkový stav a provedl veškeré dostupné důkazy, které se v této věci nabízely… Dále nebyl vyžádán znalecký posudek z oboru výpočetní techniky k provedení zkoumání zajištěných internetových stránek nalézajících se pod výše uvedenou internetovou adresou s cílem získat údaje směřující k identifikaci provozovatele freewebu i k identifikaci osoby, která uvedené stránky zřídila a která pomlouvačný text na tyto stránky umístila.*“

— Kapitola 5.

6. Exempla trahunt aneb k některým úkolům rozhodovací praxe

6. Exempla trahunt aneb k některým úkolům rozhodovací praxe
Klíčová slova — 184

6. Exempla trahunt aneb k některým úkolům rozhodovací praxe

Vlčí rozsudek
Kde potůček si bystře tek', tak stálo jehně, žíznilo.
Tu kousek výš si stoupne vlk; a když se jehně napilo,
vlk přijde blíž a chmuří se a hledá „slušné" důvody,
jak s neviňátkem začít spor. Ač pilo níž tam u vody,
hned zhurta na ně vyjede: „Mně kalíš vodu před nosem!"
A jehně: „Právě od tebe ta voda běží přímo sem."
Tak pádnou pravdou umlčen, vlk zosnuje si novou lež:
„A před rokem mě tupilos, což popírat snad nebudeš."
Tu vyděšené jehňátko: „Já tebe že jsem tupilo?
A jak bych mohlo, prosím tě, když před rokem jsem nežilo?"
„Tvůj otec – ten mě pohaněl," – a vlk zuří po straně;
a ještě dřív, než úžasem se zmohlo k nové obraně,
je popad' za krk, zadávil a už je vleče od vody…
„Můj hlad," si mručí, „přemůže i nejpádnější důvody."
Svět ezopských bajek. Praha, 1976, s. 552.

Jedním z důvodů pro volbu samotného podtitulu této publikace, tj. celkové orientace na ochranu soukromí v intencích její vyváženosti, byla zejména skutečnost, že je to právě oblast soukromí, případně ochrany osobních práv či údajů, která má již ve své podstatě zakořeněnu Dworkinovu teorii vyvažování práva (viz níže) ve smyslu poměřování jednotlivých hodnot za účelem dosažení co nejširší právně-argumentační základny.

Lze dokonce konstatovat, že je to právě současný ZoOÚ, kde je neobvykle silně promítnuta zásada proporcionality již v jeho samotném normativním znění, a to navíc způsobem aplikačně poměrně jasným a konformním. Zásluhy za tuto skutečnost samozřejmě nelze přisuzovat jen českému zákonodárci, předmětný zákon je implementačním důsledkem Směrnice. Ve své původní podobě navíc nešlo ani v tomto ohledu o implementaci úplnou (k tomu více viz část 4.1 této publikace).[534] Právě Směrnice tak představuje první významný akt sekundárního práva (tehdejších Evropských společenství), který byl k ochraně osobních údajů přijat. Zakotvení testu proporcionality je tedy jedním ze zásadních faktorů ovlivňujících aplikaci celého systému evropské ochrany osobních údajů. Důsledná aplikace této zásady (testu) tak představuje jeden z hlavních úkolů rozhodovací praxe, přičemž se zdá být v mnoha směrech žádoucí (viz níže), aby byla aplikace tohoto testu rozšířena i na řadu dalších otázek, které se této problematiky rovněž týkají, byť samotný normativní základ na tyto situace nepamatuje. Z pohledu aplikační praxe, lhostejno, zda administrativní, úřední či soudní, je tedy právě test proporcionality ve vztahu

534 K tomu rovněž srovnej MATEJKA, J. a L. VOSTRÁ. Harmonizace práva v České republice – volný pohyb služeb na příkladu práva autorského: Obchodné právo a jeho širšie kontexty. Košice: Univerzita Pavla Josefa Šafárika v Košiciach, 2010. SUCHOŽA, J. a J. HUSÁR, eds. s. 10–31. ISBN 978-80-7097-838-2.

k účelu zásadním vodítkem, které podmiňuje použití tohoto typu ochrany. Požadavek intenzity tvrzeného porušení základního práva na soukromí (ochranu osobnosti), ve vztahu k svobodě projevu, právu na informace, případně dalších hodnot,[535] je nezbytné zkoumat z pohledu proporcionality uplatňování těchto práv (a jejich ochrany). Uplatnění testu proporcionality klade nemalé nároky na soudní či úřední praxi, významná je nejenom znalost práva a logické myšlení, ale především také argumentační dovednost. Absence jakékoliv z těchto složek může vést k nejednotnosti soudního či správního rozhodování a věcné nesprávnosti takových rozhodnutí.

Základním stavebním kamenem rozhodování ve výše uvedeném významu je především přesvědčivá argumentace a kvalitní výklad dotčených právních předpisů realizovaný ve formě důsledného odůvodnění svých rozhodnutí.[536] V rámci procesu rozhodování tak musí ten, kdo rozhoduje, aplikovat jak nabyté teoretické i praktické poznatky, tak i důsledně domýšlet reálný dopad svých rozhodnutí, včetně určitého preventivního působení takového rozhodnutí do budoucnosti. Samotný text právní normy je zcela jistě zásadním faktorem a klíčovým indikátorem směru interpretace, ale jistě nesmí být toliko jediným faktorem rozhodování. I český Ústavní soud ve své poměrně konstantní judikatuře[537] již mnohokrát dovodil, že netoleruje orgánům veřejné moci a především obecným soudům v řešení sporných případů příliš formalistický postup; zdůraznil přitom mj., že obecný soud není absolutně vázán doslovným zněním zákona, nýbrž se od něj smí a musí odchýlit, pokud to vyžaduje účel zákona, historie jeho vzniku, systematická souvislost nebo některý z principů, jež mají svůj základ v ústavně konformním právním řádu jako významovém celku a že povinnost soudů nalézat právo neznamená pouze vyhledávat přímé a výslovné pokyny v zákonném textu, ale též povinnost zjišťovat a formulovat, co je konkrétním právem i tam, kde jde o interpretaci abstraktních norem a ústavních zásad.

Soudní či správní aplikace ochrany soukromí v současném právním a technologickém prostředí naráží na řadu poměrně odlišných doktrín a přístupů. Zatímco např. evropský systém ochrany osobních údajů je v tomto ohledu relativně jednotný s důrazem na veřejnoprávní regulaci (viz níže), v případě úpravy ve Spojených státech je tomu jinak. Zásahy do soukromí jsou obvykle vykládány ve smyslu zásahu státu do ochrany poskytované Čtvrtým dodatkem Ústavy upravujícím *„prohlídky osob a obydlí“*, které lze vysledovat až k níže uvedenému rozhodnutí soudce Harlana ve věci Katz proti *Spojeným státům americkým,* v němž byla zeširoka definována

535 Účel zákona tak sám o sobě nemusí být na první pohled legitimní, byť jej v řadě případů lze považovat za projev jiných principů (např. transparentnosti ve veřejné správě, což je obecný princip uznávaný také právem EU a uplatňovaný na prvním místě ve vztahu k vlastním orgánům EU. K tomu srovnej např. CRAIG, P. EU *Administrative Law.* Oxford 2006, s. 350–360

536 Ústavní soud konstatuje, že porušením práva na spravedlivý proces podle čl. 36 odst. 1 Listiny základních práv a svobod může být i situace, kdy v hodnocení skutkových zjištění absentuje určitá část skutečností, která vyšla v řízení najevo, event. nebo tím spíše – pokud ji účastník řízení namítal, nicméně obecný soud ji náležitým způsobem v celém souhrnu posuzovaných skutečností nezhodnotil, aniž by např. dostatečným způsobem odůvodnil jejich irelevantnost. Pokud obecný soud postupuje takto, dopouští se mj. i libovůle, zakázané v článku 2 odst. 2 Listiny základních práv a svobod. (Z nálezu Ústavního soudu sp. zn. I.ÚS 2232/07 ze dne 2. 6. 2010).

537 Např. nález sp. zn. Pl. ÚS 21/96, Sbírka nálezů a usnesení Ústavního soudu, svazek 7, nález č. 13, nebo nález sp. zn. 19/98, Sbírka nálezů a usnesení Ústavního soudu, svazek 13, nález č. 19.

takováto prohlídka jako porušování rozumného očekávání ochrany soukromí.[538] Soudce Harlan v tomto ohledu formuloval dvojí požadavek tohoto testu rozumného očekávání, a to za prvé, že osoba prokázala skutečné (subjektivní) očekávání ochrany soukromí, a za druhé, že očekávání je takové, že je společnost ochotna jej uznat za „přiměřené". Soudy nakonec akceptovaly tento test formulovaný soudcem Harlanem (viz např. případ *Mancusi proti DeForte,* případně *Smith proti státu Maryland*),[539] kde konstatoval, že subjektivní prvek znamená, že *„jednotlivec prokáže, že se snaží uchránit (něco) jako soukromé"*.[540] V dalších případech byly oba tyto prvky ještě vyprecizovány, výsledná zkouška má však své nedostatky. Nejvyšší soud USA sice kritiku zkoušky přiměřeného očekávání ochrany soukromí uznává, ale nadále jí prosazuje a aplikuje, aby tak dále vymezil obrysy práva na ochranu soukromí.[541] Ochrana soukromí se tak zde zjednodušeně skládá ze subjektivních i objektivních prvků rozumného očekávání ochrany soukromí, jakož i zakotvení tzv. doktríny práv třetí strany (viz níže), která omezuje prostředky ochrany soukromí u materiálů sdílených se třetími osobami (např. sdílená data apod.). Každý z těchto prvků má své slabiny, které by měly vybízet k obezřetnosti při jejich uplatňování v moderním digitálním prostředí.[542]

Subjektivní očekávání ochrany soukromí je při prokazování legitimního (tj. v tomto ohledu rozumného) soukromého zájmu zcela logickým požadavkem. Platí tedy, že pokud někdo nemá skutečné očekávání ochrany soukromí (např. při komunikaci či v prostoru), není důvod takové osobě právo na soukromí přiznávat. Určit, zda někomu svědčí subjektivní očekávání ochrany soukromí či nikoli, může být velice obtížné. Při prokazování souvisejících skutečností může být jedním z mála vodítek skutečnost, že jednotlivec musí prokázat nějakým externím důkazem, že se snaží něco chránit jako soukromé. V tomto ohledu lze připustit i důkaz opaku, tj. např. vyvozovat takovéto závěry ze samotného aktu nakládání s předmětem této ochrany. Jakkoliv jde o prostý test, jeho aplikace je v mnoha ohledech netriviální, závěr o důkazu svědčícím ve prospěch očekávání soukromí je svého druhu závěrem zobecňujícím existující subjektivní prvek na prvek-důkaz, který bude objektivně měřitelný. Existence takovéhoto důkazu, nikoliv v rovině vnitřního psychického stavu, nýbrž právě vnějšího prvku promítajícího se do reálného prostředí života člověka, musí být spojena s konkrétním projevem vůle člověka něco chránit jako soukromé.[543] Při provádění a vážení takovéhoto důkazu by mělo být přihlédnuto zejména k povaze prostředí či komunikace, jeho právnímu (smluvnímu) režimu, jakož i samotné formě a přirozeného očekávání člověka, které je formulováno mimo jiné kulturním a sociálním prostředím. V tomto kontextu nelze vycházet pouze ze smluvní povahy konkrétní sociální sítě a (před)nastavení jejich pravidel, zkoumány mají být všechny tyto atributy, včetně celkového dopadu každého jednotlivého zásahu do soukromí.

538 KAFKA, D. Komentář: Propping Up the Illusion of Computer Privacy v případu *Spojené státy americké proti Burgessovi.* 87 Denv. U. L. Rev. 747, 757 (2010).

539 Jde tak o test, zda zásahem postižená oblast byla ta, u níž existovalo přiměřené očekávání svobody a ochrany před zásahem státu. K tomu více viz WINN, P. Katz and – the Origins of the „Reasonable Expectation of Privacy" Test. 40 *McGeorge L. Rev.* 1,7 (2009).

540 VIZ RAVA, C. Komentář: Toward a Historical Understanding of Montana's Privacy Provision. 61 *ALB. L. REV.* 1681,1703, č. 159 (1998).

541 *Kyllo proti Spojeným státům americkým,* 533 U.S. 27, 34. 2001.

542 CROWTHE, B., ref. 40, s. 343.

543 Viz LEARY, M. Reasonable Expectations of Privacy for Youth in a Digital Age. 80 *Miss. L.J.* 1035,1057 (2011)

Člověk nemůže být zbaven ochrany svého práva jen proto, že něco sdělil do veřejného prostoru (jakkoliv lze uvedené považovat za významný faktor indikující subjektivní očekávání). Je nutné přihlédnout k tomu, že v prostředí Internetu, zejména pak sociálních sítí, není mnohdy vzhledem k jejich povaze možné zachovat soukromí. Jen těžko lze presumovat subjektivní očekávání soukromí tam, kde jde o údaje umisťované do veřejného prostoru.

V případě fyzických prohlídek, které se týkají hmotného statku, se obvykle zjišťuje, zda byl dotyčný kufřík, skříňka nebo jiný prostor pro ukládání věcí fyzicky zamčený.[544] S takovým vysvětlením subjektivní prvek ve většině případů při analýze moc nezmůže a v zásadě není směrodatný.[545] Další velký problém tohoto subjektivního prvku je, že jeho legitimita záleží na přesné sondě do duše daného jedince, aby se zjistilo, zda ochranu soukromí skutečně očekává. Nebude-li mít soudce k dispozici velice nepravděpodobné přiznání dotyčné osoby, že žádné soukromí neočekávala, nezbývá mu, než hádat nebo odvodit konkrétní duševní stav této osoby z jejího jednání. Nejvyšší soud toto potvrdil v případu Smith, ale výsledek je neuspokojivý, jelikož jednotlivec stejně nese těžké břemeno důkazu, že se snaží uchránit (něco) jako soukromé. Existuje zde řada situací, kdy je velice obtížné z vnějších projevů u daného jedince soudit, zda má očekávání ochrany soukromí či nikoli. Díky tomu, jak je posuzování tohoto prvku obtížné a jak nízká je jeho praktická hodnota pro vyšetřování otázek spojených s ochranou soukromí, dochází ve většině situací k tomu, že tento prvek pohltí druhý prvek zkoušky nebo s ním splyne – tedy otázka, zda očekávání ochrany soukromí je takové, že je společnost ochotna jej uznat za přiměřené. Rozhodování o tom, jaká očekávání v otázkách soukromí je společnost ochotna považovat za přiměřená, je rovněž složitý problém. Stejně jako u mnoha ostatních norem přiměřenosti nezbývá soudům než zaplňovat prázdná místa bez jakékoliv pomoci. Za čtyřicet let, které uplynuly od případu Katz, soudy sice zformulovaly některá další pravidla, kterými by se mělo řídit posuzování prvku objektivního očekávání, tato pravidla však, bohužel, nejsou příliš použitelná mimo tradiční rámec ochrany soukromí. V roce 1978 Nejvyšší soud USA prohlásil,[546] že „legitimita očekávání ochrany soukromí ze zákona musí pramenit jinde než ve Čtvrtém dodatku; musí odkazovat buď na instituty práva upravující nemovitý či movitý majetek nebo na obecné zásady, které společnost uznává a připouští".[547] Toto prohlášení se zaměřuje na tradiční prostředí ochrany soukromí, jelikož zdůrazňuje bezpečnost místa.

Patrně vhodnějším vyjádřením této objektivní složky očekávání soukromí aplikovaného ve Spojených státech by patrně bylo, aby soudy zkoumaly široce sdílená a objektivně existující sociální očekávání.[548] Ale i když se tímto posuzování zužuje na to, co společnost obecně očekává, stále nemáme žádný postup jak určit, co vlastně to sdílené očekávání je.[549] A i u této

544 *Spojené státy americké proti Andrusovi,* 483 F.3d 711, 718 (10. okrsek 2007).

545 Viz CLAUD, M. a R. GOLDBERG. Meets the Constitution: The Supreme Court, Technology and the Fourth Amendment 72 *Miss. L. J.* 5, 28. 2002.

546 CROWTHE, B. (Un)Reasonable Expectation of Digital Privacy, Brigham Young University Law Review. 343 2012, 2012.

547 *Rakas proti státu Illinois,* 439 U.S. 128, 143 č.12 (1978)

548 *Georgia proti Randolphovi,* 547 U.S. 103, 129 (2006).

549 Tento přístup k uplatňování Čtvrtého dodatku byl v případu Randolph terčem velké kritiky vyjádřené v nesouhlasném stanovisku. Nesouhlasné stanovisko poukazovalo na to, že očekávání společnosti se dramaticky mění

normy soud poznamenal, že očekávání společnosti jsou „přirozeně značně ovlivněná majetkovým právem, avšak neřídí se jeho pravidly". Propojení přiměřeného očekávání ochrany soukromí s majetkovým právem sice může být v některých situacích praktické, a to zejména, pokud jde o chování doma, ale v případě kyberprostoru, kde se pojem „místo" stává mlhavým, prakticky ničemu nepomůže a právo upravující nemovitý nebo movitý majetek není sto dát jasnou odpověď, co je společnost ochotna uznat za přiměřené očekávání ochrany soukromí. Soudy tedy mají obecně problém určit jednoznačnou objektivní normu, pomocí které by se dalo změřit očekávání společnosti, a to zejména v elektronickém prostředí. Další obecný problém tohoto prvku je, že rozvíjí právo využívající „ad hoc" přístup.[550] Ačkoli v některých případech to může být výhoda, v právu na ochranu soukromí je výsledkem vágní norma doprovázená nekonzistentním uplatňováním, které je překážkou prapůvodním soukromým zájmům.[551] Ve vztahu k rozumnému očekávání ochrany soukromí soud v případu Katz rovněž zformuloval doktrínu práv třetí strany,[552] která stanoví, že to, co někdo vědomě uveřejňuje, a to i doma nebo v kanceláři, nespadá pod ochranu Čtvrtého dodatku. Přinejmenším v některých případech doktrína práv třetí strany podstatným způsobem omezuje přiměřené očekávání ochrany soukromí jednotlivce. V mnoha případech dokáže zcela podkopat to, co by jinak vypadalo jako soukromá situace, například při rozhovoru s blízkým přítelem. Nejvyšší soud Spojených států např. uvedl,[553] že když někdo prozradí soukromou informaci druhému, bere tím na sebe riziko, že jeho důvěrník tuto informaci sdělí úřadům, a pokud se tak stane, Čtvrtý dodatek nezakazuje, aby stát tyto informace použil. Doktrína práv třetí strany má největší smysl v kontextech, z nichž byla původně odvozena. V případu *Spojené státy americké proti Millerovi* se státu podařilo získat bankovní záznamy klienta od banky, která je vedla, a v případu *Smith proti státu Maryland,* dokázal stát získat od telefonní společnosti čísla, která byla volána z telefonu žalovaného. V obou těchto případech žalovaný dobrovolně a vědomě poskytl konkrétní, omezené informace poskytovateli služeb, aby mu tento poskytovatel mohl služby poskytnout. Závěry přijaté v těchto případech se „soustředí na fakt, že dotčené informace byly prozrazeny v rámci běžné obchodní transakce mezi uživatelem a třetí stranou a byly vedeny jako záznam o takové transakci. I bez doktríny třetí strany by bylo těžké argumentovat, že žalovaný měl ve vztahu k těmto informacím subjektivní očekávání ochrany soukromí nebo že by společnost byla ochotna uznat toto očekávání za přiměřené. Nicméně, jak je uvedeno níže, v kontextu digitálního světa se tato doktrína bortí.[554] Tato doktrína totiž vznikla ještě před nástupem doby Internetu a její zastánci tehdy nemohli přesně tušit,

na základě drobných změn ve vzorech chování a že „tento posun v očekáváních není slibným základem, na kterém by se měla stavět ústavní norma". Id. na 130 (Roberts, J., nesouhlasné stanovisko).

550 WEAVER, R. The Fourth Amendment, Privacy and Advancing Technology. 80 *MISS. L. J.* 1131, 1154–55 (2011); viz také Město Ontario proti Quonovi, 130 S. Ct. 2619, 2628. 2010.

551 BLUMENTHAL, J., M. ADYA, a J.. MOGLE. The Multiple Dimensions of Privacy: Testing Lay „Expectations of Privacy." 11 *U. PA. J. CONST. L.* 331, 341 (2009).

552 Tato doktrína byla rovněž nazývána „doktrínou dobrovolného poskytnutí informací", „vědomým vystavením se ztrátě soukromí" nebo „zásadou převzetí rizika". HALLIBURTON, M. How Privacy Killed Katz: A Tale of Cognitive Freedom and the Property of Personhood as Fourth Amendment Norm. 42 *AKRON L. REV.* 803, 842. 2009.

553 *Spojené státy americké proti Jacobsenovi,* 466 U.S. 109, 117. 1984.

554 CROWTHE, B., ref. 40.

nakolik se bude společnost muset spoléhat na digitálně ukládané informace.[555] Uvážíme-li, kolik osobních informací je v ohrožení, pak je možná pravý čas tuto doktrínu práv třetí strany konečně zrušit nebo alespoň omezit její uplatňování na tradičnější prostředí ochrany soukromí, pro které byla vytvořena. Tato doktrína vzhledem k tomu, jak obrovské množství digitálních informací je v rukou třetích osob, právo na ochranu soukromí v digitálním prostředí zcela podkopává. Postupem času se stává „stále archaičtější a problematičtější", jelikož třetí strany jsou stále častěji „zdánlivě anonymní a automatičtí poskytovatelé služeb přes on-line média." Zrušení doktríny by zabránilo dalšímu poškozování ochrany soukromí v digitálním prostředí a otevřelo lepší možnosti prokazování přiměřeného očekávání. Jeden vědec optimisticky poznamenal, že trendy minulého desetiletí naznačují, že doktrína je již na úpadku a pomalu směřuje ke svému zániku.[556] Pro dobro ochrany soukromí v digitálním světě doufejme, že tento trend bude pokračovat.

Jedním z celosvětových problémů aplikační praxe týkající se ochrany soukromí v prostředí Internetu je neznalost věcné (technické) povahy tohoto prostředí. Lze si jen velmi těžko představit právo aplikujícího úředníka či soudce, který nikdy nepoužil počítač či Internet, aby aplikoval právo v tomto prostředí. Takový stav by patrně vedl k nekonzistentním postupům a matoucímu rozhodování. Bohužel se takové případy stávají. Soudy v řadě případů postrádají povědomí o základních technických skutečnostech a principech, aby mohly pochopit technologii, kterou se snaží nepřímo regulovat, mnohdy tak velmi zbytečně svěřují tuto problematiku znalci, byť nezřídka jde o otázky právní a nikoliv znalecké. Budou-li soudci lépe srozuměni s fakty, budou pochopitelně s to věci lépe odůvodnit a tedy dospět k solidnějším závěrům. Soudy by měly při rozhodování o věcech ochrany soukromí v prostředí Internetu postupovat spíše empiricky, nežli volit čistě subjektivní přístup. Vkládáním naprosté většiny svého soukromí v digitálním prostředí do rukou poskytovatelů služeb a dalších autorit v prostředí Internetu se neúmyslně vzdáváme svého práva na soukromí v mnoha sférách života, které by měly zůstat soukromé.

Klíčová slova

Aplikační praxe, digitální informace, doktrína práv třetí strany, Georgia vs. Randolph, konstantní judikatura, Kyllo vs. USA, legitimita očekávání, Mancusi vs. DeForte, odůvodnění rozhodnutí, ochrana osobních údajů, ochrana osobnosti, ochrana soukromí, poskytovatel, zásada proporcionality, Rakas vs. Illinois, sdílená data, Smith vs. Maryland, USA vs. Miller, USA vs. Jacobsen, ústavní konformita.

555 BAGLEY, A. Don't Be Evil: The Fourth Amendment in the Age of Google, National Security, and Digital Papers and Effects. 21 Alb. *L. J. Sc. & TECH.* 153, 174 (2011). Cloud computing zahrnuje ukládání dat a spouštění programů pomocí externího počítačového systému, jako jsou cizí servery.

556 HANDERSON, E. The Timely Demise of the Fourth Amendment Third Party Doctrine. 96 *IOWA L. REV. BULL.* 39, 39–40. 2011.

7. Závěr a další spekulace

7. Závěr a další spekulace

„Nejvyšší dovršení společnosti spočívá ve spojení pořádku a anarchie."[557]
Pierre-Joseph Proudhon[558]

Jedním z cílů této práce bylo především ověření hypotézy, zda současné technologické změny zasahují do existujících právních vztahů a práva natolik významně, že dochází k narušení samotné podstaty fungování některých tradičních právních postulátů. V tomto ohledu bylo opakovaně konstatováno, že právo na tyto změny věcně sice reaguje, nicméně svou povahou jde o přístup v mnoha směrech nahodilý. Navíc se zřetelem k požadavku na efektivní fungování práva v mezinárodním prostředí pak jde o reakce v mnoha směrech nejednotné, nekoordinované a v mnoha směrech nerespektující globální povahu a rozumné očekávání nositelů subjektivních práv. Uvedené je způsobeno tím, že tyto technologické změny generují normativně značně obtížně řešitelné právní problémy, které mohou vyústit v přeformulování těchto po staletí uznávaných právních institutů. Do jisté míry jde však bezesporu o jev, který dříve či později nastane u celé řady dalších institutů, lhostejno zda se tak stane z důvodů kulturních (zejména pokud jde o konflikty), politických či vlivem pokroku v poznání lidstva. V tomto ohledu však lze jistě oprávněně dovozovat, že jde o něco, co si vzhledem ke své závažnosti zasluhuje hlubší zkoumání z důvodů své přítomné či budoucí důležitosti a významu pro samotnou podstatu práva.

Je zřejmé, že dosavadní systém ochrany soukromí byl vyvinut v prostředí zcela odlišném oproti tomu, které známe nyní. Většina existujících rozhodnutí týkajících se soukromí měla svou věcnou podstatu ve zveřejňování (soukromých) údajů prostřednictvím tradičních médií. Koncept ochrany soukromí je tak postupně přestavován do podoby, aby byl schopen efektivně chránit soukromí jednotlivce v prostředí informační společnosti. Tradiční média reprezentovaná významnými subjekty (vydavateli, nakladateli, televizními společnostmi), které dosud poskytovaly obsah, představovala významnou institucionální bariéru mezi lidmi, kteří chtějí veřejně promlouvat, a jejich cílovými posluchači. Veřejné šíření informací tímto tradičním způsobem tak bylo vázáno na interakci s tímto subjektem, který tak zprostředkovával komunikaci takovéhoto projevu směrem k veřejnosti a nesl veškeré související náklady takovéhoto šíření. Významně tak ovlivňoval nejenom auditorium těchto projevů, ale v určitých případech i samotný obsah. Tyto bariéry však s nástupem informační společnosti zmizely. V současné době tak může kdokoliv vyhlásit do světa cokoli, byť i anonymně. Internet je pak ideálním prostředím, kde neplatí osvědčené modely „chování", právní postuláty a paradigmata, včetně

557 TOMEK, Václav a Ondřej SLAČÁLEK. *Anarchismus: svoboda proti moci.* Praha: Vyšehrad, 2006. ISBN 80-7021-781-2. Kapitola 4. Vlastnictví – krádež, nebo záruka svobody?, s. 87.

558 Jakkoliv byl Pierre-Joseph Proudhon spíše socialistický myslitel, povoláním však typograf, bývají jeho myšlenky týkající se vztahu práva a anarchie v souvislosti s fungováním Internetu připomínány právem. Tento autor navíc zpopularizoval tvrzení že „vlastnictví je krádež", což je podobně hojně využíváno odpůrci současné koncepce ochrany duševního vlastnictví. Více viz http://en.wikipedia.org/wiki/Pierre-Joseph_Proudhon

zcela zásadní skutečnosti, že Internet nezapomíná. Navzdory omezeným možnostem a celkové složitosti právní regulace těchto otázek, lze jistě překonat bariéry týkající se globální (nadnárodní) povahy Internetu a teritoriální efektivity práva, avšak bariéry týkající se spravedlivého řešení konkrétních situací, kde bude nutno velmi pečlivě vyvažovat veřejný zájem na jedné straně a ochranu soukromí člověka na straně druhé, nebude snadné překonat. Existuje jen velmi málo fyzických nebo technických omezení možnosti šířit takovéto projevy (obsah), a to zcela bez ohledu na množství či původní auditorium takového obsahu. V prostředí Internetu může být zaznamenáván, uchováván a dále bezbřeze šířen a zpracováván v zásadě každý sebemenší pohyb (kliknutí), mnohdy jsou pak přebírány informace (např. vyhledávači), jejichž kvalita je sporná, přičemž tyto informace zůstávají přístupné všem neomezeně dlouho, mnohdy i celý život člověka. Snaha o realizace tzv. práva být zapomenut tak může působit v obecné rovině neskutečně, z pohledu technického pak možná i zcela nereálně a neuchopitelně, nicméně jde jistě o legitimní a logické úvahy, které by měly být předmětem veřejné diskuse a důslednějšího poměřování s účely celé jinými řady jiných práv.

Zcela jistě nelze připustit, že 21. století bude stoletím, kdy došlo k upuštění od ochrany soukromí člověka. Rezignace na ochranu této hodnoty je nepřípustná, byť nelze jistě vyloučit, že obsah soukromí člověka je natolik kulturně, sociálně a technologicky proměnlivý, že jsme v současné době svědky změny celkového paradigmatu, a to zcela ve smyslu výroků, že ten kdo nemá co skrývat, nepotřebuji ochranu svého soukromí a je si toho velmi dobře vědom. Společenské výhody tohoto fenoménu jsou ohromné a v mnoha směrech již poměrně obstojně doložené.[559] Jak ale známo, nic není zadarmo. Vždy existují určité rozumné limity toho, co tradiční média zveřejní a co nikoliv. Tradiční média se obvykle snaží vyvažovat existující soukromé zájmy s právem veřejnosti na informace. Ve světě neomezeného šíření informací takovéto vyvažování nehraje tak zásadní roli, pro případné blogery tak nemusí být vůbec důležité, co veřejnost vlastně potřebuje vědět, naopak zásadní je především to, co chce osobně sdělit. Toto však zcela jistě neznamená, že výše uvedená bariéra přestala existovat, institucionální úsudek (např. redaktora tradičních novin, případně tvůrce myšlenkového obsahu médií apod.) bude mít nepochybně stále svou hodnotu. Tradiční média tak zcela jistě nezmizí, posláním médií není pouze realizace svobod projevu, snahou médií je realizovat zisk. V tomto ohledu může být výše uvedená bariéra jistou přidanou hodnotou, jež si najde své auditorium. Internetové aplikace, které uživatelům umožňují přímou komunikaci s veřejností, ponechávají rozhodnutí o tom, zda vůbec a pokud ano, tak jaký typ informací zveřejnit, na jednotlivcích nebo organizacích s úplně jiným posláním, než mají tradiční institucionalizovaná média.

Chceme-li, aby uživatelé Internetu i nadále využívali technologie v plném rozsahu, musí jim platná právní úprava (kód) dát nástroje, pomocí kterých budou moci přijímat odpovědnější rozhodnutí o míře zachování práva na soukromí. Musí to však být takové nástroje, které těmto uživatelům poskytnou dostatečné prostředky k vyjádření individuálních preferencí ve vztahu k zveřejňovanému obsahu. Zároveň musí jít o takové změny stávající platné právní

559 LEMLEY, Mark A. a L. LESSIG. The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era. 48. *UCLA Law Review.* 925, 933-32. 2001.

úpravy, které zakotví efektivní ochranu ve vztahu k zásahům do práva na soukromí, které by tyto preference nedodržovaly, a zachovají tomu přiměřené prostředky ochrany svobody projevu.

Ačkoliv se tato práce snaží nabídnout mimo jiné alternativu některých dosavadních řešení včetně těch doktrinárních či judikaturních, není jejím cílem informovat, zda jde o řešení špatná či dobrá. To nechť si posoudí čtenář sám. Publikace měla také další cíl, a to nabídnout nový či jiný úhel pohledu, včetně samotné analýzy a nástinu vybrané materie ochrany soukromí v EU. V tomto ohledu práce představuje dílčí příspěvek právní vědy k poznání tak rozmanité a rozsáhlé oblasti, jakou je okruh nových právních vztahů vznikajících zejména v souvislosti s existencí Internetu, jeho souvisejících služeb či protokolů. Oblast, kterou se tato práce zabývá, je nezřídka označována za nepředvídatelnou, právně značně nejistou až entropickou. V tomto ohledu je skutečně jistým faktem, že v prostředí Internetu skutečně existují určité anarchisticky působící faktory, narušující po technické stránce jinak velmi dobře organizovaný systém. Tyto faktory pak na právo působí značně entropicky, přičemž významným způsobem narušují existující důvěru v toto prostředí. Vzniká tak úzký vztah právní entropie a anarchie, jako nedílného důsledku omezené důvěry v právo v tomto prostředí. Pro úplnost je však třeba uvést, že prostředí Internetu nelze rozhodně považovat za zcela anarchistické, jakkoliv je určováno entropií práva *per se*, jež u kořenů jisté zdánlivé anarchie stojí. Anarchie je totiž určována především absencí jakýchkoliv autorit, případně jejich společným selháním, což nutně vede k neorganizovanosti a chaosu, samotným výsledkem anarchie je tak bezvládí.

V prostředí Internetu bezpochyby nevládne bezpráví, právo platí podobně jako všude jinde, nicméně v některých případech zde ztrácí svou efektivitu (viz níže), a to přirozeným působením své entropie. V tomto ohledu je míra anarchie tohoto prostředí v některých svých rysech srovnatelná[560] s prostředím mezinárodních vztahů, kde rovněž v některých oblastech chybí jasná právní autorita, která by mezinárodní systém organizovala, hlídala a vynucovala elementární pravidla jeho dodržování. Internet však není prostředím bez existence autorit, proto nelze hovořit o plně anarchistickém prostředí. Autority v prostředí Internetu však fungují na zcela jiných principech, jejich smyslem je především zajistit technické fungování a účinný provoz sítě, existuje-li zde vůbec právní regulace, tak jde spíše o úpravu technických parametrů vzájemné komunikace mezi těmito autoritami než o úpravu ve smyslu regulace chování uživatelů této sítě.

Právo nakonec na fenomén Internetu jistou regulací reagovalo, opačný přístup by ve svém důsledku jen prohloubil existující entropii a anarchie by zde zakořenila podstatně více. Právní regulace Internetu je však vysoce omezená, přičemž Internet je v ní uchopen pouze jako komunikační nástroj, případně jen jako existující prostředí se specifickou povahou, kterou je třeba normativně zohlednit. V tomto ohledu hraje zcela zásadní roli soudcovská tvorba (dotváření) práva, případně odpovědný právně-politický přístup osob aplikujících právo (viz výše). Výše uvedené normativní konstrukce však kromě zmíněné entropie nezřídka trpí svou vnitřní nedokonalostí, kde platí více než jinde, že mezi realitou, tedy tím, co je v prostředí Internetu skutečně realizováno, a normativitou, tedy tím, co má být (z vůle regulátora i naší), není sho-

560 KUBÁČEK, Jan a Václav NEKVAPIL. *Politologie a mezinárodní vztahy.* Praha: Tutor, 2005, s. 193.

da. Realita Internetu a jeho normativní regulace jsou tedy dvě relativně samostatné kategorie. Právní problémy týkající se Internetu je nutno posuzovat v celkovém právním i technologickém kontextu, nikoliv pouze optikou zažitých vzorců či optikou jednotlivých právních oborů *per se*.

Z důvodů shora uvedených se tato kniha zabývá primárně realizací ochrany soukromí v prostředí Internetu, ničím více, ničím méně. I takto zúžené téma však nutně vyžaduje celkový interdisciplinární záběr, v tomto ohledu bylo nezbytné si mnoho „vypůjčit" i z jiných právních oborů, ne vždy navíc zcela konzistentně s těmito obory, a to zejména u oborů, jež jsou daleko za hranicí soukromého práva, kterým se autor této publikace dosud v převážné míře zabýval. Nezbývá než věřit, že to nebylo na úkor kvality práce, ale právě naopak. V knize se autor snažil reflektovat skutečnost, že každý (nejen právní) obor je omezen sám sebou, aniž to vypovídá cokoliv o jeho správnosti. V tomto ohledu se autor snaží spíše na jiné obory synergicky navazovat, než je stavět proti sobě, a to zejména tam, kde dochází k jejich prolínání. Vliv interdisciplinárních přístupů je v tomto ohledu významný hned z několika důvodů. Jednak tyto přístupy efektivně propojují právní vědu s dalšími lidskými obory, zejména informatikou, kybernetikou, psychologií, historií, případně s ekonomií apod. Dále pak proto, že právě zamýšlený záběr této publikace podléhá tomuto trendu velmi výrazně, což se silně projevuje jak v metodách, tak i systematizaci samotné publikace.

Právo je opakovaně konfrontováno s rozvojem techniky a technologickým pokrokem, přičemž klíčovým faktorem zde má být zejména podpora rozvoje a ochrana jeho pozitivních stránek na jedné straně, a vytváření efektivních překážek a regulace souvisejících negativních důsledků na straně druhé. V úvahách v tomto smyslu je nutné ubírat se zejména směrem k zachování minimálních standardů existující míry právní ochrany ve světle možných faktických důsledků možné budoucí aplikace konkrétní technologie v novém prostředí. Předmětem právních úvah tak není pouze technologie *per se*, ale především její aplikace v podmínkách dosavadních právních standardů a postulátů. Smyslem zde tedy není čelit souvisejícím technologickým proměnám, ale především se pokusit o jejich pochopení a zařazení do existujících podmínek právní regulace. Pouze tato cesta vede k poznání toho, jaké právní problémy a nové jevy vznikají v souvislosti s existující technologií. Úvahy v této publikaci nebudou vedeny se záměrem potvrdit, či naopak vyloučit právní rizika či nebezpečnost nějaké konkrétní technologie (či služby). Podstatou úvah naopak bude snaha o popis toho, jak právo na tyto technologie reaguje.

Samotný text této práce/publikace byl z důvodů své úspornosti systematizován do sedmi částí, včetně části poslední (závěrečné), kde první část (Internet a právo v neklidu) představuje úvod do některých otázek obecné problematiky současných či budoucích metamorfóz práva, kde je v obecné rovině nastíněn hlavní cíl této práce, tj. ověření hypotézy, že současné technologické změny zasahují do obsahu dosavadních právních vztahů natolik významně, že dochází k narušení samotné podstaty fungování práva. V této části jsou uvedeny některé dílčí spekulace a historické konotace, zmíněn je rovněž zcela zásadní význam práva koňského pro právo internetové, kde autor popisuje historické souvislosti, které považuje za velmi významné ve vztahu k budoucnosti práva kyberprostoru jako pedagogické disciplíny. Autor v tomto ohledu dále popisuje (historické) vazby práva koňského a automobilového na oblasti práva internetové-

ho. Zejména zdůrazňuje tu historickou skutečnost, že pokud jde o dopady nových technologií, má právo jako normativní systém jen velmi omezené možnosti společenské regulace. Akademický spor soudce Easterbrooka a L. Lessiga dokumentuje, že dopad technologie a rozsah její interakce s vnějším světem nelze snadno prorokovat, ještě těžší je ale předvídat jak na tyto technologie bude reagovat samotné právo. Diskutován je také případ rozvoje automobilového průmyslu v minulém století ve světle jeho právní regulace, kde se právní regulace dopustila celé řady chyb, přičemž tržní síla sehrála daleko větší roli než právní regulace. Právě psaný příběh internetového práva je srovnáván s příběhem automobilového práva jako příběhem slavné technologie, která také v mnohém překvapila. Auto změnilo svět, ale především se náš právní systém ukázal jako bezmocný a nedokázal předpovědět obrovské změny, které tato technologie vyvolá. Na druhou stranu je automobilové právo rovněž povzbuzující, jelikož dokládá potenciál právního systému v některých ohledech uspět a přinést spravedlivé výsledky v soudních řízeních. Ponoříme-li se do automobilového práva, najdeme příběhy o úřednících a právních reformátorech, kteří dělali, co mohli, aby tuto technologii vylepšili co do bezpečnosti, efektivity, infrastruktury a spravedlnosti, a často při tom museli čelit velmi silnému odporu. Ne všechny příběhy o automobilovém právu vyprávějí o úspěších, ale v případě aut bylo odvedeno spoustu kvalitní právnické práce na podporu veřejného blaha. Podobně tomu snad bude i v případě práva Internetu. Cesta internetového práva je ve své podstatě především o přizpůsobení neustále se měnících zákonů neustále se rozvíjející budoucnosti. Je totiž více než jasné, že naše „zasíťovaná" společnost potřebuje více než kdy dříve velmi dobré internetové právo a schopné průvodce tímto právem. Uživatelé těchto technologií si nepochybně zaslouží takovou právní úpravu, která nejenom, že respektuje to, jak tyto technologie fungují, ale především efektivně tyto své uživatele chrání. Zpracování této oblasti práva hraje velice důležitou roli ve vzdělávání soudů, právníků i společnosti, roli, která zahrnuje budování mostů mezi právními doktrínami a komplexně se rozvíjejícími technologiemi a postupy. Pokud bychom v ideálním případě dokázali třeba jen nahlédnout do budoucnosti, mohli bychom se vyhnout některým chybám. Soudce Easterbrook tehdy neviděl budoucnost, která už přicházela. Možná ji však nevidíme jasně ani my dnes. Naše digitální technologie jsou nejen komplexní, ale vlastně jsou ve stavu permanentní evoluce. Právo je sice systém dynamický, nicméně obvykle reaguje vždy se zpožděním. Toto zpoždění je však proměnlivé, ale jeho míra může být přímo úměrná tomu, do jaké míry se dokážeme ohlédnout zpět do minulosti a nechat se inspirovat.

Druhá část knihy (Axiologie soukromí a jeho ochrany v prostředí informační společnosti) se zabývá hodnocením a samotným významem soukromí, jako základního hodnotového postulátu této ochrany. Nastíněna je problematika celkového právního a technologického kontextu, zmíněn je především interdisciplinární záběr, který se nezřídka nachází daleko za hranicí práva. Ochrana soukromí představuje v tomto prostředí svého druhu přiměřenou soudní či jinou ochranu, přičemž samotný pojem soukromí není jednoduché definovat. Jeho definici tak zpravidla nenajdeme ani v aktuální judikatuře českých či zahraničních soudů, v mezinárodních dokumentech ani významných textech právní vědy (doktríny) či praxe. Jen výjimečně lze najít některé odpovědi v rozhodnutích Evropského soudu pro lidská práva, který obvykle váže tento pojem obecně na fyzickou i psychickou integritu osoby včetně sexuálního života. Jde tak o po-

jem *per se* značně široký a flexibilní, ostatně podobně je tomu u řady jiných právních pojmů, které jsou velmi úzce navázány na další pomocné právo – vědní disciplíny (jako např. na právní sociologii aj.). Podobně jako je tomu u řady dalších pojmů (např. spravedlnost, důstojnost, svrchovanost, jistota atd.) ani v případě pojmu soukromí není taková definice patrně žádoucí, i zde totiž platí více než jinde stará římskoprávní regule *omnis definitio (in iure) periculosa es*). Implicitní definice těchto pojmů pak lze dovodit prostřednictvím metod právní argumentace. Současné potíže s vymezením práva na soukromí pak vyplývají především z jeho samotné podstaty, konkrétně pak ze skutkových okolností konkrétního případu (typicky pak ve vazbě na tzv. informační sebeurčení). Soukromí je zakotveno v normách objektivního práva (soukromého i veřejného), zároveň však představuje významné subjektivní právo jednotlivce, který je tak chráněn i proti své vůli. Zde se může střetnout závazek státu toto subjektivní právo chránit a respektovat svobodu jednotlivce. V tomto ohledu je opakovaně diskutován rozsudek Spolkového správního soudu, který se týkal možnosti vydání živnostenského povolení k provozování tzv. peep-show, kde soud konstatoval, že toto porušení lidské důstojnosti (člověk jako objekt, ne subjekt) nelze odstranit, ani oprávnit souhlasem dotyčných dam, neboť důstojnost člověka je objektivní nezcizitelná hodnota. Jde o zajímavý příklad respektu práva k autonomii vůle člověka ve vztahu k jeho soukromí. Problém s aplikací práva na soukromí pak obvykle vyplývá i ze skutečnosti, že zákaz porušování soukromí je nějak vázán na konkrétní rozsah, jaký si sama chráněná osoba vymezí vůči veřejnosti a v jakém si vymezí hranice svého informačního sebeurčení, což ve svém důsledku objektivně snižuje tzv. právo nedostupnosti soukromí (viz např. dobrovolné zveřejnění intimní informace na sociálních sítích).

V tomto ohledu je dovozováno, že objektivní právo nemůže pracovat pouze s filozofickými a etickými kategoriemi, musí je transformovat do právního jazyka. V tomto ohledu Listina pojímá otázku práva na soukromí v mnoha směrech relativně komplexně. V článku 7 odst. 1 je zakotvena obecná garance nedotknutelnosti soukromí jako lex generalis, ze které poté v Listině vybíhá celá řada konkrétních záruk jednotlivých aspektů spojených se soukromím jedince. Stačí uvést hodnoty chráněné v článku 10 odst. 1 Listiny (lidská důstojnost, osobní čest, dobrá pověst, jméno). Všechny jsou spjaty se soukromím jedince. Totéž platí pro ochranu soukromého a rodinného života ve smyslu článku 10 odst. 2 (spojnice s mezinárodními lidskoprávními úmluvami) a ochranu před zneužíváním osobních údajů. Jiným projevem soukromí je tradiční pojetí nedotknutelnosti obydlí dle článku 12 Listiny, kde je soukromí vymezeno prostorově, stejně jako ochrana uchovávaných nebo přepravovaných písemností, záznamů a zpráv podle článku 13 Listiny. Bezprostředním výrazem ochrany soukromí je pak i článek 15 odst. 1 (svoboda myšlení, svědomí a náboženského vyznání či víry). Rovněž řada politických práv a svobod je spjata s problematikou ochrany soukromí. Zejména se jedná o aspekt negativní svobody, tedy o svobodu jedince rozhodovat o sobě tak, že určitý názor neprojeví, informaci nepřijme, postoj nesdělí atd. Jazyk lidských práv je tak svého druhu vstupní branou do společného světa argumentace. Jakýkoliv konflikt mezi dotčenými právy není abstraktním konfliktem mezi různými neutrálními principy s jasným významem, který je jaksi předem daný, a to buď proto, že koresponduje s jiným hodnotovým systémem objektivního charakteru (např. morálka), anebo proto, že existuje možnost objektivně vyjádřit jejich pořadí. Snaha řešit tyto spory argumentací, která

směřuje k nalezení jednoho správného řešení, jež se opírá o objektivní významy, trivializuje závažnost konfliktu a jeho symbolický význam pro život.

Třetí část práce (Metodologická východiska a kolize autonomie vůle s právem na soukromí) se věnuje popisu metod (analytických, logických, systematických, případně komparativních nebo syntézy), které byly v této práci použity, jakož i otázkám konfliktu hodnot, jež mohou být objektivně v rozporu s právem na soukromí. Zde je nutné mít na zřeteli zejména ústavněprávní, případně lidskoprávní rozměr celého problému, zvláště pak tu část, která se týká poměřování všech práv garantovaných ústavou, tedy práv na stejné úrovni. V tomto ohledu je dovozováno, že každý jednotlivý zásah do práva na ochranu soukromí musí být posuzován individuálně se zřetelem ke všem okolnostem dané věci. V této souvislosti je třeba uvést zejména to, že žádné ústavní právo nelze *per se* absolutizovat a nadřazovat nad jiná práva, která musejí být v dané věci aplikována současně. Takový stav obvykle nazýváme kolizí, kde je v rámci právní argumentace nutné zvažovat především existující účel a smysl každého jednotlivého zásahu. Takovým zásahem do práva na ochranu soukromí může být svoboda projevu, právo na informace, případně jiný veřejný zájem či hodnota. Při aplikaci konkrétního zákonného ustanovení je třeba mít na zřeteli zejména ústavněprávní, případně lidskoprávní rozměr celého problému, zejména pak tu část, která se týká poměřování všech ústavou garantovaných práv, tedy práv na stejné úrovni. Poměřování práv je relativně běžnou agendou většiny ústavních soudů, byť tato úvaha bývá nezřídka aplikována i na úrovni soudů obecných. Ústavní soud se opakovaně vyjádřil k otázce svobody projevu a práva svobodně vyjadřovat své názory. Ústavní soud vycházel při posuzování této otázky především z toho, že tato práva a svobody jsou obsahově omezena právy jiných, přičemž tato práva mohou vyplývat jako ústavně zaručená z ústavního pořádku republiky či z jiných zásad daných zákonem chránících celospolečenské zájmy či hodnoty. Přitom právo vyjadřovat názory mohou zbavit ústavní ochrany nejen obsahová omezení, neboť i forma, jíž se názory navenek vyjadřují, je úzce spjata s ústavně zaručeným právem, k němuž se upíná. Vybočí-li publikovaný názor z mezí pravidel slušnosti, obecně uznávaných v demokratické společnosti, ztrácí charakter korektního úsudku (zprávy, komentáře) a jako takový se již zpravidla ocitá mimo meze ústavní ochrany. Ústavní soud dále výslovně judikoval, že „základní právo podle čl. 17 Listiny je zásadně rovno základnímu právu podle čl. 10 Listiny", přičemž „je především věcí obecných soudů, aby s přihlédnutím k okolnostem každého případu zvážily, zda jednomu právu nebyla bezdůvodně dána přednost před právem druhým". Že toto právo není absolutní, lze demonstrovat na skutečnosti, že ve vztahu k osobám veřejně známým či politicky činným vychází náš Ústavní soud z přesvědčení, že právo kritiky, zakotvené v čl. 17 odst. 2 Listiny a čl. 10 Úmluvy, které je neoddělitelnou součástí svobody projevu a práva na informace, musí respektovat rovnováhu mezi tímto právem a osobnostními právy konkrétního subjektu a nemůže překračovat určité hranice spojené s atributy demokratické společnosti. Takto vymezené mantinely ve vztahu k fyzické osobě, která jedná či vystupuje jako „veřejná osobnost", jsou širší než ve vztahu k osobě soukromé.

Samotné jádro práce pak obsahuje čtvrtá část (Právní regulace ochrany soukromí, její limity a možnosti), kde je nejprve realizována kritická polemika k otázkám koncepce evropského systému ochrany osobních údajů a dat (včetně úpravy české) a dále je analyzován současný

model ochrany osobních údajů v prostředí Internetu, kde je důraz kladen zejména na zásady této úpravy a související práva a povinnosti v kontextu jejich významu pro internetovou praxi. V tomto ohledu jsou řešeny klíčové otázky aplikace současné právní praxe realizované na jednání v prostředí Internetu, jako je např. právní kvalifikace IP adresy, MAC adresy a ID datové schránky jako osobního údaje, režimu agendových informačních systémů, problematiky nevyžádaných obchodních sdělení (spamu) a sociálních sítí. Uveden je nezbytný kontext souvisejících právních režimů ochrany soukromí, jako jsou civilněprávní (občanskoprávní i pracovněprávní) a trestněprávní aspekty.

Jakkoliv je tato problematika orientována zejména na českou platnou právní úpravu, včetně řady praktických a teoretických aspektů ochrany osobních údajů v prostředí Internetu, důraz je kladen také na evropský kontext této ochrany, včetně analyticko-kritického pohledu na evropský systém ochrany osobních údajů. Za klíčovou je zde třeba považovat především pravomoc EU ke sjednocování ochrany osobních údajů ve členských státech; jejich základem je v platném právu EU č. 16 odst. 2 Smlouvy o fungování EU, který stanoví, že Evropská unie přijímá pravidla o ochraně fyzických osob při zpracovávání osobních údajů členskými státy. Toto ustanovení tedy zmocňuje Evropskou unii sjednocovat právní režim ochrany osobních údajů ve členských státech. Příslušné pravomoci jsou však, jak je z výslovného znění uvedeného ustanovení zřejmé, vztaženy především na případy, kdy jde o pohyb osobních údajů přes hranice členských států, tedy na situace s jasně přeshraničním prvkem. Jde-li o ochranu osobních údajů uvnitř členských států, tedy v situacích bez přeshraničního prvku, znění čl. 16 odst. 2 klade důraz na to, že Evropská unie může svými právními akty sjednocovat ochranu osobních údajů v členských státech pouze tehdy, „pokud členské státy vykonávají činnosti spadající do oblasti působnosti práva Unie". Kromě toho je třeba poznamenat, že s ohledem na čl. 4 odst. 1 výše uvedené smlouvy náleží pravomoci EU k ochraně osobních údajů vyplývající z článku 16 smlouvy do rámce pravomocí sdílených s členskými státy, a nejde tedy jednoznačně o pravomoci výlučné, což má nutně vliv na to, v jakém rozsahu může Evropská unie sjednocování pravidel ochrany osobních údajů provádět (výkon těchto pravomocí je tak usměrňován principem subsidiarity a proporcionality). V tomto ohledu se tak unijní právo o ochraně osobních údajů v právu členských států vztahuje na ty právní normy členských států, které jsou přijímány v návaznosti na právo EU v oblastech, které spadají do působnosti tohoto práva. Zásadně jinou působnost ve vztahu k právu členských států však unijní právo o ochraně osobních údajů nebude mít ani v případě, kdy se na unijní právo o ochraně osobních údajů bude nahlížet jako na soubor pravidel, která provádějí právo na ochranu soukromého života jako základní právo garantované právem EU, ať už bude toto právo dovozováno z Listiny základních práv EU nebo z obecných zásad, které jsou pro Českou republiku a ostatní členské státy závazné. Kritický pohled na dosavadní úpravu evropského systému ochrany lze pak dovozovat ze skutečnosti, že Směrnice položila široké základní schéma zásad zpracování osobních údajů a měla velký vliv na zákony v ostatních zeměpisných oblastech. Tento systém tak dosáhl celé řady úspěchů. Navzdory těmto kladům však stále přetrvávají jeho problémy (viz níže), a to jak v oblasti hmotněprávní a programové, tak i celkového povědomí ve smyslu dostatečné sdělnosti celého tohoto systému. Podstata těchto problémů by měla být revidována v celé řadě oblastí.

Pátá část práce (Mezinárodní spolupráce jako conditio sine qua non efektivity práva v prostředí Internetu) rozebírá a popisuje jeden ze základních právních problémů Internetu – klíčovou otázku rozhodného práva a jurisdikce jako nepřímého důsledku skutečnosti, že Internet a jeho dosavadní služby fakticky vylučují fyzickou vazbu na většinu relevantních faktorů standardní mezilidské interakce. Tato základní podmínka efektivity práva je uvedena v historické souvislosti, tj. samotné skutečnosti, že Internet nikdy nebyl tvořen pro masové použití, nikdy také u jeho zrodu nebyly řešeny právní souvislosti jeho masového rozšíření. Autor v tomto ohledu dovozuje, že Internet byl již v okamžiku svého zrodu obdařen takovou vnitřní stavbou a koncepcí, že žádné státy či orgány nad ním nemohly získat úplnou kontrolu, důraz byl naopak kladen na nedůvěru k jakékoliv centralizované kontrole, což, jak bývá uváděno, bylo způsobeno vlnou idealismu z 60. let minulého století a souvisejícími hodnotami americké libertariánské ideologie. Tento koncept formoval vznik Arpanetu, předchůdce Internetu, jako decentralizované sítě, která se později stala základem struktury dnešního Internetu. Tento koncept ve svém důsledku vedl k vytvoření sítě, která kromě toho, že není postavena na centrální kontrole, postrádá jakýkoliv základní respekt k teritoriální působnosti práva, jež by umožňovala efektivní kontrolu na území jednotlivých států. Státy se tak začaly podílet na de facto globálním vynucování práva na Internetu, absence hranic vyplývající z povahy Internetu se najednou v mnoha aspektech nezdála tak výhodná a potřebnost efektivity práva se začala znovu výrazně legislativně prosazovat. Tento vývoj lze vnímat jako logický důsledek toho, že Internet přestal být vnímán jako něco zcela nedotknutelného, výjimečného a především fakticky nekontrolovatelného. Zájem států na zakotvení efektivity práva v prostředí Internetu se tak stal nejenom pochopitelný, ale zejména legitimní. Formování právních hranic tak začíná, byť pomalu, ale začíná.

Šestá část publikace (Význam a metody rozhodovací praxe) je orientována zejména na praktické aspekty rozhodování, ať již jde o správní či soudní rozhodování. Dominantním prvkem této kapitoly jsou především kritéria aplikace zásady proporcionality ve světle souvisejících trendů aplikační praxe. Důraz je kladen také na význam konstantní judikatury, zejména pak Ústavního soudu ČR, který mimo jiné mnohokrát prokázal, že netoleruje orgánům veřejné moci a především obecným soudům v řešení sporných případů příliš formalistický postup; zdůraznil přitom mj., že obecný soud není absolutně vázán doslovným zněním zákona, nýbrž se od něj smí a musí odchýlit, pokud to vyžaduje účel zákona, historie jeho vzniku, systematická souvislost nebo některý z principů, jež mají svůj základ v ústavně konformním právním řádu jako významovém celku a že povinnost soudů nalézat právo neznamená pouze vyhledávat přímé a výslovné pokyny v zákonném textu, ale též povinnost zjišťovat a formulovat, co je konkrétním právem i tam, kde jde o interpretaci abstraktních norem a ústavních zásad. Při takovéto interpretaci je nezbytné respektovat tezi, že v právním státě se nikdo svých práv dobrovolně a bezúčelně nevzdává; uvedené platí i pro otázky ochrany soukromí.

Podobně jako v jiných případech, i zde tedy platí, že jednotlivosti v právu mají význam až po jejich propojení s okolním světem. Budiž ambicí této práce pokusit se pojmenovat existující problémy a izolovat je natolik, aby bylo možné dohledat určitá obecná pravidla, u kterých by v zásadě nezáleželo na tom, jaké jsou jejich konkrétní skutkové okolnosti. Na právo

je tak možné nahlížet z celé řady hledisek, ať již z pohledu externího nezúčastněného pozorovatele či přímého účastníka konkrétního právního problému, případně jakkoliv jinak. Ve všech případech by však mělo jít o nazírání rozumné a pokud možno i praktické. Vždyť obvyklým východiskem k celé řadě odpovědí je především snaha o praktické uchopení problému. V tomto ohledu rovněž podobně platí, že věda a praxe nemohou žít jeden bez druhého, byť zdánlivě existují nezávisle na sobě a nezřídka musí slevovat ze svých ideálních představ o existenci podmínek pro vlastní existenci. Touto cestou se snaží kráčet i autor této publikace.

Existence Internetu bývá někdy přirovnávána k nástupu knihtisku. Není pochyb o tom, že z pohledu některých právních odvětví (např. autorského práva) může jít o pohled v mnohém více než přiléhavý. Tato paralela však nutně platit nemusí. Posouzení přiléhavosti takového srovnání je nutné posoudit až s odstupem, tím spíše, že ani takové hodnocení jedním právníkem by *per se* neobstálo před jakoukoliv solidní kritikou. Navzdory výše uvedenému je však třeba minimálně konstatovat, že mezi Internetem a knihtiskem zde existuje celá řada společných jmenovatelů, jež ignorovány být nemohou. Právě díky knihtisku se informace začaly šířit mnohem rychleji, efektivněji a především snadněji, kombinace těchto skutečností pak vedla k dosud nevídanému rozkvětu vzdělanosti a tvořivosti lidstva. S Internetem to může být podobné, těžko však v současnosti cokoliv v tomto ohledu kategoricky konstatovat, na to je příliš brzy. Uvedené se snaží autor respektovat i v této své práci. Posoudit výše pronesenou hypotézu o rozsahu míry významnosti zásahu existence prostředí Internetu ve smyslu zachování (přiměřeného, případně rozumného) očekávání ochrany soukromí do existujících právních vztahů a práva tak nemůže být zcela jednoznačné. Lze však konstatovat zřetelné narušení fungování standardních právních institutů, včetně souvisejících procesních záruk, ve smyslu jejich efektivity. Řada tradičních právních postulátů týkajících se soukromí je v mnoha ohledech nefunkční, případně je jejich funkčnost omezena. Zůstává tedy stále ještě otevřenou otázkou, zda je stát či mezinárodní komunita tím, kdo je schopen efektivně regulovat toto relativně neutrální[561] prostředí.

561 HAZLETT, W. T. *The fallacy of net neutrality.* New York: Encounter Books, 2011. ISBN 978-1-59403-592-0.

Resumé

Resumé

It is clear that, normatively, technological changes generate significant difficult-to-solve problems that may result in their reformulation of what have been recognised legal institutions for centuries. This is to a certain extent undoubtedly a phenomenon that will sooner or later occur with a whole range of other institutions, regardless of whether it happens for reasons of culture (in regard to conflicts), politics or the impact of advances in human knowledge. In this regard, however, it is certainly legitimate to infer that it is something that given its seriousness merits further investigation because of its present and future importance and significance for the very nature of law.

Even though this work attempts *inter alia* to offer an alternative to some existing solutions, including doctrinal and judicatory ones, its aim is not to inform the reader whether a solution is good or bad. That is up to the reader himself or herself to assess. This publication also has another aim and that is to offer a new or different point of view, including an analysis and outline of the chosen subject matter, the protection of privacy in the European Union. In this regard, the publication represents a partial contribution to jurisprudence for understanding a varied and extensive field, such as the range of new legal relationships resulting particularly in association with the Internet and its related services and protocols. The area this work deals with is often described as unpredictable, and significantly uncertain to entropic in terms of the law. In this regard, it is definitely a sure fact that there are certainly anarchic factors operating in the Internet environment that undermine the technical side of an otherwise well-organised system. These factors then act very entropically on the law wherein they considerably undermine existing confidence in this environment. The result is a close relationship between legal entropy and anarchy as an inseparable consequence of limited confidence in the law in this environment. It is necessary to state for the sake of completeness, however, that the Internet environment definitely cannot be considered to be completely anarchic whichever way one determines entropy of the law *per se* and on whose roots anarchy seemingly rests. That is to say, anarchy is determined primarily by the absence of any authority, or its failure, which necessarily leads to disorganisation and chaos, and the actual result of anarchy is hence lawlessness.

The Internet environment is undoubtedly not governed by lawlessness and the law is applied like everywhere else, nevertheless in some cases it has lost its effectiveness here (see below) through the natural action of its entropy. In this regard, the amount of anarchy in this environment is comparable in some of its features to the international relations environment where clear legal authority is also lacking in some areas where the international system wold organise, control and enforce the basic rules of compliance. The Internet, however, is not an authority-free environment and therefore one cannot speak about a completely anarchic environment. Authority in the Internet environment, however, operates on totally different principles, and its purpose lies primarily in ensuring technical operations and the efficient running of the network; if there is any legal regulation at all, it is more about the regulation of the technical parameters of communication between various authorities than about regulation in the sense of regulating the behaviour of network users.

Ultimately, the law responded to the phenomenon of the Internet with a certain amount of regulation; the opposite approach would only have had the result of deepening its existing entropy, and anarchy would essentially have become more deeply rooted. The legal regulation of the Internet is, however, highly limited wherein the Internet is understood only as a communication tool, or as the case may be, only as an environment with a specific form that can be considered normatively. In this respect, the judicial creation of rights, or as the case may be, the applicable legal-political approach of the persons applying the law (see above) plays a crucial role. The above normative construction, however, apart from the entropy referred to earlier, often suffers from its own internal imperfections that apply here more than elsewhere in that there is no conformity between reality i.e. what actually takes placed in the Internet environment, and normativity, i.e. how it should be (from our and the regulator's point of view). The reality of the Internet and its normative regulation therefore comprise two relatively independent categories. The legal problems relating to the Internet need to be assessed within the overall legal and technological context and not only through the lens of ingrained patterns or the lens of individual legal disciplines *per se*.

For the reasons mentioned above, this book deals primarily with putting into effect protection of privacy in the Internet environment, nothing more, nothing less. Even such a narrow topic, however, requires a comprehensive interdisciplinary scope, and in this respect it was necessary to "borrow" a lot from other legal disciplines and not always completely consistently with these disciplines, especially those fields that are far removed from the privacy law that the author of this publication has largely focused on until now. One can only trust that it was not at the expense of the quality of work, but rather the opposite. The author attempts in this book to reflect on the fact that every (and only legal) discipline is limited, but without saying anything about its accuracy. In this regard, the author tries to synergistically interconnect other fields rather than place them in opposition to each other, especially where an overlap occurs. The influence of interdisciplinary approaches is important in this respect for several reasons. Partly, these approaches effectively link jurisprudence to other social science fields, especially informatics, cybernetics, psychology, history, and potentially economics, etc. Also because of the fact that the intended scope of this publication is highly subject to this trend, which is greatly demonstrated both in the methodology and the systematisation of the actual publication.

The law is repeatedly confronted with the development of techniques and technological progress wherein the key factor should in particular be support for the development and protection of its positive aspects on the one hand, and the formation of effective barriers and regulation of the associated negative consequences on the other. Regulation in this sense should focus mainly on the preservation of minimum standards of the existing amount of legal protection in light of the potential consequences of the possible future applications of a specific technology in a new environment. The subject of legal regulation therefore is not only technology *per se*, but mainly its application under the conditions of existing legal standards and postulates. The purpose here is hence not to confront the associated technological transformations, but mainly to try to understand them and subsume them within the existing conditions of legal regulation. Only this way will lead to an understanding of what legal problems and new charac-

teristics are being created in connection with existing technology. The deliberations within this publication are therefore not made with the intention of confirming or denying the legal risk or danger posed by some specific technology (or services). On the contrary, the essence of these deliberations are an attempt at describing how the law responds to this technology.

The book itself is systematised into seven sections, including a final (concluding) section, and where the first section (the Internet and the law in ferment) is an introduction to some of the questions over the general issue of the present and future metamorphosis of the law where the main aim of this work is outlined at a general level, i.e. verifying the hypothesis that present technological changes impact upon the content of existing legal relationships to such a significant extent that they disrupt the very essence of the functioning of the law. Included in this section is some initial speculation and historical connotations, while reference is also made to the fundamental importance of equine law for Internet law where the author describes the historical connection, which is considered to be very significant in relation to the future of the law of cyberspace as a pedagogical discipline. In this respect, the author further describes the (historical) links between equine and automobile law to the field of Internet law. In this regard, particular emphasis is placed on the historical fact that in terms of the impact of new technology, the law as a normative system has only very limited possibilities of social regulation. The academic dispute of Judge Easterbrook and L. Lessig documents the fact that the impact of technology and the extent of its interaction on the external world cannot be easily predicted, and it is even harder to foresee how the law itself will respond to this technology.

The development of the automobile industry in the last century is also discussed in light of its legal regulation in which a whole range of mistakes were committed wherein the power of the market played a far greater role than legal regulation. The story of Internet law is comparable to the story of automobile law as a story of a celebrated technology that also produced surprises in many respects. The car changed the world, but our legal system basically proved to be powerless and incapable of predicting the huge changes that this technology brought about. On the other hand, automobile law is also encouraging by demonstrating the potential of the legal system in some regards to succeed and produce fair results in court proceedings. If we immerse ourselves in automobile law we find stories of official and legal reformers who did what they could to improve this technology in terms of safety, effectiveness, infrastructure and fairness, while at the same time they often faced very strong opposition. Not all the stories about automobile law are of success, but in the case of cars a lot of quality legal work was carried out for the sake of the public good, perhaps as may be the case with the law of the Internet. The path of Internet law is essentially mainly about on-going adaptation to changing laws and a constantly evolving future. It is more than clear that our "networked" society needs a very good Internet law and competent legal guidelines more than ever before. The users of this technology undoubtedly deserve such legislation that not only respects how this technology works, but effectively protects its users. Elaborating this area of the law plays a very important role in the education of judges, lawyers and companies, as well as the role that includes building bridges between legal doctrines and with evolving technology and methods. If in an ideal world we could simply look into the future, we could avoid some mistakes. Judge Easterbook did not

see the future that had already arrived. Maybe even we cannot see it clearly today. Our digital technology is not only complex, but is actually in a state of permanent evolution. The law is a dynamic system, but nevertheless is usually late in responding, but this delay is variable and the rate at which it responds may be directly proportionate to the rate at which we are able to look back into the past and be inspired.

The second section of the book (the axiology of privacy and its protection in the environment of an information society) deals with the assessment and actual importance of privacy as a fundamental evaluative postulate of this protection. The issue of overall legal and technological context is outlined, and it is primarily the interdisciplinary scope often located far beyond the parameters of the law that is referred to. The protection of privacy in this environment represents a type of appropriate judicial or other protection wherein the very concept of privacy is not easy to define. We generally cannot find its definition either in current Czech judicature or foreign judiciaries, international documents or significant jurisprudence text (doctrines) or practice. Only in exceptional cases is it possible to find some responses in the decisions of the European Court of Human Rights, which usually and generally links this concept to the physical and mental integrity of a person, including their sexual life, and therefore it is a concept *per se* that is very broad and flexible, as indeed is the case with many other legal concepts that are closely tied to other auxiliary jurisprudential branches (e.g. legal sociology, etc). This is similar to a range of other concepts (such as justice, dignity, sovereignty, security, etc), and nor in the case of the concept of privacy is such a definition even desirable; the old Roman rule of omnis definitio (in iure) periculosa es is applied here even more than elsewhere. Implicit definitions of these concepts can then be deduced by methods of legal argumentation. The current difficulty with defining the law of privacy then results mainly from its very essence, specifically from the factual circumstances of a particular case (typically in connection to "informational self-determination"). Privacy is enshrined in the norms of objective law (private and public), although at the same time it represents a significant subjective right of an individual who is therefore protected even against his or her own self. In this regard, this subjective right may clash with the state's commitment to protect and respect the freedom of the individual. In this respect, the author repeatedly discusses the finding of the Federal Administrative Court relating to the possibility of issuing a trade licence for the operation of a 'peep-show' where the court stated that this violation of human dignity (a person as an object and not a subject) cannot be obviated or remedied by the consent of the women concerned, as human dignity is an objective inalienable value. It is an interesting example of legal respect for the autonomy of a person's will in relation to his or her privacy. Problems with the application of the law of privacy then usually also result from the fact that the ban on the violation of privacy is usually somehow tied to a specific range, how a protected person is defined vis-à-vis the public and what the limit of his or her informational self-determination can be defined as being, which in turn objectively reduces the rights of the non-availability of privacy (see for example the voluntary disclosure of intimate information on social networks).

In this respect, it is inferred that objective law cannot work with only philosophical and ethical categories and must transform them into legal language. In this regard, the Charter

of Fundamental Rights and Basic Freedoms (of the Czech Republic) in many ways embraces the issue of the law of privacy in a relatively complex manner. A general guarantee of the inviolability of privacy is enshrined in Article 7(1) as lex generalis, on the basis of which a whole range of specific guarantees of individual aspects connected to the privacy of an individual then runs through the Charter. It is sufficient to state the values safeguarded in Article 10(1) of the Charter (human dignity, personal honour, good reputation, name). All are associated with the privacy of the individual. The same applies to the protection of private and family life in the sense of Article 10(2) (the connection with international human rights conventions) and protection from the misuse of personal data. Another manifestation of privacy is the traditional concept of the inviolability of a dwelling pursuant to Article 12 of the Charter where privacy is defined spatially, just as the protection of stored and transported documents, records and reports according to Article 13 of the Charter. An immediate expression of the protection of privacy is then found in Article 15(1) (freedom of thought, conscience and religious confession or faith). A number of political rights and freedoms are also associated with the issue of the protection of privacy. These include in particular the aspect of negative freedom, i.e. the freedom of individuals to decide for themselves that they will not evince a certain opinion, will not accept information, will not communicate a position, etc. The language of human rights is thus a kind of gateway to a common world of argumentation. Any conflict between affected rights is not an abstract conflict between various neutral principles of clear import that is somehow preordained, either because it corresponds with a different value system of an objective character (e.g. morals), or because there is the possibility of objectively expressing their sequence. An attempt to resolve these disputes through argumentation aimed at finding a just solution that relies on objective meanings trivialises the seriousness of the conflict and its symbolic meaning for life.

The third section of this work (methodological starting points and the collision of the autonomy of self-will with the law of privacy) is dedicated to a description of the methods used in this work (analytical, logical, systematic, or as the case may be, comparative or synthetic), as well as to questions of conflict of values which can be objectively at variance with the law of privacy where it is necessary to bear in mind an especially constitutional or human rights dimension of the whole problem, particularly the part that relates to balancing all constitutionally guaranteed rights, i.e. rights at the same level. In this regard, it is inferred that each individual infringement of the law of the protection of privacy must be assessed individually with regard to all the circumstances of a given matter. It is necessary in this connection to state in particular that no law can *per se* be absolute and rule supreme over another law that has to be applied simultaneously in a given matter. We usually call such a state a collision where it is necessary as part of legal argumentation to consider primarily the existing purpose and sense of each individual infringement. Such infringement of the law of the protection of privacy may be freedom of speech, the right to information, or a different public interest or value. In applying a specific legal provision it is therefore necessary to bear in mind an especially constitutional or human rights dimension of the whole problem, particular the part that relates to balancing all constitutionally guaranteed rights, i.e. rights at the same level. The balancing of rights is relatively common business for the majority of constitutional courts as this consideration is

often applied at the general level as well. The Czech constitutional court has repeatedly expressed its own opinions on the issue of freedom of speech and the right to freely express one's opinions. The constitutional court has based its assessment of this issue mainly on the fact that this right and freedom is limited in content by other rights, wherein these rights may ensue as constitutionally guaranteed from the constitutional order of the Czech Republic or from other constraints provided by the law protecting societal interests and value. At the same time, the right to express one's opinions may divest constitutional protection not only of restrictions in terms of content, but also of the form through which the opinions are outwardly expressed and is closely associated with the constitutionally guaranteed right to which it is bound. If a published opinion deviates from the limits of a democratic society's generally acknowledged rules, it will lose the character of a fair judgement (report, commentary), and as such will generally find itself beyond the realms of constitutional protection. The constitutional court has further expressly ruled that "fundamental law according to Article 17 of the Charter is essentially equal to fundamental law according to Article 10 of the Charter", wherein "it is mainly a matter for general courts that each case be considered in view of the circumstances as to whether one law was not unreasonably given preference over another law". The fact that this law is not absolute can be demonstrated by the fact that in relation to publicly well-known or politically active persons, our constitutional court has formed the belief that the right of criticism, enshrined in Article 17(2) of the Charter and Article 10 of the Convention on the Protection of Human Rights and Basic Freedoms, which is an indivisible part of the freedom of speech and the right to information, must respect the balance between that law and the personal rights of a special subject and cannot exceed certain limits associated with the attributes of a democratic society. Such defined constraints in relation to a natural person who is or acts as a "public figure" are wider than in relation to a private person.

The fourth section (legal regulation of the protection of privacy, its limits and possibilities) then contains the actual core of the work where firstly a critical polemic is undertaken regarding the concept of the European system of protection of personal information and data (including Czech regulation), as well as analysis of the current model of personal data protection in the Internet environment where emphasis is placed in particular on the principles of this regulation and the associated rights and obligations within the context of their importance for Internet work. In this respect, the key issues of the application of current legal work carried out for operating within the Internet environment, such as the legal qualification of IP addresses, MAC address and ID data boxes like personal data, agent information system regimes, the problems of unsolicited commercial messages (spam) and social networks, are dealt with. This is necessary given the context of associated legal regimes of protection of privacy, such as civil (civil and labour) and criminal law aspects.

However this issue is oriented, especially for the applicable Czech legal regulation, including the many practical and theoretical aspects of the protection of personal information in the Internet environment, emphasis is also placed on the European context of this protection, including the analytical-critical view of the European system of protection of personal information. What is necessarily to be considered of key importance here is mainly the authority

of the European Union regarding the unifying of personal information protection in member states, and their basis is contained in the valid law of the European Union Article 16(2) of the Treaty on the Functioning of the European Union, which stipulates that the European Union accepts the rules on the protection of natural persons in the processing of personal information by member states. This provision therefore empowers the European Union to unify the legal regime of personal information protection in member states. The relevant powers, however, as is evident in the express wording of the stated provision, relate primarily to cases concerning the movement of personal information across the borders of member states, i.e. to a situation with a clear cross-border element. In the case of personal information protection inside member states, i.e. in situations without a cross-border element, the wording of Article 16(2) places emphasis on the fact that the European Union may through its own legal acts unify the protection of personal information in member states only "if member states perform activities that fall within the scope of the competency of European law". Apart from this, it is necessary to point out that in view of Article 4(1) of the aforementioned treaty, the power of the European Union regarding the protection of personal information resulting from Article 16 of the Treaty pertains to the scope of power shared with member states and therefore is clearly not an exclusive power that necessarily has an impact on the extent to which the European Union may carry out the unification of personal information protection rules (the performance of this power is hence guided by the principle of subsidiarity and proportionality). In this regard, EU law on the protection of personal information within the law of member states thus relates to those legal norms of member states that are accepted in connection to the law of the European Union in the area that falls within the competency of this law. EU law on the protection of personal information, however, will not have a fundamentally different field of authority in relation to the laws of member states even in the case where EU law on the protection of personal information will be regarded as a set of rules that execute the right to the protection of private life as a fundamental right guaranteed by European Union law, whether it is law inferred from the European Union's Charter of Fundamental Rights or from general principles that are binding for the Czech Republic and other member states. A critical look at the existing regulation of the European system of protection can then be inferred from the fact the relevant European directive laid out a broad fundamental scheme of principles for processing personal information and had a great effect on the law in other geographical areas. This system has thus achieved a number of successes. Despite these positives, however, problems still persist (see below) both in terms of material and programme law, and overall understanding in the sense of the sufficient communicativeness of the whole system. The nature of these problems should be reviewed in a number of areas.

The fifth section (international cooperation as the conditio sine qua non of the effectiveness of the law in the Internet environment) analyses and describes one of the fundamental legal problems of the Internet – the key issue of the applicable law and jurisdiction as an indirect consequence of the fact that the Internet and its existing services effectively eliminate physical ties to the majority of relevant factors of standards interpersonal interaction. This basic condition for the effectiveness of the law is placed in its historical context, i.e. the very fact that the

Internet was never created for mass use, and the legal circumstances of its widespread expansion were also never addressed at its inception. The author concludes in this regard that the Internet was at the moment of its creation endowed with such an internal structure and concept that no states or other bodies could obtain full control over it, and on the contrary emphasis was placed on distrust toward any centralised control, which it is argued was caused by the wave of idealism from the 1960s and the associated values of American libertarian ideology.

This concept shaped the emergence of Arpanet, the predecessor to the Internet, as a decentralised network that then became the basis for the structure of today's Internet. The result of this concept led to the creation of a network that apart from the fact that it is not based in central control, lacks any basic respect for the territorial effect of the law which would allow effective control over the land of individual states. States thus started to participate de facto in the global enforcement of Internet law, so the absence of borders resulting from the nature of the Internet suddenly did not seem in many of its aspects so convenient and they once again began to strongly promote the need for legal effectiveness by legislative means. This development can be seen as a logical result of the fact that the Internet stopped being perceived as something totally untouchable, exceptional and effectively uncontrollable. The interest of states in enshrining the effectiveness of the law in the Internet environment hence became not only understandable, but in particular legitimate. The formation of legal barriers is thus beginning, albeit slowly.

The sixth section (importance and methods of decision-making practice) is oriented especially toward the practical aspects of decision-making, be it administrative or judicial decision-making. The dominant element of this chapter is mainly the criteria of applying the principles of proportionality in light of the associated trends in application practice. Emphasis is also placed on the importance of constant judicature, especially of the Constitutional Court of the Czech Republic, which inter alia has demonstrated many times that it does not tolerate public authorities and general courts in resolving disputed cases in an overly formalistic fashion; it has also emphasised, inter alia, that a general court is not absolutely bound by the literal wording of a law, but it can and should digress from it when required by the purpose of the law, the history of its establishment, the systematic circumstances or any principles that have their own basis in the constitutionally conforming legal order as a meaningful whole, and that the obligation of the courts to delve into the law does not mean looking directly and expressly at the instructions in the legal text, but also the obligation to identify and articulate what is a specific right even where it concerns an interpretation of abstract rules and constitutional principles. With such an interpretation it is necessary to respect the proposition that within the rule of law no-one voluntarily and purposelessly gives up their rights, and this also applies to issues of protection of privacy.

As in other cases, it also applies here that the particulars of a law have relevance after their connection to the surrounding world. So, it is this book's ambition to try to identify existing problems and isolate them to make is possible to trace certain general rules on which it would not matter in principle what their specific actual circumstances are. It is thus possible to view a law from a whole range of perspectives, either from the point of view of a disinterested

external observer or a direct participant in a specific legal problem, or in any other way. In all cases, however, it should be a sensible, and if possible, practical observation. After all, the usual starting point for a number of responses is mainly an attempt to achieve a practical understanding of the problem, and in this regard it is also similarly valid that science and practice cannot survive without each other, even though they seemingly exist independent of each other and often have to compromise on their ideals about the conditions for their own existence. The author of this publication also tries to thread a path in this manner.

The Internet is often compared to the start-up of the printing press. There is no doubt that from the point of view of some legal branches (e.g. copyright law) this view may be more than apt in many ways. This parallel, however, may not necessarily apply. Assessing the aptness of such a comparison needs to be assessed from a distance, all the more so that even such an assessment by one lawyer would not *per se* hold up against any firm criticism. In spite of this, however, it is possible to say that there are a number of common dominators between the Internet and the printing press that cannot be ignored. It is thanks to the printing press that information started to spread much more quickly, more effectively and more easily, and a combination of these facts then led to an unprecedented blossoming of education and human creativity. It may be similar with the Internet, although it is difficult to say anything at present in this regard as it is too early to tell. The author tries to respect this fact in his work.

Zusammenfassung

Zusammenfassung

Es liegt auf der Hand, dass technologische Veränderungen normativ bedeutsame und schwierig zu lösende Rechtsprobleme aufwerfen, die eine Umformulierung der über Jahrhundert hinweg angewandten Rechtsinstitute erforderlich machen. Bis zu einem gewissen Grad handelt es sich aber um eine Erscheinung, die früher oder später bei einer ganzen Reihe anderer Rechtsinstitute auftritt, gleichgültig ob aus kulturellen (insbesondere dann, wenn es sich um Konflikte handelt) oder politischen Gründen oder wegen des Erkenntnisfortschritts der Menschheit. In dieser Hinsicht kann man aber sicherlich berechtigterweise ableiten, dass es sich um etwas handelt, das im Hinblick auf seine Bedeutung eine eingehendere Untersuchung verdient hat. Die Gründe hier liegen in der gegenwärtigen oder zukünftigen Wichtigkeit und Bedeutung für das Wesen des Rechts.

Obwohl diese Arbeit u.a. bemüht ist, Alternativen für einige der bisherigen Lösungen einschließlich derer auf der Ebene von Doktrin oder der Rechtsprechung anzubieten, beabsichtigt sie keine Beurteilung darüber, ob diese nun gut oder schlecht waren. Diese Beurteilung überlassen wir dem Leser. Diese Veröffentlichung verfolgt noch ein anderes Ziel, das im Angebot eines neuen oder anderen Blickwinkels besteht. Dazu gehört eine Analyse und eine Beschreibung der hier ausgewählten Materie, der Schutz der Privatsphäre in der europäischen Union. In dieser Hinsicht stellt diese Arbeit einen Teilbeitrag der Rechtswissenschaften zur Erkenntnis eines so vielfältigen und umfangreichen Gebiets wie dem Bereich der neuen Rechtsbeziehungen dar, die insbesondere in Zusammenhang mit der Existenz des Internets, der dort angebotenen Dienste und Protokolle entstehen Der Bereich, mit dem sich diese Arbeit beschäftigt, wird nicht selten als unübersichtlich, in rechtlicher Hinsicht unsicher bis entropisch eingestuft. In dieser Hinsicht kann man mit großer Sicherheit konstatieren, dass in der Internet-Welt tatsächlich anarchistisch wirkende Faktoren am Werke sind, die Störfaktoren in einem ansonsten gut organisierten System sind. Diese Faktoren wirken destabilisierend auf das Recht ein, indem sie auf bedeutende Weise das existierende Vertrauen in diese Umgebung belasten. Somit entsteht als integrale Folge mangelnden Vertrauens in das Recht in dieser Umgebung gibt es eine enge Beziehung von Anarchie und Entropie. Aus Gründen der Vollständigkeit sei angeführt, dass man die Welt des Internets sicherlich nicht als vollkommen anarchistisch bezeichnen kann, wie auch immer man Rechtsentropie *per se* versteht, zu deren Wurzeln eine scheinbare Anarchie sicherlich gehört. Unter Anarchie versteht man vor allem die Abwesenheit irgendwelcher Autoritäten, gegebenenfalls deren gemeinsames Versagen. Das führt notwendigerweise zur Nichtorganisiertheit und zum Chaos. Die eigentliche Folge von Anarchie ist daher die Herrschaftslosigkeit.

In der Welt des Internets herrscht ganz gewiss keine Herrschaftslosigkeit. Das Recht gilt wie sonst überall. In einigen Fällen verliert es nichtsdestoweniger seine Wirksamkeit (siehe unten). Es sind die natürlichen Auswirkungen der Entropie. In dieser Hinsicht ist der Anarchiegrad dieser Umwelt in einigen seiner Facetten mit der Welt der internationalen Beziehungen vergleichbar, in der ebenfalls auf einigen Gebieten eine klare Rechtsautorität fehlt, die das internationale System organisieren, darüber wachen und zur Einhaltung der elementaren Re-

geln zwingen könnte. Das Internet ist keine Umwelt ohne bestehende Autoritäten. Man kann daher nicht von einer vollkommen anarchistischen Welt sprechen. Autoritäten in der Welt des Internets folgen jedoch vollkommen anderen Prinzipien, deren Sinn vor allem in der technischen Funktionsfähigkeit und dem wirksamen Netzbetrieb zu sehen ist. Falls es hier überhaupt rechtliche Bestimmungen gibt, dann geht es vor allem um die Einhaltung technischer Parameter der gegenseitigen Kommunikation zwischen Autoritäten als um die Regelung im Sinne einer Verhaltensregelung der Netzbenutzer.

Schließlich reagierte das Recht auf das Phänomen Internet mit gewissen Regularien. Der umgekehrte Ansatz hätte im Ergebnis die existierende Entropie nur weiter vertieft und Anarchie wäre im wesentlichen tiefer verwurzelt gewesen. Rechtliche Regulierungen des Internets sind jedoch höchst beschränkt, wobei Internet nur als Kommunikationsinstrument aufgefasst wird, gegebenenfalls nur als existierende Umwelt mit einer bestimmten Gestalt, die es gilt, normativ zu berücksichtigen. In dieser Sicht spielt die richterliche Rechtsschöpfung (Vollendung), gegebenenfalls der verantwortliche rechtspolitische Ansatz von Personen, die das Recht anwenden, (siehe unten) eine große Rolle. Die oben angeführte Normenkonstruktion leidet nicht selten neben der angegebenen Entropie auch an seiner inneren Unvollkommenheit. Mehr als anderswo gilt hier, dass die Realität, also dem, was in der Umgebung des Internets tatsächlich realisiert ist, und die Normativität, also dem, was sein soll (Wille des Regulators und unserer), nicht übereinstimmen. Realität des Internets und dessen normative Regulierung sind daher zwei relativ unabhängige Kategorien. Rechtliche Probleme, die sich auf das Internet beziehen, müssen daher im gesamten rechtlichen und technologischen Kontext bewertet werden, niemals nur die Optik angeeigneter Formeln oder die Optik eines Rechtsfaches *per se*.

Wegen es oben Angeführten beschäftigt sich dieses Buch primär mit der Realisierung des Schutzes der Privatsphäre in der Umwelt des Internets, nichts mehr und nicht weniger. Auch das somit eingeengte Thema erfordert zwingend einen ganzheitlichen interdisziplinären Ansatz. Hierzu war es notwendig, sich aus anderen Rechtsfachgebieten „auszuleihen". Das Ausgeliehene ist aber nicht immer vollständig konsistent, vor allem wenn es aus Fachgebieten stammt, die weit jenseits der Grenze des Privatrechts liegen, mit dem sich der Autor dieser Veröffentlichung bisher überwiegend beschäftigte. Bleibt zu hoffen, dass das nicht auf Kosten der Qualität der Arbeit erfolgte, sondern im Gegenteil. Im Buch bemühte sich der Autor mit der Tatsache auseinanderzusetzen, dass jedes (nicht nur rechtliche) Fach seine eigenen Grenzen hat, ohne dass das etwas über seine Richtigkeit aussagt. Der Autor ist daher bemüht, sich an andere Fächer eher synergetisch anzulehnen als sie gegenseitig auszuspielen. Das gilt insbesondere dort, wo diese sich überschneiden. Der Einfluss des interdisziplinären Ansatzes ist in dieser Hinsicht aus mehreren Gründen bedeutsam. Zum einen verbindet dieser Ansatz in effektiver Weise die Rechtswissenschaften mit anderen Fachgebieten, insbesondere Informatik, Kybernetik, Psychologie, Geschichte, manchmal mit der Ökonomik usw. Außerdem deshalb, weil die in dieser Veröffentlichung beabsichtigte Vorgehensweise diesem bedeutenden Trend unterliegt, was sowohl in den Methoden wie in der Systematisierung der eigentlichen Publikation zum Ausdruck kommt.

Das Recht wird wiederholt mit der technischen Weiterentwicklung und dem technologischen Fortschritt konfrontiert. Zentraler Punkt ist hier insbesondere die Unterstützung der Weiterentwicklung und der Schutz deren positiver Seiten auf der einen Seite und die Schaffung wirksamer Hindernisse und die Regulierung der damit zusammenhängen negativen Auswirkungen auf der anderen Seite. Derartige Überlegungen müssen insbesondere in Richtung der Aufrechterhaltung von Minimalstandards im bestehenden rechtlichen Schutz im Lichte möglicher faktischer Auswirkungen künftiger Anwendungen einer konkreten Technologie in neuem Umfeld angestellt werden. Gegenstand der rechtlichen Überlegungen ist nun nicht nur die Technologie *per se*, sondern vor allem ihre Anwendung unter den Bedingungen der bisherigen Rechtsstandards und -postulate. Der Sinn besteht nicht darin, den damit zusammenhängenden Veränderungen standzuhalten, sondern vor allem im Versuch, sie zu erfassen und in die bestehenden Bedingungen der rechtlichen Regulierung einzuordnen. Nur dieser Weg führt zur Erkenntnis der entstehenden rechtlichen Probleme und Erscheinungen bei gegebener Technologie. Solche Überlegungen wie sie in dieser Veröffentlichung angestellt werden, können die Existenz rechtlicher Risiken oder Gefahren einer konkreten Technologie (oder Dienstleistung) weder bestätigen noch ausschließen. Das Wesen der Überlegungen ist im Gegenteil vom Bemühen geleitet, zu beschreiben, wie das Recht auf diese Technologie reagiert.

Das Buch ist in sieben Teile einschließlich des Schlusskapitels aufgeteilt, wobei der erste Teil (Internet und Recht in Bewegung) als Hinführung zu verschiedenen Fragen in Verbindung mit der allgemeinen, aktuellen Problematik bzw. künftigen Rechtsmetamorphosen zu verstehen ist , Auf der allgemeinen Ebene ist das Hauptziel dieser Arbeit die Überprüfung der Hypothese, dass die gegenwärtigen technologischen Veränderungen in die bestehenden Rechtsbeziehungen in einem solch bedeutenden Maße eingreifen, dass es zu einer grundlegenden Störung der Funktionsfähigkeit des Rechtssystems kommt. In diesem Teil werden einige Detailüberlegungen angestellt und historische Konnotationen angegeben. Erwähnt wird auch die grundlegende Bedeutung des Pferderechts (Easterbrook: law of the horse) für das Internet-Recht. Der Autor beschreibt historische Zusammenhänge, die er in Bezug auf die Zukunft des Rechts im Cyberraum als pädagogische Disziplin als sehr bedeutend ansieht. In dieser Hinsicht beschreibt der Autor weiter die (historischen) Verbindungen des Pferderechts und des Automobilrechts mit dem Internet-Recht. In dieser Hinsicht wird vor allem auf die historische Tatsache verwiesen, dass das Rechtssystem als normatives System nur sehr beschränkte Möglichkeiten für gesellschaftliche Regulierungsversuche dann bietet, wenn es um die Auswirkungen neuer Technologien geht. Der akademische Streit des Richters Easterbrook und L. Lessig dokumentiert, dass man Technologiefolgen und den Umfang ihrer Interaktion mit der real existierenden Welt nur schwer vorhersehen kann. Noch schwerer ist es vorher zu sagen, wie das eigentliche Rechtssystem auf diese Technologie reagieren wird.

Auch die Entwicklung der Automobilindustrie im letzten Jahrhundert wird im Lichte seiner rechtlichen Regulierungen diskutiert, als den rechtlichen Regulierungen eine ganze Reihe von Fehlern unterliefen, wobei aller die Marktkräfte eine sehr viel größere Rolle spielten als Rechtsvorschriften. Der Verlauf des Automobilrechts als Verlauf einer erfolgreichen Technologie voller Überraschungen dient als Vergleichsgröße für den Verlauf des Internet-Rechts. Mit

dem Auto wurde die Welt verändert. Es war aber gerade unser Rechtssystem, das sich als ohnmächtig erwies und die riesengroßen Veränderungen, die diese Technologie hervorrief, nicht in der Lage war zu prognostizieren. Auf der anderen Seite ist das Automobilrecht gleichermaßen anregend, da es ein Beweis für das Potential des Rechtssystems in mancher Hinsicht ist, erfolgreich zu sein und im Zuge von Gerichtsverfahren gerechte Ergebnisse zu erzielen. Wenn wir ins Automobilrecht tiefer eintauchen, finden wir Geschichten über Reformatoren von Ämtern und Recht, die trotz erheblicher Widerstände alles in ihren Kräften stehende taten, um diese Technologie im Hinblick auf Sicherheit, Effektivität, Infrastruktur und Gerechtigkeit zu verbessern. Nicht alle dieser Geschichten fanden ein gutes Ende. Im Falle des Autos aber wurde sehr viel qualitativ hochwertige Arbeit zur Verbesserung des Allgemeinwohls geleistet. Vielleicht kann das Internet-Recht ähnliches leisten. Der Pfad des Internet-Rechts besteht daher im wesentlichen in einer laufenden Anpassung der in Bewegung befindlichen Gesetze and die sich ändernde Zukunft. Es ist doch absolut klar, dass unsere „vernetzte" Gesellschaft mehr noch als in der Vergangenheit ein sehr gutes Internet-Recht und geeignete Führer durch dieses Recht braucht. Die Nutzer dieser Technologie haben unzweifelhaft Rechtsvorschriften verdient, die nicht nur die Funktionsfähigkeit dieser Technologie nicht aus dem Auge verlieren, sondern vor allem deren Nutzer wirksam schützen. Die Herausarbeitung dieses Rechtsbereichs spielt bei der Weiterbildung der Richter, der Rechtsanwälte und der Gesellschaft eine sehr große Rolle. So können Brücken zwischen Rechtsdoktrin und der komplexen Technologie- und Verfahrensentwicklungen gebaut werden. Wenn man es schaffen würde, einen Blick in die Zukunft zu werfen, könnte man wohl manchen Fehler vermeiden. Richter Easterbrook hatte die bereits angebrochene Zukunft nicht erkannt. Vielleicht ist sie auch heute noch nicht richtig zu erkennen. Unsere digitalen Technologien sind nicht nur komplex. Die meisten von ihnen aber befinden sich noch in einem permanenten Evolutionsstadium. Das Recht ist zwar ein dynamisches System. Gewöhnlich reagiert es aber immer mit Verzögerung. Dieser Verzug ist jedoch verzeihlich. Dessen Größe ist jedoch wohl direkt proportional zu unserer Fähigkeit, in die Vergangenheit zu spähen und sich von dort inspirieren zu lassen.

Der zweite Teil des Buches (Werte der Privatsphäre und deren Schutz im Umfeld der Informationsgesellschaft) befasst sich mit der Bewertung und der Bedeutung der Privatsphäre an sich als grundlegendes Bewertungspostulat dieses Schutzes. Der gesamte rechtliche und technologische Kontext wird umrissen. Diskutiert wird vor allem der interdisziplinäre Umgriff, der nicht selten die Grenzen des Rechts weit hinter sich lässt. Der Schutz der Privatsphäre ist von seinem Wesen her in dieser Umwelt ein angemessener gerichtlicher oder andere Schutz, wobei der Begriff der Privatsphäre nicht einfach definiert werden kann. Die Definition der Privatsphäre findet sich auch nicht in der aktuellen Rechtsprechung tschechischer oder ausländischer Gerichte, internationalen Dokumenten oder wichtigen rechtswissenschaftlichen Texten (Doktrin) oder deren Praxis. Nur ausnahmsweise kann man einige Antworten in den Entscheidungen des Europäischen Gerichtshofes für Menschenrechte finden. Dort wir der Begriff gewöhnlich sehr allgemein in Bezug auf die physische und psychische Integrität einschließlich der Sexualität einer Person verstanden. Es handelt sich also um einen Begriff, der *per se* sehr breit und flexibel ausgelegt wird. Im Übrigen verhält es sich ähnlich bei einer ganzen

Reihe anderer Rechtsbegriffe, die sehr eng an andere rechtswissenschaftliche Hilfsdisziplinen gebunden sind (wie z.B.. an die Rechtssoziologie u.ä.). Das gilt aber auch in ähnlicher Weise für eine Reihe weiterer Begriffe (z.B. Gerechtigkeit, Würde, Hoheit, Sicherheit, u.ä..). Im Falle des Begriffs Privatsphäre ist eine solche Definition aber auch gar nicht erwünscht, Mehr als anderswo gilt die alte Regel aus dem römischen Recht omnis definitio (in iure) periculosa es. Eine implizite Definition dieses Begriffs kann unter Verwendung der Methode der rechtlichen Argumentation ableiten. Die gegenwärtigen Schwierigkeiten mit der Abgrenzung des Rechts auf Privatsphäre ergeben sich vor allem aus deren Wesen, konkret aus den Tatumständen im konkreten Fall (typisch ist die Bindung an die sog. informationelle Selbstbestimmung). Die Privatsphäre ist in Normen objektiven Rechts verankert (privat und öffentlich). Gleichzeitig aber stellt es ein bedeutendes subjektives Recht des einzelnen dar, das auch gegen seinen Willen geschützt ist. An dieser Stelle kann die Verpflichtung des Staates zum Schutz dieses subjektiven Rechts mit der Verpflichtung, die Freiheit des einzelnen zu respektieren, in Konflikt geraten. An dieser Stelle wird immer wieder das Urteil des Bundesverwaltungsgerichts über die Möglichkeiten zur Erteilung einer Gewerbeerlaubnis für den Betrieb einer sog. Peep-show diskutiert. Das Gericht stellte fest, dass eine solche Verletzung der Würde des Menschen (Mensch als Objekt, nicht als Subjekt) auch nicht durch die Zustimmung der betroffenen Damen geheilt werden kann, da die Würde des Menschen ein objektiver, unveräußerlicher Wert ist. Das ist ein interessantes Beispiel für den Respekt des Rechts vor dem autonomen Willen des Menschen in Bezug auf seine Privatsphäre. Ein Problem bei der Anwendung des Rechts auf Privatsphäre entsteht gewöhnlich auch aus der Tatsache, dass das Verletzungsverbot der Privatsphäre gewöhnlich irgendwie an deren konkreten Umfang gebunden ist, wie sich die geschützte Person selbst gegenüber der Allgemeinheit abgrenzt und wie die Grenze ihrer informationellen Selbstbestimmung festgelegt ist. Im Ergebnis wird damit das Recht auf Unzugänglichkeit der Privatsphäre eingeschränkt (siehe z.B. die freiwillige Veröffentlichung intimer Informationen in sozialen Netzen).

In dieser Hinsicht wird angeführt, das objektives Recht nicht nur in philosophischen und ethischen Kategorien verharren darf, sondern diese in die Sprache des Rechts umsetzen muss. In dieser Hinsicht fasst das Grundgesetz (der Tschechischen Republik) die Frage nach dem Recht auf Privatsphäre in vielen Richtungen auf relativ komplexe Weise. Im Artikel 7 Abs. 1 ist die allgemeine Garantie auf Unverletzlichkeit der Privatsphäre als lex generalis verankert, aus dem aus der Urkunde im folgenden eine ganze Reihe von konkreten Garantien abgeleitet werden, die sich auf einzelne Aspekte des privaten Individuums beziehen. Hier genügt es die Werte anzuführen, die im Artikel 10 Abs. 1 des Grundgesetzes (menschliche Würde, persönliche Ehre, guter Ruf und Name) genannt sind. Alls sind mit der Privatsphäre des einzelnen verbunden. Das gleiche gilt auch für den Schutz des Privat- und Familienlebens im Sinne des Artikels 10 Abs. 2 (Verbindungsglied zu internationalen menschenrechtlichen Bestimmungen) und den Schutz vor dem Missbrauch persönlicher Angaben. Man kann das auch so formulieren, dass die Privatsphäre ein traditioneller Ausdruck der Unverletzlichkeit gemäß Artikel 12 des Grundgesetzes, wo die Privatsphäre räumlich abgegrenzt wird. In gleicher Weise gilt das für hinterlegte oder transportierte Schriftstücke, Aufzeichnungen und Benach-

richtigungen gemäß Artikel 13 des Grundgesetzes. Unmittelbarer Ausdruck des Schutzes der Privatsphäre ist dann auch der Artikel 15 Abs. 1 (Gedanken- Gewissens- und Religions- oder Glaubensfreiheit). Ein ganze Reihe politischer Rechte und Freiheiten ist gleichermaßen mit dem Schutz der Privatsphäre verbunden. Hierbei handelt es sich insbesondere um den Aspekt der negativen Freiheiten, also um die Entscheidungsfreiheit des einzelnen darüber, dass bestimmte Meinungen nicht weiter gegeben werden, Informationen nicht angenommen werden, Standpunkte nicht mitgeteilt werden, usw. Die Sprachregelungen der Menschenrechte sind daher auf ihre Art das Eingangstor in die gemeinsame Argumentationssphäre. Jegliche Art von Konflikten zwischen den angeführten Rechten sind keine abstrakten Konflikte zwischen verschiedenen neutralen Prinzipien mit einem jeweils klaren Gehalt, der irgendwie deswegen vorgegeben zu sein scheint, weil es mit einem anderen Wertesystem objektiven Charakters (z.B. Moral) korrespondiert oder weil die Möglichkeit der Rangfolgebestimmung zwischen den Prinzipien besteht. Argumentative Bemühungen zur Lösung solcher Konflikte zielen auf das Erreichen einer einzigen richtigen Lösung ab, die sich auf objektive Prinzipien stützt die Schwere des Konfliktes und seine symbolische Bedeutung für das Leben trivialisiert.

Der dritte Teil der Arbeit (Methodischer Ausgangspunkt und die Kollision der Autonomie vůle mit dem Recht auf Privatsphäre) ist der Beschreibung der in dieser Arbeit verwendeten Methoden (analytische, logische, systematische, gegebenenfalls komparative oder wettbewerbsbezogene) sowie auch Fragen von Wertekonflikten gewidmet, die objektiv im Widerspruch mit dem Recht auf Privatsphäre stehen können. An dieser Stelle darf man insbesondere verfassungsrechtliche, gegebenenfalls menschenrechtliche Dimensionen des gesamten Problems nicht aus den Augen verlieren, insbesondere nicht den Teil, der alle verfassungsmäßig garantierten Rechte, also die Rechte auf der gleichen Ebene, gegeneinander abwägt. In dieser Hinsicht wird angeführt, dass jeder einzelne Eingriff in den Schutz der Privatsphäre getrennt unter Berücksichtigung aller Umstände im gegebenen Fall bewertet werden muss. In diesem Zusammenhang ist es besonders notwendig darauf hinzuweisen, dass kein Recht *per se* verabsolutiert werden kann und über ein anderes Recht gestellt werden, das bei den hier diskutierten Themen ebenfalls anzuwenden ist. Eine solche Situation bezeichnen wir für gewöhnlich als Rechtskollision, bei der im Rahmen einer rechtlichen Argumentationsweise vor allem der bestehende Sinn und Zweck jedes einzelnen Eingriffs angeführt werden muss. Einen solchen Eingriff in das Recht auf Privatsphäre könnte die Freiheit der Meinungsäußerung, das Recht auf Information, gegebenenfalls andere öffentliche Interessen oder Werte begründen Bei der Anwendung konkreter Rechtsbestimmungen sind dann verfassungsrechtliche, gegebenenfalls menschenrechtliche Dimensionen des Problems zu berücksichtigen, insbesondere nicht den Teil, der alle verfassungsmäßig garantierten Rechte, also die Rechte auf der gleichen Ebene, gegeneinander abwägt. Rechtsabwägung steht verhältnismäßig oft auf dem Sitzungsplan von Verfassungsgerichten Aber auch bei anderen Gerichten wird dieses Verfahren nicht selten verwandt. Das tschechische Verfassungsgericht hat sich wiederholt zur Frage der freien Meinungsäußerung geäußert. Bei der Bewertung dieser Problematik ging das Verfassungsgericht vor allem davon aus, dass dieses und diese Freiheit in seinem Gehalt von anderen Rechten begrenzt wird, wobei diese Rechte aus der republikanischen Rechtsverfassung verfassungsmä-

ßig garantiert sein können oder dieser Schutz aus anderen Gesetzesgrundlagen hervorgeht, die gesamtgesellschaftliche Interessen oder Werte schützen. Das Recht auf Meinungsäußerung kann seinen Schutz nicht nur dem Inhalt nach verlieren, da auch die Art und Weise, wie die Meinungen nach außen gebracht werden, eng mit dem verfassungsmäßig geschützten Recht verbunden ist, an das sie anknüpft. Falls die veröffentlichte Meinung von den Regeln der Höflichkeit ab, die in der demokratischen Gesellschaft gelten, verliert den Charakter eines konkreten Urteils (Nachricht, Kommentar). Als solche gerät sie in der Regel außerhalb des Schutzbereiches der Verfassung. Das Verfassungsgericht hat darüber hinaus ausdrücklich geurteilt, dass das "Grundrecht gemäß Artikel. 17 des Grundgesetzes ist grundsätzlich Grundlage des Rechts gemäß Artikel 10 des Grundgesetzes", wobei "es vor allem eine Angelegenheit der allgemeinen Gerichtsbarkeit ist, unter Heranziehung der konkreten Umstände des jeweiligen Falles abzuwägen, ob einem Recht in unbegründeter Weise Vorrang gegenüber einem anderen Recht eingeräumt wurde". Die Tatsache, dass es sich nicht um ein absolutes Recht handelt, kann man mit der Tatsache belegen, dass in der Beziehung zu öffentlich bekannten Personen oder aktiven Politikern unser Verfassungsgericht von der Überzeugung ausgeht, dass das Recht auf Kritik, das im Artikel 17 Abs. 2 des Grundgesetzes und dem Artikel 10 des Abkommens über Menschenrechte und Grundfreiheiten, das integraler Bestandteil der Meinungsfreiheit und des Informationsrechts ist, das Gleichgewicht zwischen diesem Recht und den Persönlichkeitsrechten des konkreten Subjektes erhalten bleiben muss und die Grenze der Eigenschaften einer demokratischen Gesellschaften nicht überschreiten darf. Diese so gesteckten Grenzen in der Beziehung zu natürlichen Personen, die wie „öffentliche Personen" handeln oder auftreten sind weiter als in Bezug auf private Personen.

Der eigentliche Kern der Arbeit ist Gegenstand von Kapitel vier (Rechtsbestimmungen des Schutzes der Privatsphäre , ihre Grenzen und Möglichkeiten). Dort werden zunächst die Fragen einer europäischen Konzeption des Systems des Schutzes persönlicher Angaben und Daten (einschließlich der tschechischen Bestimmungen) einer kritischen Diskussion unterzogen. Außerdem wird das gegenwärtige Modell des Schutzes persönlicher Angaben in der Umgebung des Internets analysiert. Betont werden dabei insbesondere die Grundlagen dieser Vorschriften und die damit verbundenen Rechte und Pflichten im Kontext ihrer Bedeutung für die Praxis des Internets. In diesem Zusammenhang sind die Lösungen eine Schlüsselfrage der Anwendung der gegenwärtigen Rechtspraxis, die für das Handeln in der Umgebung des Internets maßgeblich sind. Beispiele sind die rechtliche Einstufung einer IP Adresse, einer MAC Adresse und einer ID Datenbox, persönlicher Angaben, von Agenteninformationssystemen, der Problematik unerwünschter Geschäftsmitteilungen (Spam) und sozialer Netze. Angeführt wird auch der notwendige Kontext damit zusammenhängender Rechtsbereiche beim Schutz der Privatsphäre wie beispielsweise zivilrechtliche (Bürgerliches Recht und Arbeitsrecht) und strafrechtliche Aspekte.

Wenn auch diese Problematik insbesondere auf die gültigen tschechischen Rechtsvorschriften einschließlich einer Reihe praktischer und theoretischer Aspekte des Schutzes persönlicher Angaben im Internet zugeschnitten behandelt wird, ist auch der europäische Kontext dieses Schutzes einschließlich einer analytisch-kritischen Betrachtungsweise des europäischen Systems

zum Schutz persönlicher Angaben einer der Schwerpunkte. Eine Schlüsselrolle spielt hier die Vollmacht der europäischen Union zur Vereinheitlichung des Schutzes persönlicher Angaben in den Mitgliedsstaaten, dessen Grundlage die gültige Fassung im Europäischen Recht die Nr. 16 Abs. 2 des Vertrages über die Funktionsfähigkeit der Europäischen Union ist, die besagt, dass die Europäische Union bei der Verarbeitung persönlicher Angaben mit den Mitgliedsstaaten die Regeln zum Schutz von Privatpersonen übernimmt. Diese Bestimmungen erlauben es der Europäischen Union daher, die Systeme zum Schutz persönlicher Angaben in den Mitgliedsstaaten zu vereinheitlichen. Wie aus der Langfassung der betreffenden Bestimmung hervorgeht, beziehen sich die betreffenden Vollmachten vor allem auf Fälle des grenzüberschreitenden Verkehrs persönlicher Angaben über Grenzen der Mitgliedsstaaten hinweg. Es handelt sich also um Situationen mit einem klaren grenzüberschreitenden Element. Was den Schutz persönlicher Angaben innerhalb von Mitgliedsstaaten betrifft, in Situationen also ohne dieses grenzüberschreitende Element, so betont die Fassung des Artikels. 16 Abs. 2, dass die Europäische Union im Zuge ihrer Rechtsaktionen den Schutz persönlicher Angaben nur dann vereinheitlichen kann, „falls Mitgliedsstaaten Funktionen ausüben, die in den Wirkungsbereich des Unionsrechts fallen." Darüber hinaus ist anzumerken, dass im Hinblick auf den Artikel. 4 Abs. 1 des oben genannten Vertrages die Vollmacht der Europäischen Union zum Schutz persönlicher Angaben, die sich aus dem Artikel 16 des Vertrages ableiten lässt, mit den Mitgliedsstaaten geteilt wird. Es geht daher eindeutig nicht um eine ausschließliche Vollmacht. Das hat zwangsläufig Auswirkungen auf das Ausmaß, in dem die Europäische Union die Regeln zum Schutz persönlicher Angaben vereinheitlichen kann (die Ausübung dieser Vollmacht wird also vom Subsidiaritäts- und vom Proportionalitätsprinzip geleitet). In dieser Hinsicht bezieht sich das Unionsrecht zum Schutz persönlicher Angaben im Länderrecht auf jene Rechtsnormen der Mitgliedsstaaten, die im Anschluss an das Unionsrecht auf Gebieten, die in den Anwendungsbereich dieses Rechts fallen, übernommen wurden. Das Unionsrecht zum Schutz persönlicher Angaben hat keine grundsätzlich anderen Wirkungen auf die Beziehung zum Mitgliedsländerrecht auch in jenen Fällen, in denen man das Unionsrecht über den Schutz persönlicher Angaben ähnlich beurteilt wie ein Regelpaket zur Durchführung des Rechts auf den Schutz des Privatlebens als ein vom Recht der Europäischen Union garantierten Grundrecht. Dies gilt ungeachtet davon, ob das Recht im Grundgesetz geregelt wird oder aus allgemeinen Grundsätzen abgeleitet wird, die für die Tschechische Republik und andere Mitgliedsstaaten verpflichtend sind Ein kritischer Blick auf die bisherigen Bestimmungen des europäischen Schutzsystems lässt es als Tatsache erscheinen, dass mit den betreffenden europäischen Richtlinien eine breite Basis an Grundsätzen zur Verarbeitung persönlicher Angaben geschaffen wurde und großer Einfluss auf die Gesetzgebung in den übrigen Gebieten ausgeübt wurde. Dieses System kann auf eine ganze Reihe von Erfolgen zurückblicken. Trotzdem jedoch bleiben dessen Probleme sowohl im materiellen als auch im programmatischen Sinne erhalten (siehe unten), aber auch im Bewusstsein im Sinne einer ausreichenden Publizität des gesamten Systems. Das Wesen dieser Probleme sollte in einer ganzen Reihe von Bereichen revidiert werden.

Der fünfte Teil der Arbeit (Internationale Zusammenarbeit als conditio sine qua non der Rechtswirksamkeit im Internet) analysiert und beschreibt eines der grundlegenden Prob-

leme im Internet – die Kernfrage des entscheidenden Rechts und der entscheidenden Rechtsprechung als indirektes Ergebnis der Tatsache, dass das Internet und seine bisherigen Dienste die physische Bindung an den Großteil der relevanten Faktoren, die im zwischenmenschlichen Leben Standard sind, faktisch ausschließen. Diese Grundbedingung für die Rechtswirksamkeit hat eine historische Dimension. Es handelt sich um die Tatsache, dass das Internet nie zum Massengebrauch bestimmt war. An seiner Wiege gab es keine Lösungen rechtlicher Fragen in Zusammenhang mit der massenhaften Verbreitung. Der Autor führt in dieser Hinsicht an, dass das Internet bereits im Zeitpunkt seiner Geburt mit einer solchen inneren Konstruktion und Konzeption ausgestattet war, dass kein Staat oder Organ es vollkommen in den Griff bekommen konnte, Betont wird im Gegenteil das Misstrauen in jegliche Art zentralisierter Kontrolle. Wie bereits ausgeführt ist das auf eine Welle des Idealismus in den 60er Jahren des letzten Jahrhunderts und den damit zusammenhängenden Werten der amerikanischen liberalen Theorie zurück zu führen ist. Dieses Konzept führte zum Entstehen des Arpanets, dem Vorläufer des Internets, als dezentralisiertem Netz und Grundlage für die Strukturen des heutigen Internets. Dieses Konzept führte im Ergebnis zur Herausbildung eines Netzes, das sich nicht nur nicht auf eine zentrale Kontrolle verlässt, sondern auch jeglichen Respekt vor einer territorialen Anwendbarkeit von Recht vermissen lässt, die eine wirksame Kontrolle auf dem Gebiet eines einzelnen Staates ermöglichen würde. Staaten begannen sich daher an einer de facto globalen Aufdrängung von Recht auf das Internet zu beteiligen. Das Fehlen von Grenzen ergab sich aus dem Wesen des Internets, das plötzlich in vielerlei Hinsicht nicht mehr so attraktiv schien. Die Notwendigkeit eines effektiven Rechts begann erneut wieder sich in der Gesetzgebung durchzusetzen. Diese Entwicklung mag man als logisches Ergebnis der Tatsache werten, dass das Internet aufhörte, als etwas vollkommen Unberührbares, Außergewöhnliches und faktisch Unkontrollierbares betrachtet zu werden, Das Interesse von Staaten im Umfeld des Internets Rechtswirksamkeit zu verankern, wurde nicht nur verständlich, vor allem aber legitim. Die Herausbildung rechtlicher Grenzen beginnt, zwar langsam, aber immerhin.

Der sechste Teil der Veröffentlichung (Bedeutung und Methoden in der Entscheidungspraxis) beschäftigt sich vor allem mit praktischen Aspekten der Entscheidungsfindung, seien es nun Verwaltungs- oder Gerichtsentscheidungen. Die hervorragenden Elemente dieses Kapitels sind vor allem Anwendungskriterien für den Proportionalitätsgrundsatz im Lichte der damit zusammenhängenden Trends in der Anwendungspraxis. Besondere Berücksichtigung findet die Bedeutung der konstanten Rechtsprechung, insbesondere des Verfassungsgerichts der Tschechischen Republik, das u.a. oft bewies, dass es öffentlichen Organen und hier insbesondere den gemeinen Gerichten bei der Lösung von Streitfällen einen zu formalistischen Ansatz nicht durchgehen lässt. Es betonte u.a., dass Gerichte nicht absolut an die wörtliche Fassung der Gesetzesbestimmung gebunden ist, sondern davon abweichen dürfen und müssen, falls das der Gesetzeszweck, die Geschichte seiner Entstehung, ein systematischer Zusammenhang oder Prinzipien erforderlich machen, die ihren Ursprung in einer verfassungskonformen Rechtsordnung als Bedeutungsganzem haben. Die gerichtliche Pflicht zur Rechtsfindung bedeutet nicht nur die Suche nach direkten und wörtlichen Anweisungen im Gesetzestext, sondern in gleicher Weise auch die Pflicht konkretes Recht festzustellen und zu formulieren und

zwar auch dann, wenn es um eine Interpretation abstrakter Normen und Verfassungsgrundsätze geht. Bei einer solchen Interpretation muss berücksichtigt werden, dass in einem Rechtsstaat der freiwillige und zweckfreie Verzicht auf diese Rechte nicht möglich. Das gilt auch für den Schutz der Privatsphäre.

Ähnlich wie in anderen Fällen gilt auch hier, dass die rechtlichen Einzelheiten bis zur Anbindung an die reale Umwelt gelten. Der Anspruch dieser Arbeit besteht also darin, Probleme zu benennen und sie soweit zu trennen, dass es möglich wird, bestimmte allgemeine Regeln herauszufinden, die im Grundsatz unabhängig von den konkreten Tatumständen gelten. Es ist also möglich, das Recht unter einer ganzen Reihe von verschiedenen Blickwinkeln zu betrachten, sei es nun vom Standpunkt eines externen, nicht teilnehmenden Beobachter aus oder als direkter Teilnehmer eines konkreten Rechtsproblems oder irgendwie anders. Jedenfalls sollte es sich um eine vernünftige Betrachtung handeln, möglichst auch um eine praktische. Gewöhnlich ist der Ausgangspunkt für eine ganze Reihe von Antworten jedoch vor allem die Bemühung um eine praktische Erfassung des Problems. Gleichermaßen gilt hier, dass Wissenschaft und Praxis nicht ohne den jeweils anderen existieren können, Zwar existieren beide unabhängig voneinander und nicht selten müssen sie Abstriche von ihren Idealvorstellungen über die Existenz von Bedingungen für die eigene Existenz machen. Diesem Pfad folgt auch der Autor dieser Veröffentlichung.

Die Existenz des Internets wird nicht selten mit dem Aufkommen des Buchdrucks verglichen. Unzweifelhaft mag es sich aus dem Blickwinkel einiger Rechtsbereiche (z.B. Autorenrecht) um eine mehr als passende Ansicht handeln. Diese Parallele ist aber keineswegs notwendigerweise gültig. Die Bewertung der Angemessenheit eines solchen Vergleichs muss aus der Distanz erfolgen, da sonst eine solche Bewertung durch einen Juristen *per se* vor keiner soliden Kritik Bestand haben würde. Trotz der eben gemachten Ausführungen kann man feststellen, dass Internet und Buchdruck eine ganze Reihe gemeinsamer Nenner besteht, die nicht ignoriert werden dürfen. Gerade dank des Buchdrucks begannen Informationen sich schneller, effektiver und vor allem leichter zu verbreiten. Die Kombination dieser Tatsachen führte zu einer bis dahin ungekannten Blüte bei der Bildung und Schaffenskraft der Menschheit. Mit dem Internet kann das so ähnlich sein. Gegenwärtig kann man aber in dieser Hinsicht nur schwer etwas Kategorisches feststellen. Dafür ist es zu früh. Der Autor ist bemüht, das in seiner Arbeit zu respektieren.

Seznam použitých pramenů a dalších zdrojů

Seznam použitých pramenů a dalších zdrojů

ANDREE, Kamil. Několik poznámek k článku M. Kindla "K novátorským důsledkům zákona o ochraně osobních údajů". *Právní rozhledy : Časopis pro všechna právní odvětví.* 2001, roč. 9, č. 4, s. 172.
Anotace: Replika na článek v č. 2/2001. Advokát při výkonu advokacie osobní údaje soustavně a systematicky nezpracovává, pouze je eviduje a proto nelze dovodit, že by se na něho vztahovala působnost ZoOÚ a k užívání osobních údajů protistrany nepotřebuje její souhlas.

AGHA, Petr. *Herkulovo dilema.* Právník č. 2, 2013 s. 1104-1121.
Anotace: Autor se v článku zabývá teoriemi Dworkina a Alexyho a zkoumá, jak fungují v heterogenním prostředí států Rady Evropy, zejména zda a nakolik mohou být užitečné Evropskému soudu pro lidská práva při jeho rozhodování ve věcech tzv. kvalifikovaných práv (články 8-11 Úmluvy). Autor prosazuje otevřenější způsob rozhodování Soudu a poukazuje na význam doktríny volné úvahy při naplňování cílů Evropské úmluvy o ochraně lidských práv a základních svobod a pro udržení lidských práv coby důležitého a mocného nástroje při budování skutečného demokratického veřejného prostoru.

BAIER, Jaroslav, KRAMOLIŠ, Ondřej. Mezinárodněprávní aspekty zpracovávání osobních údajů a nesprávná transpozice směrnice v zákoně o ochraně osobních údajů. *Právní rozhledy : Časopis pro všechna právní odvětví.* 2012, roč. 20, č. 11, s. 385-390.
Anotace: Analýza a polemika s některými tezemi ve Stanovisku Pracovní skupiny 29. Připomenutí možných tíživých dopadů při promítnutí do českého právního řádu.

BARTA, Janusz, MARKIEWICZ, Ryszard. *Internet a prawo.* Kraków : Universitas, 1998.

BARTÍK, Václav . Oznamovací povinnost podle zákona o ochraně osobních údajů. *Právní rozhledy : Časopis pro všechna právní odvětví.* 2011, roč. 19, č. 12, s. 437-440.
Anotace: Výklad a komentář povinností správce a zpracovatele osobních údajů za situace, kdy se na správce nevztahuje žádná ze zákonem stanovených výjimek.

BARTÍK, Václav, JANEČKOVÁ, Eva. Bezpečnost osobních údajů podle zákona o ochraně osobních údajů. *Právní rozhledy : Časopis pro všechna právní odvětví.* 2010, roč. 18, č. 23, s. 839-844.
Anotace: Obsah a rozsah povinnosti zajistit bezpečnost osobních údajů. Povinnost správce nebo zpracovatele dokumentovat opatření přijatá ke splnění požadavku zajištění bezpečnosti osobních údajů. Přicházející možná rizika. Rozsah povinné mlčenlivosti.

BARTÍK, Václav – JANEČKOVÁ, Eva. Zveřejňování osobních údajů periodickým tiskem. *Právní rozhledy : Časopis pro všechna právní odvětví.* 2009, roč. 17, č. 2, s. 60-63.
Anotace: Výsadní postavení tisku. Aplikace ZoOÚ.

BOHÁČEK, Martin. DĚDIČ, Jan. *Právo & software:* I. sborník přednášek o právní úpravě ochrany a nakládání se softwarem. Praha: Dilia, 1990. ISBN 80-900120-5-1.

BOHÁČEK, Martin a kol. *Právo průmyslového a jiného duševního vlastnictví.* 1. vyd. Praha: VŠE, 1994. 220 s. ISBN 80-7079-388-0

BOHÁČEK, Martin. LOEBL, Zbyněk. *Smluvní vztahy při tvorbě a šíření software. Mechanizace a automatizace administrativy.* 1992. č. 9, s. 243-249

BOHÁČEK, Martin. *Ochrana dat v českém právu.* Praha: Kriminalistický ústav Policie ČR, 1993.

BERTRAND, André. PIETTE-COUDOL, Thierry. *Internet et le droit.* Paris: Presses Universitaires de France,1999.

BINGHAM, Tony, CONNER, Marcia. *The new social learning : a guide to transforming organizations through social media.* foreword by Daniel H. Pink, Alexandria : ASTD Press. an Francisco : Berrett-Koehler Publishers, 2010.

BOEHME-NEßLER, Volker. Internetrecht.com: Strukturen, Zusammenhänge, Regelungen. München : Deutscher Taschenbuch Verlag. 2001.

BRUNCLÍK, Zdeněk. *Právo a internet* [rukopis]. Masarykova univerzita v Brně. Právnická fakulta. Katedra právní teorie. Brno, 2001.

BURELL, Robert, COLEMAN, Alison. *Copyright Exceptions: the digital impact.* Cambridge. Nw York, N.Y. : Cambridge University Press, 2009.

Collection of WIPO domain name panel decisions. The Hague: Kluwer Law International. 2004.

Commerce électronique et propriétés intellectuelles. Paris: Librairies techniques, 2001.

ČAPEK, Jan. Ochrana dat a její některé trestněprávní aspekty ve světle judikatury Evropského soudu pro lidská práva. *Trestní právo: Odborný časopis pro trestní právo a obory související.* 2012, roč. 16, č. 3, s. 22-32.
Anotace: Souhrnná studie nad řadou rozhodnutí Evropského soudu pro lidská práva k uvedené problematice.

ČEPLOVÁ, Veronika. Právo obviněného na ochranu osobních a jiných údajů versus práva osob dle § 65 odst. 1 TrŘ. *Trestněprávní revue.* 2011, roč. 10, č. 11, s. 313-315.
Anotace: Vysloven názor, zda osobní a další údaje obviněných a svědků by neměly být vedeny mimo oficiálně přístupnou součást spisu odděleně od tohoto spisu.

ČERMÁK, Jiří. *Internet a autorské právo.* Praha : Linde, 2001.

ČERNÝ, Jakub. Nekalé obchodní praktiky na internetu Právnická fakulta Masarykovy univerzity v Brnì. Katedra obchodního práva. Brno, 2001.

ČERNÝ, Michal. Osobní údaje a jejich ochrana v právním řádu ČR. *Zdravotnictví a právo: Právní a daňový průvodce pro zdravotnictví.* 2001, roč. 5, č. 11, s. 10-16.
Anotace: Vysvětlení základních pojmů ZoOÚ. Postup a nakládání s osobními údaji. Problematika zpracování údajů bez souhlasu subjektu údajů. Zvláštní pravidla režimu pro citlivé údaje. Povinnosti správců a zpracovatelů. Nároky subjektů osobních údajů. Úřad, jeho struktura, kompetence, kvalifikační předpoklady jeho pracovníků. Zvláštní podmínky pro oblast zdravotnictví.

ČERNÝ, Miroslav. Právní ochrana známek v prostředí Internetu [rukopis]. Právnická fakulta Masarykovy univerzity v Brně. Katedra občanského práva. Brno. 2002.

ČÍRTKOVÁ, Ludmila. Patologické užívání internetu. *Právo a rodina: Rodina. Manželství. Děti a mládež. Dědictví.* 2011, roč. 13, č. 8, s. 1-5.
Anotace: Definice a jevové podoby online závislostí. Možnost terapie internetových závislostí.

DEGEN, Thomas A., DEISTER, Jochen. *Computer- und Internetrecht: Vertragsgestaltung, E-Commerce und Datenschutz.* Stuttgart [u.a.] : Boorberg, 2009.

DIETMAR, Jahnel. *Datenschutzrecht und E-Government:* Jahrbuch 2009. Wien: Neuer Wissenschaftlicher Verlag, 2009.

DISMAN, Marek. Právní úprava domény ".eu". Praha: Linde. 2011.

DOBROVIČOVÁ, Gabriela. Vplyv medzinárodného a európskeho práva na právny poriadok Slovenskej republiky. *Zborník príspevkov.* 2007, Košice: Univerzita J.P.Šafárika.

DOLEŽAL, Marek. I*nternet a autorské právo* [rukopis].2004.

DOLEŽAL, T. Problematické aspekty vztahu lékaře a pacienta zejména s ohledem na institut tzv. informovaného souhlasu. Časopis zdravotnického práva a bioetiky. Rok 2011, roč. 1, č. 1, s. 25

DOSTÁL, Otto. Elektronická zdravotnická dokumentace - její sdílení versus právo vlastnické a ochrana osobních údajů. *Zdravotnictví a právo: Právní a daňový průvodce pro zdravotnictví, 2008,* roč. 12, č. 7-8, s. 14-18.
Anotace: Význam moderní informační technologie ve zdravotnictví. Vlastnictví zdravotnické dokumentace a jeho relevance. Kdo může ke zdravotnické dokumentaci přistupovat a kde.

Problém ověřování totožnosti. Přístup ke zdravotnické dokumentaci a nahlížení do ní. Zákon o péče o zdraví lidu jako nejdůležitější právní úprava pro přístup ke zdravotnické dokumentaci.

DOSTÁL, Otto. Elektronická zdravotnická dokumentace - základní podmínky a způsoby jejího vedení. *Zdravotnictví a právo: Právní a daňový průvodce pro zdravotnictví.* 2007, roč. 11, č. 10, s. 17-23.
Anotace: Zdravotnická dokumentace podle zákona č. 20/1966 Sb. Ochrana osobních údajů. Elektronický podpis. Možné sankce.

EDWARDS, Lilian, WAELDE, Charlotte. *Law and the internet.Oxford;* Portland, Oregon: Hart, 2009.

EFFMERT, Jiří. Bezpapírová kancelář patentového zástupce. *Průmyslové vlastnictví.* 2011, roč. 21, č. 5, s. 170-185.
Anotace: Hardwarové a softwarové vybavení kanceláře patentového zástupce. Elektronické kontakty s úřady, institucemi a klienty. Elektronický podpis. Elektronické datové schránky. Elektronické účetnictví.

FENYK, Jaroslav , PETRŮ, Hana. Poskytování zdravotnické dokumentace poškozeného orgánům činným v trestním řízení. *Zdravotnické fórum: Pravidelná příloha časopisu Právní fórum.* 2012, roč. 2, č. 6, s. 29-32.
Anotace: Právo respektuje ochranu osobních údajů pacientů a jejich svobodnou vůli rozhodnout komu a kdy tyto údaje poskytnout. Právní úprava je však nedokonalá a umožňuje poškozenému účelově se svým souhlasem manipulovat. Proto se uvažuje o změně právní úpravy.

FIALOVÁ, Eva. Krádež virtuálních předmětů v příkladech z nizozemské judikatury. *Revue pro právo a technologie: Odborný recenzovaný časopis pro technologické obory práva a právní vědy.* 2010, roč. 1, č. 1, s. 23-28.
Anotace: Judikatura nizozemských soudů na případu ukradeného amuletu a krádež virtuálních předmětů v on-line hře.

FIORIGLIO, Gianluigi. *Il diritto alla privacy: nuove frontiere nell'era di internet.* Bologna: Bononia University Press, 2008.

GANEA, Peter, HEATH, Christopher, SCHRICKER, Gerhard. *Urheberrecht: Gestern - Heute - Morgen: Festschrift für Adolf Dietz zum 65. Geburtstag: mélanges dédiés a Adolf Dietz: writings in honour of Adolf Dietz/*München: C.H. Beck, 2001.

Gołaczyński, Jacek ... [et al.] *IT law in Poland: an introduction to IP law, contract law and internet liability/*Andreas Wiebe (ed.); Vienna: Verlag Medien und Recht, 2009.

GNIDA, Aleš. Několik úvah k ochraně osobnosti ve zdravotnictví. *Zdravotnictví a právo*: *Právní a daňový průvodce pro zdravotnictví.* 2004, roč. 8, č. 4, s. 7-10.
Anotace: Řeší se právní problematika pitvy a odnímání orgánů z těla zemřelé osoby a ochrana osobních údajů při poskytování informací do Národních registrů. Trestněprávní exkurs.

HABANEC, Jan. *Právo a internet z pohledu českého právního řádu.* [rukopis] Právnická fakulta Masarykovy univerzity v Brně. Katedra právní teorie. Brno, 2001.

HARDY, I. Trotter. *Project looking forward: sketching the future of copyright in a networked world : final report.* [Washington] : U.S. Copyright Office, 1998.

HÁJÍČEK, David. C. Svoboda "v síti". *Revue pro právo a technologie*: Odborný recenzovaný časopis pro technologické obory práva a právní vědy. 2012, roč. 3, č. 5, s. 12-17.
Anotace: Počítačový útok, útoky proti soukromí. Současný stav ochrany soukromí v ČR a EU. Správně právní úprava. Prosazování ochrany soukromí v ČR a EU - prosazování správněprávní úpravy, prosazování trestněprávní úpravy.

HERCZEG, Jiří. Extremismus a hranice svobody projevu na internetu. *Acta Universitatis Carolinae: Iuridica.* 2008, roč. 54, č. 4 , s. 35-49.
Anotace: Pojem extremismus. Innstitucionální zajištění postihu extremismu na internetu. Mezinárodní spolupráce - Úmluva o počítačové kriminalitě. Svoboda projevu na internetu.

HOŠTIČKA, Petr, HRDINA, Pavel, MATES, Pavel. Ochrana osobních údajů v obchodním rejstříku. *Právní rádce: Měsíčník Hospodářských novin.* 2003, roč. 11, č. 8, s. 26 - 27.
Anotace: Vztah obchodního rejstříku a ZoOÚ. Osobní údaje v obchodním rejstříku. Některé cizí právní úpravy (SRN a Rakousko).

HRÁDEK, Jiří. Princip země původu ve směrnici o e-commerce. *Právník: Teoretický časopis pro otázky státu a práva.* 2005, roč. 144, č. 5, s. 495-517.
Anotace: Směrnice Evropského parlamentu a Rady o elektronickém obchodu je založena na principu země původu, který představuje jen jedno z možných řešení, jež se pro problematiku online služeb nabízejí. Autor článku se zaměřil na problematiku principu země původu, která je zvláště v něm. literatuře hojně kritizována a která může vzhledem k některým nejasnostem zapříčinit špatné provedení směrnice. Uvádí další možná řešení k odstranění diskrepance národních právních řádů, poukazuje na existenci principu země původu v primárním právu a v některých dřívějších sekundárních aktech ES a analyzuje princip země původu ve směrnici o e-commerce.

HULEŠ, Jan. K některým otázkám účetnictví, auditu a ochrany osobních údajů. *Právní rozhledy: Časopis pro všechna právní odvětví.* 2002, roč. 10, č. 10, s. 508-510.
Anotace: Stručný popis evropské a české právní úpravy.

HUSOVEC, Martin . Zodpovednosť poskytovatela za obsah diskusných príspevkov. *Revue pro právo a technologie: Odborný recenzovaný časopis pro technologické obory práva a právní vědy.* 2011, roč. 2, č. 3, s. 40-42.
Anotace: Rozhodnutí Vrchního soudu v Praze ze dne 2.3.2011 představuje první aplikaci institut vyloučení odpovědnosti poskytovatelů služeb v podmínkách České i Slovenské republiky. Spor vznikl mezi žalobcem - společností PROLUX Consulting Int. s.r.o. zabývající se realitní činností a žalovaným - provozovatelem internetového portálu o osobních financích měšec.cz.

JAMBOROVÁ, Kateřina. Jak je to s ochranou osobních údajů v Dohodě mezi vládou ČR a vládou USA o posilování spolupráce při prevenci a potírání závažné trestné činnosti. *Právní rozhledy: Časopis pro všechna právní odvětví.* 2009, roč. 17, č. 21, s. 780-782.
Anotace: Cíle dohody. Rozsah a obsah ochrany osobních údajů v dohodě.

JANEČKOVÁ, Eva. Banky a jejich omyly. *Právní rozhledy: Časopis pro všechna právní odvětví.* 2006, roč. 14, č. 5, s. 180-185.
Anotace: V bankovní činnosti musí být respektovány zákonné předpisy o ochraně osobních údajů. Tyto předpisy však mohou být v kolizi s předpisy o opatřeních proti legalizaci výnosů z trestné činnosti. Článek se snaží nalézt cestu k řešení.

JANEČKOVÁ, Eva. Činnost obce a ochrana osobních údajů. *Právní fórum: Český právnický měsíčník.* 2006, roč. 3, č. 10, s. 372-376.
Anotace: Autorka se ve svém článku zabývá střetem mezi právem na ochranu osobních údajů a zásadou transparentnosti veřejné správy a zaměřuje se na oblasti v tomto směru nejproblematičtější, tj. zveřejňování na úřední desce, zveřejňování osobních údajů při výkonu samosprávy a projednávání přestupků.

JANEČKOVÁ, Eva, BARTÍK, Václav. Provozování kamerového systému se záznamem ve zdravotnických zařízeních. *Zdravotnictví a právo*: *Právní a daňový průvodce pro zdravotnictví.*2008, roč. 12, č. 7-8, s. 20-26.
Anotace: Kamerový systém jako prostředek k zajištění bezpečnosti osob a ochrany majetku. Kamerový systém se záznamem - zpracování osobních údajů. Účel kamerového systému. Použitelnost záznamů. Právní postavení majitele a správce kamerového systému. Použitelnost ZoOÚ. Souhlas subjektu údajů. Instalace kamerových systémů se záznamem ve zdravotnických zařízeních. Umístění kamerového zařízení. Ochrana osobních údajů zaměstnanců, pacientů a doprovodu pacientů.

JAROLÍMKOVÁ, Andrea. Nové nařízení o ochraně osobních údajů - jaké změny přinese? *Právní rádce: Měsíčník vydavatelství Economia.* 2012, roč. XX, č. 7, s. 48-50.

JOANIDIS, Tomáš. *Výpočetní technika a právo* [rukopis] . Právnická fakulta Masarykovy univerzity v Brně. Katedra právní teorie. Brno,1998.

JURAJDOVÁ, Dana. Ochranné známky a doménová jména [rukopis]. Právnická fakulta Masarykovy univerzity v Brně, Katedra obchodního práva. 2001.

JURÁŇ, Petr. Internet a autorské právo [rukopis]. Právnická fakulta Masarykovy univerzity v Brně. Katedra občanského práva. 2003.

KERSTING, Norbert. BALDERSHEIM, Harald. *Electronic voting and democrac: a comparative analysis.* Hampshire; Palgrave Macmillan, New York, 2004.

KOHL, Uta. *Jurisdiction and the Internet: a study of regulatory competence over online activity.* Cambridge; New York: Cambridge University Press, 2007.

KOLMAN, Petr. Nové správní sankce týkající se ochrany osobních údajů. *Právní rádce: Měsíčník vydavatelství Economia.* 2005, roč. 13, č. 7, s. 41.
Anotace: Ochrana osobních údajů jako nezadatelné ústavní právo. Harmonizace sjednocení podmínek v ČR s evropským právem. Závadné jednání na úseku ochrany osobních údajů jako přestupek a jako jiný správní delikt.

KOLMAN, Petr. Správní sankce na úseku ochrany osobních údajů. *Právní rádce*: *Měsíčník vydavatelství Economia.* 2009, roč. XVII, č. 10, s. 39-44.
Anotace: Sankce na úseku ochrany osobních údajů. Přestupky. Jiné správní delikty.

KOTÁSEK, Josef. Užívání doménového jména steuerberater-suedniedersachsen.de přípustné. *Revue pro právo a technologie: Odborný recenzovaný časopis pro technologické obory práva a právní vědy.* 2010, roč. 1, č. 2, s. 26-27.
Anotace: Internetová doména steuerberater-suedniedersachsen.de kombinující druhové a regionální údaje není zakázanou reklamou ve smyslu § 57 odst. 1 a § 57a zákona o daňových poradcích. Spolkový soudní dvůr StbSt/R/2/10 ze dne 1. 9 .2010.

KRAUSOVÁ, Alžběta. Evropská reforma ochrany osobních údajů. *Revue pro právo a technologie: Odborný recenzovaný časopis pro technologické obory práva a právní vědy.* 2012, roč. 3, č. 5, s. 3-9.
Anotace: Návrh nového nařízení Evropské komise o obecné ochraně úsajů. Důvody reformy, nová práva subjektů údajů, katalog povinností správců, nový institut inspektora ochrany údajů a povinnosti členských států a organizační struktura v rámci EU.

KROEGER, Detlef, CLASEN, Ralf, WALLBRECHT, Dirk. *Internet für Juristen: Weltweiter Zugriff auf juristische Informationen.* Berlin : Luchterhand, 1996.

KROEGER, Detlef, HANKEN, Claas. *Casebook Internetrecht: Rechtsprechung zum Internetrecht.* Berlin; Springer, 2003.

KROEGER, Detlef, KUNER, Christopher. Internet für Juristen: Zugang, Recherche, Informationsquellen Internet für Juristen: Zugang, Recherche, Informationsquellen. München : Verlag C.H. Beck. 2001.

KYSELOVSKÁ, Tereza. Určení mezinárodní pravomoci (příslušnosti) soudů ve sporech týkajících se porušení osobnostních práv zvěřejněním informací na internetu. *Revue pro právo a technologie: Odborný recenzovaný časopis pro technologické obory práva a právní vědy.* 2011, roč. 2, č. 4, s. 25-27.
Anotace: 1.Osoba, která se pokládá za poškozenou údajným porušením osobnostních práv obsahem informací zveřejněných na internetových stránkách, může podat žalobu na náhradu celé nemajetkové újmy buď k soudům členského státu, v němž je vydavatel tohoto obsahu usazen, nebo k soudům členského státu, v němž se nachází centrum jejích zájmů. Tato osoba může také místo žaloby na náhradu celé nemajetkové újmy podat žalobu k soudům členského státu, na jehož území je nebo byl přístupný obsah informace zveřejněné na internetu. Tyto soudy jsou příslušné pouze k rozhodování o újmě způsobené na území členského státu sídla soudu, jemuž je žaloba podána. 2.Článek 3 směrnice o elektronickém obchodu musí být vykládán v tom smyslu, že neukládá provedení do vnitrostátního právního řádu ve formě zvláštního kolizního pravidla. Pokud se však jedná o koordinovanou oblast, musí členské státy zajisti, aby (s výhradou výjimek povolených v článku 3 odst. 4 směrnice) poskytovatel služby elektronického obchodu nebyl podřízen přísnějším požadavkům, než jsou ty, které stanoví hmotné právo použitelné v členském státě, v němž je tento poskytovatel usazen. SDEU (velký senát). Sp.zn. Spojené věci C-509/09 a C-161/10. 25.10.2011

LANG, Petr. *Právo a internet*. [rukopis] : (z pohledu českého právního řádu). Právnická fakulta Masarykovy univerzity v Brně. Katedra právní teorie, 2003.

LAWRENCE, Penelope. *Law on the Internet: a practical guide.* London: Sweet and Maxwell, 2000.

LESSIG, Lawrence. *Code and other laws of cyberspace.* New York: Basic Books, 1999.

LESSIG, Lawrence. *The future of ideas: the fate of the commons in a connected world.* New York: Vintage Books, 2002.

LIPTON, Jacqueline D.,ELGAR, Edward, *Internet domain names, trademarks and free speech.* Northampton. 2010

MAGGS, Peter B.,SOMA, John T., SPROWL, James A. *Internet and computer law: cases, comments, questions.* St. Paul : West Group, 2001.

MACH, Jan. K otázce, zda jsou zdravotní pojišťovny povinny zveřejňovat informace o úhradách, a k tzv. "zlomovému rozhodnutí Nejvyššího správního soudu". *Zdravotnictví a právo*:

Právní a daňový průvodce pro zdravotnictví, 2008, roč. 12, č. 5, s. 32-33.
Anotace: Replika na článek Ondřeje Dostála v časopise *Zdravotnictví a právo* č. 11/2007 o problematice rozhodnutí Nejvyššího správního soudu ze dne 16.5.2007.

MACH, Jan. Některé problémy medicínského práva v praxi. *Zdravotnictví a právo*: *Právní a daňový průvodce pro zdravotnictví.* 2008, roč. 12, č. 3-4, s. 23-27.
Anotace: Pojem péče lege artis a z ní plynoucí konsekvence. Obsah a význam informovaného souhlasu a nesouhlasu, právní důsledky. Trestněprávní dopady porušení ochrany osobních údajů. Význam příčinné souvislosti mezi hrubou chybou a jejím následkem. Právní ochrana zdravotnických pracovníků.

MAŠTALKA, Jiří. Návrh nového ObčZ z pohledu ochrany soukromí a osobních údajů. *Právní rozhledy: Časopis pro všechna právní odvětví.* 2010, roč. 18, č. 10, s. 369-372.
Anotace: Autor považuje některá ustanovení za problematická a s návrhem polemizuje. Zejména jde o výklad pojmu "důstojnost" a "soukromí".

MAŠTALKA, Jiří. Ochrana osobních údajů. *Právní rádce: Měsíčník Hospodářských novin.*2002, roč. 10, č. 1, s. 21.
Anotace: Podrobný výklad novely zákona č. 101/2000 Sb., o ochraně osobních údajů zákonem č. 177/2001 Sb. Uvedená novela zpřesňuje ustanovení základního zákona. Modifikuje dosavadní pravidla zpracování osobních údajů. Upravuje postavení Úřadu.

MAŠTALKA, Jiří. Zákon o ochraně osobních údajů a novátorské výklady. *Právní rozhledy: Časopis pro všechna právní odvětví.*
2001, roč. 9, č. 4, s. 172-173.
Anotace: I když není výslovně uvedeno, jde o repliku na článek v č. 2/2001. Autor se snaží vyvrátit tvrzení v citovaném článku uvedené.

MATEJKA, Ján. recenze: ČERMÁK, Jiří. Internet a autorské právo. *Právník: Teoretický časopis pro otázky státu a práva.* 2002, roč. 141, č. 12, s. 1365-1366.
Anotace: V recenzované knize autor upozorňuje, převážně cestou příkladů, na nejběžnější způsoby porušování autorských a souvisejících práv prostřednictvím Internetu.

MATEJKA, J. a L. VOSTRÁ. Harmonizace práva v České republice – volný pohyb služeb na příkladu práva autorského. J. SUCHOŽA a J. HUSÁR, ed. *Obchodné právo a jeho širšie kontexty.* Košice: Univerzita Pavla Josefa Šafárika v Košiciach, 2010, s. 10–31, ISBN 978-80-7097-838-2

MATES, Pavel. Bylo třeba novely? *Právní rozhledy: Časopis pro všechna právní odvětví.* 2001, roč. 9, č. 8, s. 378-380.
Anotace: Kritický pohled na novelizaci zákona č. 101/2000 Sb., o ochraně osobních údajů

MATES, Pavel. Ochrana osobních údajů v českém právním řádu. *Bulletin advokacie.* 2000, č. 9, s. 32-42.
Anotace: Článek je zaměřen na tuto problematiku v souvislosti s využíváním výpočetní techniky. Výklad zákona a z něho vyplývající povinnosti pro zpracovatele a správce dat.

MATES, Pavel. Soud nebo Úřad? *Obchodní právo: Časopis pro obchodně právní praxi.* 2001, roč. 10, č. 3, s. 21-22.
Anotace: Argumentace k názoru, že spory plynoucí z ustanovení § 21 odst. 2 a § 23 odst. 1 zákona č. 101/2000 Sb., o ochraně osobních údajů náleží i nadále do působnosti krajských soudů a nikoliv Úřadu.

MATES, Pavel. Sdílení údajů v bankovnictví a pojišťovnictví. *Obchodní právo: Časopis pro obchodně právní praxi.* 2000, roč. 9, č. 10, s. 2-5.
Anotace: Rozsah bankovního tajemství s tím, že oznámení o podezření, že byl spáchán trestný čin nebo přestupek, které bylo učiněno příslušnému orgánu nelze považovat za porušení bankovního tajemství. Vazba údajů z bankovnictví a pojišťovnictví na zák. č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů ve znění pozdějších předpisů.

MATES, Pavel, BARTÍK, Václav. Nová úprava ochrany osobních údajů. *Právní rádce*: Měsíčník Hospodářských novin. 2004, roč. 12, č. 9, s. 42 - 46.
Anotace: Nová právní ochrana osobních údajů podle zákona č. 439/2004 Sb. Konkrétní změny. Významná upřesnění a doplnění a další změny. Sankce.

MATES, Pavel. Právo na informace a ochrana osobních údajů. *Právní rádce: Měsíčník vydavatelství Economia.* 2011, roč. XIX, č. 2 , s. 27-34.
Anotace: Ústavní zakotvení práva na informace a práva na ochranu osobních údajů. Vztah mezi oběma právy. Právo na informace a právo na ochranu osobních údajů ve veřejné správě. Veřejně činné osoby. Jednání orgánů obcí a krajů. Údaje o politické minulosti soudců a státních zástupců.

MATULA, Stephen M., WAMUKOYA, Justus M. Web information management: a cross-disciplinary textbook. Oxford : Chandos. 2007.

MERKUN, Richard. *Právo a internet* [rukopis]. Právnická fakulta Masarykovy univerzity v Brně. Katedra právní teorie. Brno, 1999.

MORÁVEK, Jakub. BCR (Binding Corporate Rules). *Právo pro podnikání a zaměstnání: Odborný časopis pro obchodní a pracovní právo, sociální zabezpečení a personalistiku.* 2009, roč. XVIII, č. 9 (2009), s. 7-14.
Anotace: Binding Corporate Rules jako závazná podniková pravidla pro garanci ochrany osobních údajů. Ochrana osobních údajů při jejich předávání do třetích zemí. Úřad na ochranu osobních údajů jako garant předávání. Pozitiva a negativa BCR.

MORÁVEK, Jakub. Ochrana osobních údajů ve zdravotnictví. *Zdravotnické fórum: Pravidelná příloha časopisu Právní fórum*. 2012, roč. 2, č. 2, s. 2-6.
Anotace: Problematika ochrany osobních údajů ve zdravotnictví. Právní prostředí. Ochrana zdraví a zdravotní péče. Účel ochrany osobních údajů ve zdravotnictví.

MORÁVEK, Jakub. K poskytování údajů o zaměstnancích odměňovaných z veřejných prostředků v kontextu rozhodnutí NSS. *Právník: Teoretický časopis pro otázky státu a práva.* 2012, roč. 151, č. 7, s. 786-809.
Anotace: Článek je věnován rozsudku Nejvyššího správního soudu sp. zn. 5 As 57/2010 ve věci poskytování informací na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, o zaměstnancích odměňovaných z veřejných prostředků. Autor se snaží poukázat na všechny související aspekty a šíři celé věci, zejména upozornit na její mimoprávní rozměr, který je pravděpodobně vůbec nejdůležitější a který bohužel zapadl a nestal se předmětem širší veřejné diskuse.

NEDOROST, Libor – DRAŠTÍK – SOVÁK. Odvodní řízení: branný zákon. *Právní rádce*. 2001, roč. 9, č. 9, s. 13-16.

NEDOROST, Libor – SOVÁK, Zdeněk. Zpracování osobních údajů souvisejících se zajišťováním zdravotní péče. *Zdravotnictví a právo*: *Právní a daňový průvodce pro zdravotnictví*. 2002, roč. 6, č. 3, s. 17-19. Zpracování osobních údajů souvisejících se zajišťováním zdravotní péče
Anotace: Charakteristika zdravotnické dokumentace, kartotéky pacientů a dalších materiálů z hlediska zákona č. 101/2000 Sb., o ochraně osobních údajů a zákona č. 260/2001 Sb., kterým se mění zákon č. 20/1966 Sb., o péči o zdraví lidu. Rozsah a výčet osob oprávněných nahlížet do zdravotnické dokumentace.

NĚMEC, Jiří. Označení domény v českém právním řádu [rukopis]. Právnická fakulta Masarykovy univerzity v Brně. Katedra občanského práva. Brno. 2002.

NONNEMANN, František. Ochrana spotřebitele a ochrana osobních údajů. *Právní rozhledy: Časopis pro všechna právní odvětví.* 2010, roč. 8, č. 22, s. 807-810.
Anotace: Mezi instituty ochrany spotřebitele a ochrany osobních údajů existuje celá řada styčných bodů. Vznikají tak situace, ve kterých mohou být uplatněny oba a je třeba řešit, v jakém rozsahu a za jakých podmínek k tomu bude docházet.

NONNEMANN, František . Ochrana osobních údajů při poskytování informací o životním prostředí. *Právní rozhledy: Časopis pro všechna právní odvětví.* 2011, roč. 19, č. 5, s. 166-171.
Anotace: Ochrana osobních údajů kontra právo na informace o životním prostředí z hlediska postavení subjektu povinného informace poskytnout. Při žádosti o poskytnutí informací je třeba posuzovat, jaké informace a v jakém rozsahu mohou být poskytnuty.

NOVÁK, Daniel. Ochrana soukromí a osobních údajů v Chartě základních práv EU. *Časopis pro právní vědu a praxi.* 2007, roč. 15, č. 5 , s. 339-344.
Anotace: Systematika Charty. Objekt ochrany soukromí a osobních údajů. Nová práva v Chartě. Práva a pravomoci. Závaznost a otázka jednotného výkladu.

NOVÁK, Daniel. Střet ochrany osobních údajů a práv duševního vlastnictví v evropské judikatuře. *Bulletin advokacie.* 2011, č. 10, s. 40-46.
Anotace: Autor se zabývá vymahatelnosti osobních údajů uživatelů internetu podezřelých z porušování práv duševního vlastnictví v judikatuře EU. Směrnice o uchovávání údajů o elektronické komunikaci a jejich využití zástupci nositelů práv z duševního vlastnictví. Judikatura ESD. Odpojení uživatele od internetu - podmínka předchozí soudní rozhodnutí.

NOVÁKOVÁ, Jitka. *Právo a internet*: *kriminalita na internetu* [rukopis] Masarykova univerzita v Brně. Právnická fakulta. Katedra právní teorie. Brno, 2000.

NOVOTNÁ, Věra. Ochrana osobních údajů a obydlí při poskytování pomoci v hmotné nouzi, sociálních služeb a sociálně-právní ochrany dětí. *Právo a rodina: Rodina. Manželství. Děti a mládež. Dědictví.* 2009, roč. 11, č. 5, s. 16-19.
Anotace: Ochrana a zpracování osobních údajů, obydlí a mlčenlivosti při poskytování pomoci v hmotné nouzi. Ústavní ochrana soukromí, osobních údajů a obydlí. Poskytování sociálně-právní ochrany dětem.

NOVOTNÁ, Věra. Vedení spisové dokumentace při poskytování sociálních služeb a sociálně-právní ochrany dětí. *Právo a rodina: Rodina. Manželství. Děti a mládež. Dědictví.* 2009, roč. 11, č. 8, s. 4-10.
Anotace: Vedení spisové dokumentace a řízení při poskytování pomoci v hmotné nouzi, při poskytování sociálních služeb, při poskytování sociálně-právní ochrany dětem.

NUTILOVÁ, Helena. Limity ochrany osobních údajů v Dohodě mezi vládou ČR a vládou USA o posilování spolupráce při prevenci a potírání závažné trestné činnosti. *Právní rozhledy: Časopis pro všechna právní odvětví.* 2009, roč. 17, č. 12, s. 446-449.
Anotace: Diplomatická jednání předcházející uzavření Dohody. Problematické aspekty Dohody.

OTEVŘEL, Richard. Soumrak užitečného internetu. (Díl. I) [online]. *JINÉ PRÁVO.* (vid. 18. 10. 2010). Dostupné na http://jinepravo.blogspot.cz/2010/10/soumrak-uzitecneho-internetu-dil-i.html

OTEVŘEL, Richard. Soumrak užitečného internetu. (Díl. I) [online]. *JINÉ PRÁVO.* (vid. 18. 10. 2010). Dostupné na http://jinepravo.blogspot.cz/2010/10/soumrak-uzitecneho-internetu-dil-ii.htm

PAULIČKOVÁ, Alena. Ochrana osobných údajov. *Právo a podnikání: Odborný časopis pro obchodní a finanční právo.* 2003, roč. 12, č. 9, s. 15-20.
Anotace: Výklad slovenské právní úpravy, vycházející ze zákona č. 528/2002, o ochraně osobních údajů. Práce s osobními údaji. Režim zákona a jeho realizace v praxi. Příklady. Sankce za porušení zákona.

PEČINKA, Karel. Problematika ochrany osobních údajů v osobních spisech státních zástupců a ostatních zaměstnanců státního zastupitelství. S*tátní zastupitelství: Profesní časopis státních zástupců a státního zastupitelství ČR.* 2006, roč. 4, č. 9, s. 3-11.
Anotace: Problematika ochrany osobních údajů. Právní úprava obecně. Zákon o ochraně osobních údajů a personální spisy. V příloze Vzor možného opatření k problematice ochrany osobních údajů v

PHAIR, Nigel. *Cybercrime: the reality of the threat.Canberra:* E-Security Publishing, 2007.

PÍCHOVÁ, Irena. K ochraně osobních údajů v pracovněprávních vztazích. *Právo a zaměstnání: Odborný časopis pro pracovní právo, sociální zabezpečení a personalistiku.* 2001, roč. 7, č. 12, s. 2-7.
Anotace: Obecná právní úprava ochrany osobnosti. Obecný přehled o obsahu ZoOÚ. Ochrana osobních údajů v pracovněprávních vztazích s ohledem na obsah ZoOÚ. Výklad povinností správce údajů. Ochrana práv subjektů v pracovněprávních vztazích.

PLACHÝ, Otto. Ochrana práv na Internetu [rukopis]. 2005.

PODHRÁZKÝ, Milan. Povinnost mlčenlivosti advokáta a ochrana osobních údajů. *Právní fórum*: *Měsíčník věnovaný soukromému právu.* 2011, roč. 8, č. 5, s. 230-232.
Anotace: Povinnost zachovávat mlčenlivost advokáty nevylučuje z působnosti ZoOÚ. Podle rozsudku Nejvyššího správního soudu ze dne 25.3.2011, čj. 2 As 21/2011-166, www.nssoud.cz

PODRECKI, Pawel. Prawo Internetu. Warszawa: LexisNexix. 2004.

POLČÁK, Radim. Doménová jména na internetu - právní aspekty registrace [rukopis] Právnická fakulta Masarykovy univerzity v Brně. Katedra obchodního práva. Brno. 2002.

POLČÁK, Radim. *Právo na internetu spam a odpovědnost ISP.* Brno Computer Press, 2007.

POLČÁK, Radim. *Internet a proměny práva.* Praha: Auditorium, 2012.

POMAHAČ, Richard. Evropský soudní dvůr: K rozsahu působnosti směrnice o ochraně fyzických osob při zpracování osobních údajů. *Právní rozhledy: Časopis pro všechna právní odvětví.* 2004, roč. 12, č. 9, s. 367-368.
Anotace: Umístění osobních dat na vlastní internetovou stránku umožňuje volný pohyb těchto

údajů, který musí být regulován v souladu se Směrnicí. ESD - rozsudek ze dne 6.11.2003 ve věci C-101/00 - Bodil Lindqvist; předběžná otázka, kterou vznesl Göta bovrätt (Švédsko).

POMAHAČ, Richard. Evropský soudní dvůr: Ochrana důvěrnosti elektronických komunikací. *Právní rozhledy: Časopis pro všechna právní odvětví.* 2008, roč. 6, č. 8, s. 306-308.
Anotace: Evropská regulace ochrany údajů při elektronické komunikaci umožňuje pouze poskytování osobních provozních údajů příslušným státním orgánům, nikoli však jejich přímé poskytování nositelům autorských práv, kteří chtějí porušování svých práv řešit v civilním řízení. Povinnost státu chránit nositele autorských práv nejde tak daleko, že by jim musely být dány k dispozici neomezené prostředky k objasňování porušení těchto práv. ESD (velký senát) - rozsudek ze dne 29.1.2008 ve věci C-275/06 - Productores de Música de Espana (Promusicae) v. Telefónica de Espana; rozhodnutí o předběžné otázce, kterou vznesl Juzgado de lo Mercantil n. 5 de Madrid (Španělsko).

POMAHAČ, Richard . Evropský soudní dvůr: Zveřejňování informací o příjemcích podpor. *Právní rozhledy: Časopis pro všechna právní odvětví.* 2011, roč. 19, č. 3, s. 113-114.
Anotace: Princip transparence nemá automatickou přednost před právem na ochranu osobních údajů. Povinnost správních orgánů zveřejňovat všechna jména fyzických osob s uvedením konkrétních částek, které tyto osoby obdržely jako finanční podporu, je vzhledem k cíli průhlednosti hospodaření s veřejnými prostředky nepřiměřené. ESD (velký senát) - rozsudek ze dne 9.11.2010 ve spojených věcech C-92/09 a C-93/09 - Volker und Markus Schecke GbR, resp. Hartmut Eifert v. Spolková země Hesensko; rozhodnutí o předběžných otázkách, které vznesl Verwaltungsgericht Wiesbaden (Německo).

POSOLDA, Petr. Právo a regulace informačního toku na Internetu [rukopis].2004.

POSPÍŠIL, Martin. *Právo a internet (zahraniční zkušenosti): aspekty ochrany osobních údajů v SRN.* [rukopis]/Masarykova univerzita v Brně. Právnická fakulta. Katedra právní teorie. Brno, 2001.

PTAŠNIK, Adam. Obchodněprávní aspekty doménových jmen [rukopis]. Právnická fakulta Masarykovy univerzity v Brně. Katedra obchodního práva. 2003.

RABAN, Přemysl, MORAVCOVÁ a kol. .eu domain name = .eu doména. Praha: C.H. Beck, 2006
RAU, Marco. Der internationale Schutz von Domainnamen und Markenrechten im Internet Analyse unter Berücksichtigung deutschen Rechts. Frankfurt am Main : Peter Lang. 2010.

RÁMIŠ, Vladan. *Zákon o audiovizuálních mediálních službách na vyžádání: se souvisejícími dokumenty, formuláři, doporučenými postupy a metodickými výklady: komentář.* Praha : Linde, 2012.

ROWLAND, Diane, KOHL, Uta, CHARLESWORTH, Andrew. *Information technology Law.* London; New York: Routledge, 2012.

ŘÍHA, Jiří. Odpovědnost providerů se zaměřením na odpovědnost host-providera a access--providera. *Acta Universitatis Carolinae: Iuridica*. 2008, roč. 54, č. 4, s. 107-129.
Anotace: Odpovědnost providerů - poskytovatelů informačních služeb. Evropské předpisy. Úprava v Německu, Rakousku a České republice.

SAUNDERS, Kurt M. *Practical internet law for business.* Boston: Artech House, 2001.

SECKER, Jane. *Copyright and e-learning: a guide for practitioners.* London: Facet, 2010.

SEHNÁLEK, David. Internet a právo: některé právní aspekty doménových jmen [rukopis]. Právnická fakulta Masarykovy univerzity v Brně. Katedra právní teorie. 2003.

SCHONBERGER-MAYER, Viktor, GALLA, Franz, FALLENBOCK, Markus. *Das Recht der Domain Namen.* Wien: Manz: Onlaw, 2001.

SCHWEIGHOFER, MENZEL, KREUZBAUER. IT in Recht und Staat: aktuelle Fragen der Rechtsinformatik 2002. Wien: Verlag Österreich. 2002.

SIEBER, Ulrich, NOLDE, Malaika. *Sperrverfügungen im Internet: nationale Rechtsdurchsetzung im globalen Cyberspace?* Berlin: Duncker & Humblot; Freiburg i.Br.: Max-Planck-Institut, 2008.

SKULOVÁ, Soňa. Nová právní úprava ochrany osobních údajů a některé její souvislosti a problémy ve veřejné správě. *Časopis pro právní vědu a praxi.* 2001, roč. 9, č. 2, s. 129-139.
Anotace: Charakteristika nové právní úpravy ochrany osobních údajů. Rozsah působnosti zákona a jeho základní pojmy. Hlavní zásady ochrany osobních údajů. Kontrolní a sankční režim. Výklad některých specifik a problémy úpravy ochrany osobních údajů v oblasti veřejné správy.

SMEJKAL, Vladimír. Má pravdu Mates nebo Sokol? K ochraně osobních údajů v advokacii potřetí. *Bulletin advokacie.* 2001, č. 3, s. 33-39.
Anotace: Pozitivistický a přirozenoprávní výklad problematiky. Přirozený výklad právního režimu ochrany osobních údajů v advokacii. Doslovný výklad některých ustanovení zák. č. 101/2000 Sb. ve vztahu k advokacii. Návrhy na řešení vzniklé situace.

SMRČINA, Otomar – GOLDSTEIN, Jiří. Některé zvláštní právní instituty v oblasti sociálně ekonomických informací. *Právník: Teoretický časopis pro otázky státu a práva.* 1972, roč. 111, č. 8, s. 659-669.
Anotace: Oprávnění provádět, popřípadě schvalovat ststistická zjišťování. Zpravodajská povin-

nost. Ochrana individuálních údajů. Ohlašovací povinnost. Přidělování rodných čísel. Zásada oficiálnosti informací. Právo vstupu do objektu a místnosti. Ukládání sankcí.

Software contracts: as adopted and promulgated by the American Law Institute at Washington, D.C., May 19, 2009. American Law Institute St. Paul, MN : American Law Institute Publishers, 2010.

SOKOL, Tomáš. K ochraně osobních údajů. *Právní rádce: Měsíčník vydavatelství Economia.* 2008, roč. 16, č. 11, s. 58 - 60.
Anotace: Zveřejnění osobních dat dlužníků nájemného a ochrana osobních údajů. Smysl ZoOÚ. Zveřejnění dlužníka jako legální forma vymáhání dluhu.

SOKOL, Tomáš. Zákon o ochraně osobních údajů se na advokáta nevztahuje. *Bulletin advokacie.* 2000, s. 23-36.
Anotace: Zásadní článek argumentující, proč se uvedená právní norma na advokáta nevztahuje, který vedl k vydání stanoviska představenstva České advokátní komory se stejným závěrem. Text tohoto stanoviska bezprostředně na článek navazuje.

SOVOVÁ, Olga. Aktuální trendy v ochraně osobních údajů. *Zdravotnictví a právo*: *Právní a daňový průvodce pro zdravotnictví.* 2007, roč. 11, č. 9 , s. 9-12.
Anotace: Nakládání s osobními údaji a jejich ochrana.

SPARROW, Andrew. *The law of virtual worlds and Internet social networks.* Farnham; Burlington: Gower, 2010.

STAMPFEL, Gerald. *Data retention: the EU Directive 2006/24/EC from a technological perspective.* Wien; Verlag Medien und Recht, München : 2008.

STOKES, Simon. *Digital copyright: law and practice*/Oxford: Hart, 2009.

SVATOŠOVÁ, Helena. Databanky v bankách opět v ústavních mezích. *Právní fórum: Český právnický měsíčník.* 2004, roč. 1, č. 5, s. 193-196.
Anotace: Zákon č. 439/2004 Sb.. kterým se mění zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, konečně vyřešil po dva roky přetrvávající selhání zákonodárce, který bez ohledu na své mezinárodní a komunitární závazky vyšel vstříc agresivním požadavkům bankovního sektoru. Klienti v Česku působících bank nepožívali po celé dva roky ochrany, kterou zaručují a požadují evropské lidskoprávní instrumenty.

SVOBODA, Přemysl, VOLEŠÁK, Jan. Pracujete na zabezpečené síti, nebo vám hrozí krádež dat? *Bulletin advokacie.* 2006, roč., č. 4, s. 52 - 54.
Anotace: Zneužití internetu pro odcizení dat. Zabezpečení sítě správcem. Typy možných útoků

na počítačovou síť. Základy ochrany počítače nebo počítačové sítě. Běžná technická zabezpečení. Bezpečnostní minimum. Mimořádné techniky zabezpečení.

ŠALOMOUN, Michal. Ochrana osobních údajů jako právo na informace sui generis. *Právní rozhledy: Časopis pro všechna právní odvětví.* 2006, roč. 14, č. 11, s. 389-396.
Anotace: Výklad povinností správců osobních údajů, které jsou svým způsobem specifickou povinností informovat subjekt údajů o zpracování jeho osobních údajů. Správci tuto povinnost opomíjejí, třebaže jim hrozí sankce.

ŠIMEK, Jan. *Obchod na internetu a občanské právo* [rukopis] Brno, 2003.

Šouba, Milan. Internet - trestněprávní aspekty zneužití této sítě a metoda jejich vyšetřování [rukopis]. Masarykova univerzita v Brně. Právnická fakulta. Katedra trestního práva. Brno. 2000.

ŠTEFKO, M. *Pracovní právo v kontextu občanského práva.* Auditorium. 2012. ISBN: 978-80-87284-24-7. s. 312
Anotace: Publikace představuje komplexní pojednání o vztahu pracovního a občanského, analyzuje nejdůležitější teoretické aspekty a zohledňuje také významné historické a komparativní souvislosti. Zejména se však zaměřuje na praktické problémy, např. vlivu smrti zaměstnavatele na pokračování pracovněprávního vztahu, počítání lhůt, odstoupení od konkurenční doložky, dohody o pracích konaných mimo pracovní poměr, ochranu odborových funkcionářů a mnoho dalších.

ŠTEFKO, M. V*ysílání zaměstnanců do zahraničí.* C.H.Beck. 2009. ISBN: 978-80-7400-110-9. s. 250
Anotace: Cílem publikace je poskytnout zaměstnavateli, který vysílá či chce vyslat zaměstnance k výkonu práce z / nebo do České republiky, Německa, Polska, Rakouska a Slovenska, vysílanému zaměstnanci, jakož i odborné veřejnosti analytické informace o relevantních pracovněprávních nárocích garantovaných vyslanému zaměstnanci domovským a hostitelským státem.

ŠTĚDROŇ, Bohumír [et al.]. *Teorie a praxe strategického a manažerského řízení v ICT.* Davle: Kernberg; Praha: Alfa Nakladatelství, 2009.

ŠVAŇHAL, Roman. Ochrana osobních údajů a ochrana osobnosti. *Obchodní právo: Časopis pro obchodně právní praxi.* 2001, roč. 10, č. 1, s. 8-16.
Anotace: Působnost zákona č. 101/2000 Sb., o ochraně osobních údajů. Zpracování osobních údajů pro osobní potřebu a jejich nahodilé shromažďování. Výklad jednotlivých pojmů, uvedených v zákoně. Obsah a rozsah povinné mlčenlivosti. Kompetence Úřadu. Vztah k obecné občanskoprávní ochraně. Kompetence k řešení sporů.

ŠVIDROŇ, Ján. *Základy práva duševného vlastníctva.* Právnická fakulta Univerzity Mateja Bela v Banskej Bystrici, Právnická fakulta Trnavskej univerzity v Trnave. Bratislava: Juga, 2000.

TÁBOROVÁ, Alice. Veřejnoprávní ochrana informační společnosti a místní působnost práva. *Revue pro právo a technologie: Odborný recenzovaný časopis pro technologické obory práva a právní vědy.* 2010, roč. 1, č. 1, s. 29-60.
Anotace: Kyberkriminalita. Trestněprávní jurisdikce v kyberprostoru. Relevantní právo úprava. Charakteristika ISP. Odpovědnost ISP. Realizace pravomoci státních orgánů blokovat či odpojovat komunikační linky.

THEUNIßEN, Christa-Maria. *Rechtswidrige Inhalte im Internet: rechtliche und tatsächliche Konsequenzen des Angebots eines Internetzuganges für Bibliotheken.* Berlin: Arbeitsgemeinschaft für juristisches Bibliotheks- und Dokumentationswesen, 2001.

TOMÁŠEK, Michal. Interkriminalität und neue Herausforderungen der Informationsgesellschaft des 21. Jahrhunderts. *Právní fórum: Měsíčník věnovaný soukromému právu.* 2011, roč. 8, č. 1, s. 41.
Anotace: Internetová kriminalita má mnoho podob a může zasahovat celou řadu zájmů chráněných současným unijním právem. Publikace přispívá k celoevropské diskuzi odborníků v oblasti harmonizace skutkových podstat trestných činů v oblasti internetové kriminality.

TOMÁŠEK, Michal, SVOBODA Pavel, KROFT Michal, BERAN Karel, EMR David, FRÝZEK Libor, VÁŇA Radek, VÍT Martin. Právní a daňové aspekty e-obchodu. *Právník: Teoretický časopis pro otázky státu a práva.* 2002, roč. 141, č. 6, s. 701-702.
Anotace: Recenzovaná práce, která je napsaná velmi přehledně, vysvětluje řadu odborných pojmů a skutečností, které s elektronickým obchodem souvisejí.

TOMÁŠEK, Michal, FENYK, Jaroslav, GŘIVNA, Tomáš, HERZEG, Jiří, HOŘÁK, Jaromír, VLASTNÍK, Jiří, FOTT, Martin. Ochrana základních práv a a svobod v procesu europeizace trestního práva. *Acta Universitatis Carolinae: Iuridica*. 2006, č. 1, s. 5-148.
Anotace: Soubor statí uvedených autorů k problematice europeizace trestního práva.

UHEREK, Pavel. Povinná mlčenlivost zdravotnických pracovníků a ochrana osobních údajů v souvislosti s klinickým hodnocením léčiv a klinickým hodnocením zdravotnických prostředků. *Zdravotnictví a právo*: *Právní a daňový průvodce pro zdravotnictví.* 2007, roč. 11, č. 12, s. 3-6.
Anotace: Řeší se některé otázky spojené s povinnou mlčenlivostí ve specifickém prostředí klinického hodnocení léčiv a zdravotnických prostředků. Obsah a hodnocení stanoviska Úřadu.

Uplatňování doménových jmen v rámci podnikatelských aktivit: [sborník příspěvků ke konferenci] Vysoká škola veřejné správy a mezinárodních vztahů v Praze ve spolupráci s Úřadem průmyslového vlastnictví ; editor Ladislav Jakl. Praha: VŠVSMV, 2007.

VESELÝ, Aleš. *Právo a internet*. [rukopis] Právnická fakulta Masarykovy univerzity v Brně. Katedra právní teorie, 2002.

VRZAL, Aleš. *Právo a internet*. [rukopis] Masarykova univerzita v Brně. Právnická fakulta. Katedra právní teorie. Brno, 2000.

WEINGARTEN, Paul. Werbeformen im Internet. Wien: WUV-Universitätsverlag, 2001.
WILLOUGHBY, Tony; ABEL, Sally M.; BETTINGER Torsten. Domain name law and practice. Oxford University Press. 2005.
2005.

WIMMER, Maria A. Electronic government: 4th international conference, EGOV 2005, Copenhagen, Denmark, August 22-26, 2005 :proceedings,Berlin: Springer, 2005.

ZEZULKA, Denisa. *Internet a mezinárodní právo soukromé.* [školitel Monika Pauknerová] V Praze: Univerzita Karlova, 2012.

Rejstřík

Rejstřík

A

absolutní práva, 56
agendový identifikátor, 76
aktivní legitimace, 146
Alexy, 55
APEC, 74
aplikační praxe, 179, 184
argumentace, 27, 37, 51, 53, 55, 65, 84, 180, 192
Arpanet, 159, 195
Asia Pacific Economic Cooperation, viz APEC
automobilové právo, 29, 190
autonomie, 215
autonomie vůle, 20, 51, 52, 53, 193
autorské právo, 30, 196, 225
axiologie soukromí, 35, 47, 202, 214

B

Barlow, 161
Bezpečnostní informační služba, 135
bezpečnost osobních údajů, 76, 83
bezpečný přístav, 70
browsewrap, 41
Bundeskriminalamt, 132

C

cache, 111, 112
Cambell vs. Hartley, 155
celní orgány, 134
Cimrman, 20
clickwrap, 41
cloud, 46
cloud computing, 123
Cohen vs. Cowles Media Co., 116
common law, 60
contra legem, 100
cookies, 41
cookiewrap smlouvy, 41
Copland vs. Spojené království, 151

COPPA, 172
CPEA, 74
Creative Commons, 1, 114
Cross-Border Privacy Enforcement Arrangement, viz CPEA
cyberbullying, 140

Č

Český telekomunikační úřad, 78

D

databáze, 62, 81, 88, 100, 111
datamining, 93
Data Protection Authority, 171
data retention, 129, 130, 131, 132, 133, 135
datová úložiště, 83, 109, 162
Deklarace nezávislosti kyberprostoru, 161
Denning, 59
Dessine-moi un bateau, 159
dichotomie, 37
Digital Millennium Copyright Act, 173
digitální informace, 184
digitální svět, 183
digitální technologie, 29
dobrá pověst, 59
doktrína práv třetí strany, 181, 183, 184
dokumentace a ohlašování, 127
doručování písemností, 110
DPA, viz Data Protection Authority
Dubai International Financial Centre, 62
důkazní spolehlivost, 174
Dworkin, 55, 179
dynamika psaní na klávesnici, 89

E

Easterbrook, 27, 29, 191
Electronic Documents Act, 172
Electronic Frontier Foundation, 161
elektronická podoba, 45

elektronická úřední deska, 110, 112
elektronické komunikace, 12, 77, 78, 128, 129, 130, 133, 135
email, 43, 45
ESLP, viz Evropský soud pro lidská práva
EU, viz Evropská unie
Eurípidés, 51
Europe v. Facebook, 120
evidence obyvatel, 78, 82, 97, 108, 109
Evropa 2020, 125
Evropská unie, 59, 60, 61, 64, 71, 73, 78, 124, 130, 132, 194
Evropský soudní dvůr, 69, 234, 236
Evropský soud pro lidská práva, 35, 191, 223
externalita, 26

F

Facebook, 41, 42
Federální obchodní komise USA, 74
Filip, 36
filtrování obsahu, 172
Financial Times Ltd vs. Spojené království, 148
Franklin, 35
Fuller, 64
Fullerova definice práva, 65
Fullerův koncept vnitřní morálky, 67

G

Gartnerova křivka, 114
gate-keeping, 119
Gelman, 119
General Data Protection Regulation, 168
Generální inspekce bezpečnostních sborů, 77, 135
generální klauzule, 136, 138, 139, 143
geolokace, 173
George Mitchell (Chesterhall) Ltd vs. Finney Lock Seeds Ltd, 59
Georgia vs. Randolph, 182
Glasenapp a Kosiek v. Německo, 149
Google, 41

H

Haagská konference soukromého mezinárodního práva, 166
Halfordová v. Spojené království, 154
Hanford Sentinel, 117
hardware, 65, 161, 172
Harlan, 180
Hart, 64
Herceg, 38
Hewitt a Haman v. Spojené království, 155
Hilton v. Spojené království, 153
Holländer, 55
homeworking, 107
Hurtado v. Švýcarsko, 153
Huvig v. Francie, 149

C

Children's Online Privacy Protection Act, 171

I

ID datové schránky, 21, 194
ideální statky, 135, 137
IMEI, 93, 94, 95, 130, 156
IMSI, 93, 94, 95, 156
indexace, 111
indikátory normativních očekávání, 37
informační společnost, 27, 35, 38, 39, 40, 43, 191, 214
informatika, 26
inspektor ochrany údajů, 125
interdisciplinární přístup, 26
Internet, 27, 31, 183, 184, 187, 189, 190, 194, 195, 196, 224, 230, 234, 235, 248
Internet a právo, 20, 190, 213
internetové identifikátory, 44, 47
internetové právo, 27
internetový prostor, 160
invazivnost sledovacích opatření, 154
IP adresa, 21, 43, 44, 89, 90, 91, 93, 94, 95, 156
IPv4, 89, 94
Iuridicum Remedium, 131

J

judikatura, 75, 84, 103, 155, 184

K

Kant, 25
Katz, 180, 181, 182
K. H. a ostatní v. Slovensko, 150
Klass a ostatní v. Německo, 149
Knapp, 26, 27
knihtisk, 31
kolizní normy, 162, 163, 174, 175
komunikační technologie, 27
komunitární právo, 59, 73, 103
konflikt, 20, 37, 38, 193, 215
koňské právo, 27, 31
konstantní judikatura, 180
Kuner, 62, 64, 65, 66, 67, 68, 72, 165, 170
kybernetika, 26
kyberprostor, 27, 29, 31, 159, 160, 183, 190, 240
Kyllo vs. USA, 181

L

Lastowka, 29
legitimita očekávání, 182
Lessig, 27, 28, 161, 191
Lindqvist, 103
Listina, 37, 54, 55, 192, 193, 194
Listina základních práv a svobod, 61, 102
logy, 109
Lufttransportunternehmen GmbH & Co. KG vs. Eurocontrol, 164
LUPA.cz, 21

M

MAC adresa, 21, 89, 93, 94, 95, 194
Malone v. UK, 149
Mancusi vs. DeForte, 181
Marckx v. Belgie, 149
Matematicko-fyzikální fakulta UK, 20, 22
materiální satisfakce, 146
metadata, 118
metamorfózy práva, 20, 190, 213

Metodologická východiska, 20, 193, 216
metodologie, 55
metody, 21, 195, 216
Mezinárodní organizace pro normalizaci, 73
mezinárodní právo soukromé, 163
mezinárodní prvek, 165
mezinárodní úmluvy, 36
Mill, 36
Ministerstvo vnitra ČR, 76, 95
morálka, 37
Moreno vs. Hanford, 117
Mouisel v. Francie, 153
Myspace.com, 115

N

nařízení Brusel I, 164
nařízení Řím I, 164
nařízení Řím II, 164, 174
Národní bezpečnostní úřad, 20
Nejvyšší soud ČR, 174
Nejvyšší správní soud ČR, 83, 84, 87, 90, 101
Niemietz, 97, 150
normativita, 25

O

občanská čest a lidská důstojnost, 110, 138, 140
obsah telefonických hovorů, 46
ochrana osobních údajů, 180, 194, 223, 224, 227, 229, 231, 232, 233, 237, 240
ochrana osobnosti, 52, 54, 180
ochrana osobnosti fyzické osoby, 135, 136, 139
ochrana soukromí, 46, 181, 182, 183, 184, 195, 214
odposlech, 128, 153
odůvodnění rozhodnutí, 180
OECD, 166
oprávněnost zveřejnění, 99, 100, 101, 114, 141, 156
Organizaci spojených národů, 167
osobní údaj, 72, 73, 74, 75, 76, 77, 79, 80, 81, 82, 83, 91, 194

P

Payment Card Industry Data Security Standard, 156
viz norma PCI DSS
Peck v. Spojené království, 152
Peev v. Bulharsko, 152
Personal Information Protection, 172
PIPEDA, 172
Plinius, 59
pluralita, 55
pojem soukromí, 35, 36
Polčák, 28
Policie ČR, 28, 88, 90, 132, 134, 174, 224
poskytovatelé, 45, 47, 129
poskytovatel služeb, 183
postuláty, 20
právní argumentace, 35
právní jistota, 19
právní norma, 51
právní principy, 79
právní řád, 128, 163, 182
právo být zapomenut, 124, 126
právo jména, 37, 88, 91, 116, 136, 138, 141, 142
pravomoc, 67, 76, 165, 166, 167, 171, 172, 194, 230, 234, 240
právo na informace, 53, 180
právo na osobní čest, 55
právo na uveřejnění dodatečného sdělení, 144, 145
preater legem, 100
přiměřené očekávání, 60
princip fair play, 154
případ Lotus, 169
příposlech, 153
příslušnost, 63, 99, 137
projevy osobní povahy, 85, 110, 138, 142, 146, 147
proporcionalita, 55, 56, 179, 180, 194, 195,
viz zásada proporcionality
prostředky ochrany proti zásahům do práva na ochranu osobnosti, 146
Proudhon, 187
provozní a lokalizační údaje, 130, 132

R

Rakas vs. Illinois, 182
registr práv a povinností, 76
registry dlužníků, 122
regulace reklamy, 11, 42, 61, 75, 78, 103, 180
Římská úmluva o právu rozhodném pro smluvní závazkové vztahy, 163
router, 94

S

satisfakce, 146
Save Our State Amendment, 169
Scalia, 39
Scarlet Extended SA vs. Societe Beige des Auteurs, Compositeurs et Editeurs SCRL, 173
sdílená data, 181
sdílený obsah, 43
sekundární právo, 179
Sharia Amendment, 169
služby informační společnosti, 78, 129, 156, 173
směrnice 95/46/ES, 12, 66, 82, 86, 88, 91, 99, 101, 125, 167, 234
směrnice 2006/24/ES, 12
Smith vs. Maryland, 181
software, 28, 44, 65, 161, 224
soudcovská tvorba práva, 189
souhlas subjektů osobních údajů, 96
soukromí, 12, 19, 20, 25, 30, 35, 36, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 51, 52, 53, 55, 59, 60, 61, 73, 74, 79, 80, 85, 90, 92, 96, 97, 98, 99, 100, 101, 102, 103, 110, 115, 116, 117, 122, 124, 128, 130, 131, 133, 135, 136, 138, 141, 144, 148, 149, 150, 152, 153, 154, 155, 156, 179, 180, 181, 182, 183, 184, 187, 188, 190, 191, 192, 193, 195, 227, 231, 234
soukromý a rodinný život, 36
spekulace, 26, 31
Spojené státy americké proti Millerovi, 183
Spolkový správní soud, 36
Stálý mezinárodní soudní dvůr, 165
státní příslušnost, 162
Strahilevitz, 116
subsidiarita, 194
svědomí a náboženské vyznání, 37
svoboda myšlení, 37
svoboda projevu, 51
synallagmatický vztah, 80

Szuluk vs. Spojené království, 153

S
šifrování, 44, 123

T
technicko-organizační opatření, 81
Telemarketing Sales, 172
televizní přenos z jednání zastupitelstva, 113
test proporcionality, 55, 152
through-click, 40
trestní řízení, 90, 132, 134

U
účel zpracování, 63, 77, 81, 101, 104, 106, 130, 132
umístění serverů, 160
Úmluva č. 108, 12, 168
Úřad pro ochranu osobních údajů, 20, 76, 77, 78, 104, 109, 111, 122, 135
Úřad pro zahraniční styky a informace, 135
USA vs. Jacobsen, 183
ústavní konformita, 180
Ústavní soud, 55, 180
Ústav státu a práva AV ČR, v. v. i., 22
Uzun vs. Německo, 150

V
vázanost soudu doslovným zněním zákona, 180
veřejná IP adresa, 91
veřejná zasedání a zveřejňování údajů, 113
Vězeňská služba České republiky, 134
vigilantibus iura scripta sunt, 156
vnější forma zásilky, 45
Vogt vs. Německo, 149
Vojenská policie, 77, 134
Vojenské zpravodajství, 135
volba práva, 165, 166
Vondel vs. Nizozemsko, 150

Všeobecná deklarace lidských práv, 59
výklad právních předpisů, 180

W

Web 2.0, 39
webové stránky, 39, 40, 43
Webster, 38

Z

základní právo, 55
základní registr agend orgánů veřejné moci, 76
základní registr obyvatel, 76
základní registr právnických osob, 76
základní registr územní identifikace, 76
základní registry, 76, 97
zákonná licence, 95, 96, 99
zákonná omezení práv osobnostních, 147
zákon o elektronických komunikacích, 77, 78, 128, 129, 130, 132, 133, 141
zákon o mezinárodním právu soukromém a procesním, 163
zákon o provozování rozhlasového a televizního vysílání, 145
zákon o zdravotnických službách, 139
zásada bezpečného přístavu, 173
zásada bezpečnosti zpracování, 63, 81, 82
zásada důvěrnosti, 63, 81, 128
zásada finality, 62, 80
zásada informovaného souhlasu, 79, 95
zásada informování, 63
zásada kvality údajů, 62, 81
zásada legitimity, 62, 79
zásada oznamovací, 63
zásada personality, 169
zásada proporcionality, 62, 69, 80, 179
zásada teritoriality, 169
zásada zákazu zpracování některých kategorií údajů, 63
zásah, 146
zásah do soukromí, 53, 54, 55, 61, 100, 101, 102, 110, 128, 131, 135, 143, 146, 193
záznam zaměstnancových telefonických hovorů, 153
zdrojový identifikátor, 76
zveřejňování dlužníků, viz registry dlužníků

Z

život a zdraví, 138, 139, 153

Ján Matejka
INTERNET JAKO OBJEKT PRÁVA:
hledání rovnováhy autonomie a soukromí

Vydal CZ.NIC, z. s. p. o.
Americká 23, 120 00 Praha 2
Edice CZ.NIC
www.nic.cz

© 2013 Ján Matejka
v licenci Creative Commons Attribution-ShareAlike (3.0),
s podporou RVO:68378122.
ISBN: 978-80-904248-7-6 (CZ.NIC, z. s. p. o.)
Knihu je možné objednat na **knihy.nic.cz**

knihy.nic.cz

ISBN 978-80-904248-7-6

9 788090 424876 >

Kniha, kterou má čtenář v rukou, je orientována na otázky vztahu svobody a soukromí člověka v prostředí Internetu. Jde o témata z nichž lze jen obtížně jedno upřednostnit před druhým, když jsou v podstatě stejného významu a navzájem se doplňují. Kniha je psána pro všechny, kteří se chtějí (či musí) zabývat těmito mnohdy konfliktními otázkami, včetně složité a stále ještě nepříliš zažité právní regulace, která se bohužel velmi často míjí se skutečným chováním v tomto prostředí. Jde o publikaci v mnohém přínosnou, postavenou na vědeckých a praktických zkušenostech autora, kterou jako pohotový manuál ocení především specialisté na otázky ochrany dat v prostředí Internetu. Autor ve své práci totiž nejenom důkladně popisuje aktuální rozhodovací praxi, ale především nabízí možná řešení, to vše v oblasti, který je obecně považována za složitou a pro nespecializovaného právníka místy až příliš nepřehlednou, kniha rovněž obsahuje řadu dosud nepublikovaných poznatků, kterých by si měl být vědom každý, kdo uvažuje o správě či zpracovávání osobních údajů v prostředí Internetu.

O autorovi **Ján Matejka** (nar. 1976 v Praze) v současné době působí jako vedoucí oddělení soukromého práva a zástupce ředitele Ústavu státu a práva Akademie věd ČR, v. v. i., kde se věnuje zejména problematice nových technologií. Dále také pedagogicky působí na Matematicko-fyzikální fakultě Univerzity Karlovy, externě pak působí na Právnické fakultě Masarykovy univerzity v Brně a Právnické fakultě Univerzity Karlovy v Praze. Působí rovněž jako člen Rozkladové komise Úřadu pro ochranu osobních údajů (od r. 2004) a předseda Hodnotícího panelu Grantové agentury ČR pro právní vědy a politologii (od r. 2009). Dále je členem redakčních rad právnických a právně orientovaných časopisů, zejména časopisů Právník, Všehrd, Revue pro právo a technologie, DSM, ITpravo.cz, aj. Je rovněž členem České advokátní komory, České společnosti pro Spojené národy, Společnosti pro právo informačních technologií, Spolku českých právníků VŠEHRD a Českého klubu skeptiků SISYFOS. V roce 2009 mu byla předsedou Akademie věd udělena prémie Otto Wichterleho, jež je udělována mimořádně kvalitním a perspektivním vědeckým pracovníkům AV ČR, kteří přispívají vynikajícími výsledky k rozvoji vědeckého poznání. V minulosti působil na Právnické fakultě Západočeské univerzity. Byl rovněž členem Expertní komise pro elektronický obchod při Úřadu pro veřejné informační systémy a členem rozkladové komise Národního bezpečnostního úřadu. Pravidelně publikuje v časopisech Právník, Bulletin advokacie, Právní rozhledy a na Internetu. Spolu s Jiřím Čermákem je zakladatelem serveru ITpravo.cz. Je autorem více jak 100 odborných a popularizujících prací. Působí rovněž jako samostatný advokát.

O edici Edice CZ.NIC je jedním z osvětových projektů správce české domény nejvyšší úrovně. Cílem tohoto projektu je vydávat odborné, ale i populární publikace spojené s Internetem a jeho technologiemi. Kromě tištěných verzí vychází v této edici současně i elektronická podoba knih. Ty je možné najít na stránkách knihy.nic.cz