Univerzita Karlova v Praze
Právnická Fakulta
Ústav autorského práva, práv průmyslových a práva soutěžního

DIPLOMOVÁ PRÁCE

Právní otázky internetu v mezinárodním a vnitrostátním právu

Petr Miroš
5. ročník
Borová 65, 547 01 Náchod

Vedoucí diplomové práce: JUDr. Petra Žikovská

Praha 2010

„Prohlašuji, že jsem tuto diplomovou práci zpracoval samostatně a že jsem vyznačil prameny, z nichž jsem pro svou práci čerpal způsobem ve vědecké práci obvyklým.“

V Praze dne 16. listopadu 2010 Petr Miroš

Poděkování vedoucí této diplomové práce:
„Děkuji paní JUDr. Petře Žikovské, vedoucí této diplomové práce, za konzultace a důležité připomínky.“

OBSAH

Úvod

Ústředním tématem, kterého se tato práce z různých aspektů dotýká, je globální počítačová síť, která výrazným způsobem zejména v průběhu posledního desetiletí změnila chování naší společnosti. Název internet je však někdy považován za nedostatečně určitý, protože některé způsoby přenosu dat probíhají na bázi jiných technologií a protokolů. Internet je totiž odvozen od tzv. IP protokolu (internet protokol). Proto namísto názvu internet bývá někdy užíván termín informační a komunikační technologie.

První část práce se zabývá obecnými otázkami od pojmu, historie a struktury internetu, přes právní pojetí a uplatnění práv jednotlivých států na síť svojí podstatou nadnárodní. V počáteční fázi existence internetové sítě bylo mnoho zastánců a obhajovatelů nezávislé povahy internetu, který podle extrémních názorů existuje nezávisle na jednotlivých státech a právních systémech. První část také uvádí pohled do práva autorského jako jednu z oblastí, kterou internetová síť ovlivňuje nejvíce.

Jakým způsobem působí na stávající právní systémy a jak se daří uplatnit tradiční právní instituty v tzv. on-line prostředí, toho se týká zejména druhá část práce. Z různých aspektů je zaměřena tato část na ochranu soukromí, osobnosti a jejích projevů. Ochrana osobnosti a osobních údajů, problematika používání virtuálních sociálních sítí jsou některé z témat, které jsou zkoumány z pohledu právní regulace naší a zahraniční, zejména ve Velké Británii. Pozornost je věnována též tzv. antiteroristické legislativě zejména ve Velké Británii, které dávají mnoha orgánům poměrně velké pravomoci například v souvislosti s odposlouchávání a monitorováním dálkové komunikace. Co v ČR může dovolit pouze soud, to na britských ostrovech dovoluje například poštovní orgán. Zvláštní pozornost je věnována pak právu autorskému z pohledu technologie peer-to-peer. Jedná se o jednu z technologií, která bývá nejvíce využívána k přenosům souborů o velkých datových objemech a mimo jiné je hlavním způsobem sdílení a rozmnožování autorských děl, ať již v souladu či v rozporu se zákonnými normami. Mimo jiné je pojednáno o tom, jak se s tímto fenoménem vyrovnávají některé státy evropské a jaké můžou být další přístupy. Nakonec je zmíněn i fenomén méně obecné povahy, totiž monitorování elektronické komunikace zaměstnavateli. Vyvinula se poměrně běžná praxe, že pracovní elektronická komunikace nemá charakter soukromí a bývá běžně kontrolována zaměstnavateli. Jaké můžou být právní důsledky takového jednání, tím se zabývá kapitola poslední. Témata jsou zkoumána z pohledu práva kontinentálního, zejména práva našeho, i angloamerického. Většina aspektů je též regulována na mezinárodní či evropské úrovni.

1. Internet a postavení státu: idea internetu bez hranic a jeho vliv na státní integritu

1.1 Obecné otázky

Soudy v různých zemích jen s obtížemi definovaly internet a aplikovaly na něj stávající právní úpravu.[1] Termín Internet tedy zůstal bez uspokojivé právní definice. Edwards popsal internet jako „veřejnou mezinárodní síť sítí".[2] Zjednodušeně řečeno, jde o uskupení počítačů fyzicky propojených mezi sebou kabely, případně jiným způsobem, ve kterém žádný subjekt nemůže plně kontrolovat všechny aktivity. Tento výrok poukazuje zejména na povahu internetu jako mezinárodní komunikační sítě mimo kontrolu jednotlivých národních autorit.[3] Tito autoři věří, že přirozenou povahou internetu je jeho nadstátní povaha, a tudíž internet by měl mít vlastní nezávislou „vládu" a regulaci. Ovšem jak uvidíme v následující části, tento bezesporu idealistický přístup s mnoho zastánci zejména v průběhu 90. let byl podroben mnoha právním analýzám v průběhu posledního desetiletí, zejména ze strany soudů. Jaká je dnešní pozice národních států a jejich právních řádů v této globální síti a jaký oboustranný vliv může mít na jejich právní i politický režim, to bude předmětem první části této práce. Nejdříve bude představena samotná podstata a unikátnost internetové sítě a krátce jeho historie. Další část se zabývá jedním ze zlomových bodů právního pojetí internetu ve vztahu k právnímu řádu jednotlivých zemí, kterým je soudní případ Yahoo.[4] Následně se budeme zabývat strukturou regulace internetu, jeho tří vrstev, a do jaké míry mají vliv jednotlivé státy na každou z nich. Poslední část potom představí příklady některých států a národních systémů, které se pokusily vykonávat co nejpřísnější kontrolu internetu v rámci svého území, zejména jaké prostředky a metody použily a jaký výsledný efekt měl střet internetu a jejich právního řádu. V poslední sekci první části se je pak uveden příklad vzájemného působení internetu a autoritářských režimů.

---

[1] Re SOCAN Statement of Royalties, Public Performance of Musical Works 1 C.P.R. (4th) 417 kde the Canadian Copyright Board v roce 1999 prohlásil, že Internet je telekomunikační sítí a popsal její specifické metody přenosu dat; or Braintech Inc. v. Kostiuk (1999) 171 DLR 4th 46 (BCCA) které pouze obecně popisuje Internet jako globální super-síť počítačových sítí.

[2] Edwards 2000, p. 1 – 3.

[3] Edwards and Waelde 2000, p. 29 – 30.

[4] League Against Racism and Antisemitism (LICRA) v. Yahoo! Inc. 20 November 2000, Tribunal de Grande Instance de Paris.

Nejprve je nutné se zamyslet nad samotnou přirozenou povahou internetu, v čem je odlišná a obtížná z pohledu regulace, a zda je tedy nutná zvláštní regulace pouze tohoto fenoménu. Jeden úhel pohledu, který je dnes považován za starší, je, že internet je pouze další druh mezinárodního komunikačního systému, který zprostředkovává výměnu informací v podstatě stejně jako telekomunikace či jiná média. Podle něho je internet pouze produktem globalizace a žádná specifická úprava pouze této sítě není zapotřebí.[5] Avšak, díky velmi širokému a globálnímu rozšíření internetu po celém světě, a tím i vzrůstajícího zájmu jak veřejného tak soukromého sektoru, mnoho problematických aspektů, jako třeba nové kriminální prostředí a aplikace starších trestních zákoníků, se začalo odhalovat a soudy jen problematicky interpretovaly staré zákony právě na prostředí internetu. Tak například v případě R v Gold ve Velké Británii v roce 1988, kdy žurnalista použil heslo, které odpozoroval od pracovníka pošty při jeho zadávání do jejich informačního systému, a díky tomu se dostal k informacím, které poté použil ke své práci. Soud prvního stupně sice uznal pachatele vinným, avšak odvolací soud i senát jej nakonec zprostily viny, když se zabývaly otázkou, zda lze informaci jako takovou, která není nikde uložena ani jinak ztělesněna v hmotné podobě ukrást, tím bylo právě užití vypozorovaného hesla, a usoudily, že dosavadní legislativa ani právní řád s tímto případem nepočítají a tudíž jej nemůžou činit vinným ani z krádeže ani z jiného trestného činu připadajícího tehdy v úvahu.[6] Tento případ byl sledován a vzbudil pozornost široké veřejnosti a poprvé ukázal na novou povahu rozšiřujícího se média a s tím spojené aplikační a výkladové problémy. Nová legislativa, specificky se zabývající internetem a elektronickými systémy, byla tedy přijata v podobě zákona o zneužití počítače v roce 1990.[7] Na druhé straně vznikl nový názor tzv. ochránců internetu, jenž je nutno považovat za extrémní, podle nichž internet je odděleným prostorem, tzv. cyberspace, nezávislým a nadřazeným všem jednotlivým státům a jejich právním řádům. Tak například, podle J. P. Barlowa je internet novým prostředím kde není třeba žádná právní regulace a existující staré státní předpisy jsou nepoužitelné a nepotřebné.[8] Jak je popsáno dále, i tento pohled je víceméně překonaný. Oba postoje je nutné tedy považovat za extrémní, a jak vývoj v posledních letech

[5] Murray 2007, str. 9 – 12.

[6] R v Gold (and Schifreen) [1988] 1 AC 1063.

[7] The Computer Misuse Act 1990.

[8] Barlow, J. P. (1996) *A declaration of the Independence of Cyberspace* [online] last accessed 05/15/2010 <https://projects.eff.org/~barlow/Declaration-Final.html>.

včetně současné legislativy ukazují, že různé aspekty internetové sítě je nutné regulovat odlišnými metodami a prostředky.[9]

Z pohledu historického vývoje internetu a jeho funkčního vývoje, krátký exkurz je poskytnut v této části. Obdobným způsobem jako užívání a rozvoj sítě mobilních telefonů, tato technologie má své kořeny ve vědecké činnosti obranných armádních složek Spojených Států Amerických. V průběhu studené války a hrozby nukleární války, ARPA (oddělení technologického vývoje pro obranné účely)[10] vyvinula novou technologii komunikace, která by mohla být používána po případné nukleární válce namísto telefonní sítě.[11] Její technická odlišnost záleží v tom, že při komunikaci je užíváno velké množství cest a informačních částí, tzv. paketů. Každá zpráva či jiný druh přenášené informace je rozdělená do velkého počtu přenášených paketů putujících k jejich příjemci samostatně po různých cestách. Navíc, v případě neprostupnosti jedné cesty, paket je přenesen přes jakoukoli jinou. Teprve v přístroji příjemce se pakety opět spojí a vytvoří přenášenou zprávu. Jak je na první pohled zřejmé, konstrukce zároveň měla téměř znemožnit odposlouchávání a zachycení celé informace v průběhu jejího přenosu. Poprvé byla vytvořena síť v roce 1969 pouze mezi čtyřmi počítači, tzv. nody nebo přístupovými body. Ještě v průběhu šedesátých let byl vyvinut internetový protokol, na jehož základě je přenos realizován, TCP/IP protokol, který je užíván dodnes.[12] Standard WWW standardizující užívání internetových stran a informací po celém světě, je příznačně zkratkou z anglického World Wide Web. Masivní růst internetového připojení ve všech částech světa byl pak zaznamenán v průběhu posledních dvou dekád a internet hraje nyní fundamentální roli v každodenním životě velké většiny obyvatel i podnikatelských subjektů.[13] Důkazem tohoto faktu je i zakotvení práva na vysokorychlostní internet jako jedno za základních lidských práv například ve Finsku v roce 2009.[14]

[9] Edwards a Waelde 2009, str. 3 – 4.

[10] The Advanced Research Projects Agency.

[11] Leiner, B. M. et col. (unknown) *Histories of the Internet. A Brief History of the Internet* [online] last accessed 05/15/2010 <http://www.isoc.org/internet/history/brief.shtml>.

[12] The Transmission Control Protocol/Internet Protocol.

[13] Lloyd 2000, str. 26 až 28.

[14] Ahmed 2009, str. 1.

1.2 Internet z pohledu autorského práva

Myšlenky a jejich výsledky (dnes chráněné jako autorská díla) nebyly v minulosti (do 18. století) považovány za něco, co by se alespoň zdánlivě podobalo předmětu vlastnictví a bylo též obdobným způsobem právně chráněno. Současné pojetí je však odlišné a zachází s duševním vlastnictvím jako s vlastnictvím sui generis zejména díky obdobnému způsobu ochrany. Důvodem, proč se práva k duševnímu vlastnictví vyvinula, je jak potřeba sebevyjádření autora, tak zejména ekonomický aspekt těchto práv. Unikátní vyjádření a kombinace myšlenek se staly něčím, co může mít značnou ekonomickou hodnotu. Autorské právo je jedním z druhů práv k duševnímu vlastnictví, vedle například práv k průmyslovému vlastnictví. Pojetí autorského práva se postupně vyvíjí společně se společností a technologií, kterou společnost využívá. Významné vývojové změny v pojetí autorského práva byly způsobeny užíváním masových médií. Tištěné noviny, fotografie, hudební nahrávky, televizní programy, videa, všechny tyto prostředky znamenaly nové výzvy k aplikaci či případné změně tehdejší autorskoprávní legislativy. Tyto změny často předcházely vážné debaty vzniklé ze střetu zájmů představitelů různých zájmových skupin. Obdobně je tomu v dnešní době, kdy předmětem znamenajícím obtížnosti zachování současné podoby autorského práva je světová počítačová síť Internet.

Internet je svojí povahou novým prostředím, kde dochází k legálnímu užívání autorských děl. Zároveň však představuje nový prostředek celosvětového a anonymního porušování autorských práv. Jeho uživatelé mají přístup k nespočetnému množství materiálů, které mohou být rozmnožovány a poskytovány dalším uživatelům během několika málo sekund. Dosud postačovalo pozměnit autorskoprávní právní předpisy tak, aby se přizpůsobily nové realitě. Podle některých autorů však toto nemusí v nastávající digitální době být dostačujícím. [15] Důkazem, jak velkou měrou změnil dosavadní pojetí autorského práva, které se musí a stále vypořádává s novými technologiemi, budiž například nové legislativní prostředky na všech úrovních: mezinárodní úmluvy WIPO (World Inellectual Property Organization) z roku 1996 (tzv. internetové úmluvy WIPO),[16] evropská směrnice o harmonizaci některých aspektů autorského práva a práv souvisejících v informační společnosti,[17] směrnice č. 2004/48/ES o dodržování práv

[15] Guadamuz, Andrés (2002) *Copyright in Cyberspace: Building Fences on the Internet*. [online] Alfa Redi, No. 109, October. navštíveno 1/10/2010. přístupné na adrese <http://ssrn.com/abstract=595362>, str. 5.

[16] Smlouva o právu autorském (v platnosti od 6.3.2002) a Smlouva o výkonech výkonných umělců a o zvukových záznamech (platnost od 20.5.2002).

[17] Směrnice 2001/29/ES z 22. května 2001 a směrnice 2004/48/ES z 29. dubna 2004.

duševního vlastnictví z roku 2004 nebo specifická národní úprava aspektů autorského práva v digitálním prostředí, např. the Digital Millenium Copyright Act z roku 1998.

Internet vzhledem ke své povaze rozdělil své účastníky do několika zájmových skupin. Na jedné straně stojí ti, jimž svědčí autorská práva, ať již osobnostní či majetkové povahy. Jejich snahou je posilování svého postavení a prostředků kontroly a ochrany svých práv. Typickým příkladem, který je i výsledkem významného postavení a lobbingu zábavního průmyslu v zemi, je např. nová legislativa ve Velké Británii, tzv. Digital Copyright Act, a ve Francii, tzv. HADOPI zákon, které se výrazným způsobem snaží zasahovat do vztahů ve prospěch větší efektivnosti ochrany subjektů autorského práva. Podrobněji je o této problematice pojednáno v části týkající se postavení poskytovatelů služeb informační společnosti. Na straně druhé jsou potom koncoví uživatelé internetové sítě (nikoli k podnikatelským účelům), kteří obhajují co nejmenší omezování tohoto prostředí a zachování maximální dostupnosti a šíření veškerých informací v tomto prostředí. Oba postoje se zdají být problematické. Je jen těžko představitelné, jakými prostředky by mohla být ochrana autorských práv plně zajištěna a kdo by měl náklady na taková opatření nést (např. ve Velké Británii je kladeno mnoho nových povinností na poskytovatele služeb, včetně monitorování činnosti svých zákazníků. Tito jsou tudíž povinni nést značné finanční náklady na přijímání potřebných opatření, ačkoli se z jejich pohledu může zdát nespravedlivé.). Druhý názor lze považovat za zcela neopodstatněný, protože jeho důsledkem by byl úplný zánik autorských práv v digitálním internetovém prostředí. Takové smýšlení je tudíž extrémní a nereálné. Právní praxe se tudíž snaží nacházet nějakou střední cestu. Typickým příkladem je aktivita neziskové organizace ve Spojených Státech Amerických Creative Commons (CC).[18] Tato organizace vydala specifické druhy licenčních smluv, které kladou důraz na osobnostní autorská práva (např. způsoby zveřejnění autorského díla, způsob uvedení autorova jména atd.) a v pozadí ponechávají práva majetková.[19] Vzhledem k angloamerickému pojetí autorského práva, které dlouhou dobu vůbec osobnostní práva autorů neuznávalo, jde o přístup velmi inovativní. Nutno však podotknout, že CC s jistotou nebude postačovat těm, pro které autorská díla znamenají hlavní zdroj zisku (jako je zábavní průmysl produkující například

[18] Carroll, Michael W. (2007) Creative Commons as Conversational Copyright. Villanova Law/Public Policy Research Paper No. 2007-8; *Intellectual property and information wealth: issues and practices in the digital age* [online] Peter K. Yu, ed., Vol. 1, pp. 445-61, Praeger. přístupné na adrese <http://ssrn.com/abstract=978813> str. 5.

[19] Ikaros, redakce (2005) *Internet kontra copyright* [online] navštíveno 1.8.2010 dostupné na adrese <http://www.ikaros.cz/internet-kontra-copyright>.

vizuální a audiovizuální díla), tedy díla vytvářená zejména z komerčních/ziskových důvodů. Na druhou stranu některé studie uvádí, že zejména méně rozvinuté země považují přílišnou ochranu a restrikce za negativní jev a výdobytek relativně malého počtu rozvinutých západních zemí, protože jejich důsledek je, že si přístup k informacím a přenášeným materiálům mnoho uživatelů ze zemí méně rozvinutých nemůže dovolit. [20] Vždy je však nutné zvažovat i další aspekty, například pro jaké účely a kým jsou chráněná díla užívána. Například jeden ze zajímavých návrhů, jak pomoci rozvíjejícímu světu, je podpora vývoje tzv. freeware nebo open source počítačových programů například za podpory vlád rozvinutých zemí, jejichž běžné užívání není nikterak omezeno finančně a každý si jej může dovolit.[21]

Jeden příklad za všechny, jaké problémy například znamenal internet pro současné pojetí autorského práva ve Velké Británii. Digitální prostředí převádí veškeré informace do datové podoby, takže jejich esenciální podoba veškerých internetových stránek je zejména v HTML jazyce. Jako takové by měly být chráněny jako autorská díla literární. Obsahem však ve velké většině jsou i díla povahy odlišné (včetně audio či audiovizuální podoby). Zároveň však nelze považovat webovou stránku za program pro nedostatek své složitosti. Výkladovými problémy se zabývaly soudy například v případě Shetland Times Ltd v. Jonathan Wills[22] či Ibcos v. Barclays Mercantile.[23] Současné pojetí je takové, že webová stránka je kompilace různých děl, která je podle CDPA považována za dílo literární povahy.

V měřítku mezinárodním existuje několik úmluv, které vytváří rámec pro ochranu autorských práv. Za počátek se považuje Bernská úmluva z 1886, dále pak úmluvy TRIPS z roku 1995 a Ženevské úmluvy WIPO z roku 1996 (the WIPO Copyright Treaty a the WIPO Performances and Phonograms Treaty). Z pohledu internetového například úmluvy TRIPS považují programy a kompilace (jimiž jsou i webová stránky) za díla literární.

Na novou digitální realitu a výkladové problémy dosavadního práva reagovaly i USA přijetím nového zákona The Digital Milenium Copyrigt Act 1998 (DMCA).

---

[20] Story, A. (2002) *Study on Intellectual Property Rights, the Internet, and Copyright*. [online] UK, Kent: Universtiy of Kent, navštíveno 24.9.2010. dostupné na adrese <http://www.iprcommission.org/papers/pdfs/study_papers/sp5_story_study.pdf> str. 4.

[21] Ibid. str. 5.

[22] Shetland Times Ltd v. Jonathan Wills and Another [1997] SLT 669.

[23] Ibcos Computer Ltd. v. Barclays Mercantile Highland Finance Ltd. [1994] FSR 275.

V neposlední řadě i právo evropské prostřednictvím směrnic uzpůsobilo některá pravidla a výklady tak, aby byla lépe použitelná v prostředí internetovém. Tak například informační směrnice ve svém čl. 3 odst. 3 uvádí, že k vyčerpání práva na rozšiřování při prvním sdělení díla veřejnosti, pokud se tak stane v nehmotné podobě (tedy např. prostřednictvím internetu), nedochází. Pouze tedy vlastník hmotné rozmnoženiny má možnost převést vlastnictví k této rozmnožení na jiného, což však nabyvatel nehmotné rozmnoženiny (např. stažením programu online) nemá.[24] Mimo jiné byla i zavedena možnost uzavřít licenční nevýhradní smlouvu i konkludentně (ve smyslu § 46 odst. 5 a 6 AZ), tudíž i provedením úkonu (například přijetím programu on-line a nainstalováním či jeho použitím) dochází k uzavření licenční smlouvy.[25]

Jaké je vlastně odůvodnění a smysl existence současného autorského práva? Lze považovat za odůvodněné úvahy o krizi autorského práva v digitálním prostředí? Důvodů vzniku a existence tohoto právního institutu je vícero povahy: morální, ekonomické, stimulační i sociální.

V minulosti bylo považováno kopírování práce jiné osoby za nemorální. V této podobě lze tedy chápat morální práva, jakožto práva zejména osobovat si autorství. Tato práva jsou typická pro kontinentální právní systémy, na rozdíl od angloamerického, který tyto aspekty převzal teprve v poslední době (např. v UK pomocí zákona The Copyrights, Designs and Patents Act of 1988, tzv. CDPA). Tato práva se odvozují od teorie přirozenoprávní, která je považuje za přirozenou součást integrity a osobní pověsti autora. Tato práva nemohou být proto ani prodána a nezanikají při zcizení majetkových autorských práv jiné osobě. Jejich ochrana je v mezinárodním měřítku reflektována i v Bernské úmluvě z roku 1886.

Ekonomické důvody jsou nepochybně hlavním hybatelem a důvodem, proč ochrana těchto práv vznikla a nyní činí tak bouřlivou diskuzi při jejich možných změnách či ohrožení. Například ústava Spojených Států Amerických považuje autorské právo za ekonomickou odměnu autora. Angloamerická úprava, jak již bylo zmíněno, donedávna poskytovala ochranu pouze majetkovému aspektu autorských práv. Autorské dílo je považováno za předmět vlastnického práva (vychází z tzv. vlastnické teorie) sui generis, zejména proto, že poskytuje jeho majiteli obdobná práva jako majiteli reálných věcí (například věc zcizit či poskytnout její užívání – v autorskoprávní terminologii prostřednictvím licenčních smluv).

[24] Dobřichovský, T. (2004) *Moderní trendy práv k duševnímu vlastnictví v kontextu evropského práva, dohody TRIPS a aktivit WIPO*. Praha: Linde Praha, a.s., str. 59.

[25] Švestka, J., Dvořák. J., a kol. (2009) *Občanské právo hmotné*, 3. díl, 5. vydání, Praha: Aspi, str. 217.

Dalším důvodem je i motivační nebo stimulační, protože autorům se za jejich snahu dostane odměny v podobě finančních prostředků. Tímto způsobem lze též dosahovat dalších pokroků, včetně technologických (ochrana mj. prostřednictvím patentového práva).

Ochrana autorských děl je též odůvodňována společenským zájmem a pokrokem, kdy v režimu ochrany autorských děl by autoři měli být více ochotni zpřístupnit svá díla, sdílet je s ostatními členy společnosti a šířit tím informace i vzdělání.[26] Smyslem autorského práva například podle Ústavy USA je napomáhání v rozvoji vědy a užitého umění.[27] Jejich smyslem je tedy vyvážení veřejného zájmu, který je základním smyslem existence autorského práva, kterého je dosahováno odměňováním autorů do výše nutné k další kreativní činnosti. Smyslem je tedy vlastně nalezení vyváženosti mezi veřejným zájmem a zájmy soukromými těch, kdo jsou vlastníky či komu svědčí práva k obsahu.[28]

Z uvedeného vyplývá, že existence institutu autorského práva a práv příbuzných není neopodstatněná. Důvodů však je mnoho a záleží vždy na vhodném nalézání kompromisu mezi ochranou subjektivních práv autorů či jiných osob a zájmem vyšším. Internet znamená novou realitu zejména v tom, že jeho rozmach doprovází i nový vývoj společnosti, která se globalizuje, urychluje a je z daleko větší míry závislá na přenosu informací ve všech podobách. Úvahy zpochybňující existenci a ochranu autorských práv jako takových jsou však neoprávněné. V zájmu soukromého užívání či pro vědecké a studijní účely existují řady výjimek pro užití takového autorského práva. Pro stimulaci dalšího vývoje a vzniků nových autorských děl však je nutné, aby existovala a zdokonalovala se právní úprava reflektující novou realitu.

Jaké jsou dopady porušování autorského práva v prostředí internetu? Jak je na první pohled patrné, největším problémem jsou ekonomické ztráty z prosušování a obcházení práv autorských. Internet výrazně přispěl a zjednodušil zejména rozmnožování autorských děl a jejich sdílení, tj. poskytování kopie jinému internetovému uživateli. Způsobů, jak sdílet taková data je mnoho. Některé z nich jsou vyhledatelné a lze užít příslušná opatření (blíže viz. kapitola peer-to-peer sdílení) k jejich omezení či zabránění, s jinými lze bojovat jen velmi obtížně. Zejména země, kde je zábavní a softwarový průmysl jedním z důležitých složek národní ekonomiky, jsou nuceni

[26] Guadamuz 2002, str. 9 a 10.

[27] Ústava USA, čl. 1, § 8 odst. 8.

[28] Schaumann, Niels B., *Copyright Infringement and Peer-to-Peer Technology* (2002). William Mitchell Law Review, Vol. 28, No. 3 [online] přístupné na adrese: <http://ssrn.com/abstract=1527189> str. 1025.

přijímat opatření k obraně či alespoň omezení porušování těchto práv a zprostředkovaně i k zamezení dalších ekonomických i daňových úniků ze země.

Pokud se hovoří o internetu, nejčastěji si lidé představí tzv. webové stránky (WWW z anglického World Wide Web) užívající protokol HTTP (the Hypertext Transfer Protocol). Vedle tohoto však existuje celá řada dalších protokolů a služeb, pomocí nichž dochází ke sdílení a přenášení informací taktéž (např. FTP – the File Transfer Protocol, IRC – Internet Relay Chat, POP3 – Post Office Protocol nebo FSP – File Service Protocol). Tyto protokoly pak umožňují kontrolovat přístup i případné monitorování (ze strany porušovatelů práv) tak, aby se jednotliví uživatelé nevystavovali riziku, že bude jejich nelegální činnost odhalena (jak tomu bývá u protokolu HTTP). Navíc je i mnoho případů, kdy servery užívající například protokol FTP vyžadují registraci a úplatu za jejich používání.[29] Takto dochází k závažnější formě porušování autorských práv, protože za poskytnutí autorských děl je přijímána úplata.

V případě porušování autorských práv prostřednictvím internetu, je důležité si uvědomovat, kdy a jak k porušování skutečně dochází. Způsobů je velmi mnoho, níže jsou uvedeny některé z nich.

Tak například pro autory zvukových a audiovizuálních děl znamenal největší ohrožení vývoj tzv. komprimovaných formátů (např. MP3 nebo AVI), díky kterým se významně zmenšila velikost kopie daného díla při zachování původní kvality, a v podstatě každý přehrávač může tyto formáty bez omezení přehrát. Potom již stačí pomocí některého z výše uvedených protokolů takové dílo poskytnout jinému.

Kromě těchto děl je od počátku problematické i poskytování počítačových programů. Rozlišují se různé způsoby porušování práv k nim: kopírování koncovými uživateli, užívání spuštěním z pevných disků, prodávání kopií programů za programy tzv. originální (legální) nebo poskytnutí programu osobám, které si nekoupili licenční oprávnění. Výsledná situace je tudíž taková, že téměř každý uživatel počítače užívá nějaký program, ke kterému nemá příslušná oprávnění. Přístup k software (nebo i souborům dat, databázím) a jeho použití, třebaže jen pro soukromé účely, je totiž porušením autorského zákona. Zde je významný rozdíl proti jiným druhům autorských děl, například audiovizuálním, jejichž užití formou shlédnutí pro osobní potřebu se za porušení autorských práv nepovažuje.

[29] Guadamuz 2002, str. 19 a 20.

V podstatě denně dochází k porušování autorských práv také tzv. Copy-and-Paste metodou. Jde v podstatě o kopírování dat či jejich částí prostřednictvím počítačových příkazů (Copy – kopírovat a Paste – vložit). Kopírování autorských děl tímto způsobem na témže počítači je jedním z nejčastějších způsobů porušování autorských práv, avšak na rozdíl od ostatních, nejde o ten, který by znamenal největší ekonomické ztráty a přímo ovlivňoval nejsilnější vlastníky autorských práv či práv příbuzných. Proto se o těchto praktikách téměř nehovoří.

Obdobně i samotné internetové (webové) stránky jsou chráněny autorským právem. Obecně lze říci, že téměř veškeré aspekty webových stránek jsou předmětem autorského práva. Chráněný je tedy například originální design i obsah takové stránky, zahrnující například odkazy, originální text, grafiku, audio, video, kód stránky vyjádřený v informačním jazyce a další originální součásti.[30]

Jakým způsobem se tedy s novou realitou vyrovnává současná právní legislativa? Základní právní rámec je položen na mezinárodní úrovni. Za prvotní dokument je považována úmluva Bernská z roku 1886 spravovaná Světovou organizací duševního vlastnictví (WIPO). Vedle ní patří mezi důležité dokumenty i Všeobecná úmluva o autorském právu z roku 1952 z Ženevy a její současná revidovaná verze z Paříže 1971, tzv. Římská úmluva z roku 1961,[31] Dohoda TRIPS (o obchodních aspektech práv duševního vlastnictví) z roku 1994, a nově zejména tzv. internetové smlouvy WIPO z roku 1996 (Smlouva WIPO o právu autorském a Smlouva WIPO o výkonech výkonných umělců a o zvukových záznamech).

V prostředí evropském se jeví jako nejpravděpodobnější cesta evropské legislativy, která by měla sjednotit právní úpravu některých aspektů tak, aby byl přístup v rámci EU jednotný. Mezi nejdůležitější přijaté dokumenty patří směrnice Informační (2001/29/ES o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti, resale směrnice (2001/84/ES o právu na opětný prodej ve prospěch autora originálu uměleckého díla) a směrnice o dodržování práv duševního vlastnictví (2004/48/ES). Do budoucna se zvažují návrhy

[30] Montecino, V. (1996) *Copyright and the Internet* [online] navštíveno 10/08/2010. Dostupné na adrese <http://mason.gmu.edu/~montecin/copyright-internet.htm>.

[31] Mezinárodní úmluva o ochraně výkonných umělců, výrobců zvukových záznamů a rozhlasových organizací, 1961, Řím.

upravující další výjimky (takovými by mohly být například pořizování kopií na tomtéž pevném disku nebo pro vzdělávací účely).[32]

Z pohledu práva vnitrostátního je úprava autorského práva komplexně obsažena v zákoně č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (dále též "autorský zákon" či AZ). Popřípadě se obecné otázky řídí občanským zákoníkem, ke kterému je AZ ve vztahu speciality.[33]

Pro určení práva, které se užije v případě přeshraničních vztahů, jsou potom důležité normy z oblasti mezinárodního práva soukromého. Na mezinárodní úrovni je významná Úmluva o právu rozhodném pro smluvní závazkové vztahy z Říma roku 1980 (u nás č. 64/2006 Sb. m. s.). V prostředí evropském jsou pak zásadní nařízení tzv. Řím I a Řím II (nařízení č. 593/2008 o právu rozhodném pro smluvní závazkové vztahy – Řím I, a nařízení č. 864/2007 o právu rozhodném pro mimosmluvní závazkové vztahy – Řím II). V neposlední řadě též bude záležet na mezinárodní spolupráci, zejména uznávání a výkonu soudních rozhodnutí. V evropském prostředí se tímto aspektem zabývá nařízení č. 44/2001 o příslušnosti a uznávání a výkonu soudních rozhodnutí v občanských a obchodních věcech.

Existuje-li tedy právní rámec, proč tedy stále dochází k porušování těchto práv? Největší problém totiž spočívá ve vymáhání dodržování, případně postihování porušování garantovaných práv. Tady se zpět vracíme k diskuzi o právním režimu internetu a možnostech vymáhání jednotlivých právních řádů v jeho prostředí. Potíže tedy zůstávají obdobné. Jednak jde o mezinárodní problém, protože nejvíce porušování a sdílení dat je přeshraniční. Servery jsou často umístěny v tzv. autorskoprávních nebích, státech bez dostatečné legislativy (např. státy Východní Evropy). Jak je zřetelné, jedině úzká mezinárodní spolupráce může napomoci důslednější ochraně. Některé ohlasy volají i po zřízení mezinárodního soudu zabývajícího se specificky spory z digitálního prostředí. Jeho efektivní fungování si však lze jen těžko představit. Existují různé způsoby, jak vymáhání existujícího práva zajistit. Vymáhání subjektivních práv je ponecháno na samotném subjektu, komu právo svědčí. V případě autorských práv lze tedy očekávat vzrůstající důležitost kolektivních správců autorských práv, kteří mimo jiné mají za úkol pečovat o autorská práva např. jejich monitorováním a vymáháním. Teprve vyšší zájem

[32] European Commission (1997) *Copyright and Related Rights in the Information Society - Proposal for Directive/Background*. 10 prosinec. přístupné na adrese <http://europa.eu.int/comm/dg15/en/intprop/intprop/1100.htm>.

[33] Švestka. Dvořák. a kol. 2009, str. 172.

může být důvodem pro vymáhání státem, např. prostřednictvím k tomu určených orgánů. Hlavním předpokladem však je identifikace toho, kdo práva porušuje. Toto je však problematické a některé služby a protokoly téměř znemožňují dohledat toho, kdo se porušování dopouští.

Dalším užívaným a do určité míry efektivním způsobem jsou opatření technického charakteru, které požívají zvláštní ochrany ve smyslu § 43 AZ. Tak například počítačové programy vyžadují zvláštní klíče, aktivační kódy či další metody, avšak i tyto bývají často obcházeny. Vynalézavost těch, kdo porušují právo i výrobce je vždy rychlejší než opatření, která jsou k jejich předcházení přijímána.

Některé státy se tudíž vydaly cestou výraznějšího zapojení těch, kdo poskytují internetové připojení koncovým uživatelům, a mají tudíž největší možnost a moc nad tím, co tento uživatel na internetové síti provádí, nebo kdo poskytují služby či hostují internetové stránky, které k porušování autorských práv jsou užívány. Podle nové legislativy např. ve Francii či Velké Británii mají tyto subjekty, např. poskytovatelé internetového připojení, tzv. ISPs (viz. kapitola o poskytovatelích služeb informační společnosti), určité povinnosti při monitorování a aktivně se účastnit vymáhání v případě protiprávní činnosti uživatelů jejich služeb.

Vedle přijímání nových legislativních opatření na všech úrovních se však zdá, že nejvíce úspěšné je přizpůsobení se nové realitě nové, na výměně informací založené společnosti. Velmi úspěšným je například nový obchodní model, který reprezentuje společnost Apple. Pomocí programu iTunes a Apple Store (jde ve své podstatě o legální formu peer-to-peer sítě) došlo k výraznému snížení porušování autorských práv k programovým i zvukovým dílům. Myšlenka je totiž taková, že díla jsou cenově dostupná, uživatelsky velmi přátelská a jednoduchá, a navíc přístroje od společnosti Apple umí pomocí technických prostředků rozeznat, zda přehrávaná díla jsou či nejsou pořízena v souladu s autorskými právy. Tímto způsobem došlo k motivaci uživatelů, aby si například hudební díla raději zakoupila. Nutno však poznamenat, že jde spíše o způsob ekonomicko-politický než právní. Avšak právě tento přístup se zdá mít daleko výraznější výsledky než neustálé prohlubování a zdokonalování stávajících pravidel založených zejména na hrozbách sankcemi.

Jaké jsou tedy aktuální trendy vývoje autorskoprávní legislativy? Autoři de Beer a Clemmer si ve své práci všímají vývoje postavení ISPs, který se z původního pasovně-reaktivního postoje (tedy reagující až na výzvu těch, jejichž práva byla počínáním uživatelů internetu porušena) stává spíše aktivně-preventivním. Tedy tito jsou povinni přijímat opatření preventivní a nést s

tím související nemalé finanční náklady.[34] Tento trend, objevující se od roku 2007, však může mít mnoho dopadů a úskalí. Jednak dochází k potlačování role soukromí a ochrany osobních údajů ve prospěch lepší možnosti vymáhat jiná práva v internetovém prostředí. Dochází také k potvrzení dominantního postavení těch, kdo poskytují služby informační společnosti, jelikož na nich záleží úspěšné vymáhání těchto práv. V neposlední řadě také jde o upřednostnění ekonomických zájmů v podstatě poměrně úzké skupiny lidí, kterým autorská práva náleží, na úkor společnosti a nové reality. Přístup (zejména ve Francii a Velké Británii) také vzbuzuje poměrně velkou nevoli z řad zastánců občanských práv a svobod s tím, že například snížení rychlosti či dokonce odpojení od internetu uživatele, který nebyl řádně uznán viným z porušování právních předpisů nestranným soudem, je odporující podstatě lidských práv a svobod. Jde v podstatě o zavedení presumpce viny ve prospěch majitelů autorských práv či práv souvisejících.[35] Obdobný přístup byl přijat na Novém Zélandě v roce 2008 a je účinný od února roku 2009.[36] Někteří vidí v těchto úpravách rozpor s článkem 15 směrnice E-Commerce, který ukládá členským státům, aby neuvalovali obecnou povinnost monitorovat informace, které přenáší nebo hostují na svých serverech pro uživatele, na poskytovatele těchto služeb. Například francouzské soudy však odůvodňují soulad tím, že nařízení blokovat a filtrovat obsah pomocí technologických prostředků není monitorováním, ale spíše prostředkem k tomu, aby se plošnému monitorování poskytovatelé vyhnuli.[37] Naopak soudy v USA existence takovýchto povinností poskytovatelů služeb odmítají.[38] De Beer a Clemmer zároveň varují, že v podstatě dochází k zavádění strategie dohlížející nad provozem sítě internet (která byla dosavadně výrazně neutrálním a pokud možno co nejméně omezovaným komunikačním prostředím) obdobně, jako k tomu dochází, ačkoli spíše z politických důvodů, například v Číně.[39]

---

[34] DeBeer, Jeremy F. and Clemmer, Christopher D. (2009) *Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries?* [online] October 1. Jurimetrics, Vol. 49, No. 4. přístupné na adrese <http://ssrn.com/abstract=1529722> str. 1 a 2.

[35] DeBeer, Jeremy F. and Clemmer 2009, str. 16 a 17.

[36] Copyright (New Technologies) Amendment Act 2008.

[37] Workman, supra note 136 (discussing SABAM v. S.A. Scarlet (formerly Tiscali), Tribunal de premiere instance de Bruxelles [T.P.I.] [Court of First Instance] Brussels, May 18, 2007 (Belg.). přístupné na adrese <http://www.juriscom.net/documents/tpibruxelles20070629.pdf>.

[38] Ibid. str. 29.

[39] Ibid. str. 33.

Závěrem této debaty vystává otázka vývoje v budoucnost. Jak již bylo uvedeno, k porušování autorských práv dochází velmi často i přes veškeré dosavadní pokusy o zamezení takové činnosti. Je tedy otázkou, zda je stále existence práv, které nelze efektivně vymáhat, nadále odůvodněná. Navíc se objevují názory, že ochrana těchto práv je v rozporu s veřejnými zájmy. Důvodem je názor, že zájem na co nejširším přístupu k informacím a vědomostem je daleko více ve veřejném zájmu, než jsou individuální majetková práva autorů či jiných osob.[40] Takové myšlenky lze však považovat za extrémní, protože jejich odůvodněnost lze promítnout do výjimek, jako jsou užití autorských děl výlučně pro osobní potřeby, pro potřeby vzdělávací či zpravodajské. Nelze však takto ospravedlnit ani odůvodnit zánik autorských práv zcela. Řešením tedy není upustit od vymáhání práv v případě, že se to jeví obtížné. Nejdůležitější je mezinárodní spolupráce zejména v tom smyslu, že i chudší státy by měly přijmout legislativní opatření, která poskytnou právní rámec pro vymáhání autorských a souvisejících práv, a postaví tak mimo zákon ty, kdo se jejich porušování dopouští. Důsledkem dnešního vývoje může být i návrat k původním, morálním aspektům autorského práva (jak se tomu děje v případě již zmíněných Creative Commons). Spolupráce mezi státy musí být založena na uznávání a výkonu soudních rozhodnutí v ostatních státech. Předpokladem je však vždy oboustranná protiprávnost, tudíž unifikace zejména prostřednictvím mezinárodních smluv a aktivní činnost WIPO je nepostradatelná.

1.3 Soudní případ Yahoo!

Za jeden z právních milníků v historii internetu je považován právě případ společnosti Yahoo,[41] ve kterém byla detailně posuzována povaha internetu a aplikace národního práva, v tomto případě francouzského. Soudní případ samotný byl slyšen v Paříži, která je považována historicky za kolébku novodobého kontinentálního práva, avšak jeho význam sahal daleko za hranice evropského kontinentu. Ve své podstatě šlo o spor mezi novou obchodní společností operující v rámci internetového prostředí a tradičním národním právem Francie a jeho aplikací právě na internetovou síť a její obsah. Základní otázkou bylo, zda je dána jurisdikce francouzského soudu nad cizími subjekty, společnostmi, obchodujícími na internetové síti. Dalším předmětem pak bylo, zda je národní právo aplikovatelné v mezinárodním cyber-

[40] Guadamuz 2002, str. 40.

[41] League Against Racism and Antisemitism (LICRA) v. Yahoo! Inc. 20 November 2000, Tribunal de Grande Instance de Paris.

prostředí. Zároveň šlo i o spor mezi obránci internetu, pro něž internet byl prostředím bez právní regulace a bez její potřeby, a těch, kdo zastávali tradiční pojetí internetu jen jako dalšího druhu komunikačního media.[42]

Faktická stránka věci byla, že v roce 2000 společnost Yahoo poskytovala službu internetové aukce na svých webových stránkách yahoo.com. V jedné z těchto aukcí bylo možnost zakoupit předměty nacistické propagandy. Z faktu, že aukce a stránky byly ve francouzském jazyce a byly zpřístupněny právě ve Francii vyplývalo, že tyto předměty jsou určené pro obyvatele Francie. Mark Knobel, francouzský žid a čelní představitel Ligy Proti Rasismu a Antisemitismu, předložil žalobu francouzskému soudu opírající se o francouzské právo. Yahoo se mimo jiné bránila, že dotčené webové stránky byly hostovány ze serveru umístěného v USA, tudíž mimo území Francie a její jurisdikce.[43]

Klíčový argument žalobce, založený na principu rovnosti a zákazu diskriminace byl, že Yahoo musí dodržovat národní zákony ze stejného důvodu, jako každá jiná mezinárodní společnost z „reálného světa“. Tak například výrobce automobilů je povinen dodržet bezpečnostní předpisy a předpisy životního prostředí každé země, třebaže se tyto liší, ve které mají být automobily prodávány.[44]

Žalovaný poukázal na několik důležitých a problematických aspektů. První se týkal teritoriální jurisdikce francouzských soudů a působnosti tamního práva tvrdící, že francouzský soud nemůže rozhodovat o oblasti, která není v jeho kontrole a působnosti. Odůvodňováno to bylo faktem, že jak společnost Yahoo, tak hostující server byly umístěny na území USA, tudíž francouzský soud tam nemá žádnou autoritu. Druhý argument varoval, že díky přirozené povaze internetu, který je bez ohledu na hranice, stránka Yahoo by tak mohla být shledána za náležící do jurisdikce práva každého jednotlivého státu na světě, což by vedlo k restrikci svobody slova a dalších lidských práv v režimu toho státního práva, které by bylo nejpřísnější. Tak by fakticky docházelo k omezování lidských práv podle například čínského práva či práva Saudské Arábie ve všech ostatních státech. Navíc by to mohlo vést i k eventuální nejistotě při určování, jaký právní řád musí být dodržován v souvislosti s internetem. Třetí obrana se pak zakládala na technické rovině, že totiž není technicky možné zajistit například omezení či zamezení přístupu na konkrétní webové stránky pouze těch, kdo se připojují z francouzského území. Bylo tvrzeno,

[42] Lloyd 2000, str. 1 až 3.

[43] Goldsmith and Wu 2006, str. 1 – 3.

[44] Goldsmith and Wu 2006, str. 5.

že by bylo nutné zajistit každý jednotlivý přístupový bod na francouzském území, což by bylo prakticky neproveditelné.[45]

Soud se vypořádal s argumenty takto. Francouzská působnost a jurisdikce byla dána na základě tzv. principu účinku trestního zákoníku, který se jinak také označuje za tzv. passive personality principle (princip ochrany). Podstatou je, že francouzské trestní právo je aplikovatelné na činy spáchané proti státním občanům Francie, bez ohledu na místo činu či národnost pachatele.[46] Druhý argument byl v podstatě podle odůvodnění žalobce odmítnut, a třetí byl vzat v potaz v tom smyslu, že bylo společnosti Yahoo přikázáno podniknout adekvátní opatření (reasonable measures) ve smyslu konečného rozhodnutí, které znělo ve prospěch žalobce, a soud společnosti Yahoo přikázal podniknout všechny nezbytné opatření k tomu, aby byl znemožněn či přerušen jakýkoli přístup přes yahoo.com do dotčené aukce.[47]

Yahoo však přesto odmítla podrobit se rozsudku s tím, že nebude filtrovat své zákazníky podle jejich národnosti. Navíc, stále obhajujíc se architekturou internetu, která nebere v potaz geografické hranice. Během určených dvou měsíců, lhůta pro Yahoo k přijetí potřebných opatření, proto soud jmenoval expertní komisi, která analyzovala technické možnosti blokování a filtrování datových přenosů do Francie a měla posoudit dostupnost případných prostředků. Její výsledek byl, že přibližně sedmdesát procent francouzských IP adres (fyzických adres) by mohlo být efektivně filtrovaných. Proto také soud rozhodl a uložil povinnost s vědomím faktu, že není možné, díky přirozené povaze internetu podniknout kroky se stoprocentní efektivitou.[48]

Přesto však Yahoo formálně nakonec dosáhla svého, když obvodní soud ve Spojených Státech odmítl uznat soudní rozhodnutí francouzského soudu a provést jej v roce 2001, s odůvodněním nedostatku pravomoci francouzského soudu. Například profesor Reidenberg se však vyjádřil k tomu, že americký soud takto rozhodl protekcionářsky a v rozporu s vlastní praxí v USA, kdy se běžně uznávaly a vykonávaly rozhodnutí soudů jednotlivých amerických států (i v oblasti internetu) podle jejich vlastních, nikoli federálních, zákonů.[49] Samotná společnost Yahoo však fakticky v době rozhodnutí soudu v USA již sama zamezila prodej rasistických předmětů z aukcí, aby se pragmaticky vyhnula přílišné a nepotřebné negativní publicitě.

[45] Goldsmith and Wu 2006, str. 6 a 7.

[46] Reidenberg 2001, str. 5.

[47] Akdeniz 2001, str. 1.

[48] Goldsmith and Wu 2006, str. 8.

[49] Reidenberg 2001, str. 9 až 11.

Nakonec i argument neproveditelnosti se ukázal být lichým, protože samotná společnost Yahoo o rok později vstoupila na trh v Číně a souhlasila s autoritářské vlády, že bude své služby filtrovat pod dozorem tamní vlády (a to i přes mnoho kritických hlasů ze strany obhájců lidských práv), čímž tacitně prokázala, že technicky proveditelné prostředky cenzury či kontroly internetu na geograficky určeném území jsou dostupné.[50]

Důležitý je též fakt, že tento soudní proces, ostře sledovaný odbornou veřejností po celém světě, rozpoutal širokou diskuzi o povaze a další regulaci internetového prostředí. Akdeniz zdůrazňuje, že hlavní devizou internetu je jeho otevřenost, přístupnost a publicita. Restrikce mohou způsobit újmy jak na soukromí a právu na svobodu slova, tak mohou snížit hodnotu internetu jako globálního sociálního, kulturního, komerčního, vzdělávacího, zábavného a komunikačního systému.[51] Na druhou stranu je však výsledek a rozhodnutí francouzského soudu je důležitým vítězstvím demokratických hodnot. Pozitivní normativní dopad rozsudku je spatřován v tom, že internetové subjekty budou muset respektovat odlišné hodnoty veřejnosti namísto pouhého upřednostňování ekonomických zájmů.[52]

1.4 Regulace internetu

Nyní je třeba se podívat, jakým způsobem se vyvinula regulace internetu po případu Yahoo. Do té doby měl internet povahu globální sítě, která však byla založena a fakticky ovládána ze Spojených Států Amerických. Spolu s velkým rozšířením a sílícím vlivem politickým i ekonomickým, se zájmy jednotlivých národních vlád více zaměřily na tento fenomén a požadovaly spoluúčast na kontrole internetové komunikační sítě. Princip účinku, užitý v soudním judikátu Yahoo byl čím dál více aplikován jednotlivými vládami. Aby se předešlo fragmentaci sítě a tím i ohrožení její dosavadní globální existence, mezinárodní spolupráce a regulace se stala nezbytnou podmínkou dalšího vývoje. Nejdůležitější otázkou bylo, do jaké míry by měly jednotlivé státy mít vliv a kontrolu nad internetem, a v jakých aspektech je nezbytná regulace mezinárodní.

Regulace internetu (z originálního termínu „internet governance“) byl termín zpočátku nejasné definice. Tento termín se běžně užívá k popisu systému vládnoucích orgánů a regulačních opatření, které tyto orgány přijímají. V širším slova smyslu však může zahrnovat i

[50] Goldsmith and Wu 2006, str. 9 a 10.

[51] Akdeniz 2001, str. 6.

[52] Reidenberg 2001, str. 2 až 4.

veškeré subjekty a instituce účastnících se internetu. Na počátku mezinárodní debaty o regulaci internetu byla povaha možné budoucí mezinárodní „vlády“ internetu chápána jako záležitost čistě veřejnoprávní, tedy měla mít povahu mezivládního orgánu nebo spolupráce.[53] Postupně ale bylo přijato širší pojetí, a tudíž na ovládání internetu se podílí také nestátní instituce popřípadě subjekty soukromé povahy. Počátkem řekněme moderního pojetí internetové vlády byl světový summit o informační technologii (WSIS) v roce 2003 v Ženevě a 2005 v Tunisu. Jejich výsledkem bylo založení mezinárodního Fóra, které se poprvé sešlo v roce 2006 v Aténách pod záštitou Organizace Spojených Národů.[54] Jeho účastníky byli, jak již bylo zmíněno, jak zástupci států, tak občanské či obchodní společnosti. Pokud jde ovšem o jeho první výsledky, jde spíše o mezinárodní diskuzi, jejímž výsledkem není právně závazný dokument. Hlavním předmětem diskuze je bezpečnost internetu, zejména zabezpečení přenášených dat. Nejdůležitější posun však byl dosažen tím, že původně lokální síť ve Spojených Státech, která i po svém celosvětovém rozšíření neustále byla pod nadvládou a hlavní kontrolou USA, se postupně stává neutrálním prostředím. USA se vzdaly svého výsadního postavení ve prospěch neutrality a mezinárodní spolupráce zahrnující i tzv. internetový průmysl, například firmy jako Google nebo Yahoo. Tento trend se výrazně projevil založením mezinárodní instituce ICANN, která vystřídala původní americký systém registrace doménových jmen. Tato mezinárodní internetová vláda je na svém počátku, ovšem jejím nejdůležitějším úkolem je dát prostor pro mezinárodní jednání a zachování univerzální struktury internetu.

Jak bylo minulostí mnohokrát dokázáno, internet je fundamentálně odlišným komunikačním prostředím, které vyžaduje novou formu vlády a regulace. Toto tzv. chápání nové reality (new-cyber approach) se však nakonec zkombinovalo s přístupem založeným na tradicích již existujícího práva (old-real approach), který neviděl žádné velké odlišnosti internetu od jiných komunikačních systémů. Tudíž jednotlivé vrstvy, které budou popsány níže, se zejména vyznačují odlišnou formou regulace. Další diskuse o formě vlády a její struktury – zda má jít o centralizovanou či decentralizovanou. Podle povahy sítě je vhodnější způsob decentralizace, avšak z hlediska finanční, organizační i personální náročnosti, a v neposlední řadě též efektivnosti, vznikly centralizované mezinárodní instituce jako ICANN či W3C.[55] Je nezbytné

[53] Kurbalija 2005, str. 9.

[54] Mathiason, J. (2009) *Internet Governance The new frontier of global institutions*. UK, London: Routledge. str. 131 a násl.

[55] Ibid. str.18. ICANN (Internet Corporation for Assigned Names and Numbers), W3C (World Wide Web Consortium).

mít stále na paměti, že internet je prostředím, kde se střetávají často protichůdné zájmy. Tak většinou rozdílné zájmy má veřejný a soukromý sektor. Největší internetové společnosti lobbují za decentralizovanou a pokud možno co nejméně regulovanou povahu tohoto celosvětového obchodního trhu. Naopak státní orgány uplatňujíc státní suverenitu a funkce mají stále větší tendenci užívat své pravomoci i v tomto virtuálním prostředí. Neopomenutelné je i hledisko politické, pro které je internet dalším prostorem politických zájmů, odlišných systémů a mezinárodních taktik. Gicomello uvádí, že čím vyvinutější je stát, tím více je a bude závislý na počítačové síti jako je internet.[56]

Z jakého důvodu je co nejvíce jednotná regulace internetu třeba? Internet má čím dál větší dopad sociální, ekonomický i politický a tudíž otázka jeho právní regulace se stává velmi aktuální. Jednotná regulace je třeba mimo jiné k zabránění fragmentace internetu (aby si zachoval svůj jednotný a globální charakter), k zajištění kompatibility a součinnosti po celém světě, k ochraně práva a definování povinností jednotlivých subjektů účastnících se internetu, k ochraně konečných uživatelů a zároveň k předcházení zneužívání internetu, k ochraně veřejných zájmů a k podpoře dalšího rozvoje.[57]

Pokud jde o přístup k právní regulaci a ovládání internetu, lze rozeznat několik různých metod. Zejména lze odlišit přístup užší povahy, který byl zaměřen na infrastrukturu internetu, jako například doménová jména, IP adresy, servery apod.) a pozici ICANN jako nejdůležitějšího aktéra v této oblasti. Širší přístup zastával názor, že mezinárodní úprava by se měla zabývat též jinými aspekty, a tudíž by měla řešit i otázky právní, ekonomické či otázky dalšího technického rozvoje. Nakonec idea spolupráce v širším slova smyslu převážila.[58]

Hlavním úkolem regulace internetu je nalezení určité vyváženosti často protichůdných zájmů a práv. Tak například svoboda slova na straně je na straně jedné a ochrana veřejného pořádku na straně druhé, což vede k diskuzím o kontrole obsahu internetu a jeho cenzuře. Obdobně protichůdné jsou zájmy soukromé osoby a ochrana jejího soukromí a například bezpečnostní otázky jak státní tak soukromých subjektů jako (například bezpečnostní systémy

[56] Gicomello 2005, str. 4.

[57] Kurbalija, J. (2005) *An Introduction to Internet Governance*. [Online] last accessed 03/31/2010 <http://www.diplomacy.edu/ISL/IG/default.htm>, str. 7.

[58] Kurbalija 2005, str. 16.

jednotlivých společností). V této souvislosti jde zejména o otázky internetové kriminality a nutného monitorování internetu. V neposlední řadě internet je nejčastějším místem porušování práv duševního vlastnictví.

Pokud jde o přístup k právní regulaci technologií, je poměrně důležité upozornit na to, že technologický pokrok je v posledních letech velmi rychlý. Tudíž regulace a právní terminologie musí být velmi opatrná avšak dostatečně široká, aby se netýkala pouze dnešní technologie. Jde tedy spíše o stanovení objektu ochrany, než o konkrétní zakázané jednání.[59]

Při popisu struktury a regulace internetu se užívá tzv. vrstvovitý model, který se skládá ze tří vrstev, jež dohromady vytváří a umožňují fungování komunikace jako celku. Zároveň jde i o vrstvy právní, jelikož odlišné prostředky a subjekty hrají rozhodující roli v odlišné vrstvě. Ta nejspodnější vrstva je nazývána vrstvou fyzickou. Zahrnuje tedy veškerý hardware umožňující z technického hlediska komunikaci jako takovou. Jedná se například o počítače, kabely, bezdrátové vysílače a přijímače a podobně. Střední vrstva, tzv. logická nebo kódovací, zahrnuje univerzální technické standardy, protokoly a software (programy) v tom smyslu, aby byly vzájemně kompatibilní a byl zachován globální a univerzální charakter sítě. Nejvyšší úroveň je pak obsahová, obsahující aktuální informace přenášené prostřednictvím sítě, jako jsou texty, obrazové snímky a další.[60] Všechny tři vrstvy mají stejnou důležitost zejména z toho hlediska, že síť nemůže plnit svoji funkci při absenci kterékoli z nich. Na druhou stranu ke kontrole internetové sítě postačí mít pod kontrolou třeba jen jedinou vrstvu, jak bude dále ukázáno na příkladu autoritářských režimů.

Současná situace ukazuje, že státní vlády hrají určitou roli v každé vrstvě. Nejvíce a nejjednodušeji kontrolovaná je vrstva fyzická. Distribuce a obchod s hardware se řídí jednotlivým národním právem a je plně pod kontrolou tamní vlády. Vrstva kódovací je však odlišná. Samoregulační orgány mezinárodní povahy vznikly právě pro účely této velmi odborně náročné práce, a mnoho méně vyvinutých zemí nemá ani ambice mít vliv na vývoj a regulaci technických standardů ovládajících internetovou síť. Tak vznikla organizace ICANN (the Internet Corporation for Assigned Names and Numbers) přidělující a regulující globální doménová jména, či W3C (the World Wide Web Consortium) vyvíjející technické parametry a specifikace. Všichni, kdo mají své zájmy na internetu, jsou v této vrstvě za jedno. Cílem je

[59] Kurbalija 2005, str. 23.

[60] Lessig 2001, str. 23.

udržování a vývoj sítě tak, aby byla co nejvíce bezpečná, stabilní a rychlá. Obsahová vrstva je nejvíce komplikovaná a diskutovaná pokud jde o její regulaci, zahrnuje totiž ochranu práv duševního vlastnictví nebo lidských práv včetně soukromí.

1.5 Státní kontrola internetu v některých autoritářských režimech

Tato část uvádí několik příkladů, jakým způsobem v praxi může být jinak globální internetová síť kontrolována jednotlivými státy. Ačkoli se někdy ozývají hlasy, že díky přirozenosti a decentralizované struktuře internetu, nemůže být tento efektivně kontrolován žádným státem, zde jsou příklady dokazující opak.

Jak již bylo zmíněno, podstatou je vykonávání kontroly alespoň nad jednou z vrstev internetu. Tak Kuba chránící svůj politický systém izolovaný od okolního světa se vydala cestou nejrazantnější, když se rozhodla mít plně v moci fyzickou vrstvu. Tamní režim přísně kontroluje veškerou distribuci počítačů, která je téměř zakázána, až na výjimky většinou pro státní účely. Pokud již je přístup k počítači, který je připojený na internet, umožněn, přesto každý přenos zpráv či jakýchkoli informací je přísně monitorován. Ve své podstatě tedy touto cestou, která již od první pohledu dokladuje nízkou vyspělost a izolovanost kubánského režimu, dokázal jak internet, tak své obyvatelstvo udržet pod svojí mocí a kontrolou.[61]

Daleko více vyspělý a sofistikovaný systém je však v Číně. Čínská vláda si velmi uvědomuje finanční příležitosti plynoucí z obchodů uskutečňovaných v prostředí internetu. Navíc cílem tamního režimu zdaleka není naprostá izolace od okolního světa. Naopak mezinárodní obchod a zahraniční investice jsou jedním z hlavních finančních zdrojů komunistické Číny. Proto tento stát musí zajistit přístupnost internetové sítě a jejího používání. Na druhou stranu ale se však tento nedemokratický režim nechce vzdát své autority a snaží se tudíž přísně vykonávat kontrolu svých obyvatel včetně jejich činností na internetu. Tak jejich systém kontroly je založen na kombinaci různých metod. Obsah internetu je neustále monitorován a cenzurován tak, aby informace a materiály nekonzistentní s existencí a fungováním režimu nebyly přístupné čínskými obyvateli. Toto je prováděno technickými prostředky, zejména specifickými programy a jejich nastaveními. Vláda provádí průběžné monitorování provozu na internetu a to i tzv. red vests, což jsou specializovaní agenti, jejichž oficiálním posláním je obrana režimu.[62] Každá společnost podnikající prostřednictvím internetu na čínském území, musí mít licenci od vlády, jejíž podmínky vláda individuálně určuje tak, aby

[61] Kalathil and Boas 2001, str. 10.

[62] Bandurski 2008, str. 1.

každá i zahraniční společnost dodržovala praktiky a zájmy režimu. Tak například společnosti Yahoo či Google souhlasily s tím, že budou cenzurovat obsah přístupný těm, kdo se připojují z území Číny. Yahoo dokonce souhlasilo i s tím, že budě na vyžádání režimu monitorovat a poskytovat informace o jednotlivých uživatelích, kteří uskuteční jakoukoli činnost odporující zájmům komunistického režimu (například reportují majitele emailové schránky, ze které jsou posílány informace o lokální situaci či potlačování lidských práv zahraničním novinářům apod.). Lokální počítače je dovoleno mít vybavené pouze dovolenými programy, jejich distribuce je rovněž kontrolována. Navíc vláda užívá i metod užívaných v minulosti i ostatními komunistickými režimy, totiž v Číně je velké množství lidí vyhledávajících, popřípadě skrytě podporujících, různá fóra, aby následně mohli upozornit úřady na každé politicky závadné uživatele. Jak je vidět, stát využívá veškerých dostupných prostředků k tomu, aby své obyvatelstvo udržel pod kontrolou, což se mu velmi efektivně daří. Přesto si ale nelze nevšimnout postupného pozitivního vlivu internetové sítě, která přispívá k demokratizaci Číny.

Tai uvádí některé příklady, jak internet pozitivně ovlivnil či urychlil společenské i politické změny v Číně směrem k větší demokratizaci režimu.[63] Uvádí, že internet umožnil poměrně lehkou komunikaci a přenášení informací napříč čínskou společností (navíc mnoho lidí nachází technické prostředky, jak obejít oficiální filtry a zajistit si tak přístup ke všem materiálům a informacím na internetu). Internet také poskytuje prostředí pro politické debaty jak o společenských, tak o politických tématech, které v některých případech nakonec i samotná vláda vzala pozitivně v potaz. Navíc je i prostředkem, jak si udržet vlastní úsudek a vyvinout nezávislé názory, které nejsou založené pouze na zkreslených informacích jinak podávaných tamním režimem. Lidé tak můžou své názory sdílet a diskutovat (ačkoli samozřejmě anonymně) mohou formovat aktivistické či protestní akce, jako například signatářské kampaně a podobně. Tai uvádí, že vláda je daleko více tolerantní k těmto formám vyjádření nesouhlasu s oficiálním stanoviskem a režimem, než je tomu ve fyzickém, reálném světě, kde každé shromáždění lidí je velmi rychle a tvrdě rozehnáno či jinak ukončeno.

Přesto však Tai ukazuje i na přetrvávající problémy, jako je stále poměrně malé procento obyvatel, kteří jsou připojeni na internetu, nebo k němu mají alespoň běžný přístup. Tím se i prohlubují rozdíly mezi rozvinutými a méně ekonomicky důležitými částmi země. Zároveň

[63] Tai 2006, str. 289 – 292.

poukazuje na stále slabou občanskou společnost, která se však díky internetu začíná rozvíjet a nabývat na aktivitách i významu.[64]

Čína poměrně tvrdě zareagovala na hrozbu v roce 2005, kdy čínský žurnalista poslal politicky nesouhlasný email na webové stránky hostované v USA, avšak naneštěstí tuto zprávu odeslal ze schránky zřízené u společnosti Yahoo. Ta však poskytuje spolupráci a informace čínské vládě, tudíž jméno žurnalisty se velmi rychle dostalo do vědomí úřadů, které jej zatkly a uložily deset let odnětí svobody. Tento případ vzbudil velkou pozornost zastánců lidských práv z různých částí světa, a Yahoo tak čelila negativním kritikám. Avšak odpověď byla velmi jednoduchá a odůvodněná tím, že každý podnikatel musí dodržovat zákony toho státu, ve kterém podniká.[65] Jedním ze současných sporů vzbuzujících pozornost zahraničních médií je mezi čínskou vládou a americkou společností Google. Tato v roce 2006 vstoupila na čínský trh a souhlasila s prováděním cenzury materiálů tak, aby nebyly všechny přístupné čínskému obyvatelstvu. Avšak v roce 2009 na objednání čínské vlády se několik hackerů nabouralo do bezpečnostního režimu Google a získali údaje a přístup ke schránkám elektronické pošty politických aktivistů a žurnalistů. Tento případ je problematický hned z několika důvodů. Jednak znovu poukázal na stále přetrvávající autoritářský režim, jehož projevy jsou zejména v omezování lidských práv a nerespektování soukromé sféry. Dalším velmi problematickým faktorem je hacking či jiné způsoby nabourávání bezpečnostních systémů internetových společností, protože jejich vývoj a přenastavení představuje obrovské finanční náklady. Tudíž se společnost Google rozhodla, že cenzurovat obsah internetu podle tamní vlády již nebude, což pravděpodobně povede k úplnému opuštění čínského trhu.[66] Pokud však jde o ostatní společnosti, jako již několikrát zmíněnou firmu Yahoo a další, tyto se k případu vůbec nevyjadřují a tiše nadále v cenzuře a porušování lidských práv pokračují.

Na případu Číny lze však nejlépe demonstrovat, jak i vliv globálního internetu může napomáhat demokratickému šíření hodnot lidských práv, jemuž se i ty nejvyspělejší systémy jen těžko mohou bránit.

[64] Tai 2006, str. 289 – 292.

[65] Goldsmith and Wu 2006, str. 10.

[66] Helft and Barboza 2010, str. 1.

2. Regulace internetu z pohledu ochrany soukromí a osobnosti

2.1 Obecná východiska

Jedna z klasických definic stanoví, že soukromí je nárok fyzických osob, skupin či institucí na určení, kdy, jak a v jaké míře jsou informace o něm sdělovány ostatním. S ohledem na moderní techniku pak existuje pojetí, že soukromí znamená schopnost a možnost subjektu kontrolovat oběh informací o něm. [67]

Otázka soukromí a ochrany osobních údajů je čím dál více aktuální, zejména v kontextu používání internetové sítě. Nejvíce citlivou otázkou je nalezení vyváženosti mezi ochranou individuální osoby a jejího soukromí, a protichůdnými zájmy, jako například ochrana před porušováním práv druhých (zejména z porušování práv k duševnímu vlastnictví), v souvislosti s monitorováním a vyšetřováním trestné činnosti, nebo v souvislosti s ochranou veřejných zájmů například bezpečnosti státu a boj proti terorismu. Zejména v posledních letech se z důvodů bezpečnostních i častého porušování práv k duševnímu vlastnictví právě pomocí internetové sítě v některých státech, například ve Velké Británii nebo Francii, upouští od důsledné ochrany individuální osoby a její identity ve prospěch zvýšení efektivity a vymáhání práv v souvislosti s internetovou sítí. Uvedené země přijaly nová legislativní opatření, která na úkor ochrany soukromí individuální osoby mají zvýšit bezpečnost internetu efektivitu vymáhání práv v jeho prostředí (viz. kapitola postavení ISP). Někteří autoři dokonce polemizují o konci práva na ochranu soukromí, jakmile se člověk stane uživatelem internetové sítě a poskytne komukoli na ní své osobní údaje či informace.[68] Z pohledu ohrožení soukromí jsou nejvíce diskutovány následující aspekty: 1) Nepřesnost a nekorektnost údajů z různých zdrojů může dát dohromady obraz, který vůbec neodpovídá realitě a pravdivosti o dané osobě či situaci. 2) Nedostatečná kontrola dotčené osoby nad svými údaji a jejich shromažďováním, jenž je výsledkem velmi širokého sledování a monitorování internetu či jiných elektronických sítí, aniž by došlo k obdržení předchozího souhlasu dotčené osoby. 3) Internet může zapříčinit ohrožení důstojnosti a

[67] Edwards a Waelde 2009, str. 304.

[68] McArthur, R., L. (2001) *Reasonable expectations of privacy*. Ethics and Information Technology 3: 123 – 128. dostupné též na adrese <http://collections.lib.uwm.edu/cipr/image/24.pdf>.

společenského postavení osoby při užití či zneužití údajů získaných bez vědomí a souhlasu dotčené osoby.[69]

V zásadě je nutné odlišit dva druhy vztahů, při kterých dochází k omezení práva na soukromí. Jsou to vertikální vztahy, kdy soukromá osoba jedná ve vztahu k orgánu veřejné moci v případě realizace jeho zákonné pravomoci, se nemůže osoba dovolávat soukromí, je-li toto omezení na základě a v rámci zákonného zmocnění. Častěji však dochází ke střetům a sporům, pokud zásahy do soukromí přichází ze strany osoby se stejným postavením, tedy tzv. horizontální vztahy (mezi osobami stejného postavení).[70]

V nejobecnější rovině lze konstatovat, že dochází ke střetu a nalézání vyváženosti mezi právem na informace a svobodu projevu (čl. 10 odst. 1 Evropské úmluvy) s právem na soukromí (jež garantuje Evropská úmluva ve čl. 8). Podle evropského přístupu ani jedno z těchto práv však nemá prioritu. Záleží tedy na soudech, aby každý konkrétní případ posoudily. Zejména tzv. osoby veřejného zájmu jsou nuceni strpět větší míru zásahů do svého soukromí než ostatní obyvatelé (jde například o politiky, umělce, sportovce apod.), jelikož je v zájmu veřejnosti vědět o těch, kdo například rozhodují o důležitých otázkách státu, daleko více informací, než o jakékoli jiné soukromé osobě. Zásahy do jejich soukromí by však neměly přesahovat určité meze, kdy zájem veřejnosti již nemůže ospravedlnit zásahy například do intimních sfér dané osoby.[71] Pojetí ve Spojených Státech jde dokonce ještě dál a klade velmi přísný důraz na neomezenou svobodu projevu, která je na rozdíl od práva na ochranu soukromí, výslovně garantována tamní ústavou. O interpretaci směrem k co nejširšímu pojetí svobody projevu pojednává i Herceg v kontextu šíření rasistických či extremistických myšlenek, kdy dokonce i v této kriminální činnosti je tamní svoboda slova hájena s tím, že její omezení je přípustné pouze tehdy, když násilí nebo porušení práva bezprostředně hrozí.[72] Mates také uvádí, že podle tamního Nejvyššího soudu nelze

[69] Rowland a Macdonald 2005, str. 303.

[70] Mates, P. 2006, str. 23.

[71] Otázkou ochrany soukromí veřejných osob se zabýval například Ústaní soud Německa ve věci Caroline von Hannover.

[72] Herceg, J. (2008) *Extremismus a hranice svobody projevu na internetu.* Český právní řád a ochrana kyberprostoru (vybrané problémy), Acta Universitatis Carolinae, Iuridica 4/2008. Praha: Nakladatelství Karolinum, str. 47.

například u politiků rozlišovat mezi soukromým a veřejným životem.[73] Pojetí a důsledky těchto práv budou detailněji představeny v další části této práce.

Pokud jde o ochranu osobnosti, je důležité mít na paměti zásadní rozdíl v přístupu kontinentálního právního systému s tradičním přístupem systému anglosaského. Zatímco v kontinentálním systému existuje tzv. všeobecné osobnostní právo, které zjednodušeně znamená právo osobnosti na ochranu všech nehmotných hodnot lidské osobnosti v jejím celku, tedy v její fyzické a morální jednotě. Je to teda souhrn všech jednotlivých dílčích osobnostních práv (jejich výčet je v zákonech demonstrativní), která jsou spjata s každou fyzickou osobou.[74] Jen pro úplnost dodávám, že vedle všeobecného osobnostního práva existují též osobnostní práva zvláštní (např. práva autorů podle AZ), jimiž se však tato práce dále specificky zabývat nebude.

V prostředí anglosaském koncepce všeobecného osobnostního práva neexistuje. Proto právní úprava, která však v některých oblastech je obdobná té naší díky harmonizačním nástrojům evropské unie, se omezuje pouze na konkrétní aspekty ochrany osobnosti prostřednictvím specifických žalob (např. ochrana před pomluvou či urážkou na cti, tzv. defamation a libel vycházejícího z common law, či podle zvláštních zákonů). Anglická teorie někdy rozlišuje dva právní aspekty ochrany osobnosti. V pozitivním slova smyslu, kdy zákon dává v souvislosti s ochranou osobních údajů a soukromí určitá pozitivní práva subjektu osobních údajů (například právo na informace), tam se řadí zejména zákon o ochraně osobních údajů z roku 1998 (dále jen DPA)[75], který provedl směrnici (dále též DPD)[76] harmonizující právní úpravu v zemích Evropské Unie, a dále pak PECR,[77] které provedlo směrnici o soukromí a elektronických komunikacích (PECD).[78] Na druhou stran lze charakterizovat i pojetí v negativním slova smyslu, které je vyjádřením práva na to, aby nebylo zasahováno do určitých soukromých oblastí daného subjektu. Sem se řadí například právo ochrany důvěrných informací,

[73] 2006, str. 28 a 29.

[74] Knap, K. a kol. (2004) *Ochrana osobnosti podle občanského práva*. 4. vydání, Praha: Linde, str. 17.

[75] The Data Protection Act 1998.

[76] Směrnice Evropského Parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (the Data Protection Directive).

[77] The Privacy and Electronic Communications Regulations 2003, SI 2003 No 2426.

[78] Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací.

které je součástí common law, ovšem v posledních letech bylo téměř celé nahrazeno přijetím Evropské úmluvě o ochraně lidských práv a základních svobod 1950 a jejího článku 8 (dále jen Úmluva či Evropská úmluva). Úmluva byla inkorporována do britského právního systému zákonem v 1998.[79] Velká Británie je příkladem monistického právního režimu, tudíž každá mezinárodní smlouva se stane jeho součástí až po přijetí zvláštního zákona, na rozdíl například od naší právní úpravy v režimu článku 10 Ústavy.

Pokud jde o první oblast, jde o ochranu určitých osobních údajů, jako například jména, adresy, data narození, detailů týkajících se zdravotní, finanční či sociální situace, rasové či etnické příslušnosti, anebo například fotografie, na kterých lze danou osobu identifikovat. Zjednodušeně řečeno poskytuje dané osobě pozitivní právo na kontrolu toho, co je o ní ostatním známo. Jde tedy o ochranu v pozitivním slova smyslu.

Druhá oblast naopak v negativním smyslu, zakazuje totiž ostatním subjektům poskytnutí nebo vyzrazení informace, která by měla být udržena v soukromí, jen mezi daným subjektem a tím, koho se tato informace týká.

Pojetí v článku 8 Evropské úmluvy bylo původně určeno k poskytnutí ochrany soukromých osob před státem, zejména díky zkušenostem z Východního bloku v průběhu studené války, kdy státní aparáty shromažďovaly široké informace zejména z politických důvodů.[80] S koncem tohoto období a rozvojem demokratické společnosti v Evropě se důraz na lidská práva včetně ochrany soukromí ještě zvýšil. Zejména v post-socialistických zemích je ochrana soukromí a osobních údajů poměrně citlivou společenskou otázkou. S postupným rozvojem informační společnosti se však tento trend začíná obracet. Edwards dokonce uvádí extrémní názor, že dnešní společnost „slepě kráčí do společnosti plně sledované“.[81] Digitální prostředí totiž umožňuje snadný přístup, shromažďování i udržování osobních údajů, které mohou být a také bývají použity k různým účelům. Například jednotlivé subjekty různé databáze kombinují, čímž lze ve výsledku získat velmi podrobný přehled osobních informací o dané osobě. Takto lze pak na určitý okruh osob zaměřit například marketingové kampaně. Právní normy se snaží na tento jev reagovat tím, že regulují jak dobu, po kterou lze osobní údaje uchovávat, tak účel, za kterým si je možné takové

[79] The Human Rights Act 1998.

[80] Edwards a Waelde 2009, 448 až 451.

[81] Ibid, str. 448.

údaje ponechat a použít. Více podrobností bude uvedeno v části týkající se ochrany osobních údajů.

Pokud však jde o trend vývoje, nelze nevidět ještě jeden aspekt, který má co dočinění s bezpečností a ochranou veřejných zájmů. Obecně se totiž přístup některých států výrazně přiklonil k omezení ochrany soukromí a individuálních osobností zejména díky vývoji po teroristickém útoku 9. září v USA a následnému boji proti terorismu. Ty státy, které jsou nejvíce ohroženy, jako je USA nebo UK, tudíž kladou výrazně vyšší důraz na bezpečnost a předcházení trestné činnosti před ochranou osobnosti. Obdobně i například opatření, které mají zajistit vyšší právní jistotu a efektivitu v internetovém prostředí (například v souvislosti s trestněprávní problematikou nebo s ochranou práv k duševnímu vlastnictví), mají poměrně zásadní dopad na omezení ochrany soukromí a zpracování osobních údajů internetových uživatelů. Jaký je přístup některých právních systémů a jak efektivní ochrany osobních údajů lze dosáhnout, to bude dalším tématem následujících částí této práce.

2.2 Ochrana soukromí vs. Svoboda slova

Tato základní lidská práva jsou vyjádřena v podstatě všemi dokumenty garantujícími ochranu lidských práv a svobod ať již na mezinárodní, evropské či vnitrostátní úrovni. Univerzální deklarace lidských práv 1948 ve svém článku 12 zaručuje právo na ochranu svého soukromí i osobnosti. Naproti tomu článek 19 deklaruje každému právo na svobodu slova a právo na informace bez ohledu na státní hranice. Obdobně je tato otázka upravena v Evropské úmluvě o ochraně lidských práv a základních svobod 1950, ve článku 8 a 10. Jak je však patrné, tyto svobody se vzájemně střetávají a je důležité najít jejich vyváženost. V prostředí internetu je situace komplikovanější zejména díky přirozené povaze internetu jako globálního media, kdy se do vztahů (ať již právních či protiprávních) dostávají lidé z různých částí světa. Otázka mezinárodní spolupráce a vymáhání práv různých právních řádů tudíž nabývá na důležitosti.

2.2.1 Svoboda slova

Jak již bylo konstatováno v této práci, Spojené Státy Americké již tradičně mají velmi silnou ochranu svobodu slova, kterou jim zaručuje první dodatek ústavy. Soudy ve velké většině případů upřednostňují právě tuto svobodu před ostatními právy jako právě třeba na ochranu osobnosti a jejího soukromí. Důkazem toho byl například případ Nejvyššího soudu ALCU

v Reno v roce 1996,[82] který zrušil nově přijatý zákon na ochranu soukromí při komunikaci (the Communications Decency Act 1996) s odůvodněním, že případné protiprávní chování podle tohoto zákona nebylo dostatečně konkrétně definované a tudíž by vedlo k nepřípustnému omezení svobody slova. Obdobně hraje tato svoboda důležitou roli v případě uznávání a vymáhání cizích soudních rozhodnutí. Kromě toho bylo též považováno za nepřípustné a nepraktické (mimo jiné i z finančních důvodů), aby ISPs kontrolovali obsah přenášených dat a případně jej cenzurovali, pod hrozbou nepřímé odpovědnosti. Tak v případě Yahoo (viz. první část této práce) bylo odmítnuto uznání a výkon francouzského soudního rozhodnutí právě díky nedostatečné konkrétnosti nařízených opatření.

Velmi veřejností sledovaný případ byl také v Německu, European Commission Communication, Illegal and harmufl content on the Internet[83] v roce 1999. Šlo o evropskou iniciativu k zavedení nové metody regulace obsahu internetu, který porušuje zákon, uvalením povinností na ISPs. Tito podle nového přístupu mají povinnost blokovat své zákazníky v přístupu k nezákonnému obsahu internetu na bázi jednotlivých případů (například určité stránky, apod.). V tomto případě došlo k požadavku ze strany německých státních zástupců, aby ISPs blokovali přístup k určitým stránkám hostovaným serverem v Nizozemí údajně podporující terorismus. Ovšem blokace znamenala zablokování přístupu ke všem stránkám tohoto serveru, tedy i těch v souladu se zákony. Proto ze strany nizozemské společnosti došlo k žalobě o porušení svobody poskytování služeb v rámci zemí EU.[84]

Problematický je však aspekt, že efektivně lze vymoci případné rozhodnutí proti hostiteli takových serverů jedině tam, kde je obdobné jednání rovněž zakázáno (podle zásady oboustranné protizákonnosti v případě uznávání soudních nebo jiných rozhodnutí). V prostředí internetu je však jednoduché přesunout své služby na území, kde takové jednání je povolené a nadále v něm pokračovat. Někdy obdobná možnost může sloužit k legitimním účelům (např. protestní skupiny proti omezování lidských práv v Číně), jindy však naopak (např. němečtí příznivci nacismu užívají a diskutují fašismus a své názory prostřednictvím stránek hostovaných serverem v USA či Kanadě, protože jejich jednání je trestné podle německého trestního práva.[85]

[82] ALCU v Reno 929 F Supp 824 (ED Pa, 1996).

[83] COM(96)0487 – C4-(0592/96).

[84] Reed 2004, str. 259 a 260.

[85] Ibid, str. 261.

2.2.2 Ochrana soukromí

Ochrana soukromí v ústavním pořádku ČR je zakotvena v Listině základních práv a svobod, kdy v článku 7 je zaručena nedotknutelnost osoby a jejího soukromí, a v článku 10 je garantováno právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života. Je pochopitelné, že znění a způsob úpravy je inspirován mezinárodněprávními dokumenty, článkem 8 Evropské Úmluvy a článkem 17 Mezinárodního paktu o občanských a politických právech z roku 1977. Zvláštním případem ochrany soukromí je pak ochrana osobních údajů podle článku 10 odst. 3 Listiny.

Jednotlivé státy se velmi liší v přístupu a odlišení toho, jaké informace se považují za osobní a soukromé, a které mohou být veřejně přístupné bez omezení. Reed uvádí, že ve Švédsku se například daňové přeplatky považují za veřejně přístupnou informaci, naopak ve Francii se však i telefonní účty považují za čistě soukromou záležitost.[86]

Pokud jde o procesní otázky, mechanismy sbírání a následného nakládání s osobními údaji, poměrně extrémní volnost je garantována v USA, kde většina úpravy je ponechána samosprávě a samoregulaci daného průmyslového odvětví, a k vymáhání dochází jedině na základě individuální žaloby. Proto, pokud jde o dopad tamní právní úpravy, tento je poměrně nezásadní v rámci mezinárodního prostředí.

Naopak nejpřísnější úprava, která má poměrně zásadní dopad fakticky po celém světě, je úprava evropská, zejména na základě směrnice č. 95/46/ES.[87] Jedním z následujících důležitých kroků však bude spolupráce s USA. Ministerstvo financí US sestavilo základní principy tzv. bezpečného přístavu (území EU a USA) v roce 1999, které reagují a v podstatě odráží základní principy směrnice.[88] Například Goldsmith uvádí, jak fakticky evropská úprava soukromí a osobních údajů má dopad celosvětový. V roce 1999 totiž společnost Microsoft představila produkt „do-NET Passport“, který měl usnadnit práci uživatelů na internetu zejména tím, že shromažďoval veškerá hesla a údaje nutné k přístupu k různým službám. Ovšem standardy zpracování, zabezpečení a nakládání s takto shromážděnými daty neodpovídaly legislativě evropské a důrazu na ochranu těchto dat. Goldsmith uvádí, že evropská směrnice a legislativní přístup je poměrně agresivní pokud jde o její teritoriální dopad. Vztahuje se totiž nejen na subjekty evropské, ale v podstatě na všechny společnosti na evropském trhu působící. Proto

[86] 2004, str. 263.

[87] o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

[88] US Department of Commerce (1999) *International Safe Harbor privacy principles*. [online] Dostupné na adrese <http://www.ita.doc.gov/td/ecom/Principles1199.htm>.

Microsoft měl v podstatě pouze dvě možnosti, buď opustit evropský trh, což je třetina jeho celkového světového trhu, anebo být v souladu s tamní legislativou. Z toho důvodu se vydal druhou cestou, ovšem z ekonomických i dalších důvodů proto celý systém bez ohledu na geografické odlišnosti nastavil dle přísnějšího evropského práva.[89]

2.3 Ochrana osobnosti (obecná ochrana podle české právní úpravy)

Nejširší úprava ochrany osobnosti je obsažena v Listině základních práv a svobod, která je východiskem pro navazující veřejnoprávní i soukromoprávní zákonnou úpravu.[90] Základem všeobecné soukromoprávní úpravy je hlava druhá zákona č. 40/1964 Sb., občanského zákoníku (dále jen OZ), Ochrana osobnosti (§ 11 až 16). V kontextu internetu je dále také významná úprava provádějící evropskou směrnici č. 95/46/ES v zákoně č. 101/2000 Sb., (idea zakotvená v čl. 10 odst. 3 Listiny) o ochraně osobních údajů v informačních systémech, jehož porušení může mít trestněprávní důsledky.

Prostředky ochrany zahrnují jak svépomoc, dožádání ochrany od orgánu státní správy, tak zejména ochranu soudní. Vedle těchto prostředků existuje podle zákona č. 101/2002 Sb. také institucionální ochrana poskytovaná Úřadem pro ochranu osobních údajů a zvláštní soudní ochrana podle tohoto zákona, ke které je příslušný obecný soud, tedy okresní. Kromě těchto standardních prostředků lze samozřejmě žádat případnou ochranu i pomocí ústavní stížnosti podle čl. 87 odst. 1 písm. d) Ústavy a § 72 odst. 1 písm. a) zákona č. 182/1993 Sb., o Ústavním soudu. Mimo vnitrostátní ochranné prostředky je nutné zmínit i systém ochrany podle Evropské úmluvy a jejího protokolu č. 11, Evropský soud pro lidská práva. Navíc významnou se jeví i činnost Veřejného ochránce práv.[91]

Zásahy do všeobecného osobnostního práva a jeho omezení jsou přípustné v několika případech. Jednak je tomu na základě vůle dotčené fyzické osoby, tedy s jejím svolením, anebo bez ohledu na vůli této osoby, dovoluje to některý ze zákonů. Jde o tzv. zákonné licence obsažené v § 12 odst. 2 a 3 OZ, a dále může jít o konkrétní případy podle zvláštních zákonů. I zde základním pravidlem je přiměřenost zásahu pouze v rozsahu nezbytném k danému dovolenému účelu.[92]

---

[89] Goldsmith a Wu 2006, str. 173 až 177.

[90] Knap, K. a kol. (2004) *Ochrana osobnosti podle občanského práva*, 4. vydání, Praha: Linde, str. 19.

[91] Knap, K. a kol. 2004, str. 36.

[92] § 12 odst. 3 OZ.

Zejména pokud jde o svolení, je důležité mít na zřeteli, že jde o právní úkon, který musí splňovat veškeré obecné náležitosti. Tedy musí být učiněna osobou k němu způsobilou, musí být její vůle projevena svobodně, vážně, určitě a srozumitelně, bez omylu či v tísni za nápadně nevýhodných podmínek. Zároveň nesmí svolení být v rozporu se zákonem, obcházet jej či se příčit dobrým mravům.[93] Pokud jde o formu, ke svolení může dojít různou formou, tedy jak písemnou, tak ústní či konkludentní, nevyžaduje-li zákon v konkrétním případě jinak. Tak například dobrovolnou účast na reklamním fotografování lze považovat za konkludentní souhlas. Na druhou stranu však je nutné upozornit, že každá osoba může kdykoli bez odůvodnění svůj souhlas odvolat. V některých případech lze však souhlas vzít zpět jen do okamžiku, dokud není zásah do osobnostního práva proveden (jako například při lékařském zákroku).

Zákonné licence podle občanského zákoníku jsou dvojího druhu. Za prvé jde o licence pro úřední účely na základě zákona (nestačí předpis nižší právní síly), § 12 odst. 2 OZ, například pro účely soudního či jiného řízení. Tyto jednotlivé případy stanoví zvláštní zákony upravující právní vztahy v konkrétních situacích (například odposlouchávání podle § 88 a násl. zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád). Za druhé jde o případ, kdy jde o vědecké a umělecké účely, dále i pro účely tiskové, filmové, rozhlasové a televizní zpravodajství, § 12 odst. 3 OZ. Zejména tzv. zpravodajská licence musí však být odůvodněna zájmem veřejnosti, který v konkrétním případě převáží zájem dotčené osoby na ochraně její osobnosti. I přesto však musí jít o přiměřený zásah nikoli v rozporu s oprávněnými zájmy dotčené osoby, jak dále uvádí tentýž odstavec.

2.3.1 Sankce a prostředky ochrany

Systém sankcí za porušení či ohrožení všeobecných osobnostních práv lze rozlišit dle povahy na soukromoprávní (podle § 13 a 16 OZ) a veřejnoprávní (včetně trestněprávních).

Soukromoprávní sankce podle občanského zákoníku jsou obsaženy v § 13 a 16 jsou zvláštními prostředky, kterým zahrnují možnost domáhat se uložení povinnosti upuštění od neoprávněného zásahu, odstranit jeho následky, či poskytnout přiměřené zadostiučinění (morální či peněžité). K sankcím ve formě uložení některé z výše uvedených povinností může dojít již při ohrožení chráněných zájmů, přičemž vzniklá újma dotčené osoby může být jak majetkové tak nemajetkové povahy. Sankce za nemajetkovou újmu podle § 13 vznikají na základě přísného objektivního principu, tedy bez ohledu na zavinění ze strany původce.[94] Nelze se tedy

[93] Knap, K. 2004, str. 108.

[94] Ibid. str. 146.

odpovědnosti zprostit například nevědomostí či jinak omluvitelným omylem. Toto je hlavní rozdíl od sankcí veřejnoprávních, kde je určitá forma zavinění vždy vyžadována. Odůvodněnost lze spatřovat v zájmu na nápravě protiprávního stavu, který znamená újmu pro dotčenou osobu, bez ohledu na to, jak k ní došlo.

V případě odpovědnosti za majetkovou újmu vyčíslitelnou v penězích vzniká odpovědnost za škodu podle § 16 OZ, která případně vznikne vedle odpovědnosti podle § 13 OZ. V dalším se řídí tato odpovědnost podle obecných ustanovení odpovědnosti za škodu podle § 415 a násl. OZ, může tedy dojít k její náhradě jak náhradou peněžení, tak naturální restitucí (uvedením v původní stav). Jejím cílem je tedy kompenzace vzniklé majetkové újmy, která je však založena na principu presumovaného zavinění podle § 420 odst. 1 a 3 OZ.

Jak tedy vyplývá z výše uvedeného, pokud jde o finanční kompenzaci, ve většině případů dochází ke kumulaci objektivního přiměřeného zadostiučinění v penězích podle § 13 OZ a odpovědnosti za škodu podle § 16 OZ.

Zásadním principem a předpokladem odpovědnosti za nemajetkovou újmu, který je někdy označován za zásadu adekvátnosti, je objektivní (nikoli subjektivní názor dotčené osoby) způsobilost zásahu vyvolat újmu, v případě nemajetkové újmy postačující ohrožení fyzické či morální integrity dotčené fyzické osoby. Jinými slovy, postihována nemají být taková jednání, která jsou svojí povahou přiměřená a odpovídající demokratické společnosti.[95] Díky tomuto principu musí dojít například při zásahu do cti ke komunikaci se třetími osobami nebo zpřístupnění této informace třetím osobám, což musí žalobce prokázat. Kromě tohoto principu je nutné splnit další podmínky k oprávněnosti sankčního požadavku: musí jít k zásahu neoprávněnému (tedy bez svolení dotčené osoby či mimo zákonné licence) a musí být prokázán kauzální nexus mezi neoprávněným zásahem a vzniklou újmou.

Občanský zákoník přece jen však poskytuje liberační důvody. Tak v případě tzv. důkazu pravdy je vyloučena odpovědnost původce za újmu na cti podle § 13. Toto však neplatí v případě osobního soukromí fyzické osoby, tzv. intimní sféru, kde i pravdivé tvrzení představuje neoprávněný zásah. Smyslem je totiž vyváženost veřejného zájmu a informace a ochrany osobní sféry dotčené osoby. Nelze tedy rozumně odůvodnit veřejným zájmem právě zásah do intimních záležitostí.

[95] Knap, K. 2004, str. 150 a 151.

V případě majetkové újmy je předpokladem vzniku oprávněného nároku na její náhradu vyžadován protiprávní úkon, vznik majetkové újmy vyjádřitelné v penězích, příčinné souvislosti a zavinění (ve formě úmyslu či nedbalosti).

Prostředky občanskoprávní ochrany teorie dělí na obecné (společné jako k ochraně jiných subjektivních práv) a zvláštní. Mezi obecné se běžně řadí svépomoc (§ 6 OZ), nutná obrana (§ 418 odst. 2 OZ), ochrana příslušným orgánem státní správy (§ 5 OZ) a ochrana soudní. Pod soudní ochranou si lze představit ochranu před zahájením řízení,[96] předběžná opatření,[97] zvláštní žaloby (viz. dále) a žaloba na náhradu škody.[98] Knap uvádí, že výčet ochranných nástrojů v § 13 OZ je demonstrativní, proto se lze žalobou domáhat i jiných výroků, například konstatování nepravdivosti daného tvrzení.[99] Kromě toho si lze představit i obchodněprávní žaloby na ochranu obchodního tajemství podle § 18 n. ObchZ[100] či na ochranu před nekalosoutěžním jednáním podle § 44 n. ObchZ.

Co se týče zvláštních prostředků ochrany podle § 13 OZ, jde o nástroje, které mají svojí konstrukcí poskytnout co největší ochranu subjektivních práv a mají v praxi také největší význam. Jedná se, jak již bylo řečeno výše, o žalobu negatorní (upuštění od neoprávněných zásahů), odstraňovací (odstranění nepříznivých následků neoprávněných zásahů) a satisfakční (poskytnutí přiměřeného zadostiučinění). Přičemž podle konkrétního případu lze tyto žalobní nároky kombinovat a doplňovat tak, aby v daném případě byly co nejpřesnější a nejúčinnější. Vždy je však nutné mít na paměti obecné náležitosti žaloby (či jiného právního úkonu), a to, že musí být dostatečně určitá a musí být patrno, čeho se žalobce (navrhovatel) domáhá.[101]

Pokud jde o příslušnost soudů, v prvním stupni jsou příslušné soudy krajské, jak uvádí § 9 odst. 2 písm. a) OSŘ. Je-li však s návrhem na ochranu osobnosti podle § 13 OZ spojen i návrh jiný, krajský soud rozhodne pouze o té části spadající pod výše uvedené ustanovení a v ostatních

[96] Smírčí řízení podle § 67 n. OZ.

[97] § 74 OZ.

[98] Knap, K. 2004, str. 171.

[99] Ibid. str. 174.

[100] Zákon č. 513/1991 Sb., obchodní zákoník (dále jen ObchZ).

[101] Knap, K. 2004, str. 176.

věcech věc postoupí k jednání a rozhodnutí příslušnému okresnímu soudu.[102] Navíc podle § 100 odst. 2 OZ je nutné mít na paměti, že všeobecná osobnostní práva jsou nepromlčitelná.

Vedle ostatních prostředků je zajištěna ochrana i v oblasti trestněprávní, a to zejména podle § 180 a násl. zákona č. 40/2009 Sb., trestního zákoníku (dále též TZ), který upravuje trestné činy proti právům na ochranu osobnosti, soukromí a listovního tajemství.

Tak podle § 180 se trestného činu neoprávněného nakládání s osobními údaji ten, kdo způsobí svým neoprávněným činem vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají. Navíc postihnutelné je jak úmyslné, tak nedbalostní jednání, jak vyplývá z dikce zákona. Odstavec třetí pak považuje spáchání činu veřejně dostupnou počítačovou sítí, kterou je například internet, za zvlášť účinný prostředek, který je podmínkou uložení vyšší sankce. Nutné je též dodat, že ke spáchání daného činu dojde již samotným neoprávněným zpřístupněním dotčených osobních údajů, tedy tím může být i prosté umístění daných údajů na webové stránky.

§ 182 TZ upravuje trestných čin porušení tajemství dopravovaných zpráv. Chráněným objektem v této souvislosti je tajemství zpráv jakékoli povahy, tedy jak písemností, tak i jiných záznamů například zvukových, obrazových či datových, zasílaných poštou či jiným způsobem, či zpráv podávaných telefonem, nebo prostřednictvím sítě elektronických komunikací. Podle § 183 TZ je pak ochrana poskytnuta i dokumentům, které nejsou přepravovány, ale jsou uchovávány v soukromí. V každém případě však musí jít o úmyslné zavinění. Pokud však jde o dokumenty uchovávané v soukromí, k naplnění skutkové podstaty nepostačí pouhý přístup k danému dokumentu pro sebe, ale až jeho zveřejněním, zpřístupněním či použitím jiným způsobem.

Odposlouchávání a záznam telekomunikačního provozu je dovolen pouze za podmínek § 86 až 87c TŘ, popřípadě sledování osob a věcí podle § 158d odst. 3, 4 TŘ, a při kontrole písemného styku k tomu povolanými orgány. Kromě zmocnění podle trestního řádu může také dojít k omezení zásahem BIS podle ustanovení § 7 až 12 zákona č. 154/1994 Sb., o Bezpečnostní informační službě, anebo složky zpravodajské či vojenského zpravodajství.[103] Posledním subjektem, který může zákonně za stanovených podmínek zasáhnout do tajemství

[102] Knap, K. 2004, str. 176.

[103] § 18 zákona č. 153/1994 Sb., o zpravodajských službách České republiky, § 7 až 15 zákona č. 289/2005 Sb., o Vojenském zpravodajství.

dopravovaných zpráv či užít operativně pátracích prostředků, je podle zákona č. 337/1992 Sb., o správě daní a poplatků, orgán provádějící celní dohled.

Konečně pak podle § 184 TZ je garantována ochrana osoby proti pomluvě, za kterou považuje sdělení nepravdivého údaje, který je způsobilý značnou měrou ohrozit vážnost u spoluobčanů nebo mu způsobit jinou vážnou újmu. Pokud k tomu dojde prostřednictvím zvláště účinného prostředku, za který odst. 2 považuje i počítačovou síť, hrozí pachateli až dvojnásobné potrestání. Je však důležité si uvědomit, že trestný čin nemůže být spáchán sdělením údaje pravdivého, třebaže může být sdělen v úmyslu ohrozit vážnost jiného u spoluobčanů.[104]

V anglosaském právním systému, například ve Velké Británii, je koncepce ochrany osobnosti a soukromí odlišná od kontinentálního pojetí. Na rozdíl od všeobecného osobnostního práva, typického pro kontinentální právní systémy, anglosaské systémy obdobný obecný institut neznají a individuální osoby se své ochrany mohou domáhat pouze v omezené míře prostřednictvím specifických žalob, hovoří o institutech jako libel a defamation, což lze chápat jako újmu na cti dotčené osoby. Co je však, díky společnému evropskému základu, obdobně regulované jsou ty oblasti, do kterých se rozhodla zasáhnout svým zákonodárstvím Evropská Unie (například úprava ochrany osobních údajů či některých otázek souvisejících s elektronickými komunikacemi, které upravily příslušné směrnice).

2.4 Ochrana osobních údajů

Základní otázky dotýkající se ochrany osobních údajů jsou, zda mají subjekty možnost dát svůj informovaný a výslovný souhlas se zpracováním jejich osobních údajů, kdo by měl být oprávněn data zpracovávat a jakým způsobem je dovoleno s takovými daty nakládat. Jak jsou tyto aspekty právně regulovány bude tématem této kapitoly.

2.4.1 Základní zásady

Základní zásady ochrany osobních údajů, které jsou jinými slovy vyjádřeny v právních dokumentech jak na evropské tak národní úrovni evropských států, byly zakotveny Úmluvou č. 108.[105] Jde o tyto principy: 1. princip legitimity zpracování (zpracovávané osobní údaje musí být získány a zpracovány poctivě a v souladu se zákony), 2. zásada účelnosti (zpracovávat lze pouze údaje nezbytné pro daný účel), 3. zásada časového omezení (údaje mají být zpracovány pouze po

[104] Šámal, P. a kol., (2010) *Trestní zákoník II. § 140 až 421. Komentář.* 1. Vydání. Praha: C. H. Beck, Str. 1643.

[105] Úmluva Rady Evropy č. 108/1981, v platnosti pro ČR od 1. 11. 2001.

dobu, po kterou je to nezbytné pro daný účel), 4. zásada potřebnosti a proporcionality dat (zpracovávané údaje musí být potřebné a přiměřené danému účelu po celou dobu jejich zpracování, nesmí být nadměrné), 5. zásada průhlednosti, transparentnosti (každý má možnost zjistit existenci automatizovaného souboru osobních údajů, jejich účely, sídlo a totožnost správce, jakož i možnost získat přehled o údajích zpracovávaných o jeho osobě), 6. zásada bezpečnosti (soubory osobních údajů musí být zabezpečeny proti neoprávněnému přístupu k nim, jejich změnám, zničení či šíření), 7. zásada práva přístupu k datům (každý má právo zjistit, zda jsou údaje v daném systému o jeho osobě zpracovávány, a na přístup k nim ve srozumitelné formě), 8. zásada práva na opravu a výmaz (jejím výrazem je spíše dnes zásada aktuálnosti a přesnosti zpracovávaných údajů, přičemž každý má právo na to, aby údaje o něm byly opraveny či aktualizovány tak, aby byly pravdivé, a ty nepravdivé, aby byly změněny či vymazány), a 9. zásada nezávislého dozoru (každá smluvní strana je povinna ustanovit nezávislý dozorčí orgán na ochranu práv a kontrolu dodržování povinností vyplývajících z této úmluvy).[106] Jak je z dnešních úprav patrné, tyto principy zůstaly zachovány.

2.4.2 Mezinárodní základy

Z obecného hlediska je ochrana osobních údajů součástí práva na ochranu soukromí, jež bylo deklarováno článkem 12 Všeobecné deklarace lidských práv z roku 1948. OSN schválila znění, které zakazuje svévolné zasahování do soukromého života, do rodiny, domova nebo korespondence. Dále zakazuje i útoky na čest a pověst. Přičemž každý má právo na ochranu proti takovým útokům a zásahům. Pod tímto vlivem byla obdobná úprava přijata v závazném dokumentu Rady Evropy v roce 1950, Úmluva o ochraně lidských práv a základních svobod, někdy též zkráceně nazývaná též jako Evropská úmluva nebo Evropská konvence. Článek 8. bývá velmi často citován a je základním východiskem a interpretačním pravidlem pro veškeré zákonné úpravy či rozhodování státních orgánů (nejčastěji soudů) jednotlivých členských států. Proto i výklad Evropského soudu pro lidská práva (ESLP), jež je nejvyšším garantem dodržování základů této konvence, je významným hlediskem pro výklad a aplikaci právních řádů v jednotlivých zemích. Článek 8 ve svém odstavci prvním zaručuje právo každého na respektování svého soukromého a rodinného života, obydlí a korespondence. Odst. 2 pak uvádí výjimky, kdy zásahy jsou oprávněné. Nejdůležitější obecné podmínky pro aplikaci výjimek jsou, zásada nezbytnosti, zákonnosti a předpokládaného účelu. Jinak řečeno, každý zásah do soukromé sféry fyzické osoby musí být v souladu se zákonem, musí být nezbytný, a musí být v zájmu

[106] Kučerová, Bartík, Peca, Neuwirt, Nejedlý 2003, str. 331 až 336.

národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných. Dalším právně závazným dokumentem pojednávajícím také o soukromí a ochraně osobních údajů je Charta základních práv EU z roku 2000. Ta v článku 8. pojednává o ochraně osobních údajů, jejich poctivému zpracování a dále obecně shrnuje většinu základních principů.

V některých případech protichůdné (ačkoli teoreticky je považováno za doplňující) právo pak zaručuje Evropská konvence v článku 10, kde každému zaručuje právo na svobodu projevu a vyjadřování, bez zasahování státních orgánů a bez ohledu na hranice. Ačkoli i zde odst. 2. uvádí podmínky, za kterých tato svoboda může být omezena, v praxi však právě nacházení vyváženosti mezi ochranou práv druhých podle čl. 8 a svobodami podle čl. 10 činí často velké problémy a je předmětem soudních sporů.

S rozvojem technických prostředků, začaly jednotlivé státy přicházet s národními úpravami ochrany osobních dat zejména v 70. letech 20. století (např. Německo, Švédsko či Francie). Postupně se však ukázalo, že pouhá národní úprava nemůže být dostačující, proto se do činnosti mezinárodní zapojila i organizace OECD[107] a Rada Evropy. Důležitým dokumentem v evropském měřítku bylo přijetí tzv. Úmluvy č. 108 (Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat č. 108) v roce 1981, která vstoupila v platnost v roce 1985, a směrnice č. 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (směrnice o ochraně osobních údajů), která se stala základním harmonizačním prostředkem národních úprav evropských států a je i základem našeho zákona o ochraně osobních údajů, č. 101/2000 Sb.

Úprava na naší národní úrovni je nejobecněji promítnuta do Listiny základních práv a svobod, která v čl. 10 zaručuje v odst. 1. právo každého na zachování jeho lidské důstojnosti, osobní cti, dobré pověsti a ochranu jména. Odst. 2 pak zaručuje ochranu před neoprávněným zasahováním do soukromého a rodinného života. A odst. 3 konečně stanoví právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě. Pokud jde o právo na informace, svobodu projevu a vyjadřování, tato práva a svobody jsou zakotveny v čl. 17 Listiny, jejichž omezení podle odst. 4 je mimo jiné přípustné v případech, kdy je to nezbytné pro ochranu práv a svobod druhých, což se promítá do celé řady zákonů a právních úprav.

[107] Organizace pro hospodářskou spolupráci a rozvoj.

Právní úprava evropská

Směrnice č. 95/46/ES, o ochraně osobních údajů (dále též DPD) uvádí základní principy nakládání s osobními údaji ve svém článku 6. Tyto pak v podstatě jednotlivé členské státy zakotvují a konkretizují, avšak podstata se nemění. Osobní údaje musí být zpracovávány zákonně, zejména pokud jde o jejich získávání (zákonným způsobem a k zákonnému účelu), pouze v rozsahu nezbytném k danému účelu a přesně (tj. aktuální a pravdivé). Uchovávat je lze pouze po dobu nezbytnou k danému účelu, přičemž musí být po celou dobu zpracování zabezpečeny odpovídajícím způsobem tak, aby nedošlo k neoprávněnému přístupu, změně, ztrátě nebo poškození zpracovávaných údajů. Kromě toho mohou být osobní údaje přeneseny i do třetích zemí (mimo EHS), avšak jedině v případě, že je zachována odpovídající ochrana a bezpečnost.

Přísnější režim pak směrnice vztahuje na osobní údaje klasifikované jako zvláštní kategorie údajů, tzv. citlivé. Jde například o data týkající se rasového nebo etnického původu, politických názorů, náboženského vyznání, psychického nebo fyzického stavu, sexuálního života (čl. 8 bod 1. DPD). Na adresu definice citlivých dat byla adresována kritika například, že nezahrnuje biometrické údaje jako například DNA nebo otisky prstů. V případě emailových adres není zcela jasné, zda například adresa obsahující další, povahou citlivý údaj, spadá do této kategorie. Půjde například o adresu petr.novák@homosexual-organization.co.uk. Tyto údaje je obecně zpracovávat zakázáno, ledaže by k jejich zpracování byla splněna alespoň jedna z těchto podmínek: a) výslovný souhlas dotčené osoby, b) vyžaduje-li to zákon z pracovněprávních důvodů, c) je-li to nutné k ochraně životně důležitých zájmů dané osoby nebo někoho jiného, d) v souvislosti se soudním nebo jiným právním řízením.

Pokud jde o výjimky, směrnice dává možnost omezit či vyloučit povinnosti a práva vyplývající z této směrnice v případě, jde-li o bezpečnost státu, obranu, veřejnou bezpečnost, z trestněprávních důvodů nebo je-li to třeba z důvodu ochrany subjektu údajů nebo práv a svobod druhých (článek 13 DPD). Sem patří například velmi rozšířený způsob sledování lidí ve Velké Británii, tzv. CCTV videokamery. Jejich úkolem je monitorování a sledování téměř veškerých veřejných míst (ovšem v mnohých případech nejen těch) právě z důvodů předcházení trestní činnosti.

DPD používá termín zpracování (processing) osobních údajů v jeho velmi širokém smyslu, ať již jde o automatizovaný nebo neautomatizovaný způsob.[108] Termín obsahuje veškeré činnosti jako přijímání, nahrávání či držení takových údajů, nebo provádění jakýchkoli operací jako organizace, změna, kombinování, užívání, poskytování, převádění, nebo také jejich zničení či výmaz. Toto velmi široké pojetí bylo užito v případě Lindqvist, ve kterém obžalovaná uveřejnila pár fotografií na webových stránkách spolu s údaji, z nichž bylo možné identifikovat její kolegyni z církve. Její obrana, že šlo pouze o výlučně osobní a domácí účely (což se nepovažuje za zpracování podle čl. 3 bodu 2. DPD) bylo odmítnuto s tím, že šlo o publikaci na internetu, tedy zpřístupnění neomezenému počtu lidí. ESD tím v podstatě vyložilo termín zpracování tak, že každá osoba uveřejňující údaje na blogu, prostřednictvím aplikace Facebook a podobně spadá do režimu DPD a tudíž musí splňovat předepsané podmínky (jako například povinnou registraci u národní instituce v případě UK). Pokud jde o další vývoj, pozdější interpretace se spíše kloní k názoru, že pokud jde o případ internetových stránek, považuje se za použití pro soukromé účely takový případ, kdy uživatel omezí přístup k těmto informacím pouze pro určitý okruh osob (což však ve většině případů v praxi nebývá). [109]

Článek 6 odst. 1 písm. a) DPD uvádí, že osobní údaje mají být zpracovány korektně a zákonným způsobem.

Jak již bylo zmíněno, k zpracování osobních údajů je zásadně nutný souhlas subjektu, nejde-li o jiný případ podle článku 7 DPD (tím je například nezbytnost k plnění smlouvy, právní povinnosti správce, výkon veřejné moci či uskutečnění oprávněných zájmů správce nebo třetí osoby). Avšak například v případě internetových sociálních sítí (např. Facebook) se však v praxi ukazuje, že takový souhlas není příliš efektivní podmínkou. Každý při registraci přijímá všeobecné podmínky, ve kterých je obdobný souhlas inkorporován, aniž by předem zvažoval jakékoli důsledky. Obdobně v případě uskutečnění oprávněných zájmů správce nebo třetí osoby (čl. 7 pís. f) DPD) bylo chápáno jako vymezení vyváženosti mezi ochranou soukromé osoby a obchodní činností jiných osob. ESD však v případě Bavarian Lager[110] v roce 2007 tento výklad více posunul ve prospěch ochrany osobnosti. V případě citlivých údajů takový souhlas navíc

[108] Čl. 3 bod 1. Směrnice Evropského Parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (směrnice o ochraně osobních údajů).

[109] Edwards a Waelde 2009, str. 461.

[110] Bavarian Lager v Commission of the EC, 8 November 2007, CFI, Case T-194/04.

musí být výslovný (čl. 8 odst. 2 písm. a) DPD), tudíž jejich prostá inkorporace do obchodních podmínek není dostatečnou.

Spolu s problematikou souhlasu vyvstává též další otázka. Po jakou dobu takový souhlas trvá? Podle výkladu britského komisaře (ICO) se použije stejný princip jako v případě samotných údajů, tedy zásada nezbytnosti pro daný účel. V praxi však zejména z komerčních důvodů převažuje snaha ze strany podnikatelů o co nejdelší zpracovávání takových údajů.

Pokud jde o věk dostatečný pro souhlas, například ve Skotsku zákon určuje, že dítě může dát takový souhlas v případě, pokud je schopné obecného porozumění takového úkonu. Za to se presumuje osoba starší 12 let.[111]

Pro posouzení zákonnosti zpracování je nutné zkoumat veškeré další právně závazné předpisy a konkrétní okolnosti. Za hlediska hodná zvláštní pozornosti se považují důvěrnost a povinnost mlčenlivosti odvozené od vztahu mezi správcem a subjektem údajům, jednání správců ultra vires, tj. mimo zákonem stanovené limity, legitimní očekávání subjektu o tom, jakým způsobem správce může s poskytnutými údaji nakládat a vztah k právu na ochranu soukromí podle čl. 8 Evropské konvence. Důraz na ochranu osobních údajů je posílen tím, že na správci leží důkazní břemeno v souvislosti se zákonností zpracovávání osobních údajů.[112]

Za legitimní důvod zjišťování osobních údajů je v poslední době považováno zjišťování uživatelů stahujících materiály v rozporu s autorskými právy, jako například v případě Promusicae.[113] ESD odmítl ochranu soukromí internetových uživatelů ve prospěch zábavního průmyslu, který podnikl nutné kroky ke zjištění totožnosti osob porušujících jejich práva k duševnímu vlastnictví.

DPD také nahradila původně zamýšlený princip univerzální registrace správců osobních údajů (pro přílišnou byrokratizaci a zvýšené náklady) principem notifikace, oznámení. Není tedy již nutné, aby se každý správce registroval u stanoveného centrálního orgánu, avšak tomuto orgánu postačí danou skutečnost oznámit.[114]

Článek 25 DPD upravuje také podmínky předávání osobních údajů do třetích zemí. Jinak řečeno, obecně platí zásada volného pohybu osobních údajů v rámci zemí EHS, kde standardy ochrany a

[111] Data Protection Act 1998, čl. 66.

[112] Lloyd 2008, str. 97.

[113] Promusicae v Telefonica, ESD, 29 Leden 2008, C-275/06.

[114] Čl. 18 DPD; Rowland a Macdonald 2005, str. 331.

nakládání s osobními údaji jsou srovnatelné. V této souvislosti je důležité také rozhodnutí (Evropského Soudního Dvora) ESD Lindqvist[115], které objasnilo, že pouhé umístění osobních dat na webové stránky se nepovažuje za poskytnutí těchto údajů na území třetích států, ačkoli přístup subjektů z těchto zemí je pravděpodobným důsledkem. Základní zásada je taková, že předání údajů do třetí země (mimo členské státy) je možné jedině v případě, že v této zemi je zaručená jejich odpovídající ochrana. Komise může akreditovat určité země konstatováním, že tyto splňují požadavky podle zmíněné zásady (článek 25 bod 6. DPD). Edwards uvádí, že dosud bylo pouze několik málo třetích zemí takto akreditováno.[116] Mezi ně patří např. Švýcarsko nebo Argentina, v případě Kanady je tak pouze, jde-li jen o některé kategorie informací, a v případě USA byla dohodnuta zvláštní dohoda o tzv. bezpečném přístavu – „safe harbor".[117]

V otázce individuálních práv subjektů údajů a jejich ochrany DPD zásadně garantuje, že dotčená osoba musí být náležitě informována správcem údajů o tom, jaké údaje, jakým způsobem jsou zpracovány, popřípadě musí být poskytnuta možnost dát či vzít zpět či omezit souhlas se zpracováním, právo subjektu na přístup ke svým osobním údajům u daného správce, námitku apod. V případě porušení těchto práv je zásadně osoba oprávněna k náhradě škody od správce (čl. 23), k opravnému prostředku ve správním řízení (čl. 22 a 28) a k soudní ochraně (čl. 22).

2.4.4 Základní úprava v České Republice

Na základě Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat[118] byl přijat zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (dále jen ZOOU), který představuje obecnou úpravu zpracování osobních údajů v našem právním řádu a je výrazem evropských tendencí vyjádřených zejména prostřednictvím směrnic.

Ochrana osobních údajů je součástí práva na soukromí, tj. všeobecného osobnostního práva, pro jehož ochranu byl na našem území zřízen zvláštní správní orgán, Úřad na ochranu osobních údajů (dále též Úřad) ve smyslu § 2 ZOOU. Jde mimo jiné i o naplnění povinnosti státu vyplývající ze směrnice č. 95/46/ES o ochraně osobních údajů.

[115] Case C-101/01 Criminal Proceedings against Lindqvist [2003] All ER (D) 77 (Nov), ECJ.

[116] Edwards a Waelde 2009, str. 454.

[117] US Department of Commerce (1999) *International Safe Harbor privacy principles*. [online] Dostupné na adrese <http://www.ita.doc.gov/td/ecom/Principles1199.htm>.

[118] Úmluva Rady Evropy č. 108/1981, v platnosti pro ČR od 1. 11. 2001.

Zákon se věcně vztahuje na veškeré zpracovávání osobních údajů (§ 3 ZOOÚ), bez ohledu na to, zda jsou tyto údaje zpracovávány automaticky či ručně (manuálně), bez ohledu na to, kdo tyto údaje zpracovává (zda veřejný orgán či soukromá osoba).

Výjimkou je pouze případ, kdy jde o zpracovávání fyzickou osobou výlučně pro její osobní potřebu (nepatří do této výjimky tedy žádná právnická osoba, ani osoba, která zpracovává údaje pro účely podnikatelské). Obdobně se zákon nevztahuje ani na zpracování pro statistické a archivní účely. Nevztahuje se ani na tzv. nahodilé zpracování (např. při poskytování služeb), nejsou-li tyto údaje dále zpracovávány či poskytovány jiným osobám např. pro reklamní účely.[119] Přičemž za nahodilé zpracování se rovněž považuje shromažďování údajů při činnosti advokátů, auditorů aj. „svobodných" povolání. Obdobně se zákon nevztahuje ani na některé orgány státní moci (např. Policie ČR či BIS).

Základní definice vychází z pojetí směrnice č. 95/46/ES o ochraně osobních údajů. Proto se rozlišují kategorie osobních údajů tzv. obecných, a těch, které jsou citlivé. Přičemž subjektem osobních údajů může být jedině fyzická osoba. Za osobní údaj se považuje jakákoli informace, ze které lze přímo či nepřímo identifikovat subjekt těchto údajů. Nejde však o ty případy, kdy ke zjištění identity je třeba nepřiměřené množství času, úsilí či prostředků.[120] Citlivé osobní údaje jsou pak takové, které se týkají národnosti, rasového či etnického původu, politických postojů, členství v odborových organizacích, náboženství a filozofického přesvědčení, odsouzení za trestný čin, zdravotního stavu a sexuálního života subjektu údajů, dále i jakýkoli biometrický či genetický údaj subjektu údajů. Tento výčet je taxativní, nejsou jím tedy například údaje o majetkových poměrech apod.

Zpracováním je potom velmi široce definovaná činnost zahrnující např. shromažďování, uchovávání, zpřístupňování (včetně zveřejnění na internetu), třídění, blokování i likvidace takových údajů. Výčet je demonstrativní, tudíž veškeré systematické nakládání s osobními údaji lze podřadit pod tuto kategorii.

Správcem je každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Může zpracováním pověřit zpracovatele, přesto však správcem zůstává tento subjekt. Správcem je každý, kdo vykonává třeba jen některou s výše uvedených činností, bez ohledu na jeho právní povahu, zda je fyzickou či právnickou osobou, a bez ohledu na to, zda tuto činnost provádí legálně či v rozporu s právními předpisy.

[119] Knap, P. 2004, str. 396.

[120] Ibid. str. 398.

Základní povinnosti subjektů se týkají zejména správce osobních údajů. Tento je povinen stanovit zejména účel zpracování osobních údajů, jež nelze libovolně v průběhu měnit podle § 5 odst. 1 ZOOÚ, a podle toho i prostředky a způsob. Zpracovat lze pouze zákonně získané údaje a pouze v rozsahu nezbytnému k danému účelu. Údaje odpovídajícím způsobem aktualizuje a zpřesňuje podle skutečného stavu. Navíc nesmí být údaje zpracovány déle, než je nezbytné k danému účelu (toto omezení neplatí u údajů pro účely statistické, vědecké či archivnické), hovoří se o tzv. zásadě přiměřenosti. Jak je na první pohled vidět, jde o převzetí základních principů ze směrnice, obdobně, jako tomu je například v DPA ve Velké Británii.

Základním pravidlem je souhlas subjektu údajů, který musí správce obdržet před samotným zpracováním osobních údajů. Souhlas není třeba v zákonem vyjmenovaných případech. Jedná se zejména o ty, kdy je to nezbytné ke splnění právní povinnosti správce (ať již zákonné či smluvní), k ochraně životně důležitých zájmů subjektu údajů (např. ochrana majetku či rodinných poměrů), v případě oprávněně zveřejněných osobních údajů (podle tiskového zákona), pokud jde o ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby, pokud jde o údaje o veřejně činné osobě vypovídající o jeho veřejné či úřední činnosti či zařazení, pokud jde výlučně o archivnický účel.

Souhlas se vyžaduje svobodný, vědomý a informovaný, přičemž písemná forma vyžadována zákonem není. Právě v případě elektronické komunikace často vznikají situace, kdy není zcela zřejmé nebo lze považovat na hranici zákona určité praktiky. Tak někteří autoři považují za nedostatečné, je-li souhlas získán způsobem, kdy například při objednávce v internetovém obchodu se v okně pro potvrzení objednávky zobrazí i předem zaškrtnuté políčko se souhlasem se zpracováním osobních údajů.[121] Argument pro takové tvrzení je zejména v tom, že souhlas musí být informovaný, což v tomto případě nelze bezpečně tvrdit, když není třeba žádný aktivní úkon subjektu samotného, tudíž například při přehlédnutí mnohdy písma v malém fontu, poskytne souhlas, aniž by si toho byl vědom.

V případě zpracování pro účely reklamní, lze použít jméno, příjmení a adresu subjektu, jsou-li tyto údaje získány z veřejného seznamu nebo v souvislosti se svou činností jako správce či zpracovatele. Jinému správci lze takové údaje předat jedině, pokud budou užity opět jen pro reklamní účely, přičemž o tom byl subjekt předem informován a nevyslovil s tím nesouhlas, přičemž nesouhlas musí být projeven písemně.

[121] Bartík, V. a Janečková, E. 2010, str. 184 a 185.

Pokud jde o citlivé údaje, tyto mohou být zpracovávány jen s výslovným souhlasem subjektu údajů. Výjimkami jsou účely poskytování zdravotní péče, účely sociálního zabezpečení či jiné případy dle zvl. zákona. Nejdůležitější výjimkou ze souhlasu je případ, kdy subjekt sám tyto údaje zveřejnil, čímž se vzdal svého soukromí, a nadále lze takové údaje zpracovávat bez jeho předchozího souhlasu.[122] Správce/zpracovatel (mají stejné povinnosti) musí dbát na zachování důstojnosti subjektu údajů a na tom, aby mu nevznikla jiná újma.

Navíc také musí být subjekt údajů informován o rozsahu, účelu, způsobu zpracování údajů o něm. Subjekt údajů musí být rovněž poučen o svých právech, mj. při poskytnutí údajů třetí osobě. Hovoří se tedy obecně o informační a poučovací povinnosti správce/zpracovatele.

Subjekt údajů má také právo na přístup k údajům, které daný správce o něm zpracovává. Jde o způsob kontroly, případně upřesnění zpracovávaných údajů samotným subjektem.

Správce má také povinnost dostatečně zabezpečit údaje tak, aby nemohlo dojít k jejich poškození, zneužití či změnám. Navíc každý zaměstnanec, přicházející do styku s osobními údaji, má generální povinnost mlčenlivosti.

Zpracovávání údajů podléhá dohledu Úřadu, jemuž musí správce předem písemně oznámit záměr zpracovávat osobní údaje, včetně povinných informací podle § 16 odst. 2 ZOOÚ. Úřad správce poté registruje a vydá o této skutečnosti osvědčení. Obdobně je nutné také oznámit ukončení této činnosti. Z povinnosti oznámení existuje několik výjimek. Tak není oznámení vyžadováno, jde-li o údaje výlučně z veřejně přístupných datových souborů, je-li zpracovávání uloženo zvláštním zákonem (například zaměstnavatelům), zpracovávání prováděné politickými stranami, občanskými sdruženími, náboženskými apod. nevýdělečnými společnostmi (pokud jde o zpracování pro vnitřní potřebu).

Úřad kromě registrace, vykonává i další činnosti, zejména kontrolu činnosti správců/zpracovatelů, má právo seznamovat se s utajovaným skutečnostmi, apod. Výsledkem kontroly může být uložení opatření k nápravě správci/zpracovateli, které ukládá inspektor. Nejzávažnějším opatřením je uložení povinnosti likvidace osobních údajů. Kromě opatření k nápravě může Úřad též uložit finanční sankce. Co je však nutné si uvědomit je fakt, že sankce uložené Úřadem jsou příjmem státním, nemají tedy povahu kompenzace chráněného subjektu

[122] Mates, P. 2006, str. 212.

údajů. Lze se tedy vedle ochrany podle zvláštního zákona domáhat i ochrany osobnosti podle obecné občanskoprávní úpravy, jak na to upozorňuje i Knap.[123]

Ochrana individuálních práv subjektů je upravena ve zvláštní části zákona. Ten se může obrátit na Úřad a žádat zajištění nápravy v případě nezákonného zpracovávání údajů o něm. Zároveň může přímo na správci/zpracovateli požadovat vysvětlení, popř. odstranění vzniklého stavu (např. opravou, doplněním, blokací či likvidací údajů). Kromě toho se může také domáhat ochrany obecné občanskoprávní, došlo-li ke vzniku nemajetkové újmy (podle § 13 OZ). Za majetkovou škodu, stejně jako za porušení povinností podle tohoto zákona, odpovídají solidárně správce a zpracovatel. Navíc je podle trestního zákona též považováno neoprávněné nakládání s osobními údaji za trestný čin.[124]

Naše úprava také převzala evropský režim předávání údajů do třetích zemí (mimo EHS). V rámci EHS není pohyb osobních údajů omezen, do třetích zemí však je nutné nejprve požádat Úřad o povolení. Úřad zejména posoudí, zda jsou údaje dostatečně zabezpečeny a zda je s nimi nakládáno tak, aby nedošlo k újmě subjektu údajů.

2.4.5 Úprava ve Velké Británii

Základním zákonem, který mimo jiné provedl i uvedenou směrnici je Data Protection Act z roku 1998 (dále též DPA). V otázce působnosti, DPA je aplikovatelný na všechny správce osobních údajů, jež jsou založeni podle předpisů Velké Británie (UK) a v rámci jejichž činnosti jsou údaje zpracovávány. Dále se vztahuje i na ty správce, kteří jsou sice založeni ve třetích zemích, avšak využívají ke zpracovávání osobních údajů prostředky nacházející se v UK, nejde-li o případ pouhé přepravy přes území UK.[125] Půjde typicky o příklad mezinárodní společnosti, která působí na území UK, ačkoli její management a skutečné sídlo je například v USA. Založený podle předpisů UK znamená podle článku 5 odst. 3 DPA: a) že správce je obyvatel UK, b) správce je právnickou osobou založenou podle právního řádu UK, c) správce je společenství nebo jiná forma asociace, která se nezakládá, avšak řídí se právním řádem UK, d) správce udržuje

[123] Knap, P. 2004, str. 411.

[124] § 180 zákona č. 40/2009 Sb., trestní zákoník.

[125] Článek 5 odst. 1 Data Protection Act 1998.

kancelář, pobočku nebo běžnou praxi na území UK. Nezáleží tudíž na místě, kde jsou data zpracovávána nebo kde se nacházejí.[126]

Základní principy, na kterých je založena ochrana osobních údajů, se v podstatě shodují s již představenými podle evropské směrnice. DPA jich vypočítává 8: 1) princip korektního a zákonného zpracování, 2) princip omezeného a zákonného účelu zpracování, 3) princip přiměřenosti, relevance, v rozsahu nepřekračujícím nutnost k danému účelu, 4) princip přesnosti a aktuálnosti údajů, 5) princip omezené doby zpracovávání údajů (pouze po dobu nezbytnou k danému účelu), 6) princip výkonu osobních práv subjektu údajů (právo přístupu k údajům, apod.), 7) princip bezpečnosti zpracovávaných údajů a 8) princip omezeného přenosu dat do třetích zemí.

Pokud jde o data považující se za osobní, což jsou taková, vztahující se k žijící osobě, která ji přímo identifikují nebo ze kterých je taková osoba identifikovatelná (ať přímo nebo nepřímo), k nakládání s těmito údaji je nutný zejména souhlas osoby, které se tato data týkají, a dále přísnější podmínky nezbytnosti pro konkrétní účel (například k plnění smluvního vztahu, výkonu práv a povinností, pro výkon veřejné moci nebo jiný legitimní účel).[127] Právě s informacemi nepřímo identifikujícími je někdy výkladový problém, proto Komisař pro ochranu osobních údajů, The Information Commissioner's Office (ICO), vydává výkladové směrnice, ve kterých se výklad nejasných termínů sjednotit.[128]

Právně závazný výklad však provádí zejména soudní orgány. Takto se odvolací soud v případu Michael John Durant v Financial Services Authority [2003] EWCA Civ 1746 zabýval například otázkou, co činí konkrétní data osobními ve smyslu tohoto zákona. Uvedl, že pouhé zmínění dané osoby v dokumentu nemusí nutně znamenat osobní údaj. Zda jde v daném případě o takový údaj, záleží na „nepřetržité relevanci nebo blízkosti" daných informací ke zmíněné osobě. Tento výklad je poměrně kontroverzní a vzbudil poměrně širokou diskuzi. Například v internetovém prostředí by mohl znamenat poměrně výrazné zúžení případů, kterých se týká.

Další otázkou vztahující se k internetovému prostředí je, zda se IP adresa (což je jediná konkrétní identifikace v internetovém prostředí) považuje za osobní údaj. Pokud nikoli, potom například společnosti provozující vyhledávače (Google, Seznam apod.) mohou shromažďovat

[126] Lloyd 2008, str. 57 a 58.

[127] Čl. 2 bod a) Směrnice č. 95/46/ES o ochraně osobních údajů a sec. 1(1) DPA.

[128] Information Commissioner's Office (neuvedeno) *Oficiální instrukce nakládání s osobními údaji*. [online] navštíveno 21/04/2010. přístupné na adrese <http://www.ico.gov.uk/>.

veškeré údaje a hesla vyhledávaná právě pomocí jejich služby, bez dalšího omezení například časového apod.[129] Proto až do nedávna Google shromažďoval takové údaje po neomezenou dobu, avšak od roku 2007 souhlasil se snížením doby na max. 24 měsíců, což lze stále považovat za velmi dlouhou (nikoli nezbytnou) dobu. Od roku 2008 se evropské pojetí více přibližuje názoru, že IP adresa by měla být považována za údaj vztahující se k dané osobě.[130]

Obdobný výklad je i v případě emailových adres. Převažuje obecný názor, že jde o informace svojí povahou osobní. Avšak vzhledem k definici osobních údajů, musí jít o takovou informaci, ze které je daná osoba identifikovatelná. Není pochyb, že v případě adresy obsahující jméno jejího uživatele, například petr.novák@gmail.com, bude se jednat o osobní údaj. V jiném případě, například ball.pen@yahoo.com, však tomu tak není. Obecný náhled a výklad však je, že obecně všechny emailové adresy spadají do kategorie osobních údajů a podle toho je s nimi nutno nakládat.[131]

Z pohledu dohledu a vymáhání lze rozlišit dva odlišné přístupy: a) evropský, kde je dohled svěřen nestranné autoritě[132] a b) přístup USA, který klade zdaleka největší důraz na aktivní přístup subjektu samotného a ochranu (včetně případného vymáhání) individuální osoby.[133]

Ve Velké Británii je orgánem dozoru, jak jej předpokládá čl. 28 DPD, nezávislý Komisař jmenovaný královnou a podávající každoroční zprávu Parlamentu.[134] Tento Komisař mimo jiné vydává výkladová pravidla a směrnice k dodržování zákonných povinností. Vedle toho hraje i aktivní roli při dohledu a vymáhání dodržování předpisů na ochranu osobních údajů. V případě podezření z porušení zákona ICO nejprve upozorní toho, kdo se porušení dopustil, prostřednictvím tzv. informačního upozornění a zároveň vyzve k nápravě a dodržování principů zpracování osobních údajů. V případě, nedojde-li k nápravě ani přes tyto výzvy, může ICO vznést žalobu k příslušnému soudu, přičemž již samotné neuposlechnutí předchozích výzev je

[129] Edwards a Waelde 2009, str. 458.

[130] Edwards a Waelde 2009, str. 459.

[131] Carey 2004, str. 233.

[132] Článek 28 Směrnice č. 95/46/ES o ochraně osobních údajů.

[133] Lloyd 2008, str. 60 a 61.

[134] The Information Commissioner's Office.

považováno za trestný čin.[135] Navíc od roku 2008 může ICO uložit i pokuty aniž by musel věc předkládat soudu.[136]

V případě soukromého sektoru jsou však nejúčinnější opatření ta, které se dotýkají dobré pověsti a důvěryhodnosti toho, kdo povinnosti při zpracování osobních údajů porušuje. Proto jednou z reforem by podle dalších návrhů měla být současná povinnost nebo alespoň uveřejnit informace o tom, že určitá společnost nebo subjekt porušuje tyto povinnosti (což je již běžné ve Spojených Státech či Japonsku). To se má týkat zejména sektoru elektronických komunikací včetně internetu.[137] Proti dosavadním návrhům se však brání zejména poskytovatelé služeb informační společnosti (ISP), protože tyto povinnosti se mají dotýkat jen veřejně dostupných služeb elektronických komunikací (podle definice v čl. 3 směrnice o elektronických komunikacích). Nezměnila by se však například pozice bank či jiných finančních společností, při jejichž činnosti také nevyhnutelně dochází k zpracovávání osobních údajů, což je dle ISP nespravedlivé.

Opatřením ICO, které je svojí povahou zejména správněprávním, nejsou nikterak dotčena práva samotného subjektu na ochranu svých osobních údajů. Ten se může mimo jiné domáhat kompenzace pomocí civilního soudního řízení na základě paragrafu 13(1) DPA. Aby však byla úspěšná, musí být prokázán kauzální nexus mezi škodou a jednáním správce v rozporu s právními povinnostmi a musí jít o škodu nebo újmu, která může být považována za ekonomickou ztrátu či poškození. Edwards dodává, že obdobných úspěšných žalob je velmi málo, což je další důvod častého nedodržování zákonné úpravy.[138]

[135] Edwards a Waelde 2009, str. 467 a 468

[136] The Criminal Justice and Immigration Act 2008, s. 144 a DPD s. 55A.

[137] Edwards a Waelde 2009, str. 469.

[138] 2009, str. 470.

2.5 Defamation (ochrana pověsti a cti podle common law)

Ve Velké Británii, jak již bylo uvedeno, neexistuje všeobecné osobnostní právo jako takové, takže jednotlivé aspekty ochrany osobnosti jsou právně upraveny individuálně. Právní úprava ochrany cti, váženosti a společenského postavení osoby se vyvinulo v poměrně samostatnou právní oblast. Úprava je obsažena v common law (jeho základem jsou právní pravidla vytvořená soudní praxí) a v některých zákonných předpisech, například v zákoně o urážce na cti z roku 1996 (dále jen DA).[139] Pozornost je také věnována urážce na cti (pomluvě), ke které internet znamená velmi snadný prostředek ve formě různých blogů, emailů či internetových stránek. V prostředí internetu se právo zaměřilo na pomluvu v trvalé podobě (psané) a ulehčila postavení žalobce do té míry, že tento nemusí dokazovat utrpěnou škodu nebo jinou újmu, ale tato újma je právně presumována.[140] Úspěšný žalobce tedy musí prokázat pouze tři aspekty: že jde o urážlivé sdělení, které je identifikovatelně spojené s osobou žalobce, a které bylo uveřejněno (čímž se rozumí poskytnutí takové zprávy alespoň jedné další, třetí, osobě).

Právě pojem uveřejnění působí v internetovém prostředí výkladové komplikace. Kohl analyzoval, které jednání se považuje za uveřejnění, a které tohoto statusu nedosahuje. Například uvádí, že za dostatečné se nepovažuje pouhé umístění informace na webové stránky. Musí totiž dojít k aktuální komunikaci, doručení informace třetí osobě, čímž je například okamžik přečtení touto osobou. Proto při rozhodování soudu bude hrát roli mimo jiné pravděpodobnost, že daná stránka byla navštívena osobou jinou než žalobcem samotným, a tudíž naplnila znaky uveřejnění v tomto smyslu.[141] Uveřejnění však například splňuje jediná emailová zpráva, jak bylo rozhodnuto v případě Slipper v BBC [1990] 1 All ER 165. Zároveň tamní právní úprava vychází z pojetí, že každé jednotlivé uveřejnění je novým žalobním titulem. Jinak je to v případě USA, kde právo aplikuje pravidlo tzv. prvního uveřejnění, tedy žalovatelné je pouze první uveřejnění defamující (urážlivé) zprávy.[142] Důležitým procesním důsledkem je zejména okamžik počátku běhu lhůty k podání případné žaloby, kdy v případě Velké Británie teoreticky nemůže dojít k jejímu marnému uplynutí, pokud je například daný blog stále navštěvován a čten, protože s každým návštěvníkem počíná běh lhůty nové.

---

[139] The Defamation Act 1996.

[140] Wild a kol. 2005, str. 25 a 26.

[141] Rawland a Macdonald 2005, str. 397.

[142] New York Times v Sullivan, 376 US 254 (1964).

Objektivní podmínkou identifikovatelnosti a toho, že osoba rozumí urážlivému kontextu je i fakt, že osoba, která přečetla danou zprávu, musí znát osobu žalobce (toho, jehož pověst utrpěla újmu) a rozumět tedy, že daná zpráva se vztahovala k němu.

Pokud dotčená osoba utrpěla újmu ve více státech, může podat kumulativní žalobu a žádat náhradu buď v jednom státě, nebo v každém zvlášť.

Je nasnadě, že žalobcem je ve valné většině případů sama osoba, jejíž pověst utrpěla daným výrokem újmu. Nyní je však třeba pojednat o druhé straně, tedy o potenciálním žalovaným, tedy osobou odpovědnou za defamující výrok. Primárně je zodpovědný sám autor daného výroku. Pokud dojde k takovému jednání v rámci výkonu pracovní činnosti pro zaměstnavatele, odpovědnost nese zaměstnavatel (podle anglické právní teorie jde o tzv. vicarious lability). Tak by tomu však nebylo, pokud by šlo pouze o čistě osobní záležitost, kterou nelze podřadit do rámce výkonu pracovní činnosti.[143]

V této souvislosti je nutné poznamenat, že právě z důvodu předcházení odpovědnosti za eventuální porušení zákona zaměstnancem, zaměstnavatelé monitorují téměř veškerou činnost zaměstnanců, včetně například jejich emailových schránek. V případě Hallford v UK[144] však Evropský soud pro lidská práva námitku, že šlo o monitorování činnosti zaměstnance zaměstnavatelem, odmítl s tím, že i zaměstnanec má právo na ochranu soukromí před svým zaměstnavatelem. Tudíž na základě tohoto rozsudku lze napadnout obdobné monitorování zaměstnanců.[145] Je otázkou, zda varování, že používání pracovního emailu či telefonu může být monitorováno, postačí k tomu, že uživatel nemůže rozumně očekávat soukromí a jeho ochranu. Proto se obecně používá ustanovení v pracovní či podobné smlouvě, kde zaměstnanec dává obecný souhlas s obdobnými praktikami. Podrobněji je o této problematice pojednáno dále v této práci.

Kromě autora a zaměstnavatele může však být odpovědný i poskytovatel informačních služeb (ISPs), kteří uveřejnili urážlivé výroky. Tento se však může odpovědnosti zprostit, prokáže-li, že uveřejnění nezavinil. DA tím poskytl účinnou obranu proti žalobě v případě, že osoba dokáže, a) že není autorem, editorem nebo uveřejnitelem daného výroku, b) že publikuje výroky s rozumnou mírou opatrnosti, c) a že nevěděl a neměl důvod se domnívat, že jeho jednání

[143] Lloyd 2008, str. 577.

[144] [1997] IRLR 471.

[145] Lloyd 2008, str. 577.

způsobilo nebo napomohlo uveřejnění urážlivého výroku.[146] Při vykládání uvedených kritérií soud přihlédne k míře odpovědnosti, konkrétním okolnostem uveřejnění i například k tomu, zda se podobné jednání vyskytlo opakovaně. Navíc se za uveřejnitele v této souvislosti nepovažuje ten, kdo nemá efektivní kontrolu nad osobou, která se urážlivého jednání dopustila. Tím je například telefonní operátor poskytující též internet, jak bylo rozhodnuto v případě Totalise plc v Motley Fool Ltd [2003] 2 All ER 872. Naopak, za odpovědného byl prohlášen jiný druh poskytovatele internetu. Šlo o poskytování internetu pomocí speciálního software, nad nímž měl celkovou efektivní kontrolu, což jej učinilo odpovědným pro nedostatečnou míru opatrnosti. Tento přístup byl přijat v rozhodnutí Godfrey v Demon Internet Ltd [1999] 4 All ER 342.[147] Směrnice o elektronickém obchodu[148] poskytuje ještě další výjimky z odpovědnosti ISPs ve článku 12, kde prohlašuje, že poskytovatel informační služby není odpovědný v případě, že se aktivně nepodílel na přenosu této informace (neinicioval, nevybral jejího příjemce, nebo se nepodílel na výběru či modifikaci přenášené informace).[149] V UK byla tato ustanovení provedena v paragrafu 19,[150] který stanoví obecnou výjimku z odpovědnosti ISP (jak trestní tak jiné) v případě, a) že o aktuálním protiprávním jednání nevěděl, případně, že nebylo zřejmé vzhledem k faktickým okolnostem, že jde o činnost protiprávní, b) anebo dozvěděl-li se o protiprávní činnosti, bez odkladu daná data vymazal nebo k nim zakázal přístup.[151] Dalším otázkám postavení a odpovědnosti ISPs je věnována samostatná kapitola.

Pokud jde o otázku, které národní právo se v případě vztahů s mezinárodním prvkem aplikuje, v rámci Evropy jí řeší článek 5(3) Bruselské úmluvy,[152] podle které žalobce může podat buď jednotnou žalobu ve státě, jehož je občanem nebo kde utrpěl újmu s účinky v ostatních státech EU, anebo může podat žalobu zvlášť v každém státě, kde utrpěl újmu na své cti. Wild k tomu

[146] The Defemation Act 1996, s 1(1).

[147] Reed 2004, str. 114.

[148] Směrnice Evropského Parlamentu a Rady č. 2000/31/ES ze dne 8.6.2000 o elektronickém obchodu.

[149] Wild a kol. 2005, str. 28.

[150] The Eletronic Commerce (EC Directive) Regulations 2002, SI 2002/2013.

[151] Lloyd 2008, str. 583.

[152] Úmluva o příslušnosti soudů a uznání a výkonu rozhodnutí ve věcech občanských a obchodních z roku 1968 (Bruselská úmluva).

uvádí, že proto bývá žaloba často podávána na území Velké Británie, protože tamní právo je pro žalobce výrazně příznivější než v jiných státech Evropské Unie.

V případě internetu řešil otázku jurisdikce australský odvolací soud v rozhodnutí Gutnik v Dow Jones [2002] HCA 2002, který shledal odpovědným deník publikovaný jen v New Yersey, ovšem na internetovém serveru. K této zprávě velmi rychle přibylo mnoho komentářů od internetových uživatelů celého světa. Australský soud rozhodl, že uveřejnitel na internetu může být shledán odpovědným jakýmkoli soudem, v jehož místě působnosti lze takový komentář stáhnout. Obdobný případ se vyskytl před anglickým soudem proti uveřejniteli v USA.[153]

Který soud bude příslušný v případě, že je dotčeno více států, posuzoval také Evropský soudní dvůr v případě Shevill and Others v Presse Alliance SA.[154] Podle tohoto rozhodnutí může dotčená osoba podat žalobu v jakémkoli nebo v každém místě, kde došlo ke škodlivé události nebo újmě. Může tedy jít o stát, ve kterém byla daná informace dána do oběhu, nebo kde byla daná informace přečtena, popřípadě kde žalobce má důležitou osobní pověst, jež byla dotčena (podle čl. 5(3) Bruselské konvence).

2.6 Ochrana soukromí při komunikaci na dálku

Tato část práce se zabývá právními aspekty různých forem elektronické komunikace. Jde o oblast velmi rychle se rozvíjející, což nese s sebou mimo jiné i mnohá rizika. Díky vysoké technické úrovni těch, kdo porušují existující bezpečnostní opatření, je velmi snadné narušit či získat obsah přenášených informací právě prostřednictvím elektronických sítí. Přestože fakticky je téměř nemožné zcela zabránit porušování soukromí a tajemství doručovaných zpráv, právní úprava se snaží přizpůsobovat nové realitě a jejím specifickým rysům.

Listina základních práv a svobod zaručuje tajemství záznamů a zpráv v článku 13, ať již jsou podávány telefonem, telegrafem či „jiným způsobem“, tedy i prostřednictvím internetu. Pokud jde o ochranu zpráv osobní povahy, vedle obecné úpravy správněprávní a trestněprávní, je zásadně poskytována i ochrana obecnou občanskoprávní úpravou v rámci všeobecného osobnostního práva podle § 11 a násl. OZ. Tyto prostředky však nelze aplikovat v případě zpráv jiné, nikoli osobní povahy. Tady pak je poskytována ochrana zejména veřejnoprávní, a to jak trestněprávní, tak správněprávní. Zatímco nedotknutelnost poštovních zpráv a zásilek je stanovena v zákoně o poštovních službách,[155] za sdělení chráněné tímto zákonem se zásadně

[153] King v Lewis [2004] EWHC 168.

[154] [1995] All ER (EC) 289.

[155] Zákon č. 29/2000 Sb., o poštovních službách a o změně některých zákonů (zákon o poštovních službách).

považuje pouze písemnost v listinné podobě. Proto tato ochrana se nevztahuje na tzv. emailové zprávy (zprávy zasílané prostřednictvím elektronických datových schránek) či zprávy zasílané pomocí jiných elektronických sítí.[156] Pro tuto oblast byl na základě evropské směrnice[157] přijat zvláštní zákon č. 127/2005 Sb. o elektronických komunikacích, jež uvedl naší úpravu do souladu s uvedenými evropskými cíly. Tento zákon je vyjádřením a transponováním druhotných předpisů evropského práva (směrnic), jejichž společným jmenovatelem je tzv. technologická neutralita. Jinak řečeno, stejné předpisy platí pro telekomunikační sítě stejně jako pro jiné sítě informačních technologie.[158]

Obsahem tohoto zákona a souvisejících předpisů je úprava systému přenosu, nikoli úprava obsahu přenášených zpráv. Zásadně se tedy tento zákon nezabývá obsahovou stránkou poskytovaných služeb ve formě textu, obrazu, zvuku apod. Orgánem dozoru této technické úpravy a jejího dodržování je pak Český telekomunikační úřad (ČTÚ), jenž je ústředním správním úřadem podle tohoto zákona. Hovoří se o tzv. oddělení regulace přenosu od regulace obsahu (§ 1 odst. 2). Vedle technických otázek však také pojednává o bezpečnosti poskytovaných služeb, ochraně osobních údajů a povahou blízkých údajů (provozní a lokalizační). Tzv. telekomunikační tajemství se vztahuje např. i na údaje o počátku a konci uskutečněného hovoru.

Jak vyplývá z definice sítí elektronických komunikací, jedná se o přenosové systémy, zařízení a jiné prostředky, zahrnující jak radiové, televizní, telefonní služby, včetně mobilních, dále například i přenos a poskytování služeb internetových (bez ohledu na to, zda je pozemní, satelitní či kabelová). Tuto definici položila již zmíněná rámcová směrnice č. 2002/21/ES.[159]

Zákon zejména zjednodušil podnikání v této oblasti, podle kterého po splnění stanovených požadavků existuje tzv. všeobecné oprávnění (podle § 8), které nahradilo do té doby obtížnou praxi poměrně složitého získávání individuálních licencí. Tím se v podstatě zavedla tržní pravidla a principy i do této ekonomické oblasti, do nichž by měl orgán dohledu zasahovat co nejméně. Přičemž však není dotčena ochrana hospodářské soutěže, v jejímž rámci provádí

[156] Mates, P. 2006, str. 138.

[157] Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích).

[158] Vaníček, Z. 2008, str. 14.

[159] Směrnice Evropského parlamentu a Rady 2002/21/ES ze dne 7. března 2002 o společném předpisovém rámci pro sítě a služby elektronických komunikací (rámcová směrnice).

vedle ČTÚ též Úřad na ochranu hospodářské soutěže. Ústřední správu v této oblasti provádí Ministerstvo průmyslu a obchodu, které zejména podporuje podnikání a infrastrukturu v této oblasti a nesmí žádným způsobem upřednostňovat některé subjekty či technologie tak, aby nedocházelo k narušování či ovlivňování hospodářské soutěže v této oblasti (§ 5 a 6 zákona).

Podle definice regulovaných komunikačních činností, se jedná o zajišťování sítí elektronických komunikací, poskytování služeb elektronických komunikací a provozování přístrojů (§ 7 odst. 1 zákona). Za podnikání v elektronických komunikacích se pak považuje zajišťování veřejných komunikačních sítí či poskytování služeb elektronických komunikací, jak uvádí § 8 odst. 1 písm. a) a b). Všeobecné podnikatelské oprávnění podle § 9 poté doplňuje pravomoc ČTÚ stanovit konkrétní podmínky, včetně opatření v souvislosti s ochranou osobních údajů a soukromí podle § 10 odst. 1 písm. f).

Základním principem ochrany soukromí podle tohoto zákona je důvěrnost zpráv a dalších údajů, kterou je povinen každý provozovatel veřejné komunikační sítě zajistit. Takové údaje nesmí být odposlouchávány, ukládány ani jinak zachycovány či sledovány jinou osobou než uživatelem samotným, leda by k tomu jiná osoba měla souhlas dotčených uživatelů. Výjimkou jsou opět tzv. zákonné licence, např. podle § 88 trestního řádu,[160] podle kterého policejní orgány jsou při vyšetřování trestné činnosti za stanovených podmínek oprávněny provádět odposlouchávání a záznam telekomunikačního provozu. Další výjimkou je například tzv. technické ukládání údajů, které je nezbytné z technických důvodů pro samotný přenos zasílaných zpráv.

Mají-li být jakkoli využívány či zpřístupněny údaje uložené v koncových zařízeních uživatelů (např. osobních počítačů), ti, kdo takové údaje hodlají využívat, mají povinnost předem uživatele informovat o rozsahu a účelu a nabídnout možnost toto odmítnout (výjimkou je opět technické ukládání či přístup nezbytný pro samotnou realizaci přenosu).

Ten, kdo poskytuje veřejně dostupnou službu elektronických komunikací, má také povinnost zabezpečit ochranu osobních údajů, provozních a lokalizačních údajů a důvěrnost komunikací. Vhodné zabezpečení je důležitým pravidlem, které stanovila také směrnice o soukromí a elektronických komunikacích v článku 4. Dopad tohoto ustanovení je dvojí, poskytovatel služby a provozovatel sítě musí přijmout vhodná bezpečnostní opatření a zároveň uživatel musí být informován o případném riziku a jeho předcházení.[161] Jde o opatření, které má

[160] Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád).

[161] Lloyd 2008, str. 165.

předcházet hrozbám označeným v preambuli této směrnice v bodě č. 24, jako je špionážní software, webové štěnice a podobné hrozby narušení bezpečnosti i soukromí bez vědomí samotného uživatele. Problematické, vzhledem k přirozené povaze elektronické komunikace, je nastavení úrovně ochrany, která má odpovídat stávajícím technickým možnostem, přiměřeným nákladům a existujícím rizikům ochrany. Opatření musí být zpracována formou vnitřního předpisu, který kontroluje úřad dohledu. V případě zvláštního rizika musí poskytovatel upozornit i samotného účastníka či uživatele včetně poučení o možnostech nápravy.

Další otázkou úzce spjatou s elektronickou komunikací jsou údaje o provedené komunikaci. Tyto se netýkají čistě obsahu přenášených informací, ale obsahují informace vedlejší, například časové a místní určení dané komunikace. Zákon i směrnice je nazývá údaji provozními a lokalizačními. Jejich zvláštní úprava je odůvodněna tím, že pomocí dostatečného množství takových údajů lze vytvořit obraz velmi dobře využitelný například pro komerční účely, ale také lze tímto způsobem získat poměrně přesný obraz o konkrétní osobě. Téměř každý dnes používá mobilní telefon, email či něco vyhledává na internetových stránkách. Všechny tyto údaje bývají v praxi prodávány většinou telekomunikačními operátory třetím stranám, kteří jejich pomocí prodávají své služby či je jinak využívají zejména k marketingovým účelům.

Provozní údaje, podle § 90 zákona č. 127/2005 Sb., o elektronických komunikacích (i podle čl. 2 písm. b) směrnice o soukromí a elektronických komunikacích) jsou všechny údaje, které jsou zpracovány pro potřeby přenosu zprávy nebo pro její zúčtování. Řadí se mezi ně například údaje jako číslo účastníka, čas, kdy byla daná zpráva odeslána, kdo jí odeslal a jaké byla datové velikosti. Tyto mohou být zpracovány pouze pro stanovený účel, tedy pro technické uskutečnění přenosu a pro vyúčtování. Dále mohou být zpracovány i pro účely poskytování služeb s přidanou hodnotou či pro účely marketingu, v těchto případech však musí být zákazník informován a vyžádán jeho souhlas, který může také vzít kdykoli zpět. Stejně jako u zpracování jiných osobních údajů platí zásada nezbytnosti (zpracování dat pouze v nezbytném rozsahu a po nezbytnou dobu).

Lokalizační údaje jsou definovány jako údaje, které určují zeměpisnou polohu koncového zařízení uživatele veřejně dostupné služby elektronických komunikaci, např. mobilních telefonů.[162] Zvláštní úprava se však týká jen těch, které jsou odlišné od provozních údajů.[163] Tyto

[162] Čl. 2 písm. c) směrnice o soukromí a elektronických komunikacích a § 91 zákona č. 127/2005 Sb., o elektronických komunikacích.

[163] Čl. 9, ibid.

údaje musí být anonymizovány, anebo musí být k jejich zpracování vždy dán předchozí souhlas daného zákazníka či uživatele. Přičemž tento souhlas musí být jednoduše a zdarma umožněno vzít zpět nebo omezit (a to při každém připojení k síti či přenosu sdělení).
Obojí, jak provozní tak ostatní lokalizační údaje pak může zpracovávat pouze poskytovatel služeb elektronické komunikace či osoba jím pověřená, popřípadě poskytovatelem služeb s přidanou hodnotou, přičemž vždy pouze při dodržení zásady nezbytnosti.

Povinností je, že tyto údaje, jakmile se stanou nepotřebnými k danému účelu, musí být anonymizovány nebo smazány. Zachování je nutné pouze ve stanovených případech, kterými je oprávněné provádění odposlechu a záznamu zpráv (§ 97 zákona), nebo je-li to nezbytné k provedení vyúčtování služby (pouze však do konce promlčecí doby pro případné napadení vyúčtování), anebo pokud je to nutné k zajištění propojení sítí, vyúčtování či k identifikaci zneužívání sítě a služeb v rámci jiné sítě elektronických komunikací. Poskytovatelé si tedy mohou údaje mezi sebou předávat k uvedeným účelům, aniž by bylo třeba souhlasu uživatele. V neposlední řadě jsou poskytovatelé oprávnění zpracovávat provozní údaje i pro účely marketingu služeb či poskytování služeb s přidanou hodnotou (tzv. nabídka dalších služeb). I zda však platí zásada, že lze zpracovávat pouze údaje nezbytné pro daný účel, přičemž podmínkou v této souvislosti je předchozí souhlas uživatele, který může být kdykoli odvolán. Navíc účastník/uživatel musí být o rozsahu údajů a době jejich zpracování poskytovatelem informován. Je nutné si také uvědomit, že pokud pomocí těchto údajů je identifikovatelná osoba, tyto údaje spadají svojí povahou do kategorie osobních a podle toho s nimi musí být při jejich zpracování nakládáno.

Sledování zpráv a omezení ochrany zpráv i telekomunikací je možné pouze v režimu článku 8 odst. 2 Evropské úmluvy[164]. Navíc podle výkladu Evropského soudu je ochrana poskytována jak komunikacím uskutečněným ze soukromého, tak ze služebního přístroje.[165] Omezení je tedy v ČR přípustné pouze na základě zákona a pro stanovený účel. Tak ve většině případů jde o orgány činné v trestním řízení v rámci stíhání a předcházení trestné činnosti (zejména podle § 88 trestního řádu), dále o Bezpečnostní informační službu a Vojenské obranné zpravodajství. Navíc o každém takovém oprávnění je nutné předložit rozhodnutí soudu, popř. souhlas samotného

[164] Evropské úmluvě o ochraně lidských práv a základních svobod 1950.

[165] Mates, P. 2006, str. 147.

účastníka. Provozovatelé jsou povinni uchovávat údaje provozní a lokalizační po dobu nejdéle 12 měsíců, které musí být na požádání Policie ČR poskytnuty.

V této souvislosti je třeba upozornit na to, že bez příslušného souhlasu, nelze provádět kontrolu či odposlouchávání žádného druhu komunikace. Tedy za protiprávní se považuje například odposlouchávání a kontrola zaměstnaneckých emailových zpráv bez dostatečného souhlasu. Zaměstnavatel má však právo monitorovat počet emailů zasílaných z pracoviště, má právo např. vnitřními předpisy zakázat užívání pracovních emailových schránek pro soukromé účely, musí však o tomto zaměstnance předem a srozumitelně informovat. Jak uvádí doc. Mates, v žádném případě však nemá právo číst obsah předávaných zpráv.[166] K této otázce také je nutné uvést, že ne vždy dochází k zpracovávání osobních údajů monitorováním emailových zpráv zaměstnavatelem ve smyslu zákona o ochraně osobních údajů. Zpracováním totiž není nahodilé zpracování, tedy například nahodilé prohlédnutí emailových zpráv by zřejmě do rámce tohoto zákona nespadalo. To však neznamená, že takové nahodilé kontrolování či čtení elektronické pošty zaměstnanců je dovoleno. Podle všeobecného osobnostního práva ve smyslu § 11 a násl OZ jsou písemnosti osobní povahy chráněny (§ 12). Navíc ochrana, jak je blíže pojednáno v části týkající se tohoto tématu je poskytnuta v rámci jiných záruk tohoto základního lidského práva, jako je v našem právním řádu čl. 13 Listiny základních práv a svobod a mimo jiné i prostřednictvím práva trestního.[167] V některých případech samotná adresa elektronické pošty naplňuje znaky zákonem chráněného osobního údaje, a to v případech, kdy obsahuje osobní údaje svého majitele, jako například jméno a příjmení.[168]

Zákon o elektronických komunikacích, pokud jde o ochranu osobních údajů, odkazuje na zvláštní úpravu podle zákona č. 101/2000 Sb., o ochraně osobních údajů v § 87 odst. 1, přičemž v odstavci 2. prohlašuje, že za souhlas se zpracováním osobních údajů podle tohoto zákona se považuje i souhlas učiněný pomocí elektronických prostředků, zejména vyplněním formuláře v obsahu stránky poskytované na internetu.

V § 93 pak zákon o elektronických komunikacích zakazuje zneužití elektronické adresy odesílatele, za které považuje použití adresy elektronické pošty pro odeslání zprávy nebo zpráv třetím osobám bez souhlasu držitele této adresy.

---

[166] 2006, str. 150.

[167] § 182 zákona č. 40/2009 Sb., trestního zákoníku.

[168] Macková, A., a Štědroň, B. 2009, str. 363.

V této souvislosti je též důležité upozornit na úpravu odposlechu a záznamu zpráv podle § 97 zákona o elektronických komunikacích. Tak na základě písemné žádosti a rozhodnutí příslušného soudu, o které mohou požádat pouze uvedené subjekty (Policie ČR, BIS, Vojenské zpravodajství), je povinen podnikatel zřídit a zabezpečit (na náklady žadatele) zařízení pro odposlech a záznam zpráv. Kromě toho je podnikatel povinen vždy povinen uchovávat provozní a lokalizační údaje po dobu mezi 6 až 12 měsíci také pro účely případného vyžádání příslušnými subjekty (§ 97 odst. 3 téhož zákona). Tato povinnost byla uložena na základě směrnice o uchovávání údajů č. 2006/24/ES (data retention).[169] Jde o poměrně rozporuplné ustanovení, které mimo jiné znamená nemalé náklady pro podnikatele.

Dalším nástrojem, který tento zákon zavádí, je zamezení zobrazení účastnického čísla, což je provozovatel sítě či poskytovatel služby povinen zajistit jednoduchým a bezplatným způsobem. Navíc také účastník (uživatel) musí mít možnost jednoduchým způsobem zamezit automatické přesměrování volání třetí stranou.

Pokud jde o vydávání seznamů účastníků (ať v elektronické či tištěné podobě), k zařazení účastníka do seznamu a uveřejnění jeho údajů je nezbytný předchozí souhlas daného účastníka, anebo možnost uvést, že si nepřeje být kontaktován pro marketingové účely.

Dalším opatřením je identifikace zlomyslných a obtěžujících volání podle § 67 zákona o elektronických komunikacích. Na žádost účastníka je povinen podnikatel zajistit na náklady účastníka službu identifikace účastnického čísla, z kterého byla uskutečněna zlomyslná nebo obtěžující volání, a to zpětně u konkrétních volání (nejpozději však 2 měsíce zpětně od jejich uskutečnění). Tím se rozumí poskytnutí údajů o fyzických či právnických osobách, které dané volání provedly.

Nedodržení povinností či podmínek podle tohoto zákona jsou správními delikty (podle § 118 zákona o elektronických komunikacích), za které může být uložena pokuta až do výše 10 milionů Kč (například neoprávněné podnikání v této oblasti, či nesplnění povinností souvisejících se shromažďováním osobních údajů). Za delikt například zneužívající elektronickou adresu bez souhlasu jejího majitele lze uložit pokutu až 5 milionů Kč. Těchto správních deliktů se však může dopustit jedině právnická či podnikající fyzická osoba.

[169] 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.

Fyzické osoby jsou odpovědné za přestupky podle § 120 téhož zákona, například za uskutečnění zlomyslného volání na tísňové číslo, zneužitím adresy elektronické pošty či nabídnutím marketingové reklamy v rozporu s právními povinnostmi. Za takový přestupek může být uložena pokuta do 100 000 Kč.

Jak přestupky, tak správní delikty, projednává ČTÚ, který navíc v případě recidivy (opakování porušení zákona v průběhu 2 let) může uložit až dvojnásobek stanovené sazby.

Opravným prostředkem proti rozhodnutí ČTÚ je pak podle § 123 odvolání nebo rozklad. V ostatních věcech se řídí právní vztahy obecnými předpisy správního práva.

V souvislosti s tématem ochrany soukromí a osobních údajů a případné odpovědnosti za jejich porušení je významné ustanovení § 61 odst. 5, které zásadně vylučuje odpovědnost podnikatele poskytujícího veřejně dostupnou službu elektronických komunikací za obsah přenášených zpráv. Takovou odpovědnost nese v plném rozsahu jeho původce.[170]

2.7 Přímé obchodování

V důsledku velkého rozvoje internetu a produktů či služeb, které v jeho rámci bývají nabízeny a prodávány, byla právní úprava nucena zareagovat. Praktiky, které se pro různé obchodní a marketingové účely začaly používat, totiž výrazným způsobem zasahují do soukromé oblasti každého uživatele, který o tom často nemá ani tušení. Navíc některé způsoby reklamy se stávají čím dál více obtěžujícími pro každého uživatele internetu. Jak bývá internet užíván a zneužíván pro obchodní účely, to je předmětem této části práce.

2.7.1 Reklama a spam

Regulace reklamy, která je svojí podstatou neosobním, jednostranným sdělením, jehož cílem je podat potenciálnímu zákazníkovi informaci o nabízených službách či výrobcích, je regulována napříč právním systémem. Občanskoprávní úprava všeobecného osobnostního práva zejména omezuje užívání podobizen, hlasových projevů apod. pro reklamní účely. Obchodněprávní úprava zakazuje nekalosoutěžní jednání. Veřejnoprávní regulace se pak zaměřuje na ty jevy, které jsou v širším zájmu. Úprava reklamní činnosti je obsažena v zákoně č. 40/1995 Sb., o regulaci reklamy a v zákoně č. 231/2001 Sb., o provozování rozhlasového a televizního vysílání.

Právní předpisy hovoří o tzv. komunikačních médiích, jejichž příkladmý výčet v zákoně o regulaci reklamy zahrnuje periodický i neperiodický tisk, rozhlasové i televizní vysílání, ale také pro tuto oblast důležité počítačové sítě, audiovizuální produkce či nosiče.

[170] Vaníček, Z. 2008, str. 226.

Podle § 2 jsou některé druhy reklam, například tzv. podprahové (působící na podvědomí člověka), nevyžádané či skryté, zakázány zcela. Zejména, pokud jde o nevyžádanou reklamu, jedná se o takovou, která může adresáta obtěžovat a tím narušovat jeho soukromou sféru. Jejím projevem je například vhazování reklamních letáků do schránek, kde je jasné prohlášení o tom, že si to její majitel nepřeje. V rámci elektronického světa, § 95 zákona o elektronických komunikacích dává obdobnou možnost prohlášení také účastníkovi (uživateli) elektronických sítí a služeb.

Zákon o regulaci reklamy pak rozděluje odpovědné osoby za porušení tohoto zákona na zpracovatele (kdo pro sebe či jiného zpracovává reklamu), zadavatele (kdo u jiného reklamu objednal) a šiřitele (kdo reklamu veřejně šíří. Zpracovatel plně odpovídá za obsah reklamy, pokud jí zpracoval pro vlastní potřeby. Jinak za zákonnost reklamy solidárně odpovídají jak zpracovatel, tak zadavatel reklamy. Odpovědnost šiřitele je dána pouze za způsob šíření dané reklamy.

Odlišný přístup z pohledu legislativního je zvolen ve Velké Británii, kde je základní právní úprava reklamní činnosti ponechána na orgánech samoregulace. Tyto vydávají závazné předpisy ve formě zásad a stanov,[171] na které dohlíží a vynucuje jejich dodržování příslušná komise.[172]

Spam

Za zvlášť obtěžující formu reklamy, proti které je obrana velmi nákladná, se považuje tzv. spam nebo junk mail, který je typický svojí elektronickou podobou. Důkazem důležitosti a aktuálnosti tohoto jevu je i přijetí zvláštní úpravy podle směrnice č. 2000/31/ES o elektronickém obchodu a směrnice č. 2002/58/ES o soukromí a elektronických komunikacích, které byly mimo jiné transponovány do zákona o některých službách informační společnosti v roce 2004.[173] Podle něj je upraveno šíření obchodních sdělení (přičemž však spam může ve své podstatě znamenat jakékoliv hromadné, obtěžující a opakující se sdělení, ovšem naše právní úprava se bohužel vztahuje jen na obchodní) elektronickou poštou (v jejím širším slova smyslu, tudíž zahrnuje i telemarketing či SMS zprávy). Dovoleno je využít elektronickou poštu pro účely marketingové pouze, pokud s tím dal zákazník předem souhlas (§ 7 odst. 2) Souhlas však není třeba v případě, že potřebné údaje jsou získány od uživatele v rámci prodeje výrobku či služby, pokud bylo

[171] The British Code of Advertising, Sales Promotion and Direct marketing, nebo the Direct marketing Association Code of Practice.

[172] The Committee on Advertising Practice (CAP).

[173] Zákon č. 480/2004 Sb., o některých službách informační společnosti.

zákazníkovi jasně a zřetelně umožněno jednoduchým způsobem odmítnout souhlas s takovým využitím v každém jednotlivém případě zaslání obchodního sdělení (tzv. opt-in metoda). Náležitosti souhlasu se řídí ustanovením § 4 písm. n) zákona o ochraně osobních údajů, tudíž musí být mimo jiné vždy prokazatelný. Jinak je šíření obchodních sdělení zakázáno. Zakázáno je šíření sdělení, které není za obchodní sdělení označeno, které neobsahuje či skrývá totožnost odesilatele, nebo které je zasláno bez platné adresy (§ 7 odst. 4). Problematický boj, jenž ve své podstatě nelze vyhrát, je však se spamem ze zahraničí, který je jen velmi těžko postižitelný a dohledatelný. Poskytovatelé služeb (jako například služeb elektronické pošty) tedy musí přijímat velmi nákladná filtrovací opatření, aby k obtěžování jejich zákazníků docházelo co nejméně.

Orgánem dozoru v těchto věcech je zásadně Úřad pro ochranu osobních údajů, popřípadě samosprávná profesní komora, jedná-li se o činnost regulovaného subjektu.

Pokud jde o odpovědnost podle tohoto zákona souvisejících s šířením obchodních sdělení, právnická osobě může být za porušení povinností podle tohoto zákona uložena pokuta až 10 000 000 Kč, právnické osobě vykonávající regulovanou činnost pak 1 000 000 Kč. Přičemž odpovědnosti se zprostí, pokud prokáže vynaložení veškerého úsilí, které je možné požadovat, aby porušení právní povinnosti zabránila, podle § 12 odst. 1 zákona. Přičemž v odst. 3 paragrafu 12 je prekluzivní lhůta subjektivní 1 rok a objektivní 3 roky, po jejímž uplynutí odpovědnost za správní delikt zaniká. Stejná odpovědnost se vztahuje i na fyzické osoby při podnikání.

Pojetí odpovědnosti v souvislosti se spamy je přísnější v USA, kde je tato činnost mimo jiné i kriminalizována. [174]

Spam z pohledu ochrany osobních údajů

Vedle samotného způsobu využití elektronických prostředků k obchodním účelům, je právně upraveno i samotné zpracování osobních údajů v souvislosti s marketingem. Samotné nakládání s údaji jako je elektronická pošta pro účely zaslání spamu je svojí povahou zpracováním ve smyslu ochrany osobních dat. Správce tak může zpracovávat pouze údaje nezbytné (jimi jsou jméno, příjmení a adresa). Nesmí tedy bez souhlasu dotčené osoby užívat například údaje o majetkových poměrech či povolání, jak vyplývá z dikce § 5 a 6 zákona o ochraně osobních údajů. Navíc předávání těchto údajů jinému správci za účelem nabízení obchodu a služeb, je možné jen, pokud tyto údaje byly získány v souvislosti s jeho činností, budou využity pouze k stejnému (marketingovému) účelu, a subjekt byl o tomto postupu předem informován a

[174] The Controlling the Assault of Non-solicited Pornography and Marketing Act 2003.

nevyslovil s tím nesouhlas (písemně). Další aspekty a odpovědnost za porušování stanovených povinností se řídí podle zákona o ochraně osobních údajů (viz. kapitola o ochraně osobních údajů).

Velkým problémem však v této oblasti zůstává, že pokud jde o ochranu osobních údajů, pouze dotčená osoba má na této ochraně zájem. Pro ni je jen těžko myslitelné podniknout kroky bránit se proti původci spamu, ať již z finančních nebo praktických důvodů, natož pak mít možnost bránit se preventivně. Z toho důvodu jsou hlavní osobou, které se dotýkají ekonomické dopady, právě ISPs. Rozšíření jejich pravomocí jak pokud jde o možnost soudní ochrany, tak pokud jde o vyšetřování (vysledování původce spamu) by bylo zdaleka efektivnější. Lze tedy uzavřít, že otázka spamu je většinou porušováním systému ochrany soukromí a osobních údajů, avšak právní prostředky ochrany jsou ve skutečnosti jen málo efektivní. Problematické je také to, že cestou technického řešení je vyřešení spamu také téměř nemyslitelné, protože spolu s technickým pokrokem se dostávají do popředí i ti, kdo technologie využívají nezákonným způsobem. Navíc obrana proti anonymním spamům či těm, které pochází z míst mimo EU je téměř nemožná.

2.7.2 Cookies

Malé textové soubory, do kterých se ukládají informace o daném internetovém uživateli, například o slovech, které vyhledával, o produktech, o které se zajímal, a podobně, se označují za tzv. cookies. Tyto soubory se ukládají do počítače uživatele, a nejvíce je využívají při internetoví obchodníci (jako např. eBay nebo Amazon) za účelem usnadnění prohlížení stránek při příští návštěvě internetu. Díky nim dokáže daná stránka či vyhledávač nabízet uživatelem často hledané výrazy a slova, aby tento nemuselo příště psát celé slovo a urychlil tak svojí práci. Vedle toho, však tyto údaje mohou být využity i k jinému účelu. Obchodníci se jejich pomocí mohou zaměřit na určité druhy zákazníků, provádět průzkumy trhu, anebo je využít k reklamním účelům. Takové informace mohou mít poměrně vysokou tržní hodnotu a bývají proto prodávány třetím osobám.

Nutno je však upozornit, že ne všechny cookies jsou svojí povahou osobními údaji. Vrátíme-li se zpět k základní definici, musí z nich být dotčená osoba alespoň nepřímo identifikovatelná. Typicky jimi budou takové soubory, které si pamatují uživatelská jména a přístupová hesla k internetovým stránkám či službám. Na druhou stranu i ta, která se nespadají do této kategorie, jsou regulována směrnicí o elektronických komunikacích v tom smyslu, že

jejich užití musí být vysvětleno uživateli a musí mu být dána možnost odmítnout umístění souborů cookies do jeho počítače.[175]

V době projednávání směrnice 2000/31/ES o elektronickém obchodu[176] byl původní záměr zakázat užívání cookies zcela. Nakonec však úprava byla přijata až v rámci směrnice o elektronických komunikacích, kde článek 5 odst. 3 uvádí povinnost předchozího jasného a úplného informování uživatele a poskytnutí možnosti takovéto zpracování údajů odmítnout. Otázkou, zda je v souladu s tímto ustanovením praxe, že při první návštěvě dané stránky je písmem velmi malé velikosti napsáno upozornění a předem je zaškrtnuto políčko „souhlasím", dostatečné, to je při nejmenším diskutovatelné.[177] Pokud jde o provedení směrnice v UK, žádné konkrétnější ustanovení co do způsobu informování uživatele o cookies neexistuje. Přesto však mají uživatelé právo požadovat po daném správci, aby nezpracovával a neužíval jeho údaje například k reklamním účelům, čemuž je správce povinen do 21 dnů vyhovět například právě zakázáním používání cookies ve vztahu k danému uživateli.[178]

2.8 Některé související aspekty

V této části je představeno několik specifických oblastí, které jsou velmi aktuální problematikou spojenou s internetovou sítí. Půjde zejména o čím dál více užívaný nástroj komunikace mezi lidmi, tzv. sociální sítě, pomocí kterých dochází nejen k častému odhalování a zasahování soukromí samotných uživatelů, ale také k zneužívání informací pro různé protiprávní činnosti. Dalším tématem je proces odhalování a stíhání trestné činnosti pomocí internetu. Zejména kontroverzní se jeví úprava ve Velké Británii, kde jsou dány velmi široké pravomoci při odposlouchávání komunikace. Dalším tématem jsou peer-to-peer sítě, které jsou z pohledu autorského práva jedním z nejčastějších nástrojů porušování práv. Na to navazuje i úprava postavení poskytovatelů služeb informační společnosti, jejichž role se zdá být čím dál více důležitá. Nakonec je uvedeno i několik informací k monitorování komunikace zaměstnanců zaměstnavateli a možné důsledky.

[175] Carey 2004, str. 238.

[176] Směrnice 2000/31/ES o elektronickém obchodu, ze dne 8. června 2000.

[177] Edwards a Waelde 2009, str. 514.

[178] Carey 2004, str. 239.

2.8.1 Sociální sítě

Jak již bylo zmíněno, v internetovém prostředí je velmi jednoduché a rychlé přemístit server či webovou stránku. Navíc v takto propojeném prostředí se velmi rychle přenáší data mimo území EU, takže samotné zpracování osobních údajů probíhá většinou mimo evropský právní režim. Spolu s rozvojem elektronické komunikace se i přístup společnosti k některým jejím dopadům výrazně mění. Zejména mladší generace má tendenci neohlížet se příliš na vlastní soukromí. Důkazem je velký rozvoj a otevřené používání různých druhů elektronických sociálních sítí, jejichž prostřednictvím lidé sdělují často velmi detailní informace o svém osobním životě, bez ohledu na možné důsledky.

Demonstrativním případem byl v roce 2007 student filozofie na univerzitě v Oxfordu. Díky údajům od společnosti Facebook, provozující jednu z největších sociálních síti na světě, byl student odhalen při porušování disciplinárních pravidel univerzity a sankcionován. Student byl pobouřen a poukazoval na to, že jde o nepřípustný zásah do jeho soukromého života. Klíčovou otázkou však v této souvislosti je, zda se skutečně prostředí elektronických sociálních sítí považuje za soukromé, kde je rozumné očekávat ochranu poskytnutých údajů. Anebo zda jde povahou internetu jako takového o veřejně přístupné místo, kde nelze rozumně očekávat soukromí a její ochranu. Podle dosavadního přístupu právní i soudní praxe se internetové prostředí v některých situacích považuje za soukromé prostředí.[179]

Z pohledu zpracování osobních údajů je pozice poskytovatelů služeb elektronických sociálních sítí poměrně jasná. Považují se za správce údajů, který ke zpracování osobních údajů každého uživatele musí mít jeho předběžný souhlas. Tak nejpozději v průběhu registrace, jejíž součástí je i přijetí obecných podmínek, dochází k udělení potřebného souhlasu. Problematičtější je však případ jednání samotných uživatelů, kteří například zveřejní informace (například fotky) o jiné osobě. Takto byla úspěšná žalobkyně v případě Lindqvist, protože na internetové síti její kolegyně z náboženské společnosti uveřejnila fotky, na kterých byla mimo jiné vyobrazena i ona, aniž si předem vyžádala její souhlas. Nejvíce problematické je však zpřístupnění mnoha osobních údajů třetím osobám. Tak například zaměstnavatelé prověřují své zaměstnance či žadatele o práci, obchodní partneři vyhledávají informace a případné záminky při obchodním jednání, pachatelé trestné činnosti mohou zjistit údaje potřebné k zamýšlenému účelu (například,

[179] Listina základních práv Evropské Unie z roku 2000 čl. 8, soudní rozhodnutí německého ústavního soudu z roku 2008 (přístupné na adrese http://bendrath.blogspot.com/2008/02/germany-new-basic-right-to-privacy-of.html), nebo rozhodnutí soudu New Jersey ze stejného roku (New Jersey v Reid, Supreme Court of New Jersey (A-105-06) 21 April 2008).

zda dotčená osoba je či není aktuálně doma), a v neposlední řadě média takto zjišťují informace o veřejně známých osobách. Edwards upozorňuje, že taková data i po jejich vymazání či zrušení účtu zcela zůstávají uložená a případně přístupná či dohledatelná na příslušných hostitelských serverech.[180] Tento trend však více než právním je společenským, neboť platí jedna ze základních zásad, že každý by měl dbát svých práv a zejména, jde-li o soukromí, ochrana může být poskytnuta toliko tomu, kdo sám své soukromé údaje chrání a nezpřístupní je veřejnosti.

2.8.2 Odhalení a stíhání trestných činů v internetovém prostředí

Jak již bylo zmíněno, internetové prostředí se stalo mimo jiné i novým prostředím, kde, nebo jehož pomocí, lze páchat trestnou činnost. V souvislosti s tím se vyvinuly i nové trestné činy, na což se snaží reagovat mezinárodní i vnitrostátní právní úprava. Společně s trestnou činností se však musí měnit i prostředky, jak takovou činnost vysledovat, či pokud možno, jak jí předcházet. Proto v následujících odstavcích se budeme zabývat tím, jaký je právní rámec vyšetřovacích nástrojů, a jaké jsou jejich dopady na soukromí jednotlivců.

Základní právní rámec, kterým je umožněno omezit právo na soukromí fyzických osob, tvoří článek 8 odst. 2 Evropské konvence a evropská směrnice 2002/58/ES o elektronických komunikacích (čl. 15) společně se směrnicí č. 2006/24/ES o uchovávání údajů. Podle nich je možné omezit právo na soukromí a uchovávat údaje o komunikaci, je-li to nezbytné z důvodů obrany, národní bezpečnosti nebo prevence, vyšetřování a stíhání trestné činnosti. Vždy musí být dodržena zásada proporcionality a nezbytnosti, avšak právě jejich pojetí a výklad činí možnost odlišného přístupu v různých zemích Evropské Unie.

Z pohledu metodologického, lze rozeznat několik druhů sledování: fyzické, psychologické a sledování datové.[181] Tento výklad se zaměřuje na nejvíce pasivní metodu, sledování dat, jež bývá využívána v prostředí elektronických sítí. Ačkoli je nutné si uvědomovat, že výsledky všech metod bývají převáděny do elektronické podoby, čímž se jejich povaha dostává do režimu datového (jak je tomu například při sledování digitálními kamerami jak veřejných míst, tak například na pracovišti).

Důležitou událostí, která předznamenala budoucí vývoj v oblasti odposlouchávání a sledování provozu na internetu (tzv. internet surveillance), byly teroristické útoky 11. září 2001 v USA,

[180] 2009, str. 480.

[181] Lloyd 2008, str. 12.

v roce 2003 v Madridu a 2005 v Londýně. Za účelem boje proti terorismu a ochraně státní a veřejné bezpečnosti byla přijata opatření, která na jednu stranu posilují a zefektivňují zejména prevenci i vyšetřování trestné činnosti, avšak jejichž logickým důsledkem je restrikce soukromí individuálních osobností. Nejvíce ohrožené země, zejména USA a UK zaujaly poměrně razantní přístup, odlišný od ostatních zemí EU.

V UK je ponechána velmi široká pravomoc orgánům výkonné moci, které mohou autorizovat a dohlížet nad odposlouchávání a sledováním provozu elektronických sítí, aniž by do toho zasahovaly soudní orgány. Tak může sledování nařídit v podstatě každé ministerstvo, národní i místní orgány státní správy, a dokonce i některé další orgány jako poštovní kancelář či orgán dohlížející na standardy potravin.[182] V ostatních zemích EU je výrazně větší důraz na dohled a autorizaci prostřednictvím orgánů moci soudní. Přístup UK je obhajován zejména otázkou rychlosti a efektivity, a také tím, že pro soudní povolení by bylo nutné odkrýt mnoho citlivých údajů, zejména pokud jde o metody sledování, což by mohlo znamenat jejich neefektivnosti v budoucnu. Právě vědomí pachatelů trestných činů, že mohou být sledovány či odposlouchávány, má mít preventivní účinky. Na druhou stranu je nutné vždy dodržovat zásadu proporcionality, což je v případě počtu a typu institucí, které mají oprávnění autorizovat odposlouchávání v UK, při nejmenším diskutabilní.

2.8.2.1 Z pohledu lidských práv a svobod

Přístup z pohledu lidských práv a ochrany soukromí a soukromého života je vyjádřen jak v článku 12 Univerzální Deklarace Lidských Práv z roku 1948, tak v článku 8 Evropské konvence z roku 1950 (dále též Konvence). Konvence uvádí, že každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence. Zásahy do práva na soukromí jsou dovolené jen státním orgánem, v souladu se zákonem, je-li to nezbytné v demokratické společnosti v zájmu národní nebo veřejné bezpečnosti, z ekonomických důvodů země, z důvodů předcházení trestných činů a porušování veřejného pořádku, z důvodů ochrany zdraví a morálky nebo z důvodu ochrany práv a svobod druhých.[183]

K metodám utajeného odposlouchávání se vyjádřil Evropský soud pro lidská práva (ESLP) v případě Klass v Germany[184], který posuzoval odposlouchávání telekomunikačních konverzací. Prohlásil, že i toto prostředí je soukromým ve smyslu článku 8 Konvence. Obdobně i

[182] Schedule 1. The Privacy and Electronic Communications (EC Directive) Regulations 2003.

[183] Článek 8 odst. 2 Evropské konvence.

[184] [1978] 2 EHRR 214.

v případě emailu a jiného způsobu užívání internetu se považuje za prostředí spadající pod článek 8.[185]

Konvence se stala součástí britského právního řádu od roku 2000, kdy vstoupil v účinnost zákon (the Human Rights Act 1998) který jí inkorporoval. Tamní právní systém je příkladem monistického právního systému, tudíž, na rozdíl od našeho (dualistického), předpisy mezinárodního práva se stávají jeho součástí nikoli schválením a ratifikací, ale po ratifikaci musí být přijat zvláštní zákon, jenž jej inkorporuje. Od té doby tedy soudy kladou větší důraz na výklad a aplikaci domácího práva ve světle a v souladu s Konvencí než tomu bylo do té doby. Přesto však v případě UK bývá z hlediska Konvence často shledáváno, že dává příliš velké pravomoci k zásahům do práva na soukromí zejména sekundárními prameny práva (jako například směrnicemi, nařízeními či instrukcemi) na rozdíl od primárních zákonů, čímž činí poměrně složité pro fyzické osoby předvídat a kontrolovat, kdy a v jakém rozsahu mohou být jejich práva omezena.[186] Navíc v případě angloamerického právního systému může zákonné omezení vyplývat i z common law založeného na soudních precedentech, jak bylo vyloženo ESLP v případě Malone v UK.[187]

Každé omezení (například v zájmu národní bezpečnosti) musí být vždy na základě proporcionality mezi chráněným zájmem (individuální soukromí) a důvodem zásahu do něj.[188] Zároveň je stát povinen zajistit zásah v co nejmenší nutné míře, jak bylo potvrzeno v případě Campbell v UK [1993] 15 EHRR 137.

Od roku 2000 byl ve Velké Británii přijat nový zákon zabývající se pravomocemi spojenými s vyšetřováním protiprávní činnosti, the Regulation of Investigatory Powers Act 2000 (RIPA), který mimo jiné založil základní legální rámec a pravidla pro odposlouchávání a monitorování komunikace prostřednictvím internetu. Zákon zavedl obecný delikt, protiprávní odposlouchávání (§ 1 RIPA). Aby bylo sledování a odposlouchávání zákonné, musí být dodrženy následující podmínky. Primárním pravidlem je nezbytný předchozí souhlas jak odesílatele, tak příjemce zprávy. Toto pravidlo má výjimky, zejména v případě poskytovatele komunikační služby, je-li to

[185] Copland v UK [2007] ECHR 62617/00.

[186] Edwards a Waelde 2009, str. 550.

[187] [1984] 7 EHRR 14.

[188] Jersil v Denmark [1995] 19 EHRR 1.

nutné k provozu dané služby, anebo je-li to nezbytné k plnění jeho zákonných povinností.[189] Pokud nejde o tento případ, je zásadně nezbytné provádět takovou činnost jedině na základě autorizace příslušným státním orgánem či institucí.

Zákon neposkytuje žádnou zvláštní ochranu důvěrných informací, avšak tato kategorie má být respektována podle směrnic vydaných vládou, podle nichž má být s takovými informacemi nakládáno se zvláštní opatrností, přičemž tyto informace mohou být odposlouchávány jen v souvislosti s podezřením z trestné činnosti. Jde například o informace čistě důvěrné osobní povahy.[190]

Článek 12 RIPA potom umožňuje uložení povinnosti veřejným poskytovatelům telekomunikací (ISPs) provádět a tudíž i financovat příslušné odposlouchávání. Tento článek se samozřejmě setkal s velkou kritikou zejména ze stany ISPs. Proto vláda souhlasila s nárokem na částečnou náhradu případných nákladů, jak je předpokládáno v článku 14.

Dohled v rámci RIPA je svěřen zvláštnímu Komisaři[191] (článek 57 a násl. RIPA) a Tribunálu (článek 65 a násl. RIPA). Komisař zejména monitoruje a dohlíží na výkon a dodržování tohoto zákona. Ovšem pokud jde o výkon a autorizaci odposlouchávání, jeho rozhodnutí je konečné. Jak již bylo zmíněno v úvodu této části, nejde o nestrannou soudní instituci, jak je to běžné v ostatních evropských státech.

Navíc následná ochrana a přezkum před Tribunálem je velmi omezená faktem, že zákon neukládá povinnost toho, kdo odposlouchávání prováděl, oznámit odposlouchávanému subjektu, že tato akce byla provedena. Tudíž se ve většině případů daná osoba vůbec nedozví, že k takové činnosti došlo, a nemá tedy možnost se proti tomu případně bránit.[192]

Zároveň v této souvislosti je však nutné upozornit na důležitý fakt, že data získaná odposlouchávaním (tedy například obsah konverzace) podle tohoto zákona nelze užít jako důkaz při soudním řízení vyšetřovaného trestného činu, na rozdíl od údajů o komunikaci, které jsou diskutovány dále.[193] Proto podobné údaje mohou sloužit pouze a jen k dalšímu vyšetřování.[194]

[189] RIPA s. 3(1) a (2).

[190] The Interception Code of Practice 2002.

[191] The Intrception of Communications Commissioner.

[192] Edwards a Waelde 2009, str. 561.

[193] Wild 2005, str. 196, čl. 17 RIPA.

2.8.2.2 Kódování a přístup k chráněným údajům

Různé formy ochrany a kódování přenášených dat se začaly využívat právě k ochraně přenášených dat zejména v průběhu jejich přenosu. Jedná se například o tzv. enkryptování, tedy o změnu dané informace na nečitelný kód, který se pomocí opačného postupu zase zpět převede do čitelné podoby v přijímacím přístroji. K enrkypci dochází jak privátní (tedy obě strany si dobrovolně zvolí kód a heslo, pomocí kterého pouze oni mohou mít přístup k přenášeným informacím), tak veřejný, bez nutnosti individuálního hesla. Nejdůležitější povahu mají tyto informace při přenášení obchodních transakcí a využívání například bankovních produktů.

Z pohledu odposlouchávání a přístupu k takovým informacím, však subjekty podle seznamu č. 2 RIPA, mohou vyžádat od kterékoli osoby (zejména ISPs) poskytnutí takového klíče, pokud je to nutné k provádění odposlechu v rámci daného zákona. Takové vyžádání je možné, je-li to v zájmu národní bezpečnosti, prevence nebo vyšetřování trestného činu nebo ekonomického blahobytu země, jak uvádí článek 49(3) RIPA. V této souvislosti je nutné upozornit na to, že jde o velmi širokou konstrukci, obdobně jako je omezení práva na soukromí v článku 8(2) Evropské Konvence. Povinnost poskytnout klíč či heslo chránící soukromá data je pak stanovena v článku 50 RIPA.

Navíc neposkytnutí daného hesla či kódu se považuje za trestný čin, a pachatel se vystavuje pokutě nebo trestu odnětí svobody až na 2 roky, nebo obojímu, jak uvádí článek 53(3) RIPA. Přičemž pozice obviněného je velmi ztížena i tím, že podle odstavce 2. leží důkazní břemeno na obviněném. Tudíž on musí dokázat, že nebyl v držení daného hesla v době, kdy obdržel výzvu k jeho poskytnutí, ani poté. Toto ustanovení lze považovat za porušení zásady presumpce neviny v trestním řízení, a případné dokazování by nemělo být dostačující bez předložení pozitivních důkazů ze strany žalobce, jak naznačil soud UK v rozhodnutí R v S ans A [2008] EWCA 2177.

Současně se za trestný čin s možností odnětí svobody až na 5 let považuje porušení mlčenlivosti každé osoby, od které bylo vyžádáno heslo nebo klíč, jakož I každé osoby, která se o tom dozvěděla.[195] Edwards uvádí, že v tomto ohledu jde o ochranu metod a průběhu vyšetřování a odposlouchávání, a proto je zde limit sankce takto vysoký.[196]

---

[194] Chilcot, J. (2008) *Privy council review of intercept as evidence.* Report pro vládu UK [online] dostupné na adrese <http://www.official-documents.gov.uk/document/cm73/7324/7324.pdf> str. 78.

[195] RIPA s. 54.

[196] 2009, str. 568.

2.8.2.3 Údaje o komunikaci

Další otázkou úzce spjatou s elektronickou komunikací je také nakládání s údaji a informacemi, které se netýkají čistě obsahu přenášených informací (jejich sledování upravuje RIPA), jak již bylo představeno v dřívějších částech, jde o provozní a lokalizační údaje. Jejich uchovávání je zásadně zakázáno, jak uvádí směrnice o elektronických komunikacích v čl. 6, ale vzhledem k tomu, že jde o součást opatření na ochranu soukromí a osobnosti, výjimky v zájmu národní bezpečnosti, obrany či prevence a stíhání trestné činnosti jsou zmíněny v čl. 15 odst. 1 téže směrnice. Lze tedy konstatovat, že nakládání s těmito daty je omezeno. Pokud však jde o výjimky uvedené v článku 15 směrnice o elektronické komunikaci, státy samy určující prováděcí legislativou například na jak dlouhou dobu mohou požadovat zadržování těchto údajů. V případě UK to byl tzv. anti-teroristický zákon, the Anti-Terrorism Crime and Securities Act 2001, v rámci kterého byl přijat i dobrovolný praktický kodex.[197] Podle něj provozovatelé komunikační sítě mohou zadržet údaje o emailové či jiné internetové komunikaci po dobu 6 měsíců. V případě nutnosti může povinné zadržení údajů uložit státní orgán.[198]

Od roku 2004 na evropské úrovni některé státy (UK či Francie) navrhovaly přijmout opatření, ukládající zadržování daných údajů na dobu mezi 12 až 36 měsíci vztahující se na všechna data generovaná provozovateli elektronických komunikačních sítí. Toto bylo kritizováno jako příliš zavazující pro poskytovatele a zároveň příliš dlouhé z pohledu ochrany osobních údajů, a konečná verze tzv. směrnice o uchovávání údajů[199] uvádí v čl. 6 rozmezí 6 až 24 měsíců ode dne komunikace. Otázka finanční náhrady nebo alespoň částečné kompenzace pro poskytovatele informačních služeb jsou ponechány na jednotlivých státech, stejně jako nakládání či přístup k těmto datům pomocí státních složek právě v rámci ochrany národní bezpečnosti či trestné činnosti.

V UK byla směrnice provedena zvlášť pro telefonní linky a mobilní telefony v roce 2007[200] a pro internetová data je dosud pouze ve formě návrhu.[201] Návrh počítá s uchováním dat po dobu 12 měsíců (článek 5), a k možné finanční kompenzaci (článek 11).

---

[197] The Retention of Communications Data (Code of Practice Order 2003 (SI 2003/3175).

[198] The Secretary of State.

[199] Směrnice č. 2006/24/ES, 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, ze dne 15. března 2006.

[200] The Data Retention (EC Directive) Regulations 2007, SI 2007/2199.

Směrnice o uchovávání údajů odkazuje ve svém čl. 4, že přístup k takovým údajům má být upraven vnitrostátními předpisy v souladu se zásadami nezbytnosti a přiměřenosti. Podle právní úpravy UK je přístup k údajům o komunikaci garantovaný vyjmenovaným institucím a osobám v článku 25 odst. 2 RIPA. Stanovený účel podle článku 22 odst. 2 RIPA je poměrně široce formulován, zahrnující kromě národní bezpečnosti či trestné činnosti též ochranu veřejného zdraví či pro účely vybírání daní a poplatků. Zda daný okruh účelů a subjektů je v souladu s principem nezbytnosti a proporcionality omezení práva na soukromí podle článku 8 Evropské konvence, je poměrně často diskutovanou otázkou.[202] Kritizováno bývá například, že směrnice o uchovávání údajů ve svém článku 1(1) uvádí jako důvod uchovávání takových údajů souvislost se stíháním závažných trestných činů. RIPA však tento důvod výrazně rozšířila a orgány jsou kritizovány za to, že ustanovení RIPA bývá užíváno i v případě činů výrazně méně závažných.[203] Navíc podle případu Ewber and Saravia v Germany,[204] ESLP rozhodl, že národní úprava musí poskytnout takovou právní úpravu, která bude předvídatelná. Což v případě RIPA a jejích prováděcích předpisů je poměrně složité.

2.8.3 P2P sítě z pohledu autorského práva

Technologie tzv. peer-to-peer (P2P) sítí byla vynalezena z jiných důvodů než pro porušování autorských práv. Jde o síť rovnocenných počítačů, které na rozdíl od případu, kdy existuje jeden server, ke kterému se veškeré ostatní počítače připojují, předchází přetížení a výpadkům funkcí počítačové sítě právě svojí decentralizovanou strukturou. Každý zúčastněný počítač se tedy chová zároveň jako server i klient. Takto tudíž se pomocí vyhledávacího programu vždy připojují uživatelé přímo mezi sebou. Hlavními výhodami je zejména stabilita a zároveň není třeba uchovávat nespočetná množství dat na serverech, což mimo jiné ušetří i značné množství finančních nákladů. Při analyzování právních důsledků je třeba si povšimnout i struktury dané konkrétní sítě. Rozlišují se sítě centralizované, kde probíhá přenos přes centrální sever, Jedna z prvních takových sítí byla síť spravovaná z Kalifornie, Napster. Napster server tudíž udržoval pouze vyhledávací software, který udržoval a poskytoval uživatelům informace o tom, kdo a na

[201] The Data Retention (EC Directive) Regulations 2009.

[202] Edwards a Waelde, str. 588 až 590.

[203] Edwards a Waelde, str. 592.

[204] ECHR, No 54934/00, 29 červen 2006.

jaké adrese má vyhledávaná data.[205] Jiné sítě jsou decentralizované, které jsou nejvíce vystižené popisem z úvodu této kapitoly. Žádný centrální server není třeba. Jde například o síť Gnutella. Vždy existuje i střední cesta, využívající některé sdílené huby (spojovací místa). Takové jsou například Grokster nebo KazaA. Obdobnou technologií je i využívání tzv. torrent sítí (např. BitTorrent). Zvláštností této sítě je, že při stahování požadovaného souborů (resp. jeho částí) dochází zároveň ke zpřístupňování stahovaných dat ostatním uživatelům sítě. Navíc pro každé připojení se vytváří v podstatě vlastní síť, tudíž je velmi obtížné daného uživatele vysledovat. Podle některých údajů technologie P2P představuje vice než 60 % celkově přenesených dat v síti Internet.[206]

Jaké jsou tedy dopady a důsledky autorského práva na účastníky a aktivity na P2P sítích? V prvé řadě je nutno si uvědomit smysl ochrany autorských práv a práv od nich odvozených. Ten je všeobecně chápán (v USA dokonce ústavně vyjádřen) jako vyvážení mezi veřejným zájmem na pokroku vědy a užitého umění a zájmem soukromým, tj. autorů a těch, komu autorská práva odvozená svědčí. Je však nutné si uvědomit, že autorskoprávní legislativa není výsledkem, který by odrážel zájmy veřejnosti. Jde spíše o kompromis dosažený mezi největšími subjekty autorských práv, který je vyjádřen v zákonné podobě.[207] Proto veřejný zájem a volný přístup k dílům veřejností je vyjádřen zejména výjimkami. Zásadní otázkou je tedy, jaké zacházení s autorskými díly je veřejnosti zákonem dovoleno, a jaké je bez dovolení autora či jiné osoby považováno za nezákonné. Zároveň je nutno brát v potaz, že různá práva často svědčí různým osobám. Tak například práva k představení děl hudebních typicky náleží skladateli a tomu, kdo dílo zveřejnil, zatímco práva reprodukce jsou vlastněna nahrávacími společnostmi.[208]

Z výše uvedených důvodů je tedy důležité rozlišovat subjekty, které mají na P2P aktivitách podíl. Jedná se zejména o ty, kdo stahují (klienti) a o distributory (ti, kdo sdílejí). Přičemž jedna

[205] Schaumann, Niels B., *Copyright Infringement and Peer-to-Peer Technology* (2002). William Mitchell Law Review, Vol. 28, No. 3 [online] přístupné na adrese: <http://ssrn.com/abstract=1527189> str. 1020 a 1022.

[206] Giblin, Rebecca and Davison, Mark (2006) *Kazaa goes the way of Grokster' Authorization of Copyright Infringement via Peer-to-Peer Networks in Australia*. [online] Australian Intellectual Property Journal. přístupné na adrese <http://ssrn.com/abstract=1028653> str. 24.

[207] Ibid. Str. 1025.

[208] Toto odlišení bylo detailněji posuzováno v soudním případu Napster, ve kterém si nahrávací společnosti osobovaly i práva, která jim nenáležela. A & M Records, Inc. v. Napster, Inc., 114 F.Supp. 2d 896, 913 (N.D. Cal. 2000) a 239 F 3d 1004 (9th Cir 2001).

osoba je často obojím zároveň. Tyto činnosti jsou nemyslitelné bez dalších subjektů, zejména toho, kdo danou síť provozuje, vytváří vyhledávací programy, popř. provozuje servery nebo huby (poskytovatelé). V neposlední řadě hrají důležitou roli i poskytovatelé internetového připojení jako takového. Dle vývoje v posledních letech jsou právní legislativou aktivně zapojováni právě ti, kdo technicky zprostředkovávají připojení k internet a službám a protokolům užívaným k činnosti P2P sítí (blíže viz. následující kapitola o postavení ISPs).

Klienti jsou ti, kdo hledají na síti určité informace (např. autorská díla), které následně přímo od jiného uživatele internetu stáhnou do svého přístroje. Zde jsou potenciálně dva druhy porušení autorského práva klienty: vyhledávaní na síti a samotné stažení díla. Vyhledávání samo o sobě neporušuje žádné autorské právo. Vyhledávací služby jsou samy o sobě pouze poskytnutím seznamu názvů souborů nacházejících se na počítačích uživatelů fungujících jako servery. Tyto názvy nejsou vytvořeny vlastníky autorských práv, na rozdíl od jejich skutečného obsahu, třebaže většinou obsahují název daného díla. Stažení souboru z P2P sítě však již znamená v podstatě vytváření kopie daného souboru. Tato činnost je tedy obecně porušením autorského práva ve smyslu § 13 odst. 1 a 2 AZ. Naproti tomuto tvrzení lze však vznést dva druhy obhajoby. Jednak je to princip tzv. fair use (užívaný zejména v USA) a jednak případ, kdy dochází k vytváření kopie výlučně pro soukromé nekomerční užití fyzické osoby. Toto neplatí, jde-li o počítačový program či elektronickou databázi (ve smyslu § 30 AZ), ve kterém se výjimka užití pro soukromé účely neuplatní.[209] Zejména díky dopadu na trh byla úspěšná žaloba proti činnosti společnosti Napster, jelikož tato činnost snížila počet prodaných CD mezi uživateli (vysokoškolskými studenty) a navíc bylo argumentováno tím, že se vytváří omezení možnosti autorů a nahrávacích společností vstoupit na trh s digitální podobou hudby (tudíž takové užití soud nepodřadil pod výjimku fair use).[210] Lze však konstatovat, že pokud jde o stahování děl jiných než počítačových programů či elektronických databází, a jde-li o užití pouze pro soukromé potřeby, nedopouští se klient (stahující uživatel) porušování autorských práv.

Distributoři jsou ti, kdo jsou v P2P síti servery. Jinak řečeno, kdo poskytují autorská díla ostatním uživatelům prostřednictvím umožnění přístupu ke svým počítačům (resp. pevným diskům). Tito ve své podstatě vždy porušují práva autorů či jiných osob ve smyslu uvedeném

[209] Doktrína Fair use je používána v USA. Soud je povinen vzít v úvahu několik faktorů, dle kterých posuzuje, zda užití daného díla bylo ospravedlnitelné: účel a charakter užití, povaha kopírovaného díla, počet pořízených kopií a dopad užití této kopie na trh. Schaumann, Niels B., *Copyright Infringement and Peer-to-Peer Technology* (2002). William Mitchell Law Review, Vol. 28, No. 3 [online] přístupné na adrese: <http://ssrn.com/abstract=1527189> str. 1029.

[210] A & M Records, Inc. v. Napster, Inc., 114 F.Supp. 2d 896, 913 (N.D. Cal. 2000) a 239 F 3d 1004 (9th Cir 2001).

níže. Jak je naznačeno na začátku, záleží na struktuře sítě a na technologii, kdo je distributorem. Buď je tím zvláštní subjekt, který provozuje servery či místa, kde jsou díla uložena (např. v tomto postavení byla firma Napster). Častěji však dnes bývají užívány sítě, kdy sám klient se stává při procesu stahování zároveň distributorem.

Zvláštní postavení mají ti, kdo provozují sítě a udržují vyhledávací systémy. Opět záleží na struktuře sítě, protože někdy existuje centrální subjekt provozující servery, na nichž jsou daná díla uložena (např. Napster). Jinak tomu však je v případě, kdy daný subjekt pouze udržuje vyhledávací program (BitTorrent), který pouze poskytuje službu vyhledávání názvů souborů uložených u jiných uživatelů. V případě českého práva autorského je jejich činnost chráněna v § 18 odst. 3 AZ, podle kterého se provozování zařízení umožňujícího nebo zajišťujícího sdělování nepovažuje za sdělování díla veřejnosti. V jiných zemích (blíže viz. dále) může být postavení provozovatelů sítí odlišné.

Poslední skupinou jsou již několikrát zmínění poskytovatelé internetového připojení (ISPs), kteří jsou zvlášť chráněni od odpovědnosti, zprostředkovávají-li pouze přístroj či technologii, která pak bývá užita mimo jiné i k protiprávní činnosti. Blíže je postavení těchto subjektů věnována zvláštní kapitola v této práci.

K čemu vlastně nejčastěji dochází při (zne)užívání P2P sítí z pohledu práva autorského? Předmětem ochrany jsou autorská díla a z pohledu majetkových práv zejména jejich užití. Jde o legislativní zkratku, kterou dle § 12 odst. 4 AZ je myšleno právo dílo rozmnožovat, rozšiřovat, pronajímat, půjčovat, vystavovat a sdělovat dílo veřejnosti. Zásadně tyto činnosti jsou právem autora, ačkoli se mohou lišit podle druhu autorského díla Tento výčet je demonstrativní.

Na síti P2P dochází nejčastěji k porušování práva dílo rozmnožovat ve smyslu § 13 AZ. Definice výslovně zahrnuje i zhotovování rozmnoženin dočasných či nepřímých, a to jak díla celého, tak jeho částí, za použití jakýchkoli prostředků a forem (včetně forem elektronických). Sdílení i stahování díla z P2P sítě je v tomto kontextu užitím díla podle uvedené definice. Výsledkem této aktivity je totiž vytvoření rozmnoženiny díla, včetně tzv. technických rozmnoženin (např. v jiném formátu). K tomu je nutné poznamenat, že v souladu s evropskými předpisy existuje dle § 38a AZ zákonná licence pro vytváření dočasných rozmnoženin tvořící nezbytnou součást technologického procesu (například přenosu díla počítačovou sítí), nemají-li žádný samostatný hospodářský význam (s výjimkou počítačových programů dle § 66 odst. 2 AZ).

Dalším způsobem neoprávněného užití díla pomocí P2P sítě je sdělování díla veřejnosti ve smyslu § 18 odst. 1 AZ, neboli jeho zpřístupnění v nehmotné podobě, živě nebo ze záznamu, po drátě i bezdrátově. Kříž k tomu uvádí, že jde o generální klauzuli zahrnující veškeré možné způsoby zpřístupňování včetně umožnění přístupu k dílu.[211] Za sdělování veřejnosti zákon v § 18 odst. 2 považuje i zpřístupňování na místě a v čase podle vlastní volby (tzv. on demand). Odst. 4 téhož paragrafu navíc dodává, že tímto sdělováním díla veřejnosti nedochází k vyčerpání tohoto práva. Důležitým ustanovením je i část stanovící, že poskytovatelé připojení k internetu včetně těch, kdo technologii P2P provozují, jsou výslovně vyňati ze sdělování díla veřejnosti, protože dochází k pouhému provozování zařízení umožňujícího nebo zajišťujícího sdělování, nikoli k sdělování jako takovému.[212]

Nutno je také poznamenat, že tzv. volným užitím, které definuje § 30 odst. 1 AZ jako užití pro osobní potřebu fyzické osoby, není-li účelem dosažení hospodářského či obchodního prospěchu (přímého či nepřímého), nedochází k porušení autorských práv. Soukromá osoba si tedy za uvedených podmínek může zhotovit záznam, rozmnoženinu či napodobeninu díla, jak výslovně uvádí odst. 2 téhož paragrafu. Důležitou výjimkou je však užití počítačového programu či elektronické databáze, u nichž se výslovně za užití považuje i případ užití jen pro osobní účely fyzickou osobou. K tomu je třeba vždy aplikovat obecné ustanovení § 29, kdy odst. 1 uvádí tzv. třístupňový test známý již z dokumentů mezinárodněprávních. Podle něho lze tedy uplatnit výjimky a omezení autorského práva pouze tehdy, je-li to ve zvláštních případech stanovených zákonem, pokud takové užití není v rozporu s běžným způsobem užití díla a ani jím nejsou nepřiměřeně dotčeny oprávněné zájmy autora. Navíc podle odst. 2 téhož ustanovení se vztahují takové výjimky jen na dílo zveřejněné. Tudíž tedy opatřování děl z nelegálního zdroje či opatřování díla dosud neuveřejněného je porušením práva dílo užít a výše uvedené výjimky z něj se neuplatní.

Vedle práva autorského je zároveň důležitá i problematika práv s právem autorským souvisejících. V případě P2P sítí jsou nejvýznamnější práva výrobce zvukového (§ 75 a násl. AZ) a zvukově obrazového záznamu (§ 79 a násl. AZ) k tomuto záznamu a právo vysílatele (rozhlasového a televizního) k jeho vysílání (§ 83 a násl.). Obsah těchto práv je velmi obdobný právu autorskému (tedy právo záznam či vysílání užít). Zvláštní úprava je také pro pořizovatele databáze. Společný je i režim volného užití dle § 74, 78, 82 a 94 AZ odkazující na obdobné užití

[211] Kříž, Jan. et. al. (2005) Autorský zákon: Komentář a předpisy související, 2. Aktualizované vydání. Praha: Linde, str. 780.

[212] § 18 odst. 3 AZ.

ustanovení pro právo autorské. Z toho důvodu se někdy užívá pojem autorské právo v širším smyslu zahrnujícím i práva s autorským právem související.

Například v případě protiprávního šíření hudebních skladeb dochází k současnému porušování několikero práv: autorské právo autora textu a hudby, právo výkonného umělce zpívajícího danou skladbu i právo výrobce zvukového záznamu.

Co je tedy nového na tom, co bylo výše uvedeno, a čím jsou P2P sítě považovány majiteli autorských práv za tak ohrožující? Nejde o zcela nový jev, lze jej podřadit a klasifikovat podle existující legislativy. Avšak obavy vzbuzuje distribuční kapacita této technologie, která se vymyká kontrola vlastníků práv k poskytovanému obsahu. Ve snaze znovuzískat kontrolu, nebo jí alespoň zvýšit, dochází k zapojování a zavádění sekundárních povinností i případné sekundární odpovědnosti dalších subjektů (zejména ISPs). Mnoho technologií totiž výrazně ztěžuje vymáhání práv. Příkladem jsou třeba Gnutella nebo FreeNet programy, které zdarma umožňují podílet se na takové síti, kde není žádná centrální osoba odpovědná za obsah nebo datový přenos. Takto tedy musí ti, komu práva náleží, monitorovat velmi široké možnosti cest, kudy mohou být data přenášena. Proto nová úprava zapojující ISPs stojí na myšlence, že lze vysledovat IP adresu počítače užívaného k protiprávnímu jednání. Potom, prostřednictvím jeho poskytovatele internetu lze získat jeho adresu a identitu. Teprve poté je možné podniknout konkrétní kroky k vymáhání autorských práv či práv souvisejících. Jak je na první pohled patrné, takové činnosti jsou velmi ekonomicky nákladné a jejich návratnost od jednotlivých zejména malých uživatelů je mizivá. Porušovatelů je totiž příliš mnoho a příliš malých. Prakticky tedy bude docházet jen zřídka k sankcionování malých uživatelů (porušovatelů) autorských práv, a majitelé se budou spíše orientovat na ty největší. Problém však vyvstává, zda bude v budoucnu těch velkých zapotřebí, když každý v síti P2P může být zároveň serverem i klientem, tudíž zde jsou zapojeni "pouze" uživatelé malého významu.

Co tedy lze s tímto faktem udělat? Vlastníci autorských práv potřebují centrální autoritu, na které by se mohli efektivně domáhat náhrady svých porušených práv. Proto se objevují snahy o vymáhání prostřednictvím sekundární odpovědnosti těch, kdo tyto systémy udržují a provozují. Tak bylo rozhodnuto například v USA či Austrálii.[213] V USA Nejvyšší soud rozhodl, že třetí osoba, která provozuje nebo distribuuje zařízení (vč. software) umožňující porušování autorských práv s cílem takovou činnost podporovat, nebo pokud podnikne kroky k umožnění

[213] MGM Studios, Inc. v. Grokster, Ltd. 545 U.S. 913 (2005) a Universal Music Australia v Sharman License Holdings (2005) 65 IPR 289.

takové činnosti, bude odpovědná za činnost uživatelů, bez ohledu na to, že takové zařízení může být užito i pro činnosti v souladu s právním řádem.[214] Zda takto široké pojetí je ospravedlnitelné, to bylo předmětem širokých diskuzí. V Australském případě byl provozovatel P2P softwaru KaZaA (podle toho také někdy bývá případ nazýván) uznán odpovědným, avšak s poněkud jiným odůvodněním. Šlo o výklad tamního ustanovení, že odpovědným je každý, kdo autorizuje porušování autorských práv podle čl. 101(1A).[215] Přitom za hlediska autorizace se považuje, zda tato osoba měla moc k tomu, aby znemožnila porušení autorského práva v daném případě, povaha vztahu mezi danou osobou a osobou, která se porušení dopustila, a v neposlední řadě též, zda tato osoba učinila nějaké kroky k zamezení či předcházení takového porušování autorského práva. Za takový krok by soud podle svých slov například považoval možné užití filtrů ve vyhledávači tak, aby nezobrazoval soubory se jmény autorů či názvů autorských děl (například na základě katalogu nahrávacích společností). Jinak řečeno, australský soud takto vytvořil povinnost opatrnosti a péče k tomu, aby přijali ti, kdo vytváří či provozují P2P software, vhodné standardy a mechanismy k předcházení jeho zneužití k porušování autorských práv. Sekundární odpovědnost může být tedy dovozena, pokud tento subjekt nepodnikl ekonomicky rozumné kroky k prevenci před takovou nezákonnou činností. [216] Tento druhý přístup lze považovat za více citlivý a praktický. Nevýhodou však je, že technické filtry však mohou znemožnit užití veškerých děl a informací i pro účely v souladu se zákonem, např. vzdělávací či vědecké. Takové omezení se může jevit jako nepřijatelné.

Správnou cestou není ani zákaz užívání technologie P2P nebo jakékoli jiné zcela. Tím by byl soukromý zájem upřednostněn před zájmem veřejným, pokrokem vědy a umění. Další vývoj by se tedy měl spíše zaměřit a přizpůsobit nové realitě. Typickým příkladem je praxe uvalení tzv. autorské daně (levy) na přístroje a média, která mohou být k privátnímu ukládání a užívání autorských děl použita. Tyto daně by mohly být uvaleny například i na provozovatele či distributory peer-to-peer software a sítí s tím, že tyto sítě mohou být užívány pouze pro soukromé, nekomerční účely. Takto vybrané prostředky jsou pak poměrně přerozdělovány majitelům autorských práv či práv souvisejících jako náhrada za ztráty tím, že privátní kopie

[214] Pessach, Guy (2006) *An International-Comparative Perspective on Peer to Peer File-Sharing & Third-Party Liability in Copyright Law - Framing Past - Present and Next-Generation's Questions.* [online] Vanderbilt Journal of Transnational Law, Forthcoming. přístupné na adrese <http://ssrn.com/abstract=924527> str. 5.

[215] Giblin, Rebecca and Davison, Mark (2006) str. 7 a násl.

[216] Pessach, Guy (2006) str. 6 a 7.

nejsou zpoplatňovány (tak se to například děje u prázdných médií jako CD, DVD nebo MP3 přehrávačů, někde i u osobních počítačů).[217]

Pokud jde o další vývoj, je nutné učinit několik poznámek. Tzv. DRM (z anglického digital rights management), digitální správa práv, je opatření, kterým se zejména výrobci autorských děl snaží zabránit dalšímu nelegálnímu šíření autorských děl. Dobřichovský se domnívá, že právě rozvoj technických prostředků ochrany, možnosti identifikace předmětu ochrany i případného konkrétního uživatele internet je nezbytným předpokladem účinné úpravy a ochrany autorských práv v digitálním prostředí.[218] Zda není tento názor příliš přeceňující DRM, s tím lze polemizovat. Jisté však je, že vynalézavost těch, kdo nemají v úmyslu se právní úpravou řídit a respektovat jí, je vždy o krok napřed a veškeré druhy ochranných prostředků typu heslování, vodoznaky či monitorování užívání lze obejít. Mnohem zajímavější a v skutku fungující je využití P2P sítí i jiných technologií způsobem v souladu se zákony. Nový obchodní model prodeje nehmotných podob autorských děl právě prostřednictvím sítí P2P, jak k tomu dochází například prostřednictvím sítě iTunes od společnosti Apple, je zcela nepochybně budoucností a prostředkem k efektivnějšímu šíření legální cestou. Bude-li zakoupení těchto děl cenově přijatelné, není důvod si nemyslet, že mnoho uživatelů si požadovaná díla zakoupí. Jak je vidět, motivace pozitivní, tzn. podpora prodeje a jednoduchého přístupu k dílům, je výrazně účinnější, než hledání všech možných cest, jak nelegální činnosti zabránit nebo ji potrestat. Je totiž nutné přiblížit obecné vnímání a chování společnosti existujícím právním normám. Jinak bude v mnoha případech stale docházet k hledání cest, jak právní normy obejít či porušit. Zvlášť, je-li to tak jednoduché, jako prostřednictvím internetové sítě a technologie P2P či torrent.

2.8.4 Právní postavení poskytovatelů služeb informační společnosti

Důvodem, proč je věnována samostatná kapitola odpovědnosti poskytovatelů služeb, je fakt, že vzhledem ke struktuře a fungování internetu jako takového, efektivní aplikace práva a kontroly činnosti jednotlivých účastníků sítě je možné dosáhnout jedině efektivní kontrolou těch, kdo fakticky hrají nejdůležitější roli v existenci používání této sítě. Jde tedy o subjekty, které zajišťují připojení k síti, a také o ty, kdo v rámci sítě poskytují své služby (například poskytují služby

[217] Danay, Robert Jacob, (2005) *Copyright Vs. Free Expression: The Case of Peer-to-Peer File-Sharing of Music in the United Kingdom* [online] 8 Yale Journal of Law & Technology 32. přístupné na adrese <http://ssrn.com/abstract=847905> str. 35.

[218] Dobřichovský, T. (2004) *Moderní trendy práv k duševnímu vlastnictví v kontextu evropského práva, dohody TRIPS a aktivit WIPO*. Praha: Linde Praha, a.s., Str. 77 až 80.

elektronické pošty, fulltextové vyhledávání či provozují elektronické sociální sítě). Souhrnně se tyto subjekty označují za ISP, z anglického internet service provider, nebo též poskytovatelé služeb informační společnosti.

Směrnice o elektronickém obchodu (dále jen SEO) [219] ve svém článku 12 vylučuje odpovědnost poskytovatele služby, pokud není původcem přenosu, nevolí příjemce přenášené informace a nevolí a nezmění obsah přenášené informace. Obdobně není ani obecně odpovědný v případě tzv. caching, ukládání do vyrovnávací paměti, které je pouze dočasným ukládáním sloužícím k efektivnímu přenosu a je zejména technického charakteru (čl. 13 SEO). Jinými slovy, poskytovatelé služeb informační společnosti neodpovídají za prostý přenos informace. Poskytovatel služby spočívající v ukládání informací poskytovaných příjemcem služby není také odpovědný za informace ukládané na žádost příjemce, pokud nebyl seznámen či není si vědom skutečností, že jde o protiprávní jednání, nebo pokud jednal s cílem odstranit tyto informace či zajistit jejich nepřístupnost, jakmile se o tom dozvěděl.[220] Poměrně důležitý je v této souvislosti též článek 15 SEO, který uvádí, že neexistuje obecná povinnost poskytovatelů služeb dohlížet nad přenášenými a ukládanými informacemi, či jinak aktivně vyhledávat skutečnosti a okolnosti poukazující na protiprávní činnost.

Hlavní úprava odpovědnosti poskytovatelů služeb informační společnosti v ČR je v zákoně č. 480/2004 Sb., o některých službách informační společnosti. Do jeho působnosti spadá každá fyzická či právnická osoba, která poskytuje některou ze služeb informační společnosti podle § 2 písm. e). Obecně lze mezi tyto osoby zařadit jak ty, kdo zprostředkovávají přístup k internetu či jiné elektronické síti, tak ti, kdo poskytují služby v jeho rámci (například provozovatelé webových či jiných internetových služeb).

Podle § 3 odst. 1 poskytovatel služby odpovídá za obsah přenášených informací jen, pokud přenos sám iniciuje, zvolí uživatele přenášené informace, anebo zvolí či změní obsah přenášené informace. Kromě toho provozovatel odpovídá i za obsah informací automaticky dočasně meziukládanýcch, tedy těch, které se dočasně ukládají za účelem uskutečnění přenosu (podle § 4), ovšem pouze v případě porušení svých povinností, anebo v případě, že obsah informace sám změní. Obdobně i v případě ukládání informací pro uživatele, může být

[219] 2000/31/ES směrnice o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu, 8. června 2000.

[220] Čl. 14 odst. 1 SEO.

poskytovatel takové ukládací služby odpovídat za obsah těchto informací, pouze ale, pokud o protiprávnosti mohl vzhledem k předmětu své činnosti a okolnostem a povaze případu vědět (§ 5 odst. 1 písm. a), anebo pokud neučinil patřičné kroky, dozvěděl-li se prokazatelně o protiprávnosti jednání či povaze daných informací. Poskytovatelé služeb nejsou však povinni dohlížet na obsah přenášených informací, ani jinak aktivně vyhledávat skutečnosti a okolnosti poukazující na protiprávní obsah informace, jak stanoví § 6 daného zákona. Zjednodušeně řečeno, poskytovatelé služeb informační společnosti neodpovídají za obsah, pokud se aktivně nepodílejí na formování či změně dané informace, anebo pokud uživatel není pod jejich rozhodujícím vlivem (§ 5 odst. 2)

Následující zákonné úpravy z posledních let ve Velké Británii a Francii ukazují, jakým směrem by se mohla úprava internetu v příštích letech vyvíjet. Výrazně totiž přibývá ekonomických dopadů těch, kdo porušují práva prostřednictvím internetu. Zejména v zemích, kde zábavní průmysl hraje důležitou roli pro tamní ekonomiku, potírání porušování autorských a jiných práv je zásadní prioritou pro tamní vládu. Proto se právní opatření zaměřují na ty, kdo mohou nejefektivněji přispět k dodržování zákona uživateli internetové sítě, tedy poskytovatelé příslušných služeb. Jaké je postavení těch, na koho stát uvaluje čím dál více povinností a s tím spojených nákladů, to je uvedeno dále.

2.8.4.1 Digital Economy Act 2010

V roce 2010 byl přijat na britských ostrovech nový zákon, který má přispět k rozvoji a nové regulaci internetového prostředí. Je výsledkem lobbistických snah ze strany těch, kdo neustále zaznamenávají obrovské finanční úniky způsobené zneužíváním a obcházením práv k duševnímu vlastnictví prostřednictvím internetové sítě. Úniky zábavního průmyslu (audio a audiovizuálního) i těch, kdo produkují počítačový software, jsou však i významnými položkami v příjmech státního rozpočtu. Proto se vláda rozhodla upřednostnit tyto zájmy a uvalit povinnosti na některé zúčastněné subjekty. Opět tedy legislativa stála před stejným problémem, jak efektivně chránit tato autorská práva či práva k průmyslovému vlastnictví za současného zachování co největší globální volnosti internetové sítě?

Mezi uživatelem a internetem samotným stojí vždy subjekt, který se nazývá poskytovatel služby informační společnosti, z anglického Internet Service Provider (ISP). Právě regulace a uvalení povinností na tyto subjekty se prozatím jeví za nejvíce efektivní a zřejmě jedinou cestu. Kromě ostatních oblastí, jako je modernizace infrastruktury či rozvoj veřejných služeb, důležitá z pohledu této práce je část týkající se porušování práv k duševnímu vlastnictví a opatření

k zamezení těchto činností. Podstatou tedy je zavedení druhotné odpovědnosti ISP za obsah internetu a přenášených informací. Zároveň je jim uložena povinnost, aby v případě vědomí o protiprávnosti přenášené informace podnikli kroky k předcházení či zastavení takového protiprávního jednání. Nové povinnosti zahrnují zejména kooperovat s majiteli chráněných práv a, je-li to nezbytné, přijmout i opatření technické povahy proti těm, kdo se dopouští porušování těchto práv.

Obecně, odpovědnost za vysledování porušování práv leží nadále na těch, jimž práva svědčí, tedy majitelům práv k duševnímu vlastnictví. Oni budou nadále monitorovat internetový provoz a vyhledávat, jaký počítač, stránka či technologie bývá využívána ke sdílení chráněných materiálů. Nově pak mají tito možnost do jednoho měsíce zaslat oznámení IPS o tom, že určité osoby či IP adresy bývají užívány k nelegální činnosti.[221] ISP mají povinnost vypracovat pro majitele porušovaných práv seznam těch uživatelů, kdo jsou podezřelí z jejich porušování. Zároveň mají ISP povinnost písemně upozornit uživatele, že jeho počítač je používán k porušování autorských či jiných práv. Dále je poskytovatel služeb povinen spolupracovat s majiteli práv tím, že poskytne evidenční podklady o tom, že k porušování práv dochází. Pokud uživatel přesto pokračuje, ISP jsou povinni podniknout i opatření technického charakteru. Nejprve má dojít ke snížení rychlosti a kapacity internetového připojení daného uživatele, k zamezení užívání jeho připojení k určitým službám či protokolům, a pokud ani toto nepostačí, pak může být daný uživatel odpojen od internetové sítě zcela. Náklady technických opatření leží na ISP. Navíc, v případě nepodniknutí žádných technických opatření, může být ISP vystaven poměrně vysokým pokutám až do výše 250 000 britských liber.

Jak je patrné, úprava na jednu stranu zavádí opatření k zamezování a sledování těch, kdo porušují práva jiných, na druhou stranu však uvaluje povinnosti a náklady na subjekty jiné. ISP jsou tudíž vystaveni dalším finančním nákladům, ať již spojeným se samotnými technickými opatřeními, tak se zpracováním osobních údajů, správou a výkonem notifikačních povinností vůči těm, kdo jsou podezřelí z porušování práv. Proto se zvedla velká vlna protestů zejména ze strany největších poskytovatelů (např. Google, Facebook, Ebay či Yahoo) a samozřejmě i ze strany samotných uživatelů. Kritika nového zákona je založena na několika východiscích.

Na základě této úpravy je ISP dána přílišná pravomoc přímo zasahovat do soukromí uživatelů a majitelé chráněných práv si mohou vyžádat od ISP report o údajích (například o stahování všemi uživateli v rámci daného ISP), k čemuž postačí jen minimální důkazy a

[221] Office of Public Sector Information (2010) *Digital Economy Act 2010* [online] navštíveno 15/04/2010 <http://www.opsi.gov.uk/acts/acts2010/ukpga_20100024_en_1>.

odůvodnění. Navíc, díky technickým opatřením, může dojít k odpojení či velkému omezení internetového připojení uživatele ještě před tím, než by skutečně došlo k obvinění a dokázání jeho viny či neviny.[222] Další problém je spatřován v tom, že pomocí technických odpojení určitých protokolů, může být způsobena škoda či zamezení služeb, kterých se porušování chráněných práv vůbec netýká. Navíc obecné zamezení pro všechny uživatele by tím omezovala práva těchto ostatních uživatelů bez ohledu na to, zda se oni kdykoli dopustili protiprávního jednání. ISP sami tvrdí, že nejsou těmi, kdo plně kontrolují a mají kontrolovat internet jako takový. Jejich službou je pouze technické poskytnutí určité konkrétní služby, například připojení k internetové síti jako takové. Ukládání povinností těmto subjektům, aby podnikali opatření k tomu, aby internet byl užíván pouze legálně, se jeví jako nespravedlivé. Je to, jako by docházelo k ukládání odpovědnosti či povinností výrobci automobilů, aby zajistil, že automobily budou užívány pouze legálním způsobem. Navíc náklady vyplývající z této úpravy budou podle ISP neúměrně vysoké. Vzhledem k úpravě mezinárodní, zejména evropské, se tudíž poskytovatelé brání s odůvodněním, že nová úprava je velmi nedokonalá a ve své podstatě v mnoha ohledech, zejména stran ochrany soukromí, protiprávní

Orgánem dohledu byl zřízen the Office of Communications (zkráceně OFCOM), jenž má přijmout prováděcí kodex, podle kterého budou vyřešeny praktické a procedurální aspekty, a mimo jiné bude každých pět let podávat zprávu o aktuální situaci státnímu sekretariátu.

2.8.4.2 Zákon HADOPI

Obdobným směrem jako Velká Británie se vydala i Francie, která v zájmu ochrany práv k duševnímu vlastnictví zavádí tzv. hadopi zákonem[223] z roku 2009 postup, jakým hodlá zasáhnout proti těm uživatelům, jež sdílejí či jinak používají internet k porušování či obcházení chráněných práv. Označení hadopi je odvozeno od zvláštní instituce tímto zákonem vytvořené (High Authority of Diffusion of the Art Works and Protection of the (Copy)Rights on Internet), která vykonává dohled a příslušné aktivity (například žádá učinění příslušných kroků dále pospaných) v této oblasti. V čele nově vytvořené instituce je devítičlenné představenstvo, jehož tři členové jmenuje vláda, dva legislativní orgán, tři soudní orgány a jeden je jmenován institucí

[222] Meyer, D. (2010) *Digital Britain minister concedes file-sharer "disconnection"* [online] navštíveno 24/03/2010 <http://www.zdnet.co.uk/blogs/communication-breakdown-10000030/digital-britain-minister-concedes-file-sharer-disconnection-10015403/.>.

[223] Loi favorisant la diffusion et la protection de la création sur Internet (tzv. HADOPI zákon) <http://www.laquadrature.net/wiki/HADOPI_full_translation#CHAPTER_I> (anglický překlad), účinný od května roku 2009.

pro ochranu uměleckého a literárního majetku působícího pod francouzským ministerstvem kultury.

Daný postup (z anglického three-strike) zahrnuje tří-instanční zakročení proti těm, kdo užívají internet nelegálním způsobem ve smyslu tohoto zákona. Na žádost toho, kdo se domáhá svých autorských či jiných práv, je zaslána emailová zpráva příslušnému uživateli internetového připojení podle vysledované IP adresy a doby, kdy k protiprávnímu činu došlo. ISP je pak povinen sledovat činnost daného uživatele, poskytnout údaje o uživateli dané IP adresy, včetně instalace specifického technického filtru na přístroj daného uživatele. Druhým krokem, pokud se porušování objeví znovu do šesti měsíců od uvedeného prvního opatření, je zvláštní certifikovaný dopis, jenž je zaslán majiteli internetového připojení, uživateli. V případě nedostatečnosti a opakování porušování práv v období 1 roku od přijetí certifikovaného dopisu, třetím opatřením je majitel připojení zařazen do černé listiny, a ostatní poskytovatelé internetových služeb (ISPs) těmto nesmí poskytnout internetové připojení, přičemž stávající připojení je uživateli odpojeno, a to na 2 až 12 měsíců. Navíc mu může být uložen i finanční postih, nebo i dvouleté vězení. Zatímco první dvě opatření nemohou být přezkoumány soudy, třetí ano.

Jak nové průzkumy po roce působení daného zákona uvádí, výsledek, kterým mělo být výrazné snížení porušování autorskoprávních a jiných duševních práv, dosažen z velké části nebyl. Daný zákon donutil ty tzv. piráty najít jiné cesty, podle kterých není jejich identifikace a IP adresa téměř dohledatelná.[224]

2.8.5 Kontrola zaměstnanců

Kontrola zaměstnanců zaměstnavatelem je běžnou praxí ve většině společností. Zda však je takové počínání oprávněné, popřípadě do jaké míry mají zaměstnanci právo na ochranu svého soukromí včetně tajemství doručovaných zpráv v jakékoli podobě, to je často diskutovanou otázkou.

Zaměstnavatelé uvádí, že jejich počínání je opodstatněné hned z několika důvodů. V případě, že zaměstnanec není v práci, jeho pracovní komunikace je někdy nutná k pokračování v jeho práci. Kromě toho mají zaměstnavatelé nepochybně právo kontrolovat, zda byla práce

[224] PC Magazine Online (2010) *"French Anti-Piracy Law Actually Increases Piracy."* [online] navštíveno 11/08/2010, dostupné na adrese <http://find.galegroup.com/gtx/infomark.do?&contentSet=IAC-Documents&type=retrieve&tabID=T003&prodId=AONE&docId=A222470126&source=gale&srcprod=AONE&userGroupName=mmucal5&version=1.0>.

odvedena podle instrukcí zaměstnavatele, a zda je například dodržováno obchodní tajemství zaměstnanci.[225]

Na druhou stranu je však nutné položit si otázku, zda k těmto cílům je přiměřeným a jediným prostředkem naprostá kontrola činnosti zaměstnanců. Často je totiž zaměstnancům odpíráno veškeré právo na soukromí i tajemství doručovaných zpráv, pokud ke komunikaci dochází v pracovní době nebo při používání služebních prostředků. Takové počínání je však z několika aspektů nezákonné. Například monitorování webových stránek prohlížených zaměstnanci je obecně považováno za zakázané, leda by zaměstnanci byli předem informováni, že je monitorování prováděno a pro jaký účel.[226]

Poněkud volnější práva a povinnosti mají zaměstnavatelé ve Velké Británii, kde podle RIPA je stanovena výjimka z obecného zákazu odposlouchávání komunikace pro zaměstnavatele, podle které je umožněno odposlouchávat či sledovat komunikace zaměstnanců, pokud je to pro některý z uvedených účelů (například k shromáždění dostatku faktických údajů potřebných k obchodu, předcházení nebo zjištění trestného činu, k zajištění dodržování všech předpisů, včetně vnitřních).

[225] Carey 2004, str. 226 a 227.

[226] Ibid, str. 227.

ZÁVĚR

Internetová síť výrazným způsobem zasahuje do současné společnosti, do jejího chování, a tím i do právní regulace veškerých dotčených aspektů. Používání internetu je součástí každodenního chování většiny obyvatelstva. Někteří jej užívají jako pracovní nástroj, jiní pro soukromé účely. Kromě pozitivních důsledků, kterými může být například urychlená komunikace včetně té přeshraniční, obecně výrazně snadnější a rychlejší informovanost obyvatelstva i jeho vzdělávání. Internetová síť skýtá i mnohé podnikatelské příležitosti. Na druhou stranu nelze si nevšimnout vlivů negativních. Je to nové prostředí, které s rychlým globálním rozvojem představuje i ohrožení mnoha dosavadních prvních institutů. Ochrana osobnosti a osobních údajů se zdá být čím dál obtížnější. Objevují se nové druhy činů, které posléze trestní zákoníky uznávají za činy trestné. Mnohé instituty práva autorského se zdají být jen těžko udržitelné. Velmi mnoho právních pojmů je nově vykládáno v souvislosti s dopadem užívání internetové sítě. Typickým příkladem může být ochrana autorských práv, která bývají porušována nejvíce. Vzhledem ke struktuře internetové sítě lze očekávat vývoj, jaký se objevuje v posledních letech v některých státech, například ve Francii či Velké Británii, kde se výrazným způsobem zapojují do procesu dodržování právních předpisů a monitorování činnosti uživatelů internetu i poskytovatelé internetového připojení či jiných služeb informační společnosti.

Na druhou stranu však tato síť může být výrazným hybatelem právních systémů, které se ve velké míře sbližují. Globální charakter této počítačové sítě totiž nelze uchopit jinak než jednotným přístupem všech členů mezinárodního společenství. Státy, ve kterých je internet druhořadou záležitostí, jsou častým cílem těch, kdo internet hodlají zneužívat k protiprávní činnosti. Jen změnou přístupu těchto států může dojít k pozitivnímu vývoji a dodržování objektivního práva v budoucnu.

Bibliografie

Ahmed, S. (2010) *Fast Internet access becomes a legal right in Finland* [online] updated 10/15/2010, navštíveno 03/29/2010 <http://www.cnn.com/2009/TECH/10/15/finland.internet.rights/index.html>.

Akdeniz, Y. (2001) *Case Analysis of League Against Racism and Antisemitism (LICRA), French Union of Jewish Students, v Yahoo! Inc. (USA), Yahoo France, Tribunal de Grande Instance de Paris (The County Court of Paris), Interim Court Order, 20 November, 2000.*

Akdeniz, Y., Clive, W. and Wall, D. (2000) *The Internet, law and society*. UK, Harlow: Longman.

Bandurski, D. (2008) *China's Guerrilla War fot the Web*. Far Eastern Economics Review [online] publikováno červenec 2008, nav3t9veno 02/25/2010 <http://www.feer.com/essays/2008/august/chinas-guerrilla-war-for-the-web>.

Barlow, J. P. (1996) *A declaration of the Independence of Cyberspace* [online] last accessed 05/15/2010 <https://projects.eff.org/~barlow/Declaration-Final.html>.

Bartík, V. a Janečková, E. (2010) *Ochrana osobních údajů v aplikační praxi (vybrané otázky). Praktická právnická příručka*. 2. vydání, Praha: Linde.

Blahož, J. (2008) *Lidská práva a právní politika boje proti terorismu*. Editor Josef Blahož, Praha: Vysoká škola aplikovaného práva.

Budai. D (2010) *Ve Francii začal platit protipirátský zákon „HADOPI"* [online] navštíveno 21/07/2010 <http://www.itbiz.cz/zakon-hadopi-zacal-platit>.

Carey, P. (2004) *Data Protection. A Practical Guide to UK and EU Law*. 2nd edition, Oxford: University Press.

Carey, P. (2004) *Data Protection. Handook*, London: The Law Society.

Carroll, Michael W. (2007) Creative Commons as Conversational Copyright. Villanova Law/Public Policy Research Paper No. 2007-8; *Intellectual property and information wealth: issues and practices in the digital age* [online] Peter K. Yu, ed., Vol. 1, pp. 445-61, Praeger. přístupné na adrese <http://ssrn.com/abstract=978813>.

Central Computer and Telecommunications Agency (1996) *Legal Issues and the Internet. Reference Book*. London: HMSO Publications Centre.

Cousens, M. (2004) *Surveillance Law*, London: the LexisNexis UK.

Čermák, J. (2003) *Internet a autorské právo*. 2. Rozšířené vydání, Praha: Linde.

Danay, Robert Jacob, (2005) *Copyright Vs. Free Expression: The Case of Peer-to-Peer File-Sharing of Music in the United Kingdom* [online] 8 Yale Journal of Law & Technology 32. přístupné na adrese <http://ssrn.com/abstract=847905>.

Davidson, A. (2009) *The Law of Electronic Commerce*, Australia, Prot Melbourne: Cambridge University Press.

DeBeer, Jeremy F. and Clemmer, Christopher D. (2009) *Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries?* [online] October 1. Jurimetrics, Vol. 49, No. 4. přístupné na adrese <http://ssrn.com/abstract=1529722>.

Dobřichovský, T. (2004) *Moderní trendy práv k duševnímu vlastnictví v kontextu evropského práva, dohody TRIPS a aktivit WIPO*. Praha: Linde Praha, a.s.

Edwards, L. and Waelde, Ch. (2009) *Law and the Internet*. *A framework for Electronic Commerce*. 2nd edition, Oxford and Portland, Oregon: Hart Publishing.

Electronic Business Law Reports, vol. 1, issue3, pp. 110 – 120 [online] navštíveno 03/29/2010 <http://www.cyber-rights.org/documents/yahoo_ya.pdf>.

European Commission (1997) *Copyright and Related Rights in the Information Society - Proposal for Directive/Background*. 10 prosinec. přístupné na adrese <http://europa.eu.int/comm/dg15/en/intprop/intprop/1100.htm>.

Everard, J. (2000) *Virtual States. The Internet and the boundaries of the nation-state.* London: Routledge.

Giacomello, G. (2005) *National Governments and Control of the Internet. A digital challenge*. Abingdon, Oxon: Routledge.

Giblin, Rebecca and Davison, Mark (2006) *Kazaa goes the way of Grokster' Authorization of Copyright Infringement via Peer-to-Peer Networks in Australia*. [online] Australian Intellectual Property Journal. přístupné na adrese <http://ssrn.com/abstract=1028653>.

Goldsmith, J. and Wu, T. (2006) *Who Controls the Internet? Illusions of a Bordless World*. Oxford: Oxford University Press.

Guadamuz, Andrés (2002) *Copyright in Cyberspace: Building Fences on the Internet*. [online] Alfa Redi, No. 109, October. navštíveno 1/10/2010. přístupné na adrese <http://ssrn.com/abstract=595362>.

Helft, M. and Barboza, D. (2010) *Google Shuts China Site in Dispute Over Censorship* [online] publikováno 3/22/2010, navštíveno 4/2/2010 <http://www.nytimes.com/2010/03/23/technology/23google.html>.

Herceg, J. (2008) *Extermismus a hranice svobody projevu na internetu.* Český právní řád a ochrana kyberprostoru (vybrané problémy), Acta Universitatis Carolinae, Iuridica 4/2008. Praha: Nakladatelství Karolinum.

The Huffington Post (2010) *Google Threatening To Leave China Over Hacking, Email Leak* [online] publikováno 01/12/2010, last updated 03/18/2010, navštíveno 04/02/2010 <http://www.huffingtonpost.com/2010/01/12/google-threatening-to-lea_n_420857.html>.

Chilcot, J. (2008) *Privy council review of intercept as evidence*. Report pro vládu UK [online] dostupné na adrese <http://www.official-documents.gov.uk/document/cm73/7324/7324.pdf>.

Ikaros, redakce (2005) *Internet kontra copyright* [online] navštíveno 01/08/2010 dostupné na adrese <http://www.ikaros.cz/internet-kontra-copyright>.

Information Commissioner's Office (neuvedeno) *Oficiální instrukce nakládání s osobními údaji*. [online] navštíveno 21/04/2010. přístupné na adrese <http://www.ico.gov.uk/>.

Kalathil, S. and Boas, C. T. (2001) *The internet and State Control in Authoritarian Regimes: China, Cuba, and the Counterrevolution*. Peer-Reviewed Journal on the Internet, vol. 6, issue 8, publikováno 08/06/2001.

Klíma, K. a kol. (2009) *Komentář k Ústavě a Listině. 2. díl.* 2. rozšířené vydání, Plzeň: Aleš Čeněk.

Knap, K. a kol. (2004) *Ochrana osobnosti podle občanského práva*. 4. vydání, Praha: Linde.

Kříž, Jan. et. al. (2005) *Autorský zákon: Komentář a předpisy související*, 2. Aktualizované vydání. Praha: Linde.

Kučerová, A., Bartík, V., Peca, J., Neuwirt, K., Nejedlý, J. (2003) *Zákon o ochraně osobních údajů. Komentář*, Praha: C. H. Beck.

Kurbalija, J. (2005) *An Introduction to Internet Governance*. [online] navštíveno 03/31/2010 <http://www.diplomacy.edu/ISL/IG/default.htm>.

Leiner, B. M. et col. (neuvedeno) *Histories of the Internet. A Brief History of the Internet* [online] navštíveno 05/15/2010 <http://www.isoc.org/internet/history/brief.shtml>.

Lessig, L. (2001) *The Future of Ideas* [online] navštíveno 03/31/2010 <http://thefutureofideas.s3.amazonaws.com/lessig_FOI.pdf>.

Lim, Y., L. (2007) *Cyberspace Law. Commentaries and Materials*. 2nd edition, Oxford: University Press.

Lloyd, I. J. (2008) *Information Technology Law.* 5th edition, Oxford: Oxford University Press.

Lloyd, I. (2000) *Legal Aspects of the Information Society*. London: Butterwoths.

Macková, A. a Štědroň, B. (2009) *Zákon o elektronických úkonech a autorizované konverzi dokumentů s komentářem včetně souvisejících zákonů a prováděcích předpisů*, Praha: Woletrs Kluwer ČR, a.s.

Maštalka, J. (2008) *Osobní údaje, právo a my*, Praha: C. H. Beck.

Mates, P. (2006) *Ochrana sourkomí ve správním právu*. 2. vydání, Praha: Linde.

Mates, P. a Smejkal, V. (2006) *E-Government v českém právu*, Praha: Linde.

Mathiason, J. (2009) *Internet Governance The new frontier of global institutions*. UK, London: Routledge.

Matoušková, M. a Hejlík, L. (2008) *Osobní údaje a jejich ochrana*. 2. vydání, Praha: ASPI.

McArthur, R., L. (2001) *Reasonable expectations of privacy*. Ethics and Information Technology 3: 123 – 128. dostupné též na adrese <http://collections.lib.uwm.edu/cipr/image/24.pdf>.

Meyer, D. (2010) *Digital Britain minister concedes file-sharer "disconnection"* [online] navštíveno 24/03/2010 <http://www.zdnet.co.uk/blogs/communication-breakdown-10000030/digital-britain-minister-concedes-file-sharer-disconnection-10015403/.>.

Montecino, V. (1996) *Copyright and the Internet* [online] navštíveno 10/08/2010. Dostupné na adrese <http://mason.gmu.edu/~montecin/copyright-internet.htm>.

Murray, A. D. (2007) *The Regulation of Cyberspace*. *Control in the Online Environment*. The UK, Oxon: Routledge-Cavendish.

Office of Public Sector Information (2010) *Digital Economy Act 2010* [online] navštíveno 15/04/2010 <http://www.opsi.gov.uk/acts/acts2010/ukpga_20100024_en_1>.

PC Magazine Online (2010) *"French Anti-Piracy Law Actually Increases Piracy."* [online] navštíveno 11/08/2010, dostupné na adrese <http://find.galegroup.com/gtx/infomark.do?&contentSet=IAC-Documents&type=retrieve&tabID=T003&prodId=AONE&docId=A222470126&source=gale&srcprod=AONE&userGroupName=mmucal5&version=1.0>.

Pessach, Guy (2006) *An International-Comparative Perspective on Peer to Peer File-Sharing & Third-Party Liability in Copyright Law - Framing Past - Present and Next-Generation's Questions*. [online] Vanderbilt Journal of Transnational Law, Forthcoming. přístupné na adrese <http://ssrn.com/abstract=924527>.

Reidenberg, Joel, R. (2010) *The Yahoo Case and the International Democratization of the Internet*. Fordham Law & Economics Research Paper No. 11, April 2001 [online] navštíveno 02/04/2010 <http://ssrn.com/abstract=267148>.

Reed, Ch. (2004) *Internet Law. Text and Materials.* 2nd edition, Cambridge: Unviersity Press.

Rigby, B. (2010) *Yahoo Knew of Google Attacks, Kept Quiet* [online] publikováno 01/10/2010, navštíveno 04/02/2010 <http://www.pcmag.com/article2/0,2817,2358175,00.asp>.

Rowland, D. and Macdonald, E. (2005) *Information Technology Law*, 3rd edition, London: Cavendish Publishing Limited.

Schaumann, Niels B., *Copyright Infringement and Peer-to-Peer Technology* (2002). William Mitchell Law Review, Vol. 28, No. 3 [online] přístupné na adrese: <http://ssrn.com/abstract=1527189>.

Smejkal, V. (2004) *Právo informačních a telekomunikačních systémů*. 2. vydání. Praha: Linde.

Story, A. (2002) *Study on Intellectual Property Rights, the Internet, and Copyright*. [online] UK, Kent: Universtiy of Kent, navštíveno 24.9.2010. dostupné na adrese <http://www.iprcommission.org/papers/pdfs/study_papers/sp5_story_study.pdf>.

Šámal, P. a kol., (2010) *Trestní zákoník II. § 140 až 421. Komentář.* 1. Vydání. Praha: C. H. Beck.

Švestka, J., Dvořák. J., a kol. (2009) Občanské právo hmotné, 3. díl, 5. vydání, Praha: Aspi.

Tai, Z. (2006) *The Internet in China. Cyberspace and Civil Society*. New York, USA: Routledge.

Univerzita Karlova v Praze (2008) *Český právní řád a ochrana kyberprostoru* (vybrané problémy), Acta Universitatis Carolinae, Iuridica 4/2008. Praha: Nakladatelství Karolinum.

US Department of Commerce (1999) *International Safe Harbor privacy principles*. [online] Dostupné na adrese <http://www.ita.doc.gov/td/ecom/Principles1199.htm>.

Vaníček, Z. (2009) *Právní předpisy související se zákonem o elektronických komunikacích*. *Praktická právnická příručka*, Praha: Linde.

Vaníček, Z. (2008) *Zákon o elektronických komunikacích*. *Komentář*, Praha: Linde.

Wild, Ch., Weinstein, S. and MacEwan, N. (2005) *Internet Law*. UK, London: Old Bailey Press.

Použité právní předpisy

Mezinárodní smlouvy

Evropské úmluvě o ochraně lidských práv a základních svobod 1950.
Mezinárodní pakt o občanských a politických právech z roku 1977.
Mezinárodní úmluva o ochraně výkonných umělců, výrobců zvukových záznamů a rozhlasových organizací, 1961, Řím.
Smlouva Světové organizace duševního vlastnictví (WIPO) o právu autorském, Ženeva 1996.
Smlouva Světové organizace duševního vlastnictví (WIPO) o výkonech výkonných umělců a o zvukových záznamech, Ženeva 1996.
Univerzální deklarace lidských práv 1948.
Úmluva o příslušnosti soudů a uznání a výkonu rozhodnutí ve věcech občanských a obchodních z roku 1968 (Bruselská úmluva).
Úmluva Rady Evropy č. 108/1981.
Listina základních práv Evropské Unie z roku 2000.

Právní předpisy Evropské Unie

Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích).
Směrnice Evropského Parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (směrnice o ochraně osobních údajů).
Směrnice Evropského parlamentu a Rady 2002/21/ES ze dne 7. března 2002 o společném předpisovém rámci pro sítě a služby elektronických komunikací (rámcová směrnice).
Směrnice Evropského parlamentu a Rady 2001/29/ES ze dne 22. května 2001 o harmonizaci některých aspektů autorského práva a práv s ním souvisejících v informační společnosti.

Směrnice Evropského parlamentu a Rady 2004/48/ES ze dne 29. dubna 2004 o dodržování práv duševního vlastnictví.
Směrnice Evropského Parlamentu a Rady č. 2000/31/ES ze dne 8. června 2000 o elektronickém obchodu.
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.

Předpisy České Republiky
Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.
Zákon č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů.
Zákon č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů.
Zákon č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů.
Zákon č. 337/1992 Sb., o správě daní a poplatků, ve znění pozdějších předpisů.
Zákon č. 1/1993 Sb., Ústava České Republiky, ve znění pozdějších předpisů.
Zákon č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů.
Zákon č. 182/1993 Sb., o Ústavním soudu, ve znění pozdějších předpisů.
Zákon č. 154/1994 Sb., o Bezpečnostní informační službě, ve znění pozdějších předpisů.
Zákon č. 29/2000 Sb., o poštovních službách a o změně některých zákonů (zákon o poštovních službách), ve znění pozdějších předpisů.
Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.
Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.
Zákon č. 480/2004 Sb., o některých službách informační společnosti, ve znění pozdějších předpisů.
Zákon č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů.
Zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

Předpisy Velké Británie
The Anti-Terrorism Crime and Securities Act 2001.
The Computer Misuse Act 1990.

The Copyright (New Technologies) Amendment Act 2008.
The Data Protection Act 1998.
The Defamation Act 1996.
The Digital Economy Act 2010.
The Eletronic Commerce (EC Directive) Regulations 2002, SI 2002/2013.
The Human Rights Act 1998.
The Regulation of Investigatory Powers Act 2000.
the Telecommunications (Data Protection and Privacy) (Amendment) Regulations 2000, SI 2000/157.

Předpisy Francie
Loi favorisant la diffusion et la protection de la création sur Internet (tzv. HADOPI zákon) <http://www.laquadrature.net/wiki/HADOPI_full_translation#CHAPTER_I> (anglický překlad), účinný od května roku 2009.

Předpisy USA
Ústava Spojených Států Amerických.
The Controlling the Assault of Non-solicited Pornography and Marketing Act 2003.

Citované soudní případy

A & M Records, Inc. v. Napster, Inc., 114 F.Supp. 2d 896, 913 (N.D. Cal. 2000) a 239 F 3d 1004 (9th Cir 2001).
ALCU v Reno 929 F Supp 824 (ED Pa, 1996).
Braintech Inc. v. Kostiuk (1999) 171 DLR 4th 46 (BCCA).
Campbell v UK [1993] 15 EHRR 137.
European Commission Communication, Illegal and harmufl content on the Internet COM(96)0487 – C4-(0592/96), 1999.
Godfrey v Demon Internet Ltd [1999] 4 All ER 342.
Gutnik v Dow Jones [2002] HCA 2002.
Hallford v UK [1997] IRLR 471, ECHR.
Ibcos Computer Ltd. v. Barclays Mercantile Highland Finance Ltd. [1994] FSR 275.
Jersil v Denmark [1995] 19 EHRR 1.
King v Lewis [2004] EWHC 168.

Klass v Germany [1978] 2 EHRR 214.
League Against Racism and Antisemitism (LICRA) v. Yahoo! Inc. 20 November 2000, Tribunal de Grande Instance de Paris.
ESD Lindqvist, Case C-101/01 Criminal Proceedings against Lindqvist [2003] All ER (D) 77 (Nov), ECJ.
Malone v UK [1984] 7 EHRR 14.
MGM Studios, Inc. v. Grokster, Ltd. 545 U.S. 913 (2005).
Universal Music Australia v Sharman License Holdings (2005) 65 IPR 289.
Michael John Durant v Financial Services Authority [2003] EWCA Civ 1746.
New York Times v Sullivan, 376 US 254 (1964).
Promusicae v Telefonica, ESD, 29 Leden 2008, C-275/06.
R v Gold (and Schifreen) [1988] 1 AC 1063.
Re SOCAN Statement of Royalties, Public Performance of Musical Works 1 C.P.R. (4th) 417.
Totalise plc v Motley Fool Ltd [2003] 2 All ER 872.
Shevill and Others v Presse Alliance SA [1995] All ER (EC) 289.
Shetland Times Ltd v. Jonathan Wills and Another [1997] SLT 669.
Slipper v BBC [1990] 1 All ER 165.
Caroline von Hannover, Ústavní soud SRN.
UK v rozhodnutí R v S ans A [2008] EWCA 2177.
Workman, supra note 136 (discussing SABAM v. S.A. Scarlet (formerly Tiscali), Tribunal de premiere instance de Bruxelles [T.P.I.] [Court of First Instance] Brussels, May 18, 2007 (Belg.).

Shrnutí

Právní otázky internetu v mezinárodním a vnitrostátním právu

Globální síť internet změnila sociální, politický i obchodní život většině lidí světa. Komunikace je výrazně rychlejší, tok informací po celém světě trvá několik málo vteřin. Výměna politických, osobních či obchodních informací, děl chráněných autorským právem či jiných informací je nezadržitelná. Členové mezinárodního společenství se pokouší vyrovnat s touto novou výzvou jejich právních i politických systémů.

Tato diplomová práce se zabývá několika oblastmi soukromého práva, ve kterých internet hraje nejvýznamnější roli a jeho dopadem se mění výklad mnoha právních norem. Práce je rozdělena do dvou hlavních částí. První se věnuje obecným aspektům internetu, jako je historie, struktura, rozdílné regulační vrstvy, autorské právo on-line, obecné právní otázky vyvstávající ze soudního případu Yahoo! a dopady, které internet má na některé politické systémy. Druhá část pojednává podrobněji o jednotlivých oblastech z pohledu ochrany osobnosti, soukromí a osobních dat v on-line prostředí. Konkrétněji, obsahuje kapitoly zabývající se komunikačními programy, sociálními sítěmi, přímým obchodováním a jiným užíváním internetu pro obchodní účely. Zvláštní kapitola je věnována technologii peer-to-peer a jejího (zne)užívání spojené s užíváním autorskoprávních děl. Úzce související s protiprávními aktivitami internetových uživatelů a nástrojů právní regulace je i postavení poskytovatelů služeb informační společnosti. V průběhu posledních let byly přijaty nové zákony některými rozvinutými státy jako je Francie či Velká Británie, které právě po poskytovatelích vyžadují více pro-aktivní roli týkající se porušování autorských práv. V případě, že tak neučiní, poskytovatelé mohou být subjekty sekundární odpovědnosti. Poslední část popisuje právní důsledky ochrany zaměstnanců komunikujících elektronickými prostředky.

Jednotlivá témata jsou řešena z mezinárodního, evropského i vnitrostátního hlediska, je-li to nezbytné. Výklad je zaměřen zejména na úpravu v České Republice ve srovnání s úpravami jiných států, zejména Velké Británie, popřípadě i Spojených Států Amerických (USA) a Francie.

Summary

Legal issues of the Internet from the scope of international and national law

Global internet network has changed the social, political and business life of most people in the World. Communication is much faster, the flow of information all around the World takes a few seconds. Exchange of political opinions, personal and business information, works protected by copyright and other information has become unstoppable. Members of the international community are trying to tackle this new challenge to their legal and political systems.

This diploma thesis is describing some arreas of private law where Internet plays the most important role and has changed the scope and interpretation of many legal rules. The work is dividend into two main parts. The first one deals with general aspects of the Internet such as its history, architecture, different regulatory layers, the copyright law on-line, general legal issues arising from the Yahoo! case and its impact on political systems. The second part describes more specific areas mainly focused on the protection of personality and personal data in the on-line environment. To be more specific, there are chapters dealing with communication software, social networks, direct business and usage of the Internet for business reasons. Specific chapter is dedicated to peer-to-peer technology and its (mis)use when using copyrighted works. Closely related with unlaflul activities of internet users and regulatory instruments is the position of ISPs (International Service Providers). During last years, new pieces of legislation has been enacted by developed states such as France or the United Kingdom (the UK), which require ISPs to play much more pro-active role while dealing with copyright infringement. In the case of failure to do so, ISPs may be subject of secondary liability. The last part provides the legal isuess concerned with protection of employees communicating by electronic means.

When necesary, international, european and national regulatory framework is provided. The comments are focused on legal system of the Czech Republic in comparision with others, mainly with the UK, eventually with the USA and France.

Klíčová slova: internet, ochrana osobnosti a osobních dat, autorské právo, peer-to-peer sítě

Key words: internet, protection of personality and personal data, copyright, peer-to-peer networks