UNIVERZITA KARLOVA V PRAZE
PRÁVNICKÁ FAKULTA

RIGORÓZNÍ PRÁCE

Tradiční a nové právní instituty v prostředí internetové sítě

Traditional and new legal concepts in the environment of internet network

Konzultant: JUDr. Tomáš Dobřichovský, Ph.D.

Zpracovatel: Mgr. Petr Miroš

Květen 2011

„Prohlašuji, že jsem tuto rigorózní práci zpracoval samostatně, že jsem vyznačil prameny, z nichž jsem pro svou práci čerpal způsobem ve vědecké práci obvyklým, a že tato práce nebyla využita k získání jiného nebo stejného titulu.“

V Praze dne 23. května 2011 Mgr. Petr Miroš

Poděkování za konzultace:

„Děkuji panu JUDr. Tomáši Dobřichovskému, Ph.D. za konzultace a připomínky.“

Tradiční a nové právní instituty v prostředí internetové sítě
Traditional and new legal concepts in the environment of internet network

Obsah

1. Úvod

Ještě před dvěma desítkami let bylo něco jako globální internetová síť, díky které lze snadno a během několika málo vteřin komunikovat s kýmkoli třeba na jiném kontinentě něčím, co si pouze někteří vědci a literární autoři uměli představit. Rychlý technický pokrok, jehož jsme v současné době svědky, klade nové výzvy a to jak na společnost a její chování, tak na její právní regulaci. Společnost se čím dál více stává globální, s rozvojem vzdělanosti a snadnou dostupností informací jsou geografické hranice opomíjeny a překonávány. Internetová síť, obdobně jako užívání mobilních telefonů, které se dnes již bez připojení k internetu téměř také neobejdou, je novým nástrojem a prostředím, ve kterém se členové společnosti dostávají do vzájemných vztahů, a to i z hlediska právního. Zejména v průběhu poslední dekády, kdy se dostupnost informační technologie výrazně přiblížila obyčejným lidem vyspělého světa a rozšiřuje se dále i do zemí méně rozvinutých, znamená internet mimo jiné i významné místo v ekonomickém a podnikatelském světě. Dnes je již pravidlem, že každý podnikatel je nějakým způsobem účastníkem internetu, dokonce i největší světové společnosti dnes mohou mít formu čistě virtuální. Ovšem i pro soukromé účely je internet dnes již nezbytným nástrojem. Rozvoj sociálních sítí, užívání elektronických komunikačních prostředků namísto telefonu či dopisů je dnes již běžnou součástí naší komunikace.

Globální charakter internetového prostředí s sebou přináší mnohé výhody i nevýhody zároveň. Mezi nesporné výhody patří již zmíněná informovanost a šířící se vzdělanost dnešní společnosti. Internet je zároveň vhodným komunikačním kanálem, ať se jedná o písemné, zvukové či vizuální formy komunikace. Důkazem mohou být i velmi se rozvíjející sociální sítě, které každým dnem zaznamenávají více registrovaných a aktivních uživatelů. Pro podnikatele může tato počítačová síť znamenat velmi zajímavé možnosti z různých úhlů pohledu. Poskytované služby mohou využívat lidé bez ohledu na jejich geografické umístění. Internet je také způsobem, jak oslovit mnohem více zákazníků, a to i z pohledu příhraničního. Tak například původně garážová firma Google je dnes jednou z nejznámějších a největších obchodních společností světa.

Z pohledu druhého však internetová síť přináší i mnohé problémy a hrozby pro soukromé i veřejné zájmy. Komunikační prostředky mohou být předmětem a nástrojem páchání protiprávní i trestní činnosti. Prostřednictvím internetu lze ovlivnit veřejné mínění a pověst známých lidí na území mnoha států během velmi krátké doby. Zásahy do osobní integrity a soukromí jsou velmi častým problémem, na který se právní úprava snaží reagovat. Prostřednictvím internetu lze účinně a snadno zasahovat i do podnikání ostatních. Je nástrojem pro páchání různých forem

nekalosoutěžního jednání, ale i způsobem, jak dochází k porušování práv k nehmotným statkům. V neposlední řadě i páchání trestné činnosti je v době globálního propojení internetem výrazně jednodušší. Tím bývá zasahováno i do veřejných zájmů a bezpečnosti.

Z pohledu této práce je důležité, že internet zasahuje a mění kromě faktického života dnešní společnosti také právní regulaci jejího chování, a to jak na mezinárodní tak vnitrostátní úrovni. Mezinárodní povaha vyžaduje úzkou a jednotnou spolupráci i v oblasti regulace internetu a vztahů, které v jeho rámci vznikají. I z tohoto důvodu je první část práce věnována obecné charakteristice, struktuře a přístupu některých států k internetové síti a její regulaci jako takové. Další část se týká institutu autorských práv, který zaznamenal s rozvojem nových technologických prostředků výrazné ohrožení a změny. Internet s sebou přináší i nové instituty, do té doby neznámé, na které bylo nutné aplikovat stávající, popřípadě přijmout novou právní regulaci. Významným prostředkem, který kromě jiného přinesl i zásadní orientační zjednodušení v rámci internetové sítě, jsou doménová jména. Jejich význam a úprava je předmětem další části této práce. Poslední kapitola se pak zabývá již zmíněnými dopady na soukromí a osobní integritu uživatelů internetu z různých pohledů a právních aspektů.

2. Právní povaha internetu

2.1 Obecné otázky a vývoj internetové sítě

Vzhledem k tomu, že tato práce si jako hlavní cíl vytyčila posoudit stav právní regulace některých právních institutů a případné nedostatky při jejich aplikaci v prostředí internetu, je třeba nejdříve zvážit samotnou povahu a obecné aspekty tohoto fenoménu posledních desetiletí. Soudy v různých zemích se od počátku potýkají s obtížemi jak definovat internet a jak na něj aplikovat stávající právní úpravu.[1] Termín Internet tak zůstal bez uspokojivé právní definice. Edwards jej popsal jako „veřejnou mezinárodní síť sítí".[2] Tato teze však není příliš vypovídající. Internet je, zjednodušeně řečeno, uskupení počítačů fyzicky propojených mezi sebou kabely, případně jiným způsobem. Důležitým důsledkem této decentralizované struktury je, že žádný subjekt nemůže plně kontrolovat všechny aktivity, které v jeho rámci probíhají. Autor tak poukazuje zejména na povahu internetu jako mezinárodní komunikační sítě, která přesahuje kontrolu jednotlivých národních autorit.[3] Zastánci této základní myšlenky tak zdůrazňují, že přirozenou povahou internetu je jeho nadstátní povaha, a tudíž internet by měl mít vlastní, na žádném státu závislou, „vládu" a regulaci. Ovšem jak je patrno dále, tento bezesporu idealistický přístup s mnoho zastánci zejména v průběhu 90. let byl podroben mnoha právním analýzám v průběhu posledních dvou desetiletí, a to zejména v důsledku sporů, ke kterým byly nuceny soudy zaujmout právní stanovisko. 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 historie internetové sítě. Následně je nastíněna struktura a regulace internetu, jeho tří vrstev, a do jaké míry mohou jednotlivé státy vykonávat svůj vliv na některou z nich. Pojednáno bude také o přístupu v některých autoritářských státech a národních systémech, které se pokusily vykonávat co nejpřísnější kontrolu internetu v rámci svého území. Zejména stojí za zmínku, jaké prostředky a metody byly použity a jaký výsledný efekt měl střet internetu a jejich právního řádu a politického systému. Přiblížen bude také odborné veřejnosti známý tzv. soudní případ Yahoo,

[1] Re SOCAN Statement of Royalties, Public Performance of Musical Works 1 C.P.R. (4th) 417, kde se kanadský senát zabýval internetem a jeho specifickým způsobem přenosu dat; nebo Braintech Inc. v. Kostiuk (1999) 171 DLR 4th 46 (BCCA), kde bylo pouze obecně popsán internet jako globální super-síť počítačových sítí.

[2] Edwards 2000, p. 1 – 3.

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

který je považován za jeden z mezníků pro vývoj právního pojetí internetu a jeho vztahu k právním řádům jednotlivých zemí.[4]

Blíže tedy k přirozené povaze internetu. V čem je vlastně odlišná a obtížná z pohledu regulace, a je tedy nutná zvláštní regulace pouze tohoto fenoménu? Na tyto otázky existují protichůdné názory. 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 telekomunikační síť či jiná obdobná média. Podle něho je internet pouze produktem globalizace a žádná specifická úprava 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 aplikovaly stávající právní předpisy právě na činnosti v 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 získal tak neoprávněný přístup k informacím, které následně použil při své práci. Soud prvního stupně sice uznal pachatele viným z trestného činu krádeže, avšak odvolací soud i senát jej nakonec zprostily viny. Zabývaly se totiž otázkou, zda lze informaci jako takovou, která není nikde uložena ani jinak ztělesněna v hmotné podobě, ukrást. Pouhé užití vypozorovaného hesla nelze považovat za hmotný substrát způsobilý k tomu, aby byl ukraden, a tak soud dovodily, že dosavadní legislativa ani právní řád s tímto případem nepočítají a tudíž pachatele nelze vinit ani z krádeže ani z jiného trestného činu připadajícího v úvahu.[6] Tento případ vzbudil pozornost široké veřejnosti a poprvé ukázal na novou povahu rozšiřujícího se média a s tím spojené případné aplikační a výkladové problémy stávajících právních institutů. Následně byla přijata nová legislativa, která se specificky zabývá internetem a podobnými elektronickými systémy, zákon o zneužití počítače z roku 1990.[7] Toto je pouze jeden z příkladů, kdy v důsledku rozvoje internetu a činností ve virtuálním světě byl přijat zvláštní zákon, případně upravena stávající regulace.

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

[5] Murray 2007, str. 9 – 12.

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

[7] The Computer Misuse Act 1990.

Na druhé straně vznikl názor fundamentálně odlišný. Tak zvaní ochránci internetu prohlašovali, že internet je odděleným prostorem od reálného světa, tzv. cyberspace, který je nezávislý a nadřazený 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 poměrně extrémní a nerealistické. Jak vývoj právní úpravy v posledních letech ukazuje, některé aspekty internetové sítě je nutné regulovat odlišnými metodami a prostředky než jak je tomu v reálném (hmotném) světě.[9]

Historicky se internet vyvinul obdobným způsobem jako užívání a rozvoj sítě mobilních telefonů, tato technologie má své kořeny ve vědecké činnosti obranných armádních složek USA. V průběhu studené války a případné hrozby nukleární války, ARPA (oddělení technologického vývoje pro obranné účely)[10] vyvinulo novou komunikační technologii, která by byla používána po případné nukleární válce namísto telefonní sítě.[11] Její technická odlišnost záleží v tom, že při komunikaci je přenášeno přes velké množství cest mnoho malých částí informace, tzv. paketů. Každá zpráva či jiný druh přenášené informace je tak rozdělená do velkého počtu přenášených paketů putujících k jejich příjemci samostatně po různých cestách. Proto v případě neprostupnosti jedné cesty je paket přenesen přes cestu jinou, a navíc takový paket sám o sobě nemá žádný význam. Teprve v přístroji příjemce se pakety opět spojí dohromady a znovu vytvoří přenášenou informaci. Jak je zřejmé, konstrukce zároveň měla téměř znemožnit odposlouchávání a zachycení celé informace v průběhu jejího přenosu. Poprvé byla vytvořena síť v roce 1969, která byla pouze mezi čtyřmi počítači (nody nebo také přístupovými body). Ještě v průběhu šedesátých let byl vyvinut také internetový protokol, na jehož základě je přenos realizován. Jde o tzv. TCP/IP protokol, který je užíván dodnes.[12] Následovalo také zavedení mezinárodního standardu WWW, které napomohlo jednotnému užívání internetových stránek a přenášení informací po celém světě, je příznačně zkratkou z anglického World Wide Web. Masivní růst

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

[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] <http://www.isoc.org/internet/history/brief.shtml>.

[12] The Transmission Control Protocol/Internet Protocol.

internetového připojení ve všech částech světa byl však zaznamenán zejména v průběhu posledních dvou dekád. Lze poměrně bez nadsázky konstatovat, že internet hraje nyní fundamentální roli v každodenním životě velké většiny obyvatel i podnikatelských subjektů.[13] Důkazem významného postavení internetu je i zakotvení práva na vysokorychlostní internet mezi jedno za základních lidských práv, ke kterému došlo například ve Finsku v roce 2009.[14]

Pokud jde o právní přístup k internetu, za jeden z důležitých okamžiků v historii internetu je považován soudní případ týkající společnosti Yahoo,[15] ve kterém byla detailně posuzována povaha internetu a aplikace národního, v tomto případě francouzského, práva ve virtuálním prostředí. Soudní případ samotný byl sice slyšen ve francouzské Paříži, která je považována historicky za kolébku novodobého kontinentálního práva, avšak jeho význam sahal daleko za hranice evropského kontinentu. V podstatě se jednalo o spor mezi obchodní společností podnikající v rámci internetové sítě a tradičními hodnotami chráněnými národním právem Francie. Výkladové problémy se totiž ukázaly již se samotnou aplikovatelností tamního národního práva ve virtuálním prostředí internetové sítě. S tím úzce souvisela též otázka jurisdikce francouzského soudu nad cizími subjekty, např. společnostmi obchodujícími na internetové síti. Z obecnějšího hlediska to byl také koncepční spor mezi obránci internetu, pro něž internet byl prostředím bez právní regulace a bez její potřeby (kteří hájili neaplikovatelnost francouzského práva a nedostatek jurisdikce tamního soudu nad americkou společností fyzicky nikterak spojenou s francouzským územím), a těch, kdo zastávali tradiční pojetí internetu jen jako dalšího druhu komunikačního media.[16]

Fakta byla taková, že společnost Yahoo v roce 2000 poskytovala službu internetové aukce na svých webových stránkách www.yahoo.com. V jedné z aukcí se objevily na prodej předměty nacistické propagandy, které francouzské právo v důsledku druhé světové války postavilo mimo zákon. Fakt, že tyto předměty byly určeny pro prodej na území Francie, byl dovozen zejména z toho, že aukce a stránky byly ve francouzském jazyce a byly přístupné na území Francie. Mark Knobel, francouzský žid a čelní představitel Ligy Proti Rasismu a

[13] Lloyd 2000, str. 26 až 28.

[14] Ahmed 2009, str. 1.

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

[16] Lloyd 2000, str. 1 až 3.

Antisemitismu, podal žalobu k francouzskému soudu, opírající se o francouzské právo, z důvodu protiprávnosti činnosti společnosti Yahoo a na odstranění těchto předmětů z prodeje.

V této souvislosti bylo vzneseno několik relevantních argumentů obecného dosahu. Hlavní argument žalobce založený na principu rovnosti a zákazu diskriminace byl, že Yahoo musí dodržovat národní zákony obdobně, jako každá jiná mezinárodní společnost podnikající v „reálném světě“. Tak například výrobce automobilů je povinen dodržet bezpečnostní předpisy a předpisy životního prostředí každé země, ve které mají být automobily prodávány, třebaže mohou být podmínky a požadavky jednotlivých států odlišné.[17]

Žalovaná společnost vznesla několik důležitých a problematických námitek. První se týkala 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.[18] Druhý argument varoval, že díky přirozené povaze internetu, který nebere ohled na státní hranice v reálném světě, webová stránka Yahoo by tak mohla být shledána za náležící do jurisdikce práva každého jednotlivého státu na světě. To by mohlo v konečném důsledku vést až k restrikci svobody slova a jiných lidských práv, jelikož by se muselo uplatňovat vždy právo toho státu, jehož právní úprava je nejvíce restriktivní. Tím by fakticky docházelo k omezování lidských práv například podle práva čínského či Saudské Arábie, a to i na území všech ostatních států. Navíc by to mohlo vést i k eventuální nejistotě při určování, jaký právní řád musí být dodržován v souvislosti s internetem. Třetí námitka se pak zakládala na technické rovině. Bylo tvrzeno, že není technicky možné zajistit například omezení či úplné zamezení přístupu na konkrétní webové stránky z určitého geografického území (např. z území Francie), aniž by to mělo dopad na ostatní uživatele internetu. Bylo by tedy nutné zajistit každý jednotlivý přístupový bod (počítač) na francouzském území, což by bylo prakticky neproveditelné.[19]

Soud se vypořádal s argumenty takto. Francouzská působnost a jurisdikce byla dovozena na základě tzv. principu účinku trestního zákoníku, který se jinak také označuje za tzv. passive personality principle. Podstatou je, že francouzské trestní právo je aplikovatelné na činy spáchané proti státním občanům Francie, bez ohledu na místo činu či národnost pachatele.[20]

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

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

[19] Ibid. str. 6 a 7.

[20] Reidenberg 2001, str. 5.

Druhý argument byl v podstatě odmítnut jako irelevantní. Technická otázka byla zohledněna při formulaci povinnosti, jelikož společnosti Yahoo bylo přikázáno podniknout adekvátní opatření (reasonable measures), kterým měly být všechny nezbytné kroky k tomu, aby byl znemožněn či přerušen jakýkoli přístup francouzských občanů přes yahoo.com do dotčené aukce.[21] Konečné rozhodnutí tedy bylo ve prospěch žalobce.

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 stanovené dvouměsíční lhůty na 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.[22] Přesto však Yahoo formálně nakonec dosáhla svého, když americký obvodní soud následně odmítl uznat toto rozhodnutí francouzského soudu a vykonat jej pro nedostatek pravomoci. Profesor Reidenberg se však vyjádřil k tomu, že americký soud takto rozhodl z protekcionářských důvodů, ačkoli to bylo dokonce v rozporu se zavedenou praxí v USA. Uvádí, že se v té době již běžně uznávaly a vykonávaly rozhodnutí soudů jednotlivých amerických států (i v oblasti internetu) podle jejich vlastních, nikoli federálních, zákonů.[23] K tomu lze jen dodat, že Yahoo však fakticky v době rozhodnutí soudu v USA již sama zamezila prodej rasistických předmětů na svých aukcích, ovšem z ryze pragmatických důvodů. Přílišná negativní publicita nemůže být žádné globální společnosti ku prospěchu. Navíc svojí další činností sama poukázala na to, že technický argument není pravdivý, protože samotná společnost Yahoo o rok později vstoupila na trh čínský s podmínkou zdejší vlády, že bude své služby filtrovat a podrobovat jejímu dozoru (navzdory mnoha kritickým ohlasům ze stran obhájců lidských práv). Tím tacitně prokázala, že prostředky cenzury či kontroly internetu ve vztahu ke geograficky určenému území existují.[24]

V důsledku dění okolo tohoto soudního procesu, který byl sledovaný odbornou veřejností po celém světě, se rozpoutala diskuze o povaze a další regulaci internetového prostředí. Na jednu stranu je rozhodnutí francouzského soudu vítězstvím demokratických hodnot. Pozitivní

[21] Akdeniz 2001, str. 1.

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

[23] Reidenberg 2001, str. 9 až 11.

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

normativní dopad rozsudku je spatřován v tom, že internetové subjekty budou muset respektovat odlišné hodnoty veřejnosti namísto pouhého upřednostňování ekonomických zájmů.[25] Akdeniz však na druhou stranu zdůrazňuje, že hlavní devizou internetu je jeho otevřenost, přístupnost a publicita. Přílišné 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.[26] Naznačený vývoj ukazuje, že koncepční otázky nejsou zcela vyřešeny, avšak z právního hlediska je jasné, že se nejedná o žádný super-prostor oddělený a nezávislý na reálném světě, a že nad subjekty a jejich činnostmi mají jednotlivé státy moc i jurisdikci. Jakým způsobem svojí moc vykonávají, to bude podrobněji popsáno v následujících částech této kapitoly.

2.3 Struktura a regulace

Od počátku existence internetové sítě mají největší vliv na její strukturu a fungování Spojené státy americké. Vždyť také tam byla tato globální síť založena a fakticky ovládána. Spolu s globálním rozšířením a stále vzrůstajícím vlivem politickým i ekonomickým, se vlády jednotlivých národních států více zaměřily na tento fenomén a začaly požadovat spoluúčast na kontrole této 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 veškeré subjekty a instituce účastnící se internetové sítě. Na počátku mezinárodních debat o regulaci internetu byla myšlenka vytvořit mezinárodní „vládu“ internetu, která byla chápána jako záležitost čistě veřejnoprávní a měla tak mít povahu mezivládního orgánu či srovnatelného typu spolupráce.[27] Postupně ale převážilo širší pojetí, že se na regulaci a ovládání internetu mají podílet také subjekty nestátní povahy, včetně osob soukromých. Počátkem internetové vlády v širším smyslu byl světový summit o informační technologii, který se konal (WSIS) v roce 2003

[25] Reidenberg 2001, str. 2 až 4.

[26] Akdeniz 2001, str. 6.

[27] Kurbalija 2005, str. 9.

v Ženevě a v roce 2005 v Tunisu. Jejich výsledkem bylo založení mezinárodního Fóra, které se poprvé sešlo v roce 2006 v Aténách pod záštitou Organizace Spojených Národů.[28] Jeho účastníky byli, jak již bylo zmíněno, zástupci jednotlivých států, obchodních i jiných společností. Pokud jde ovšem o jeho první výsledky jednání Fóra, jde prozatím spíše o formu mezinárodní diskuze, jejímž výsledkem není žádný právně závazný dokument. Hlavním předmětem diskuze je bezpečnost internetu, zejména zabezpečení přenášených dat. Nejdůležitější posun však byl dosažen tím, že původně lokální síť v USA, která i po svém celosvětovém rozšíření neustále byla pod nadvládou a hlavní kontrolou tamní vlády, se postupně stává neutrálním mezinárodním prostředím. USA se vzdaly svého výsadního postavení ve prospěch neutrality a mezinárodní spolupráce, a to včetně spolupráce se zástupci internetového průmyslu jakými jsou například firmy Google nebo Yahoo. Tento trend dokladuje i založení mezinárodní instituce ICANN,[29] která vystřídala původní americký systém registrace doménových jmen. Tato mezinárodní internetová vláda je stále na svém počátku, ovšem jejím nejdůležitějším úkolem je vytvořit prostor pro mezinárodní jednání a zachování unifikované globální struktury internetu.

Jak bylo v posledních letech mnohokrát dokázáno, internet je svojí podstatou a dosahem odlišným komunikačním prostředím, které do určité míry vyžaduje novou formu vlády a regulace. Takto je chápána potřeba regulace nového kyberprostoru (new-cyber approach). Na druhé straně existuje přístup založený na tradicích již existující regulace a právních institutů (old-real approach), podle něhož není na internetu nic tak odlišného od jiné komunikační sítě. Za nejúčinnější a pragmatickou je však třeba považovat jakousi střední cestu. Součástí diskuze o formě vlády a její struktury byla i otázka, zda má být taková vláda centralizovaná či nikoli. Podle povahy sítě je vhodnější způsob decentralizovaný, avšak z hlediska finančního, organizačního i personální náročnosti, a v neposlední řadě též z hlediska efektivnosti, bylo nutné přiklonit se k určité míře centralizace ve formě mezinárodních institucí, jako jsou ICANN či W3C.[30] Současně je nezbytné povědomí o tom, že internet je prostředím, kde dochází ke střetu různých protichůdných zájmů, zejména mezi veřejným a soukromým sektorem. Největší internetové společnosti lobbují za decentralizovanou a pokud možno co nejméně regulovanou povahu tohoto celosvětového obchodního trhu. Naopak státní orgány uplatňující státní moc a suverenitu mají větší tendenci užívat svých pravomoci i ve virtuálním prostředí internetu. Neopomenutelné je i

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

[29] ICANN je zkratka z anglického Internet Corporation for Assigned Names and Numbers.

[30] Mathiason 2009, str.18. W3C je z anglického World Wide Web Consortium.

hledisko politické, pro které je internetové síť dalším prostorem politických zájmů, odlišných systémů a mezinárodních taktik. Gicomello uvádí, že čím vyvinutější stát je, tím více je a bude závislý na této počítačové síti.[31] Internet má čím dál větší dopad sociální, ekonomický i politický, a tudíž otázka a potřeba maximálně jednotné právní regulace je velmi aktuální. Cílem unifikace mělo být zejména zabránění fragmentace internetu, zajištění kompatibility a činnosti po celém světě, ochraně práv a definování povinností jednotlivých subjektů účastnících se internetu. V neposlední řadě je také nutné brát v potaz ochranu konečných uživatelů, předcházení zneužívání internetu, ochranu veřejných zájmů i podporu dalšího společenského a ekonomického rozvoje společnosti.[32]

Pojem regulace a ovládání internetu může být vykládán v různém smyslu. V užším smyslu se jedná o infrastrukturu internetové sítě v technickém slova smyslu. Sem spadá regulace například doménových jmen, IP adres a podobných institutů, a nejdůležitějším subjektem je ICANN. Širší přístup, který lépe charakterizuje současný stav je, že mezinárodní úprava by se měla zabývat též jinými souvisejícími aspekty. Měla by řešit otázky právní, ekonomické i otázky dalšího technického rozvoje.[33]

Hlavním úkolem právní regulace internetu je nalezení určité vyváženosti často protichůdných zájmů a práv. Tak například protichůdnost svobody slova na straně jedné a ochrany veřejného pořádku na straně druhé může vést k diskuzím o vykonávání kontroly nad obsahem internetu a přípustnosti jeho cenzury. Obdobně protichůdné jsou zájmy soukromé osoby a jejího soukromí oproti bezpečnostním zájmům státním, popř. i soukromých subjektů (například bezpečnostní systémy jednotlivých společností). V této souvislosti jde zejména o otázky internetové kriminality, monitorování internetu a odhalování trestné činnosti za pomoci a v prostředí internetové sítě. V neposlední řadě je internet také nejčastějším místem a nástrojem pro různé formy porušování práv duševního vlastnictví. Kromě nalézání této vyváženosti různých zájmu je nutné mít také na zřeteli značnou nevýhodu právní regulace technologií. Technologický vývoj je totiž zejména v posledních letech velmi rychlý, a tak regulace a právní terminologie spíše reaguje na negativní jevy, které případný vývoj přináší. Při pokusech o obecnější regulaci zejména do budoucna je totiž velmi náročné formulovat právní předpisy

[31] Gicomello 2005, str. 4.

[32] Kurbalija, J. (2005) *An Introduction to Internet Governance*. [online] <http://www.diplomacy.edu/ISL/IG/default.htm>, str. 7.

[33] Kurbalija 2005, str. 16.

dostatečně přesně ale zároveň široce tak, aby se netýkaly pouze dnešní situace. V tomto ohledu Kurbalija uvádí, že je důležitější stanovit obecný objekt ochrany, než se snažit o vymezení a zákaz konkrétního jednání.[34] V tomto pohledu může být výhodnější právní systém angloamerický, který je na základě soudních precedentů více flexibilní a je schopen lépe reagovat na další vývoj v budoucnosti.

Při popisu struktury a regulace internetu bývá využíván tzv. vrstvovitý model. Podle něho se internet skládá ze tří vrstev, které dohromady vytváří celek a umožňují tak fungování požadované komunikace. Kromě technických odlišností jsou také tyto vrstvy odlišné svojí právní povahou, jelikož každá vrstva je upravena odlišnými právními nástroji a ovládána různými subjekty. 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 jiný obsah.[35] Všechny tři vrstvy mají stejnou důležitost zejména z toho hlediska, že síť nemůže plnit svoji funkci při absenci kterékoli z nich. Z toho také vyplývá, že ke kontrole internetové sítě na určitém geografickém území postačí mít pod kontrolou třeba jen jedinou vrstvu.

Role jednotlivých států a jejich vlád je nezanedbatelná a do určité míry přítomná 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 tamních státních orgánů. 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 nebo W3C (the World Wide Web Consortium) vyvíjející technické parametry a specifikace. Všichni, kdo uplatňují své zájmy na internetu, jsou v této vrstvě za jedno. Cílem je udržování a vývoj sítě tak, aby byla co nejvíce bezpečná, stabilní a rychlá. Obsahová vrstva je nejvíce komplikovaná co do její regulace. Jedná se o konkrétní obsah

[34] Kurbalija 2005, str. 23.

[35] Lessig 2001, str. 23.

internetových stránek, přenášených informací či poskytovaných služeb. Zde vznikají problémy týkající se porušování právních předpisů, ohrožování a porušování práv ostatních subjektů, ať se již jedná o lidská práva, práva obchodněprávní povahy či práv k duševnímu vlastnictví. Má-li však být činnost efektivně regulována a případně vymáhána, je důležité při regulaci vycházet z vědomí vrstevnaté struktury internetu a z tzv. down-up metody. Tedy v čím nižší vrstvě se s regulací začne, tím větší efektivity lze dosáhnout. Typickým příkladem snahy o zvýšení efektivity v oblasti ochrany práv autorských je vývoj v posledních letech, kdy se část povinností i pravomocí přenáší na ty, kdo v podstatě ovládají vrstvy nižší, jak bude blíže popsáno v dalších částech této práce.

2.4 Státní kontrola v některých autoritářských režimech

Zde je uvedeno 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 fenomén efektivně kontrolován žádným státem, zde je několik příkladů dokazujících opak.

Jak již bylo zmíněno, podstatou je výkon kontroly alespoň nad jednou z vrstev internetu. Například Kuba chránící svůj politický systém izolovaný od okolního světa se vydala cestou nejrazantnější a fatální, jelikož má na svém území plně v moci vrstvu fyzickou. Tamní režim přísně kontroluje veškerou distribuci počítačů, která je téměř zakázána, až na některé výjimky pro státní účely. Pokud již je přístup k počítači připojenému k internetu umožněn, každý přenos zpráv či jakýchkoli informací je přísně monitorován a cenzurován. Ve své podstatě tedy touto cestou, jejímž důsledkem je maximální izolace kubánského obyvatelstva od ostatních částí světa, dokázal kubánský režim internet i své obyvatelstvo udržet pod svojí mocí a kontrolou.[36]

Daleko vyspělejší a sofistikovaný systém je nastaven v Číně. Čínská vláda si je vědoma finančního potenciálu a příjmů plynoucích z obchodů uskutečňovaných v prostředí internetu. Navíc cílem tamního režimu zdaleka není naprostá izolace od okolního světa. Je tomu právě naopak, mezinárodní obchod a zahraniční investice jsou jedním z hlavních finančních zdrojů komunistické Číny. Proto tento stát zajišťuje přístup na internetovou síť. Na druhou stranu ale tento nedemokratický režim nechce dovolit podkopávání své autority a snaží se tudíž přísně kontrolovat své obyvatelstvo ve všech rovinách, tedy i jeho činnost na internetu. Systém kontroly je založen na kombinaci různých metod. Přístupný obsah internetu je neustále monitorován a cenzurován tak, aby informace a materiály svojí povahou protirežijní nebyly přístupné čínským

[36] Kalathil a Boas 2001, str. 10.

obyvatelům. To je prováděno zejména technickými prostředky, specifickými programy a jejich nastavením. Kromě toho je provoz na interesu průběžně monitorován i „červenými vestami“ (red vests), což jsou specializovaní agenti, jejichž oficiálním posláním je obrana režimu.[37] Dalším prostředkem, který je zároveň povahou předběžné kontroly, jsou povinné licence každé společnosti podnikající na čínském trhu. Každá společnost podnikající prostřednictvím internetu na čínském území musí obdržet licenci od vlády, jejíž podmínky vláda individuálně určuje tak, aby každá i zahraniční společnost dodržovala politiku 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 činnost odporující zájmům komunistického režimu (například reportují majitele emailové schránky, ze které jsou posílány informace o lokální situaci či potlačování lidských práv zahraničním novinářům). Počítače je dovoleno mít vybavené pouze povolenými programy, jejich distribuce je rovněž kontrolována. Navíc vláda užívá i metod užívaných v minulosti komunistickými režimy, kterými je podkopávání vlastní společnosti a důvěry jejich členů. V Číně totiž existuje velké množství lidí vyhledávajících, popřípadě skrytě podporujících, různá fóra či skupiny, 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 poměrně efektivně daří. Přesto si ale nelze nevšimnout postupného pozitivního vlivu internetové sítě, která přispívá k demokratizační transformaci čínského politického režimu.

Tai uvádí některé příklady, jak internet pozitivně ovlivnil či urychlil společenské i politické změny v Číně směrem k větší demokratizaci režimu.[38] 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 o společenských i politických tématech, které v některých případech nakonec i samotná vláda bere v potaz. Navíc je i prostředkem, jak si pomocí nezávislých informací udržet vlastní úsudek a zaujmout názor, které není založen pouze na zkreslených informacích podávaných tamními médii. Lidé pak můžou své názory sdílet a diskutovat (ačkoli samozřejmě anonymně) mohou formovat aktivistické či protestní akce, jako například signatářské kampaně a podobně. K tomu Tai též poznamenává, že vláda je daleko více tolerantní k těmto formám vyjádření nesouhlasu

[37] Bandurski 2008, str. 1.

[38] Tai 2006, str. 289 – 292.

s oficiálním stanoviskem režimu, než je tomu ve fyzickém, reálném světě, kde každé shromáždění lidí či obdobná protestní akce je velmi rychle a tvrdě rozehnáno a potlačeno. Přesto však přetrvávají problémy. Na území Číny je stále poměrně malé procento obyvatel, kteří jsou připojeni na internetu nebo k němu mají běžný přístup. Tím se navíc prohlubují rozdíly mezi rozvinutými a méně ekonomicky důležitými částmi země. Zároveň Tai poukazuje na stále slabou občanskou společnost, která se však díky internetu začíná rozvíjet a nabývat na aktivitách i významu.[39] Důkazem, že k demokracii má režim ještě daleko, může být následující událost.

Čína poměrně tvrdě zareagovala na hrozbu v roce 2005, kdy čínský žurnalista poslal email s politicky „závadným" obsahem na webové stránky hostované v USA. Naneštěstí tuto zprávu odeslal ze schránky zřízené u společnosti Yahoo. Ta však poskytuje spolupráci a informace čínské vládě, což je jedna z podmínek udělení licence, tudíž jméno žurnalisty se velmi rychle dostalo do vědomí úřadů. Novinář byl zatčen a odsouzen na deset let odnětí svobody. Případ vzbudil velkou nevoli zastánců lidských práv z různých částí světa, a Yahoo tak čelila negativním kritikám. Avšak odpověď Yahoo byla velmi jednoduchá. Každý podnikatel je povinen dodržovat zákony toho státu, ve kterém podniká.[40]

Jedním ze současných sporů vzbuzujících pozornost zahraničních médií je spor 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 může vést k úplnému opuštění čínského trhu.[41] Ostatní společnosti, včetně Yahoo, se k případu vůbec nevyjadřují a tiše nadále v cenzuře a porušování lidských práv pokračují. Zda a v jakém časovém horizontu může dojít k obratu tohoto stavu, to je jen velmi těžko odhadnutelné.

[39] Tai 2006, str. 289 – 292.

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

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

Na případu Číny lze však nejlépe demonstrovat, jakým nástrojem může globální počítačová síť být. Na jedné straně může napomáhat šíření demokratických hodnot, lidských práv, vzdělanosti a vzniku občanské společnosti. Na druhé straně může být i mocným nástrojem jak k šíření, tak k odhalování trestné či společensky škodlivé činnosti.

2.5 Důsledky a pohled do budoucnosti

Internet, jako počítačová síť sítí, je virtuálním statkem, který není ve vlastnictví žádného subjektu či státu. Jako takový je zcela závislý na univerzálním technickém řešení, bez něhož by jednotlivé přístroje nemohly být vzájemně kompatibilní, a komunikace by mezi nimi nemohla probíhat. Z tohoto důvodu je důležité vytvoření nezávislých institucí typu ICANN, které zajišťují kromě jiného také jednotný rozvoj a standardy užívané v této počítačové síti. Z pohledu struktury internetu však toto je pouze krok v rámci logické vrstvy. O vrstvě fyzické není třeba příliš diskutovat, jelikož jak dokazují případy méně vyvinutých zemí, distribuce fyzických přístrojů umožňujících vůbec připojení a užívání internetu je plně v moci jednotlivých států a veřejné moci na jejím území. Pokud však jde o vrstvu nejvyšší, obsah je již výrazně složitější efektivně ovlivňovat. Zatímco na logické vrstvě se jeví mezinárodní spolupráce poměrně jednoduchá a jednotná, žádný stát nechce příliš omezit své promoci a suverenitu směrem k větší jednotě a mezinárodní spolupráci v oblasti regulace jednotlivých aspektů obsahové vrstvy. Některými instituty se zabývají i další části této práce a je vidět, že jsou poměrně značné rozdíly v jejich pojetí v jednotlivých zemích, nemluvě ani o zemích méně rozvinutých či zemích třetího světa, kde je situace ještě obtížnější.

V neposlední řadě také pojetí legální a aplikace národních práv zejména z pohledu mezinárodního práva soukromého hraje a bude hrát čím dál důležitější roli. V případě Yahoo byly některé problémy a názory poprvé posuzovány, zdá se však, že dnešní situace je mnohem jasnější, a to zejména pokud jde o vztahy mezi státy Evropské Unie, na které se vztahují příslušná nařízení. Přesto však určitá míra diskrece je na státech ponechána, a to zejména pokud jde o uznávání a výkon cizích rozhodnutí. Zásada oboustranné protiprávnosti totiž může v jednotlivých případech činit problémy. Proto užší snahy o jednotný výklad a aplikaci zásadních institutů by měl být snahou mezinárodní komunity. Kromě nástrojů mezinárodněprávních i přenesení některých pravomocí na centrální instituce může být efektivním a vhodným nástrojem.

Jak ukazují i zmíněné případy, dopady internetové sítě mohou mít i z našeho pohledu pozitivní vliv směrem k vývoji a efektivnímu fungování politické a občanské společnosti. Dokonce i takový stát, jako je Čína, může být v konečném důsledku ovlivněn směrem k budoucí demokratizaci tamního politického režimu. I ostatní státy, které nechtějí a dnes již ani dost dobře

nemohou existovat v izolaci, budou v budoucnu osud Číny následovat. I z pohledu rozvoje mezinárodní kontroly a dodržování práv je internet důležitým nástrojem. Nezávislé fungování médií a tím i necenzurované kontroly činností jednotlivých států a společností je v dnešní době velmi důležité. Je zájmem naší společnosti zachovat demokratizovanou povahu internetové sítě.

3. Internet z pohledu autorského práva

Tato kapitola zkoumá institut autorského práva, případně práv s ním souvisejících, a jakým způsobem jej ovlivnil vznik a používání internetové sítě. Je zajímavé sledovat, jak některé funkce lze jen těžko naplňovat a efektivně vymáhat, a to právě kvůli decentralizované a technicky velmi rychle se rozvíjející struktuře internetové sítě. Dosavadní vývoj dokonce došel tak daleko, že na jedné straně jsou zpochybňovány samotné základy existence a ochrany autorských práv, a na straně druhé ve vyspělých zemích a za účelem efektivní ochrany práv vyplývajících z autorskoprávní legislativy dochází k omezování a potlačování některých aspektů lidských práv a ochrany soukromí jednotlivců. O to více je pozoruhodné, že k největším omezením dochází ve státech, kde demokracie a ochrana lidských práv má nejdelší kořeny (např. Francie či Velká Británie).

Nejprve bude výklad směřovat ke vzájemnému působení internetu a autorského práva, následně je výklad zaměřen na jeden z nejzávažnějších nástrojů porušování autorských práv v počítačové síti, tzv. peer-to-peer sítě. Na závěr je pojednáno o postavení a přístupu poskytovatelů internetového připojení či užívaných technologií a otázka jejich činnosti a případné odpovědnosti za porušování autorských práv.

3.1 Autorské právo a internet

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 předmětem vlastnictví 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 při aplikaci a iniciovaly případné změny 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 při zachování současné podoby autorského práva je světová počítačová síť internet.

Internet je novým prostředím, kde dochází k legálnímu užívání autorských děl. Zároveň však představuje nový prostředek celosvětového a mnohdy i 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. [42] 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),[43] evropská směrnice o harmonizaci některých aspektů autorského práva a práv souvisejících v informační společnosti,[44] směrnice č. 2004/48/ES o dodržování práv duševního vlastnictví z roku 2004 nebo specifická národní úprava aspektů autorského práva v digitálním prostředí, např. Digital Millenium Copyright Act z roku 1998, který přijaly USA.

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, Digital Copyright Act 2010, a ve Francii, tzv. HADOPI zákon, které se výrazným způsobem snaží zasahovat do vztahů ve prospěch větší efektivnosti ochrany subjektů autorského práva. Na straně druhé jsou potom jednotliví uživatelé internetové sítě užívající síť k soukromým účelům, kteří obhajují co nejmenší omezování tohoto prostředí a zachování maximální dostupnosti a šíření veškerých informací v tomto prostředí. Oba postoje se

[42] Guadamuz, Andrés (2002) *Copyright in Cyberspace: Building Fences on the Internet*. [online] Alfa Redi, přístupné na adrese <http://ssrn.com/abstract=595362>, str. 5.

[43] 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).

[44] Směrnice 2001/29/ES z 22. května 2001 (dostupná na adrese <http://knihovna.nkp.cz/pdf/0104/nk0104273.pdf>) a směrnice 2004/48/ES z 29. dubna 2004 (dostupná na adrese <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:17:02:32004L0048:CS:PDF>).

zdají být problematické. Je jen těžko představitelné, že existují prostředky, které by mohly ochranu autorských práv zajistit plně. Navíc úzce související je též otázka nákladů na taková opatření, a kdo by je měl v konečném důsledku 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 legislativa i praxe se tudíž snaží najít střední cestu. Typickým příkladem je aktivita neziskové organizace ve Spojených Státech Amerických Creative Commons (CC).[45] 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.[46] 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 vizuální a audiovizuální díla), tedy díla vytvářená zejména z komerčních/ziskových důvodů.

Některé studie dokonce 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. [47] 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.[48]

---

[45] 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.

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

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

[48] Ibid. str. 5.

Tak například internet přinesl výkladové problémy pro současné pojetí autorského práva ve Velké Británii, kde se soudy musely vypořádat se samotnou povahou internetových stránek jako autorských děl. Digitální prostředí převádí veškeré informace do datové podoby, takže základní 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 hudebních či audiovizuálních. 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[49] či Ibcos v. Barclays Mercantile.[50] Současné pojetí je takové, že webová stránka je kompilace různých děl, která je podle CDPA považována za dílo literární povahy.[51]

V mezinárodním prostředí 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).

V neposlední řadě i právo evropské prostřednictvím směrnic uzpůsobilo některá pravidla a jejich výklad tak, aby byla lépe použitelná v prostředí internetové sítě. Tak například informační směrnice ve svém čl. 3 odst. 3 uvádí, že nedochází k vyčerpání práva na rozšiřování při prvním sdělení díla veřejnosti, stane-li se tak v nehmotné podobě (tedy např. prostřednictvím internetu). Pouze tedy vlastník hmotné rozmnoženiny má možnost převést vlastnictví k této rozmnožení na jiného, což však nabyvatel nehmotné rozmnoženiny (např. stažením programu online) nemůže.[52] Zavedena byla také možnost uzavřít licenční nevýhradní smlouvu i konkludentně (ve smyslu § 46 odst. 5 a 6 AZ), tudíž i provedením určitého úkonu. Typickým úkonem je například přijetí či stažení programu on-line a jeho nainstalování či použití.[53]

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

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

[51] Copyright, Designs and Patents Act 1988.

[52] 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.

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

V souvislosti s internetovou sítí se objevují také úvahy o krizi autorského práva v digitálním prostředí, a někteří dokonce předpovídají zánik institutu autorského práva tak, jak jej známe dnes. Odpovědi na tyto názory můžeme najít při zamyšlení se nad samotnou podstatou a důvody, které vedly ke vzniku a existenci tohoto právního institutu. Důvodů je hned několik, a to jak morální, ekonomické, stimulační i sociální povahy.

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 chrání až 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, proto se o nich někdy hovoří též jako o právech osobnostních. Tato kategorie práv nemůže 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 rozměru 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. Tudíž jej lze například zcizit či umožnit jeho užívání – v autorskoprávní terminologii prostřednictvím licenční smlouvy.

Dalším důvodem je i motivační nebo též stimulační, protože autorům se za jejich snahu dostane odměny v podobě finančních prostředků. Tímto způsobem lze též dosahovat dalších společenských a kulturních pokroků. Obdobně lze dosahovat pokroků technologických, k jehož stimulaci mimo jiné má působit patentové právo.

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.[54] Smyslem autorského práva například podle Ústavy USA je napomáhání v rozvoji vědy a užitého umění.[55] Jejich smyslem je tedy vyvážení veřejného zájmu, který je základním smyslem existence autorského práva, kterého

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

[55] Ústava USA, čl. 1, § 8 odst. 8.

je dosahováno odměňováním autorů do výše nutné k další kreativní činnosti. Jeho důsledkem je tedy v podstatě nalezení vyváženosti mezi veřejným zájmem a individuálními zájmy těch, kdo jsou vlastníky či komu svědčí práva k danému dílu.[56]

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 rozvoj doprovází také nový vývoj společnosti, která se globalizuje, urychluje a je v daleko větší míře závislá na přenosu informací v různých 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.

Dopady porušování autorského práva v prostředí internetu jsou zejména ekonomické ztráty z prosušování a obcházení práv autorských. Internet výrazně přispěl a zjednodušil zejména rozmnožování autorských děl a jejich sdílení, tj. poskytování rozmnoženin jinému internetovému uživateli. Způsobů, jak sdílet taková data je mnoho. Některé z nich jsou vyhledatelné a lze užít příslušná opatření k jejich omezení či zabránění, s jinými lze bojovat jen velmi obtížně. Zejména země, kde je zábavní a softwarový průmysl důležitou složkou národní ekonomiky, jsou nuceni přijímat opatření k obraně či alespoň omezení porušování těchto práv a tím i k zamezení dalších ekonomických důsledků, zejména ve formě daňových ztrát.

Z technického hlediska je nejčastěji internet vnímán jako tzv. webové stránky (WWW z anglického World Wide Web), které užívají protokol HTTP (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 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.[57] Takto dochází k nejzávažnější formě porušování autorských práv, protože za protiprávní poskytnutí autorských děl je přijímána úplata.

---

[56] 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.

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

Faktických způsobů porušování však je velmi mnoho. Tak například pro autory zvukových a audiovizuálních děl znamenal největší ohrožení vznik komprimovaných formátů (např. MP3 nebo AVI), díky kterým se významně zmenšila velikost kopie daného díla při zachování původní kvality. Navíc dnes v podstatě každý přehrávač umí tyto formáty bez omezení přehrávat. Takto malá data lze pak pomocí některého z výše uvedených protokolů velmi snadno poskytnout jinému uživateli.

Kromě těchto děl je od počátku problematické i poskytování počítačových programů. Rozlišují se různé způsoby porušování práv k nim. Dochází například k jejich rozmnožování koncovými uživateli, užívání spuštěním z pevných disků, prodávání kopií programů za programy tzv. originální (legální) nebo poskytnutí programu osobám, které si nezaplatili příslušné 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 zhlédnutí pouze pro osobní potřebu se za porušení autorských práv nepovažuje.

V podstatě denně dochází k porušování autorských práv také tzv. Copy-and-Paste metodou. Jde v podstatě o rozmnožování děl či jejich částí prostřednictvím počítačových příkazů (Copy – kopírovat a Paste – vložit). Kopírování autorských děl tímto způsobem na témže počítači, nejde-li o volná užití, 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.[58]

Jakým způsobem se tedy s novou realitou vyrovnává současná právní legislativa? Základní právní rámec je položen na mezinárodní úrovni. Předním dokumentem je Bernská úmluva z roku 1886, kterou spravuje Světovou organizací duševního vlastnictví (WIPO). Vedle ní patří mezi

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

důležité dokumenty i Všeobecná úmluva o autorském právu z roku 1952 z Ženevy a její současná revidovaná verze z Paříže 1971. Dále pak tzv. Římská úmluva z roku 1961,[59] Dohoda TRIPS o obchodních aspektech práv duševního vlastnictví z roku 1994, a z poslední doby též 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 nejvhodnější cesta úpravy pomocí nástrojů evropské legislativy, která by měla sjednotit právní úpravu tak, aby byl přístup členských států EU pokud možno jednotný. Mezi nejdůležitější přijaté dokumenty patří tzv. informační směrnice (č. 2001/29/ES o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti), resale směrnice (č. 2001/84/ES o právu na opětný prodej ve prospěch autora originálu uměleckého díla) a směrnice o dodržování práv duševního vlastnictví (č. 2004/48/ES). Do budoucna se zvažují návrhy upravující další výjimky jako například volné pořizování kopií na tomtéž pevném disku nebo pro vzdělávací účely.

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.[60]

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. V neposlední řadě bude též v případě vztahů s třetími zeměmi nutné aplikovat zákon č. 97/1963 Sb. o mezinárodním právu soukromém. Všechny tyto předpisy upřednostňují volbu rozhodného práva, ke které ve většině licenčních smluv zároveň dochází. Není-li tomu tak, běžně se vychází z toho, že se užije právo státu, ve kterém má ten, kdo poskytuje charakteristické plnění v daném smluvním vztahu, své

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

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

sídlo nebo bydliště, případně též ze zásady rozumného uspořádání vztahů. V případě mimosmluvních závazkových vztahů (např. z porušení práv duševního vlastnictví) se zásadně užije právo země, pro kterou je ochrana těchto práv uplatňována, případně kde k porušení došlo.

Základní právní rámec tedy existuje, přesto však stále dochází k častému porušování těchto práv. Největší problém totiž spočívá ve správě, vymáhání a postihování porušování autorských 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 přeshraničních. Provozovatelé i jednotlivé 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 a efektivnější 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 efektivitu a vymahatelnost 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 může být důvodem pro vymáhání státem, např. prostřednictvím k tomu určených orgánů. Hlavním předpokladem však je identifikace toho, kdo tato 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 jednotlivým účastníkům internetu nejblíže. Oni tak mají největší moc nad tím, co konkrétní uživatel na internetové síti provádí, nad přístupností služeb či internetových stránek, které jsou k porušování autorských práv nejčastěji užívány. Podle nové legislativy např. ve Francii či Velké Británii mají právě poskytovatelé internetového připojení či obdobných služeb povinnosti aktivně se účastnit efektivního vymáhání

autorských práv v případě, že jsou vyzvání nebo sami zjistí protiprávní činnost konkrétních uživatelů.

Vedle přijímání nových legislativních opatření na všech úrovních se však zdá, že nejvíce úspěšné je přizpůsobení se nové na výměně informací založené společnosti. Takovým přizpůsobením může být například velmi úspěšný obchodní model, který reprezentuje například společnost Apple. Pomocí programu iTunes a Apple Store, které jsou ve své podstatě legální formou využití technologie 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, a jiná díla přehrávat bez dalšího nedovolí. Tímto způsobem došlo k motivaci uživatelů, aby si například hudební díla raději zakoupili, než složitými technickými kroky systém produktů Apple obcházeli. Nutno však poznamenat, že jde spíše o ekonomicko-politický vývoj, než o opatření právní. Avšak právě tento přístup se zdá mít daleko pozitivnější výsledky než neustálé prohlubování a zdokonalování stávajících pravidel, které jsou založené zejména na hrozbách sankcemi.

Uvedené legislativní opatření aktivně zapojující poskytovatele internetového připojení, případně i jiných služeb informační společnosti, může být efektivní pouze tehdy, je-li zjistitelné a odhalitelné, kdo je původcem a provozovatelem technologií, sítí a webových stránek, které jsou k porušování autorských práv používány. Jedno z nejvíce rozšířených a užívaných technologií jsou peer-to-peer sítě. Blíže se tedy bude výklad zabývat právě jimi, a to zejména z pohledu autorskoprávní legislativy.

3.2 Peer-to-peer 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 svojí decentralizovanou strukturou. Každý zúčastněný počítač se chová zároveň jako server i klient. Pomocí vyhledávacího programu se vyhledají v podstatě pouze adresy jednotlivých počítačů, a uživatelé se pak připojují přímo mezi sebou. Hlavními výhodami je již zmíněná stabilita a zároveň není ni třeba uchovávat nadměrná množství dat na pevných discích serverů, což mimo jiné šetří i značné množství finančních nákladů. Toto je základní model, který však může být různými způsoby modifikován.

Při analyzování právních důsledků je třeba si povšimnout struktury dané konkrétní sítě. Rozlišují se sítě centralizované a decentralizované. V centralizovaných probíhá přenos přes centrální sever. Jedna z prvních takových sítí byla síť Napster spravovaná z Kalifornie. Problémem bylo, že společnost Napster však udržovala pouze server s vyhledávacím software, který pak poskytoval jednotlivým uživatelům informace o tom, kdo a na jaké adrese má vyhledávaná data.[61] Decentralizované sítě, které jsou nejvíce vystižené popisem z úvodu této kapitoly, žádný centrální server nepotřebují a použitím k tomu určeného programu je zajištěno i samotné vyhledávání. Takovou sítí je například Gnutella. Vždy existuje i střední cesta, využívající některé sdílené spojovací místa (huby). Takové jsou například sítě jako Grokster nebo KazaA. Obdobnou technologií je i využívání tzv. torrent sítí (např. BitTorrent). Zvláštností těchto sítí je, že při stahování požadovaného souboru (resp. jeho částí) dochází zároveň ke zpřístupňování těchto 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 více než 60 % celkově přenesených dat v síti Internet.[62]

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.[63] Proto je veřejný zájem a volný přístup k dílům veřejností 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

[61] 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.

[62] 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.

[63] Ibid. Str. 1025.

osobám. Tak například práva k představení děl hudebních typicky náleží skladateli a tomu, kdo dílo zveřejnil, zatímco práva reprodukce jsou vlastněna nahrávacími společnostmi.[64]

Z výše uvedených důvodů je tedy důležité rozlišovat jednotlivé subjekty a jejich případnou odpovědnost. Hlavními účastníky jsou klienti, kteří stahují informaci od distributorů, tedy těch, kdo své data sdílejí a umožňují tak jejich rozmnožování. Přitom při použití technologie P2P je jedna osoba často v postavení obojím zároveň. Tyto činnosti jsou nemyslitelné bez dalších subjektů, zejména těch, kdo danou síť provozují, vytváří vyhledávací programy, popř. provozují servery nebo huby. O nich se hovoří jako o poskytovatelích. V neposlední řadě mohou hrát důležitou roli také poskytovatelé internetového připojení jako takového, bez nichž by k přenosu vůbec dojít nemohlo.

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 pouze poskytnutím seznamu názvů souborů nacházejících se na počítačích uživatelů fungujících jako servery. Tyto názvy nejsou vytvořeny vlastníky autorských práv, na rozdíl od jejich případného obsahu, třebaže většinou obsahují název daného díla. Stažení souboru z P2P sítě však již znamená v podstatě vytváření kopie (rozmnoženiny) 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.[65] Zejména díky dopadu na trh byla úspěšná žaloba proti činnosti společnosti Napster, jelikož tato činnost snížila počet prodaných CD mezi uživateli (vysokoškolskými studenty). Navíc bylo argumentováno tím, že se vytváří omezení možnosti autorů a nahrávacích společností vstoupit na trh s digitální podobou hudby, tudíž takové užití

[64] 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).

[65] 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.

soud nepodřadil pod výjimku fair use.[66] 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 porušování autorských práv. K tomuto závěru dospívá valná většina uživatelů, avšak ani tento není zcela jednoznačný. V žádném případě tomu tak nebude, pokud nejsou naplněny obecné ustanovení § 29 AZ. Z nich mimo jiné vyplývá, že výjimky se týkají pouze zveřejněných děl. Dále ani nelze výjimku aplikovat, není-li naplněna generální podmínka obsažená též v § 30 odst. 1 AZ, totiž v případě, že motivem je dosažení hospodářského či obchodního prospěchu, a to jak přímého tak nepřímého. Kromě toho i vědomí uživatele, že dané dílo pochází z nepoctivých a protiprávních zdrojů může být důvodem, proč nelze jeho počínání považovat za v souladu se zákonem.

Dalšími subjekty jsou distributoři. To jsou ti, kdo provozují zařízení zastávající v síti místo serverů. Jinými slovy, kdo poskytují například autorská díla ostatním uživatelům například prostřednictvím umožnění přístupu ke svým počítačům a jejich pevným diskům. Tito ve své podstatě vždy porušují práva autorů či jiných osob ve smyslu uvedeném 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 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. Toto pojetí vychází jak ze směrnice o elektronickém obchodu, tak z našeho zákona o některých službách informační

[66] 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).

společnosti.[67] Dle vývoje v posledních letech však to jsou právě oni, kdo jsou aktivně zapojováni do procesu předcházení a vymáhání autorských práv.

Předmětem právní regulace a ochrany jsou autorská díla ve smyslu § 2 AZ. Z pohledu majetkových práv je pak zásadním právo dílo užít. Jde o legislativní zkratku, kterou dle § 12 odst. 4 AZ je myšleno právo dílo rozmnožovat, rozšiřovat, pronajímat, půjčovat, vystavovat a sdělovat dílo veřejnosti (výčet je demonstrativní, jak uvádí odst. 5). Zásadně dílo užít je právem autora, ačkoli jednotliví složky se mohou lišit podle druhu autorského díla.

Na síti P2P dochází k porušování práva dílo užít z různých hledisek. Nejčastějším způsobem je 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 činnosti je totiž vytvoření rozmnoženiny díla, a to včetně tzv. technických rozmnoženin (např. převedením do jiného digitálního 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.[68] Za sdělování veřejnosti zákon v § 18 odst. 2 považuje i zpřístupňování na místě a v čase podle vlastní volby (tzv. on demand), zejména počítačovou nebo obdobnou sítí. Odst. 4 téhož paragrafu navíc dodává, že sdělováním díla veřejnosti nedochází k vyčerpání tohoto práva. To tedy znamená, že na rozdíl od rozšiřování hmotné podoby díla, kdy jeho prvním prodejem či převodem je toto právo vyčerpáno, a lze jej tedy obdobně jako věc následně také převést na další osobu, v elektronické podobě tomu tak není. 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

[67] § 3 až 6 zákona č. 480/2004 Sb.

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

dochází k pouhému provozování zařízení umožňujícího nebo zajišťujícího sdělování, nikoli k sdělování jako takovému.[69]

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 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.

Z uvedeného vyplývá, že ve své podstatě P2P sítě nejsou již zcela novým jevem a lze je podřadit a klasifikovat podle existující legislativy. Avšak obavy vzbuzuje distribuční kapacita této technologie, která se vymyká kontrole vlastníků práv k přenášenému obsahu. Ve snaze znovuzískat kontrolu, nebo jí alespoň zvýšit, dochází k zapojování a zavádění sekundárních

[69] § 18 odst. 3 AZ.

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 záleží v tom, že velkých porušovatelů již není zapotřebí. Každý jednotlivec v síti P2P může být zároveň serverem i klientem, tudíž zde jsou zapojeni "pouze" uživatelé malého významu a vést řízení proti každému jednotlivému uživateli je v praxi neproveditelné.

Co tedy lze s tímto faktem udělat? Vlastníci autorských práv potřebují nějaký vyšší subjekt, na kterém 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.[70] 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 která podnikne kroky k umožnění 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.[71] Zda takto široké pojetí je ospravedlnitelné 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 odpovědný je každý, kdo porušování autorských práv „autorizuje", jak uvádí čl. 101(1A).[72] Přitom za hlediska autorizace se považuje, zda tato osoba měla moc k tomu, aby znemožnila porušení autorského práva v

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

[71] 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.

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

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. [73] 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 pak jeví jako neúčelné a nepřijatelné.

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 nejsou zpoplatňovány (tak se to například děje u prázdných médií jako CD, DVD nebo MP3 přehrávačů, někde i u osobních počítačů, resp. jejich úložných zařízení typu pevných či přenosných disků).[74]

Vedle toho i širší užití tzv. DRM (z anglického digital rights management) může být účelné. 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 internetu je nezbytným předpokladem účinné úpravy a ochrany autorských práv v digitálním prostředí.[75] Zda není tento názor příliš přeceňující DRM, s tím lze polemizovat.

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

[74] 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.

[75] 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.

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.

3.3 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 zapojením těch, kdo fakticky hrají nejdůležitější roli v existenci a používání této sítě. Jde tedy zejména o subjekty, které zajišťují připojení k síti, a dále i osoby, které v rámci sítě poskytují své služby (například poskytují služby 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 též SEO) [76] ve svém článku 12 vylučuje odpovědnost poskytovatele služby, pokud nehraje určitou aktivní roli v průběhu procesu umístění a přenosu informací. Aktivní role znamená, že je původcem přenosu, volí příjemce přenášené informace či volí nebo mění 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

[76] 2000/31/ES směrnice o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu, 8. června 2000.

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.[77] 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.

Obdobná 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 takové 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 meziukládaných, 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 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). Právě otázka rozhodujícího vlivu byla v minulosti poměrně diskutována a stala se jakýmsi výkladovým můstkem od stávající legislativy k dovození odpovědnosti těchto osob v prvních zahraničních případech.

Uvedené pojetí odráží poměrně volné a neodpovědné postavení poskytovatelů služeb informační společnosti, které více či méně může být také odrazem jejich silného ekonomického postavení. To se na druhou stranu nelíbí osobám, kdo se snaží efektivně domáhat nápravy

[77] Čl. 14 odst. 1 SEO.

v případě porušení jeho subjektivních práv. V tomto případě majitelé práv autorských a sním souvisejících, zejména pak zástupci zábavního průmyslu se snaží prosadit koncept, aby způsob boje proti protiprávnímu jednání uživatelů internetu byl co možná nejúčinnější. Proto v některých státech, kde je jejich ekonomická pozice nejvýznamnější, přijaly poměrně zásadní právní opatření. V posledních letech hlavně ve Velké Británii a Francii byly přijaty zákonné úpravy aktivně zapojující ISPs do procesu ochrany před protiprávními aktivitami uživatelů internetu. Z pohledu regulatorně-metodologického jsou tato právní opatření nejúčinnější, jelikož odráží již zmíněnou down-up metodu. Zaměřují se totiž na ty, kdo mohou nejefektivněji přispět k dodržování zákona uživateli internetové sítě, tedy poskytovatelé příslušných služeb. Tito mají k uživatelům nejblíže a mohou se tak aktivně podílet na prosazování práva v elektronickém světě.

3.3.1 Digital Economy Act 2010

V roce 2010 byl na britských ostrovech přijat nový zákon, Digital Economy Act (zkráceně DEA) který má přispět k efektivní regulaci internetového prostředí. Ve skutečnosti je výsledkem lobbistických snah ze strany těch, kdo neustále zaznamenávají obrovské finanční úniky způsobené zneužíváním a obcházením práv k duševnímu vlastnictví, zejména práv autorských, prostřednictvím internetové sítě. Úniky hudebního a filmového průmyslu jsou mimo jiné též významnými položkami v příjmech tamního státního rozpočtu. Proto se vláda rozhodla chránit tyto zájmy a uvalit povinnosti na některé zúčastněné subjekty. Opět tedy legislativa stála před stejným problémem, jak efektivně prosadit právní pravidla za současného zachování co největší globální volnosti internetové sítě.

Mezi uživatelem a internetem samotným stojí vždy subjekt poskytovatel dané služby informační společnosti, anglicky nazývaný Internet Service Provider (zkráceně ISP). Právě regulace a uvalení povinností na tyto subjekty může být poměrně efektivní cestou. DEA kromě jiného reguluje činnosti ISPs a to i ve vztahu k porušování práv k duševnímu vlastnictví. Podstatou nového konceptu je zavedení sekundární odpovědnosti ISPs 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.

Zásadně odpovědnost za vysledování porušování práv leží nadále na těch, jimž práva svědčí, tedy majitelům práv k duševnímu vlastnictví. Oni proto musí monitorovat internetový provoz a vyhledávat, jaký počítač, stránka či technologie bývá využívána ke sdílení chráněných

materiálů či jinému způsobu porušování autorských práv. Podle DEA pak mají možnost do jednoho měsíce zaslat oznámení poskytovateli internetového připojení o tom, že určité osoby či IP adresy bývají užívány k nelegální činnosti.[78] ISP má poté povinnost vypracovat pro majitele porušovaných práv seznam těch uživatelů, kdo jsou podezřelí z jejich porušování. Zároveň mají povinnost písemně upozornit uživatele, že jeho počítač je používán k protiprávní činnosti a vyzvat jej k nápravě. Dále je poskytovatel služeb povinen spolupracovat s majiteli práv tím, že poskytne evidenční podklady o tom, že k porušování autorských práv dochází. Pokud uživatel přesto v takové činnosti pokračuje, ISP jsou povinni podniknout i opatření technického charakteru. Nejprve má dojít ke snížení rychlosti a kapacity internetového připojení daného uživatele, případně též k zamezení užívání jeho připojení k určitým službám či protokolům. Pokud ani toto nepostačí, pak může být daný uživatel odpojen od internetové sítě zcela. V případě nepodniknutí žádných technických opatření, může být ISP vystaven poměrně vysokým pokutám až do výše 250 000 britských liber. Problematické jsou náklady takových technických opatření, jelikož samozřejmě ISPs nesouhlasí s tím, aby ležely na nich. Zákon počítá s možností náhrady těchto nákladů z veřejných rozpočtů, ovšem implementační legislativa prozatím k tomuto bodu vydána nebyla. Mimo jiné i proto účinnost tohoto zákona je oddalována a nyní je předpokládána nejdříve v roce 2012.

Zejména ze strany největších poskytovatelů internetových služeb (např. Google, Facebook, Ebay či Yahoo) a samozřejmě i ze strany samotných uživatelů se zvedla poměrně značná kritika, která je založena na několika argumentech.

Na základě této úpravy je ISP dána značná pravomoc (i povinnost) přímo zasahovat do soukromí uživatelů, shromažďovat údaje o nich. Majitelé autorských práv si mohou vyžádat od ISP vyžádat report například o stahování provedených jednotlivými uživateli. Navíc k daným opatřením stačí jen minimální důkazy a odůvodnění. 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.[79] Další problém je také v tom, že pomocí zablokování některých protokolů může být způsobena škoda tím, že dojde k zamezení služeb, kterých se porušování autorských práv vůbec netýká. Navíc obecné zamezení pro všechny uživatele by omezovalo práva ostatních bez ohledu na to, zda se oni kdykoli dopustili

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

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

protiprávního jednání. ISPs sami tvrdí, že nejsou těmi, kdo plně kontrolují a mají kontrolovat internet jako takový. Předmětem jejich podnikání 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 jim jeví jako nespravedlivé a přesahující předmět jejich podnikání. Argumentují, že 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 neúměrně vysoké. Vzhledem k úpravě mezinárodní, zejména evropské, se pak 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. Právě OFCOM se vyjádřil k několika problémům, které má v úmyslu výkladem v praxi zajistit. Jednak má být označení a další kroky vůči konkrétnímu uživateli podloženo dostatečnými důkazy. Kromě toho má být zajištěno i odvolání k nezávislému orgánu. Přičemž daná pravidla by zpočátku měla platit pouze pro velká ISPs, tedy s min. 400.000 uživateli, jelikož podle dostupných informací 96 % těch, kdo porušují autorská práva, jsou právě uživatelé služeb těchto velkých poskytovatelů.[80]

3.3.2 Zákon HADOPI

Druhou výraznou zemí, kde rovněž zábavní průmysl má důležité postavení i z hlediska veřejného zájmu je Francie. V roce 2009 proto přijala tzv. HADOPI zákon,[81] který zavedl nový postup, jak zasáhnout proti uživatelům podílejícím se na porušování či obcházení autorských práv prostřednictvím internetové sítě. Označení zákona 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 uplatňuje nápravné prostředky v této oblasti. V čele nově vytvořené instituce je devítičlenné představenstvo, jehož tři členové jmenuje vláda,

[80] OFCOM (2010) *Online Infringement of Copyright and the Digital Economy Act 2010. Draft Initial Obligations Code.* [online] <http://stakeholders.ofcom.org.uk/binaries/consultations/copyright-infringement/summary/condoc.pdf>.

[81] 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.

dva legislativní orgán, tři soudní orgány a jeden je jmenován institucí 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 tzv. piráty najít jiné cesty, podle kterých není jejich identifikace a IP adresa téměř dohledatelná.[82]

Proces aplikace a implementace daného zákona je však stále v začátcích. Hovoří se například o zavedení povinnosti na vyžádání instalovat zvláštní spyware, což je program, který sleduje veškeré činnosti na konkrétním počítači, a tímto způsobem monitorovat a zabránit protiprávnímu užívání daného přístroje. Zvažuje se i jeho povinné instalování do prodávaných routerů či užívaných antivirových a jiných zabezpečovacích programů. Výsledkem má být zajištěny důkazy o způsobu užívání daného přístroje. Problém však je, že jen těžko lze tímto způsobem zjistit, kdo skutečně tento přístroj k protiprávní činnosti používá, zda jeho vlastník, nebo například soused užívající jeho domácí bezdrátovou síť či přímo daný počítač.[83] Takové

[82] PC Magazine Online (2010) *"French Anti-Piracy Law Actually Increases Piracy."* [online] 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>.

[83] Roettgers., J. (2010) *Hadopi Gone Wild: France Plans Spyware for Three Strikes*. [online] dostupné na adrese <http://gigaom.com/video/hadopi-gone-wild-france-plans-spyware-for-three-strikes/>.

nástroje jsou však trnem v oku ochráncům soukromí a základních lidských práv, jelikož tímto krokem by došlo k faktickému sledování a odposlouchávání každého uživatele, což je podle mnoha nepřípustné.[84] Proto nově má být koncept těchto programů být čistě dobrovolný a bude záležet na každém uživateli, zda jej vypne či nikoli. K tomu však nutno poznamenat, že tím se efektivita celého opatření velmi výrazně snižuje.

3.4 Institut autorských práv on-line a jeho perspektivy

Institut autorského práva se v důsledku internetové sítě stal velmi diskutovanou otázkou. Vznik nové technologie usnadňující šíření a přístup k autorským dílům, obdobně jako dříve vznik videorekordérů či nahrávacích audio zařízení, je důvodem pro revizi a přizpůsobení stávajících autorskoprávních pravidel. Význam internetu je natolik zásadní, že dokonce extrémní názory předpovídají zánik autorských práv jako takových. Jejich existence je však fundamentální pro další kulturní, společenský i ekonomický rozvoj a vzdělání naší společnosti. Autorská práva jsou totiž motivačním prostředkem pro další práci a snahy jednotlivých autorů, kteří za svou práci legitimně očekávají odměnu. V případě autorských děl zábavního průmyslu, tedy zejména hudebních a audiovizuálních navíc samotná produkce je natolik nákladná, že bez příslušné ochrany a odměn by nebyla ani představitelná. Proto je i v zájmu veřejném, aby autorskoprávní ochrana nadále existovala a zdokonalovala se.

V současném vývoji bude zásadní nalézt vyvážení mezi zájmy těch, komu dosavadní legislativa poskytuje autorskoprávní ochranu, a zájmy veřejnosti. Ty jsou dnes již tradičně vyjádřeny prostřednictvím výjimek, v naší legislativě označovaných jako volná užití a zákonné licence, v prostředí angloamerickém také jako doktrína fair use. Jejich rámec je mimo jiné stanoven již na evropské úrovni, např. směrnicí 2001/29/ES o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti. Zapracování výjimek podle jejího čl. 5 odst. 2 do vnitrostátní legislativy je však ponecháno na vůli jednotlivých národních orgánů. Ta se však v jednotlivých státech velmi liší, jak vyplývá ze zprávy Evropské komise z roku 2007.[85] Například výjimka pro soukromé účely fyzických osob je velmi omezeně provedena ve Velké Británii. I z tohoto důvodu probíhají nyní konzultace na úrovni Evropské komise, zda nenastal čas na větší unifikaci a zavedení hlavních výjimek jako mandatorních. Na

[84] KCRG News (2011) *Hadopi: the first registered letters will be leaving soon*. [online] přístupné na adrese <http://kcrg.biz/2011/01/hadopi-the-first-registered-letters-will-be-leaving-soon/>.

[85] Evropská komise (2007) *Report to the Council, the European Parliament and the Economic and Social Committee on the application of Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society*. [online] přístupné na adrese <http://ec.europa.eu/internal_market/copyright/docs/copyright-infso/application-report_en.pdf>.

druhé straně však stojí ti, jimž práva autorská a související svědčí. Jejich zájmem se spíše ubírá směrem k maximální ochraně stávajících práv, který se odráží například v zapojování poskytovatelů internetových připojení a služeb do procesu ochrany autorských práv.

Jak již bylo popsáno, současný trend autorskoprávní legislativy je zejména v západních zemích poměrně ochranářský vůči majitelům autorských práv. Autoři de Beer a Clemmer popisují vývoj postavení ISPs, který se z původního pasivně-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.[86] 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 snadnější vymahatelnosti jiných práv v internetovém prostředí. Dochází také k zesílení již tak poměrně dominantního postavení těch, kdo poskytují služby informační společnosti, jelikož zejména na nich úspěšné vymáhání těchto práv záleží. 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. Tento trend proto 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.[87] Obdobný přístup byl přijat také na Novém Zélandě v roce 2008 a je účinný od února roku 2009.[88] Někteří vidí v obdobných úpravách na území EHS také rozpor s článkem 15 směrnice o elektronickém obchodu, který ukládá členským státům, aby neuvalovali obecnou povinnost monitorovat informace, které přenáší nebo hostují na svých serverech pro uživatele, na poskytovatele těchto služeb.[89] Například francouzské soudy však odůvodňují soulad tím, že nařízení blokovat a filtrovat obsah pomocí technologických prostředků není monitorováním, ale spíše prostředkem k

[86] 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.

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

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

[89] Směrnice EP a Rady 2000/31/ES ze dne 8. Června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu).

tomu, aby se plošnému monitorování poskytovatelé mohli vyhnout.[90] Obdobné pojetí a návrh na přijetí příslušné legislativy podaly i organizace zastupující kanadské autory vizuálních děl, kteří mimo jiné navrhují, aby byli právě ISPs uznány za solidárně odpovědné společně s porušovateli práv autorských. Možností liberace by mělo být leda prokázání, že přijaly veškeré rozumně dostupné opatření a prostředky k zabránění porušování autorských práv prostřednictvím služeb, které poskytují. Přitom i finančních náklady by měli nést oni a zahrnout jejich náhrady do poplatků za služby, které poskytují.[91] Naopak soudy v USA existenci takovýchto povinností poskytovatelů služeb odmítají.[92] 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 například v Číně, ačkoli tam je to spíše z politických důvodů.[93]

Vystává tedy otázka vývoje v budoucnosti a prostředků, které mohou k efektivnímu zakotvení autorských práv a jejich aplikace vést.

Vzhledem k již uvedenému je třeba, aby docházelo k další unifikaci v mezinárodním měřítku. Zejména systém výjimek by měl vycházet z obdobného základu, a neměl by se lišit v poměrně zásadních oblastech. V prostředí evropském by například výjimky pro účely čistě soukromé či vzdělávací měly být zakotveny jako mandatorní.

Základním prostředkem umožnění užití autorských děl, nejde-li o výjimky, je poskytnutí určitých práv formou smluvní, tedy licencí. Právě unifikované licenční prostředky jsou jedním z nástrojů ke zvýšení efektivity právní ochrany. Jedním z návrhů Evropské komise je i rozšíření tzv. kolektivních licencí pro určité způsoby užití autorských děl online, které by pokrývali území všech členských států EU. Za určitou formu unifikovaného licencování, které je však podstatě ochranou morálních aspektům autorského práva, jsou již zmíněné licenční smlouvy Creative Commons. Zejména však pro účely komerční je třeba systém příhraniční správy a licencování autorských práv co nejvíce zjednodušit. Na druhou stranu musí být odlišný přístup zachován

[90] 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>.

[91] CARFAC a RAAV (2006) *Proposals for the improvement of the Copyright Act to Favor of the Amelioration of the Socioeconomic Conditions of Canadian Visual artists.* [online] přístupné na adrese <www.raav.org/pls/htmldb/adu?p=528726109203373380>.

[92] Ibid. str. 29.

[93] Ibid. str. 33.

k odlišným druhům autorských děl, jelikož například u hudebních či audiovizuálních děl jsou majiteli různých práv různé osoby, mezi které je následně nutné vhodně rozdělit i finanční prostředky.[94]

Z pohledu globálního je také důležitý systém správy autorských práv. Zatímco některá práva jsou spravována kolektivně, jiná takovouto formu nemají. Možným řešením může být i vznik nových kolektivních správců, jejichž činnost by byla cíleně zaměřena na oblast užití a prosazování autorských práv v prostředí internetovém. V některých státech je systém kolektivních správců postaven na monopolním konceptu, což není úplně šťastné řešení. Právě soutěž, ať již hospodářská či jiná je motivem pro zvyšování kvality služeb, které jsou i ze strany kolektivních správců očekávány. Zároveň úzká mezinárodní spolupráce mezi kolektivními správci je v prostředí, které svojí povahou je zejména mezinárodním, velmi důležitá.[95] Je otázkou, zda by nebylo vhodné v tomto ohledu zavést i alternativní způsob správu, například vedle správy kolektivní, která by mohla v důsledku zjednodušit i licenční nástroje pro území více států. Současná situace je totiž taková, že kromě jiného je třeba vždy individuálně vyjednat i podmínky s každým jednotlivým národním kolektivním správcem autorských práv a práv souvisejících. O takové metodě se někdy hovoří také jako o metodě „one-stop-shop".

Dalším prostředkem, jak dosáhnout vyšší efektivity je již zmíněný a velmi diskutovaný koncept aktivního zapojení poskytovatelů internetu a souvisejících služeb. V tomto se však velmi odlišuje přístup jednotlivých členských zemí EU. Je poměrně zajímavé, že státy s již tradičně velmi silným důrazem na lidská práva a základní svobody se jejich ochrany poměrně snadno vzdávají. Praktické otázky však jak v UK tak Francii činí mnoho problémů a jedině čas ukáže, zda tato koncepce může mít naději na úspěch. V tomto ohledu jsou samozřejmě zájmy protichůdné, jelikož majitelé práv autorských a souvisejících by rádi přenesli odpovědnost i na tyto subjekty, protože by pro ně mimo jiné bylo také jednodušší dožadovat se nápravy a odpovědnosti na nich nežli na jednotlivých ISPs. To se však z druhé strany jeví jako velmi nespravedlivé pro ISPs. Z pohledu metodologického však aktivnější zapojení těchto subjektů, kteří jsou ve velmi strategických pozicích, je nutným a nevyhnutelným nástrojem.

---

[94] Evropská komise (2009) *Creative Content in a European Digital Single Market: Challenges for the Future.* 22. října 2009. [online] přístupné na adrese <http://ec.europa.eu/internal_market/consultations/docs/2009/content_online/reflection_paper%20web_en.pdf>.

[95] K tomu blíže viz. Doporučení komise ze dne 18.5.2005 o kolektivní přeshraniční správě autroského práva a práv s ním souvisejících pro zákonné on-line hudební služby. Přístupné též na adrese <http://www.mkcr.cz/assets/autorske-pravo/eu-a-autorske-pravo/07-02753-Doporu_en__EK_o_kolektivn__p_eshrani_n__spr_v__AP_a_pr_v_s_n_m_souvisej_c_ch_pro_z_konn__on-line_hudebn__slu_by__2005_737_ES__1.pdf>.

V souvislosti se zapojením ISPs se objevují i názory na možné hledání alternativních cest odměňování majitelů autorských práv, například závislých na objemu stažených (download) a odeslaných (upload) dat. Koncept by byl obdobný náhradám za prázdná úložná média. Na druhou stranu však se zdá být problematické, jak by obdobný systém odlišil objem komunikovaných dat užívaných v souvislosti s díly podléhajícími autorskoprávní ochraně. Zpoplatnit totiž veškerá data může být v konkrétních případech velmi nespravedlivé.

Internet je kromě jiného také velkou příležitostí a může být využit i majiteli autorských práv jako nástroj nových obchodních modelů. Velmi úspěšným se stalo využívání P2P technologií společností Apple či Nokia, které tímto způsobem snadno dovolují svým zákazníkům prostřednictvím svých elektronických přístrojů zakoupit za velmi příznivé ceny požadovaná autorská díla typu hudebních skladeb či počítačových programů. Pro další rozvoj obdobných iniciativ je však zapotřebí zjednodušení a rozvoj licenčních i finančních mechanismů. Těmi mohou být již zmíněný rozvoj a spolupráce kolektivních či alternativních správců, dále též spolupráce s ISPs například ve formě provozování obchodních modelů založených třeba na poplatcích za registraci, což je pro uživatele přijatelnější než platit poplatky za každé jednotlivé dílo.

Zásadní obecnou otázkou budoucnosti, jak ji nastínil i předseda WIPO Dr. Francis Gurry v lednu 2011 na konferenci v Sydney tedy je, jak zpřístupnit kulturní díla za cenu, kterou si může každý dovolit, a co největšímu počtu uživatelů, při současném ekonomickém odměnění autorů, výkonných umělců a společností podílejících se na tvorbě autorských děl.[96] Na jedné straně tedy musí být zajištěna přístupnost děl, avšak zároveň kontrola nad jejich distribucí. Internet výrazně přispěl k vysoké dostupnosti děl a tím i zvýhodnil spotřebitele oproti těm, kdo autorská díla produkují. Nyní je tedy nutné přijmout opatření, které opět najde správné vyvážení se zájmy majitelů autorských a souvisejících práv tak, aby bylo možné zajistit jim spravedlivé ekonomické odměny za jejich práci. Kromě již uvedených možností je zároveň nutné, aby z pohledu konečného uživatele byly zachovány základní podmínky. Těmi jsou zejména jednoduchý přístup k dílům a dostupná cena. Každý systém, který nebude tyto podmínky respektovat je odsouzen k neúspěchu, jelikož jednotlivci budou vždy hledat způsoby jak jej obejít.

[96] http://www.apo.org.au/video/wipo-director-general-addresses-future-copyright.

4. Právní úprava doménových jmen

4.1 Obecně o doménových jménech

Z obecného hlediska jsou doménová jména (dále i domény) základním orientačním vodítkem uživatelů internetu, jejímž prostřednictvím jsou vyhledávány požadované informace. Bez takového systému by nebylo v podstatě vůbec možné se v nezměrném množství internetových stránek a informací v nich obsažených vůbec orientovat. Každé takové místo v síti má tedy jedinečné označení, obdobně jako ve fyzickém světě například číslo popisné u budov. Co je však odlišné, je fakt, že takový jedinečný název své internetové stránky si může každý zvolit sám. Přesto tato volnost není neomezená. Může totiž a také tomu tak v mnoha případech bývá dojít ke konfliktu s jinými právními instituty, např. ochranou obchodní firmy či ochranné známky. Mimo jiné totiž hlavním motivem při výběru názvu doménového jména je hledisko ekonomické. Čím více potenciálních klientů bude stránky navštěvovat, tím větší je pravděpodobnost uzavřených obchodů. Obchodníci proto volí co nejjednodušší a nejvýstižnější názvy, pokud možno vycházející z jejich vlastního názvu, obchodní firmy či oblasti, ve které provozují svoji činnost.

Pokud jde o sytém, jakým doménová jména fungují, nejde o nic jiného než systém označení určitého místa (tzv. DNS systém, z anglického the Domain Name System), počítače, v síti, který překládá skutečné číselné označení daného místa (tzv. IP adresy, z anglického the Internet Protocol address). Jeho smyslem je jednodušší a přehlednější orientace a zapamatovatelnost daného místa, nebo webové stránky, zjednodušeně řečeno. Po jeho zadání do internetového prohlížeče (např. Internet Exploreru) dojde k automatickému přeložení do systému číselného a vyhledání požadovaného místa v síti. DNS systém je uspořádán hierarchicky do tří kategorií (nejvyšší, druhé a třetí úrovně). Nejvyšší, tzv. Top Level, doménová jména jsou dvojí druhu: obecná (obsahující třípísmenná označení (například .com, .net a .org), tzv. gTLDs a ta, která jsou typická pro označení určitého státu (například .cz, .fr, nebo .de), tzv. ccTLDs.[97] Označení druhé úrovně tvoří většinou hlavní název doménového jména (například „google“). Pokud obsahuje doména i další označení, tato jsou úrovně třetí (např. v adrese www.ip.mpg.de je označení „ip“ doménou třetí úrovně). Některé domény nejvyšší úrovně jsou omezeny a nemohou

[97] Např. nezisková společnost EURid pro registraci domény .eu nebo zájmové sdružení právnických osob CZ.NIC pro registraci domén .cz.

být registrovány každým. Takovou je například obecná doména .gov, která je vyhrazena výhradně vládě USA. [98]

Subjekt, který registruje doménová jména nejvyšší úrovně, se nazývá registrem. Ten mimo jiné ukládá a udržuje aktuální seznam registrovaných domén a je odpovědný za poskytování licencí komerčním registrátorům, kteří poskytují registrační služby při registraci domén druhé úrovně konečným uživatelům, resp. těm, kdo mají zájem o registrací vlastní domény. Na vrcholu této pyramidy registrátorů je již v předchozích kapitolách zmíněná instituce ICANN (z anglického the Internet Corporation for Assigned Names and Numbers).[99] Jde o neziskovou organizaci kromě jiného odpovídající za údržbu obecných domén nejvyšší úrovně na základě exkluzivní smlouvy s vládou USA. ICANN poté delegoval administraci obecných jmen národního charakteru na vlády, resp. registrátory, jednotlivých států.[100]

V neposlední řadě nelze nezmínit ani zvláštní skupinou uživatelů internetu registrujících domény tzv. cybersquatters. Ti zejména v průběhu 90. let přišli na veliký ekonomický potenciál internetové sítě a zaregistrovali si mnoho domén odpovídajících obchodním jménům významných institucí a obchodní společností, nebo jejich obchodním známkám z důvodů čistě spekulativních. Následně se je pokoušeli prodávat skutečným vlastníkům ochranných známek či jmen v nich obsažených. Na tomto základě došlo k prvním významným sporům, kdy společnosti typu Marks&Spencer se domáhaly přiznání práv k doménám s názvy svých obchodních firem z různých titulů. Existují i další způsoby této činnosti, např. inkorporace známých názvů či ochranných známek do svých domén tak, aby tím došlo k nalákání uživatelů internetu na své webové stránky. Další takovou činností je také pasivní registrace domén, kdy cílem není ani zisk příjmů na základě dobrého jména či pověsti jiné osoby, ani z prodeje této domény. Cílem není ani provozování webových stránek pod takovým názvem. Může tedy v daném případě jít například o omezování konkurence podnikající například ve stejném odvětví.

Stejně jako u jiných ekonomicky významných institutů i v případě doménových jmen vyvstává mnoho problémů a sporů. Ať již pro funkci propagační, vyhledávací, informační či soutěžní, pro ekonomické subjekty může být doménové jméno obdobně důležité, jako např. obchodní firma či ochranná známka. Jaký je jejich vzájemný vztah a jakými způsoby se případné spory či kolize řeší, bude předmětem samostatné části této kapitoly.

---

[98] Efroni., Z. () *Names as Domains, Names as Marks: Issues concerning the Interface between Internet Domain Names and Trademark rights.* [online] přístupné na adrese <http://ssrn.com/abstract=15NamesasDomains> str. 3 a 4.

[99] Raban., P. Moravcová., M. a kol. (2006) *.eu domain name .eu doména.*Praha: C. H. Beck, str. 32.
[100] Efroni (2007) str. 3 a 4.

4.2 Vymezení pojmu z právního hlediska

Doménové jméno z hlediska své povahy je sledem znaků, které jednoznačně identifikují jedinečné místo v internetové síti. Veškerá práva k němu jsou založena na výhradně smluvní bázi, na základě smlouvy o registraci doménového jména. Na druhé straně však právní postavení je determinováno také právním postavením třetích osob, například držitelů ochranných známek či obchodních firem, s jejichž právy může být právo registrovanému doménovému jménu v poměru antagonistickém.[101] Pojem doménové jméno není podle české právní úpravy legálně definován. Právní kategorie, do které se doménová jména nejčastěji zařazují, je tzv. jiná majetková hodnota ve smyslu § 118 OZ. O majetkovou hodnotu se jedná mimo jiné i z toho důvodu, že doménová jména lze ocenit penězi a souvisí s majetkovou sférou fyzických či právnických osob. Názor, že jde o subjektivní právo se zdá být neopodstatněný, jelikož samotné doménové jméno je spíše předmětem jednotlivých subjektivních práv k němu založených. Věcí být zřejmě také nemůže, jelikož z povahy věci se v případě doménového jména nejedná o hmotný předmět, tudíž ani o vlastnictví v právním slova smyslu se hovořit v souvislosti s doménami nelze. Skutečná klasifikace může však z nejrůznějších důvodů být obtížná a je stále předmětem diskuse.[102] Z pohledu jiné klasifikace je pak nutné zvážit, zda lze doménová jména zařadit mezi druh nehmotných statků. Mimo jiné je tedy nutné zvážit, zda je doménové jméno nadáno zvláštní vlastností, tzv. potenciální ubiquitou. Ta se vyznačuje tím, že předmět může tedy být vnímán na neomezeném počtu míst, neomezeným počtem osob současně, bez jakékoli hmotné újmy na tomto statku. V případě doménových jmen však tato vlastnost dána není, jelikož doména může být užívána pouze jedinou osobou, totiž tou, pro kterou byla zaregistrována.[103] Z toho by však nutně plynul závěr, že o druh duševního vlastnictví nejde.[104] Důsledkem však je, při neexistenci zvláštního právního předpisu ani klasifikaci, že práva k doménovému jménu nemají povahu absolutních práv, ale práv relativních. Tedy vzniklých na základě smlouvy o jeho registraci, ze které vyplývá závazek registrátora nepřevést jej na jinou osobu a neumožnit žádné

[101] Efroni (2007) str. 1 a 2.

[102] Mališ., P. (2011) *Co to jsou doménová jména, aneb nad právní povahou doménových jmen*. [online] přístupné na adrese <http://www.elaw.cz/cs/pravo-it/334-co-to-jsou-domenova-jmena-aneb-nad-pravni-povahou-domenovych-jmen.html>.

Odlišný názor je prezentován například Sehnálkem v polemice *Právní povaha doménového jména* přístupném na adrese <http://www.itpravo.cz/index.shtml?x=132115>.

[103] Pelikánová a Čermák (2000) str. 47.

[104] Opačný názor vyjadřuje např. Dobřichovský (k tomu více srov. Dobřichovský., T. (2004) *Moderní trendy práv k duševnímu vlastnictví v kontextu evropského práva, dohody TRIPS a činnosti WIPO*. Praha: Linde. Str. 179).

třetí osobě užívání této domény. Oprávnění však svým obsahem a důsledky připomíná práva odpovídající právu vlastnickému, tj. doménové jméno užít, pobírat z něj užitky a disponovat s ním, resp. s právem k němu užít.[105]

Ani zahraniční pojetí a literatura není jednotná v teoretickém základě a právní povahy doménových jmen. Značná majetková hodnota doménových jmen i obtížně uchopitelné spory týkající se například domén obsahujících obecné názvy (například sex.com) bývají často důvodem, proč někteří autoři poukazují na potřebu jasného právního vymezení doménových jmen.[106]

Ať se přikloníme k názoru tomu či onomu, faktem je, že pokud jde o právní režim a nakládání s doménovými jmény, judikatura i praxe se poměrně ustálila a nečiní jí existence rozdílných teoretických základů problém při výkladu a sporech o práva s nimi související.

Z pohledu povahy práv k doménovému jménu může dojít také ke kolizi s jinými právy, např. k ochranné známce, obchodní firmě. K registraci doménového jména totiž dochází na principu časovém, tj. kdo o ní první požádá (v angličtině též známé „first come, first served"), přičemž registr není povinen kontrolovat například kolizi s registrovanými ochrannými známkami. Registrace a užívání některých doménových jmen (obdobných či snadno zaměnitelných např. s obchodní firmou) může být klasifikováno i jako nekalosoutěžní jednání dle obchodního práva. Tyto rozdíly a kolize jsou často otázkou soudních sporů před českými soudy.[107] Na rozdíl od úprav jiných institutů, např. ochranných známek či obchodního firmy, které jsou poměrně přesně zakotvené, lze považovat současný stav české právní úpravy v souvislosti s doménovými jmény za nedostatečný a často nejasný. Kromě jiného lze jistě užít i případy odpovědnosti za škodu. V otázkách cybersquattingu (viz. úvod) byl v USA přijat zvláštní zákon, který posiluje ochranu majitelů ochranných známek.[108] Tito se mohou domáhat ochrany před každým, kdo bez dobré víry užívá, obchoduje či zaregistruje stejné nebo zaměnitelné doménové jméno, přičemž tento návrh lze podat i proti neznámému žalovanému (čímž lze dosáhnout alespoň zákazu užívání dotčené domény).[109]

---

[105] Mališ (2011).

[106] Nguyen., Xuan-Thao. (2001) *Cyberproperty and Judicial Dissonance: The Trouble with Domain Name Classification*. George Mason Law Review. [online] Přístupné na adrese <http://ssrn.com/abstract=1493482>.

[107] Např. Čermák., J. (2005) *Předběžné opatření ve sporu Prace.cz vs. Sprace.cz – rozhodnutí o odvolání*. [online] Přístupné na adrese <http://www.itpravo.cz/index.shtml?x=323025>.

[108] Federal Trademark Dilution Act of 1995.

[109] Pelikánová a Čermák (2000) str. 58 – 60.

K tomuto je nutné doplnit též české právní vymezení do budoucna. To se kloní k názoru, že je nutné i s nehmotnými statky a právy zacházet obdobně jako s věcmi v právním smyslu, a výslovně i tyto ostatní kategorie do pojmu věc zahrnuje a prohlašuje za věci nehmotné, obdobně například jako ochranné známky.[110] Napříště tedy již nebude otázkou diskuse, zda je správně hovořit o vlastnictví a majiteli doménového jména, o jeho prodeji či povaze práv s ním souvisejících. Proto i tyto pojmy budou v dalším výkladu používány.

4.3 Kolize doménových jmen s jiným právy

4.3.1 Obecná problematika

Zabýváme-li se otázkou právního vymezení a povahy užívání doménových jmen, nelze se nezabývat též otázkou kolize a případné odpovědnosti při porušení jiných práv, která mohou být se zájmy registrovaného majitele doménového jména v poměru antagonistickém. Jedná se zejména o kolize s různými druhy práv na označení (ať se jedná o průmyslová práva jako např. ochranné známky, nebo o obchodní firmu či práva ke jménům fyzických či právnických osob). Kromě toho je důležitým faktorem též obchodněprávní úprava nekalé soutěže, která je poměrně účinným prostředkem obrany. V případech ochrany těchto práv jsou právní prostředky formulovány obdobně. Jedná se zejména o nárok zdržovací a odstraňovací, náhradu škody, vydání bezdůvodného obohacení a přiměřeného zadostiučinění jako náhrady za nemajetkovou újmu.[111] Kromě těchto nároků se může také žalobce domáhat zveřejnění rozhodnutí na náklady žalovaného.

Zejména pokud jde o první dva nároky, je nutné vždy zvážit způsob realizace těchto nároků. Soud zpravidla nedovolí příliš extenzivní výklad takového nároku a je třeba poměrně přesná konkretizace. Tak se například vedou spory, zda je vůbec v souvislosti s doménovými jmény přijatelné nařídit povinnost převést doménové jméno na žalobce (např. majitele porušované ochranné známky). Na první pohled se může zdát, že taková povinnost jako konkretizace přiznaného odstraňovacího nároku je přijatelná.[112] Avšak z pohledu důkladnějšího mohou vyvstat další související otázky. Tak například bude-li doménové jméno používáno pro

[110] § 470 odst. 2 návrhu nového občanského zákoníku. K tomu blíže viz. <http://obcanskyzakonik.justice.cz/cz/vlastnictvi-a-dalsi-vecna-prava/konkretni-zmeny/zmena-chapani-pojmu-veci.html> nebo návrh zákona a důvodová zpráva ve znění z ledna 2011 – přístupný na adrese <http://obcanskyzakonik.justice.cz/cz/navrh-zakona.html>.

[111] Viz. § 53 až 54 ObchZ a § 4 odst. 1 a § 5 odst. 1 a 4 zákona č. 221/2006 Sb., o vymáhání práv z průmyslového vlastnictví, dále též § 19b odst. 2 a 3 OZ.

[112] K tomu pozn. Za zastaralý lze považovat názor, že takovou povinnost nelze uložit, jelikož tato není výslovně v žádném právním předpise zakotvena a umožněna.

jiné, nepodnikatelské účely, které nemají za účel nikterak zmást zákazníky či přivodit zaměnitelnost s chráněnou známkou, která je vždy pouze k určitému druhu zboží či služeb, není v takovém případě příliš omezující přiznat povinnost převést doménu na majitele ochranné známky a tím fakticky ochranu a dopad ochranných známek výrazně rozšířit? Nemůže v takovém případě být postačujícím pouhé uložení povinnosti neužívat danou doménu pro stejné podnikatelské záměry, pro které byla ochranná známka registrována? Současná praxe se přiklání k řešení prvnímu, přičemž obvykle jsou obranné nároky opírány i z tvrzeného nekalosoutěžního jednání, kdy judikatura vykládá soutěžní vztah na internetu velmi široce, v podstatě bez ohledu na to, pro jaký účel je dané doménové jméno registrováno a fakticky užíváno. Potom povinný je zavázán takový převod zjednat, jelikož registrátor v této souvislosti není vykonavatelem veřejné moci, ale pouze soukromou třetí osobou, která je povinna poskytnout součinnost. Dnes již v samotných podmínkách registrace (smlouvy) české domény u CZ.NIC je ustanovení o možnosti registrátora provést změnu v registrované osobě mimo jiné i na základě soudního rozhodnutí.[113] K realizaci zdržovacího nároku pak Čermák dodává, že nemusí vždy dojít k zrušení registrace doménového jména. Z obecné povinnosti přiměřenosti zásahů do subjektivních práv může být postačujícím omezení určitého způsobu užívání takové domény, např. pro účely obchodování s danou službou či výrobkem.[114] Nárok odstraňovací však takové modality neposkytuje a jeho důsledkem může být jedině zrušení registrace domény. Na druhou stranu je nutné si zároveň uvědomovat teritoriální ochranu práv, se kterými se dostávají doménová jména do kolize. Tak například soudy v případech, kdy je přikázáno zdržet se a odstranit závadný stav v souvislosti s užíváním doménového jména národní úrovně (u nás s koncovkou .cz), většinou zamítají obdobný požadavek pro případ ostatních druhů domén. Jelikož užívání generické domény (např. s koncovkou .com) nemusí naplnit stejné znaky a ochrana lokálních označení by tak byla příliš extenzivní.

Co se týká ostatních nároků, je nutné se zároveň zaměřit na některé obecné aspekty odpovědnosti v soukromém právu. Dle české právní úpravy vycházející z obecné úpravy občanského zákoníku má odpovědnost za delikt několik důležitých předpokladů. Obdobně se i na ostatní delikty užijí ustanovení o obecné odpovědnosti za škodu dle § 415 a následujících OZ, zejména pak ustanovení § 420 odst. 1 OZ. Každý tedy odpovídá za škodu, kterou způsobil porušením právní povinnosti. Minimálními předpoklady je tedy protiprávní jednání, zásah do

[113] Viz. Rozsudek Vrchního soudu v Praze sp. Zn. 3 Cmo 293/2003/10.8.2004 (Horáček., R. a Macek., J. (2007) *Sbírka správních a soudních rozhodnutí ve věcech průmyslového vlastnictví*. Praha: C. H. Beck. Str. 65 – 69).

[114] Pelikánová a Čermák (2000) str. 189.

práva jiného (způsobení škody či jiný zásah) a příčinná souvislost mezi jednáním a zásahem. Dále je třeba též zvážit otázku subjektivního vztahu k takovému jednání a následku, tedy zavinění. Otázka zavinění však mnohdy v souvislosti s doménovými jmény a delikty souvisejícími není relevantní.

Protiprávnost může vyplývat jak z výslovného zakotvení v zákoně, tak z existence přiznaného subjektivního práva, jelikož nikdo z povahy věci nesmí takové právo porušovat, nejde-li o okolnosti protiprávnost vyučující (např. plnění zákonné povinnosti či výkon subjektivního práva). Čermák k tomu poznamenává, že takovým subjektivním právem může být například právo svobodně podnikatelské a jiné hospodářské činnosti ve smyslu čl. 26 odst. 1 Listiny základních práv a svobod.[115]

Problematickou otázkou může být také příčinná souvislost, jelikož ta mimo jiné závisí také na předvídatelnosti následku daného jednání.

Nutno však podotknout, že většina protiprávních jednání zejména ve vztahu k institutům zmíněným v této práci (ochranné známky, ochrana obchodního jména či nekalosoutěžní jednání) vyplývá ze zvláštních zákonných ustanovení.

4.3.2 Doménová jména a práva na označení

4.3.2.1 K právům na označení obecně

Jedna z primárních funkcí doménových jmen, jak již ze samotného názvu tohoto institutu vyplývá, je funkce rozlišovací a vyhledávací, orientační. V širším slova smyslu tak je prostředkem, jak odlišit svojí adresu, nejčastěji internetovou stránku, od jiných. Obdobnou funkci plní i řada právu známých a dlouho existujících pojmů. Ochrana je poskytována také jménu fyzických osob, jakožto součásti osobnosti chráněné podle § 11 OZ. Zda je však doménové jméno v rozporu s osobnostními právy fyzické osoby v daném konkrétním případě, bude záležet vždy na individuálních okolnostech. Ochrana je totiž poskytována pouze, pokud jde o specifické funkce například jména fyzické osoby. Tak například nemusí být vždy doména obsahující příjmení nějaké osoby protiprávní. Kromě toho může dojít i ke kolizi s názvy osob právnických osob, které jsou rovněž chráněny, a to včetně jejich dobrého jména (§ 19b odst. 2 a 3 OZ). Obdobně i obchodní firma, název podnikatele dle zápisu v obchodním rejstříku, je chráněna proti neoprávněnému užívání ve smyslu § 12 ObchZ. Kromě těchto, svojí povahou ryze identifikačních nástrojů, mají mimo jiné obdobnou funkci i jiné formy označení, zejména

[115] Pelikánová a Čermák (2000) str. 176.

ochranné známky či označení původu, nehmotné statky řadící se mezi tzv. průmyslová vlastnictví.

Společným jmenovatelem všech uvedených práv, s nimiž je možný střet s doménovými jmény poměrně nasnadě, je obdobný způsob ochrany. V případě protiprávního zásahu se totiž lze dožadovat, jak již bylo zmíněno výše, aby se takového jednání dotčený zdržel, odstranil závadný stav a jeho následky, případně také nahradil škodu, vydal bezdůvodné obohacení a poskytl přiměřené zadostiučinění jako náhradu za způsobenou nemajetkovou újmu, která může být přiznána i v penězích. V některých případech se lze též domáhat uveřejnění rozhodnutí. Vedle odpovědnosti soukromoprávní může být porušovatel chráněných označení odpovědný i trestněprávně, dopustí-li se osoba protiprávního porušení úmyslně.[116] Ve vztazích obchodněprávních je potom účinným prostředkem ochrany též úprava nekalé soutěže, které se bude týkat samostatná část této práce.

4.3.2.1 Doménová jména a ochranné známky

Jak již bylo uvedeno, základní funkcí ochranných známek je funkce rozlišovací (nebo též identifikační). Jsou určeny k rozlišení výrobků a služeb pocházejících od dané osoby. Kromě dalších funkcí mají plnit i funkci ochrannou, tj. že výlučně vlastník ochranné známky je oprávněn užívat ochrannou známku k označování svých produktů, leda by jiné osoby měly její souhlas. V neposlední řadě mají také funkci propagační a soutěžní.[117] Jak bylo uvedeno v úvodu, obdobné funkce plní i doménová jména. Jde tedy také o způsob označení. Který druh označení má tedy v případě konfliktu přednost?

Z Jednotných zásad ICANN vyplývá, že v případě konfliktu ochranné známky a doménového jména je nutné dát přednost straně, která zažádala o registraci svého označení jako první. Dále tato pravidla vyvozují presumpci absence dobré víry v případě, že z okolností daného případu vyplývá, že k registraci či nabytí domény došlo za účelem jejího dalšího prodeje či nájmu majiteli ochranné známky nebo v úmyslu znemožnit registraci takové domény majiteli ochranné známky. Obdobně je to i v případě známek zaměnitelných či registrace domén bez jejich dalšího užití.

Podmínkou aplikovatelnosti institutu ochranné známky však je jeho užití v obchodním styku, při označení specifických výrobků či služeb (tzv. zásada speciality) dle § 8 odst. 1 ZOZ.[118]

[116] § 268 zákona č. 40/2009 Sb., trestní zákoník.

[117] Slováková., Z. (2007) *Průmyslové vlastnictví*. *I.dotisk druhého, doplněného a rozšířeného vydání*. Praha: LexisNexis CZ s.r.o., str. 129.

[118] Zákon č. 441/2003 Sb. o ochranných známkách.

Tato úprava však již neposkytuje ochranu například vůči spekulaci s doménou ani před její registrací osobou nezabývající se činností, pro kterou byla daná ochranná známka zaregistrována, resp. například se vůbec netýká podnikatelské činnosti.[119] Avšak i taková jednání někdy mohou být na újmu majiteli ochranné známky. Na druhou stranu však již lze podřadit pod danou situaci případ, kdy spekulant se pokusí například nabídnout danou doménu k převodu. Tím lze považovat, že vstoupil do hospodářské soutěže, resp. obchodního styku a ochrana z titulu ochranné známky by tak byla po právu.

Zároveň také dochází ke konfliktu teritoriálního dosahu ochranné známky. Přijmeme-li za svou situaci, kdy se úspěšně domůže ochrany majitel ochranné známky proti tomu, kdo má registrovanou doménu, velmi často dojde k této situaci. Ačkoli ochranná známka je třeba zaregistrována a chráněna na území jednoho státu, zamezí užívání doménového jména i na území ostatních států díky globální povaze internetu. Z tohoto důvodu bývá často předmětem sporů, zda je žádoucí takovouto extenzivní ochranu zaregistrovaných známek poskytovat. Tento rozpor je interpretací vysvětlitelný v případech registrace domény národní (.cz), ze které lze vyvozovat, že se obrací na uživatele na území České Republiky. Více problematická je však situace doménových jmen generických (typicky .com), kde dostatečné sepětí s územím ochrany ochranné známky by muselo být prokázáno například skutečnou činností subjektu užívajícího dotčené doménové jméno.

Takovému stavu lze předcházet již při registraci domény, kdy vhodný mechanismus kontroly, zda není ochranná známka obsažena v nově požadovaném doménovém jménu, by mohl předejít mnohým sporům. Na druhou stranu však zřejmě nelze požadovat, a nebylo by to ani praktické, aby registrátor plnil funkci rozhodujícího a kontrolního orgánu při posuzování případné kolize s jinými právy či instituty. Proto nezbývá jiné řešení než dodržet princip, že každý má dbát svých práv a chránit je, a případné kolizní situace řešit z vlastní iniciativy.

Důležitý je také institut všeobecně známé ochranné známky s dobrým jménem, jelikož její ochrana je širší než pouze v souvislosti s určitými výrobky a službami.[120]

Z druhé strany je nutné vzít v potaz § 10 odst. 2 ZOZ, které dává povinnost majiteli ochranné známky strpět její užívání, je-li to v souladu s obchodními zvyklostmi a dobrými mravy soutěže. Toto ustanovení se aplikuje například v případě konfliktů se jmény, obchodním jménem, označení některých vlastností výrobků apod. Tak například registrace domény

[119] K tomu více např. v rozsudku Vrchního soudu v Praze sp. Zn. 3 Cmo 321/2005/31.1.2006.

[120] Ve smyslu § 3 písm. d) ve spojení s § 7 odst. 1 písm. d) ZOZ.

obsahující obchodní firmu toho, kdo ji zaregistroval, by měla být z tohoto pohledu legitimním titulem k její registraci a užívání, není-li takové počínání vedeno spekulativními záměry.[121]

V praxi se objevují i opačné tendence, kdy v důsledku nepřesné nebo spíše neexistence zvláštní úpravy ochrany doménových jmen dochází ke snahám dosáhnout pevnější právní postavení jejich registrací jako ochrannou známku. Nutno však dodat, že zdaleka ne každé doménové jméno je tomu způsobilé. Ani argumentace, že každé takové jméno je z povahy věci jedinečné a nezaměnitelné neobstojí, jak uvádí Úřad průmyslového vlastnictví ve svých rozhodnutích.[122]

Yee Fen Lim se podrobněji zabývá situací v Austrálii. Dle tamního Nejvyššího soudu se dopouští porušení práv k ochranné známce každý, kdo třebaže pouze registruje doménové jméno, které je zároveň existující ochrannou známkou jiné osoby.[123]

Jedním z nejdůležitějších soudních případů zahraničí je také známý případ ve Velké Británii, Marks & Spencer plc v One in a Million Ltd[124]. V tomto případě se vrchní soud zabýval otázkami doménového jména ve vztahu k ochranným známkám a deliktního jednání (tzv. passing off, což je specifický institut porušení práv k duševnímu vlastnictví v angloamerické jurisdikci). Jde o případ, kdy společnost One in a Million Ltd registrovala množství vysoce hodnotných doménových jmen s úmyslem je následně prodat jejich běžným uživatelům v komerční sféře (dnes známý nežádoucí jev, tzv. cybersquatting). V něm na rozdíl od výše uvedeného přístupu australského je mimo jiné judikováno, že samotné registrování takové domény není uváděným deliktem, tedy passing off. Nakládání s nimi způsobem, který ohrožuje jméno registrované ochranné známky, však již tento delikt naplňuje. Vyšší instance však i pouhé registrování takové domény za porušování ochranné známky považovaly.[125]

Všem těmto oblastem (Austrálii i UK) však je společné, co již bylo zdůrazněno a platí i pro ostatní jurisdikce, že k ochraně pomocí institutu ochranné známky je nutné prokázat, že

[121] K tomu též Pelikánová a Čermák (2000) str. 151.

[122] Např. ÚPV O-171663/17.12.2003 *Název domény na Internetu* (Horáček., R. a Macek., J. (2007) *Sbírka správních a soudních rozhodnutí ve věcech průmyslového vlastnictví*. Praha: C. H. Beck. Str. 65 – 69).

[123] Soudní rozhodnutí ve sporu *Fletcher Challenge Ltd v Fletcher Challenge Pty Ltd 1981* (Yee Fen Lim (2007) *Cyberspace Law. Commentaries and Materials. Second Edition.* Australia. South Melbourne, Victoria: Oxford University Press. Str. 577).

[124] (1997) 42 IPR 309 z 10. května 2001.

[125] Yee Fen Lim (2007) str. 577 – 583.

došlo k jejímu použití či registraci při obchodním styku vztahujícímu se k výrobkům a službám, ke kterým byla daná ochranná známka registrována.[126]

Obdobné upevnění právního postavení těch, komu svědčí ochranné známky, bylo zaznamenáno i v případě USA. Postavení proti cybersqautterům bylo předmětem případu Panavision Internation L.P. v Toeppen. V tomto rozhodnutí bylo mimo jiné judikováno, že užívání chráněného označení v doménovém jménu snížilo identifikační a rozpoznávací funkci registrované ochranné známky při poskytování výrobků a služeb na Internetu. Tomu nezabránil ani fakt, že dotčená doména byla užívána čistě k nekomerčním účelům (zobrazování fotografií města Pana). V tomto případě však byl za komerční užití shledán pokus o prodej dotčené domény osobě, která pod takovým jménem své obchodní aktivity provozovala. Na základě takových zkušeností došlo také k přijetí nové legislativy zabývající se zejména tímto jevem, the Anti-Cybersquatting Consumer Protection Act (ACPA) z roku 1999. Tento zákon výslovně činí protiprávní i pouhou registraci domény identickou nebo zaměnitelnou se známou značkou ve zlé víře se záměrem zisku. Předpokladem je tedy existence jména či značky právně chráněné (včetně osobních jmen), které bez souvislosti s konkrétním zbožím či službami byly použity v doménových jménech, pokud byla tato jména zaregistrována či jinak užita s úmyslem ekonomického zisku ve zlé víře (ustanovení 1125 ACPA). Přičemž žalobu lze dle tohoto zákona vznést u soudu dle místa, kde byla taková doména registrována (tzv. pravomoc in rem, tedy dle místa registrátora), což zjednodušilo otázku, kde žalovat toho, komu doména svědčí, jelikož dohledání takové osoby může být velmi obtížné.[127] Tento legislativní krok se stal účinným prostředkem ochrany proti cybersquattingu před tamními federálními soudy. Z praktického hlediska to však znamená, že každý, kdo si registruje a užívá doménové jméno .com podlého jurisdikci soudů v USA (Virginii).[128]

Konečně, obdobnou konstrukci lze nalézt i v UDRP (soft law vydané ICANN), které definuje cybersquatting jako případy, kdy se jedná o registraci či jiné užití domény identické či zaměnitelné s označením, ke kterému má stěžovatel právo, registrovaný nemá legitimní zájmy k danému doménovému jménu a bylo-li takové jméno registrováno a užito ve zlé víře.

K uvedené doktríně lze uvést i některé kritické poznámky. Tímto systémem není dostatečně odlišeno, zda dané jméno je či není registrováno či užíváno pro obchodní účely.

[126] Ibid. Str. 588. (pro další podrobnosti např. soudní případ Pitman Training Ltd. v Nominet UK z roku 1997).

[127] Efroni (2007) str. 9 až 12.

[128] K tomu blíže např. Hrubešová., H. (2006) *Proč si neregistrovat doménové jméno pod doménou nejvyššího stupně ".com" aneb jak je to s jurisdikcí amerických soudů.* [online] <http://www.itpravo.cz/index.shtml?x=1928185>.

V takovém případě dochází k extenzivnímu zbytnění práv k chráněnému označení (ať jím je ochranná známka, obchodní jméno či jiné označení). Z procedurálního hlediska je také kritizováno v případě sporů řešených alternativní (mimosoudní) cestou, že jejich rychlé a poměrně nenákladné řešení však nedává dostatečný prostor pro obranu. Zatímco stěžovatel má na přípravu podkladů proti majiteli doménového jména času výrazně více, na obranu jsou dány velmi krátké lhůty. To platí pro všechna mimosoudní řízení (např. před WIPO či NAF).[129]

4.3.2.2 Doménové jméno a obchodní firma

Jiným případem označení subjektu je užití obchodního jména (firmy). Každá třetí osoba je povinna zdržet se užívání shodného nebo zaměnitelného označení (§ 8 – 12 ObchZ). Dopad tohoto institutu je širší než v případě ochranných známek, jelikož není vázán jen na určité výrobky či služby. Významným však pro posouzení zaměnitelnosti je obor podnikání a užívání daného označení. Při určení protiprávnosti registrace a užívání doménového jména bude důležité posoudit otázku funkce, jakou v daném případě plní. Za protiprávní je třeba považovat takové činnosti, kdy je doména užívána k propagaci, hospodářské soutěži či jiné výdělečné činnosti, kdy je zpravidla zneužíváno toho, že jde o shodné nebo zaměnitelné jméno s obchodním jménem jiného podnikatele. Takto je nutné postihnout i případy spekulativní registrace za účelem zamezení jejího užívání či úplatného převodu na toho, kdo takové obchodní jméno má.[130] V tomto ohledu lze uvést jako příklad soudní rozhodnutí Vrchního soudu v Praze ve věci doménového jména ceskapojistovna.cz.[131] Na druhou stranu toto rozhodnutí má i negativní stránky z toho pohledu, že například přiznaný nárok na převedení doménového jména na žalobce nemá oporu v našem objektivním právu, třebaže je do budoucnosti krokem správným.[132] I z tohoto důvodu lze považovat za nedostatečný stav dnešní právní úpravy ve vztahu k doménovým jménům. Praxi však nucený převod registrace doménového jména problém nečiní a rozhodnutí bývají postavena na tom, že jde o pouhou konkretizaci právem přiznaného nároku zdržovacího a odstraňovacího ve smyslu § 12 odst. 1 ObchZ.

[129] Efroni (2007) str. 16 až 18.

[130] Pelikáno a Čermák (2000) str. 155 – 157.

[131] Rozhodnutí č. j. 2 Cm 290/2001-39.

[132] K tomu též Aujezdský., J. (2005) *Rozsudek ohledně domény ceskapojistovna.cz. Co je špatně?* [online] <http://www.itpravo.cz/index.shtml?x=220507>.

4.3.3 Doménová jména a právo nekalé soutěže

Na rozdíl od ochranných známek je použitelnost práva na ochranu proti nekalé soutěži širší z toho ohledu, že generální klauzule umožňuje její použití v poměrně širokém množství případů. Základní premisa však musí být splněna i zde, totiž že dochází k jednání v hospodářské soutěži. Musí tedy být mezi oběma subjekty soutěžní vztah. Lze tedy namítat, že v případě užití pro osobní nebo jiný účel než podnikatelský tedy nelze institut nekalé soutěže využít.[133] Záleží však, jak je pojem soutěžitele a existence soutěžního vztahu v tomto kontextu vykládána. Navíc úprava dle § 41 a násl. ObchZ má širší dopad než pouze na podnikatele.

Společným jmenovatelem však je, že vždy musí být naplněny znaky tzv. generální klauzule, tj. že musí jít o jednání v hospodářské soutěži, které je v rozporu s dobrými mravy soutěže a je způsobilé přivodit újmu jiným soutěžitelům nebo spotřebitelům (§ 44 odst. 1 ObchZ). Systematika právní úpravy nekalé soutěže totiž vychází pojetí, že generální klauzule musí být naplněna vždy, a jednotlivé skutkové podstaty jsou pouze její konkretizací a kategorizací jednotlivých případů, přičemž jejich výčet (§ 44 odst. 2 ObchZ) je povahy demonstrativní.

Jednání v hospodářské soutěži může záviset jak na existenci soutěžního vztahu, tak na charakteru a povaze konkrétního chování subjektu. Může jít i o jednání v hospodářském styku, která jsou v rozporu se zásadou slušnosti či dobrých mravů při obchodování, ačkoli není mezi osobami soutěžní vztah.[134] Tento širší výklad je daleko praktičtější i v posuzování otázek ve vztahu k doménovým jménům. V praxi je zřejmé, že v prostředí internetu bývá pojem soutěžního vztahu vykládán velmi široce, ačkoli nejde o oblast stejných služeb či výrobků, pro které je daná doména používána či registrována.[135]

Dalším atributem je rozpor s dobrými mravy soutěže, tedy jednání odporuje jejímu smyslu a účelu. Výklad tohoto pojmu může být někdy složitý, obecně se však jako hledisko berou dopady na hospodářskou soutěž, neboli podporu konkurence a výkonnosti soutěžitelů.[136] Za nekalosoutěžní jednání tak lze považovat i spekulativní registrace doménových jmen shodných nebo zaměnitelných s označeními užívanými při obchodní činnosti jiným subjektem,

[133] Pelikánová a Čermák (2000) str. 31.

[134] Pelikánová a Čermák (2000) str, 162 a 163.

[135] Srov. Rozhodnutí č. 00013 uveřejněné 8.10.2010, Rozhodčí nález Rozhodčího soudu při HK ČR a AK ČR (přístupné na adrese <http://domeny.soud.cz/adr/decisions/index.php>).

[136] Horáček, R., Čada,L., Hajn, P. (2005) *Práva k průmyslovému vlastnictví*. 1. vydání. Praha: C. H. Beck, str. 397.

mají-li za důsledek hospodářský zisk například jejich pozdějším prodejem či pronájmem tomu, jehož jméno je v nich obsaženo. Takové jednání je bezesporu v rozporu s dobrými mravy hospodářské soutěže.

Zároveň musí jít o jednání, které je způsobilé přivodit újmu jiným soutěžitelům či spotřebitelům. Pojem újma je daleko širší než škoda, přičemž může být i nehmotného charakteru. Například v případě ochranných známek je újmou i roztříštění jejího dopadu a funkce (tzv. rozmělnění ochranné známky).[137] Újma spotřebitelům bude způsobena i jejich zmatením či ovlivňováním jejich rozhodování pomocí protiprávního užívání či registrace doménového jména.

Dopad nekalosoutěžní úpravy je také širší v tom smyslu, že nechrání pouze označení registrovaná (např. ochranné známky, firmy či názvy právnických osob), ale také jiná označení užívaná soutěžitelem, která se v dané souvislosti stala jakousi další hodnotou podniku daného soutěžitele.[138]

Dle individuálních okolností může být poté subsumován případ pod konkrétní skutkovou podstatu nekalé soutěže, např. klamavou reklamou, zlehčováním, vyvoláním nebezpečí záměny či parazitováním na pověsti, anebo může jít o jiný druh jednání, který naplnil generální klauzuli. Tak například se považuje za nekalosoutěžní i jednání pro rozpor s jinými právními normami, například právními úpravami průmyslových práv. Je také v podstatě pravidlem, že kromě protiprávního jednání ve vztahu například k ochranným známkám bývá také odůvodňován právní nárok i na základě obecného nekalosoutěžního jednání.

Jak již bylo poznamenáno, z hlediska nároků, které lze uplatnit z titulu nekalé soutěže, jde jak o nárok zdržovací, odstraňovací a satisfakční (přiměřené zadostiučinění), přičemž může být přiznáno též právo na uveřejnění rozsudku na náklady žalovaného. Kromě toho se lze domáhat i náhrady škody a vydání bezdůvodného obohacení dle obecné úpravy zejm. v občanském zákoníku. Odpovědnost porušitele hospodářské soutěže, je-li tato porušena úmyslně a dopady jsou většího rozsahu, může mít i povahu trestněprávní, jelikož naplní znaky trestného činu Porušení předpisů o pravidlech hospodářské soutěže ve smyslu § 248 odst. 1 TZ.

4.4 Spory související s doménovými jmény

4.4.1 Metody a prameny řešení sporů

Z hlediska sporů týkajících se doménových jmen je nutné hned od počátku rozlišit dva hlavní způsoby jejich nezávislého řešení. Primárním způsobem dle klasické právní teorie je řízení

[137] Ibid. str. 398 a 399.

[138] Pelikánová a Čermák (2000) str, 164.

soudní. Jeho nevýhody však lze spatřovat hned v několika směrech. Kromě větší nákladnosti a časové náročnosti soudního řízení může být často problematická i otázka jurisdikce. Dále i prameny, na základě kterých je rozhodováno mohou být odlišné. Tak například v případě arbitrážním může být rozhodováno na základě soft-law (např. ve formě UDRP), avšak v případě soudního rozhodování jsou závazné pouze zákonné normy. V druhém, z pohledu četnosti a praktičnosti daleko více využívaným způsobem, jsou tzv. ADR způsoby neboli alternativní řešení sporů.[139] Jejich výsledkem také zpravidla bývá autoritativní rozhodnutí, např. rozhodčí nález, který je mimo jiné též exekučním titulem. Z tohoto pohledu je třeba zdůraznit, že globální charakter internetu a unifikovaný přístup v takových otázkách, jako jsou doménová jména, je třeba považovat za prioritní. Proto tyto alternativní způsoby řešení sporů jsou preferovány, jelikož se často v praxi přenáší rozhodování na k tomu specializovaná pracoviště, např. Rozhodčí a mediační centrum WIPO. Na důležitosti i kreditu takto nabývá i Rozhodčí soud při HK ČR a AK ČR (dále též „český rozhodčí soud“), který je rovněž oprávněn rozhodovat spory týkající se nadnárodních doménových jmen evropských (.eu) i generických (.com, .org a další).

Jak již bylo naznačeno, hlavním důvodem vznikajících sporů je ekonomický rozměr domén, které se užívají také jako prostředek identifikace obchodníků a dostávají se do kolize s jinými identifikátory, např. obchodní firmou či ochrannou známkou. Nejvýznamnější spory vznikaly v průběhu 90. let zejména na území USA, kdy jediným mechanismem řešení těchto sporů bylo soudní řízení. Problematické však byly jak otázky nákladnosti, doby trvání, jurisdikce a teritoriálních pravomocí jednotlivých národních soudů. Proto ICANN vydala několik souborů pravidel, která v podstatě znamenala harmonizační hmotněprávní i procedurální pravidla (svojí povahou soft-law nezávazné pro vnitrostátní soudy) jako podklad pro rozhodování sporů o doménová jména při rozhodování pomocí ADR (dále jen Jednotné zásady).[140] Jednotné zásady jsou povinným základem a unifikačním prostředkem pro rozhodování sporů ohledně generických doménových jmen a v různých modifikacích se prosazují a aplikují i pro jména nižších úrovní. Rozhodováním takových sporů jsou pověřeny profesionální, mimosoudní instituce.[141] Jedná se v podstatě o rozhodčí soudy či obdobné orgány, které rozhodují spory o doménová jména, a to

[139] Z anglického Alternative Dispute Resolution.

[140] UDRP (Uniform Rules for Domain Name Resolution Policy) a RUDRP (Rules for Uniform Domain Names Dispute Resolution Policy), blíže na adrese <http://www.icann.org/en/udrp/>.

[141] Těmi jsou např. WIPO – World Intellectual Property Organization, CPR – Institute for Dispute Resolution, ADNRC – Asian Domain Name Dispute Resolution Centre nebo Rozhodčí soud HK ČK a AK ČR.

jak v případě nejvyšších domén generických, tak i mnohých národních domén (pokud tuto pravomoc národní manažeři domén těmto soudům svěřili).

Obdobně je otázka podmínek a řešení případných sporů upravena i pro národní domény, kde je příslušnost ke sporům o doménová jména .cz svěřena Rozhodčímu soudu při Hospodářské Komoře ČR a Agrární Komoře ČR (jak vyplývá z pravidel registrace doménových jmen c ccTLD .cz).[142] V případě národní domény .sk na Slovensku je rozhodování sporů nadále ponecháno řádným soudům.[143] Právním základem použití daných pravidel při řešení sporů jsou potom ustanovení smlouvy o registraci domény, které na daná pravidla odkazují. Kromě procesních otázek jsou také odlišné prameny, na základě kterého se případné spory rozhodují. Tím často nebývají zmíněná Jednotná pravidla či jiné obdobné normy soft-law, ale řeší se na základě tamního vnitrostátního právního řádu. Jednotlivé vnitrostátní právní normy jsou samozřejmě leckdy odlišné, což z pohledu unifikačního není pozitivním jevem. Z tohoto hlediska je třeba podotknout, že by bylo vhodné, aby tento proces byl maximálně sjednocen a v zájmu právní jistoty registrujících i těch, kdo se ochrany svého označení domáhají, došlo k maximálnímu použití Jednotných pravidel i pro ostatní druhy domén. Přičemž z praktického hlediska i příslušnost by mohla být obdobná jako u generických doménových jmen, tj. např. Arbitrážní a mediační centrum WIPO nebo jiný obdobný orgán, který by mimo jiné také zaručil jednotné a ustálené postupy a rozhodování, což by výrazně upevnilo i právní jistotu v dané oblasti bez ohledu na to, o jaký druh doménového jména se jedná.[144]

Pokud jde o evropská doménová jména .eu, registrovaná u společnosti EURid, v případě sporů se mimo jiné užije i evropské nařízení č. 874 z roku 2004, které v článku 21 ve spojení s článkem 10(1) výslovně zakazuje spekulativní či zneužívající registrace.[145] Nelze si nevšimnout, že konstrukce je velmi obdobná té, kterou obsahují UDRP vydané ICANN (aplikovatelné pro globální generické domény). Přičemž za důvod revokace je považován zejména v případě registrace doménového jména stejného nebo zaměnitelného s jiným chráněným označením, pokud toto jméno bylo zaregistrováno jejím držitelem bez legitimních zájmů k danému jménu, anebo pokud bylo zaregistrováno či užíváno ve zlé víře (článek 21(1) písm. a) a b) tohoto nařízení). Za legitimní zájem se považuje například předchozí užívání např.

[142] Přístupné také na adrese <http://www.nic.cz/files/nic/doc/Pravidla_registrace_CZ_ccReg_20080930_fin.pdf>.

[143] Raban, Moravcová a kol. (2006) str. 41, k tomu blíže viz. čl. 14 na adrese <https://www.sk-nic.sk/kontakty/pravidla.10.9.2010.jsp>.

[144] K tomu blíže viz. Dobřichovský (2004) str. 182 až 185.

[145] Nařízení ES č. 874/2004 z 24. dubna 2004 (přístupné též na http://www.eurid.eu/files/ec20874_en.pdf).

poskytováním zboží či služeb, nebo pokud šlo o osobu obecně známou pro danou doménu (ačkoli nejde o registrované či jinak právem chráněné označení), nebo pokud jde o případ, kdy držitel provádí nekomerční užívání doménového jména bez úmyslu poškodit jméno či zmást zákazníky držitele jiného chráněného označení (čl. 21(2) téhož nařízení). Část 3. Článku 21 potom uvádí demonstrativně, jak lze prokázat zlou víru: 1) okolnosti ukazující, že k registraci došlo primárně s cílem ji prodat, pronajmout či jinak převést na držitele chráněného označení, 2) registrace byla provedena s úmyslem zabránit užívání chráněného jména tomu, komu svědčí (např. okolnosti a způsob, jakým došlo k registraci, neužívání domény min. 2 roky od její registrace či pokud došlo k projevu úmyslu takové jméno používat osobou, jejíž označení je chráněno), 3) bylo-li doménové jméno registrováno primárně z důvodu narušení profesionálních činností soutěžitele, 4) bylo-li úmyslně užito k vylákaní uživatelů internetu pro komerční účely, vytvořením podobnosti a zaměnitelnosti s chráněným označením či jeho existující webovou stránkou, nebo 5) je-li registrované doménové jméno je jménem osobním, přičemž mezi danou osobou a držitelem domény neexistuje žádné propojení. Tak například lze uvést, že toto ustanovení je hlavním a poměrně jednoduchým podkladem k rozhodování případných sporů, jako tomu bylo například v případě domény čSOB.eu v roce 2010.[146]

4.4.2 Přístup v angloamerických právních řádech

Pelikánová uvádí, že národní soudy rozhodují věci doménových jmen v podstatě podle principů platných pro duševní vlastnictví a na základě spravedlivého uspořádání soukromoprávních vztahů. Všímá si tudíž, že rozhodování konfliktů se příliš neliší, ať k nim dochází v systému kontinentálním nebo angloamerickém.[147]

V USA, podle jejichž úpravy lze dovodit příslušnost tamních soudů poměrně snadno (konal-li na jejich území systematicky a trvale určité úkony, anebo je-li to přiměřené vzhledem k úzkému vztahu činnosti dotčeného subjektu se sférou, která spadá do jurisdikce tamních soudů)[148] lže žalovat porušení práva na základě několika právních institutů. Zejména v případě absence dobré víry lze nárok odůvodnit porušením práva k registrované ochranné známce, práva proti nekalé soutěži či porušení práva na ochranu osobnosti. Podmínkou však je, že kromě zlé víry došlo k obchodnímu užívání dané domény. Za ten se běžně nepovažuje pouhá registrace doménového jména, ale například pokus o její prodej by tuto podmínku již splnit měl. Vždy však

[146] Blíže viz. <http://eu.adr.eu/adr/decisions/decision.php?dispute_id=5670>.

[147] Pelikánová a Čermák (2000) str. 55.

[148] Dle soudních rozhodnutí Helicopteros Nacionales de Colombia, SA v. Hall, 1984, nebo World-Wide Volkswagen Corp v. Woodson 1980.

záleží na konkrétních okolnostech a motivech již samotné registrace doménového jména. Na druhou stranu je také nutné varovat před přílišnou ochranou například ochranných známek, ke které mohou některé případy vést. Jedná se zejména o případy nekomerční registrace a používání doménového jména, jehož omezování je v podstatě zasahováním do ústavních práv a svobod zaručených Prvním Dodatkem Ústavy USA.[149] V tomto ohledu například soud určil, že mimo jiné by soud měl zvážit doménové jméno jako takové, záměry registrující osoby, obsah internetových stránek a technický protokol užívaný v daném systému doménových jmen.[150] Barrett tak popisuje, co se za nekomerční užití považuje a je tedy nutné považovat za legitimní (například komentáře, parodie, kritika či zpravodajství).[151]

Dále je nutné podotknout z procesního hlediska, že vedle arbitrážního řešení sporů dle UDRP se mohou majitelé ochranných známek také obrátit civilní žalobou na obecný soud. Podle některých autorů může být toto řešení výhodnější mimo jiné i z toho hlediska, že soud může vzít v potaz i další aspekty než ty, které jsou zmíněné v UDRP, a zároveň má širší možnost pro případné dokazování, třebaže to může být časově výrazně náročnější. Je-li poměrně jednoduché dokázat například zlou víru, potom je i pro tamní právníky doporučeno využít arbitráže dle UDRP.[152]

V případě Velké Británie je národním registračním orgánem NOMINET UK, který vede seznam rozhodců pro spory ohledně národních domén .uk. Orgán, který poskytuje řešení sporů, tzv. DRS (Dispute Resolution Service) je součástí společnosti NOMINET UK. Řešení sporů má dvě metody. První je v podstatě mediace, kdy je zdůrazněna snaha o smírné řešení. Není-li možné dosáhnout dohody, řeší daný spor nezávislý odborník (přidělen je podle pořadí v seznamu). Rozhodování má potom dvě instance, je tedy přípustné odvolání k tříčlennému senátu odborníků, přičemž jej lze následně napadnout též soudní žalobou. Kromě toho lze samozřejmě též využít soudní řešení sporu, což však je z hlediska nákladnosti i času velmi nevýhodné.[153] Pokud jde o jurisdikci tamních orgánů, obecné pravidlo, které se v mimo jiné

[149] Barrett., M. (2007) *Domain Names, Trademarks, and the First Amendment: Searching for Meaningful Boundaries*. Connecticut Law Review. [online] Přístupné na adrese <http://ssrn.com/abstract=928261> str. 4 - 5.

[150] Soudní rozhodnutí Name.Space, Inc. v. Network Solutions, Inc., 202 F.3d 573 (2d Cir. 2000).

[151] (2007) str. 58 a 59.

[152] Fryer., W., T. (2008) *Handling Internet Domain Name Arbitration*. The Maryland Bar Journal. [online] Přístupné na adrese <http://ssrn.com/abstract=1639140>.

[153] Bližší informace jsou na adrese <http://www.nominet.org.uk/disputes/drs/>, přičemž soft-law v tomto případě je předpis obsahující procesní otázky: *Dispute Resolution Service Procedure* <http://www.nominet.org.uk/disputes/drs/?contentId=5240> a hmotněprávní: *Dispute Resolution Service Policy* <http://www.nominet.org.uk/disputes/drs/?contentId=5239>.

aplikuje je, že je nutné vždy dokázat určitý vztah k území Velké Británie. Takovým může být například místo způsobené újmy[154] či místo, na které je činnost daného subjektu či internetová stránka alespoň zaměřena.[155] Jinak řečeno, samotné tvrzení, že dané místo na internetu lze navštívit odkudkoli není považováno za dostatečné.

4.4.3 Rozhodné právo

Vzhledem k tomu, že jde o závazkové poměry ze smluv, pro veškeré aspekty, včetně náhrady škody vzniklé porušením smluvních závazků se použijí pravidla obsažená v nařízení Řím I.[156] V případech zbylých je nutné aplikovat § 9 odst. 1 ZMPS.[157] Obojí za základní pravidlo považují možnost volby rozhodného práva, ke které může dojít také tacitně, zpravidla však smlouva s registrátorem takové ustanovení obsahují, přičemž nejčastěji je tedy právem rozhodným právo státu, ve kterém má registrátor sídlo. V případě absence volby se užije pravidlo § 10 ZMPS, tedy zásada rozumného uspořádání vztahů, podle nařízení Řím I se hovoří o místě charakteristického plnění, resp. místo, se kterým smlouva nejúžeji souvisí. V praxi se i v tomto případě dovozuje příslušnost dle sídla registrátora, jelikož ten dodává charakteristické plnění z tohoto druhu smluv.

V případě závazkových vztahů z deliktů, popř. náhrady škody je situace řešena nařízením Řím II[158] a § 15 ZMPS. Rozhodným právem dle ustanovení ZMPS je právo dle místa, kde škoda vznikla, anebo místo, kde došlo ke skutečnosti zakládající nárok na náhradu škody (tj. protiprávního jednání). To však v případě internetu může být nanejvýše složitou otázkou, nehledě na to, že je nutné určit pouze právo jedno, třebaže ke škodě mohlo dojít na území více států.[159] Z tohoto pohledu považuji za nejrozumnější přiklonit se k výkladu, že místem charakteristického jednání v případě doménových jmen bude místo, kde došlo k jeho registraci, tj. sídlo registrátora. Ačkoli v některých případech může být úžeji spojen vztah s místem a tím i právem jiným.

V případě kolize s jiným chráněným právem, např. s právem k nehmotným statkům se aplikují vždy normy toho státu, kde je právo k danému nehmotnému statku zaregistrováno nebo

[154] Bonier Media Ltd v Smith and Kestrel Trading Corporation 2002.

[155] Euromarket Designs Inc v Peter & Another 2000.

[156] Nařízení ES č. 593/2008 o právu rozhodném pro smluvní závazkové vztahy, vycházející též z Římské úmluvy z roku 1980.

[157] Zákon č. 97/1963 Sb. o mezinárodním právu soukromém a procesním.

[158] Nařízení ES č. 864/2007 o právu rozhodném pro mimosmluvní závazkové vztahy.

[159] K tomu blíže viz. Pelikánová a Čermák (2000) str. 132 a násl.

chráněno. Tak například v případě kolize s ochrannou známkou bude příslušným orgán dle místa, kde je tato známka registrována.[160]

V otázkách nekalé soutěže je situace obdobná ochraně práv k nehmotným statkům, tj. založená na zásadě teritoriality. Základní otázkou je trh (na němž došlo k porušení hospodářské soutěže), který je v daném případě dotčen. Tento je zároveň hraničním určovatelem pro stanovení, které právo je v daném vztahu rozhodné.[161]

4.4.4 Pravomoc a příslušnost soudů

Pokud je vyřešena otázka rozhodného práva, další logicky navazující problematika je, jaký soud bude příslušný a pravomocný. Na úrovni Evropské Unie se na tuto otázku vztahuje tzv. nařízení Brusel (č. 44/2001 ES) navazující na Bruselskou úmluvu o pravomoci soudů, uznání a výkonu rozhodnutí v občanských a obchodních věcech z roku 1968.[162] Základním kritériem pro určení pravomoci soudu v případě civilních deliktů je místo, kde došlo nebo může dojít ke škodné události (čl. 5 bod 3).

V případě doménových jmen je nutné také vycházet z obecného ustanovení § 37 odst. 1 ZMPS, dle kterého české soudy mají pravomoc rozhodovat majetkové spory, ve kterých je dána jejich příslušnost. Na úrovni vnitrostátních norem jí pak řeší § 9 odst. 3 písm. k) a následující OSŘ a určuje, že příslušnost bude mít obvykle krajský soud, v jehož obvodu se nachází bydliště či sídlo žalovaného, v případě práv z průmyslového vlastnictví a jejich porušení jím bude Městský soud v Praze.[163] V případě cizinců lze dovodit příslušnost i dle místa, kde se nachází dotčený majetek (§ 86 odst. 2 OSŘ), kterým se v této souvislosti považují i jiná majetková práva, tedy práva k doménovému jménu.

K otázce pravomocí je nutné zmínit také jeden z nejdůležitějších institutů v souvislosti s užíváním doménových jmen, kterým je předběžné opatření ve smyslu § 74 a násl. OSŘ. Podmínkou pro jeho vydání je nutnost zatímní úpravy poměrů účastníků řízení či existence obavy, že by výkon soudního rozhodnutí byl ohrožen. Z povahy věci a užívání internetu velmi často právě čas hraje důležitou roli. Samotné řízení může trvat delší dobu, avšak užívání či pouhá registrace doménového jména například s nekalosoutěžním úmyslem může pro žalobce

[160] Čl. 8 nařízení Řím II.

[161] Bod 21 úvodních ustanovení nařízení Řím II.

[162] Reed., Ch. a Angel., J. (2007) *Computer Law. The Law and Regulation of Information Technology*. Sixth edition. UK. Oxford: Oxford University Press. Str. 452.

[163] Zákon č. 99/1963 Sb. občanský soudní řád a § 6 odst. 1zákona č. 221/2006 Sb. o vymáhání práv z průmyslového vlastnictví.

znamenat značné nejen finanční ztráty. Nejčastěji se tudíž budou navrhovatelé domáhat zdržovacích nároků, tj. zejména zdržet se užívání doménového jména, převodu práv k němu na jinou osobu či jakýchkoli jiných právních úkonů s ním souvisejících (např. zřízení zástavního či předkupního práva k němu). Velmi důležitá je v této souvislosti formulace konkrétního nároku, která by měla postihovat pokud možno veškeré úkony, které mohou být v rozporu se zájmy žalobce, resp. navrhovatele.[164]

4.5 Závěry a vývojové tendence v oblasti doménových jmen

Z hlediska současného právního pojetí a regulace doménových jmen lze konstatovat, že současný stav není dostačující. Nejasné vymezení se týká již samotné právní povahy domény, přičemž někteří jí přiznávají povahu duševního vlastnictví, jiní však nikoli. Z povahy věci některé funkce a způsob užití velmi připomínají např. charakter ochranné známky, tudíž analogicky by se mohla některá práva považovat za absolutní obdobně jako je to u práv k jiným nehmotným statkům. Na druhou stranu absence legislativního podkladu odůvodňuje závěr některých autorů, že veškerá práva vznikají jedině na podkladě smluvním (na základě smlouvy o registraci doménového jména) a tudíž mají bez výjimky povahu relativní. V takovém případě však nikdo nemá právní nárok k jakékoli doméně a poměrně často užívaná soudní praxe přiznávat mimo jiné povinnost převodu domény na jinou osobu by neměla právní oporu. Všeobecně je však tento postup přijímán, což nasvědčuje spíše pojetí doménových jmen jako nehmotných statků, které jsou předmětem duševního vlastnictví. Bylo by však nanejvýš vhodné udělat v této otázce jasno a vyhnout se tak dalším výkladovým problémům. K tomu lze pozitivně hodnotit přístup v návrhu nového občanského zákoníku, který zařadí mimo jiné i doménová jména stejně jako jiné nehmotné statky mezi věci v právním smyslu, se kterými bude možné obdobně jako s jinými věcmi možné disponovat, vlastnit je a užívat. Zároveň je však potřeba poznamenat, že ani současný stav nečiní v rozhodovací praxi problémy a otázky kolize s jinými právy, jak bylo podrobněji popsáno, jsou řešeny poměrně ustáleně a konstantně.

Za nedostatečný stav lze považovat také fakt, že současná pravidla CZ.NIC neobsahují odkaz na UDRP ani jiné soft-law, která jsou prostředkem unifikovaného rozhodování v této oblasti, na rozdíl od jiných států a jejich národních domén. V případě národních domén .cz však zůstává realita taková, že Pravidla registrace doménových jmen v ccTLD .cz v ustanovení 13, ve kterém pouze konstatují, že držitel není oprávněn doménové jméno užívat, či umožnit jeho užívání k účelům, které jsou v rozporu s právními předpisy či právy nebo oprávněnými zájmy

[164] Liberda., A. (2008) *Předběžná opatření ve sporech o doménová jména*. [online] Přístupné na adrese <http://www.pravoit.cz/article/predbezna-opatreni-ve-sporech-o-domenova-jmena>.

třetích osob. Přičemž dále stanoví odpovědnost za škodu způsobenou sdružení CZ.NIC. Žádné ustanovení, které by např. poskytovalo výkladové vodítko v případě registrace ve zlé víře či v rozporu s jinými právy, jakou obsahují například UDRP, však v našem prostředí nenalezneme a je nutné vždy vycházet z existujících vnitrostátních právních předpisů, které se však v jednotlivých státech mohou lišit.[165] Za vhodnou alternativu lze považovat i řešení pro evropské domény .eu, jelikož nařízení zakotvuje i hmotněprávní pravidla obdobně jako UDRP.

V neposlední řadě je nutné zmínit též pozitivní vývoj týkající se rozhodování sporů ohledně doménových jmen v ADR řízení. Rozhodčí soud při HK ČR a AK ČR v Praze byl ICANN autorizován pro řešení sporů z generických doménových jmen typu .com, .org a další, čímž jeho pozice mimo jiné i na mezinárodním poli se výrazně upevnila. Kromě generických a národních domén je oprávněn rozhodovat spory ohledně domén evropských (s příponou .eu). Názory tedy, že by bylo vhodné delegovat rozhodování ohledně národních domén do místa, kde se rozhoduje i o ostatních druzích doménových jmen (jako je například WIPO), považuji tímto za neopodstatněné, protože unifikace rozhodování by měla být zaručena i u tohoto orgánu.

Zároveň ani úprava podle UDRP není bez nedostatků. Někteří autoři kritizují nedostatečné teoretické základy úpravy doménových jmen, která se tudíž omezuje pouze na úpravu některých aspektů s ohledem na problémy, které již v minulosti vyvstaly. Tak ochrana je poskytována pouze ochranným známkám a označením služeb dle čl. 4(a)i UDRP, ovšem touto cestou již nejsou řešeny kolize s jinými právy, např. se jménem fyzické osoby.[166] Bylo by vhodným nástrojem přiznat možnost arbitráže dle UDRP i v případech netýkajících se ochranných známek například pomocí obecnějších teoretických základů, čímž by se zajistila efektivní a rychlá ochrana i pro držitele jiných práv než jsou práva z ochranných známek. V tomto ohledu jsou pravidla týkající se například evropských doménových jmen (ADR rules)[167] či národních domén Velké Británie (DRS Policy)[168] širší a umožňují tak řešit způsobem alternativním také případy kolize s ostatními druhy právem chráněných jmen či označení.

---

[165] CZ.NIC (2010) *Pravidla registrace doménových jmen v ccTLD .cz* [online] <http://www.nic.cz/files/nic/doc/Pravidla_registrace_CZ_DSDng_20100101.pdf>.

[166] Lipton., D., J. (2009) *Bad Faith in Cyberspace: Grounding Domain Name Theory in Trademark, Property and Restitution.* Harvard Journal of Law and Technology [online] <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1484763> str. 25 a 26.

[167] Ve smyslu ustanovení B 1(b) (9), znění dostupné na adrese <http://eu.adr.eu/adr/adr_rules/index.php>.

[168] Ve smyslu ustanovení 2 a. i., dostupné na adrese <http://www.nominet.org.uk/disputes/drs/?contentId=5239>.

5. Ochrana soukromí a osobnosti na internetu

Dalším právním institutem, kterým je třeba se v souvislosti s internetovým prostředím zabývat, je otázka ochrany osobnosti a jejího soukromí. Internet totiž zásadním způsobem ovlivnil chování jednotlivců. Zejména s rozvojem internetových obchodů či jiných služeb, které vyžadují registraci svých uživatelů, v poslední době pak zdaleka nejvíce ohrožujícím faktorem z pohledu ochrany osobnosti a jejího soukromí je rozvoj tzv. sociálních sítí, vyvstává otázka, zda je naše osobnosti, soukromí včetně osobních údajů a dalších aspektů dostatečně a účinně chráněno i v tomto prostředí. Kromě zásadních otázek typu jurisdikce a efektivní vymahatelnosti například vůči serverům umístěným v zahraničí, tím spíše pak v třetích zemích, je nutné si položit i některé koncepční otázky. Ozývají se dokonce i názory, že v prostředí internetu nemůže rozumný člověk očekávat ochranu svých osobních údajů a soukromí, jelikož si musí být vědom rizika a otevřenosti internetové sítě. Přirovnávají tak internetovou síť k veřejnému prostranství obdobnému náměstí či veřejné ulici. Dokonce ani v případě zakódovaného přístupu (např. pomocí hesla) není podle některých rozumné a tudíž ani právně chráněné soukromí a jiné aspekty osobnosti, protože je velmi snadné takovéto způsoby bezpečnosti obejít. Na druhé straně však nelze souhlasit s touto fatalistickou tezí a rezignovat na osobností práva, na nichž mimo jiné je náš demokratický právní systém založen jen proto, že užíváme nový způsob komunikace. Následující výklad se bude zabývat různými jevy právě z hlediska ochrany osobnosti, jejího soukromí a osobních údajů.

5.1 Obecná východiska

Z obecného hlediska lze soukromí definovat jako nárok fyzických osob, skupin či institucí na určení kdy, jak a v jaké míře jsou informace o něm sdělovány ostatním. Aplikujeme-li obdobné pojetí na moderní technologii, lze konstatovat, že soukromí znamená zejména schopnost a možnost subjektu kontrolovat oběh informací o něm. [169]

Otázka soukromí a ochrany osobních údajů je čím dál více aktuální, zejména v kontextu používání internetové sítě. Velmi 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 bezpečnostních zájmů. Zejména v posledních letech lze z důvodů bezpečnostních i častého porušování práv k duševnímu vlastnictví právě pomocí internetové sítě v některých státech,

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

například v USA, Velké Británii či Francii, sledovat výrazný posun směrem od důsledné ochrany individuální osoby a její identity ve prospěch efektivního vymáhání práv a povinností v prostředí internetové sítě. 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.[170] Mezi jevy nejčastěji diskutovanými v souvislosti s ohrožováním soukromí patří 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 kontinuálního sledování a monitorování internetu a jiných elektronických sítí, aniž by byl vyžádán potřebný předchozí souhlas dotčené osoby; 3) internet může ohrozit důstojnost a společenské postavení osoby, dojde-li jeho prostřednictvím k užití či zneužití údajů získaných bez vědomí a souhlasu dotčené osoby.[171]

Hovoříme-li o institutu ochrany osobnosti, je důležité rovněž upozornit na zásadní koncepční rozdíl mezi přístupem kontinentálního právního systému a tradičního 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.[172] Vedle všeobecného osobnostního práva existují též zvláštní osobnostní práva, například práva autorů podle autorského zákona. V prostředí anglosaském však koncepce všeobecného osobnostního práva neexistuje. Proto anglosaská právní úprava, která však v některých oblastech je obdobná té naší mimo jiné i díky harmonizačním nástrojům evropské unie, se omezuje pouze na konkrétní aspekty ochrany osobnosti, prostřednictvím zvláštních druhů žalob či úpravy některých jevů zvláštními zákony.[173]

V nejobecnější rovině lze sledovat, že hlavním předmětem je nalézání vyváženosti mezi právem na informace popř. svobodu projevu (čl. 10 odst. 1 Evropské úmluvy) a právem na soukromí (jež garantuje Evropská úmluva v čl. 8). Podle evropského přístupu ani jedno z těchto

[170] 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>.

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

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

[173] K tomu blíže viz. defamation law či zákon o ochraně osobních údajů (Data Protection Act 1998).

práv však nemá prioritu. Záleží tedy vždy na konkrétním soudu, aby každý případ posoudil individuálně. Tak například tzv. osoby veřejného zájmu (např. politici, umělci, sportovci apod.) jsou nuceny strpět daleko větší míru zásahů do svého soukromí než ostatní obyvatelé, jelikož je v zájmu veřejnosti vědět o nich daleko více informací, než o jakékoli jiné soukromé osobě. To platí zejména o osobách, které zastávají důležité veřejné funkce a rozhodují o důležitých otázkách státu. Přesto ani v takovém případě nesmí zásahy přesahovat meze, kdy zájem veřejnosti již takové zásahy ospravedlnit nemůže (jedná se například o intimní sféry těchto osob).[174] Koncepce USA je příkladem, že vyváženost může být pojímána různým způsobem. Tamní soudy kladou velký důraz na neomezenou svobodu projevu, která je na rozdíl od práva na ochranu soukromí, výslovně garantována tamní ústavou. O interpretaci směrem k co nejširší ochraně svobody projevu píše i doc. Herceg v kontextu šíření rasistických či extremistických myšlenek. Uvádí, že dokonce i v případě této kriminální činnosti je v popředí svoboda slova s tím, že její omezení je přípustné pouze tehdy, když násilí nebo porušení práva skutečně bezprostředně hrozí.[175] Mates nato uvádí, že dle vyjádření tamního Nejvyššího soudu nelze například u politiků rozlišovat mezi soukromým a veřejným životem.[176]

Pro detailnější pochopení znění článku 8 Evropské úmluvy lze uvést, že původně bylo určeno k poskytnutí ochrany soukromých osob před státem. Jeho význam se zvýšil také v důsledku zkušeností z Východního bloku (z období studené války), kdy státní aparáty shromažďovaly detailní informace o každém obyvateli a ty následně různými způsoby zneužívaly.[177] Zejména tedy 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, že dnešní společnost „slepě kráčí do společnosti plně sledované“.[178] Digitální prostředí totiž umožňuje snadný přístup, shromažďování i udržování osobních údajů, které mohou být a také bývají použity k různým i protiprávním účelům. Jednotlivé databáze bývají kombinovány, čímž lze ve výsledku získat velmi podrobnou představu o požadované osobě. Informace mají také velký obchodní význam.

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

[175] 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.

[176] 2006, str. 28 a 29.

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

[178] Edwards a Waelde 2009, str. 448.

Pomocí nich se lze například zaměřit na určitý okruh osob při marketingové kampani či sestavování obchodních projektů. Právní normy se snaží na tento negativní jev reagovat regulací. A to zejména jaké údaje lze shromažďovat, po jakou dobu, za jakým účelem. Více podrobností bude uvedeno v části týkající se ochrany osobních údajů.

Pokud však jde o trend současného vývoje, je rovněž důležité si povšimnout, že ochrana osobnosti díky různým okolnostem je potlačována a zdaleka není v popředí veřejných zájmů. Zásadní událostí, v jejímž důsledku je důraz na ochranu jednotlivců a jejich soukromí zatlačován do pozadí, byl teroristický útoku 11. září 2001 na USA. V jeho důsledku a ve jménu boje proti terorismu, ty státy, které jsou událostí nejvíce dotčeny (USA a UK), kladou výrazně vyšší důraz na bezpečnost státu a předcházení trestné činnosti. Kromě toho také opatření, jejichž účelem je zajistit vyšší právní jistotu a efektivitu právní regulace v internetovém prostředí (například v souvislosti s trestněprávní problematikou nebo s ochranou práv k duševnímu vlastnictví), mají poměrně zásadní dopad na omezování ochrany soukromí a zpracování osobních údajů internetových uživatelů.

5.2 Ochrana soukromí a svoboda slova

Ochrana soukromí i svoboda slova se řadí mezi základní lidská práva, která jsou garantována v podstatě všemi dokumenty týkajícími se ochrany lidských práv a svobod ať na úrovni mezinárodní, evropské či vnitrostátní. Například univerzální deklarace lidských práv 1948 ve svém článku 12 zaručuje právo na ochranu svého soukromí i osobnosti. Článek 19 potom deklaruje každému, že má právo na svobodu slova a právo na informace bez ohledu na státní hranice. Obdobně je také otázka upravena v Evropské úmluvě o ochraně lidských práv a základních svobod 1950 (též Evropská úmluva) v článku 8 a 10. Jak je však patrné, tyto svobody se mohou vzájemně střetávat a v konkrétním případě je třeba dát přednost některé z nich. V prostředí internetu je situace o to komplikovanější, že díky globální povaze internetu se do vztahů i střetů dostávají lidé a subjekty z různých částí světa, kde může ono požadované vyvážení být posuzováno odlišně. Otázka mezinárodní unifikace a spolupráce při vymáhání práv a cizích rozhodnutí tudíž nabývá na důležitosti.

Jak již bylo konstatováno v této práci, Spojené státy americké velmi dbají na ochranu svobody slova, kterou jim také zaručuje první dodatek ústavy. Soudy ve velké většině případů upřednostňují právě tuto svobodu před ostatními právy včetně práv na ochranu osobnosti či soukromí. Mimo jiné i proto Nejvyšší soud díky případu ALCU v Reno v roce 1996 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 příliš extenzivnímu a nepřípustnému omezení svobody slova.[179] Toto pojetí se promítá i do případného uznávání a vymáhání cizích soudních rozhodnutí. Obdobně byl také prohlášen za nepřípustný koncept (mimo jiné i z finančních důvodů), podle kterého by ISPs měli kontrolovat obsah přenášených dat a pod hrozbou nepřímé odpovědnosti jej cenzurovali.

Restriktivní postoj byl hájen v sledovaném případu v Německu, European Commission Communication, Illegal and harmufl content on the Internet v roce 1999.[180] Jednalo se o evropskou iniciativu ve prospěch zavedení nové metody regulace protiprávního obsahu internetu uvalením určitých povinností na ISPs. Podle toho by měli povinnost blokovat své zákazníky v přístupu k nezákonnému obsahu internetu na bázi jednotlivých případů (například určité stránky, apod.). V daném případě došlo k požadavku ze strany německých státních zástupců, aby ISPs blokovali přístup k určitým stránkám hostovaným serverem v Nizozemí, který údajně podporoval terorismus. Ovšem blokace by znamenala zablokování přístupu ke všem stránkám tohoto serveru, tedy i k těm, které byly v souladu se zákony. Proto ze strany nizozemské společnosti došlo k žalobě na porušení svobody poskytování služeb v rámci zemí EU.[181]

V rámci právního systému České republiky je svoboda projevu i práva na informace zaručena v čl. 17 odst. 1 a násl. Listiny základních práv a svobod. Avšak podle odst. 4 téhož článku může dojít k zákonnému omezení při nezbytnosti pro ochranu práv a svobod druhých, bezpečnost státu, veřejnou bezpečnost, ochranu veřejného zdraví a mravnosti. Jak je vidět, pojetí v našem právu je velmi obdobné evropskému, přičemž nelze jedno právo či svobodu nadřadit druhému.

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 nikoli (např. němečtí příznivci nacismu

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

[180] COM(96)0487 – C4-(0592/96).

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

užívají a diskutují fašismus a své názory prostřednictvím stránek hostovaných serverem v USA či Kanadě, protože jejich jednání je trestné podle německého trestního práva).[182]

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. Hovoříme-li zároveň o omezení práva na soukromí, je nezbytné odlišit dva druhy vztahů, při kterých k omezení dochází. Jednak jde o vztahy vertikální povahy, kdy soukromá osoba jedná ve vztahu k orgánu veřejné moci při realizaci jeho pravomocí. Soukromá osoba se nemůže dovolávat ochrany svého soukromí, je-li toto omezení vykonáváno na základě a v rámci zákonného zmocnění. Problematičtější jsou však vztahy mezi osobami stejného postavení, tedy ve vztazích horizontální povahy (mezi osobami stejného postavení).[183]

Z pohledu ochrany soukromí je v internetovém prostředí zřejmě nejdůležitějším institut zpracování a jiné nakládání s osobními údaji. 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.[184] 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.[185] Důležitým následným krokem je snaha o unifikovaný přístup a spolupráci s USA. Ministerstvo financí USA sestavilo základní principy tzv. bezpečného

[182] Reed 2004, str. 261.

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

[184] 2004, str. 263.

[185] o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (též z anglického znění označována jako DPD).

přístavu, safe harbor, (území EU a USA) v roce 1999, které reagují a v podstatě odráží základní principy směrnice.[186] 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, jelikož výklad slova zpracování a tím i místo kde k němu dochází je poměrně široký. Společnost Microsoft měla 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.[187]

5.3 Ochrana osobnosti v českém právním řádu

Nejobecnější právní úprava ochrany osobnosti je obsažena v Listině základních práv a svobod, která je východiskem pro navazující veřejnoprávní i soukromoprávní zákonnou úpravu.[188] Základem všeobecné soukromoprávní úpravy je pak hlava druhá zákona č. 40/1964 Sb., občanského zákoníku (dále jen OZ). V kontextu internetu je 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 (dále též ZOOU), jehož porušení může mít i trestněprávní důsledky.

Hovoříme-li o ochraně osobnosti, je důležité si též uvědomovat, jaké prostředky lze k ochraně využít. Bránit se lze zejména svépomocí, dožadováním se ochrany u orgánu státní správy a samozřejmě též prostřednictvím soudu. V případě osobních údajů vedle těchto prostředků existuje také institucionální ochrana poskytovaná Úřadem pro ochranu osobních údajů a zvláštní prostředky soudní ochrany podle ZOOU, ke které je příslušný obecný, okresní soud. Kromě těchto standardních prostředků lze samozřejmě žádat případnou ochranu i pomocí

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

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

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

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 vnitrostátních ochranných prostředků existuje také systém ochrany podle Evropské úmluvy a jejího protokolu č. 11, k němuž je příslušný Evropský soud pro lidská práva. Navíc významnou úlohu může hrát také činnost Veřejného ochránce práv.[189]

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.[190]

Zejména pokud jde o svolení, je důležité mít na zřeteli, že jde o právní úkon, který musí splňovat veškeré obecné náležitosti. Musí tedy být učiněn způsobilou osobou, jejíž vůle byla projevena svobodně, vážně, určitě a srozumitelně, při současné absenci omylu, a nikoli v tísni za nápadně nevýhodných podmínek. Zároveň nesmí být svolení ani v rozporu se zákonem, obcházet jej nebo se příčit dobrým mravům.[191] 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.

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

[190] § 12 odst. 3 OZ.

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

5.3.1 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, které zahrnují možnosti domáhat se uložení povinnosti upuštění od neoprávněného zásahu (povinnost zabraňovací), odstranit jeho následky (povinnost odstraňovací), či poskytnout přiměřené zadostiučinění (morální či peněžité – povinnost satisfakční). 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.[192] Nelze se tedy 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. Z uvedeného tak vyplývá, že finanční kompenzaci lez ve většině případů žádat jako 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, která však v případě nemajetkové újmy může být méně intenzivní. Postačí totiž, dojde-li k pouhému ohrožení fyzické či morální integrity dotčené fyzické osoby. Postihována nemají být pouze taková jednání, která jsou svojí povahou přiměřená a odpovídající demokratické společnosti.[193] 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

[192] Knap, K. 2004, str. 146.

[193] Ibid. str. 150 a 151.

sankčního požadavku. Musí se jednat o zásah neoprávněný (tedy bez svolení dotčené osoby či mimo zákonné licence) s nímž je vzniklá újma prokazatelně v přímé souvislosti. Občanský zákoník poskytuje též 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 sféry, nebo též citlivých údajů. V takovém případě i pravdivé tvrzení představuje zásah protiprávní. Smyslem je totiž vyváženost veřejného zájmu a legitimního práva na informace s ochranou osobní sféry dotčené osoby. Nelze tedy rozumně odůvodnit veřejným zájmem právě zásah do intimních záležitostí dotčené osoby.

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,[194] předběžná opatření,[195] zvláštní žaloby (viz. dále) a žaloba na náhradu škody.[196] Knap uvádí, že výčet ochranných nástrojů v § 13 OZ je demonstrativní, proto se lze žalobou domáhat i jiných výroků, například konstatování nepravdivosti daného tvrzení.[197] Kromě toho si lze představit i obchodněprávní žaloby na ochranu obchodního tajemství podle § 18 n. ObchZ[198] 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.

[194] Smírčí řízení podle § 67 n. OZ.

[195] § 74 OZ.

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

[197] Ibid. str. 174.

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

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.[199]

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 věcech věc postoupí k jednání a rozhodnutí příslušnému okresnímu soudu.[200] Navíc podle § 100 odst. 2 OZ je nutné mít na paměti, že všeobecná osobnostní práva jsou nepromlčitelná.

Kromě ostatního může protiprávní zásah do osobnostních práv naplnit také znaky některého z trestných činů. Jedná se 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.

Podle § 180 TZ 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.

Trestné je také porušování tajemství dopravovaných zpráv podle § 182 TZ. Chráněným objektem je zde tajemství zpráv jakékoli povahy. Jedná se tedy jak o písemnosti, tak o jiný druh záznamů, například zvukových, obrazových, datových, zasílaných poštou či jiným způsobem. Dotýká se to i zpráv podávaných telefonem nebo prostřednictvím sítě elektronických komunikací, kam patří zejména počítačová síť. Podle § 183 TZ je pak ochrana poskytnuta i dokumentům, jsou pouze uchovávány v soukromí, aniž by docházelo k jejich přepravě. 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 trestný čin je naplněn až jeho zveřejněním, zpřístupněním či použitím jiným způsobem.

S otázkou tajemství dopravovaných zpráv ještě úzce souvisí velmi diskutovaný vyšetřovací prostředek, odposlouchávání a záznam telekomunikačního provozu. Ten je dovolen

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

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

pouze za podmínek § 86 až 87c TŘ. Obdobně může být též přípustné sledování osob a věcí podle § 158d odst. 3, 4 TŘ, a případná kontrola písemného styku, kterou provádí k tomu povolané orgány. Kromě zmocnění podle trestního řádu může také dojít k omezení zásahem BIS (Bezpečnostní a informační služba) podle ustanovení § 7 až 12 zákona č. 154/1994 Sb., o Bezpečnostní informační službě, anebo složkami zpravodajského či vojenského zpravodajství.[201] Kromě toho může zákonně, za stanovených podmínek, zasáhnout do tajemství dopravovaných zpráv či užít operativně pátracích prostředků orgán provádějící celní dohled, v režimu zákona č. 337/1992 Sb., o správě daní a poplatků.

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 (v takovém případě by se nejednalo o pomluvu), třebaže byl sdělen v úmyslu ohrozit vážnost jiného u spoluobčanů.[202]

Jak již bylo zmíněno na začátku kapitoly, v anglosaském právním systému, zejména 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 regulováno obdobně, 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).

5.4 Law of Defamation

Jak již bylo uvedeno v úvodu této kapitoly, angloamerický právní systém nezná pojem všeobecného osobnostního práva. Jednotlivé aspekty ochrany osobnosti jsou tak právně upraveny specifickými instituty. Vedle výše upravené ochrany osobních údajů, kterou mimo jiné zavedla v případě Velké Británie právní úprava evropská, je nejznámějším institutem tamní

[201] § 18 zákona č. 153/1994 Sb., o zpravodajských službách České republiky, § 7 až 15 zákona č. 289/2005 Sb., o Vojenském zpravodajství.

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

právní úprava ochrany cti, váženosti a společenského postavení fyzické osoby. Jedná se o poměrně samostatný právní koncept nazývaný též Law of Defamation, nebo jen zkráceně defamation. Základy úprava pochází z nepsaného common law (jeho základem jsou právní pravidla vytvořená soudní praxí), která je v posledních letech nově upravována a konkretizována pomocí psaných zákonných předpisů. Příkladem je zákon o urážce na cti, Defamation Act z roku 1996 (dále jen DA). Pozornost je mimo jiné věnována urážce na cti (pomluvě) způsobené pomocí internetu, jenž je velmi snadným nástrojem, například ve formě různých blogů, emailů či internetových stránek. V prostředí internetu je pak úprava zaměřena na pomluvu v trvalé podobě, tedy psané, a ulehčila postavení žalobce tím, že tento nemusí dokazovat utrpěnou škodu nebo jinou újmu, ale tato újma je právně presumována.[203] 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).

Pojem uveřejnění někdy 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 dané informace třetí osobou. Proto při rozhodování soudu může hrát roli mimo jiné i pravděpodobnost, že daná stránka byla navštívena osobou jinou než žalobcem samotným, a tudíž naplnila znaky uveřejnění v tomto smyslu.[204] Uveřejnění však například splňuje třeba jen jediná emailová zpráva adresovaná třetí osobě, jak bylo rozhodnuto například v případě Slipper v BBC [1990] 1 All ER 165.

Právní úprava v UK navíc vychází z pojetí, že každé jednotlivé uveřejnění je novým žalobním titulem, tedy například každý jednotlivý přístup a přečtení dané informace zakládá nové právo a lhůtu k uplatnění žalobního nároku. Jinak je to v případě USA, kde právo aplikuje pravidlo tzv. prvního uveřejnění, tedy žalovatelné je pouze první uveřejnění defamující (urážlivé) zprávy.[205] Důležitým procesním důsledkem je zejména okamžik počátku běhu lhůty k podání případné žaloby. 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.

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

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

[205] 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. Žalobcem ve valné většině případů je sama osoba, jejíž pověst utrpěla daným výrokem újmu.

Za defamující výrok je zásadně 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.[206]

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[207] 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.[208] 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.

Kromě autora a jeho zaměstnavatele může být sekundárně odpovědným i poskytovatel informačních služeb (ISPs), kteří se na uveřejnění urážlivého výroku aktivně podíleli. Ten 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 způsobilo nebo napomohlo uveřejnění urážlivého výroku.[209] 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

[206] Lloyd 2008, str. 577.

[207] [1997] IRLR 471.

[208] Lloyd 2008, str. 577.

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

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.[210] Směrnice o elektronickém obchodu[211] poskytuje ještě další výjimky z odpovědnosti ISPs ve svém článku 12. 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).[212] V UK byla tato ustanovení provedena v paragrafu 19,[213] 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.[214] Obdobné pojetí je zakotveno i v našem právním řádu zákonem č. 480/2004 Sb., o některých službách informační společnosti, konkrétně v jeho ustanovení § 3 až § 6.

Úzce související je též otázka, které národní právo se v případě vztahů s mezinárodním prvkem aplikuje. V rámci Evropy jí řeší článek 5(3) Bruselské úmluvy, 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. [215] Wild k tomu 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 (např. z důvodu již zmíněné presumované újmy).

[210] Reed 2004, str. 114.

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

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

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

[214] Lloyd 2008, str. 583.

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

V případě internetu řešil otázku jurisdikce australský odvolací soud v rozhodnutí Gutnik v Dow Jones [2002] HCA 2002, který shledal odpovědným deník, který byl sice publikovaný jen na území New Yersey, ovšem díky globální přístupnosti internetového serveru byla dovozena i jurisdikce australského soudu. K uveřejněnému článku se navíc velmi rychle přidalo 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.[216]

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.[217] 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).

5.5 Ochrana osobních údajů

Institut ochrany osobních údajů je diskutovaný v prostředí internetové sítě velmi často. Právě údaje, jiným slovem též jakékoliv informace o konkrétní osobě, jsou nástrojem, který bývá používán pro porušování osobnostních práv prostřednictvím internetové sítě zřejmě nejvíce. Podstata sítě je přece přenos informací jakéhokoli druhu. Proto také z pohledu ochrany osobnosti a jejího soukromí je logicky největší obava z porušování předpisů o získávání, přenosu, uchovávání a jiném nakládání s údaji osobní, tím více pak citlivé povahy. V ústředí této problematiky jsou tak otázky typu. 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 dále nakládat?

Rozlišit lze dva právní aspekty ochrany osobních údajů. V pozitivním slova smyslu, kdy jsou v souvislosti s ochranou osobních údajů a soukromí zaručena určitá pozitivní práva subjektu osobních údajů (například právo na informace). V negativním smyslu jde o práva na to, aby nebylo zasahováno do určitých soukromých oblastí a informací o daném subjektu. Jde například o právo ochrany důvěrných informací.

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

[217] [1995] All ER (EC) 289.

5.4.1 Základy a vývoj právní ochrany osobních údajů

Ochrana osobních údajů je nedílnou součástí práva na ochranu soukromí, které bylo zakotveno již článkem 12 Všeobecné deklarace lidských práv z roku 1948. Podle jeho znění se zakazuje svévolné zasahování do soukromého života, do rodiny, domova nebo korespondence. Dále se zakazují též útoky na čest a pověst. Přičemž každý má právo na ochranu proti takovým útokům a zásahům. Závazného vyjádření se pak dostalo v 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 lze zásahy považovat za oprávněné. Přičemž u všech výjimek musí být zachována zásada nezbytnosti, zákonnosti a předpokládaného účelu. Jinými slovy, každý zásah do soukromé sféry fyzické osoby musí být v souladu se zákonem, musí být nezbytný, a musí být pro daný účel. Tím mlže být zájem národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, předcházení nepokojům a zločinnosti, ochrany zdraví či morálky nebo ochrany práv a svobod jiných.

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[218] 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,[219] 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, nebo jen DPD), která se stala základním harmonizačním prostředkem národních úprav evropských států. Dalším právně závazným dokumentem pojednávajícím také o soukromí a ochraně osobních údajů je Charta základních práv EU z roku 2000.

[218] Organizace pro hospodářskou spolupráci a rozvoj.

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

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.

V zákonné rovině je potom úprava v ČR vyjádřena zákonem č. 101/2000 Sb. o ochraně osobních údajů (dále jen ZOOU), který zejména zapracovává a provádí příslušné evropské směrnice. Na jeho základě byl také zřízen zvláštní dozorčí orgán, Úřad na ochranu osobních údajů ve smyslu § 2 ZOOU (dále též Úřad). Zákon se věcně vztahuje na veškeré zpracovávání osobních údajů (§ 3 ZOOÚ), bez ohledu na to, zda jsou tyto údaje zpracovávány automaticky či ručně (manuálně), anebo kdo tyto údaje zpracovává (zda veřejný orgán či soukromá osoba). Výjimkou jsou pouze případy, 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 (třeba pro reklamní účely).[220] 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).

Obdobné pojetí bylo přijato i na území Spojeného království (UK). Základním zákonem, který mimo jiné provedl i směrnici DPD je Data Protection Act z roku 1998 (dále též DPA). Poměrně zajímavá je otázka jeho působnosti, která je vykládána velmi široce. DPA je aplikovatelný na všechny správce osobních údajů, jež jsou založeni podle předpisů Velké Británie 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.[221] Půjde typicky o příklad mezinárodní společnosti, která působí na území UK, ačkoli její management a

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

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

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 kancelář, pobočku nebo běžnou praxi na území UK. V takovém případě nezáleží na místě, kde jsou data zpracovávána nebo kde se nacházejí.[222] Jako dozorčí orgán byl ustanoven úřad Komisaře pro ochranu osobních údajů (dále též ICO).[223]

5.4.2 Obecné otázky a pojmy

Obecná definice osobních údajů vychází z pojetí směrnice DPD. Proto se rozlišují dvě kategorie osobních údajů, a to obecné a citlivé. Přičemž subjektem osobních údajů může být jedině fyzická osoba. Za osobní údaj se tak považuje jakákoli informace, ze které lze přímo či nepřímo identifikovat subjekt těchto údajů. Nejde však o ty případy, kdy ke zjištění identity dotčené osoby je třeba nepřiměřené množství času, úsilí či prostředků.[224]

S informacemi nepřímo identifikujícími může být výkladový problém. Proto jednotlivé národní orgány přispívají k jednotnému výkladu svými stanovisky. Tak například ICO ve Velké Británii vydává výkladové směrnice.[225] Právně závazný výklad však provádí zejména soudní orgány. Takto se tamní 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 DPA. 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 úprava dotýká.

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 veškeré údaje a hesla vyhledávaná právě pomocí jejich služby, bez dalšího omezení.[226] Důkazem

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

[223] The Information Commissioner's Office.

[224] Knap, P. 2004, str. 398.

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

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

budiž, že až do nedávna společnost Google shromažďovala tyto údaje po neomezenou dobu. Od roku 2007 souhlasila 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.[227]

Obdobně je tomu 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 tomu tak bude. V jiném případě, například ball.pen@yahoo.com, však tak jasná situace není. Postupně se i v této věci aplikuje poměrně extenzivní výklad, že obecně všechny emailové adresy spadají do kategorie osobních údajů a podle toho je s nimi nutné nakládat.[228]

Stručně lze říci, že k nakládání s těmito údaji je zásadně nezbytný souhlas osoby, které se tato data týkají, přičemž mimo jiné musí být zachovány i další zásady, např. rozsah údajů pouze nezbytný pro konkrétní účel (například k plnění smluvního vztahu, výkonu práv a povinností, pro výkon veřejné moci nebo jiný legitimní účel).[229]

Druhou skupinu pak tvoří osobní údaje směrnicí DPD klasifikované jako zvláštní kategorie údajů, u nás označované za citlivé. Jedná se o údaje týkající se národnosti, rasového nebo etnického původu, politických názorů, členství v odborových organizacích, náboženského vyznání, filozofického přesvědčení, odsouzení za trestný čin, psychického nebo fyzického stavu, sexuálního života (čl. 8 bod 1. DPD). Na adresu definice citlivých dat byla adresována kritika například, že nezahrnuje biometrické či genetické údaje, jako například otisky prstů či DNA. Naše úprava však i tyto údaje za citlivé označuje v § 4 písm. b) ZOOU. Uvedený výčet je taxativní, tedy například údaje o majetkových poměrech nespadají do této kategorie.

V případě emailových adres není zcela jasné, zda například adresa obsahující další, povahou citlivý údaj, spadá do této kategorie. Půjde například o adresu petr.novak@homosexualni_organizace.cz. Pokud však vyjdeme z uvedených definic, jde o údaj, ze kterého je osoba dokonce přímo identifikovatelná, a navíc se týká i jejího sexuálního života. Tudíž by měla takové informace být užívána jedině v režimu citlivých osobních údajů.

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

[228] Carey 2004, str. 233.

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

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.[230]

Pro nakládání s osobními údaji se používá obecný termín zpracování (z angl. processing) osobních údajů, který je vykládán velmi široce a zahrnuje jakýkoli způsob zpracování, ať již jde o automatizovaný nebo neautomatizovaný.[231] Zpracování znamená veškeré činnosti jako přijímání, nahrávání či držení osobních údajů, provádění jakýchkoli operací jako organizace, změna, kombinování, užívání, poskytování, převádění, nebo také jejich zničení či výmaz. Výčet je v tomto případě demonstrativní, proto každé systematické nakládání s osobními údaji je zpracováním ve smyslu právní úpravy osobních údajů.[232]

Toto velmi široké pojetí bylo užito i v poněkud kontroverzním soudním případě Lindqvist. Žalovaná 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), byla odmítnuta s tím, že došlo k publikaci na internetu, což vlastně znamená zpřístupnění neomezenému počtu lidí. ESD tím v podstatě vyložil termín zpracování tak, že každá osoba uveřejňující údaje na blogu, prostřednictvím aplikace Facebook a podobně spadá do režimu směrnice 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).[233]

Subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj, se nazývá správce. Ten může zpracováním pověřit zpracovatele, přesto však

[230] Tak uvádí čl. 8 odst. 2 směrnice o DPD.

[231] 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, DPD).

[232] Obdobné pojetí zakotvuje i náše úprava v § 4 písm. e) ZOOU.

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

primárně odpovědným zůstává správce. 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.

Základní povinností správce je zejména stanovit účel zpracování osobních údajů, jež nelze libovolně v průběhu měnit podle § 5 odst. 1 ZOOÚ, a podle toho i prostředky a způsob, jak bude proces zpracovávání probíhat. 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 DPD, obdobně, jako tomu je například v DPA ve Velké Británii. Blíže k těmto povinnostem bude pojednáno u jednotlivých zásad.

Vedle obecné úpravy jsou také stanoveny přípravy, kdy lze práva a povinnosti z této právní úpravy omezit či zcela vyloučit. Systém výjimek, který v podstatě zakotvuje již Evropská konvence o lidských právech, konstatuje též směrnice DPD. Jde totiž o případy, kdy je v sázce bezpečnost státu, jeho obrana, veřejný pořádek a vnitřní bezpečnost, z trestněprávních důvodů nebo je-li to třeba z důvodu ochrany subjektu údajů nebo práv a svobod druhých (článek 13 DPD). ZOOU tyto výjimky zakotvuje a upřesňuje v § 3 odst. 6. Mezi ně též spadá například velmi rozšířený způsob sledování lidí ve Velké Británii, tzv. CCTV videokamery, jejichž úkolem je monitorování a sledování téměř veškerých veřejných míst (ovšem v mnohých případech nejen těch) právě z důvodů předcházení a odhalování trestné činnosti.

Za značné ohrožení a tudíž i otázku, kterou se zabývá směrnice v článku 25, se považuje předávání osobních údajů do třetích zemí. Obecně platí zásada volného pohybu osobních údajů v rámci zemí EHS, kde standardy ochrany a nakládání s osobními údaji jsou srovnatelné. Má-li však dojít k předání údajů do třetí země, je to 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.[234] 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

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

dohodnuta zvláštní dohoda o tzv. bezpečném přístavu – „safe harbor“.[235] V této souvislosti je důležité také rozhodnutí (Evropského Soudního Dvora) ESD Lindqvist[236], ve kterém soud vyložil, 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. Naše úprava také převzala evropský režim předávání údajů mimo území členských států EHS, přičemž je nutné nejprve požádat Úřad na ochranu osobních údajů (dále též Úřad či ÚOOÚ) o povolení. Ten zejména posoudí, zda jsou údaje dostatečně zabezpečeny a zda je s nimi nakládáno tak, aby nedošlo k újmě subjektu údajů.

Dojde-li k porušení povinností vyplývajících z právní úpravy ochrany osobních údajů, hlavním garantem a tím, kdo by měl autoritativně zjednat nápravu je orgán dozoru. V naší právní úpravě je zaručena ochrana individuálních práv subjektů ve zvláštní části ZOOU. Dotčený se může obrátit na Úřad a žádat zajištění nápravy v případě nezákonného zpracovávání údajů o něm. Zároveň může přímo na správci, popř. zpracovateli, požadovat vysvětlení a případné napravení vzniklého stavu (např. opravou, doplněním, blokací či likvidací údajů). Samozřejmě vedle těchto možností může také využít obecné občanskoprávní úpravy, a to zejména, došlo-li ke vzniku nemajetkové újmy (podle § 13 OZ). Za majetkovou škodu, stejně jako za jiné porušení povinností podle ZOOU, odpovídají správce a zpracovatel solidárně. Navíc je podle trestního zákona též kvalifikované (je-li způsobena vážná újma) neoprávněné nakládání s osobními údaji označeno za trestný čin.[237] Odst. 3 § 180 TZ potom považuje spáchání tohoto trestného činu veřejně přístupnou počítačovou sítí za důvod pro vyšší trestní sazbu, jelikož je to z povahy věci velmi účinný způsob (obdobně, jako třeba veřejná média typu rádia, televize či tisk).

V případě Velké Británie hraje aktivní roli při dohledu a vymáhání dodržování předpisů na ochranu osobních údajů Komisař (dále jen ICO). Existuje-li podezření z porušení zákona, ICO nejprve upozorní toho, kdo se porušení dopustil, tzv. informačním upozorněním, a zároveň jej vyzve k nápravě a dodržování principů zpracování osobních údajů. V případě, nedojde-li k nápravě ani přes tuto výzvu, může ICO vznést žalobu k příslušnému soudu, přičemž již samotné neuposlechnutí předchozích výzev je považováno za trestný čin.[238] Navíc od roku 2008

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

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

[237] § 180 zákona č. 40/2009 Sb., trestní zákoník.

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

může ICO uložit i pokuty aniž by musel věc předkládat soudu.[239] 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 jeden z důvodů poměrně častého nedodržování zákonné úpravy.[240]

Týká-li se však protiprávní jednání soukromého sektoru, za jedna z nejúčinnějších opatření lze považovat ta, která se dotýkají pověsti a důvěryhodnosti podnikatele, který nedodržuje zákonné povinnosti při zpracování osobních údajů. Proto jednou z reforem by podle dalších návrhů měla být současná povinnost nebo alespoň možnost žádat uveřejnění informace či rozhodnutí o tom, že určitá společnost nebo subjekt porušuje tyto povinnosti (což je již běžné ve Spojených Státech či Japonsku). Takové opatření by se mělo týkat zejména sektoru elektronických komunikací.[241] 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 rozsáhlému zpracovávání osobních údajů. Takové upřednostnění osob nevyužívajících elektronické sítě se jim jeví jako nespravedlivé. K tomu lze dodat, že takové nástroje mohou být účinné, a není důvod je omezovat pouze na elektronické komunikace. Možnost uveřejnění či oznámení rozhodnutí o porušování zásad zpracování osobních údajů může zvýšit účinnost a ve výsledku též dodržování těchto právních předpisů.

5.4.3 Základní zásady

Obecná východiska, jež se promítají do právní úpravy mezinárodní, evropské i vnitrostátní ve formě základních zásad ochrany osobních údajů, byly v evropské oblasti zakotveny tzv. Úmluvou č. 108 a v podstatě v nezměněné podobě jsou přebírány i do ostatních předpisů.[242] Jedná se o principy: 1. princip zákonnosti zpracování (zpracovávané osobní údaje musí být

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

[240] 2009, str. 470.

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

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

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 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).[243]

Princip zákonnosti je zároveň zdůrazněn v článku 6 odst. 1 písm. a) směrnice DPD. Ten uvádí, že osobní údaje mají být zpracovány korektně a zákonným způsobem. V této souvislosti je zásadním pravidlem, že ke zpracování (tedy již k zisku) osobních údajů je zásadně nutný souhlas dotčené osoby. Souhlas není třeba pouze ve 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. Základní případy vyplývají z článku 7 téže směrnice, v našem případě pak z § 5 odst. 2 ZOOU.

Otázka souhlasu nemusí být vždy zcela jednoznačná. Souhlas se vyžaduje svobodný, vědomý a informovaný, přičemž písemná forma vyžadována není. 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 zvláštního zákona. Nejdůležitější výjimkou ze souhlasu je ale případ, kdy subjekt sám tyto údaje zveřejnil, čímž se

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

vzdal svého soukromí. Nadále pak lze takové údaje zpracovávat bez jeho předchozího souhlasu.[244] Správce či zpracovatel (mají stejné povinnosti) musí dbát na zachování důstojnosti subjektu údajů a na tom, aby mu nevznikla jiná újma. Zajímavá je též otázka věku dostatečného pro tento souhlas. Například ve Skotsku zákon určuje, že dítě může dát takový souhlas v případě, pokud je schopné obecného porozumění takového úkonu. Za takovou se presumuje osoba starší 12 let.[245]

V případě elektronické komunikace poměrně často vznikají situace, kdy není zcela zřejmé, zda lze určité praktiky považovat za zákonné nebo již hranici překračující. 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.[246] 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. Obdobně například v případě internetových sociálních sítí (např. Facebook) se v praxi ukazuje, že nezbytnost souhlasu není příliš efektivní podmínkou. Každý při registraci přijímá všeobecné podmínky, ve kterých je obdobný souhlas inkorporován. Uživatel, aniž by předem zvažoval jakékoli důsledky, tak zákonem požadovaný souhlas vyslovuje. Pouze v případě citlivých údajů je třeba souhlasu výslovného (např. dle čl. 8 odst. 2 písm. a) DPD), tudíž jejich prostá inkorporace do obchodních či jiných podmínek nemůže být dostatečná.

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. Navíc zásada nezbytnosti je poměrně nejasný a nedefinovaný pojem.

Pro posouzení zákonnosti zpracování je zároveň 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

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

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

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

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.[247]

Za legitimní důvod zjišťování osobních údajů je v poslední době považováno zjišťování uživatelů stahujících materiály v rozporu s autorskými právy, jako například v soudním případě Promusicae.[248] Evropský soudní dvůr odmítl ochranu soukromí internetových uživatelů ve prospěch zábavního průmyslu, který tehdy podnikl nezbytné kroky ke zjištění totožnosti osob porušujících jejich práva k duševnímu vlastnictví.

Zásada účelnosti znamená, že zpracovávat lze údaje pouze pro konkrétní účel. Tak například 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. O konkrétním účelu musí být mimo jiné každý informován při udělování souhlasu se zpracováním, případně též kdykoli o tuto informaci správce či zpracovatele požádá.[249] Účel zpracování musí být také oznámen dohlížejícímu orgánu, který jej zanese do registru.[250]

Zásada časového omezení znamená, že údaje mohou být uchovávány pouze po dobu, která je nezbytná k účelu jejich zpracování. Takto je princip pospán i v naší úpravě, konkrétně v ustanovení § 5 odst. 2 písm. e) ZOOU. Z každého pravidla existují výjimky, proto i zde pro statistické, vědecké či archivnické účely je možné při zachování ochrany před neoprávněným zasahováním do soukromého a osobního života údaje zpracovávat po delší dobu. I zde souvisí časové omezení s informovaným souhlasem, jelikož každý by měl být před udělením souhlasu zároveň informován o době, po kterou budou údaje zpracovávány. Otázka časová je samozřejmě poměrně citlivá, jelikož čím dál více přibývá případů a obav například v souvislosti se sociálními sítěmi či jiným druhem využívání internetu jako komunikačního nástroje, který mimo jiné též přenáší a uchovává mnohé i velmi citlivé osobní údaje. Může se totiž stát, že například údaje

[247] Lloyd 2008, str. 97.

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

[249] § 12 odst. 2 písm. a) ZOOU.

[250] § 16 odst. 2 písm. b) ve spojení s § 35 odst. 1 ZOOU.

formou fotografií, které následně uživatel vymaže, zůstanou uchovány na serveru samotném, případně již byly nějakým jiným způsobem použity, a tím můžou danou osobu pronásledovat a případně způsobit újmu v budoucnosti. I proto je tato otázka zakotvena, a to nejen v souvislosti s osobními údaji, ale též například jim poměrně blízké údaje o komunikaci, jak bude blíže popsáno v jiné části této práce. Platí zároveň pravidlo, že i v případě výjimek by mělo při delším zpracování dojít co nejdříve k anonymizaci údajů právě v zájmu neohrožení subjektu údajů v budoucnosti.

Další zásadou je pak zásada potřebnosti a proporcionality. Zpracovávat osobní údaje je zásadně možné pouze v případě, je-li to potřebné a přiměřené danému účelu, a to po celou dobu jejich zpracování. Nesmí tedy přesahovat míru s ohledem na daný konkrétní účel. Takto jej definuje i DPD ve svém článku 6, bod 1. písm. c). Obdobně je potom princip zakotven i v jednotlivých národních úpravách. Míra proporcionality může však být často poměrně diskutabilní. V případě internetového obchodu by například neměly být zpracovávány, tudíž ani vyžadovány, informace přesahující rámec procesu prodeje daného zboží či služby. Lze tedy říci, že například vyžadování informací o osobním stavu či národnosti by do kategorie nezbytných údajů spadat nemělo.

Zásada průhlednosti, transparentnosti znamená, že každý by měl mít možnost zjistit existenci souboru osobních údajů, jejich účely, sídlo a totožnost správce, jakož i možnost získat přehled o údajích zpracovávaných o jeho osobě. Z tohoto důvodu je základní povinností správce spravovat údaje pouze otevřeně a zároveň nikoli pod záminkou jiného účelu nebo jiné činnosti.[251] S touto otázkou také souvisí zásady přístupu k údajům a případného práva na opravu či výmaz, jak bude popsáno dále.

Zásada bezpečnosti zpracovávání a uchovávání osobních údajů je také otázkou poměrně úzce spjatou s elektronickými komunikacemi, jelikož případný přístup do online databází a soborů obsahujících osobní údaje může být poměrně jednoduchý. Zásada znamená, že soubory osobních údajů musí být zásadně zabezpečeny proti neoprávněnému přístupu k nim, jejich změnám, zničení či šíření, za což odpovídá správce popř. zpracovatel. Navíc každý zaměstnanec, který přichází do styku s osobními údaji, má generální povinnost mlčenlivosti. Tyto povinnosti mají

[251] § 5 odst. 1 písm. g) ZOOU.

správci, zpracovatelé a jejich zaměstnanci i po skončení zpracovávání těchto údajů či jejich vzájemných vztahů.[252]

Zásada přístupu k datům, která zaručuje každému právo zjistit, zda jsou údaje v daném systému či u daného správce o jeho osobě zpracovávány. Je-li tomu tak, potom má tato osoba právo na přístup k nim ve srozumitelné formě. Mimo jiné musí být také poskytnuta informace 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 obecně o informační a poučovací povinnosti správce ve smyslu § 11 ZOOU. Ve své podstatě je to způsob kontroly a případného upřesnění zpracovávaných údajů ze strany samotného subjektu osobních údajů. Směrnice DPD rovněž upravuje otázku individuálních práv. Uvádí, že dotčená osoba musí být náležitě informována správcem údajů o tom, jaké údaje a jakým způsobem jsou zpracovány. Musí být poskytnuta možnost dát, omezit či vzít zpět svůj souhlas se zpracováním osobních údajů. Každý subjekt má též právo na přístup ke svým osobním údajům u daného správce. Úzce související je i právo na opravu a výmaz, které souvisí s kvalitou údajů, které jsou zpracovány a uchovány. ZOOU také předpokládá, aby se subjekt údajů sám domáhal ochrany svých osobních údajů a tím i svého soukromého a osobního života, a to jak žádostí o vysvětlení a nápravu od správce či zpracovatele, tak přímo od Úřadu.[253]

Zásada práva na opravu a výmaz se projevuje hlavně v požadavku na 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.[254]

Společně s uvedenými povinnostmi a zásadami souvisí také dohled a dozor nad jejich dodržováním. Z tohoto pohledu lze rozlišit dva přístupy: a) evropský, kde je dohled svěřen nestranné autoritě[255] a b) přístup USA, který klade zdaleka největší důraz na aktivní přístup subjektu samotného a ochranu (včetně případného vymáhání) individuální osoby.[256] V prostředí evropském se pak hovoří o zásadě nezávislého dozoru, jehož garantem je nezávislý a nestranný

[252] § 13 a násl. ZOOU.

[253] § 21 ZOOU.

[254] Čl. 6 bod 1. písm. c) DPD a § 5 odst. 1 písm. c) ZOOU.

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

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

orgán, předpokládá úmluva č. 108 i směrnice DPD v čl. 28. Podle ní každá smluvní strana je povinna ustanovit nezávislý dozorčí orgán na ochranu práv a kontrolu dodržování vyplývajících povinností. V našem případě byl dozor svěřen již zmíněnému Úřadu pro ochranu osobních údajů. Ve Velké Británii je jím nezávislý Komisař (ICO) jmenovaný královnou a podávající každoroční zprávu Parlamentu.[257] Dozorčí orgán mimo jiné zajišťuje též jednotný výklad aplikaci právní úpravy, a tudíž vydává výkladová pravidla a směrnice, stanoviska apod.

V souvislosti s výkonem dozorčí činnosti směrnice 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 daného centrálního orgánu, ale tomuto orgánu postačí danou skutečnost oznámit.[258] Našemu Úřadu tak musí správce předem písemně oznámit záměr zpracovávat osobní údaje, přičemž musí též oznámit s tím související informace podle § 16 odst. 2 ZOOU. Úřad správce poté registruje a vydá o této skutečnosti osvědčení, ačkoli i bez něj může správce zahájit zpracování osobních údajů, a to po uplynutí lhůty 30 dnů ode dne doručení výše popsaného oznámení.[259] Obdobně je nutné také oznámit ukončení této činnosti.

Z povinnosti oznamovací existuje několik vyjímek. 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 údajů. Lze se tedy vedle ochrany podle zvláštního zákona domáhat i ochrany osobnosti podle obecné občanskoprávní úpravy, jak na to upozorňuje i Knap.[260]

[257] The Information Commissioner's Office.

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

[259] § 16 odst. 3 ZOOU.

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

K tomu je také důležité dodat názor Úřadu pro ochranu osobních údajů ve vztahu k zveřejňování osobních údajů na internetu, podle kterého je ochrana prostřednictvím ZOOU a správněprávního trestání z něj vyplývajícího poměrně limitovaná, jedná-li se o soukromoprávní aktivity účastníků internetu. Dovozuje totiž z analogického výkladu principu ultima ratio trestní represe, že veřejnoprávní prostředky ochrany lze užít pouze v případě, že jiné (soukromoprávní) nepřichází v úvahu nebo by jejich využití bylo zjevně neúčelné. Z praktického hlediska Úřad uvádí, že například uveřejnění tzv. černých listin dlužníků na webových stránkách obchodních společností či obcí, pod tento zákon podřadit lze, a to zejména z důvodů užití osobních údajů pro jiné účely, než pro které byly tyto údaje získány a zpracovávány, což je protiprávní. Naopak však jednotlivé informace publikované v rámci blogů, zájmových stránek, diskuzí či sociálních sítí tomuto režimu odpovídat nebudou, jelikož v těchto případech v podstatě vždy je možné využít soukromoprávních prostředků k ochraně. Tudíž ochrana prostřednictvím Úřadu není možná a je třeba využít nástrojů pro obecnou soukromoprávní ochranu osobnosti.[261] K tomuto analogickému výkladu lze uvést tolik. V případě, že nejsou naplněny znaky zpracování, anebo jde o zpracovávání nahodilé či jiné mimo režim ZOOU, potom samozřejmě nelze užít ochrany prostřednictvím Úřadu. Přílišné zúžení správněprávního trestání analogickou aplikací trestněprávní zásady ultima ratio však může vést k opakovanému porušování zákonných povinností v případě menších zpracovatelů. Poměrně malé procento subjektů, jejichž osobní údaje a jejich ochrana jsou porušovány, využije totiž z nejrůznějších (např. časových a finančních) důvodů občanskoprávní ochrany, a k nápravě tudíž dojde jen ve velmi omezených případech.

5.6 Právní otázky elektronické komunikace na dálku

Elektronické komunikace je 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

[261] Úřad na ochranu osobních údajů (2010) *K problémům z praxe č. 4/2010. Zveřejňování osobních údajů na internetu.* [online] přístupné na adrese <http://www.uoou.cz/uoou.aspx?menu=14&loc=729>.

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. Nedotknutelnost poštovních zpráv a zásilek je stanovena v zákoně o poštovních službách,[262] za sdělení chráněné tímto zákonem se však považuje pouze písemnost v listinné podobě. Nelze jí tedy aplikovat například na emailové zprávy, chaty či jiné zprávy zasílané v elektronické podobě.[263] Pro tuto oblast byl na základě evropské směrnice o soukromí a elektronických komunikacích[264] přijat zvláštní zákon č. 127/2005 Sb. o elektronických komunikacích, jež uvedl naší úpravu do souladu s uvedenými evropskými pravidly. Je v podstatě 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 elektronických či informačních technologií.[265]

Obsahem této úpravy je zejména systém 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 na našem území Český telekomunikační úřad (ČTÚ), jenž je ústředním správním úřadem podle tohoto zákona. Obecně se tak hovoří o oddělení regulace přenosu od regulace obsahu (§ 1 odst. 2). Vedle technických otázek však také pojednává o bezpečnosti poskytovaných služeb, ochraně osobních údajů a údajů jim svojí povahou velmi blízkých (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 rámcová směrnice č. 2002/21/ES.[266]

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

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

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

[264] 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).

[265] Vaníček, Z. 2008, str. 14.

[266] 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).

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 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. e) zákona o elektronických komunikacích. Konkretizace ochrany údajů, služeb a sítí elektronických komunikací je potom obsahem hlavy V. téhož zákona.

Základním principem ochrany uživatelů podle tohoto zákona je důvěrnost zpráv a dalších údajů, kterou je povinen každý provozovatel veřejné komunikační sítě zajistit.[267] Údaje nesmí být odposlouchávány, ukládány ani jinak zachycovány či sledovány jinou osobou než uživatelem samotným, leda by samotní uživatelé dali souhlas. Výjimkou jsou opět tzv. zákonné licence, např. podle § 88 trestního řádu,[268] 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).

Jak bylo řečeno na výše, poskytovatel veřejně dostupné služby elektronických komunikací má mimo jiné povinnost zabezpečit ochranu osobních údajů, provozních a lokalizačních údajů a důvěrnost komunikací. Vhodné zabezpečení je důležitým pravidlem, které

[267] § 89 zákona o elektronických komunikacích.

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

stanovila 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.[269] Jde o opatření, které má 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.[270]

Poměrně často diskutovanou otázkou je také zisk, nakládání a uchovávání údajů o provedené komunikaci. Jedná se o údaje, které se netýkají čistě obsahu přenášených informací, ale obsahují informace vedlejší, například časové a místní určení provedené komunikace. Zákon i směrnice je nazývá údaji provozními a lokalizačními. Svojí povahou tyto údaje nespadají do kategorie osobních údajů podle definice obsažené v ZOOU, avšak jejich zvláštní právní úprava má své odůvodnění. Pomocí dostatečného množství takových údajů lze vytvořit podrobný obraz velmi dobře využitelný například pro komerční účely, navíc také lze tímto způsobem získat poměrně přesný obraz o konkrétní osobě, jejích zájmech a činnosti. 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 nebo je jinak využívají zejména k obchodním a 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 číslo účastníka, čas, kdy byla daná zpráva odeslána, kdo jí odeslal nebo datová velikost odeslané zprávy. 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

[269] Lloyd 2008, str. 165.

[270] K tomu též § 88 odst. 1 písm. d) zákona o elektronických komunikacích.

informován a vyžádán jeho souhlas, který může také vzít kdykoli zpět.[271] Navíc účastník/uživatel musí být o rozsahu zpracovávaných údajů a době jejich zpracování poskytovatelem informován. Je nutné mít také na zřeteli, že pokud pomocí těchto údajů je identifikovatelná osoba, tyto údaje spadají do kategorie údajů osobních a na jejich zpracování se vztahuje také ZOOU. Navíc obdobně, jako u zpracování osobních údajů, platí zásada přiměřenosti a časového omezení, tedy zpracování dat o komunikaci je přípustné 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.[272] Zvláštní úprava se však týká jen těch, které jsou odlišné od provozních údajů.[273] Tyto 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, může zpracovávat pouze poskytovatel služeb elektronické komunikace či osoba jím pověřená, popřípadě poskytovatelem služeb s přidanou hodnotou, přičemž vždy pouze při dodržení uvedených zásad.

Stanou-li se údaje 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 o elektronických komunikacích), 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 tak mohou údaje mezi sebou předávat k uvedeným účelům, aniž by bylo třeba souhlasu uživatele.

Zákon o elektronických komunikacích poskytuje ochranu elektronických adres před jejich zneužitím. Za zneužití se považuje každé použití adresy elektronické pošty pro odeslání zprávy nebo zpráv třetím osobám bez souhlasu držitele této adresy, jak uvádí ustanovení § 93.

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

[271] § 90 odst. 6 zákona o elektronických komunikacích.

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

[273] Čl. 9, ibid.

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.

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

Jak přestupky, tak správní delikty, projednává Český telekomunikační úřad (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 případné odpovědnosti poskytovatelů je důležité také ustanovení § 61 odst. 5 tohoto zákona, které obdobně jako zákon o některých službách informační společnosti zásadně vylučuje odpovědnost podnikatele poskytujícího veřejně dostupnou službu elektronických komunikací za obsah přenášených zpráv. Případnou odpovědnost nese tedy v plném rozsahu původce takového protiprávního obsahu.[274]

5.6.1 Přímé obchodování v prostředí sítě elektronické komunikace

Sítě elektronických komunikací jsou zejména mocným nástrojem a prostředkem obchodních aktivit. S faktem, že čím dál více lidí aktivně využívá internetovou síť při každodenním životě, i obchodní a marketingové postupy se tomu přizpůsobují. Důsledkem je také velký rozvoj produktů a služeb, které v rámci internetu bývají nabízeny a prodávány. Některé praktiky, které se pro tyto účely používají, však mohou výrazným způsobem zasahovat do soukromé oblasti jednotlivých uživatelů, a to i bez jejich vědomí. Navíc některé způsoby reklam jsou pro mnohé uživatele internetu velmi nepříjemné a obtěžující. Jak bývá internet užíván i zneužíván pro obchodní účely a jaké to může mít právní důsledky je popsáno v následujícím výkladu.

5.6.1.1 Reklama a spam

Reklama je ve své podstatě neosobním jednostranným sdělením, jehož cílem je podat potenciálnímu zákazníkovi informaci o nabízených službách či výrobcích. Tento fenomén je regulován napříč právním systémem. Občanskoprávní úprava všeobecného osobnostního práva

[274] Vaníček, Z. 2008, str. 226.

omezuje zejména užívání podobizen, hlasových projevů a podobných osobnostních projevů pro reklamní účely. Obchodněprávní předpisy zakazují zejména nekalosoutěžní jednání, například ve formě klamavé či srovnávací reklamy. Veřejnoprávní regulace se pak zaměřuje na ty jevy, které dosahují širšího společenského 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 práci důležité počítačové sítě, audiovizuální produkce či nosiče.

Podle § 2 zákona o regulaci reklamy jsou některé druhy reklam zcela zakázány. Jedná se například o tzv. podprahové reklamy, působící na podvědomí člověka, nebo o nevyžádané či skryté reklamy. Zejména v souvislosti s nevyžádanou reklamou je třeba zabývat se více. Jedná se o takovou reklamu, která může adresáta obtěžovat a tím narušovat jeho soukromou sféru. Jejím projevem je například vhazování reklamních letáků do schránek, kde je výslovné prohlášení o tom, že si to její majitel nepřeje. V rámci elektronického světa je to velmi obdobné. Podle § 95 zákona o elektronických komunikacích má každý uživatel či účastník elektronických sítí a služeb mít možnost učinit prohlášení, že si nepřeje dostávat zprávy a informace za účelem reklamy.

Zákon o regulaci reklamy pak rozlišuje osoby odpovědné 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,[275] na které dohlíží a vynucuje jejich dodržování příslušná komise.[276]

Spam

Za zvlášť obtěžující formu elektronické reklamy, proti které je obrana velmi obtížná a nákladná, se považuje tzv. spam nebo též junk mail. Důkazem důležitosti a aktuálnosti tohoto jevu je i

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

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

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 u nás transponovány do zákona o některých službách informační společnosti v roce 2004.[277] Ten mimo jiné upravuje šíření obchodních sdělení elektronickou poštou v § 7. Spam obecně však může ve své podstatě být jakékoliv hromadné, obtěžující a opakující se sdělení, bez ohledu na jeho obsah. Naše právní úprava se však bohužel vztahuje jen na sdělení obchodní povahy. Výraz elektronickou poštou je vykládán v širokém slova smyslu. Zahrnuje tudíž i telefonické prostředky jako telemarketing či SMS zprávy. Dovoleno je využít elektronickou poštu pro účely marketingové pouze, pokud s tím dal zákazník předem souhlas, jak uvádí § 7 odst. 2. Ten však není třeba v případě, že potřebné údaje byly získány od uživatele v rámci prodeje výrobku či služby, pokud bylo zákazníkovi jasně a zřetelně umožněno jednoduchým způsobem odmítnout souhlas s užitím pro reklamní účely. Možnost jednoduše odepřít souhlas navíc musí být dána v každém jednotlivém obchodním sdělení (tzv. opt-in metoda). Náležitosti souhlasu jsou obdobné jako v případě osobních údajů, tedy užije se ustanovení § 4 písm. n) zákona o ochraně osobních údajů. Důležitým aspektem je, že musí být vždy prokazatelný. Jinak je šíření obchodních sdělení zakázáno. Kromě toho je zakázáno také šíření sdělení, které není sice za obchodní sdělení označeno, ale neobsahuje či skrývá totožnost odesilatele, nebo které je zasláno bez platné adresy (§ 7 odst. 4).

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 související s šířením obchodních sdělení podle tohoto zákona, 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, jak uvádí § 12 odst. 1 téhož 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, došlo-li k porušení tohoto zákona při podnikání nebo v přímé souvislosti s ním.

Pojetí odpovědnosti v souvislosti se spamy je přísnější například v USA, kde je tato činnost považována za trestný čin.[278]

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

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

Spam je však i přes určitý právní rámec stále velmi problematickým jevem. Zejména spam ze zahraničí je jen velmi těžko dohledatelný a tudíž bez jeho původce nelze postihnout. Poskytovatelé elektronických služeb, například služeb elektronické pošty, musí přijímat velmi nákladná technicko-organizační opatření, např. filtry, aby k obtěžování jejich zákazníků docházelo co nejméně.

Vedle samotného způsobu využití elektronických prostředků k obchodním účelům, je právně upraveno i samotné zpracování osobních údajů v souvislosti s marketingem. Nakládání s údaji jako je elektronická pošta pro účely zaslání obchodních sdělení, popř. i spamu většinou naplní znaky zpracování ve smyslu ochrany osobních údajů. 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 ke stejnému účelu, a subjekt byl o tomto postupu předem informován a nevyslovil s tím písemně nesouhlas. Poměrně výhodné i v této oblasti je, že orgán dozoru je stejný jako v případě spamu, tedy Úřad pro ochranu osobních údajů, na kterého se lze i pomocí jednoduchých elektronických formulářů se svými stížnostmi a podněty obracet.

Problematické 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 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, např. 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 poměrně 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 o to více komplikovaná, že původci spamů jsou v podstatě téměř nedohledatelní.

5.6.1.2 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 internetoví

obchodníci (jako např. eBay nebo Amazon) a provozovatelé webových vyhledávačů (Google či Seznam) za účelem usnadnění a urychlení prohlížení stránek při příští návštěvě internetu. Díky nim dokáže daná stránka či vyhledávač nabízet uživatelem často hledané výrazy a slova, aniž by musel 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.[279]

V době projednávání směrnice 2000/31/ES o elektronickém obchodu[280] 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.[281] 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.[282]

Pracovní skupina zřízená podle čl. 29 DPD se ve svém stanovisku z roku 2008 v souvislosti s internetovými vyhledávači vyslovila v tom smyslu, že soubory cookies je nutné považovat za osobní údaje, jelikož každý obsahuje též jedinečné identifikační označení, pomocí

[279] Carey 2004, str. 238.

[280] směrnice 2000/31/ES o elektronickém obchodu, ze dne 8. června 2000.

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

[282] Carey 2004, str. 239.

kterého je možné uživatele identifikovat. Tudíž je nutné s nimi zacházet v režimu předpisů o zpracování osobních údajů, a to jak při jejich získávání, tak dalšího nakládání a uchovávání.[283]

5.7 Sociální sítě

V souvislosti s ochranou osobnosti a jejího soukromí v internetovém prostředí lze sledovat trend posledního desetiletí, který velmi významným způsobem ovlivňuje jak tuto sféru, tak zároveň obsahuje velmi cenné údaje a prostředky například z marketingového hlediska. Tímto trendem je rozvoj a používání internetových sociálních sítí, jejichž prostřednictvím lidé sdělují často velmi detailní informace o svém osobním i rodinném životě. Toto je trend zejména poslední doby a tudíž i mladší generace, která se příliš nezamýšlí nad důsledky, jaké může takovéto odhalení svého soukromí přinést. Navíc v takto globálně propojeném prostředí se velmi rychle přenáší data i mimo území EU. 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 bylo, zda se skutečně prostředí elektronických sociálních sítí považuje za soukromé, zda je tedy rozumné očekávat ochranu takto poskytnutých údajů, anebo jde-li díky povaze internetu jako takového o veřejně přístupné místo, kde nelze rozumně očekávat soukromí ani jeho ochranu. Podle dosavadního přístupu právní i soudní praxe se i internetové prostředí považuje za soukromé prostředí, dodrží-li se některé podmínky.[284]

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 jednání samotných uživatelů, kteří například zveřejní informace (například fotky) o jiné osobě. Takto byla úspěšná žalobkyně v již zmíněném soudním případě Lindqvist, protože na

[283] Pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů (2008) *Stanovisko k otázkám ochrany údajů v souvislosti s vyhledávači.* Znění účinné od 13.11.2008. [online] přístupné na adrese <http://www.beck-online.cz/legalis/document-view.seam?type=html&documentId=oz5f6mrqga4f6njql44f65lpn52s2ma&groupIndex=1&rowIndex=1&conversationId=659608#selected-node>, publikované též ve Věstníku Úřadu pro ochranu osobních údajů č. 50 z roku 2008.

[284] 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).

internetové síti její kolegyně z náboženské společnosti uveřejnila fotky, na kterých byla mimo jiné vyobrazena i ona, aniž si předem vyžádala její souhlas. Za toto jednání byla paní Lindqvist udělena pokuta. Nejvíce problematické je pak zpřístupnění mnoha osobních údajů třetím osobám. Tak například zaměstnavatelé prověřují své zaměstnance či žadatele o práci, obchodní partneři vyhledávají informace a případné záminky pro obchodní jednání, pachatelé trestné činnosti mohou zjistit údaje potřebné k zamýšlenému účelu (například, 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 uživatelského účtu mohou zůstávat nadále uložená a tak i přístupná a dohledatelná na příslušných hostitelských serverech.[285] Tento trend je však více než právním spíše společenským problémem, neboť platí jedna ze základních zásad, že každý by měl dbát svých práv. To platí tím spíše, jedná-li se o soukromí dané osoby. Ochrana může být poskytnuta toliko tomu, kdo sám své soukromé údaje chrání a dobrovolně je nezpřístupňuje veřejnosti.

5.8 Odhalování trestné činnosti v prostředí internetu

Internetová síť se stala také mocným nástrojem a prostředím, kde čím dál častěji dochází k páchání trestné činnosti. V souvislosti s tím se vyvinuly i nové trestné činy, na což se snaží reagovat mezinárodní i vnitrostátní právní úprava. V této souvislosti se také mění prostředky, jakými lze trestnou činnost odhalit a případně jí předcházet. Proto v následujících odstavcích se budeme zabývat tím, jaký je právní rámec sledovacích vyšetřovacích nástrojů, a jaké jsou jejich dopady například na soukromí jednotlivců. Z pohledu metodologického se rozeznává několik druhů sledování: fyzické, psychologické a sledování datové.[286] 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 elektronických osobních údajů, jak je tomu například při sledování veřejných míst či pracoviště pomocí videokamer

Základní právní úprava, která umožnila omezení práva na ochranu osobnosti soukromí fyzických osob, je obsažena v článku 8 odst. 2 Evropské konvence, a dále pak v jednotlivých evropských směrnicích, například ve směrnici o ochraně osobních údajů, nebo ve směrnici č. 2002/58/ES o elektronických komunikacích (v čl. 15) společně se směrnicí č. 2006/24/ES o uchovávání údajů. Podle nich je možné omezit právo na soukromí a uchovávat údaje o

[285] 2009, str. 480.

[286] Lloyd 2008, str. 12.

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 dávají možnost poměrně výrazně odlišného přístupu v jednotlivých zemích Evropské Unie.

Důležitou událostí, která předznamenala budoucí vývoj v oblasti odposlouchávání a sledování provozu na internetu (z anglického internet surveillance), byl teroristický útok 11. září 2001 v USA, a dále pak další teroristické činy v Madridu (2003) a Londýně (2005). Za účelem boje proti terorismu a ochraně státní a veřejné bezpečnosti byla přijata opatření, která na jednu stranu posilují a zefektivňují zejména prevenci a vyšetřování trestné činnosti, avšak jejich negativním důsledkem je značná restrikce soukromí individuálních osobností ve prospěch orgánů veřejné moci. Nejvíce ohrožené země, zejména USA a UK zaujaly poměrně razantní postoj, významně odlišný od ostatních zemí EU.

V UK je například ponechána velmi široká pravomoc veřejnoprávním institucím, které mohou autorizovat a dohlížet nad odposloucháváním a sledováním provozu elektronických sítí, aniž by do toho zasahovaly nezávislé 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.[287] V ostatních zemích EU je výrazně větší důraz na dohled a autorizaci prostřednictvím orgánů moci soudní. Tuto koncepci zásadně dodržuje i naše právní úprava, jelikož předpokladem k sledování a odposlouchávání je příkaz soudu podle § 88 a § 88a zákona č. 141/1961 Sb., trestního řádu, který poté zabezpečuje samotný provozovatel veřejné komunikační sítě či služby na základě § 97 zákona č. 127/2005 Sb. o elektronických komunikacích. Přístup UK je však odůvodňován potřebou rychlosti a efektivity. Kromě toho je významným důvodem také fakt, že pro soudní povolení by bylo nutné odkrýt mnoho důležitých údajů, a to zejména metody sledování, což by mohlo znamenat jejich neefektivnost v budoucnu. Právě vědomí pachatelů trestných činů, že mohou být sledovány či odposlouchávány, má mít hlavní 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.

5.8.1 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

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

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.[288]

K metodám utajeného odposlouchávání se vyjádřil Evropský soud pro lidská práva (dále též ESLP) v případě Klass v Germany,[289] který posuzoval odposlouchávání telekomunikačních konverzací. Soud mimo jiné konstatoval, že i toto prostředí je soukromé ve smyslu článku 8 Konvence. Obdobně i v případě emailu a jiného způsobu užívání internetové sítě se považuje za prostředí spadající pod článek 8.[290]

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) systému, předpisy mezinárodního práva se stávají jeho součástí nikoli schválením a ratifikací, ale po ratifikaci musí být přijat zvláštní zákon, který 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 dříve. 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. Tím činí poměrně složité pro jednotlivce předvídat a kontrolovat, kdy a v jakém rozsahu mohou být jejich práva omezena.[291] Navíc v případě angloamerického právního systému může zákonné omezení vyplývat i z common law založeného na soudních precedentech, což bylo potvrzeno též ESLP v případě Malone v UK.[292]

Každé omezení (například v zájmu národní bezpečnosti) musí být vždy při zachování zásady proporcionality mezi chráněným zájmem (individuální soukromí) a důvodem zásahu do

[288] Článek 8 odst. 2 Evropské konvence

[289] [1978] 2 EHRR 214.

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

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

[292] [1984] 7 EHRR 14.

něj.[293] Zároveň je stát povinen zajistit zásah v co nejmenší nutné míře, jak bylo potvrzeno v případě Campbell v UK [1993] 15 EHRR 137.

V roce 2000 byl ve Velké Británii přijat zákon regulující zejména pravomoci spojené s vyšetřováním protiprávní činnosti, the Regulation of Investigatory Powers Act 2000 (RIPA). Zákon tvoří základní právní rámec a pravidla také pro odposlouchávání a monitorování komunikace uskutečňované v internetové síti. Kromě toho také 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 nutné k provozu dané služby, anebo je-li to nezbytné k plnění jeho zákonných povinností.[294] Pokud nejde o tento případ, je zásadně nezbytné provádět takovou činnost jedině na základě autorizace příslušným státním orgánem či institucí. Zákon, ačkoli neposkytuje žádnou zvláštní ochranu důvěrným informacím, tato kategorie má být respektována podle prováděcích směrnic vydaných vládou.[295] Podle nich má být s takovými informacemi nakládáno se zvláštní opatrností, přičemž tyto informace mohou být odposlouchávány jen v souvislosti s podezřením z trestné činnosti. To se týká zejména informací čistě důvěrné povahy.

Článek 12 RIPA potom umožňuje státním orgánům uložit povinnost veřejným poskytovatelům telekomunikací (ISPs), aby prováděli a tudíž i financovali příslušné odposlouchávání. Tento článek se samozřejmě setkal s velkou kritikou zejména ze stany ISPs, a vláda souhlasila s nárokem na částečnou náhradu případných nákladů, jak je předpokládáno v článku 14 RIPA.

Dohled nad dodržováním pravidel obsažených v RIPA je svěřen zvláštnímu Komisaři[296] a Tribunálu podle jeho článku 57 a 65. 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 je prováděna. Tudíž se ve většině

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

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

[295] The Interception Code of Practice 2002.

[296] The Intrception of Communications Commissioner.

případů daná osoba vůbec nedozví, že k jejímu odposlouchávání dochází, a nemá tedy možnost se proti tomu případně bránit.[297]

Zároveň v této souvislosti je však nutné upozornit na důležitý fakt, že data získaná odposlouchávaním (tedy například obsah konverzace) podle RIPA nelze užít jako důkaz při soudním řízení vyšetřovaného trestného činu, na rozdíl od údajů o komunikaci, které jsou diskutovány dále.[298] Proto podobné údaje mohou sloužit pouze a jen k dalšímu vyšetřování.[299]

5.8.2 Kódování a přístup k chráněným údajům

K ochraně přenášených dat zejména v průběhu jejich přenosu se začaly používat různé formy ochrany a kódování. 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 enkryptování dochází jak privátně (tedy obě strany si dobrovolně zvolí kód a heslo, pomocí kterého pouze oni mohou mít přístup k přenášeným informacím), tak veřejně, 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.

Neposkytnutí daného hesla či kódu se zároveň považuje za trestný čin, a pachatel se vystavuje poměrně vysokým sankcím, kterými je pokuta a případný trest odnětí svobody až na 2 roky, jak uvádí článek 53(3) RIPA. 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 je diskutované a někteří autoři jej označují za odporující základní zásadě trestního práva, kterou je presumpce neviny. Případné dokazování by však nemělo být dostačující bez předložení pozitivních důkazů ze strany

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

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

[299] 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.

žalobce, jak naznačil soud UK v rozhodnutí R v S ans A [2008] EWCA 2177, čímž dopad tohoto ustanovení v praxi zmírnil.

Kromě výše uvedeného se za trestný čin s trestem odnětí svobody až na 5 let považuje porušení povinnosti mlčenlivosti o tom, že dané heslo nebo klíč byl vyžádán. Tuto povinnost má každá osoba, od které bylo vyžádáno heslo nebo klíč, jakož i každý, kdo se o tom dozvěděl.[300] Edwards uvádí, že v tomto ohledu jde o ochranu metod a průběhu vyšetřování a odposlouchávání, proto je zde limit sankce tak vysoký.[301]

5.8.3 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 určují prováděcí legislativou, 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.[302] 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.[303]

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[304] uvádí v čl. 6 rozmezí 6 až

[300] RIPA s. 54.

[301] 2009, str. 568.

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

[303] The Secretary of State.

[304] 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.

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[305] a pro internetová data je dosud pouze ve formě návrhu.[306] Návrh počítá s uchováním dat po dobu 12 měsíců (článek 5), a k možné finanční kompenzaci (článek 11). 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.[307] 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.[308] Navíc podle případu Ewber and Saravia v Germany,[309] ESLP rozhodl, že národní úprava musí poskytnout takovou právní úpravu, která bude předvídatelná. Což v případě RIPA a jejích prováděcích předpisů je poměrně složité.

V našem právním řádu je stanovena povinnost uchovávat údaje lokalizační a provozní pro účely Policie ČR, Bezpečnostní a informační služby nebo Vojenského obranného zpravodajství v § 97 odst. 3 zákona o elektronických komunikacích. Provozovatelé jsou povinni uchovávat tyto údaje po dobu nejméně 6 měsíců a nejdéle 12 měsíců a na vyžádání je uvedeným orgánům poskytnout. I zde je však předpokladem příkaz soudcem či předsedou senátu podle § 88a odst. 2 trestního řádu.

---

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

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

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

[308] Edwards a Waelde, str. 592.

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

5.9 Shrnutí a perspektivy dalšího vývoje

Čím vice je otevřený a propojený svět, tím větší je ohrožení našeho soukromí i osobnosti. Kromě protiprávních činů je výrazným ohrožením i samotná dobrovolná činnost každého uživatele. Právo se snaží reagovat na některé jevy, avšak zejména chování samotných uživatelů a subjektů ochrany je tím nejdůležitějším faktorem. Zejména s rozvojem virtuálních sociálních sítí nechávají uživatelé ostatním přátelům, mnohdy však také osobám zcela neznámým k dispozici mnoho dokonce i citlivých údajů. Tím za sebou nechávají mimo jiné též nesmazatelnou stopu, které v budoucnosti mohou velmi litovat.

Ochrana soukromí a osobnosti je jedním ze základních lidských práv a svobod v demokratické společnosti, která byla v minulosti předmětem mnoha revolucí. Mezinárodní úmluvy a důraz na jejich ochranu se zdály být jedním z hlavních cílů mezistátní spolupráce. V prostředí internetovém se však zdá, že ve prospěch efektivity a prosazování jiných právních odvětví a zájmů se dostává soukromí do pozadí. K tomu nepřispělo ani současné dění ve světové politice, kde ve jménu boje proti terorismu je ochrana jednotlivců vůči veřejné moci naprosto minimální. Zejména nejvíce ohrožené státy jako je USA či UK dávají široké pravomoci například při odposlouchávání a sledování lidí, kteří jsou podezřelí z trestné činnosti, aniž by předem muselo dojít k prokázání opodstatněnosti daného podezření před nezávislým orgánem. Ochrana soukromých zájmů je vždy limitována a v podstatě stojí v určité antagonii k zájmům veřejným. Proto také každá mezinárodní i vnitrostátní úprava poskytuje katalog výjimek, kdy může být ochrana soukromých práv omezena. Důvody jsou zejména veřejné, tedy ochrana státu, jeho zřízení, ekonomických zájmů, veřejné bezpečnosti či ochrana před trestnou činností. Lidská práva také limitují sebe navzájem, jelikož totéž právo či svoboda by neměla zasahovat do stejného práva jiné osoby. Je tedy zásadní otázkou, jak najít vyvážení a správnou míru, kdy je ještě přípustné zasahovat do soukromí a osobnosti jednotlivců ve prospěch prosazování zájmů jiných, a kdy je tato míra již překročena.

Virtuální svět internetu s sebou přináší další výzvu, jelikož právní systémy se každý den dostávají do vzájemných vztahů a téměř každý vztah na internetu má prvky mezinárodní. Určení rozhodného práva, příslušného orgánu a zejména pak vynucování rozhodnutí zahraničních orgánů je zásadní problematikou, bez které veškerá regulace při současném respektování suverenity jednotlivých států je bezvýznamná. V ochraně osobnosti je situace o to problematičtější, že na rozdíl od kontinentálního právního pojetí, které poskytuje generální všeobecnou ochranu osobnosti, angloamerický svět se zaměřuje pouze na některé konkrétní aspekty prostřednictvím zvláštních žalob a institutů. Vzájemná inkompatibilita těchto dvou systémů pak může být důvodem, proč nebudou některé zahraniční rozhodnutí efektivní, jelikož

dané jednání musí být protiprávní podle právního řádu obou zemí. Tak například ve Spojených státech amerických je poměrně složité bránit své soukromí, jelikož tamní soudy výrazně upřednostňují svobodu slova svých občanů.

Jedním z projevů osobnosti, který je ve virtuálním prostředí nejdůležitější, je otázka osobních údajů. Hovoří se dnes o informační společnosti, proto právě informace o každé osobě jsou tím, co je v prostřednictví internetu předmětem činnosti a tudíž i právní úpravy. Získávání, užívání i ukládání různých údajů se proto stalo i zvláštním předmětem pozornosti legislativních orgánů. Zpracování údajů, jehož výklad zahrnuje téměř veškeré činnosti týkající se údajů, z nichž lze poměrně snadno identifikovat jejich subjekt, podléhá základním principům a dohledu zvláštních nezávislých orgánů. Regulace se zaměřila i na údaje svojí povahou připomínající údaje osobní, které svým obsahem mohou poskytnout obraz o činnosti, záměrech i zájmech jednotlivých uživatelů. Hovoří se o údajích o komunikaci. Zásadním principem této úpravy je souhlas, který ve většině případů je ke zpracování osobních údajů nezbytný, v případě údajů citlivých je třeba souhlas výslovný. Z praxe se však ukazuje, že ani tento požadavek není všemocný. Zahrnutí souhlasu do podmínek či předem zaškrtnuté pole při registraci uživatele na dané stránky je typickým příkladem, jak uživatelé dávají souhlas, aniž by tomu věnovali větší pozornost. Navíc svým vlastním chováním konkludentně samy souhlas udělí již tím, že některé údaje sami ostatním zpřístupní např. prostřednictvím již zmíněných sociálních sítí, blogů, chatů a jiných elektronických nástrojů.

V neposlední řadě také vývoj v posledních letech ukazuje, že státy, kde již tradičně mají lidská práva a svobody nejhlubší základy, nyní v zájmu vyšších a zejména ekonomických ochrany jednotlivců v rámci internetové sítě velmi opouští. Zejména v důsledku ochrany práv autorských dokonce ukládají povinnosti na ty, kdo zprostředkovávají danou službu či samotné připojení k internetu, aby na vyžádání aktivně sledovali a omezovali jednotlivé uživatele, shromažďovali údaje o nich a poskytovali je jiným osobám. Ve Francii dokonce zvláštní sledovací program může být v budoucnu povinně nainstalován do přístrojů jednotlivých uživatelů. Tím může skutečně dojít k naplnění tezí, že naše společnost slepě kráčí do budoucnosti, ve které budou všichni sledování a monitorováni, a to z různých veřejných i soukromých důvodů.

6. Závěr

Na počátku rozvoje internetové sítě jen málokdo tušil, jak důležitým nástrojem může v budoucnu být. Dnes si jen těžko lze představit každodenní život bez internetu. Kromě nástroje sloužícího ke komunikaci mezi lidmi jde také o virtuální prostředí zejména z obchodního hlediska. Velká většina služeb, programů a stránek je motivována ekonomickými cíly. Z tohoto pohledu je pro podnikatele nejvhodnější, aby byla maximálně zachována demokratická podoba bez přílišných omezení. Na druhou stranu však také internet představuje nástroj k porušování veřejných i soukromých zájmů a práv. Internet jako globální počítačová síť s sebou kromě jiného přinesl také mnohé nové společenské a tudíž i právní jevy. Tradiční právní instituty čelí nové realitě více či méně úspěšně a jejich regulace i aplikace doznávají mnohých změn tak, aby i ve virtuálním prostředí, pro které geografické hranice v podstatě neexistují, mohly nadále plnit svoji úlohu. Virtuální prostředí však přineslo také nové jevy, které se v mnoha zemích objevují také jako samostatné právní instituty. Tato práce se postupně zabývala tradičními i novými právními instituty a jejich aplikací v prostředí globální počítačové sítě. S tímto technickým pokrokem totiž ruku v ruce je i rozvoj a změny v chování společnosti a tudíž i právní regulace je nucena dříve či později na tyto společenské změny reagovat a přizpůsobovat se nové realitě.

Z obecného hlediska je důležité nadále udržovat v univerzální podobě infrastrukturu, bez které nemůže síť v takto globálním měřítku existovat. ICANN, které je fakticky pod jurisdikcí Spojených států amerických, by se mělo ještě více osamostatnit a stát se skutečně absolutně nezávislým a neutrálním orgánem mezinárodního charakteru. Na takovouto instituci, ve které by proporcionálně byly zastoupeny všechny části světa, by bylo možné přesunout i další role, které z části již dnes zastává. Zejména totiž prohlubování mezinárodní spolupráce například v boji proti závažné a specificky internetové kriminalitě je nadmíru důležité a mohlo by vyústit ve sjednocující mezinárodní smlouvu. ICANN by měla také mít funkci mezinárodního fóra, které je prostředníkem dialogu mezi všemi na internetu zúčastněnými stranami, a to státy, obchodními korporacemi i jednotlivými uživateli.

Z hlediska autorskoprávního je internet poměrně komplikovaným prostředím, kterému se současný stav musí nadále přizpůsobovat spíše, než se mu bránit. Lpění na bezvýjimečné ochraně autorských práv a stíhání každého jednotlivce je již dávno nemožné. Unifikace v oblasti výjimek je jednou ze základních nutností, jak zajistit co nejvíce jednotnou úpravu ochrany autorských práv za současného umožnění přístupu k dílům v odůvodněných případech. Zejména pak užití pro čistě soukromé a vzdělávací účely by mělo být zakotveno v závazné podobě i na mezinárodní úrovni, tím spíše na úrovni evropské. Rovněž přeshraniční spolupráce je důležitá již

ze samotné globální podstaty internetové sítě, proto i otázky mezinárodního práva soukromého jsou neopomenutelné. Určení rozhodného práva a příslušného orgánu k rozhodování ve věcech autorských práv a jejich porušování by mělo také zaznamenat jednotnější úpravu. Podle současného stavu je nejúčinnější dožadovat se nápravy tam, kde jsou umístěné servery a lze tak zajistit skutečnou nápravu. Na druhou stranu však servery je velmi jednoduché přemístit do zemí, kde je úprava na nižší úrovni. I proto je nutné zdůraznit unifikaci na mezinárodní úrovni. Při užití práva země, pro kterou je ochrana práv vymáhána, je k efektivitě takového rozhodnutí důležité, aby i v místě faktické kontroly dané osoby či serveru bylo toto rozhodnutí uznáno a vymáháno. V zájmu ochrany osob, jimž autorská práva svědčí, se objevují trendy, které na jedné straně mají logický odůvodnění, na straně druhé však skýtají i mnohá nebezpečí. Volání po aktivnějším zapojování poskytovatelů internetového připojení či jiných služeb informační společnosti a případného zakotvení jejich odpovědnosti za porušování autorských práv případně i práv jiných může být efektivním nástrojem, jelikož ISPs mají bezesporu strategické postavení. Na druhou stranu však důsledkem může být i nutná kontrola a monitorování činnosti každého uživatele, čímž se demokratická povaha včetně ochrany soukromí a osobnosti jednotlivých uživatelů zatlačují velmi do pozadí. Pravda však je, že základní otázkou je kontrola nad kanály, kterými dochází ke zpřístupňování a rozšiřování děl pomocí internetové sítě, a tu může vykonávat nejefektivněji jedině poskytovatel dané služby. Za současného stavu je důležité zajistit, aby byla autorská díla snadno přístupná, pokud možno za jednotných podmínek a přijatelné ceny. Nástrojem, jak takového stavu dosáhnout může být i vytvoření jednotné správy a licenčních nástrojů pro co nejširší území. Dnešní stav, kdy je nutné vyjednávat individuálně s každým kolektivním správcem v dané zemi zvlášť je zbytečně zdlouhavý. Usnadnění tohoto stavu může napomoci při realizaci a prodeji děl při zachování autorskoprávní ochrany. Do budoucna se tedy jeví za nejpřijatelnější hledat efektivní nástroje pro podporu a usnadnění obchodních služeb a produktů tak, aby si uživatelé mohli jednoduše a za finančně dostupných podmínek dané dílo zakoupit, než hrozbami finančních či jiných přísných postihů se snažit jednotlivé uživatele zastrašovat.

Internetová síť mimo jiné s sebou přináší i nové obchodní a marketingové nástroje a příležitosti. Zejména z tohoto důvodu se doménová jména stávají předmětem mnohých sporů a jako identifikátor obdobný například ochranným známkám může mít tento institut poměrně vysokou ekonomickou hodnotu. S rozvojem využívání internetové sítě i pro obchodní účely zpočátku někteří předvídaví uživatelé ve snaze jednoduše získat nemalé finanční prostředky využili principu first come, first served a zaregistrovali si doménová jména shodná se jmény a jinými druhy označení největších světových obchodních organizací a známých osobností. Těm

dalo následně poměrně hodně práce a snahy získat tyto domény pro sebe zpět a dát tím důvod pro změnu systému a zakotvení rychlých a efektivních prostředků nápravy, před těmi, kdo se ze spekulativních či zcela protiprávních důvodů snaží využít jména či označení jiných subjektů. I proto je pozitivním krokem úprava alternativního způsobu řízení ve sporech o doménová jména. Navíc tato řízení se v dnešní době konají online bez nutnosti ústního jednání a dalších výdajů, většinou z časového hlediska trvají asi dva měsíce, což v porovnání s využitím řízení před soudy je velmi rychlý způsob řešení. Z hlediska právní povahy by v našem právním řádu neměly být již pochyby o doménových jménech, jelikož nový občanský zákoník je řadí obdobně jako jiné nehmotné statky mezi věci, které tak bude možné vlastnit, užívat je i disponovat s nimi. Z hlediska již zmíněných alternativních řešení sporů však může být situace v našem případě lepší. Zatímco jiné státy, resp. jejich národní registrátoři, využily možnosti delegovat rozhodování o případných sporech na WIPO podle jednotných principů aplikovaných a vydaných organizací ICANN, v našem případě tomu tak není. Metody ponechání kompetencí na Rozhodčím soudu při HK ČR a AK ČR, který se stal i autorizovanou institucí pro řešení domén generických i evropských nelze nikterak kritizovat, ovšem jediným podkladem pro rozhodování sporů v případě národní domény .cz je naše platná legislativa. Nástroje soft-law přitom mohou rozhodování i kritéria hodnocení výrazně usnadnit a přispět také k mezinárodní unifikaci v přístupu a rozhodování doménových sporů. Z hlediska praktického je nutné pozitivně hodnotit, že pražský rozhodčí soud úspěšně plní funkci takového sjednocovatele.

Dalším zkoumaným a často diskutovaným institutem je ochrana osobnosti a jejího soukromí v on-line prostředí. Internet se stal pro soukromé osoby nezbytnou součástí života. Zejména mladší lidé užívají tuto síť pro komunikaci s ostatními, vytváří virtuální komunity a sdílí mnohé informace včetně těch velmi intimních a důvěrných prostřednictvím velkého fenoménu posledních let, sociálních sítí. Nejen sociální sítě, ale i jinými způsoby mohou být údaje o každém jednotlivci zpřístupněny a dále využity i zneužity jinými osobami. I proto je jednou z hlavních oblastí, na kterou i právní úprava reaguje, zpracovávání osobních údajů. Jak bylo nastíněno, základní principy jsou v rámci evropské právní regulace poměrně jasně stanoveny, přesto však některé oblasti poskytují poměrně široké možnosti provedení a výkladu. I proto je v důsledku dnešního vývoje v mezinárodních vztazích odůvodňováno celkem široké omezování a shromažďování osobních údajů, dále i prováděno odposlouchávání a sledování internetového provozu a komunikace s odůvodněním, že je to nezbytné pro zajištění veřejné bezpečnosti a odhalování protiprávních činů a kriminality. Ukazuje se navíc, že dnešní společnost klade čím dál méně pozornosti a důležitosti ochraně své vlastní osoby a soukromí, a neuvědomují si, jaké důsledky může jejich zpřístupnění mnoha důvěrných informací jiným

uživatelům internetu v budoucnosti přinést. Je nutné brát ohled na soukromí a šetřit zásahy do něj i při prosazování jiných práv a svobod. Tak například již zmíněné tendence uvalit na ISPs povinnosti aktivně zasahovat a bránit protiprávní činnosti v souvislosti s ochranou autorských práv může vést k významnému omezení práv na soukromí v zájmu práv autorských. Zda je to přípustné a je skutečně zájem na autorských právech, tj. právech poměrně úzké skupiny subjektů, vyšší než zájem každého jednotlivce na ochraně svých základních lidských práv a svobod, na to se mohou názory lišit a lze najít jistě mnohé důvody pro i proti. Je však vždy nutné nacházet vhodné vyvážení všech zájmů. Nelze souhlasit s přílišným omezením jednoho práva na úkor práv jiných. Lze si představit například tendence, které se ukazují při implementaci zákona na ochranu autorských práv ve Velké Británii, kdy jednou z podmínek další činnosti a sledování konkrétních uživatelů na výzvu majitelů autorských práv by mělo podle dosavadního záměru být předložení dostatečného důkazu o tom, že dané podezření o konkrétním uživateli je oprávněné. Obdobně je tomu i v případě sledování a odhalování trestné činnosti prostřednictvím internetu. Současný stav například ve Velké Británii lze považovat za nedostatečný. Na rozdíl od pojetí kontinentálního, který na ochranu soukromí klade v tomto ohledu daleko větší důraz a nařídit sledování a odposlouchávání může jedině nezávislý soud, tamní úprava dává tyto pravomoci velmi širokému okruhu institucí. Kromě právních nástrojů je třeba zdůraznit, že ani sebedokonalejší legislativa nemůže nahradit a ochránit chování jednotlivých členů společnosti. Proto i širší upozornění a vzdělávání veřejnosti o možných rizicích a zneužití údajů, které mnozí v internetovém prostředí zpřístupňují je z hlediska budoucího vývoje společnosti velmi důležité.

Bibliografie

Ahmed, S. (2010) *Fast Internet access becomes a legal right in Finland* [online] <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.

Aujezdský., J. (2005) *Rozsudek ohledně domény ceskapojistovna.cz. Co je špatně?* [online] <http://www.itpravo.cz/index.shtml?x=220507>.

Bandurski, D. (2008) *China's Guerrilla War fot the Web*. Far Eastern Economics Review [online] přístupné na adrese <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] přístupné na adrese <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.

Barrett., M. (2007) *Domain Names, Trademarks, and the First Amendment: Searching for Meaningful Boundaries*. Connecticut Law Review. [online] Přístupné na adrese <http://ssrn.com/abstract=928261>.

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] <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.

CARFAC a RAAV (2006) *Proposals for the improvement of the Copyright Act to Favor of the Amelioration of the Socioeconomic Conditions of Canadian Visual artists.* [online] přístupné na adrese <www.raav.org/pls/htmldb/adu?p=528726109203373380>.

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.

Čermák., J. (2005) *Předběžné opatření ve sporu Prace.cz vs. Sprace.cz – rozhodnutí o odvolání*. [online] Přístupné na adrese <http://www.itpravo.cz/index.shtml?x=323025>.

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.

Efroni., Z. (2007) *Names as Domains, Names as Marks: Issues concerning the Interface between Internet Domain Names and Trademark rights*. [online] přístupné na adrese <http://ssrn.com/abstract=957750>.

Electronic Business Law Reports, vol. 1, issue3, pp. 110 – 120 [online] <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>.

Evropská komise (2007) *Report to the Council, the European Parliament and the Economic and Social Committee on the application of Directive 2001/29/EC on the harmonisation of certain*

aspects of copyright and related rights in the information society. [online] přístupné na adrese <http://ec.europa.eu/internal_market/copyright/docs/copyright-infso/application-report_en.pdf>.

Evropská komise (2009) *Creative Content in a European Digital Single Market: Challenges for the Future.* 22. října 2009. [online] přístupné na adrese <http://ec.europa.eu/internal_market/consultations/docs/2009/content_online/reflection_paper%20web_en.pdf>.

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

Fryer., W., T. (2008) *Handling Internet Domain Name Arbitration*. The Maryland Bar Journal. [online] Přístupné na adrese <http://ssrn.com/abstract=1639140>.

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. přístupné na adrese <http://ssrn.com/abstract=595362>.

Helft, M. and Barboza, D. (2010) *Google Shuts China Site in Dispute Over Censorship* [online] <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.

Horáček, R., Čada, L., Hajn, P. (2005) *Práva k průmyslovému vlastnictví*. 1. vydání. Praha: C. H. Beck.

Horáček., R. a Macek., J. (2007) *Sbírka správních a soudních rozhodnutí ve věcech průmyslového vlastnictví*. Praha: C. H. Beck.

Hrubešová., H. (2006) *Proč si neregistrovat doménové jméno pod doménou nejvyššího stupně ".com" aneb jak je to s jurisdikcí amerických soudů.* [online] <http://www.itpravo.cz/index.shtml?x=1928185>.

The Huffington Post (2010) *Google Threatening To Leave China Over Hacking, Email Leak* [online] <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] dostupné na adrese <http://www.ikaros.cz/internet-kontra-copyright>.

Information Commissioner's Office (neuvedeno) *Oficiální instrukce nakládání s osobními údaji*. [online] 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.

KCRG News (2011) *Hadopi: the first registered letters will be leaving soon*. [online] přístupné na adrese <http://kcrg.biz/2011/01/hadopi-the-first-registered-letters-will-be-leaving-soon/>.

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] <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] <http://www.isoc.org/internet/history/brief.shtml>.

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

Liberda., A. (2008) *Předběžná opatření ve sporech o doménová jména*. [online] Přístupné na adrese <http://www.pravoit.cz/article/predbezna-opatreni-ve-sporech-o-domenova-jmena>.

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

Lipton., D., J. (2009) *Bad Faith in Cyberspace: Grounding Domain Name Theory in Trademark, Property and Restitution*. Harvard Journal of Law and Technology [online] <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1484763>.

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

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

Mac Sithigh., D. (2010) *More than Words: The Introduction of Internationalised Domain Names and the Reform of Generic Top-Level Domains at ICANN* [online] University of East Anglia Law School Working Paper No. 2010-DMS-2. Přístupné na adrese <http://ssrn.com/abstract=1715955>.

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.

Mališ., P. (2011) *Co to jsou doménová jména, aneb nad právní povahou doménových jmen*. [online] přístupné na adrese <http://www.elaw.cz/cs/pravo-it/334-co-to-jsou-domenova-jmena-aneb-nad-pravni-povahou-domenovych-jmen.html>.

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] <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] 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.

Nguyen., Xuan-Thao (2001) *Cyberproperty and Judicial Dissonance: The Trouble with Domain Name Classification*. George Mason Law Review. [online] Přístupné na adrese <http://ssrn.com/abstract=1493482>.

OFCOM (2010) *Online Infringement of Copyright and the Digital Economy Act 2010. Draft Initial Obligations Code.* [online] dostupné na adrese <http://stakeholders.ofcom.org.uk/binaries/consultations/copyright-infringement/summary/condoc.pdf>.

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

PC Magazine Online (2010) *"French Anti-Piracy Law Actually Increases Piracy."* [online] 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>.

Pelikánová., R. a Čermák., K., Jr. (2000) *Právní aspekty doménových jmen*. Praha: Linde Praha, a.s. - Právnické a ekonomické nakladatelství Bohumily Hořínkové a Jana Tuláčka.

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>.

Pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů (2008) *Stanovisko k otázkám ochrany údajů v souvislosti s vyhledávači.* Znění účinné od 13.11.2008. [online] přístupné na adrese <http://www.beck-online.cz/legalis/document-view.seam?type=html&documentId=oz5f6mrqga4f6njql44f65lpn52s2ma&groupIndex=1&rowIndex=1&conversationId=659608#selected-node>, publikované též ve Věstníku Úřadu pro ochranu osobních údajů č. 50 z roku 2008.

Raban., P. Moravcová., M. a kol. (2006) *.eu domain name .eu doména.*Praha: C. H. Beck.

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

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

Reed., Ch. a Angel., J. (2007) *Computer Law. The Law and Regulation of Information Technology*. Sixth edition. UK. Oxford: Oxford University Press.

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

Roettgers., J. (2010) *Hadopi Gone Wild: France Plans Spyware for Three Strikes*. [online] dostupné na adrese <http://gigaom.com/video/hadopi-gone-wild-france-plans-spyware-for-three-strikes/>.

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

Sehnalek., D. (2003) *Právní povaha doménového jména*. [online] přístupné na adrese <http://www.itpravo.cz/index.shtml?x=132115>.

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>.

Slováková., Z. (2007) *Průmyslové vlastnictví. I. dotisk druhého, doplněného a rozšířeného vydání*. Praha: LexisNexis CZ s.r.o.

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, 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>.

Úřad na ochranu osobních údajů (2010) *K problémům z praxe č. 4/2010. Zveřejňování osobních údajů na internetu.* [online] přístupné na adrese <http://www.uoou.cz/uoou.aspx?menu=14&loc=729>.

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.

Yee Fen Lim (2007) *Cyberspace Law. Commentaries and Materials. Second Edition.* Australia. South Melbourne, Victoria: Oxford University 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.

Římské úmluva o právu rozhodném pro smluvní závazkové vztahy z roku 1980.

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

Doporučení komise ze dne 18.5.2005 o kolektivní přeshraniční správě autroského práva a práv s ním souvisejících pro zákonné on-line hudební služby. Přístupné též na adrese <http://www.mkcr.cz/assets/autorske-pravo/eu-a-autorske-pravo/07-02753-Doporu_en__EK_o_kolektivn__p_eshrani_n__spr_v__AP_a_pr_v_s_n_m_souvisej_c_ch_pro_z_konn__on-line_hudebn__slu_by__2005_737_ES__1.pdf>.

Nařízení ES č. 593/2008 o právu rozhodném pro smluvní závazkové vztahy (Řím I).

Nařízení ES č. 864/2007 o právu rozhodném pro mimosmluvní závazkové vztahy (Řím II).

Nařízení ES č. 874/2004 z 24. dubna 2004 (týkající se evropské domény .eu, přístupné též na adrese http://www.eurid.eu/files/ec20874_en.pdf).

Nařízení ES č. 44/2001 o příslušnosti a uznávání a výkonu soudních rozhodnutí v občanských a obchodních věcech.

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. 97/1963 Sb. o mezinárodním právu soukromém a procesním.

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. 441/2003 Sb. o ochranných známkách.

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.
Zákon č. 221/2006 Sb., o vymáhání práv z průmyslového vlastnictví.
Zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.
Návrh nového občanského zákoníku, dle stavu k lednu 2011. Návrh i důvodová zpráva jsou k dispozici na adrese <http://obcanskyzakonik.justice.cz/cz/navrh-zakona.html>.

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.
Anti-Cybersquatting Consumer Protection Act (ACPA) z roku 1999
The Controlling the Assault of Non-solicited Pornography and Marketing Act 2003.
Federal Trademark Dilution Act of 1995.

Soft law a další prameny

CZ.NIC (2010) *Pravidla registrace doménových jmen v ccTLD .cz* [online] <http://www.nic.cz/files/nic/doc/Pravidla_registrace_CZ_DSDng_20100101.pdf>.

SK-NIC (2010) *Pravidlá poskytovania menného priestoru v internetovej doméne sk*. [online] <https://www.sk-nic.sk/kontakty/pravidla.10.9.2010.jsp>.

UDRP (Uniform Rules for Domain Name Resolution Policy).

RUDRP (Rules for Uniform DOmain Nams Dispute Resolution Policy).

NOMINET UK (2008) *Dispute Resolution Service Procedure* [online] <http://www.nominet.org.uk/disputes/drs/?contentId=5240>.

NOMINET UK (2008) *Dispute Resolution Service Policy* [online] <http://www.nominet.org.uk/disputes/drs/?contentId=5239>.

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).

Bonier Media Ltd v Smith and Kestrel Trading Corporation 2002.

Braintech Inc. v. Kostiuk (1999) 171 DLR 4th 46 (BCCA).

Campbell v UK [1993] 15 EHRR 137.

Euromarket Designs Inc v Peter & Another 2000.

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.

Helicopteros Nacionales de Colombia, SA v. Hall, 466 US 408, 414-16 1984.

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.

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.

Name.Space, Inc. v. Network Solutions, Inc., 202 F.3d 573 (2d Cir. 2000).

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

Panavision Internation L.P. v Toeppen 141 F.3 z roku 1998.

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.).

World-Wide Volkswagen Corp v. Woodson, 444 US 286, 297 1980.

Rozhodčí nález Rozhodčího soudu při HK ČR a AK ČR, *Rozhodnutí č. 00013* uveřejněné 8.10.2010. přístupné na adrese <http://domeny.soud.cz/adr/decisions/index.php>.

Rozhodnutí Rozhodčího soudu HK ČR a AK ČR *ve věci doménového jména čSOB.eu* z roku 2010, přístupné na adrese <http://eu.adr.eu/adr/decisions/decision.php?dispute_id=5670>.

Shrnutí

Internet se stal největším fenoménem posledních dvou desítek let. Výrazným způsobem působí na společnost a mění její chování v soukromém, obchodním i veřejném životě. Snadným propojením s téměř jakoukoli částí světa se stala dnešní společnost skutečně globální. Usnadnění a výrazné urychlení komunikace a přenosu i dat poměrně velkého objemu s sebou přináší i mnohé obtíže a rizika. Z tohoto důvodu se tato práce zaměřila na některé jevy a odpovídající právní instituty, včetně těch, které jsou díky vývoje internetu povahy zcela nové. Práce je rozdělena do čtyř hlavních částí podle oblastí, kterých se týká. První část se věnuje obecným otázkám internetu, jeho vzniku a základních otázek z hlediska jeho struktury, fungování a právních dopadů. Další část popisuje internet z pohledu práv autorských a dopadů na tento právní institut. Právní dopady P2P sítí, postavení ISPs a legislativní vývoj v některých zemích, jehož důsledkem je omezování základních lidských práv a svobod ve prospěch vyšší efektivity při aplikaci autorskoprávní legislativy, je rovněž předmětem této části. Třetí část se zabývá zcela novým institutem, doménovými jmény. Přestože jejich právní povaha v mnoha zemích včetně České Republiky není dosud zcela jasná, tento nástroj může mít mnohé obchodněprávní i ekonomické dopady. Poslední institut zkoumaný v prostředí internetu je ochrana soukromí a dalších aspektů osobnosti. Globální komunikační prostředek, který je snadno přístupný širokému počtu uživatelů, s sebou zároveň nese snadnější přístup k veškerým informacím, včetně těch osobních i důvěrných. Popsány jsou tedy právní důsledky chování jednotlivých aktérů na internetu, zasahování do osobnosti druhého, získávání a jiné formy zpracování osobních údajů, užívání různých údajů pro obchodní či jiné účely, rozvoj a možné dopady sociálních sítí a v neposlední řadě též metody vyšetřování a odhalování trestné činnosti páchané prostřednictvím internetové sítě.

Summary

The internet has become the biggest phenomenon of last two decades. In a significant manner it affects our society and changes its behaviour in private, commercial and public life. Through an easy connection with almost any part of the world our current society has become global indeed. Facilitation and significant acceleration of communication and transfer of relatively large amount of data bears many difficulties and risks. Therefore this thesis is focused on some aspects and corresponding legal concepts, including those, which are of entirely new nature because of the internet evolvement. The work is divided into four main parts according to areas they are related to. First one introduces general matters of the internet, its formation and fundamental issues of its structure, operation and legal consequences. Next part describes the internet from the scope of copyright and impacts on this legal concept. Legal implications of P2P networks, position of ISPs and statutory development in some countries whereof consequence is the limitation of fundamental human rights and freedoms in favour of higher efficiency in application of copyright protection is also subject of this chapter. Third part concerns entirely new instrument and concept – domain names. Though its legal nature is not defined and perfectly clear in many countries including the Czech Republic, this instrument may have many commercial and economic impacts. Last concept analysed in the environment of internet is the protection of privacy and other aspects of personality. Global communication tool, which is easily accessible to a large number of users, means also easily available information and data, including personal and confidential ones. Legal consequences of a conduct of each subject to the internet are described as well as the interference into others personality; collection and other form of processing of personal data; usage of different data for commercial and other purposes; development and eventual impact of social networks; and last but not least methods of investigation and disclosure of criminal acts committed by means of the internet network.

Klíčová slova: internet, autorské právo, peer-to-peer sítě, doménová jména, ochrana osobnosti

Key words: internet, copyright, peer-to-peer networks, domain names, protection of personality