UNIVERZITA KARLOVA V PRAZE

PRÁVNICKÁ FAKULTA

DIPLOMOVÁ PRÁCE

2009 Milada Kürtösiová

Univerzita Karlova v Praze

Právnická fakulta

Milada Kürtösiová

Ochrana osobních údajů

(Personal Data Protection)

Diplomová práce

Vedoucí diplomové práce: Doc. JUDr. Vladimír Vopálka CSc.

Katedra správního práva

Datum vypracování práce: 1.12.2009

Prohlášení

Prohlašuji, že jsem předkládanou diplomovou práci na téma „**Ochrana osobních údajů**“ vypracovala samostatně za použití zdrojů a literatury v ní uvedených.

V Praze dne _____

_____

Milada Kürtösiová

Obsah

Seznam použitých zkratek

Centrální úložiště	Centrální úložiště elektronických receptů
ČR	Česká republika
EK	Evropská komise
ES	Evropská společenství
EU	Evropská unie
ICCP	Kimise pro oblasti informací, počítačů a komunikace (*Committee for Information, Computer and Communication Policy*)
Komise	Evropská komise
OECD	Organizace pro hospodářskou spolupráci a rozvoj
OECD Guidelines	Pravidla pro ochranu soukromí a přeshraniční toky osobních údajů *(Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)*
OSN	Organizace spojených národů
Pracovní skupina WP29	Pracovní skupina pro ochranu osob s ohledem na zpracování osobních údajů (*Working Party on the Protection of Individuals with regard to the Processing of Personal Data*)
Směrnice	Směrnice Evropského parlamentu a Rady č. 95/46/ES, ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
SÚKL	Státní ústav pro kontrolu léčiv
Úmluva č. 108	Úmluva č. 108 – na ochranu osob se zřetelem na automatické zpracování osobních dat
Úřad	Úřad pro ochranu osobních údajů
USA	Spojené státy americké
WPISP	Skupina pro informační bezpečnost a ochranu osobních údajů (*Working Party on Information Security and Privacy Policy*)
Zákon	Zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů

Úvod

Přestože ke zpracování osobních údajů lidí docházelo vždy, v různé podobě, zájem o problematiku ochrany osobních údajů spojujeme především s moderní dobou a rozvojem vyspělých technologií. Stále častěji se hovoří o zpracování osobních údajů, o možnosti jejich zneužití či krádeži. Ochrana osobních údajů se stala jakýmsi novým rozměrem práva na soukromí. Ale je tomu skutečně tak? Norman Lewis, autor článku „Právo na soukromí v době Facebooku" (ang. *Right for Privacy in the Age of Facebook"*) ilustruje vnitřní rozpory, které jsou v pojmu práva na soukromí (a ochrany osobních údajů) obsaženy: *„můžeme setkat s lidmi, kteří se budou velmi zajímat o shromažďování jejich osobních údajů a jejich možného zneužití ze strany státu, ale na druhé straně schopnými odhalovat jejich nejhlubší osobní myšlenky na sociálních sítích"*.

Při zadání hesla „ochrana osobních údajů" do internetového vyhledávače Google zjistíme, že máme na výběr takřka z 1 930 000 odkazů. Pokud položíme ten samý dotaz v anglickém jazyce („ *personal data protection"*) Google nám nabídne dokonce 2 430 000 možných odpovědí. Je tedy zřejmé, že ochrana osobních údajů představuje téma, které jde ruku v ruce s pokrokem vědy a moderních technologií. S určitou nadsázkou můžeme říci, že s každým dalším dnem (a s každým dalším člověkem používajícím moderní komunikační technologie) se svět okolo nás stává menším. Naše osobní údaje již dávno nejsou zpracovávány ve státech, kde jsme občany nebo kde žijeme – naše osobní údaje jsou často předávány do zahraničí, tedy cestují a žijí do jisté míry vlastní život. V citovaném článku pak N. Lewis pokládá otázku „*Je dnes ještě možné tvrdit, že ochrana osobních údajů je stále důležitá*?"[1]

Přestože většina lidí intuitivně vnímá obsah pojmů osobní údaje, jejich zpracování a předávání, ukazuje se v praxi, že právní vymezení těchto pojmů je poněkud odlišné. Jaké jsou tedy základní pojmy, se kterými se v oblasti ochrany osobních údajů setkáváme a jaké jsou jejich vzájemné základní vazby? Jaké instituce a organizace se touto oblastí zabývají? To jsou otázky, na které by měla odpovědět tato diplomová práce.

[1] Ang. *Can one serisously argue that privacy is generally regarded as important today?*

Velmi často slyšíme, že „osobní údaje jsou předávány do zahraničí“ nebo „jsou zpřístupňovány členům skupiny společností“. Co však tyto termíny znamenají? Je možné osobní údaje do zahraničí libovolně předávat nebo jsou zde nějaká omezení? Jaké možnosti při předávání osobních údajů mají jednotlivé subjekty k dispozici? Je všeobecně známo, že dnešní doba je charakterizovaná doslova raketovým růstem užití informačních technologií. Reaguje právní rámec na tento rozvoj? I tyto otázky by měly být zodpovězeny v rámci této diplomové práce.

Jak již v samotném úvodu této práce zaznělo – ochrana osobních údajů je tématem veskrze aktuálním, tématem, v rámci kterého jsou denně diskutovány nové podněty, otázky i problémy. Z tohoto důvodu by v této diplomové práci neměla chybět část věnující se aktuálním otázkám, kde by bylo možné seznámit čtenáře s některými zajímavými případy či problémy, které se týkají problematiky ochrany osobních údajů.

Vlastní diplomová práce je rozčleněna do tří kapitol. První kapitola má za úkol čtenáře uvést do problematiky ochrany osobních údajů a jejího regulatorního rámce. Smyslem této kapitoly je poskytnout obraz vývoje právní úpravy ochrany osobních údajů v historii, seznámit čtenáře s její současnou podobou a především poskytnout určitý vhled do používané terminologie. Nelze opomenout ani institucionální rámec související s oblastí ochrany osobních údajů, a to jak na úrovni české, evropské nebo mezinárodní.

Druhá kapitola se již zaměřuje na vlastní problematiku ochrany osobních údajů v rámci jejich předávání do zahraničí. V rámci kapitoly se čtenář seznámí s právním rámcem předávání osobních údajů do zahraničí, s různými možnostmi, které se nabízejí, s jejich výhodami a úskalími.

Na závěr diplomové práce je zařazena kapitola, v rámci níže jsou představeny témata z oblasti ochrany osobních údajů, která jsou v současnosti diskutována nebo ta, která vyvolávají některé zajímavé otázky a problémy.

Téma ochrany osobních údajů je, nicméně, natolik široké, že nemůže být komplexně pojato v jediné vědecké práci. Z tohoto důvodu je v této diplomové práci kladen důraz na aktuální aspekty problematiky a zejména na oblast předávání osobních údajů do zahraničí, které byla v českém prostředí věnována zatím jen menší pozornost.

Tato diplomová práce byla zpracovávána především na podkladě zahraničních zdrojů dostupných prostřednictvím internetu, a to právě s ohledem na aktuálnost zvoleného tématu a na nedostatek české literatury. Autorka diplomové práce vycházela z podkladů a z právní úpravy, která byla k dispozici, ke dni 1. prosince 2009.

1 Úvod do problematiky ochrany osobních údajů

Problematika ochrany osobních údajů představuje, jak již bylo nastíněno v úvodu této práce, ze své povahy nejen téma, které je veskrze aktuální, ale navíc téma, které se dotýká každého z nás. V dnešním světě, propojeném v procesu globalizace médii a jinými technickými prostředky, dochází stále častěji k nejrůznějším formám shromažďování a zpracování osobních údajů, a to včetně zpracování formou předávání osobních údajů do zahraničí. Předtím, než se tato diplomová práce zaměří na vlastní problematiku předávání osobních údajů do zahraničí, je vhodné si téma ochrany osobních údajů představit, a to z hlediska historických kořenů, současné právní úpravy a stejně tak z pohledu základních stavebních prvků a principů ochrany osobních údajů tak, jak jsou zohledněny v české právní úpravě. Na závěr je též začleněn nástin institucionálního rámce, včetně stručné informace o některých nevládních organizacích, které se této problematice věnují.

1.1 Prameny právní úpravy v ochraně osobních údajů

1.1.1 Mezinárodní a evropská právní úprava

Při hledání základů právní úpravy ochrany osobních údajů je potřeba mít na paměti, že osobní údaje představují jen jeden z mnoha aspektů týkajících se osobnosti člověka a jeho života. Je ve všeobecném povědomí, že problematika ochrany lidských práv a svobod se dostává do středu zájmu mezinárodního společenství po druhé světové válce, zejména v souvislosti se založením a vznikem Organizace spojených národů (OSN) a posléze s přijetím **Všeobecné deklarace lidských práv a svobod** (1948)[2], která se později stala jedním z nejvýznamnějších dokumentů svého druhu a rovněž inspirací pro činnost dalších mezinárodních institucí a organizací a pro přijímání dalších mezinárodních smluv, věnujících se též problematice ochrany osobních údajů.

[2] Všeobecná deklarace lidských práv ve svém článku 12 stanoví, že *„nikdo nesmí být vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence, ani útokům na svou čest a pověst, každý má právo na zákonnou ochranu proti takovým zásahům nebo útokům“*.

V případě evropské právní úpravy (ve smyslu právní úpravy týkající se celého evropského kontinentu) nalezneme základní kameny ochrany osobních údajů v **Evropské úmluvě o ochraně lidských práv a svobod** (1950), a to konkrétně v rámci ochrany soukromého a rodinného života. V článku 8 úmluva stanoví, že „*každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence*“[3] a v rámci ustanovení článku 10 týkajícího se práva svobody projevu - „*každý má právo na svobodu projevu. Toto právo zahrnuje svobodu zastávat názory a přijímat a rozšiřovat informace nebo myšlenky bez zasahování státních orgánů a bez ohledu na hranice…*“[4] Obsah výše-uvedených základních lidských práv je dotvářen v procesu vývoje zejména judikaturou **Evropského soudu pro lidská práva**.[5]

Během 60. a 70. let 20. století se v souvislosti s rozvojem informačních technologií nabízela stále silněji otázka, zda je tehdejší úroveň ochrany osobních údajů postačující a zda není potřeba právní úpravu revidovat. Průzkum provedený na žádost Parlamentního shromáždění Rady Evropy v evropských státech potvrdil skutečnost, že národní (ani dosavadní mezinárodní) úprava neposkytuje soukromí jednotlivců dostatečnou míru ochrany.[6] Navíc se ukazovalo, že rostoucí propojení a možnost pohybu informací mezi státy, a stále častější předávání osobních údajů do zahraničí, bude potřeba řešit cílenou úpravou zaměřenou na ochranu osobních údajů, a to jak na úrovni národní, tak na úrovni evropské a mezinárodní.[7]

Rok 1980 přinesl v oblasti ochrany osobních údajů další významný posun – Organizace pro hospodářskou spolupráci a rozvoj (OECD) přijala **Pravidla pro ochranu soukromí a přeshraniční toky osobních údajů** *(Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)*(dále též jako „**OECD Guidelines**“). Přestože tento dokument není právně závazný a má spíše povahu doporučení, formuluje některé zásadní principy ochrany osobních údajů, které by měly být v oblasti ochrany osobních

[3] Evropská Úmluva o ochraně lidských práv a základních svobod ze dne 4. listopadu 1950, článek 8.
[4] Tamtéž, článek 10.
[5] Viz. například EUROPEAN COURT OF HUMAN RIGHTS. *Key case law-issues. The concepts of „private and family life“* ze dne 24.ledna 2007 anebo EUROPEAN COURT OF HUMAN RIGHTS. *Key case law-issues. The concepts of „home and correspondence“* ze dne 31. ledna 2007
[6] Zákon o ochraně osobních údajů. Komentář, s.25
[7] V letech 1973 a 1974 byly vypracovány dvě rezoluce Výboru ministrů ES týkající se ochrany dat v soukromém a posléze veřejném sektoru. Během 80. let 20. století se ochrany osobních údajů začíná být upravována formou přijímání národní legislativy např. v Německu či Švédsku a v některých státech dokonce byla upravena na nejvyšší, ústavní rovině (např. Rakousko). Více viz. Zákon o ochraně osobních údajů. Komentář, s.26

údajů dodržovány i v současné době. O významu tohoto dokumentu a vůli států uvedené principy respektovat svědčí i skutečnost, že mnohé z nich se podařilo promítnout do dalších, již právně závazných mezinárodních úmluv, a rovněž do Směrnice Evropského parlamentu a Rady č. 95/46/ES, ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Z principů formulovaných těmito pravidly je možné zmínit zejména princip omezeného shromažďování osobních údajů, který je vyjádřením evropského pohledu na ochranu osobních údajů – jako na oblast ochrany soukromí a součást lidských práv jedince. Další zásady stanovené v těchto pravidlech OECD jsou uvedeny dále, v podkapitole věnované principům ochrany osobních údajů.

Dalším výrazným posunem v oblasti ochrany osobních údajů bylo přijetí **Úmluvy č. 108 – na ochranu osob se zřetelem na automatické zpracování osobních dat** ze dne 28. ledna 1981, v rámci Rady Evropy (dále jen „**Úmluva č.108**“). Tato úmluva byla za Českou republiku ratifikována dne 9. července 2001 a v platnosti je na území našeho státu ode dne zveřejnění ve sbírce mezinárodních smluv, tj. od dne 1. listopadu 2001.[8]

V preambuli Úmluva č. 108 zmiňuje jeden ze svých cílů, totiž *„rozšířit ochranu práv a základních svobod každého, zejména právo na soukromý život, se zřetelem k zesílenému toku automatizovaně zpracovávaných osobních údajů přes hranice.“*[9] Cílem tedy bylo chránit osobní údaje každé osoby, která se nachází na území daného smluvního státu v souvislosti s automatizovaným zpracováním osobních údajů (včetně jejich předávání do zahraničí). Novinkou, oproti předchozí úpravě, je právě částečná úprava problematiky předávání osobních údajů do zahraničí. Podle definice pojmů v této úmluvě se automatizovaným zpracováním osobních údajů rozumí celá řada činností v úmluvě vyjmenovaných, bez ohledu na to, zda jsou vykonávány zcela či jen částečně automatizovaně, a to: *„ukládání na nosiče dat, provádění logických a/nebo aritmetických operací s těmito daty, jejich změna, výmaz, vyhledávání nebo rozšiřování“*.[10] Je zřejmé, že Úmluva č. 108 měla za cíl reagovat na technický vývoj a rozvoj moderních metod zpracování a uchovávání osobních údajů. Úmluva č. 108 je koncipována jako určitý minimální základ pro právní úpravu v oblasti ochrany osobních údajů, o čemž svědčí

[8] Úmluva č. 108 byla podepsána dne 8. září 2001, ratifikována 9. července 2001 a zveřejněna ve Sbírce mezinárodních smluv pod č. 115/2001, dne 1. listopadu 2001.
[9] Úmluva č. 108, Preambule.
[10] Úmluva č. 108, čl. 2 – definice, pís. (c)

i možnost smluvních stran rozšířit její aplikovatelnost i na ne-automatizovaná zpracování osobních údajů. V této souvislosti nelze opomenout skutečnost, že v době přijetí Úmluvy č. 108 již probíhají integrační tendence mezi státy Evropských společenství (a tedy členských států Rady Evropy) a objevuje se stále častěji s tím související volání po svobodě pohybu (včetně svobody pohybu informací). Právní úprava ochrany osobních údajů obsažená v Úmluvě č. 108 je postavena na respektování základních zásad tam uvedených, jako jsou: požadavky týkající se kvality údajů a jejich zpracování, dále zabezpečení osobních údajů při jejich zpracování, respektování zvýšené míry ochrany poskytované specifickým kategoriím osobních údajů, stanovení sankcí a opravných prostředků jako nástrojů zabezpečujících realizaci ochrany osobních údajů a požadavky stanovené při pohybu osobních údajů přes hranice států.[11] Z hlediska úpravy předávání osobních údajů do zahraničí v Úmluvě č. 108 je zásadní zavedení principu volného pohybu zpracovávaných osobních údajů přes hranice, mezi smluvními stranami.[12] Význam Úmluvy č. 108 je z hlediska vývoje problematiky ochrany osobních údajů zásadní. Možnost smluvně převzít závazky vyplývající z Úmluvy č. 108 je dána rovněž nečlenským státům Rady Evropy; do současné doby byla tak úmluva ratifikována celkem čtyřiceti jedna státy. [13]

K dalšímu zásadnímu posunu v oblasti právní úpravy ochrany osobních údajů došlo až přijetím Směrnice Evropského parlamentu a Rady č. 95/46/ES, ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „**Směrnice**“). Členským státům Evropských společenství (ES) byla dána transpoziční lhůta v délce tří let k tomu, aby právní úpravu vymezenou v této Směrnici převedly (transponovaly) do svých právních řádů. Oproti předchozí Úmluvě č. 108 se Směrnice dotýká nejen automatizovaného, ale i manuálního zpracování osobních údajů. Z textace úvodních ustanovení Směrnice je zřejmé, že mezi hlavní cíle přijetí Směrnice patří usnadnění volného pohybu osobních údajů a tím umožnění dalšího rozvoje vnitřního trhu ES (dnes EU), to vše při respektování základních lidských práv

[11] Více viz. čl.4-čl.12 Úmluvy č. 108
[12] Úmluva č. 108 stanoví rovněž výjimky z tohoto principu volného pohybu osobních údajů přes hranice mezi smluvními stranami, a to jednak z důvodů ochrany specifických, stanovených, kategorií osobních údajů (za předpokladu, že druhá strana těmto osobním údajům nemůže zaručit „stejnou míru ochrany“) a jednak pokud by mělo jít o přenos přes území smluvní strany Úmluvy č. 108, přičemž konečným cílem zpracovávaných osobních údajů by byl nesmluvní stát (s cílem obcházení právní úpravy ve státě zdrojovém).
[13] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; CETS No.: 108; Status as of: 15/2/2009.

a svobod. Základním východiskem je úvaha, že rozdílná úprava ochrany osobních údajů ve členských státech, a tím pádem i rozdílná míra ochrany, která je poskytována osobním údajům (a základním lidským právům – právu na ochranu soukromí a rodinného života), může vytvářet překážky volného pohybu těchto osobních údajů. Následně může ovlivňovat vznik překážek z hlediska volného pohybu osob, zboží, služeb, kapitálu, dokonce může negativně působit na hospodářskou soutěž. Zároveň je zdůrazněno, že ochrana osobních údajů podle této Směrnice je poskytována všem fyzickým osobám na území ES (respektive EU) a též, že podřídit se právní úpravě vymezené Směrnicí budou muset všechny osoby, i právnické, bez ohledu na právní formu a charakter, na které dopadá působnost práva ES. Stěžejním východiskem pro právní úpravu vymezenou ve Směrnici je zákaz omezování volného pohybu osobních údajů mezi členskými státy odůvodňovaný ochranou základních lidských práv a svobod, zejména právem na soukromí.

Na závěr připomeneme, že s ohledem na stále větší význam informačních technologií jsou připravovány i právní předpisy zaměřující se na s tím spojené specifické aspekty ochrany osobních údajů – například Směrnice Evropského parlamentu a Rady č. 2000/31/ES ze dne 8. června 2000, o určitých aspektech služeb informační společnosti, zejména elektronického obchodního styku v rámci vnitřního trhu a Směrnice Evropského parlamentu a Rady č. 2002/58/ES ze dne 12. července 2002, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací.[14]

1.1.2 Právní úprava ochrany osobních údajů v českém právním řádu

Česká právní úprava ochrany osobních údajů vychází ze stejných zásad, jako právní úprava mezinárodní a evropská, a jejím základem jsou výše-uvedené mezinárodní úmluvy (v souladu s principem přednosti mezinárodních smluv před zákonem zakotveném v ustanovení článku 10 Ústavy ČR). Zásady ochrany soukromí, rodinného života, včetně tajemství dopravovaných zpráv a souvisejícího práva na informace jsou

[14] Tato směrnice byla změněna Směrnicí Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006, o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES

zakotveny též v ústavním pořádku, konkrétně v ustanoveních Listiny základních lidských práv a svobod.[15]

Nejdůležitější právní předpis našeho právního řádu, který se věnuje specificky oblasti ochrany osobních údajů, nalezneme v podobě **zákona č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů** (dále jen „**Zákon**“)[16]. Navzdory skutečnosti, že se jedná o poměrně mladý zákon, byl již mnohokrát novelizován, zejména v souvislosti se vstupem České republiky do Evropské unie. Základní principy právní úpravy ochrany osobních údajů vymezené tímto Zákonem jsou nastíněny v další části této kapitoly. Z dalších souvisejících zákonů je potřeba zmínit zákon č. 480/2004 Sb., o některých službách informační společnosti, ve znění pozdějších předpisů (dále jen „**zákon o službách informační společnosti**“), který „*upravuje v souladu s právem Evropských společenství odpovědnost a práva a povinnosti osob, které poskytují služby informační společnosti a šíří obchodní sdělení*“[17]. V dnešní moderní době má tento zákon stále větší význam s ohledem na rostoucí počet marketingových materiálů zasílaných formou elektronických zpráv (e-mailů nebo textových zpráv), ať už zasílaných v souladu s principy v tomto zákoně uvedenými nebo v rozporu s tímto zákonem[18]. Z dalších zákonů můžeme zmínit zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (dále jen „**zákon o elektronických komunikacích**“), ve znění pozdějších předpisů.

Dále je potřeba upozornit, že s aspekty ochrany osobních údajů (respektive aspekty souvisejícími se zpracováním osobních údajů) se setkáváme v celé řadě dalších specifických zákonů, které se dotýkají zejména důležitých veřejných zájmů, jako jsou například: obrana ČR, ochrana veřejného pořádku a vnitřní bezpečnosti, předcházení, vyhledávání, odhalování trestné činnosti a stíhání trestných činů nebo například též výkonu kontroly, dozoru, dohledu a regulace spojených s výkonem veřejné moci.[19]

---

[15] Viz ustanovení článků 7, odst. 1, a čl. 13 a 17 Listiny základních lidských práv a svobod.
[16] Předchůdcem současného Zákona byl zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech (zrušen současným Zákonem).
[17] § 1 zákona o službách informační společnosti
[18] § 7, tamtéž.
[19] Viz například Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky, ve znění pozdějších předpisů; zákon č. 283/1991 Sb., o Policii České republiky, zákon č. 166/1993 Sb., o Nejvyšším kontrolním úřadu. Přehled souvisejících právních předpisů je možné najít na stránce Úřadu pro ochranu osobních údajů (www.uoou.cz), v sekci „Právní předpisy“, a dále v podsekci „Oblasti zpracování osobních údajů“

1.1.3 Revize právní úpravy

Vzhledem k tomu, že Směrnice byla přijata v roce 1995 (Zákon v roce 2000) objevuje v současnosti stále častěji volání po revizi těchto základních kamenů současné právní úpravy ochrany osobních údajů v Evropské unii (respektive v České republice). Hlavními argumenty jsou zejména technologický pokrok, nové způsoby zpracování osobních údajů a rozšiřování možností jejich zpracování, ale i větší prostor pro jejich zneužití. Navzdory konstrukci Směrnice i Zákona jako obecných právních předpisů se ukazuje, že v mnoha případech vznikají otázky, jak je na určité moderní způsoby zpracování osobních údajů aplikovat. Prozatím byly tyto situace řešeny zpravidla formou vydávání stanovisek Pracovní skupiny WP29 (viz například kapitola 3, sociální sítě), nicméně není pochyb o tom, že nastal čas pro revizi Směrnice a následnou odpovídající harmonizaci národních legislativ.

Jedním z prvních, poměrně komplexních, materiálů na toto téma vznikl, nese označení „Revize evropské směrnice o ochraně osobních údajů.“[20] Za velice zajímavé považuji některé návrhy na změny v pojetí evropské ochrany osobních údajů. První výzvu, totiž zaměřit se na praktickou aplikaci revidované právní normy, na její přizpůsobení skutečným rizikům v této oblasti, nelze než přivítat. Autoři této zprávy zmiňují tzv. „*risk-based approach*“, tedy přístup vycházející z hodnocení rizik. Přestože tento prvek by snad na první pohled mohl být nahlížen jako vnášení ekonomických přístupů do oblasti práva, domnívám se, že je velmi vhodný a žádoucí. Současná právní úprava (poplatná době svého zrodu) je zaměřena spíš obecně a právě proto zaostává za metodami zpracování osobních údajů, ale především za metodami zneužívání osobních údajů. Autoři práce dále apelují na vytvoření základního výkladového dokumentu (jakési „charty“ nebo „listiny“)[21], který by sjednotil výklad terminologie v oblasti ochrany osobních údajů napříč Evropskou unií.

Za jeden z klíčových návrhů považuji odklon od současného principu oznamovacího k principu naprosto opačnému. Autoři navrhují, aby oznamovací povinnosti podléhala jen taková zpracování osobních údajů, která vytvářejí silný potenciál rizika anebo jsou

[20] Volně přeloženo z anglického „Review of the European Data Protection Directive“; tento dokument vznikl na podnět Information Commissioner Office v květnu roku 2009 v RAND Corporation.
[21] Autoři používají termín „Charter for European DPAs“ –tedy „Charta pro Evropské orgány ochrany osobních údajů“ (volně přeloženo).

složitá. Přestože rozumím kritice oznamovacího principu z hlediska skutečné efektivnosti, nemohu považovat tento návrh za aplikovatelný a skutečně řešící problém transparentnosti zpracování osobních údajů. Tento návrh totiž, podle mého názoru, přibližuje evropskou právní úpravu americkému konceptu „sebe-regulace“, ale především povede k zmenšení možnosti kontroly a skutečné vymahatelnosti práva v ochraně osobních údajů. Jinak řečeno, tento koncept nemůže být akceptovatelný za podmínky, že bude postaven na základech současné, existující právní úpravy.

Druhá skupina návrhů na revizi Směrnice se zaměřuje na princip „odpovídající míry ochrany osobních údajů“, jakožto klíčového požadavku pro předávání osobních údajů do zahraničí. Na tomto místě autoři vyzývají k větší míře použití standardních smluvních doložek a závazných podnikových pravidel (k oběma pojmům viz dále). Především autoři volají po zaměření pozornosti nikoliv na hodnocení právní úpravy a přístupů v oblasti ochrany osobních údajů (ve státě, kam mají být osobní údaje předávány), ale na skutečnou vymahatelnost práva, na skutečnou nezávislost orgánů ochrany osobních údajů a roli judikatury. Takovýto přístup by jednoznačně znamenal přínos pro subjekty údajů, pro ochranu jejich osobních údajů, nicméně je otázkou, zda je v současné době v praxi realizovatelný.

Za přínosný považuji názor autorů zmíněné zprávy, že by bylo vhodné do oblasti ochrany osobních údajů zavést prvek tzv. „*best-practices*“, tedy poměřovat požadavky kladené na ochranu osobních údajů s takovými přístupu, které jsou v dané době z hlediska účelu, tedy ochrany osobních údajů, nejlepší dostupné[22].

Jak bude osvětleno dále, jedním z klíčových problémů současné právní úpravy ochrany osobních údajů je, že jde zde rozdíl mezi tím, jak svá práva vnímají ti, k jejichž ochraně normy ochrany osobních údajů slouží a jak jsou tyto normy odborníky, tedy právníky, interpretovány. Z tohoto důvod autoři správně volají po větší spolupráci s podnikatelskou sférou (tedy nejčastějšími správci a zpracovateli osobních údajů) a s organizacemi k ochraně spotřebitelů. Tyto návrhy považuji za snahu iniciovat jakousi

[22] Uplatnění tohoto nového prvku by však vyžadovalo vyřešit otázku zpřístupňování nebo informování dotčené veřejnosti o tom, co je obsahem těchto principů. Částečnou inspiraci by bylo možné hledat v odvětví práva životního prostředí, kde se tyto principy již uplatňují delší dobu.

celospolečenskou diskusi na téma ochrany osobních údajů, což je, dle mého soudu, v současné době nezbytné.

V souvislosti s českou právní úpravou se v současné době návrhy na revizi právní úpravy zaměřují na některé ad hoc aspekty jakou jsou kamerové systémy nebo řešení problémů v souvislosti se zpracováním osobních údajů z receptů na léky. Prozatím však chybí návrhy na nějaké koncepční řešení.

1.2 Základní pojmosloví a principy v ochraně osobních údajů

Východiskem pro výklad problematiky ochrany osobních údajů při předávání do zahraničí je nepochybně osvětlení základní terminologie používané v této oblasti. Ochrana osobních údajů vždy představovala důležitý prvek ochrany soukromí fyzických osob, avšak v době dnešní tzv. informační společnosti potřeba ochrany osobních údajů získává zcela nové rozměry. V tomto smyslu se rovněž vyjádřil i Nejvyšší správní soud ve svém rozhodnutí 9 As 34/2008 ze dne 12.2.2009, ve kterém uvádí *„nepopiratelnou skutečností zároveň je, že jedním z nejohroženějších lidských práv v podmínkách současné „informační společnosti" je právo na soukromí….plná identita fyzické osoby v současných podmínkách technologicky vyspělé společnosti, tj. za vysokého stupně rozvoje elektronických a jiných médií, která jsou většině populace snadno dostupná, ve své podstatě neznamená nic jiného, než možnost tuto osobu určitým způsobem kontaktovat, aniž by bylo nutné znát místo jejího aktuálního pobytu.*"

1.2.1 Subjekt údajů a druhy osobních údajů

Základním stavebním prvkem tématu ochrany osobních údajů je, samozřejmě, pojem samotného osobního údaje – v současné právní úpravě (§ 4, odst. 1, pís. (a) Zákona) je definován jako *jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu*. Při posuzování zpracovávání osobních údajů z hlediska jejich ochrany vždy máme na mysli osobní údaje (data, informace) vztahující se k fyzické osobě, kterou

v této souvislosti označujeme jako tzv. subjekt údajů.[23] Zjednodušeně je možno říci, že osobní údaje představují jakýsi klíč, na základě kterého je možné k tomuto osobnímu údaji přiřadit konkrétní osobu, a to jak přímo, tak nepřímo. Stejně tak je možné si představit situaci, kdy k identifikaci subjektu údajů nebude stačit jeden jediný údaj či informace, ale kdy bude daný subjekt určitelný až na základě souhrnu těchto informací, které bude možné v jejich propojení za osobní údaje považovat.[24] Až do roku 2007 byl pojem osobního údaje vymezen též negativně, tj. o osobní údaj se nejednalo tehdy, pokud by *bylo třeba ke zjištění identity subjektu nepřiměřené množství času, úsilí či materiálních prostředků*. Současná právní úprava již toto vymezení neužívá a reflektuje tak přesněji jednak mezinárodní i evropskou právní úpravu, jednak umožňuje pojem osobního údaje chápat v širším smyslu. Právní úprava se tak snaží reagovat na technický a kulturní rozvoj společnosti a tím vznikající prostor pro zpracování (respektive možnost zneužití) osobních údajů.

Navzdory skutečnosti, že ochrana osobních údajů je téma, které není úplně nové a které je poměrně často diskutováno, ukazuje se, že stále existují pochyby o tom, co jsou osobní údaje a co nikoliv, a tedy kdy se tato právní úprava má aplikovat. Pro ilustraci je možné zmínit kauzu v souvislosti s činností Fondu ohrožených dětí, která byla diskutována na počátku roku 2009. Tato instituce na svých webových stránkách uvedla nejen fotografie dětí, které byly k dispozici pro adopci, ale rovněž připojila celou řadu jejich citlivých osobních údajů.[25] Tento případ ukázal nejen na to, že mezi veřejností neexistuje dostatečné povědomí o problematice ochrany osobních údajů. Velmi důležitou otázkou, která v této v souvislosti vyvstala (a která byla jedním z hlavních argumentů pro publikaci osobních údajů těchto dětí na zmíněných internetových stránkách) bylo, zda ochrana osobních údajů má přednost před právem těchto dětí být součástí rodiny, být vybrán k adopci, respektive, zda ochrana osobních údajů, součást práva na ochranu soukromí, nezasahuje a neomezuje příliš jiná, důležitá práva dětí (subjektů údajů). Domnívám se, že principy ochrany osobních údajů měly být v této souvislosti

[23] Současná právní úprava (mezinárodní, evropská i česká) upravuje pouze zpracování osobních údajů fyzických osob.
[24] V roce 2001 Úřad pro ochranu osobních údajů vyslovil zajímavý názor, že z hlediska možné identifikace subjektu správce osobních údajů „*je rozhodující je skutečnost, že správce identifikaci osob "vlastní" nebo ji může bez vynaložení neúměrného úsilí získat*“. Za osobní údaje by pak bylo možno považovat informace, které by byly sdruženy v různých databázích, jejichž propojení (navzdory pravděpodobného důvodu existence rozdílných účelů zpracování osobních údajů) by identifikaci subjektu umožnilo. Více viz. Úřad pro ochranu osobních údajů k problémům z praxe – č. 1- 2. K pojmu osobní údaj.
[25] Více viz. Trestní oznámení na šéfku Fondu ohrožených dětí. Kvůli fotkám.

dodržovány, neboť smyslem ochrany osobních údajů je chránit samotné subjekty údajů před nepříznivými důsledky zveřejnění osobních údajů či jejich zneužití. Nerespektování těchto principů, byť s dobrým úmyslem, může mít fatální důsledky a může, kupříkladu tyto děti, provázat i v jejich budoucnosti.

V dokumentu nazvaném „Úřad pro ochranu osobních údajů k problémům z praxe – č. 1/2001“ upozorňuje na provázanost a komplexnost právní úpravy ochrany osobních údajů: „*na definici osobních údajů není možné pohlížet izolovaně, bez znalosti dalších okolností zpracování osobních údajů.*“ Použitá formulace má vyjadřovat skutečnost, že osobní údaje zpracovávané o osobách a přístupné správci (nebo zpracovateli) osobních údajů musí být vždy posuzovány ve vzájemném působení nebo z hlediska jejich vzájemného působení. Dále je vždy nutné zkoumat jakými prostředky a jakými formami ke zpracování osobních údajů má docházet. Ke zpracování osobních údajů totiž může docházet různými způsoby a v různých formách, s rozdílnými výsledky. Pokud jsou předmětem zpracování osobní údaje, které „*v původním tvaru nebo po provedeném zpracování nelze vztáhnout k určenému nebo určitelnému subjektu údajů*“[26], hovoříme o tzv. anonymních osobních údajích[27]. Tento druh osobních údajů (v obecném slova smyslu) nachází své uplatnění zejména při zpracování dat pro účely statistické či vědecké apod.; účelem takového zpracování pak není identifikace subjektu údajů. Z tohoto důvodu je zpracování anonymních údajů značně zjednodušeno a mj. není závislé na poskytování souhlasu subjektů údajů s takovým zpracováním (a tedy ani s předáváním anonymních údajů do zahraničí). Logickým opakem je situace, kdy zpracovávané osobní údaje umožňují danou osobu určit (daný subjekt údajů je, dle terminologie Zákona, označován jako subjekt údajů *určený či určitelný* - viz. výše). Schopnost osobního údaje jednoznačně identifikovat subjekt údajů je tedy jeho klíčovou vlastností.[28]

Osobní údaje je možné kategorizovat z mnoha různých hledisek. Určitý návod pro kategorizaci osobních údajů poskytuje „*Oznámení o zpracování (změně zpracování) osobních údajů podle § 16 zákona č. 101/2000 Sb.*“, které slouží pro oznamování zpracování osobních údajů Úřadu pro ochranu osobních údajů a které je k dispozici

[26] Zákon o ochraně osobních údajů, § 4, odst. 1, pís. (c)
[27] Anonymní údaje představují takové data (informace), které mohou obsahovat například jen jeden prvek (př. seznam adres bez uvedení jména, pro účely posouzení geografické skladby zákazníků obchodu), který by ve spojení s dalšími byl považován za osobní údaj. Více viz. Zákon o ochraně osobních údajů. Komentář, s.52.
[28] Úřad pro ochranu osobních údajů k problémům z praxe – č. 1- 2. K pojmu osobní údaj

formou internetového formuláře na webových stránkách této instituce.[29] V tomto oznámení se uvádí (pro účely registrace zpracování osobních údajů) následující kategorie osobních údajů: *osobní údaje adresní a identifikační, citlivé osobní údaje, popisné osobní údaje, údaje o jiných osobách a zbytkovou kategorii jiných osobních údajů.* Nutno dodat, že typizace osobních údajů je nutná především z důvodů ochrany osobních údajů; jednotlivé typy osobních údajů se liší nejen účelem použití těchto údajů a jejich vztahem k subjektu údajů (respektive z hlediska jejich schopnosti subjekt údajů identifikovat), ale zejména požadavky, jejichž naplnění Zákon požaduje k jejich zpracovávání. Z hlediska ochrany osobních údajů jsou významné, a nejčastěji používané, zejména osobní údaje adresní a popisné, zvláštní pozornost si zasluhují zejména osobní údaje citlivé. Autoři publikace „Osobní údaje a jejich ochrana" uvádějí, že „*k narušení soukromí může dojít až při použití dalších údajů (kontaktních a popisných),k nimiž jsou identifikační osobní údaje pouze klíčem.*"[30]

Identifikační osobní údaje, zjednodušeně řečeno, obsahují charakteristiku subjektu údajů, která je určitým způsobem ustálená, použitelná ve společenském styku nebo například též pro účely identifikace ze strany subjektů veřejného práva. Velmi blízké k identifikačním osobním údajů jsou svojí povahou osobní údaje kontaktní[31]. V mnoha případech je zařazení určitého osobního údaje jen do jedné z těchto skupin velmi složité.

Velmi specifickým druhem osobních údajů jsou tzv. citlivé osobní údaje. Do této kategorie osobních údajů Zákon řadí osobní údaje vypovídající o: *národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektů údajů.*[32] Obecně a zjednodušeně řečeno je možné za citlivé osobní údaje považovat takový „*údaj, který může být použit k diskriminaci subjektu údajů bez vazby na hodnoty dalších osobních údajů téhož subjektu.*"[33] Zákon však pro účely ochrany osobních údajů použil, v případě citlivých osobních údajů, metodu taxativního výčtu – tedy za citlivé budou pro účely ochrany osobních údajů považovány jen takové údaje, které Zákon vyjmenovává.

[29] Více viz. http://www.uoou.cz/uoou.aspx?menu=29&submenu=31&loc=487
[30] Osobní údaje a jejich ochrana, s. 21
[31] Příjmení je příkladem identifikačního osobního údaje a telefonní číslo zas příkladem kontaktního osobního údaje.
[32] Zákon o ochraně osobních údajů, § 4, odst. 1, pís. (b)
[33] Osobní údaje a jejich ochrana, s. 80

Z tohoto důvodu došlo v nedávné době k novelizaci Zákona, a to v souvislosti s rozvojem moderních technik identifikace osob. Zákon nově mezi citlivé osobní údaje řadí též tzv. *biometrické osobní údaje* (například zobrazení obličeje[34]), které umožňují přímou identifikaci nebo autentizaci subjektu údajů. Navzdory použité formě taxativního výčtu mohou vznikat otázky, zda určitý osobní údaj je či není údajem citlivým. V takových případech nezbývá než hledat odpověď v praxi orgánů ochrany osobních údajů a soudů. Kupříkladu Soudní dvůr Evropských společenství uvedl, v souvislosti se zpracováním osobních údajů ve formě jejich uvedení na internetových stránkách, že odkaz (pouhá zmínka) o tom, že si určitá osoba (identifikovaná jménem) poranila nohu a ze zdravotních důvodů pracuje na tzv. zkrácený úvazek, musí být považován za osobní údaj o zdravotním stavu – tedy citlivý osobní údaj.[35]

Volba taxativního výčtu pro identifikaci citlivých osobních údajů je na jedné straně pochopitelná – umožňuje velmi snadno „zatřídit" některé typy osobních údajů do této kategorie a vyžadovat přísnější režim při jejich zpracovávání. Nicméně, naprostá většina lidí, za citlivé osobní údaje považuje i jiné druhy informací, které se týkají jejich osoby a které do jejich soukromí subjektivně citelně zasahují. Ukazuje se totiž, že zde vzniká určitá diskrepance mezi tím, jak pojem citlivých osobních údajů vnímá Zákon, a jak jej vnímá široká veřejnost. Tento rozdíl má své logické kořeny. Například informace o kreditní kartě, finančních prostředcích nebo pouze o rodinných problémech určitých osob mohou být velmi snadno zneužitelné, a s velkými následky. Navíc lze očekávat, že rozvoj vědy a technologií povede ke vzniku dalších osobních údajů, které se budou současných kategoriím vymykat. Proto by dle mého názoru bylo vhodné zákonnou definici osobních údajů doplnit o ustanovení, které by dalo prostor pro posouzení ad hoc, zda určitý osobní údaj, v případě konkrétní osoby, má aspekty citlivého osobního údaje, byť nejde o některý z taxativně vyjmenovaných osobních údajů.

[34] Vyhláška č. 415/2006, ze dne 18. srpna 2006, kterou se stanoví technické podmínky a postup při pořizování a dalším zpracovávání biometrických údajů obsažených v nosiči dat cestovního dokladu

[35] Ang. „Reference to the fact that an individual has injured her foot and is on half-time on medical grounds constitutes personal data concerning health within the meaning of Article 8(1) of Directive 95/46." (C-101/01 ze dne 6.11.2003)

1.2.2 Zpracování a shromažďování osobních údajů

Zákon poskytuje ochranu osobním údajům tím způsobem, že stanoví meze a pravidla pro nakládání osobními údaji – tedy pro jejich zpracování. Podle § 3, odst. 2 Zákona, který blíže konkretizuje působnost Zákona, se tento vztahuje na *veškeré zpracování osobních údajů, ať k němu dochází automatizovaně nebo jinými prostředky*. Pod pojem zpracování osobních údajů můžeme tedy zahrnout veškeré myslitelné typy nakládání s osobními údaji, počínaje jejich shromažďováním, včetně provádění nejrůznějších typů operací (třídění, seskupování, předávání aj.) až po jejich likvidaci. Je rovněž nerozhodné, zda jde o zpracování osobních údajů prováděné ze strany státních orgánů, orgánů územní samosprávy, jinými orgány veřejné moci, či zpracování provádění ze strany fyzických či právnických osob (§ 3, odst. 1 Zákona). Výjimkou jsou taková zpracování osobních údajů, která jsou prováděna fyzickou osobou výlučně pro svoji potřebu (§ 3, odst. 3 Zákona) anebo jde o zpracování nahodilé, kdy takto zpracované osobní údaje již nejsou dále zpracovávány (§ 3, odst. 4 Zákona). Zásadním požadavkem na to, aby se na operace s osobními údaji nahlíželo z pohledu Zákona, je požadavek *systematického zpracování osobních údajů*. Komentář k Zákonu o ochraně osobních údajů naznačuje, že „*pouhé ukládání obchodních či jiných smluv na určená místa bez použití znaků pro jejich třídění…nelze bez dalšího považovat za systematické zpracování osobních údajů.*“[36]

Pod pojem „zpracování“ osobních údajů Soudní dvůr Evropských společenství v rozhodnutí C-101/01 ze dne 6.11.2003 zahrnuje též uvádění a identifikace osob jejich jmény nebo jinými prostředky, například uváděním jejich telefonních čísel, pracovních podmínek, koníčků, na internetových stránkách (a jde tedy o zpracování osobních údaje ve smyslu Směrnice).[37] Z uvedeného rozhodnutí tedy vyplývá důležitý závěr pro tvůrce a provozovatele webových stránek, totiž že by si vždy měli opatřovat souhlas subjektů údajů, jejichž osobní údaje na svých internetových stránkách zveřejní. V této souvislosti se nabízí celá řada otázek, které jsou spojeny s ochranou osobních údajů ve vztahu

[36] Zákon o ochraně osobních údajů. Komentář, s. 42

[37] Ang. The act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes ‘the processing of personal data wholly or partly by automatic means’ within the meaning of Article 3(1) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

k jejich publikaci na internetových stránkách – otázka prokazování souhlasu, otázka doby zpracovávání osobních údajů. Nicméně protože jde o témata poměrně široká, dovolím si je ponechat k diskuzi dalším autorům.

V souvislosti s pojmem „zpracování osobních údajů“ vyvstala v průběhu praxe teoretická výkladová otázka, totiž zda pojem „zabezpečení osobních údajů“ je rovněž druhem zpracování osobních údajů. Je totiž povinností správce osobních údajů zpracovávaná data zabezpečit tak, aby byla chráněna před zneužitím vnitřním (tj. ze strany vlastních zaměstnanců) a vnějším (před neoprávněným přístupem a zneužitím třetími osobami). Správce osobních údaje je podle Zákona povinen v tomto směru přijmout opatření technická, organizační, právní a jiná. Nejvyšší správní soud ve svém rozhodnutí 3 As 21/2005 ze dne 10.5.2006 výkladem dovodil, že jde o pojmy druhově odlišné, neboť „*s ohledem na znění směrnice, jakož i současné znění § 1 zákona, byla a je cílem právní úpravy v této oblasti ochrana osob ve vztahu ke zpracování osobních údajů, resp. naplnění jejich práva na ochranu před neoprávněným zasahováním do jejich soukromí v souvislosti se zpracováváním osobních údajů, nikoli ochrana údajů sama o sobě. Rovněž povinnost zabezpečení se netýká údajů samotných, nýbrž celé škály úkonů zahrnovaných pod zákonný pojem zpracování.*“

1.2.3 Správce, zpracovatel, příjemce osobních údajů

Zákon počítá s účastí různých osob při zpracování osobních údajů. V prvé řadě půjde vždy o osobu osobní údaje poskytující (přímo nebo nepřímo) – tedy subjekt údajů. Samotné zpracování osobních údajů provádí nebo zajišťuje správce – tedy *subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj*. Rozhodující vlastností správce osobních údajů je jeho vztah k účelu zpracování osobních údajů, konkrétně určení účelu (a tedy i jeho znalost). Naproti tomu pro Zákon není rozhodující, zda správcem osobních údajů je osoba fyzická, právnická, osoba soukromého či veřejného práva.

Účelem právních předpisů týkajících se ochrany osobních údajů je stanovit pravidla pro jejich zpracování (pro nakládání osobními údaji) a zajistit, že „*subjekt údajů si může být jist, že jeho osobní údaje jsou zpracovány řádným a zákonným způsobem, což znamená, že zejména základní osobní údaje, které se ho týkají, jsou přesné a jsou zpřístupňovány*

jen oprávněným příjemcům…“[38] Prostředkem k dosažení tohoto účelu jsou především povinnosti, které jsou na správce (respektive na zpracovatele) osobních údajů kladeny zejména § 5 Zákona.

Při zpracování osobních údajů je správce povinen: *stanovit účel, prostředky a způsob zpracování osobních údajů, zpracovávat přesné osobní údaje, osobní údaje shromažďovat a zpracovávat osobní údaje výhradně k stanovenému účelu a jen v rozsahu nezbytném.* Zákon dále vyžaduje, aby tak správce osobních údajů činil vždy „*otevřeně*“, tedy aby deklarovaný a skutečný účel zpracování osobních údajů byly totožné; osobní údaje shromážděné k různým účelům nelze sdružovat. Získané osobní údaje nelze v žádném případě uchovávat na dobu neurčitou, byť by si správce osobních údajů dobu zpracování takto sám vymezil, nebo na jinak specifikovanou, nepřiměřenou dobu. Na tomto místě se však jeví jako vhodné podotknout, že takovýto způsob určení doby zpracovávání osobních údajů je poměrně oblíbený a rozšířený (byť je zcela evidentně v rozporu s platnou právní úpravou). Rozhodujícím kritériem pro jakákoliv zpracování osobních údajů je tedy účel takového zpracování. Předávání osobních údajů do zahraničí je též formou zpracování osobních údajů a podléhá tedy výše-uvedeným pravidlům.[39]

Odrazem výše-uvedených povinností při zpracování osobních údajů je i další, informační povinnost správce osobních údajů, kdy je správce povinen subjekt údajů před poskytnutím souhlasu informovat o účelu, době, rozsahu zpracování osobních údajů a jasně identifikovat osobu správce. Poskytnutý souhlas musí být správce schopen prokázat po celou dobu zpracování daných osobních údajů.

V souvislosti s dobou, po kterou jsou osobní údaje zpracovávány (a pro kterou je udělován souhlas s jejich zpracováním) si můžeme pokládat otázku – zda je možné, aby subjekt údajů například souhlas uděloval opakovaně a tím dobu zpracování prodlužoval? V případě takových forem zpracování osobních údajů, kdy nejde o zpracování osobních

[38] Ang. That right to privacy means that the data subject may be certain that his personal data are processed in a correct and lawful manner, that is to say, in particular, that the basic data regarding him are accurate and that they are disclosed to authorised recipients. As is stated in recital 41 in the preamble to the Directive, in order to carry out the necessary checks, the data subject must have a right of access to the data relating to him which are being processed. (Rozsudek Soudního dvora C-553/07 ze dne 7.5.2009)

[39] V této souvislosti se někdy hovoří o tzv. „sekundárním zpracování osobních údajů“. Více k tomuto termínu v článku nazvaném Zpracování osobních údajů pro zpracování osobních údajů (napsal Jiří Maštalka; vyšlo v Právním rádci 11/2009).

údajů vyplývající ze zákonných povinností správce (zjednodušeně řečeno), totiž správce podává na Úřad oznámení o zpracování osobních údajů a sděluje i dobu, po kterou zamýšlí dané osobní údaje zpracovávat. Úřad vyžaduje, v souladu s principy ochrany osobních údajů, aby byly osobní údaje zpracovávány po dobu, která je přiměřená účelu. Domnívám se však, že odpověď na uvedenou otázku není jednoznačná a závisela by především na účelu, pro který jsou dané osobní údaje zpracovávány.

Další, potenciálně účastnou osobou, je osoba zpracovatele, kterého ke zpracování osobních údajů zmocňuje nebo kterého tímto zpracováním pověřuje správce (zpracovatelem je i osoba, jejíž pověření zpracovávat osobní údaje je dáno *na základě zvláštního zákona*). V § 6 Zákona je stanovena nezbytná podmínka pro smluvní zpracování osobních údajů zpracovatelem, a to uzavření smlouvy o zpracování osobních údajů. Rozhodující je samozřejmě obsahová stránka takového právního úkonu, a nikoliv jeho označení. Zákon stanoví, že taková smlouva o zpracování osobních údajů musí výslovně stanovit: „*v jakém rozsahu, za jakým účelem a na jakou dobu se uzavírá a musí obsahovat záruky zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů*.“[40] Rozlišení mezi tím, zda určitý subjekt vystupuje v roli správce nebo zpracovatele osobních údajů rovněž není úplně jednoduché. Možné příčiny určité míry nejasností spojené s těmito pojmy, dle mého názoru, mají své kořeny ve vnímání osob, které osobní údaje zpracovávají. Dovolím si vyslovit domněnku, že například jen omezený počet podnikatelů – obchodníků si uvědomuje, že nakládá osobními údaji fyzických osob, svých klientů, když vede jejich evidence, když jim zasílá své nabídky. Zákon používá jakožto klíčový rozlišovací znak pojem „účel“. Nicméně osobám, které osobní údaje zpracovávají, nemusí být zcela jasné, co Zákon tímto pojmem má na mysli. Má snad účelem daného zpracování osobních údajů být výkon podnikatelské činnosti? Nebo snad oslovování potenciálních klientů? Další problémy mohou pramenit ze skutečnosti, že jedna a tatáž osoba zpracovávající osobní údaje, může v určité roli vystupovat jako jejich správce a v jiném momentě jako zpracovatel. V takovýchto situacích, ač je to zásadní z hlediska práv a povinností, je velmi obtížné jednotlivé role pečlivě rozlišit.[41]

[40] § 6 Zákona
[41] Viz například Stanovisko Úřadu pro ochranu osobních údajů č. 1/2005 vztahujícím se k činnosti pojišťovacích zprostředkovatelů.

1.2.4 Základní principy ochrany osobních údajů

Přestože prostor pro úvodní seznámení s problematikou ochrany osobních údajů a jejím pojmoslovím je jen omezený, je potřebné a účelné alespoň stručně nastínit základní principy ochrany osobních údajů.

V případě ochrany osobních údajů můžeme identifikovat celou řadu principů – mezi tři základní principy můžeme zařadit princip důvěrnosti (*principle of confidentiality*), princip autonomie (*principle of autonomy*), někdy též označovaný jako princip souhlasu (*principle of content*) a princip aktivního práva na informace (*right to information*).[42]

Všechny výšeuvedené principy jsou pak následně rozvedeny do detailnějších zásad, nebo principů, které by měly být aplikovány na všechna zpracování osobních údajů. Z těchto zásady vycházejí jednak Směrnice, ale i další dokumenty, byť nikoliv právně závazné[43], a rovněž Zákon.

Zásada omezeného shromažďování osobních údajů (*collection limitation principle*) je obsažena v § 5, odst. 1, písm. d) Zákona, neboť shromažďovat osobní údaje lze jen tehdy, pokud tyto odpovídají stanovenému účelu a v rozsahu nezbytném pro naplnění tohoto účelu. Smyslem tohoto principu je tedy předejít neoprávněnému shromažďování osobních údajů, jejich shromažďování v rozsahu, které neodpovídá danému účelu anebo shromažďování s cílem jejich využití pro úplně odlišný účel. S uvedenou zásadou rovněž velmi úzce souvisí princip zpracování pouze přesných osobních údajů (*data quality principle*). Následuje rovněž zásada stanovení a uvádění účelu (*purpose specification principle*), za kterým jsou osobní údaje zpracovávány. Tento požadavek je klíčovou zásadou i v případě Zákona – neboť právě účel je rozlišujícím kritériem pro rozdílná zpracování osobních údajů, o čemž svědčí i způsob, jakým jsou zpracování osobních údajů oznamována Úřadu pro ochranu osobních údajů. Jinak řečeno, osobní údaje lze shromažďovat a zpracovávat jedině pro přesně stanovený účel. Není přípustné, aby osobní údaje byly (bez předchozího souhlasu subjektů údajů) použity pro další účel zpracování. Z dalších je nutné zmínit princip zpřístupnění jen oprávněným osobám (*use limitation principle)* nebo zásadu zabezpečení osobních údajů (*security safeguards*

[42] The regulation of privacy and data protection in the use of electronic health information.
[43] Například: OECD Guidelines

principle), informování o nakládání osobními údaji (*openness principle*), princip aktivního práva na informace (*individual participation principle*) nebo princip odpovědnosti správce osobních údajů (*accountability principle*). Posledním principem, který OECD Guidelines zmiňují je princip mezinárodního toku osobních údajů a přiměřených omezení (*free flow and legitimace restrictions*).

Vzhledem k tomu, že východiskem ochrany osobních údajů jsou základní práva a svobody, hlavním činitelem zde tedy bude subjekt údajů nadaný jistými právy. Na straně druhé bude stát správce či zpracovatel osobních údajů, jemuž zákon stanoví především povinnosti, které při zpracování osobních údajů musí dodržovat. Povinnosti správce osobních údajů je možno členit do několika skupin: povinnosti týkající se souhlasu subjektu údajů, informační povinnosti vůči subjektu údajů (před poskytnutím souhlasu se zpracováním i během zpracování), povinnosti týkající se samotného zpracování osobních údajů (včetně povinností při zabezpečení osobních údajů a jejich likvidaci), předávání osobních údajů jiným správcům, povinnosti týkající se zpracování citlivých osobních údajů a rovněž povinnosti vůči Úřadu pro ochranu osobních údajů.

Právní úprava týkající se ochrany osobních údajů je založena *„na zásadě, podle níž právo disponovat osobními údaji náleží fyzické osobě, k níž se tyto informace vztahují (subjektu údajů), a nikoliv k tomu, kdo je jejich držitelem.“*[44] Zpracování osobních údajů je, až na výjimky, obecně podmíněno poskytnutím souhlasu subjektu údajů. Zákon v § 5, odst. 2 taxativně stanoví případy, kdy je možné osobní údaje zpracovávat i bez souhlasu subjektu údajů, mj. *pokud je nezbytné pro plnění právní povinnosti správce, pro plnění smlouvy se subjektem údajů, k ochraně životně důležitých zájmů subjektu údajů, v případě oprávněně zveřejněných osobních údajů aj.* V případě tzv. citlivých osobních údajů je potřeba poskytovat souhlas předchozí, informovaný a výslovný.

Práva subjektu údajů souvisejí zejména s povinností správce či zpracovatele údajů dbát práv subjektu údajů – tedy mj. zpracovávat osobní údaje na základě poskytnutého souhlasu. Správci osobních údajů jsou v mnoha případech kromě ochrany osobních údajů podrobeni též celé řadě veřejnoprávních povinností vyplývajících například ze skutečnosti, že jsou zaměstnavateli, veřejnoprávními orgány či jinými subjekty, které

[44] Rozhodnutí Nejvyššího správního soudu 9 As 34/2008 ze dne 12.2.2009

k plnění některých svých zákonných povinností musí nutně pracovat s některými osobními údaji. V takovém případě půjde o zákonné zmocnění (a povinnost) osobní údaje subjektů údajů zpracovávat, aniž by takové zpracování vyžadovalo poskytnutí souhlasu daného subjektu údajů.

Velmi důležitým aspektem koncepce zpracovávání osobních údajů na podkladě poskytování souhlasu je též možnost jednou poskytnutý souhlas odvolat, vzít zpět. Následně by měl správce osobních údajů přestat osobní údaje takového subjektu údajů zpracovávat (maximálně by je mohl dál uchovávat, pokud by mu toto nařizovaly právní předpisy). Právě v tomto bodě dochází ke vzniku celé řady nejasností v oblasti ochrany osobních údajů. Předně lidé si většinou neuvědomují, že za jistých okolností zde může skutečně existovat právní povinnost správce údajů některé osobní údaje dál uchovávat, tedy zpracovávat. Na druhé straně se však můžeme setkat s tím, že správci osobní údaje, které by po odnětí souhlasu měli zlikvidovat (tedy nenávratně zničit), dál uchovávají. V této souvislosti je nutné poukázat na další důležitý princip – totiž, že je možné zpracovávat jen osobní údaje nezbytné a přiměřené pro daný účel. Jak jsme již zmínili dříve, pojem účelu není správci a zpracovateli osobních údajů interpretován a chápán shodně. Nelze se pak divit, že začlenění neurčitých pojmů „nezbytné“ a „přiměřené“ nutně vytváří prostor pro takovou argumentaci osob zpracovávacích osobní údaje, která je pro ně výhodná (ať už skutečně nebo jen domněle). V této souvislosti je možné zmínit názor českého Veřejného ochránce práv (publikovaný dne 11. listopadu 2009) v článku nazvaném „Práva osob při ochraně osobních údajů“. Zástupkyně ombudsmana zde vyslovila názor, že „*celkový rozsah osobních údajů, které banky vyžadují, není podle zástupkyně ochránce často přiměřený účelu. Snaha o minimalizaci rizik spojených s poskytováním úvěrů vede banky ke shromažďování maximálního množství informací o klientovi, včetně např. kopírování osobních dokladů. Jak zástupkyně ochránce rovněž zjistila, banky zpracovávají osobní údaje, i když obchod či vztah nebyl se zájemcem nakonec uzavřen.*“ Ačkoliv ochrana osobních údajů představuje oblast norem, které mají sloužit jednoznačně k ochraně slabší strany – tedy subjektů údajů, mnohdy tomu tak není. V uvedeném článku tuto skutečnost zástupkyně ombudsmana potvrdila, když uvedla „*podmínky zpracování osobních dat v obou sektorech nejsou nastaveny optimálně a situace je neuspokojivá. Na vině je zejména skutečnost, že právní úprava je komplikovaná, nejednoznačná a zvýhodňuje postavení finančních institucí vůči klientům. Samotné banky mají navíc tendenci vykládat zákon o bankách a zákon o některých*

opatřeních proti legalizaci výnosů z trestné činnosti a financováni terorismu široce, často na úkor ochrany soukromí klientů. Běžní občané pak mají pocit, že se při jednání s bankou ocitají v nerovném postavení a jejich údaje nejsou dostatečně chráněny."

Na závěr této podkapitolky si dovolím upozornit na směšování dvou zásadních principů – principu zpracování osobních údajů se souhlasem subjektů údajů a principu oznamovacího. Zatímco první z principů pramení z logiky, že pokud je zdrojem osobních údajů subjekt údajů (fyzická osoba), pak skutečnost, zda svoje osobní údaje někomu poskytne, plyne čistě z jeho vůle (zjednodušeně řečeno[45]). Na druhé straně princip oznamovací vyjadřuje, podle mého názoru, prvek veřejnoprávní. Vzhledem k tomu, jak je současná právní úprava konstruována, je právě prvek oznamovací důležitým instrumentem pro zefektivnění dozoru a kontroly v oblasti ochrany osobních údajů. Oba dva principy mohou působit jak ve vzájemném působení, tak zcela samostatně. Lze si představit situace, kdy osobní údaje budou zpracovávány na principu plnění zákonné povinnosti (bez souhlasu subjektu údajů) nebo v souvislosti s plněním smluvního vztahu (taktéž bez souhlasu subjektu údajů), ale kdy bude plněna oznamovací povinnost.[46] Jak bylo zmíněno výše, otázka skutečného přínosu oznamovacího principu v evropské právní úpravy ochrany osobních údajů je předmětem diskuzí a v rámci návrhů revize Směrnice se uvažuje o jeho zrušení. Domnívám se, že tyto snahy jednoznačně pramení ze složitosti právní úpravy a nejednoznačnosti ustanovení Zákona. Vzhledem k tomu, že tato právní úprava má sloužit a být používána především laiky (ne-právníky), je především nutné uvažovat nad změnou použitých formulací tak, aby byly eliminovány výkladové problémy a aby se právní úprava stala skutečným nástrojem k ochraně osobních údajů.

1.3 Institucionální rámec ochrany osobních údajů

K tomu, aby byla právním řádem poskytovaná ochrana osobních údajů skutečně vymahatelná, je potřeba vytvořit rovněž odpovídající institucionální rámec – tedy začlenit do dané právní úpravy jednak orgán, který bude bdít nad dodržováním daných

[45] Pro účely ilustrace rozporu uvedených dvou principů si dovolím odhlédnout od forem zpracování osobních údajů, kde není potřeba získávat souhlas subjektů údajů.
[46] Úřad ve svém stanovisku 1/2005 osvětlil, že v rámci činnosti pojišťovacích zprostředkovatelů může docházet k situacím, kdy tyto osoby budou vystupovat v rámci čistě své podnikatelské činnosti (získávání klientů) a budou tedy v pozici správce údajů. Nicméně Úřad dovodil, že v rámci této své činnosti nebudou podléhat oznamovací povinnosti, z důvodu výjimky dle § 18 odst. 1, písm. b) Zákona.

právních předpisů, jednak vytvořit potřebné mechanismy, které umožní práva osob, jejichž osobní údaje jsou zpracovávány, účinně chránit a domáhat se jejich dodržování po osobách, které s jejich osobními údaji jakkoliv nakládají. Nebude tedy překvapením, že s požadavkem na zřízení odpovídajícího dozorového orgán se setkáme jednak v Úmluvě č. 108 (čl. 1 Dodatkového protokolu k úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat o orgánech dozoru a toku dat přes hranice ze dne 8. listopadu 2001) a rovněž ve Směrnici, v Kapitole 6 – orgán dozoru a pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů.

Jaké vlastnosti by měly takový dozorový orgán a jeho činnost charakterizovat? V prvé řadě půjde o pravomoci dohlížet nad dodržováním příslušných předpisů a tedy i nad ochranou osobních údajů; v případě pochybností či potřeby ověřit dodržování stanovených pravidel pro nakládání osobními údaji se uplatní pravomoci vyšetřovat a v případě potřeby činit (nařizovat) opatření (tedy pravomoc zasahovací).

Je nezbytné, aby orgány ochrany osobních údajů byly nadány rovněž rozhodovacími pravomocemi, neboť jen tak je možné účinně prosazovat ochranu osobních údajů. Na druhé straně, vzhledem k tomu, že jde zpravidla o proces v oblasti správního práva, je potřebné umožnit subjektům nakládajícím osobními údaji bránit se proti rozhodnutím takového orgánu před soudy (tedy princip přezkoumatelnosti rozhodnutí soudem). Je přirozené, že pokud požadujeme, aby subjekty zpracovávající osobní údaje dodržovaly přísná pravidla na jejich ochranu, musíme požadovat rovněž po kontrolních orgánech, aby se zjištěnými informacemi bylo nakládáno jako s důvěrnými.

S ohledem na stále komplexnější problematiku ochrany osobních údajů prolínající se s rozšiřováním informačních technologií do nejrůznějších aspektů lidského života, je nezbytné, aby orgány ochrany osobních údajů spolupracovaly na mezinárodní úrovni (i formou konzultací na úrovni vnitrostátní) a přispívaly tak k flexibilitě norem ochrany osobních údajů. Na závěr je potřeba zmínit další, snad nejdůležitější, požadavek kladený na orgány ochrany osobních údajů – požadavek nezávislosti. Vzhledem k tomu, že ve většině států je orgán ochrany osobních údajů státním orgánem, nejde o nezávislost stejného druhu, jako v případě soudů. Nezávislost orgánů ochrany osobních údajů je

symbolizována jejich pravomocemi, které dopadají jak na subjekty soukromého práva, tak na ostatní státní orgány, a to bez rozdílu.[47]

1.3.1 Úřad pro ochranu osobních údajů

Dle § 23 zákona č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech, bylo projednávání sporů v oblasti ochrany osobních údajů svěřeno do působnosti soudů. S přijetím nového Zákona (respektive ode dne 1.6.2000, kdy Zákon nabyl účinnosti) byla tato oblast přesunuta do kompetence Úřadu pro ochranu osobních údajů. Zvláštní senát Nejvyššího soudu ve svém rozhodnutí Konf 11/2003 ze dne 10.3.2004 změnu v příslušnosti orgánů dohlížejících na ochranu osobních údajů deklaroval následovně: *„není rozhodnutí o takové žádosti v pravomoci soudu, ale Úřadu pro ochranu osobních údajů. Nic na tom nemění, že takový návrh byl podán v době od 1.6. do 31.12.2002, kdy ustanovení § 9 odst. 2 písm. b) o. s. ř., ve znění tehdy účinném, upravovalo věcnou příslušnost krajských soudů pro rozhodování ve sporech vyplývajících z uplatňování práv a povinností podle právních předpisů o ochraně osobních údajů v informačních systémech podle staršího zákona č. 256/1992 Sb.; nešlo o ustanovení kompetenční, zakládající pravomoc soudu, a po datu 1.6.2002 se stalo obsoletním.“* [48]

V České republice byl vytvořen jediný úřad, do jehož působnosti problematika dohledu nad dodržováním předpisů v oblasti nakládání osobními údaji patří, a to Úřad pro ochranu osobních údajů (dále jen „**Úřad**“). K zakotvení Úřadu do českého právního řádu došlo zákonem č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů (v ustanoveních § 2 a § 28-43 Zákona), nicméně do jeho působnosti patří dohled nad

[47] V případě českého Úřadu pro ochranu osobních údajů je princip nezávislého orgánu naplňován hned několika způsoby: (i) tento úřad je koncipován jako samostatný orgán, který není podřízen žádnému ministerstvu ani jinému státnímu úřadu, (ii) předseda úřadu je jmenován do své funkce prezidentem republiky a (iii) jeho fungování je zabezpečeno též samostatným financováním ze státního rozpočtu.

[48] Podobně - Rozhodnutí Ústavního soudu IV. ÚS 143/02 ze dne 28.8.2002 *„Nabytím účinnosti zákona č. 101/2000 Sb. …došlo ke změně kompetencí, neboť oblast ochrany osobních údajů byla svěřena do působnosti zmíněného Úřadu [Úřadu pro ochranu osobních údajů]… citovaný zákon se výslovně nevyjádřil k otázce postupu soudů v řízeních zahájených podle derogovaného zákona č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech, a ke dni jeho derogace neskončených. Pokud za této situace krajský soud dospěl k závěru, že není dána jeho kompetence ve věci ochrany osobních údajů, a z tohoto důvodu řízení zastavil, nelze z ústavněprávního hlediska v jeho postupu shledat pochybení. To proto, že podle ustanovení § 154 občanského soudního řádu pro rozsudek je rozhodující stav v době jeho vyhlášení; v době rozhodování krajského soudu v souzené věci již nabyl účinnosti zákon č. 101/2000 Sb., který přiznával kompetenci rozhodovat o ochraně osobních údajů Úřadu pro ochranu osobních údajů. Krajský soud tedy neporušil právo stěžovatele na soudní ochranu, jestliže se řídil základním principem právního státu, podle něhož státní orgán může činit pouze to, co mu zákon výslovně dovoluje (srov. čl. 2 odst. 2 Listiny základních práv a svobod).“*

dodržováním celé řady právních předpisů spojených s oblastí ochrany osobních údajů. Aby bylo při zřizování Úřadu, jako orgánu dozoru, učiněno zadost požadavkům kladeným evropskou a mezinárodní legislativou, bylo potřebné vytvořit též záruky pro jeho činnost jako nezávislého orgánu. Zákon zajišťuje naplnění tohoto požadavku jednak tím, že Úřad prohlašuje za nezávislý orgán, který se řídí pouze zákony a jinými právními předpisy (§ 28 Zákona). Smyslem tohoto ustanovení tedy je zdůraznit, že Úřad zaujímá v soustavě státních úřadů zcela samostatné místo a není žádnému jinému orgánu podřízen. K zajištění samostatného a nezávislého působení Úřadu, a to i ve směru kontroly nakládání osobními údaji jinými státními orgány, slouží i zabezpečení prostředků na financování činnosti Úřadu ze samostatné rozpočtové kapitoly.[49]

Pravomoci Úřadu jsou v Zákoně koncentrovány v ustanovení § 29, odst. 1; jako první je v Zákoně uvedeno provádění *„dozoru nad dodržováním povinností stanovených zákonem při zpracování osobních údajů*“. Dozorová činnost Úřadu je vykonávána formou správního dozoru (dohled na subjekty mimo vztahy nadřízenosti a podřízenosti), jako vysoce specializované a výlučné činnosti. Jde o správní dozor především jednorázový (tzv. incidentní dozor) a průběžný, neboť k realizaci kontrolních pravomocí dochází na základě určitého podnětu – ať už vnitřního, nebo vnějšího (stížnost nebo jiný vnější podnět) – a předmětem kontroly je dodržování zákonných povinností v průběhu činnosti kontrolovaného subjektu.[50] Spoluautoři publikace „Osobní údaje a jejich ochrana“, M. Matoušová a L. Hejlík, ve svém díle uvádějí, že *„dozorovou činnost a působnost spoluvytvářejí registrace zpracování osobních údajů, přijímání podnětů a stížností občanů na porušení zákona o ochraně osobních údajů, kontrolní činnost a do jisté míry poskytování konzultací*“ (s.322). Pod dalšími písmeny tohoto odstavce jsou uvedeny další důležité aktivity Úřadu, jako jsou činnost registrační[51] a též přijímání podnětů, stížností a jejich řešení.

Velmi důležitou činností, kterou Úřad vykonává, byť není výslovně v Zákoně zmíněna, je působení na veřejnost, na obyvatele (subjekty údajů) i na subjekty osobní údaje zpracovávající (ať už jako správci osobních údajů nebo jejich zpracovatelé) k větší informovanosti o právu na soukromí a o právech (a povinnostech) spojených s ochranou

[49] Viz. Zákon, § 28, odst.3
[50] Úřad pro ochranu osobních údajů, Správní dozor, http://www.uoou.cz/uoou.aspx?menu=10
[51] Tedy vedení registru zpracování osobních údajů.

osobních údajů. Snad můžeme shrnout tyto aktivity pod pojem činnosti informační a vzdělávací. Provádění dozoru je úzce spjato s aktivitami konzultačními, a to jednak směrem k subjektům zpracovávajícím osobní údaje a jednak vůči různým orgánům podílejícím se na legislativním procesu. Úřad se v rámci své činnosti podílí na tvorbě legislativy související s problematikou ochrany osobních údajů, ať už české či evropské. V rámci výšeuvedených činností spolupracuje s jinými národními úřady pro ochranu osobních údajů v EU.[52] K efektivnímu naplňování účelu činnosti Úřadu a k ochraně osobních údajů přispívá rovněž pravomoc správního trestání – tedy pravomoc stíhat správní delikty a udělovat za ně sankce stanovené zákonem.[53]

1.3.2 Institucionální rámec ochrany osobních údajů na evropské úrovni

Na evropské úrovni se můžeme setkat s několika orgány, které se věnují problematice ochrany osobních údajů, a to:

- Evropská komise, Generální ředitelství pro svobodu, spravedlnost a bezpečnost (*European Commission, DG Freedom, Justice and Security*);
- Pracovní skupina pro ochranu údajů WP29 jako nezávislý poradní orgán Evropské komise;
- Evropský inspektor ochrany údajů (European Data Protection Supervisor).

Evropská komise, respektive Generální ředitelství pro svobodu, spravedlnost a bezpečnost, působí v rámci evropských institucí především jako orgán výkonný, nelze však zapomínat ani na další důležitou činnost a pravomoc – totiž tvorbu návrhů legislativy, účast na legislativním procesu a následně též na monitoringu uplatňování přijatých norem. Evropská komise také představuje styčný orgán pro jednání s jinými státy a organizacemi, též v oblasti ochrany osobních údajů.

[52] Zákon, § 29, odst. 1, písm, i.): Úřad…spolupracuje s obdobnými úřady jiných států, s orgány Evropské unie a orgány mezinárodních organizací působícími v oblasti ochrany osobních údajů. Úřad v souladu s právem Evropských společenství plní oznamovací povinnost vůči orgánům Evropské unie.

[53] Pozn. Porušování povinností v souvislosti s ochranou osobních údajů je zabezpečováno jednak existencí správní deliktů v Zákoně uvedených a dále rovněž možností stíhat jednání s vyšším stupněm nebezpečnosti jako trestné činy (konkrétně jde o trestný čin neoprávněného nakládání osobními údaji – dle § 178 zákona č. 140/1961 Sb., trestního zákona).

Pracovní skupina pro ochranu údajů WP29[54](dále jen „**Pracovní skupina WP29**“) byla založena na základě článku 29 Směrnice jako nezávislý poradní orgán Evropské komise. Pokud jde o složení Pracovní skupiny WP29 – je tvořena zástupci představitelů orgánů zabývajících se problematikou ochrany osobních údajů v jednotlivých členských státech a jejich protějšků na půdě Evropské unie a též zástupcem Evropské komise.[55]

Mezi základní okruhy činností Pracovní skupiny WP29 patří zprostředkování odborných stanovisek z úrovně jednotlivých členských států Evropské komisi, podpora jednotné aplikace principů vyplývajících ze Směrnice prostřednictvím spolupráce jednotlivých dozorčích orgánů v jednotlivých členských státech, poskytování konzultací a stanovisek k opatřením zasahujícím do práv a svobod osob ve vztahu k zpracování osobních údajů a vydávání doporučení určených jak široké veřejnosti, tak evropským institucím.[56]

Nařízením Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů byl zřízen institut **Evropského inspektora ochrany údajů (**čl. 41), jako nezávislého orgánu dozoru nad dodržováním právních předpisů o zpracování osobních údajů na půdě evropských institucí a orgánů. Evropský inspektor ochrany údajů nemá pravomoci týkající se zpracování osobních údajů na půdě jednotlivých členských států, ale jen na půdě orgánů ES (EU).[57] Pravomoci Evropského inspektora ochrany jsou obdobné těm, které mají národní dozorové orgány: pravomoc dozorová (dohlíží na respektování pravidel ochrany osobních údajů na půdě orgánů EU), dále se věnuje činnostem poradenským a konzultačním (připomínkování legislativních návrhů a poskytování výkladových

[54] Celým označením jde o „Working Party on the Protection of Individuals with regard to the Processing of Personal Data (volně přeloženo - Pracovní skupina pro ochranu osob s ohledem na zpracování osobních údajů).

[55] V čele Pracovní skupiny WP29 stojí předseda volený na období dvou let, a to i opakovaně.

[56] Konkrétní výčet úkolů Pracovní skupiny WP29 podle čl. 30 Směrnice zahrnuje: *„posuzovat veškeré otázky týkající se uplatňování vnitrostátních předpisů přijatých k provedení této směrnice s cílem přispívat k jejich jednotnému uplatňování, zaujímat pro Komisi stanovisko o úrovni ochrany ve Společenství a ve třetích zemích, poskytovat Komisi poradenství o všech návrzích změn této směrnice, o všech návrzích doplňujících nebo zvláštních opatření, která by měla být přijata pro ochranu práv a svobod fyzických osob v souvislosti se zpracováním osobních údajů, jakož i o všech ostatních návrzích opatření ve Společenství, která mají vliv na tato práva a svobody a zaujmout stanovisko ke kodexům chování vypracovaným na úrovni Společenství.*“

[57] Evropský inspektor ochrany údajů je jmenován na období pěti let, a to i opakovaně, ze seznamu kandidátů navržených ze strany Evropské komise na základě společného rozhodnutí Evropského parlamentu a Rady.

stanovisek a dokumentů) a rovněž se zapojuje do spolupráce s národními orgány dohledu nad dodržováním principů ochrany osobních údajů.

1.3.3 Instituce zabývající se ochranou osobních údajů na mezinárodní úrovni

Na mezinárodní úrovni působí celá řada institucí, které se věnují problematice ochrany osobních údajů, a to buď jako své hlavní činnosti nebo v jako doplňku k dalším aktivitám, ať už zaměřených do oblasti ekonomické, právní nebo jiné.

Jako první příklad můžeme uvést **Organizaci pro hospodářskou spolupráci a rozvoj**, v rámci které působí **Skupina pro informační bezpečnost a ochranu osobních údajů** (WPISP).[58] Toto mezivládní fórum zabývající se mj. problematikou informační bezpečnosti, ochrany soukromí a osobních údajů a dalšími souvisejícími oblastmi jako jsou šifrování, biometrické údaje či nevyžádaná korespondence (spamy), působí v rámci **Committee for Information, Computer and Communication Policy** (ICCP) v OECD. WPISP se zaměřuje na monitoring nových trendů, slouží jako pole pro výměnu informací, poskytuje analýzy dopadů technologií na informační bezpečnost a soukromí a rovněž poskytuje metodické pokyny k těmto tématům.

Z dalších organizací je možné uvést **Privacy International**, první neziskovou organizaci založenou k propagaci práva na soukromí a ochranu osobních údajů[59] a působící dnes po celém světě. Tato organizace se věnuje sledování vývoje v oblasti ochrany osobních údajů, informuje o možných rizicích a nástrahách souvisejících s rozvojem moderních technologií, vyvíjí informační a konzultační aktivity. Pro zajímavost můžeme zmínit, že Privacy International v roce 2007 vydala hodnocení států z hlediska míry dodržování a ochraňování lidských práv, včetně práva na soukromí (a ochrany osobních údajů) – **Privacy and Human Rights Report**. Organizace (ve spolupráci s americkým střediskem -Electronic Privacy Information Center (viz dále)) kritizuje zejména přijímání legislativy umožňující stále větší zásahy států do soukromí obyvatel a ospravedlňované veřejným zájmem, bezpečností, potřebou umožňovat výkon práva, bojem proti terorismu a proti

[58] Volný překlad – anglicky Working Party on Information Security and Privacy Policy (WPISP)
[59] Privacy International je neziskovou organizací (*non-profit práváte limited company*) založenou v roce 1990 ve Velké Británii; více informací o této organizaci je možné nalézt na http://www.privacyinternational.org/

nelegální imigraci.[60] V případě hodnocení České republiky se objevuje kritika za sdílení osobních údajů (*data sharing)* a za nepřípustné nahlížení do obsahu předávaných zpráv (*communication interception*).[61] V této souvislosti je nicméně nutné podotknout, že zveřejněné hodnocení je všeobecně velmi kritické, i k státům jako je právě Velká Británie, která bývá označovaná za kolébku evropské demokracie. Z dalších institucí zmíníme například **Electronic Privacy Information Center –** americkou nevládní organizaci věnující se problematice ochrany lidských práv, práv zaručených americkou ústavou a též práva na soukromí, v rámci kterého se věnuje též ochraně osobních údajů). V rámci svých aktivit se tato organizace věnuje též sledování vývoje v oblasti ochrany osobních údajů a publikování článků týkajících se tohoto tématu.

Vedle institucionalizovaných organizací sehrávají v dnešní době stále větší internetově vydávané noviny a časopisy, které umožňuje prakticky okamžitě reagovat na vývoj problematiky ochrany osobních údajů. Jako příklad je možné uvést, vedle internetových stránek českého Úřadu, internetový časopis **Data Protection Review** vydávaný španělským úřadem pro ochranu osobních údajů[62], dalším zdrojem jsou internetové stránky **OUT-LAW.com** (vydávané mezinárodní advokátní kanceláří Pinsent Masons, zaměřující se na oblasti IT a e-commerce). Z českých zdrojů, které se věnují této problematice, je možné uvést internetové stránky věnované ochraně osobních údajů (www.oou.cz) nebo též internetové stránky organizace **Iuridicum Remedium, o.s.**, která se v rámci své činnosti též věnuje problematice ochrany osobních údajů. Tato organizace každoročně uděluje tzv. Ceny Velkého bratra (*Big Brother Awards*), které mají upozorňovat na zneužívání moderních technologií a porušování lidských práv, včetně porušování ochrany osobních údajů (http://www.bigbrotherawards.cz).

[60] Cit. http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559597 dne 23.10.2009
[61] Hodnocení ČR (volně přeloženo z anj. a upraveno): „*Ochrana osobních údajů je zaručena čl. 7, 10, 13 Listiny); existuje zde komplexní právní úprava ochrany osobních údajů, Úřad uděluje za porušení Zákona pokuty, odmítá povolit předávání osobních údajů do zahraničí, v široké míře se podílí na informování veřejnosti, existují zde soudní záruky proti zneužití osobních údajů, prvky ochrany proti praní špinavých peněz, zaměstnavatel nesmí číst zaměstnancům e-maily, s výjimkou předmětu zprávy; sporná je problematika zdravotních registrů, nárůst použití kamerových systémů, uvažuje se o sdílení přístupů k osobním údajům mezi státními orgány a úřady*“. Dostupné na http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559597
[62] Data Protection Review (http://www.dataprotectionreview.eu/);

2 Předávání osobních údajů do zahraničí

2.1 Základy právní úpravy předávání osobních údajů do zahraničí

Pojem předávání osobních údajů není Zákonem definován, nicméně je zmíněn v ustanovení § 4, písm. e) definujícím pojem „zpracování osobních údajů". Z uvedeného tedy vyplývá, že předávání osobních údajů je formou jejich zpracování. Jde tedy o vztah mezi správcem osobních údajů a třetí osobou, příjemcem osobních údajů.[63] V této souvislosti je nutné upozornit, že musíme rozlišovat mezi předáváním osobních údajů jiným příjemcům v rámci jednoho státu od situace, kdy osobní údaje překračují hranice a míří do zahraničí, a mnohdy mimo EU. Nicméně určité obavy mohou vyvstávat při předávání osobních údajů do zahraničí, tedy do států, jejichž úroveň právního systému a míra ochrany poskytovaná osobním údajům se mohou značně lišit.

Kdy jde o předávání osobních údajů do zahraničí? V naprosté většině případů půjde o situace, kdy osobní údaje (nejčastěji v podobě elektronických dat) budou pomocí elektronických zařízení odeslány ze strany správce osobních údajů a na druhé straně budou přijaty jejich příjemcem. Půjde o vztah, kdy přesně můžeme identifikovat obě dvě strany, mezi nimiž osobní údaje proudí a které jsou příslušníky různých států. Můžeme si ale položit otázku, zda takovým předáváním osobních údajů je i jejich zpřístupnění na internetových stránkách, čímž jsou takové osobní údaje přístupné příslušníkům nejrůznějších států. Odpověď na tuto otázku poskytl ve svém rozhodnutí C-101/01 ze dne 6.11.2003 též Soudní dvůr Evropských společenství: „*pokud jednotlivec v členském státě umístí své osobní údaje na internetovou stránku …která je provozována fyzickou nebo právnickou osobou v daném nebo jiném členském státě, čímž dojde ke zpřístupnění takových osobních údajů třetím osobám, včetně osob z jiných států, nejde o předávání osobních údajů ve smyslu čl. 25 Směrnice 95/46.*[64] Můžeme tedy shrnout, že uvedení

[63] Dle ustanovení § 4, písm.o) Zákona je „příjemcem každý subjekt, kterému jsou osobní údaje zpřístupněny."

[64] Ang. „There is no 'transfer [of data] to a third country within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loads personal data onto an internet page which is stored on an internet site on which the page can be consulted and which is hosted by a natural or legal person who is

osobních údajů na internetových stránkách není předáváním osobních údajů do zahraničí, ale jde o formu zpracování osobních údajů (která vyžaduje splnění zákonných povinností kladených na správce osobních údajů).

2.1.1 Právní úprava předávání osobních údajů do zahraničí

V rámci české právní úpravy se problematice předávání osobních údajů věnuje Zákon ve své hlavě III – Předávání osobních údajů. V souvislosti se vstupem České republiky do Evropské unie došlo k zásadní novelizaci textu Zákona, konkrétně zákonem č. 439/2004 Sb., kterým se mění zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „**euronovela**"), a to včetně ustanovení týkajících se předávání osobních údajů do zahraničí. Počínaje dnem 26. července 2004, kdy euronovela Zákona nabyla své účinnosti, se do prvního odstavce § 27 Zákona dostává zákaz omezování předávání osobních údajů do členských států Evropské unie, jako odraz ustanovení článku 1, odst. 2 Směrnice.[65] Předešlá právní úprava (tj. Zákon ve znění před euronovelou) umožňovala předávání osobních údajů do třetích států „*za podmínky, že právní úprava státu, kde mají být (osobní) údaje zpracovány, odpovídá požadavkům stanoveným v tomto zákoně*" (cit. § 27, odst. 1). Kromě již uvedeného předávání osobních údajů do členských států EU současná právní úprava výslovně zakazuje omezování předávání osobních údajů v případech, kdy je takovýto závazek vymezen v mezinárodní smlouvě[66] nebo též pokud by se jednalo o předávání osobních údajů na základě rozhodnutí orgánů EU (viz dále). Cílem ustanovení Zákona vymezujících podmínky, za kterých lze osobní údaje do zahraničí předávat, je zajistit minimální srovnatelnou úroveň ochrany osobních údajů. Podobně je tomu v případě harmonizace legislativ členských států EU. Implementace Směrnice by měla zajistit ve všech členských státech potřebnou míru ochrany osobních údajů. Pokud jde o poslední ze situací, tedy o zákaz omezování předávání osobních údajů v případě předávání osobních údajů na základě rozhodnutí orgánu EU – kompetentním orgánem je Evropská komise. Do těchto států je pak možné předávat osobní údaje za podmínek v těchto rozhodnutích

established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country."

[65] „Členské státy zajišťují v souladu s touto směrnicí ochranu základních práv a svobod fyzických osob, zejména jejich soukromí, v souvislosti se zpracováním osobních údajů. (čl. 1, odst.1, Směrnice). Členské státy nemohou omezit ani zakázat volný pohyb osobních údajů mezi členskými státy z důvodů ochrany zajištěné podle odstavce 1. (čl. 1, odst.2 Směrnice).

[66] Jde o mezinárodní smlouvy, k jejichž ratifikaci dal souhlas Parlament ČR a kterými je ČR vázána.

stanovených. Dalším případem, který bychom též mohli přiřadit do kategorie předávání osobních údajů na základě rozhodnutí Evropské komise, je předávání údajů na základě smlouvy, která bude obsahovat tzv. standardní smluvní doložky (ty představují vlastně závazek smluvních stran osobní údaje předávat při respektování pravidel v těchto rozhodnutích Evropské komise stanovených, čímž je zaručena při předávání osobních údajů do třetích států potřebná míra ochrany osobních údajů). Ve všech ostatních případech je nezbytnou podmínkou pro předávání osobních údajů do třetích států získání povolení k předávání osobních údajů do zahraniční, a to ze strany Úřadu, ovšem za předpokladu, že z této povinnosti není stanovena výjimka (viz dále).

2.2 Předávání na základě Rozhodnutí Evropské komise

Jak již bylo naznačeno v úvodní části této kapitoly, k předávání osobních údajů bez prokazovaní dodatečných záruk může docházet v případech, kdy Evropská komise svým rozhodnutím potvrdila tzv. *odpovídající úroveň ochrany* osobních údajů předávaných ze států EU do příslušného státu. Až do současné doby byla přijata následující rozhodnutí Evropské komise:

- Rozhodnutí Komise ze dne 30. června 2003 podle Směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně osobních údajů v Argentině (2003/490/ES);
- Rozhodnutí Komise ze dne 8. května 2008 podle Směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně osobních údajů v Jersey (2008/393/ES);
- Rozhodnutí Komise ze dne 28. dubna 2004 o odpovídající ochraně osobních údajů na Ostrově Man (2004/411/ES);
- Rozhodnutí Komise ze dne 21. listopadu 2003 o odpovídající ochraně osobních údajů v Guernsey (2003/821/ES);

Kromě výšeuvedených případů je umožněno předávat osobní údaje na základě rozhodnutí Evropské komise též do Spojených států amerických a Kanady:

- Rozhodnutí Komise ze dne ze dne 26. července 2000 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně poskytované podle zásad bezpečného přístavu a s tím souvisejících často kladených otázek vydaných Ministerstvem obchodu Spojených států (2000/500/ES); a
- Rozhodnutí Komise ze dne 20. prosince 2001 o odpovídající ochraně osobních údajů, kterou poskytuje kanadský zákon o ochraně osobních informací a elektronických dokumentech (Personal Information Protection and Electronic Documents Act) (2002/2/ES).

Rozdíl oproti předešlým případům spočívá v tom, že předávání osobních údajů do Spojených států amerických není možné realizovat na základě uvedených rozhodnutí v každém případě; jinak řečeno, předávání osobních údajů na základě dotčených rozhodnutí vyžaduje naplnění specifických podmínek a okolností tam uvedených. Pokud by tomu tak nebylo, bylo by nutné k předávání osobních údajů použít jiné rozhodnutí (například o standardních smluvních doložkách) nebo jít cestou povolení předávání osobních údajů. O předávání osobních údajů do Spojených států amerických na základě uvedeného rozhodnutí bude pojednáno níže, v rámci samostatné podkapitoly.

K tomu, aby bylo možné osobní údaje předávat do třetích zemí, je třeba splnit celou řadu podmínek. Směrnice vyžaduje, aby předávání osobních údajů bylo realizováno za splnění podmínek stanovených v legislativě členských států (a tedy i ve Směrnici) a jen do takových třetích států, které zajišťují předávaným osobním údajům odpovídající úroveň ochrany. Podle čl. 25, odst. 2 Směrnice se skutečnost, zda daná země poskytuje odpovídající úroveň ochrany osobních údajů, posuzuje „*s ohledem na všechny okolnosti související s předáním nebo předáváním údajů*“. Ustanovení je doplněno též demonstrativním výčtem kritérií, která mají být při posuzování adekvátní úrovně ochrany osobních údajů zohledňována, a to: *povaha údajů, účel a trvání předpokládaného či předpokládaných zpracování, zemi původu a zemi konečného určení, právním předpisům (obecným i zvláštním) platným v dotčené třetí zemi, jakož i profesním pravidlům a bezpečnostním opatřením, která jsou ve třetí zemi dodržována.*“

Přijetí uvedených rozhodnutí Evropské komise vždy předcházelo podrobné hodnocení míry ochrany, která je osobním údajů v příslušné zemi poskytována. Je zajímavostí, že tři

z uvedených rozhodnutí se týkají nikoliv států, ale závislých území Britské koruny, totiž ostrovů Jersey, Guernsey a Isle of Man. Rozhodnutí Komise týkající se těchto tří států uvádějí, že ačkoliv se jedná o správní oblasti Britské koruny, těší se tyto nezávislosti (nejsou ani územím Velké Británie, ani její kolonií), s výjimkou mezinárodních vztahů a obrany, a proto i tyto ostrovy jsou považovány za třetí státy ve smyslu Směrnice. Přímo v rozhodnutích Evropské komise jsou též uvedeny záruky ochrany osobních údajů vyplývající z právních předpisů platných na daném ostrově, včetně ujištění, že „*právní normy obsahují všechny základní zásady nezbytné pro zajištění odpovídající úrovně ochrany fyzických osob*; *uplatnění těchto norem je zaručeno soudními opravnými prostředky a nezávislým dozorem prováděným orgánem vybaveným pravomocemi k provádění šetření a zásahů.*“[67]

2.3 Předávání osobních údajů do Spojených států amerických – pravidla Safe Harbor (Zásady bezpečného přístavu)

Rozhodnutí Komise č. 2000/500/ES ze dne ze dne 26. července 2000 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně poskytované podle zásad bezpečného přístavu a s tím souvisejících často kladených otázek vydaných Ministerstvem obchodu Spojených států (dále jen „**Rozhodnutí o Safe Harbor**“) představuje druhou alternativu předávání osobních údajů do Spojených států amerických ke smlouvě o předávání osobních údajů, obsahující standardní smluvní doložky. Hlavním účelem přijetí Rozhodnutí o Safe Harbor bylo usnadnit vzájemnou výměnu informací adále rozvíjet obchodní vztahy mezi Spojenými státy americkými a EU, zejména v rámci tzv. e-commerce (obchodování prostřednictvím elektronických komunikačních prostředků) a tím překonat odlišnosti v přístupu k ochraně osobních údajů, které vyplývají jednak z rozdílných právních tradic a východisek. Jak je uvedeno v Příloze 1 Rozhodnutí o Safe Harbor: „*Spojené státy přistupují k otázkám ochrany soukromí odlišně, než Evropská Unie. Spojené státy uplatňují odvětvový přístup, který je založen na kombinaci právních předpisů, nařízení a samoregulace.*“[68] V této souvislosti je nutno upozornit, že nejde o právní úpravu blížící se charakterem obecně závaznému právnímu

[67] Rozhodnutí o odpovídající úrovni ochrany v Jersey, preambule, bod 9.
[68] Rozhodnutí o Safe Harbor, s.6

předpisu. Rozhodnutí respektovat Zásady bezpečného přístavu[69] je jen na rozhodnutí dané organizace a představuje možnost, jak usnadnit předávání osobních údajů z EU do Spojených států. Je zcela na rozhodnutí dané organizace, zda pro účely přijímání osobních údajů ze EU zvolí tuto metodu nebo dá přednost předávání osobních údajů na podkladě smlouvy obsahující standardní smluvní doložky (či jinou metodu).

2.3.1 Pojem Pravidel Safe Harbor (Zásady bezpečného přístavu)

Pravidla Safe Harbor (dále jen „**Pravidla**“) představují formu záruk, jejichž respektování zaručuje, že osobním údajům předávaným z území EU do Spojených států amerických bude poskytována „odpovídající úroveň ochrany“. K tomu, aby bylo možné se na tyto Pravidla odvolávat jako na právní a závazný podklad, bylo nutné je inkorporovat do evropské legislativy. Rozhodnutí o Safe Harbor obsahuje vlastní text rozhodnutí Evropské Komise a především zahrnuje v Příloze 1 text Zásad bezpečného přístavu (text Pravidel), a dále v Příloze 2 související „často kladené otázky“ (tzv. FAQ) vydané Ministerstvem obchodu Spojených států amerických (ze dne 21.7.2000). Tyto dvě přílohy, představují zásady bezpečného přístavu neboli Pravidla, v užším slova smyslu.

Organizace, které mají být adresáty předávaných osobních údajů podle Pravidel ve Spojených státech amerických, musí splňovat kumulativně následující základní pravidla, uvedená v článku 1, odst. 2 Rozhodnutí o Safe Harbor:

- Jedná se o organizaci, která se jednoznačně a veřejně zavázala dodržovat Pravidla a tyto provádět v souladu s odpověďmi uvedenými v rámci často kladených otázek; a
- jde o organizaci, která podléhá pravomocím orgánu veřejné správy Spojených států amerických, který je uveden v Příloze 7 Rozhodnutí o Safe Harbor (tedy buď Federal Trade Commission (Komise pro federální obchod) anebo Ministerstvu dopravy Spojených států).

Naplnění prvního z výšeuvedených požadavků organizace dosáhne uveřejněním tzv. Prohlášení o ochraně soukromí (ang. *privacy policy statement*) a přihlášením se u Ministerstva obchodu Spojených států, které vede seznam všech organizací, které

[69] Pravidla Safe Harbor a Zásady bezpečného přístavu jsou synonymní pojmy.

podléhají americké jurisdikci, zamýšlejí být či jsou adresáty osobních údajů a které se zavázaly tato Pravidla respektovat. Přestože pro účely přihlášení se k respektování Pravidel stačí učinit požadované veřejné prohlášení jednou, je nutné každoročně obnovovat přihlášení se u Ministerstva obchodu Spojených států (tzv. „self-certification“[70]).

2.3.2 Obsah Pravidel Safe Harbor

Rozhodnutí o Safe Harbor stanoví jako první ze zásad, které potřeba respektovat **zásadu oznamovací povinnosti**. Organizace dodržující Pravidla a přijímající osobní údaje z EU má povinnost informovat fyzické osoby (občany EU) o účelu shromažďování a využívání jejich osobních údajů, o možnosti a způsobu organizaci v této souvislosti kontaktovat, o možnosti a prostředcích omezení organizace v používání a předávání těchto osobních údajů a o tom, jakým třetím osobám tyto informace předává. V Pravidlech je stanoveno, že *„toto oznámení musí být učiněno jasně a zřetelně při první příležitosti, při které je fyzická osoba **požádána**, aby poskytla organizaci své osobní údaje, nebo co možná nejdříve poté, avšak v každém případě předtím, než tato organizace takové osobní údaje použije pro účely jiné, než pro jaké je předávající organizace původně shromáždila či zpracovala, nebo než je poprvé předá třetí osobě.“*[71] Pojem „organizace“ v těchto Pravidlech označuje tu společnost, která má být / je příjemcem osobních údajů předávaných z EU.

V této souvislosti je nutné poukázat možná úskalí použitých termínů a pojmů. Jako první je možné poukázat (při striktním slovním výkladu), že tato Pravidla předpokládají situaci, kdy bude fyzická „požádána“ o poskytnutí osobních údajů. Z praktického hlediska lze předpokládat spíše situaci, kdy daná fyzická osoba bude poskytovat souhlas se zpracováním osobních údajů osobě z EU a tento souhlas bude poskytovat i pro účely předávání osobních údajů do zahraničí, respektive do USA. Z uvedené formulace je možné dovozovat, že je zde jednak možnost osoby předávající osobní údaje, aby požádala danou fyzickou osobu o poskytnutí jejích osobních údajů nebo též by připadalo do úvahy, aby tuto žádost vznesla přímo daná (americká) organizace. Jako poněkud

[70] Americký systém je založen na jiném principu regulace – oproti evropskému modelu centrální regulace je v případě USA použita metoda, kdy regulace není obecně nařizována, ale je přijímána subjekty z vlastní vůle. Tyto subjekty se tedy nepodléhají předchozí kontrole, ale sami prokazují, že naplnily stanovená pravidla – tedy certifikují se samy (*self-certification).*

[71] Rozhodnutí o Safe Harbor, s.8

problematické lze shledat ustanovení o tom, že toto oznámení (tedy poskytnutí základních informací o účelu, zpracování, limitaci a možnosti kontaktovat) může být učiněno i *„co nejdříve poté (co byla fyzická osoba požádána o poskytnutí osobních údajů“)*. Je zřejmé, že účelem této zásady je zabezpečit, že osobní údaje nebudou zpracovávány a předány do zahraničí nebo třetím subjektům bez vědomí subjektu údajů. Dostatek informací o povaze a formě zpracování osobních údajů je předpokladem, proto aby daná osoba svůj souhlas se zpracováním osobních údajů omezila či jej popřípadě vůbec neposkytla.

Mohla by se nabízet otázka, zda je či není tato oznamovací povinnost aplikovatelná na situace, kdy daná organizace zamýšlí zpracování poskytnutých osobních údajů pro stejné účely, jako organizace osobní údaje předávající. Při hodnocení použité formulace jako celku musíme dojít k následujícímu závěru – výšeuvedenou informační povinnost je potřebné splnit vždy, i tehdy, kdy by daná organizace zamýšlela přijaté osobní údaje zpracovávat pro stejný účel, jako je osoba předávající osobní údaje. I v tomto případě, bude potřeba danou fyzickou osobu požádat o poskytnutí osobních údajů a tím o vyjádření souhlasu s jejich zpracováním a předáváním. Ostatně takovýto výklad je zcela konsistentní se zásadami stanovenými evropskou právní úpravou, která odlišuje souhlas se zpracováním osobních údajů a souhlas s jejich předáváním.

V této souvislosti se jeví jako problematická druhá část výšeuvedené definice, a to: *„předtím, než je použije pro účely jiné…“*. Tato formulace by mohla vést k úvahám o tom, zda je potřebné subjekt údajů informovat o tom, že jeho osobní údaje budou předávány do Spojených států amerických v případě, kdy je zahraniční příjemce údajů bude zpracovávat pro stejný účel?[72] Měl by v tomto případě být subjekt údajů o předávání informován? Odpověď je jednoznačná – ano. Subjekt údajů by měl být vždy informován o všech aspektech zpracování osobních údaj, včetně předávání. A v případě předávání osobních údajů do Spojených států amerických, by měl být informován, že k předání bude docházet na principu Pravidel.

[72] Jako zjednodušený příklad si můžeme představit skupinu společností, členy které jsou jak česká, tak americká společnost. Česká společnost zpracovává osobní údaje svých zaměstnanců a klientů, pro účely naplňování politiky řízení lidských zdrojů (zaměstnanci) a hodnocení obchodní strategie (klienti). Osobní údaje by měla zasílat do USA, kde budou zpracovány pro tytéž účely.

Nadto, z označení této povinnosti jako „oznamovací“ by se v této souvislosti nabízela otázka, zda pouhé „oznámení“ (informování) je dostačujícím podkladem pro to, aby mohlo docházet ke zpracování osobních údajů pro jiné účely, než původně, nebo jejich poskytování třetím osobám. Jak již bylo zmíněno, oznámení a souhlas jsou propojenými prvky, které musí být z velké části používány společně. V případě předávání osobních údajů do zahraničí na principu Pravidel by se dokonce dalo říci, že jedno bez druhého ani není možné.

2.3.3 Možnost volby a citlivé osobní údaje

Další důležitou zásadou v Pravidlech je „možnost volby“. Tato zásada je promítnuta v dvou rovinách, jednak jde o možnost volby mezi tím, že daná fyzická osoba umožní či neumožní poskytování svých osobních údajů třetím osobám ze strany organizace, jednak jde o možnost odmítnout použití poskytnutých osobních údajů pro jiné účely, než ke kterým byly původně shromážděny či ke kterým dala daná fyzická osoba souhlas dodatečně.[73] V tomto ustanovení Pravidel je rovněž zakotvena povinnost umožnit v případě zpracování a předávání citlivých osobních údajů „potvrzující či výslovnou volbu“ zda mohou být citlivé osobní údaje předávány třetím osobám nebo zpracovávány pro jiné účely. Zásady rovněž stanoví, že „*by měly organizace s jakýmikoliv informacemi, které třetí osoba označí jako citlivé a takto s nimi zachází, zacházet jako s citlivými informacemi.*“

Vzhledem k tomu, že v Pravidlech je v tomto ustanovení uveden jen příkladmý výčet osobních údajů, které jsou považovány za citlivé, nabízí úvahu, že ochrana poskytovaná citlivým údajů je dokonce širší, než v případě úpravy evropské, která obsahuje výčet taxativní (v Směrnici o zpracování osobních údajů - v rámci oddílu III, *zvláštní kategorie zpracování*). Otázkou však je, zda je takto široký přístup vůbec v praxi realizovatelný. Můžeme si totiž představit situaci, kdy by různí lidé označili za citlivé různé druhy jejich osobních údajů. Jak by v takovém případě měla postupovat jak vysílající, tak přijímající organizace? Dokonce by mohly vznikat situace, kdy by evropská strana předávající

[73] *“Organizace musí fyzickým osobám dát možnost zvolit (odmítnout), zda jejich osobní údaje mohou být a) předány třetí osobě nebo b) použity k účelu, který je neslučitelný s účelem (účely), ke kterému (kterým) byly původně shromážděny nebo následně dotčenou fyzickou osobou schváleny. Dotčeným fyzickým osobám musí být umožněn výkon jejich práva na volbu jasným, srozumitelným, snadno dostupným a finančně přijatelným postupem*“, Rozhodnutí o Safe Harbor, s. 8

osobní údaje tyto za citlivé nepovažovala a americká strana, osobní údaje přijímající, by tak činit musela, a to s ohledem na přání subjektů údajů. Zvolený přístup zde vytváří prostor pro to, aby předávající osoba, v úmyslu poskytovat ještě větší ochranu osobním údajům, než požaduje zákon, označila některá data za citlivá a s nimi i tomto duchu nakládala. Zákon a evropská legislativa sice používají taxativní výčet pro citlivé údaje a přesně stanoví požadavky kladené na zpracovávání citlivých osobních údajů, je ale jednoznačné, že nelze příslušná ustanovení vykládat tak, že by nebylo možné stejný vysoký stupeň ochrany poskytovat jakýmkoliv dalším druhům osobních údajů.

Toto ustanovení Pravidel je však nutné vykládat v souvislosti s často kladenými otázkami. První z nich („FAQ-1 – Citlivé údaje“) vymezuje taxativně možnosti, kdy je možné citlivé osobní údaje zpracovávat, aniž by bylo potřebné *„vždy poskytnout možnost výslovné volby (svolení)*“. Konstrukci použitou v tomto případě je možné připodobnit ke zpracovávání osobních údajů bez souhlasu subjektu údajů.[74]

2.3.4 Předávání osobních údajů třetím osobám

Vedle zásady oznamovací je organizace povinna umožnit fyzické osobě odmítnout udělit souhlas s předáním osobních údajů třetím osobám. Tato Pravidla zakotvují odpovědnost organizace za to, že třetí osoba nakládá s poskytnutými osobními údaji v souladu s principy ochrany osobních údajů – organizace je totiž povinna se ujistit o tom, že třetí osoba buď *„přijímá zásady „bezpečného přístavu“nebo podléhá směrnici [o ochraně osobních údajů]nebo je u ní jinak zajištěna odpovídající úroveň ochrany, anebo s takovou třetí osobou uzavře písemnou dohodu, v níž se požaduje, aby tato třetí osoba zajistila nejméně stejnou úroveň ochrany, jakou vyžadují příslušné zásady bezpečného přístavu.*“[75] Toto ustanovení má rovněž za cíl zajistit ochranu americké organizace pro případ, že třetí osoba, které osobní údaje předala, s nimi nebude nakládat tak, aby byla zajištěna jejich odpovídající míra ochrany. *„Jestliže organizace splní tyto požadavky,*

[74] FAQ 1 – Citlivé údaje. Musí organizace vždy poskytnout možnost výslovné volby (svolení)? *„Ne, taková možnost volby se nevyžaduje, pokud je zpracování (1) v životně důležitém zájmu subjektu údajů nebo jiné osoby; (2) nezbytné pro uplatnění právních nároků nebo pro obhajobu; (3) nezbytné k poskytnutí zdravotní péče nebo určení diagnózy; (4) prováděno v rámci zákonné činnosti nadace, sdružení nebo jakékoli jiné neziskové organizace s politickým, filosofickým, náboženským nebo odborářským zaměřením a za podmínky, že se zpracování týká výhradně členů této organizace nebo osob, které s ní jsou v pravidelném kontaktu v souvislosti s jejími cíli a že údaje nebudou předány třetím osobám bez souhlasu subjektů údajů; (5) nezbytné pro splnění povinností této organizace vyplývajících z pracovního práva; nebo (6) pokud se týká údajů, které dotčená fyzická osoba prokazatelně zveřejnila.*“

[75] Rozhodnutí o Safe Harbor, s. 9

neponese odpovědnost (pokud se sama nedohodne jinak), pokud třetí osoba, které tyto informace předá, je zpracuje v rozporu s omezeními nebo se svými prohlášeními, ledaže by organizace věděla nebo musela vědět, že tato třetí osoba údaje zpracuje takovým nepřípustným způsobem, a neučinila náležité kroky, aby takovému zpracování zabránila nebo je zastavila.“[76] V opačném případě by totiž za takové porušení musela nést druhotnou odpovědnost.

Další záruky, které Pravidla stanoví, se týkají zajištění bezpečnosti zpracování osobních údajů: „*Organizace, které vytváření, uchovávají, používají nebo šíří osobní údaje, musí učinit přiměřená bezpečnostní opatření, aby zabránily jejich ztrátě, zneužití a neoprávněnému přístupu k nim, jejich předávání, změně nebo jejich zničení.*“[77]

Následující zásada, označená jako „Integrita údajů“ pracuje s požadavkem zpracovávat osobní údaje jen k tomu účelu, pro který byl udělen souhlas s takovým zpracováním nebo k němuž je daná organizace oprávněna tyto údaje zpracovávat i bez poskytnutí souhlasu. Za poněkud nejasný je možno označit požadavek Pravidel, aby osobní údaje byly „**podstatné** pro účely, pro které se mají použít“[78]. Takto použitá formulace by na první pohled mohla svádět k úvahám o tom, zda by osoba osobní údaje zpracovávající měla zájem zpracovávat osobní údaje, které by pro její konkrétně určený účel „nebyly podstatné“. Nicméně smyslem ustanovení je, podobně jako v případě evropské právní úpravy zajistit, že budou předávány a následně zpracovávány jen takové osobní údaje, které jsou pro daný účel nezbytné. Účelem této formulace je předejít tomu, aby docházelo k předávání celé masy osobních údajů, byť by následně mělo docházet ze strany organizace ke zpracování jen malé části těchto osobních údajů. Pravidla dále stanoví požadavek, aby nedocházelo ke zpracování osobních údajů k jinému účelu, než „*pro který byly původně shromážděny nebo následně fyzickou osobou dodatečně schváleny.*“[79] Pravidla, v ustanovení týkajícím se „integrity údajů“ dále vyslovují požadavek, aby organizace učinila „*přiměřené kroky, aby zajistila **spolehlivost** údajů pro zamýšlený účel, jejich přesnost, úplnost a aktuálnost*“.[80] Na jednu stranu je zřejmé, že bezpodmínečný závazek zpracovávat jen přesné osobní údaje, tak jak je stanoveno

[76] Rozhodnutí o Safe Harbor, s.8
[77] Rozhodnutí o Safe Harbor, s. 9
[78] Tamtéž.
[79] Tamtéž.
[80] Tamtéž.

v Zákoně, je v případě toho, kdy organizace obdrží osobní údaje od předávajícího subjektu, jen obtížně aplikovatelný a splnitelný. V této souvislosti je potřeba připomenout, že mezi subjektem přijímajícím osobní údaje a subjektem tyto osobní údaje předávajícím může jít v zásadě o dva základní typy vztahů: jednak vztah správce-správce, na druhé straně si lze představit i situaci správce-zpracovatel. V této souvislosti není úplně jasné, jakým způsobem by měla být ze strany přijímající organizace zajištěna „spolehlivost" přijímaných osobních údajů a ani není zcela jasné, co přesně tento termín má označovat.

Podobně, jako Zákon, Pravidla stanovují požadavek, že fyzickým osobám (o nichž jsou osobní údaje zpracovávány a předávány) musí být umožněn „*přístup k osobním údajům, které o nich organizace uchovává a musí mít možnost opravit, změnit nebo vymazat ty [osobní údaje], které jsou nepřesné…*"[81] V případě, že by poskytnutí takového přístupu vyžadovalo „*náklady neúměrné ohrožení soukromí fyzické osoby nebo kdyby byla porušena práva osob jiných než dotčené fyzické osoby*"[82] je možné uvedený přístup k úpravě nepřesných osobních údajů odepřít. Je nicméně otázkou, zda je možné v některých případech poměřovat náklady spojené s opravou určitého osobního údaje a míru, s jakou může být zasaženo do soukromí osoby, zejména v případě zpracování mylných citlivých osobních údajů o určité osobě.[83] Na druhé straně je možné položit otázku, zda a jak by takovéto náklady měly být měřeny. Není zde jednoznačná hranice mezi tím, kdy by tyto náklady přesáhly stanovenou míru, a staly se neúměrnými, a kdy by ještě dosahovaly akceptovatelné výše. Částečnou odpověď na tyto úvahy můžeme nalézt v rámci často kladených otázek, FAQ 8 – Práva na přístup. Tam je totiž uvedeno, že finanční pojetí nákladů nemůže být absolutní argumentem pro odepření takového přístupu, zejména pokud má takovýto krok, pro daný subjekt údajů, zásadní význam.[84]

[81] Rozhodnutí o Safe Harbor, s. 9
[82] Tamtéž.
[83] Lze si například představit hypotetickou situaci, kdy jisté své osobní údaje uvede uživatel nějaké internetové sociální sítě do svého profilu. Je zřejmé, že časem může vyvstat potřeba tyto údaje upravit.
[84] Rozhodnutí o Safe Harbor, s. 17 „*Náklady a zátěž představují důležité hledisko a musí být brány v úvahu,avšak nejsou rozhodující pro určení toho, zda je poskytnutí přístupu únosné. Například, jestliže se informace využívají při rozhodnutích, která mají na fyzickou osobu podstatný dopad (např. zamítnutí či přiznání důležitých výhod, jako je pojištění, hypotéka nebo zaměstnání), pak je v souladu s ostatními ustanoveními těchto FAQ organizace povinna tyto informace předat i v případě, .e je to relativně obtížné nebo nákladné*."

K tomu, aby bylo možné uvedené principy realizovat, je potřeba zabezpečit též možnost kontroly dodržování Pravidel, zavedení sankcionování při jejich porušování a též je potřeba začlenit úpravu řešení sporů. Dle Pravidel by řešením sporů měl být pověřen takový orgán, který by umožnil „*snadnou dostupnost a finanční přijatelnost*" řešení sporů. Rovněž by měly být stanoveny další kontrolní a sankční postupy a mechanismy zajišťující, že organizace, které se zavázaly k respektování Pravidel, je budou skutečně respektovat a jejich porušení budou odstraňovat.

2.3.5 Kritika Pravidel

Navzdory skutečnosti, že přijetí Pravidel je považováno za veliký úspěch a pokrok v oblasti předávání osobních údajů mezi Spojenými státy americkými a EU, ukazuje se potřeba monitorování a neustálého hodnocení jejich dodržování, případně též jejich revize. První kritiky Pravidel, respektive jejich praktického fungování se objevily v roce 2002, kdy bylo vydáno Stanovisko Komise (volně přeloženo z ang. *Commission Start Working Paper*) ze dne 13.2.2002 potvrzující, že „*podstatný počet společností, které se přihlásily k dodržování Pravidel, zřejmě nedodržuje požadovaný stupeň transparentnosti, pokud jde o jejich celkové závazky (v oblasti ochrany osobních údajů) a pokud jde o obsah jejich politik nakládání osobními údaji*."[85]

Za klíčový prvek ke skutečnému fungování Pravidel je považována schopnost vynutit jejich dodržování a popřípadě ukládat sankce (*enforcement*). Nicméně v této oblasti byly ze strany Evropské komise shledány značné rezervy. Hlavním problémem, který přetrval i do dnešních dob, je skutečnost, že společnosti, které se přihlašují k Pravidlům, nesplní svoji povinnost uveřejnit tento svůj závazek a dále nedodrží povinnost zpřístupnit jejich politiku nakládání osobními údaji (k jejímuž dodržování se v rámci přihlášení se k Pravidlům zavázaly).[86] Tento závazek (povinnost) stanovený Pravidly je obecně formulovaný a závazný, a nelze se tedy jeho dodržování jakkoliv vyhýbat. V tomto smyslu, například taková praxe společnosti, která se přihlásila k Pravidlům za účelem realizace přenosu osobních údajů zaměstnanců, kdy je o svém závazku dodržovat Pravidla informuje jen formou vnitřně závazných dokumentů, je praxí v rozporu

[85] Commission Staff Working Paper ze dne 13.02.2002, s.2
[86] Tamtéž, s.8

s Pravidly.[87] Je nutno si uvědomit, že účelem zavedení Pravidel je zabezpečení transparentnosti při nakládání osobními údaji. Ačkoliv je v EU nakládání osobními údaji upraveno velmi podobě díky procesu harmonizace, v případě Spojených států amerických tomu tak není. Je tedy nezbytné, aby byla (pokud má být na nakládání osobními údaji v konkrétní společnosti USA shledáno, jako zajišťující adekvátní míru ochrany) konkrétní pravidla a závazky společnosti obecně přístupné. Lze si totiž například přestavit situaci, kdy osobní údaje zaměstnanců jsou zpracovávány i určitou dobu po té, kdy zaměstnanec společnost opustí. Takový bývalý zaměstnanec by nemusel mít aktuální údaje týkající se nakládání jeho osobními údaji a o tom, kde a jakým způsobem se může domoci svých práv s tím souvisejících. Pokud by šlo jen o interně přístupné podklady, nemusel by mít možnost se k materiálům ohledně zpracování osobních údajů vůbec dostat.

Některé z uvedených problémů ohledně dodržování Pravidel byly zmíněny i v případě Stanoviska Komise ze dne 20.10.2004 (chybějící veřejná deklarace o přihlášení se k Pravidlům, nezpřístupnění politiky nakládání osobními údaji).[88] Kromě toho Komise rovněž konstatovala, že některé společnosti se zavázaly Pravidla respektovat ohledně vybrané skupiny osobních údajů, byť k předávání (zpracování) osobních údajů dochází ohledně širšího rozsahu osobních údajů.[89]

Dalším problémem může být rozsah společností, které se mohou k respektování Pravidel přihlásit a které mohou tento způsob certifikace pro předávání osobních údajů do EU využít. Jak již bylo zmíněno na začátku této podkapitoly, může se jednat jen o organizace, které podléhají buď Federal Trade Commission nebo americkému Ministerstvu dopravy.[90] Kupříkladu tato Pravidla nejsou přístupná vzdělávacím institucím, kterým takto nezbývá než zvolit jinou z možností pro předávání osobních údajů do zahraničí.

Orgány, které měly na respektování Pravidel dohlížet, po dlouhou dobu čelily kritice, že na dodržování Zásad bezpečného přístavu nekladou dostatečný důraz. Zdá se však, že

[87] Tamtéž.
[88] Commission Staff Working Paper ze dne 20.10.2004, s. 6
[89] Tamtéž.
[90] V obou případech jde o orgány, které působí na federální úrovni, tedy v oblastech, které nejsou svěřeny do výlučné pravomoci členských států Spojených států amerických.

i v tomto směru dochází k obratu. Od září tohoto roku americká Federaál Trade Commission zahájila několik řízení, ve kterých přezkoumávala dodržování Pravidel a jejichž výsledkem byly dohody (nebo spíše doporučení) pro dané společnosti, které musí realizovat, pokud chtějí nadále předávat a přijímat osobní údaje na bázi Safe Harbor.[91] Přesto se ukazuje se, že zavedení Zásad bezpečného přístavu může být přínosem pro realizaci předávání osobních údajů mezi EU a Spojenými státy americkými. Chris Connoly ve svém článku „*The US Safe Harbor – Fact or Fiction*" uvádí, že k září roku 2008 bylo evidováno takřka 1 700 společností, které se respektování Pravidel přihlásily. Nicméně je potřeba reagovat na nové trendy v oblasti zpracování osobních údajů a rovněž není možné opomenout skutečnost, že tato Pravidla byla schválena (vypracována) v roce 2000. Vzhledem k tomu, že každý rok přináší nové a nové otázky a problémy, měla by být zvažována novelizace Pravidel a jejich přizpůsobení dnešní době.

2.4 Standardní smluvní doložky

V případě, že předávané osobní údaje směřují k příjemci ve státě, jehož právní řád neposkytuje předávaným osobním údajům odpovídající úroveň ochrany, je možné k předávání osobních údajů přistoupit za předpokladu, že mezi předávajícím a přijímajícím subjektem bude uzavřena smlouva, která bude obsahovat tzv. *standardní smluvní doložky.*

2.4.1 Pojem standardních smluvních doložek

Tyto standardní smluvní doložky jsou obsaženy ve třech rozhodnutích Evropské komise, a to:

- Rozhodnutí Komise 2001/497/ES ze dne 15. června 2001 o standardních smluvních doložkách pro předávání osobních údajů do třetích zemí podle směrnice 95/46/ES (dále jen „Rozhodnutí o standardních doložkách");
- Rozhodnutí Komise 2004/915/ES ze dne 27. prosince 2004, kterým se mění rozhodnutí 2001/497/ES, pokud jde o zavedení alternativního souboru

[91] Více viz. The EU-US Safe Harbor Does Not Protect US Companies with Unsafe Privacy Practices.

standardních doložek pro předávání osobních údajů do třetích zemí (dále jen „Rozhodnutí o alternativních doložkách“);

- Rozhodnutí Komise 2002/16/ES ze dne 27. prosince 2001 o standardních smluvních doložkách pro předávání osobních údajů zpracovatelům usazeným v třetích zemích podle směrnice 95/46/ES (dále jen „Rozhodnutí o standardních doložkách pro zpracovatele“).

S ohledem na zachování flexibility smluvních (a zejména obchodních) vztahů bývají tyto standardní smluvní doložky začleňovány nejčastěji do samostatných smluv věnujících se problematice ochrany a předávání osobních údajů. Zpravidla jde o smlouvy označované jako „Smlouva o předávání osobních údajů“ (v angličtině „*Data Transfer Agreement*“). Z logiky věci je nicméně možné, a Rozhodnutí o standardních doložkách tuto skutečnost potvrzuje, tyto doložky začlenit i do smlouvy zakládající například vzájemnou obchodní (i jinou spolupráci) – ovšem za předpokladu, že jiná ustanovení takových smluv nebudou v rozporu s doložkami na ochranu předávných osobních údajů. Nicméně je vhodné upozornit, že ani smlouva obsahující standardní smluvní doložky ve znění dle uvedených rozhodnutí Evropské komise nezbavuje subjekt předávající osobní údaje tento typ zpracování oznámit Úřadu (tedy *notifikovat*). Obsahem zmíněných rozhodnutí jsou následující doložky:

Doložka / Dodatek	Charakteristika obsahu (Rozhodnutí o standardních smluvních doložkách / Rozhodnutí o standardních smluvních doložkách pro zpracovatele
Doložka 1	Definice základních pojmů
Doložka 2	Podrobnosti předávání
Doložka 3	Doložka ve prospěch třetí strany
Doložka 4	Povinnosti vývozce údajů
Doložka 5	Povinnosti dovozce údajů
Doložka 6	Odpovědnost
Doložka 7	Mediace a soudní příslušnost
Doložka 8	Spolupráce s orgány dozoru
Doložka 9	Vypovězení doložek / Rozhodné právo
Doložka 10	Rozhodné právo / Změna smlouvy
Doložka 11	Změna smlouvy / Povinnosti po ukončení poskytování služeb spojených se zpracováním osobních údajů
Dodatek 1	
Dodatek 2	Povinné zásady ochrany údajů uvedené v prvním odstavci doložky 5 písm. b) / Popis technických a organizačních bezpečnostních opatření zavedených dovozcem údajů
Dodatek 3	Povinné zásady ochrany údajů uvedené v druhém odstavci doložky 5 písm. b) / Není součástí

Jak již bylo naznačeno výše, standardní smluvní doložky jsou určeny pro předávání osobních údajů mimo území EU (respektive EHP) jednak ve vztahu správce – správce, a na druhé straně též ve vztahu správce – zpracovatel. Tomuto rozčlenění odpovídá i odlišná textace *Doložky 1* v Rozhodnutích o standardních smluvních doložkách a v Rozhodnutí o standardních smluvních doložkách pro zpracovatele. Porovnání definice *dovozce údajů* v obou výše uvedených rozhodnutích:

Dovozce údajů	
Rozhodnutí o standardních smluvních doložkách	Rozhodnutí o standardních smluvních doložkách pro zpracovatele
Správce údajů, který se zavazuje přijímat od vývozce údajů osobní údaje za účelem jejich dalšího zpracování v souladu s podmínkami těchto doložek a který nepodléhá systému třetí země zajišťující odpovídající ochranu	Zpracovatel usazený v třetí zemi, který se zavazuje přijímat od vývozce údajů osobní údaje určené ke zpracování jménem vývozce údajů po předání v souladu s jeho pokyny a podmínkami tohoto rozhodnutí a který nepodléhá systému třetí země zajišťující odpovídající ochranu

Definice subjektu osobní údaje předávajícího (tedy *vývozce údajů*) je v obou případech stejná – je jím „*správce, který předává osobní údaje*“. Ostatní pojmosloví (např. *pojmy osobní údaje, zvláštní kategorie údajů, subjekt údajů* apod.) je v obou případech řešeno odkazem na Směrnici.

Evropská i česká právní úprava vymezuje jako klíčový pojem – účel, pro který jsou osobní údaje zpracovávány. Význam účelu, jako základního kritéria je do určité míry omezen v případě předávání osobních údajů na základě standardních smluvních doložek. Rozhodnutí o standardních smluvních doložkách z roku 2001 požadovalo, aby smluvní strany v „Dodatku 1“ vymezily pro jaké účely je předávání osobních údajů „nezbytné“. Na druhé straně, Rozhodnutí obsahující alternativní standardní doložky požaduje vymezení účelu předávání osobních údajů, ale už nestanovuje výslovně požadavek, aby použité osobní údaje byly pro tyto účely nezbytné. V případě předávání osobních údajů ze strany správců zpracovatelům, standardní smluvní doložky požadavek zpracování osobních údajů pro stanovený účel výslovně nezmiňují. Ve skutečnosti, je tento požadavek zahrnut pod závazek správce předávajícího osobní údaje zpracovateli, že „zpracování osobních údajů, včetně předávání samotného, bylo a bude i nadále prováděno v souladu s příslušnými ustanoveními použitelného (vnitrostátního) práva na

ochranu osobních údajů.“[92] Omezení zpracování pro konkrétní účel (ve vztahu správce – zpracovatel) plyne i z logiky daného smluvního uspořádání – tj. správce uzavírá danou smlouvu o zpracování osobních údajů do zahraniční, mimo území EU, ale pro přesně stanovený účel. Správce, který zpracovává osobní údaje a (i podle definice v zákonné i evropské úpravě) stanovuje účel zpracování daných osobních údajů, potřebuje „pomoc zpracovatele“ s tímto zpracováním. Zpracovatel je oprávněn (v rámci plnění smlouvy) zpracovávat osobní údaje jen dle dané smlouvy, a nemůže se v žádném případě od stanoveného účelu jakkoliv odchylovat.

V rámci Dodatku 1 Rozhodnutí o standardních smluvních doložkách se požaduje, aby mezi správci osobních údajů v smluvních vztahu byla stanovena *doba uchovávání* předávaných osobních údajů. V tomto případě, je použita následující formulace „*předávané osobní údaje mohou být uchovávány nejdéle … (měsíce, roky).*“[93] Alternativní smluvní doložky již tuto poměrně striktní formulaci neobsahují. Místo toho je doba uchovávání poskytnutých osobních údajů zahrnuta mezi „další užitečné informace (doby uchovávání a další relevantní informace)“.

2.4.2 Řetězení zpracování osobních údajů

Přestože v praxi dochází k situacím, kdy zpracovatel osobních údajů využívá subdodávky třetích osob pro takovéto zpracování, jde o situaci, která je z hlediska aplikace právních předpisů k ochraně osobních údajů poměrně nejasná a sporná. V případě českého práva vznikla pochybnost o tom, zda je vůbec takovýto vztah podle Zákona přípustný, jinak řečeno – je vůbec zpracovatel (který má se správcem uzavřenou dohodu o zpracování osobních údajů) oprávněn uzavírat následnou smlouvu o zpracování osobních údajů se svým subdodavatelem? K uvedenému problému se vyjádřil negativně Úřad ve svém lednovém stanovisku č. 1/2009[94]. Úřad jednak odmítl, že by subdodavatelé zpracovatelů spadali pod definici pojmu zpracovatele v Zákoně („*ze znění tohoto ustanovení zcela jednoznačně vyplývá, že tuto smlouvu může uzavřít pouze správce se zpracovatelem, nikoli zpracovatel s dalším subjektem*“).[95] Úřad odkazuje správce i zpracovatele v tomto

[92] Rozhodnutí o standardních smluvních doložkách pro zpracovatele, s. 10 (Doložka 4)
[93] Rozhodnutí o standardních doložkách, s. 13
[94] Stanovisko č. 1/2009 Úřadu pro ochranu osobních údajů Zpracování osobních údajů na základě smluv uzavíraných se zpracovateli (tzv. řetězení zpracovatelů osobních údajů).
[95] Dle § 4, písm. K) Zákona je zpracovatelem každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona.

případě na ustanovení § 14 Zákona, když uvádí „*správce i zpracovatel však samozřejmě mohou využívat práce či služeb jiných osob (fyzických i právnických), a to v režimu § 14 zákona o ochraně osobních údajů. Toto ustanovení se vztahuje na zaměstnance správce či zpracovatele a dále na jiné osoby (fyzické i právnické), které zpracovávají údaje na základě smlouvy se správcem nebo zpracovatelem. Smlouvou je v tomto ustanovení myšlena pracovní či jiná obdobná smlouva, nikoli smlouva o zpracování osobních údajů podle § 6 zákona o ochraně osobních údajů.*“ Domnívám se, že takovýto přístup není správný. Jednak je potřeba zohlednit, že je zde objektivní potřeba takovéto vztahy zařadit do právního rámce ochrany osobních údajů, jelikož potřeba úpravy subdodavatelských právních vztahů plyne z obchodní praxe. Vzhledem k tomu, že Zákon je v tomto směru poměrně přísně koncipován a není příliš flexibilní, je na místě některá jeho ustanovení vykládat extensivně, do doby, než dojde k přizpůsobení právní úpravy novým podmínkám. Pokud je smyslem Zákona chránit subjekty údajů a jejich osobní údaje, tak to není možné činit tím, že bude určitá situace běžná v dnešním světě jednoznačně odmítnuta jako nepřípustná. Tím by jednak subdodavatelské vztahy byly vytlačeny do ilegality a jednak by došlo nutně k omezování svobody podnikání.

O tom, že jde o situaci stále běžnější, se kterou je potřeba se vypořádat svědčí i vydání Stanoviska č. 3/2009 k předloze rozhodnutí Komise o standardních smluvních doložkách pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích podle směrnice 95/46/ES (od správce údajů k zpracovateli údajů) Pracovní skupiny WP 29 (dále jen „**Stanovisko WP 3/2009**“).[96] V tomto Stanovisku WP 3/2009 se pracovní skupina vyjadřuje k další rovině uvedeného problému subdodávek zpracovatelům osobních údajů, a to zpracování osobních údajů subdodavateli z třetích zemí (mimo EU nebo EHP). Hovoří se tedy o problematice „řetězení“ zpracovatelských vztahů v oblasti ochrany osobních údajů. Už z existence tohoto Stanoviska WP 3/2009 je jasné, že pokud Evropská komise připouští existenci těchto typů vztahů, měl by svůj postoj Úřad přehodnotit. Pracovní skupina WP 29 v tomto dokumentu uvádí názor, že „*aniž jsou dotčena práva a povinnosti vnitrostátních orgánů dozoru podle vnitrostátních právních předpisů s ohledem na vydávání povolení podle čl. 26 odst. 2 směrnice, pracovní skupina vnitrostátní orgány dozoru vybízí, aby v případě smluv o mezinárodním dílčím*

[96] Stanovisko č. 3/2009 k předloze rozhodnutí Komise o standardních smluvních doložkách pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích podle směrnice 95/46/ES (od správce údajů k zpracovateli údajů).

zpracování uzavřených mezi správcem a zpracovatelem v EU/EHP považovaly za přiměřenou záruku to, že se v nich analogicky uplatňují stejné zásady a záruky jako ve standardních smluvních doložkách.“[97] Na evropské úrovni se totiž zvažuje změna standardních smluvních doložek pro zpracovatele tak, aby tyto nové subdodavatelské vztahy (i směrem vně EU či EHP) byly umožněny. Ochrana osobních údajů subjektů předávaných osobních údajů by měla být zajištěna formou analogické aplikace standardních smluvních doložek i na subdodavatelské vztahy, omezením možnosti jejich řetězení a dále upravením povinnosti správce osobních údajů v tom smyslu, že by měl umožnit jedno kontaktní místo pro celý řetězec zpracování osobních údajů, kde by subjekty údajů mohly svá práva uplatnit. Domnívám se, že takovýto přístup je přijatelný s ohledem na to, že hlavní odpovědnost za ochranu předávaných osobních údajů nadále zůstane koncentrována u správce (a v jediné osobě vývozce) osobních údajů.

2.5 Závazná podniková pravidla (Binding Corporate Rules)

V souvislosti s problematikou předávání osobních údajů a s postupujícím procesem globalizace světové ekonomiky vznikala stále častěji otázka, jakým způsobem efektivně přistupovat k řešení otázek souvisejících s ochranou osobních údajů a jejich zpracováním zejména v nadnárodních společnostech. V současné době nebude překvapením, že přestože většina nadnárodních společností má své sídlo ve státech EU, ostatní členové skupin těchto společností působí v různých státech světa. V této souvislosti tedy vznikala otázka, jakým způsobem umožnit předávání osobních údajů mezi členy skupin nadnárodních společností, a to jak na území EU, tak mimo ně.

2.5.1 Pojem závazných podnikových pravidel

V roce 2003 Pracovní skupina WP29 přijala první Pracovní dokument „WP 74“[98], který se týkal závazných podnikových pravidel pro předávání osobních údajů do zahraničí. Tato pravidla ve své podstatě představují další způsob, jakým umožnit a zjednodušit proces předávání osobních údajů do zahraničí v rámci jediné skupiny společností;

[97] Stanovisko č. 3/2009 k předloze rozhodnutí Komise o standardních smluvních doložkách pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích podle směrnice 95/46/ES (od správce údajů k zpracovateli údajů), s.3

[98] Výstupem Pracovní skupiny 29 jsou dokumenty označené jako „Working Documents“ – tedy v českém překladu jako „Pracovní dokumenty“, označované anglickými zkratkami „WP“ a pořadovým číslem.

přinášejí značné úspory a výhody jak pro společnosti samotné, tak pro orgány zabývající se ochranou osobních údajů. Pro společnosti představují alternativu, jak umožnit intra-skupinové předávání osobních údajů na jiném právním základě, než jsou předávání osobních údajů na podkladě rozhodnutí Komise či povolení k předávání osobních údajů do zahraničí pro jednotlivé společnosti. Základním východiskem je článek 26, odst. 2 Směrnice, který stanoví, že „ *…může členský stát povolit předání nebo předávání osobních údajů do třetí země, která nezajišťuje odpovídající úroveň ochrany (osobních údajů) ve smyslu čl.25, odst. 2 (Směrnice), pokud správce poskytne dostatečná ochranná opatření pro ochranu soukromí a základních práv a svobod, jakož i pro výkon odpovídajících práv…*“ Závazná podniková pravidla mohou představovat formu záruky správce osobních údajů ohledně naplnění a poskytování dostatečných opatření k ochraně zpracovávaných a předávaných osobních údajů, nicméně Pracovní dokument WP74 zdůrazňoval, že závazná podniková pravidla nenahrazují ani nepřekonávají použití smluvního řešení (včetně použití tzv. standardních smluvních doložek) pro účely předávání osobních údajů do zahraničí.

2.5.2 Charakteristika závazných podnikových pravidel

Závazná podniková pravidla (BCR) můžeme definovat jako formu podnikových pravidel komplexně řešících problematiku nakládání osobními údaji a jejich předávání v rámci jediné skupiny společností, která jsou závazná pro všechny členy dané skupiny společností, jsou vytvořena v souladu s principy Směrnice a v souladu s příslušnými právními předpisy týkajícími se ochrany osobních údajů. Pracovní dokument WP 74 zdůrazňuje tři základní aspekty závazných podnikových pravidel, a to:

- právní závaznost a vynutitelnost;
- společenstevní aspekt (použití ve společnostech); a
- účelem jejich existence je hlavně mezinárodní předávání osobních údajů[99].

První zmiňovaný aspekt, právní závaznost a vynutitelnost, je odlišujícím znakem těchto závazných podnikových pravidel od jiných vnitropodnikových dokumentů a směrnic, byť by se týkaly problematiky nakládání osobními údaji či jejich ochrany. Autoři Pracovního dokumentu WP 74 zdůrazňují, že právě tato jejich vlastnost je klíčová z hlediska

[99] Pracovní dokument WP 74, s. 8

naplnění požadavků Směrnice, neboť jen závazná pravidla či dokumenty mohou představovat dostatečnou míru ochrany osobních údajů. Druhý, společenstevní, aspekt koresponduje s použitím této formy k realizaci jednotné, závazné politiky týkající se osobních údajů, a to v rámci celé skupiny společností. Jedině jednotnou aplikací a závazností v rámci všech členských subjektů dané skupiny může být naplněn poslední klíčový znak, a to předávání osobních údajů do zahraniční jako hlavní důvod jejich existence. Požadavek na kompletní úpravu problematiky nakládání osobními údaji a jejich předávání v rámci skupiny v rámci závazných podnikových pravidel, který jsem zahrnula do úvodní definice, je podle mého názoru důležitým znakem, který by měl být zdůrazněn a měl být doplněn mezi klíčové znaky závazných podnikových pravidel v pojetí autorů Pracovního dokumentů WP 74. Rovněž je třeba zdůraznit, že tato pravidla řeší jedině mezinárodní předávání osobních údajů mezi společnostmi – členy skupiny, a nikdy nemohou být použita pro předání osobních údajů vně skupiny (tzv. „*onward transfer*“).

Tato závazná podniková pravidla jsou v prvním Pracovním dokumentu WP 74 používána synonymně s tzv. pravidly nakládání osobními údaji (v ang. originále tzv. *codes of conduct*). Nicméně již rok po vydání tohoto dokumentu, tedy v roce 2004, byla vydána Zpráva ICC ohledně závazných podnikových pravidel pro mezinárodní předávání osobních údajů[100], která tyto dva pojmy považuje za odlišné. Hlavním odlišujícím faktorem je účel použití těchto dvou nástrojů – pravidla nakládání osobními údaji jsou chápána jako společný závazný typ dokumentů, jehož závaznost je dána příslušenstvím subjektů k určitému odvětví, k specifické skupině podnikatelů či jinému subjektu a jejichž obsahem jsou návody či instrukce o tom, jakým způsobem má být osobními údaji nakládáno, zatímco závazná podniková pravidla jsou nástrojem vnitro-skupinového předávání osobních údajů do zahraničí. Jedním z nejzákladnějších odlišností je míra přizpůsobení dokumentu struktuře a potřebám skupiny společností, oproti poněkud obecnějšímu charakteru pravidel nakládání osobními údaji ve výšeuvedeném smyslu.

[100] Volně přeloženo „*ICC report on binding corporate rules for international transfers of personal data*“ ze dne 28.10.2004

2.5.3 Obsah Závazných podnikových pravidel

Požadavky na obsah BCR vyplývají jednak z charakteru činnosti dané skupiny společností (musí být vypracovány tak, aby odpovídaly způsobům zpracování osobních údajů, které jsou v dané skupině společností skutečně používané), dále je potřeba, aby BCR odpovídaly požadavkům, které na ně kladou jednotlivé dokumenty Pracovní skupiny WP 29. Tím by se mělo zajistit v obecné rovině, že daná skupina společností se zaváže k takovým postupům a způsobům ochrany osobních údajů, že dokáže naplnit míru ochrany osobních údajů požadovanou Směrnicí. V roce 2008 byl vydán dokument Pracovní skupiny WP29 (*Pracovní dokument stanovující tabulku se základními prvky a principy, které by měly být obsaženy v BCR)*[101] obsahující výčet požadavků jednak na obsah BCR, jednak na náležitosti žádosti o schválení BCR. Můžeme shrnout, že dle uvedeného dokumenty by zpracovávané BCR měly obsahovat zejména : záruky vnitřní a vnější závaznosti, převzetí odpovědnosti za dodržování BCR a zabezpečení efektivní aplikace BCR, vytvoření systému pro řešení stížností a sporů, vytvoření kontrolních mechanismů, přijetí povinnosti k spolupráci s příslušnými dozorovými orgány členských států. Tento dokument reflektuje požadavky a doporučení orgánů ochrany osobních údajů, i organizací reprezentující zájmy společností (i nadnárodních) a vlastně představuje pro nadnárodní společnosti jakési vodítko tvorby závazných podnikových pravidel.

BCR jsou koncipovány jako nástroj „*self-regulation*“ – reprezentují tedy aktivní přístup samotných společností, které samy vytváří pravidla nakládání osobními údaji ve společnostech dané skupiny a rovněž vytvářejí mechanismy pro zajištění jejich dodržování. BCR, podle výšeuvedeného dokumentů Pracovní skupiny WP 29 a podle Zprávy ICC, mají obsahovat záruky vnitřní závaznosti (vyslovení závazků BCR dodržovat jako závazné) a záruky závaznosti vnější. Ty musí jednak umožnit efektivní možnost subjektů údajů domoci se svých práv vyplývajících z BCR (zahrnující jak práva domoci se svých práv soudní cestou, tak právo na finanční odškodnění), jednak musí zajistit, skutečnou realizovatelnost takových práv (přijetí závazku k finančnímu odškodnění subjektů údajů ze strany společností a zajištění tohoto závazku existencí

[101] Volně přeloženo z ang. *Working Document setting up a table with elements and principles to be found in Binding Corporate Rules*, ze dne 24.6.2008

dostatečného množství aktiv[102]). V této souvislosti je potřeba upozornit na to, že uvedená práva může subjekt údajů realizovat vždy v Evropské unii, byť by k porušení BCR došlo společností dané skupiny, která leží vně teritoria Evropské unie.

Velmi zajímavým požadavkem je přijetí povinnosti důkazního břemena pro případ řešení sporů – pokud tedy bude subjekt údajů ve sporu namítat porušení BCR pravidel společností v rámci skupiny mimo EU, bude to organizace, která převzala závazek odpovědnosti za dodržování BCR v rámci celé skupiny, která bude prokazovat, že k porušení těchto pravidel nedošlo. Předpokladem k efektivní realizaci práv subjektů údaje ovšem je, že budou o svých právech a o právech vyplývajících z BCR dobře informováni – tedy, že k nim budou mít přístup. Na druhé straně BCR vyžadují, aby všechny společnosti k jejich aplikaci přistupovaly jednotně – tedy musí zde existovat určitý vzdělávací program a závazky zaměstnanců (kteří mají k zpracovávaným osobním údajům přístup) tak, aby i oni BCR respektovali. Možností, jak toho jednotlivé společnosti mohou docílit, je celá řada – počínaje vytvořením informačních materiálů, kurzů až po doložky o závaznosti těchto pravidel začleňované do pracovně-právních smluv (a jejich porušování sankcionováno disciplinárními opatřeními). Skupiny společností využívající BCR vyžadují existenci systému pro řešení stížností a sporů ze strany subjektů údajů. Celý systém může skutečně zajišťovat ochranu osobních údajů, pokud budou vytvořeny odpovídající kontrolní mechanismy – vnitřní (systém kontroly, sledování změn a vnitřních auditů) i vnější (povinnost společností spolupracovat s orgány dozoru nad dodržováním předpisů v oblasti ochrany osobních údajů a BCR). Jedním z nejdůležitějších požadavků je popis zpracovávaných (a předávaných) osobních údajů a datových toků v rámci skupin společností, neboť jen tak může být aplikace BCR dostatečně transparentní a kontrolovatelná.

Přestože BCR představují vhodný způsob, jak řešit otázku ochrany osobních údajů ve společnosti a umožnit snadnější předávání osobních údajů do zahraničí, je vždy potřeba pamatovat na limity jejich použití. Pokud mají BCR plnit dobře svůj účel, je potřebné, aby byly aplikovatelné ve stejné (nebo velmi podobné) podobě ve všech společnostech skupiny. Zpráva ICC o závazných podnikových pravidlech pro předávání osobních údajů

[102] Společnost se k výši svých aktiv ve vztahu k zajištění závazků k případné náhradě škody nevyjadřuje v samotných BCR, ale v žádosti o jejich schválení, kterou předkládá daným dozorovým orgánům.

do zahraničí[103] (z roku 2004) upozorňuje na nejednotný přístup ke schvalování BCR v rámci jednotlivých členských států EU a na možnost národních úřadů pro ochranu osobních údajů požadovat změny v předložených BCR.[104] Domnívám se, že tyto obavy lze překonat dvěma způsoby. Za prvé lze tato pravidla ochrany osobních údajů „nastavit" tak, aby reflektovaly přísnější právní úpravu, čímž by byla jednak zajištěna jednotná aplikace pravidel a navíc by tento přístup nepochybně uvítaly dozorové orgány členských států, a především subjekty údajů (tedy osoby zpracováním osobních údajů dotčené). Kromě toho další záruky ve směru jednotné tvorby BCR poskytuje i samotný schvalovací proces, během kterého jsou střídány fáze tvorby návrhů BCR a jejich konzultace s jednotlivými dozorovými orgány. Úřad ve svém dokumentu „Závazná podniková pravidla (Binding Corporate Rules) jako nástroj bezpečného předávání osobních údajů do třetích zemí" vysvětluje schvalovací proces BCR: „*Vytvoření a konečné schválení BCR je poměrně složitý a časově náročný proces. V rámci zemí EU je určen dozorový úřad, který je nejvhodnější autoritou pro předložení žádosti (většinou se jedná o dozorový úřad země, která je zároveň sídlem mateřské společnosti), a která následně koordinuje celý schvalovací proces. Žadatel, na základě jednání s odpovědným dozorovým úřadem (tzv. lead authority), vytvoří návrh BCR, který je zaslán k připomínkám dozorovým úřadům v EU působícím v zemích, z nichž jsou data předávána. Přijaté připomínky jsou předány zpět žadateli k vyjádření. Po vypořádání připomínek je připraven finální návrh, který je schválen relevantními dozorovými úřady*."

Přestože předávání osobních údajů na podkladě BCR není v praxi zatím příliš časté, objevují se první skupiny společností, které se touto cestou vydaly, a jejichž závazná podniková pravidla byla schválena. Například ve Velké Británii byly v září tohoto roku schváleny BCR skupiny společností Hyat Hotels, které se staly pátou skupinou, která bude osobní údaje v rámci skupiny předávat tímto způsobem.[105]

[103] Volně přeloženo z ang. *ICC report on binding corporate rules for international transfers of personal data*.
[104] Tamtéž, s.12
[105] Více viz. Hyatt signs up to EU binding corporate rules for data transfers

2.6 Předávání osobních údajů do zahraničí na základě povolení Úřadu

Předávání osobních údajů do zahraničí, mimo územích Evropské unie, pokud nepůjde o žádný z výšeuvedených případů, se může uskutečňovat výhradně na základě povolení Úřadu pro ochranu osobních údajů. Ustanovení § 27, odst. 3 Zákona stanoví, že *„před předáním osobních údajů do třetích zemí* podle *odstavce 3 (§ 27) je správce povinen požádat Úřad o povolení k předání, nestanoví-li zvláštní zákon jinak"*. Takové předávání i na základě povolení Úřadu nicméně vyžaduje, aby správce prokázal splnění alespoň jediné z podmínek uvedených v § 27, odst. 3, pod písmen a) až g). Toto však nelze vykládat tak, že předložení žádosti o povolení a uvedení některého ze zákonem stanovených důvodů automaticky povede k vydání povolení k předávání osobních údajů do zahraničí ze strany Úřadu. V každém případě předložení žádosti vede ke komplexnímu posuzování celého případu tak, aby byla zajištěna a ověřena ochrana předávaných osobních údajů. V případě, že Úřad rozhodne negativně, nelze osobní údaje do zahraničí předávat. V opačném případě je výsledkem takového posuzování na základě podané žádosti povolení, ve kterém Úřad stanoví dobu po kterou *„může správce předání provádět.*" V rámci žádosti správce předkládá i svoji představu, po kterou hodlá předávat (a teda zpracovávat) dané osobní údaje. Z výšeuvedené formulace však plyne, že od představ správce údajů se Úřad ve svém rozhodnutí může odchýlit a stanoví dobu pro předávání osobních údajů dle svého uvážení.

První podmínkou, a zpravidla nejčastěji uplatňovanou, je předávání osobních údajů *„se souhlasem nebo na základě pokynu subjektu údajů*" (§ 27, odst. 3, písm. a) Zákona). Další možností je, že správce prokáže, že *„jsou v třetí zemi, kde mají být osobní údaje zpracovány, vytvořeny dostatečné zvláštní záruky ochrany osobních údajů, například prostřednictvím jiných právních nebo profesních předpisů a bezpečnostních opatření*" (§ 27, odst. 3, písm. b) Zákona). Dle § 27, odst. 3, pís. c) je možné osobní údaje předávat též v případě, že *„ jde o osobní údaje, které jsou na základě zvláštního zákona součástí datových souborů veřejně přístupných nebo přístupných tomu, kdo prokáže právní zájem; v takovém případě lze osobní údaje zpřístupnit jen v rozsahu a za podmínek stanovených zvláštním zákonem*", podobně lze osobní údaje předávat pokud *„je předání nutné pro uplatnění důležitého veřejného zájmu vyplývajícího ze zvláštního zákona nebo z mezinárodní smlouvy, kterou je Česká republika vázána*". Další, velmi častou variantou

je „*předání nezbytné pro jednání o uzavření nebo změně smlouvy, uskutečněné z podnětu subjektu údajů, nebo pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů*“. Jistou podobu s předchozím můžeme nalézt též v případě předávání dle § 27, odst. 3, písmena f), a to při předávání „*nezbytném pro plnění smlouvy uzavřené v zájmu subjektu údajů mezi správcem a třetí stranou, nebo pro uplatnění jiných právních nároků*“. A konečně v případě, že „*předání nezbytné pro ochranu práv nebo životně důležitých zájmů subjektu údajů, zejména pro záchranu života nebo pro poskytnutí zdravotní péče*“.

2.6.1 Řízení o povolení předávání osobních údajů do zahraničí

V této souvislosti je na místě upozornit, že dle § 41 Zákona se v řízeních upravených Zákonem obecně postupuje podle správního řádu (pokud není stanoveno jinak). Podáním žádosti o povolení předávání osobních údajů do zahraničí je zahájeno „klasické“ správní řízení o žádosti a uplatní se zde i lhůty pro vyřízení věci dle správního řádu. Vzhledem k tomu, že se však jedná o poměrně složitou problematiku s potenciálními závažnými důsledky z hlediska ochrany osobních údajů a soukromí subjektů údajů, nebývá obvyklé získání takového rozhodnutí ve lhůtě 30 dní. Rovněž je velice pravděpodobné, že si Úřad vyžádá od žadatele (správce údajů) další podklady a vysvětlení, pročež zpravidla správní řízení přeruší.

V této souvislosti je potřeba zdůraznit, že povolení k předávání osobních údajů do zahraničí samo o sobě k takovémuto zpracování osobních údajů nestačí. Jednak, zpravidla bude předávání údajů předcházet jejich shromažďování a jiné zpracovávání (například setřídění apod.) zpravidla vyžadující souhlas subjektů údajů, jednak po předání bude k jejich zpracování docházet ze strany jiného subjektu. V tomto smyslu je potřeba zabezpečit, že s předanými osobními údaji bude zacházeno jen určitým způsobem a bude zabezpečena jejich ochrana, je tedy nezbytné, aby mezi osobou předávající a přijímající osobní údaje existoval smluvně podepřený vztah týkající se nakládání osobními údaji. Nejčastěji půjde o smlouvu o předávání osobních údajů (tzv. *data transfer agreement*), kterou můžeme klasifikovat jako smlouvu o zpracování osobních údajů ve smyslu § 6 Zákona. Přestože toto ustanovení zmiňuje smlouvu uzavřenou mezi správcem a zpracovatelem osobních údajů, je namístě analogicky toto ustanovení aplikovat též na vztahy správce – správce. Přestože Zákon výslovně

s možností smluvních vztahů tohoto typu výslovně nepočítá, v praxi se i takovéto vztahy objevují, o čemž svědčí i to, že standardní smluvní doložky připravované Evropskou komisí i v této podobě existují. Potřeba smluvního zabezpečení předávání osobních údajů do zahraničí rovněž implicitně vyplývá z povinností kladených správcům osobních údajů v České republice (odesílatelům osobních údajů), zejména pak v § 13 Zákona. Navzdory uzavření soukromoprávní smlouvy vymezující blíže podmínky zpracování a předávání osobních údajů je potřeba mít neustále na mysli, že „*odpovědnosti za správní delikt v oblasti veřejného práva se zásadně nelze vyhnout poukazem na smluvní ujednání mezi účastníky soukromoprávního vztahu.*“[106]

[106] Rozhodnutí Nejvyššího správního soudu 9 As 34/2008 ze dne 12.2.2009

3 Aktuální otázky zpracování osobních údajů

K ilustraci skutečnosti, že ochrana osobních údajů je veskrze aktuálním a neustále se vyvíjejícím se tématem, je na konci této diplomové práce zařazena kapitola věnující se aktuálním otázkám zpracování našich osobních údajů. Účelem zařazení následujících několika málo příkladů je nastínit některé situace v souvislosti se zpracováním osobních údajů, se kterými se často setkáváme nebo můžeme setkat, a zaměřit pozornost čtenáře na problémy v oblasti ochrany osobních údajů, které jsou v současné době diskutovány, případně též upozornit na další, méně diskutované aspekty dané problematiky.

Věřím, že zvolené příklady jsou demonstrativní a nadmíru aktuální. Nicméně je nutné poznamenat, že nejde, v žádném případě, o výčet vyčerpávající. Aktuálnost této problematiky nadále vyvolává a přináší stále nové a nové otázky, které však, s ohledem na rozsah a téma této práce není možné zohlednit.

Vlastní text je rozčleněn do tří základních okruhů, z hlediska toho, zda a v jaké míře si uvědomujeme, že dochází ke zpracování našich osobních údajů a z hlediska toho, zda je zpracování našich osobních údajů zcela dobrovolné (a tedy plně závislé na poskytnutí našeho souhlasu), zda je „vynuceně dobrovolné“ nebo zda jde o situace, kdy naše osobní údaje poskytujeme ke zpracování povinně.

3.1 Zpracování osobních údajů na bázi plné dobrovolnosti

3.1.1 Sociální sítě

V souvislosti s rozvojem informačních technologií a procesem globalizace dochází ke stále častějšímu zpracovávání osobních údajů a zejména k jejich předávání do zahraničí. V posledních letech bylo předávání osobních údajů do zahraniční nejčastěji spojováno s rozvojem obchodu, zejména internetového obchodování. Také asi nebude překvapením, že k největší výměně osobních údajů dochází mezi Evropou a Spojenými státy americkými, jako dvěma centry světové ekonomiky. Zcela novým fenoménem, který je neustále na vzestupu, jsou tzv. sociální sítě (ang. *social network*s)- místa na

internetu, která jednak usnadňují navazování a udržování kontaktů mezi lidmi, ale též umožňují zpracování osobních údajů ve velmi široké míře – s nejrůznějšími pozitivními, ale i negativními důsledky.

Mezi velmi známé sociální sítě patří například: **Facebook, MySpace či Linked.** Velmi zjednodušeně řečeno jde o takové služby uživatelům internetu, které jim umožňují vytváření osobních webových stránek zpravidla přístupných ostatním uživatelům dané služby a které jsou na sebe propojeny prostřednictvím sítě odkazů a souvisejících aplikací (služeb). Na jedné straně sociální sítě přinášejí svým uživatelům možnosti získávat o svých přátelích informace takřka v reálném čase, být informován o jejich životě, na straně druhé je nutné si uvědomit, že stejné informace poskytují uživatelé sami. Dle některých názorů neustále roste obliba sociálních sítí a počet jejich uživatelů roste dokonce přímo geometrickou řadou.[107] *„Osobní údaje zveřejněné na internetových stránkách sociálních sítí mohou využít třetí strany k řadě účelů, včetně obchodních, a mohou představovat značná rizika, jako je krádež totožnosti, finanční ztráty, ztráta obchodních příležitostí či možnosti zaměstnání a tělesná újma*“[108]. Internet umožňuje svým uživatelům dopřát si luxus v podobě anonymity nebo umožňuje vytvářet zcela nové, virtuální, identity. V tomto prostředí existuje riziko, že osobní údaje zpřístupněné přátelům v rámci sociální sítě mohou být přístupné dalším, nežádoucím osobám, a to díky řetězení odkazů mezi stránkami uživatelů dané sociální sítě. Navzdory skutečnosti, že provozovatelé takových sociálních sítí jsou často nuceni přijímat opatření posilující prvky ochrany osobních údajů, rizika zde budou existovat vždy.

Nejen v souvislosti s provozováním internetových sociálních sítí, ale obecně v důsledku rozvoje komunikace prostřednictvím Internetu vyvstala celá řada otázek s přesahy do oblasti ochrany osobních údajů. Jako jeden z klíčových problémů se ukázala otázka právního rámce (respektive jurisdikce), který bude na provozovatele dané sociální sítě dopadat. Jde rovněž o to, že uživatelé daných sítí zpravidla ani nemusí mít skutečnou představu o tom, v jaké zemi sídlí daný provozovatel a kde dochází k faktickému zpracování osobních údajů. Subjekty údajů, ačkoliv zpravidla udělují k takovým formám zpracování svých osobních údajů souhlas, musí mít garantována i další práva s tím spojená. A především musí mít možnost se jich reálně domáhat. Pracovní skupina WP29

[107] Stanovisko č. 5/2009 k internetovým sociálním sítím, s.4
[108] Tamtéž.

ve svém Stanovisku 1/2008 k otázkám ochrany údajů v souvislosti s vyhledávači ze dne 4. dubna 2008 přistoupila k poměrně širokému vymezení aplikovatelnosti Směrnice na provozovatele „internetových vyhledávačů“ a dovodila, že evropské předpisy na ochranu osobních údajů by měly být aplikovány v případě, kdy na území EU (respektive EHP) existuje „stálá provozovna“ takového provozovatele internetových vyhledávačů nebo *„z důvodů používání prostředků“*[109]. V podobném duchu se nesly i úvahy nad aplikovatelností evropského právního rámce pro ochranu osobních údajů v případě sociálních sítí. „*Na poskytovatele [služeb sociálních sítí] se ve většině případů vztahují ustanovení směrnice o ochraně údajů, a to i tehdy, jestliže se jejich ústředí nacházejí mimo EHP*.“[110] Otázkou je, zda budou mít uživatelé těchto sítí skutečnou šanci úspěšně svá práva uplatňovat. Určitou naději v této oblasti přináší rozhodnutí některých státních orgánů zabývajících se ochranou osobních údajů – například kanadský úřad pro ochranu osobních údajů několikrát upozornil na nedostatky sociální sítě Facebook z hlediska ochrany osobních údajů a vyzval k jejich odstranění tak, aby bylo učiněno zadost požadavkům kanadské legislativy.[111] S ohledem na charakter a oblibu sociálních sítí lze očekávat, že v této oblasti dojde k právním sporům a k následnému přizpůsobování právních norem těmto novým fenoménům.

3.1.2 Soutěže a hry

Dalším příkladem toho, kdy lidé odhalují veřejnosti své nejosobnější informace, jsou nejrůznější soutěže a hry. Zcela nový rozměr toto zpřístupňování osobních údajů získalo popularizací tzv. reality show – televizních soutěží, ve kterých jsou účastníci pod drobnohledem kamer a kdy zcela ztrácí jakékoliv soukromí. Podobně soutěžní hry, kdy soutěžící zcela dobrovolně sděluje moderátorovi své nejsoukromější úvahy, zážitky – své osobní údaje - s vidinou získání určitých částek peněz, představují formy zpracování osobních údajů. Otázkou jde, zda jsou si účastníci těchto her a soutěží vědomi toho, že takto zpřístupněné osobní údaje (a tím i své životy) dávají k dispozici takřka neomezenému počtu osob, a to nejen prostřednictvím televizních kamer, ale

[109] Stanovisko č. 1/2008 k otázkám ochrany osobních údajů v souvislosti s vyhledávači, s. 10 *Vyhledávače, které používají prostředky na území členského státu (EHP) pro zpracování osobních údajů, také spadají do oblasti působnosti práva dotčeného členského státu v oblasti ochrany údajů. Právo členského státu v oblasti ochrany údajů se použije, pokud správce […] používá za účelem zpracování osobních údajů prostředků, automatizovaných či nikoli, umístěných na území zmíněného členského státu, ledaže jsou tyto prostředky použity pouze pro účely tranzitu přes území Společenství* .“

[110] Stanovisko č. 5/2009 k internetovým sociálním sítím, s.5

[111] Více viz. Office of the Privacy Commissioner of Canada, Facebook agrees to address Privacy Commissioner‘s Concerns, http://www.priv.gc.ca/media/nr-c/2009/nr-c_090827_e.cfm .

i prostřednictvím internetu. Samotní účastníci ztrácí nejen své soukromí, ale rovněž nemají skutečnou kontrolu nad zpracováním svých osobních údajů, neboť jsou to velmi často pořadatelé těchto soutěží, kdo rozhodují o tom, které získané záběry budou odvysílány a které osobní údaje budou zpřístupněny celé veřejnosti. V této souvislosti se můžeme ptát, zda vůbec a v jaké podobě na podobné soutěže dopadá regulatorní rámec ochrany osobních údajů. Lze v této souvislosti vůbec hovořit o ochraně osobních údajů a o souhlasu s jejich zpracováním? Domnívám se, že nikoliv. Přestože samotní účinkující mohou mít do značné míry alespoň rámcovou představu o tom, co je v dané soutěži čeká (a tedy jaké jejich osobní údaje budou zpracovávány), realita může být zcela jiná. Pořadatelé mohou (a pravděpodobně tomu tak často i je) získané informace veřejnosti sdělovat ve zcela účelové podobě, kterou účastník zpravidla nemá možnost ovlivnit, a mohou tak získané osobní údaje zneužít. Pokud Zákon předpokládá, že získané osobní údaje mají být zpracovávány jen pro předem stanovený účel, můžeme se ptát – jaký je skutečný účel zpracování osobních údajů formou odvysílání a uchovávání záznamů z těchto soutěží? Domnívám se, že současná právní úprava na tyto otázky nedává zcela jednoznačnou odpověď.

3.2 „Vynuceně dobrovolné“ zpracování osobních údajů

Další skupinou poměrně sporných případů zpracování osobních údajů představují situace, kdy subjekt údajů sice své osobní údaje poskytuje dobrovolně a se svým souhlasem (ať už výslovným nebo implicitním), ale kdy je v takovém zpracování osobních údajů obsažen i prvek donucení k poskytnutí osobních údajů nebo k jejich poskytnutí nad minimální požadovaný rámec. Jde o „vynuceně dobrovolné“ poskytování osobních údajů a jejich následného zpracování. Pokud by totiž subjekt údajů svoje osobní údaje neposkytl, neměl by přístup k některým, pro něj důležitým službám apod. Z tohoto důvodu jsem podobné případy nazvala „vynuceně dobrovolným“ zpracováním osobních údajů. Zmíněné praktiky ilustrují následující tři příklady – případ uchazečů o zaměstnání a zaměstnanců, zasílání marketingových a jiných reklamních sdělení a použití tzv. čipových karet (elektronických peněženek).

3.2.1 Uchazeči o zaměstnání a zaměstnanci

V případě, kdy se uchazeč o zaměstnání obrací na potenciálního zaměstnavatele a zasílá mu svůj životopis (a popřípadě jiné požadované podklady) dochází ke zpracování osobních údajů uchazečů o zaměstnání v souladu s výjimkami uvedenými v § 5, odst. 2, písm. a) až b) Zákona. Takové osobní údaje je tedy možné zpracovávat i bez (výslovného) souhlasu daného uchazeče (či posléze zaměstnance).[112] Nicméně můžeme dovozovat, že uchazeč o zaměstnání svůj implicitní souhlas se zpracováním osobních údajů poskytuje, byť nepůjde o souhlas ve smyslu Zákona. Na druhé straně je potřeba zdůraznit, že pokud by snad zaměstnavatel zpracovával poskytnuté osobní údaje v širším než nezbytném rozsahu nebo k dalším účelům, než k plnění povinností mu stanovených zákonem nebo vyplývajících z jednání o uzavření pracovněprávní smlouvy, byl by povinen opatřit si od příslušného uchazeče o zaměstnání nebo zaměstnance informovaný souhlas.[113]

V této souvislosti může vyvstat otázka, jak postupovat v případě, kdy kupříkladu uchazeč o zaměstnání zahrne do svého životopisu informace nad rámec požadavků potenciálního zaměstnavatele, uvede informace, na jejichž pokladě potenciální zaměstnavatel může dovozovat například citlivé osobní údaje o dané osobě nebo jak reagovat v případě, kdy poskytnutí informací nad rámec požadavků stanovených zákonem nebo vyplývajících z jednání o pracovně-právním vztahu požaduje zaměstnavatel sám.[114] Je evidentní, že v některých případech mohou být informace, které zaměstnavatel po uchazeči požaduje, velmi citlivé (byť nikoliv citlivé údaje ve smyslu Zákona).[115] Je všeobecně známo, že někteří zaměstnavatelé vyžadují informace o rodinných poměrech uchazeče, o možném vývoji rodinných poměrů, o jeho zdravotním stavu, byť tyto informace ani nemusí být

[112] Pozn. Zákon č. 262/2006 Sb. , Zákoník práce, vymezuje celou řadu povinností zaměstnavatele zasahujících do oblasti ochrany osobních údajů. Jedná se například o povinnosti týkající se uchazečů o zaměstnání (§ 30, odst. 2 tohoto zákona, viz níže), dále kupříkladu povinnosti týkající se evidence pracovních úrazů a nemocí z povolání (§ 105 tohoto zákona), vedení osobního spisu zaměstnance a poskytování potvrzení po ukončení pracovně-právního vztahu (§ 312-314 tohoto zákona) nebo povinnosti směřující k zabezpečení práva na soukromí zaměstnanců (§ 312).

[113] Dle § 30, odst. 2 Zákoníku práce *„zaměstnavatel smí vyžadovat v souvislosti s jednáním před vznikem pracovního poměru od fyzické osoby, která se u něj uchází o práci, nebo od jiných osob jen údaje, které bezprostředně souvisejí s uzavřením pracovní smlouvy*.“

[114] Pozn. Lze si například představit situaci, kdy uchazeč o zaměstnání uvede informace o svém rodinném životě, byť toto zaměstnavatel nepožaduje. Stejně tak může vzniknout situace, kdy uchazeč uvede například mezi svými neprofesními aktivitami členství v různých organizacích, ze kterých lze usuzovat na jeho politické smýšlení a názory.

[115] Například údaje o počtu dětí či rodinném stavu.

pro výkon daného povolání relevantní. Tyto způsoby zpracování osobních údajů jsou zařazeny do této části kapitoly, neboť je, bohužel, časté, že poskytnutí takových osobních údajů bývá vyžadováno pod citelnou sankcí – nezařazení do dalších výběrových kol výběrových řízení.

3.2.2 Zasílání marketingových a jiných reklamních sdělení

Přestože se na první pohled může zdát, že jde o natolik specifické téma, které jde nad rámec ochrany osobních údajů, dovolila jsem si zařadit jeden příklad z této oblasti do této práce. Na první pohled se může zdát, že v tomto případě ani tak nejde o oblast ochrany osobních údajů. Nicméně opak je pravdou. Velmi diskutovaným problémem, který souvisí přímo se zpracováním osobních údajů, je udělování automatického souhlasu pro účel oslovování klientů společností reklamními a marketingovými materiály (v dnešní době nejčastěji pomocí prostředků elektronických komunikací), vytváření databází a uchovávání takových osobních dat. Jde o to, že udílení zmiňovaného souhlas je technicky řešeno jako automatické, takže klient nemá možnost udělení souhlasu odmítnout a navíc, by se tak vystavil (v případě neudělení) riziku, že mu služby, o které má zájem, nebudou poskytnuty.

Na tomto místě je potřeba upozornit, že zde dochází k propojování dvou aspektů ochrany osobních údajů – poskytnutí osobních údajů pro marketingové účely a zasílání reklamních a jiných podobných sdělení formou elektronických prostředků.[116] Přestože zákon o některých službách elektronických komunikací připouští oslovování klientů společnosti formou prostředků elektronických komunikací, a to „ *v souvislosti s prodejem výrobku nebo služby …pro potřeby šíření obchodních sdělení týkající se vlastních obdobných výrobků nebo služeb, pokud má zákazník jasnou a zřetelnou možnost jednoduchým způsobem…odmítnout souhlas s takovým využitím svého elektronického kontaktu i při zasílání každé jednotlivé zprávy, pokud původně toto využití neodmítl.*“[117] Navzdory výšeuvedeným požadavkům je v praxi běžné, že poskytnutím některých svých kontaktních osobních údajů (například pro účely moderní elektronické komunikace s bankami a jinými poskytovateli služeb) klient automaticky uděluje souhlas se

[116] Zasílání marketingových a jiných reklamních materiálů formou elektronických sdělení je regulováno § 7 zákona č. 480/2004 Sb. zákona o některých službách informační společnosti.
[117] § 7, odst. 3 zákona č. 480/2004 Sb. zákona o některých službách informační společnosti

zpracováním osobních údajů pro nejrůznější účely a též pro účely marketingové. Ještě zajímavější jsou situace, kdy jde o udělování souhlasu k zasílání obchodních sdělení ze strany členů skupiny daného poskytovatele služeb (může být též taktéž automaticky zahrnováno). Pokud bychom teoreticky uvažovali o možnosti existence takové skupiny společností, které jsou sice propojeny, ale zabývají se nejrůznějšími aktivitami – nebude takto koncipovaný souhlas v rozporu s vlastním obsahem a účel právní úpravy? Domnívám se, že i v takovýchto případech by měla být osobám, jejichž souhlas je získáván, dána jednoznačná a skutečná možnost vybrat, kdo jej bude moci oslovit a zda vůbec.

3.2.3 Čipové karty (elektronické peněženky)

Rozvoj platebního styku se projevuje nejen tím, že naprostá většina lidí má nějakou formu debetní nebo kreditní platební karty, ale začínají se stále častěji objevovat i prostředky umožňující placení nejen elektronickými penězi (ang. *e-money*) prostřednictvím tzv. elektronických peněženek nebo nově též pomocí mobilních telefonů (ang. *m-money*). Elektronické peněženky mají v současné době často podobu karty (obdobně jako platební karty) a obsahují čip, na kterém jsou nahrány údaje o výši elektronických peněz k dispozici.

Od původního určení, jako pouhého platebního prostředku, získávají elektronické peněženky na oblibě a používají se k nejrůznějším účelům: jako slevové karty, identifikační průkazy nebo jako platební prostředky. Zde je však potřeba mít na paměti, že s rozšiřováním možností uplatnění těchto karet zpravidla roste i počet osobních údajů, které jsou na takové elektronické peněžence zaznamenány. Ruku v ruce s tím rostou možnosti zpracování takových osobních údajů při používání takových elektronických peněženek. Vzniká tak prostor pro možnosti shromažďování osobních údajů i k jiným účelům nebo i jejich zneužití.

Veškeré moderní technologie v sobě nesou společné znaky – rozvoj vědy a techniky směřuje k jejich stále častějšímu používání v každodenním životě. Technologie i produkty, které je ztělesňují, jsou stále složitější. Jejich složitost vede k tomu, že lidé, kteří tyto produkty používají, ani nemusí mít ponětí o tom, že určitý produkt nese jejich osobní údaje a že je předává dalším subjektům. Moderní technologie a produkty na jedné

straně usnadňují život, na druhé straně vedou ke ztrátě kontroly nad tím, které osobní údaje skutečně chceme zpřístupnit ostatním a které nikoliv.

Výšeuvedená rizika mohou být o to markantnější, pokud jsou lidé velmi silně motivováni (až nuceni) elektronické peněženky používat. Příkladem by mohlo být zavedení karty „Opencard“ v Praze – jako elektronické tramvajenky či registrační karty pro přístup do městské knihovny.[118] Dalším příkladem – tentokráte z oblasti mobilních telefonů – je zakoupení jízdenky na pražskou hromadnou dopravu prostřednictvím zaslání sms. Při zavedení možnosti placení jízdenek formou sms pražský dopravní podnik původně zamýšlel získané osobní údaje uchovávat po dobu celých deseti let. Po zásahu a prověřování ze strany Úřad se ukázalo, že pro naplnění účelů stačí, pokud získané osobní údaje bude podnik uchovávat pouhých 90 dní![119] Je nepochybné, že s rostoucí dobou zpracovávání (uchovávání) osobních údajů roste i potenciál pro jejich zneužití.

3.2.4 Uvěrové registry

Takřka každý den slyšíme z televize, rádia nebo čteme v novinách, že si můžeme půjčit velmi snadno takřka jakoukoliv částku a pořídit si to, na co nám zrovna prostředky nedostačují. V této souvislosti bych ráda upozornila na tzv. úvěrové registry a jejich vztah k problematice ochrany osobních údajů. Pokud bychom si pořizovali úvěr od bankovní instituce, velmi často, v rámci smlouvy o úvěru, zároveň udělíme souhlas příslušné bankovní instituci k tomu, aby si dotazem v některém z úvěrových registrů ověřila, zda máme nějaké jiné půjčky, zda je splácíme a jak si vůbec vedeme celkově na finančním poli. Není snad ani třeba připomínat, že pokud bychom tento souhlas neposkytli, velmi pravděpodobně žádnou půjčku od dané bankovní instituce nezískáme. A na tomto místě vzniká prostor pro jednak tzv. nebankovní úvěrové společnosti, jednak pro nejrůznější typy úvěrových registrů. Zatímco první skupina společností si zakládá na tom, že poskytne úvěr žadateli, aniž by si ověřovala jeho platební disciplínu a schopnost v úvěrovém registru, druhá skupina společností profituje ze snahy nejrůznějších státních orgánů, institucí, právnických či fyzických osob zjistit, že jiná osoba je nebo není vedena

[118] Mnoho obyvatel Prahy bylo nuceno si tuto kartu pořídit s ohledem na to, že oblíbenou roční tramvajenku bylo možné pořídit výhradně v elektronické podobě. Viz. www.opencard.cz

[119] Tisková zpráva Úřadu pro ochranu osobních údajů ze dne 21. 10. 2009: „*Naopak úspěšná a konstruktivní byla jednání Úřadu s Dopravním podnikem hl. m. Prahy a společností Erika v souvislosti se zpracováním osobních údajů při využívání SMS jízdenek; projekt vyžadoval dobu uchování osobních údajů 10 let. Po vyjádření Ministerstva financí ČR a dalších konzultacích se ukázalo jako dostatečné uchovávání údajů po dobu 90 dní, které navrhl Dopravní podnik hl. m. Prahy.*“

v příslušném úvěrovém registru. Jak totiž plyne z označení, úvěrové registry by měly obsahovat informace výhradně o osobách, které nějaký úvěr mají / mají možnost dostat. Fungování úvěrových registrů je založeno výhradně na principu poskytování souhlasu se zpracováním osobních údajů, tedy se zařazením informací o své osobě do určitého registru (se kterým má banka nebo úvěrová společnost smlouvu). Nějaké detailnější právní úprava v této oblasti nicméně chybí.[120] A to se projevuje v několika problematických aspektech: málokdo si je skutečně přesně vědom, zda a jaké osobní údaje jsou o jeho osobě zpracovávány, v jakém úvěrovém registru a za jakých podmínek. Na druhé straně vznikla celá řada úvěrových registrů, a tak se může stát, že se daná instituce nebo osoba dotáže do nesprávného registru (respektive do jiného úvěrového registru) a získá mylnou informaci o platební schopnosti osoby, jíž hodlá poskytnout půjčku. Domnívám se, že by měla být přesněji dána pravidla fungování úvěrových registrů, jejich možnosti zpracovávat a uchovávat osobní údaje, zejména s ohledem na velkou možnost zneužití obsažených dat a jen mizivou možnost skutečné kontroly nad tím, jaké osobní údaje jsou v registru zpracovávány.[121]

3.3 Zpracování osobních údajů na bázi povinnosti

Jak již bylo osvětleno v úvodní kapitole této diplomové práce, za jistých okolností dochází ke zpracování našich osobních údajů, aniž bychom si toto uvědomovali, a to s ohledem na argument „ochrany veřejného zájmu“ nebo z jiných důvodů, jímž je přikládán větší, celospolečenský význam, který je prezentován jako nadřazený ochraně soukromí jednotlivců, včetně ochrany osobních údajů. Jak si ukážeme na příkladu evidence osobních údajů pasažérů cestujících do Spojených států amerických, může se dokonce jednat o zpracování osobních údajů především z veřejného zájmu jiného státu, než kterého je daný subjekt údajů občanem.

Obecně předpokládáme, že oblasti, kdy je poskytování našich osobních údajů povinné, jsou stanoveny obecně závazným právním předpisem, nejčastěji zákonem. Ne vždy tomu tak skutečně v plném rozsahu je, o čemž svědčí druhý uvedený příklad – zpracování osobních údajů studentů ze strany státních orgánů a samotných škol. Jako poslední je

[120] Problematiku právní úpravy bankovního tajemství v této souvislosti záměrně opomíjíme.
[121] Naprostá většina lidí se kupříkladu neuvědomuje, že pouhé vlastnictví tzv. kreditní karty (úvěrové karty) povede k registraci osobních údajů v příslušném registru ze strany banky.

uvedena problematika související s databází elektronických receptů (a tedy se zpracováváním citlivých osobních údajů o pacientech, respektive lidech užívajících léky).

3.3.1 Evidence osob cestujících letadly do a na území USA

V souvislosti se změněnou bezpečností situací ve Spojených státech amerických (USA) po tragických teroristických útocích v září roku 2001, administrativa Spojených států amerických přišla s požadavkem větší kontroly nad pohybem osob využívajících jako prostředek dopravy letadla, a to v případě osob cestujících do USA nebo v rámci jejich území. Problematickou situaci leteckých společností, které byly na jedné straně povinny dodržovat evropské požadavky na zpracování osobních údajů a na straně druhé byly tyto osobní údaje nuceny poskytovat pod hrozbou sankcí ze strany USA, mělo vyřešit uzavření mezinárodní smlouvy mezi Evropskými společenstvími a USA. První takováto dohoda uzavřená v roce 2004 byla v důsledku rozhodnutí Soudního dvora Evropských společenství ze dne 30. května 2006 (rozhodnutí C-317/04[122]), nicméně nikoliv z obsahových, ale formálních důvodů. Následně byly uzavřeny další dvě mezinárodní dohody, první dočasná a druhá trvalá, ze dne 26. července 2007, které nadále umožňují americkým úřadům přímo nahlížet do rezervačních systémů leteckých společností obsahujících celou škálu osobních údajů cestujících.

V této souvislosti je potřeba upozornit na několik zásadních skutečností. V prvé řadě je nutno upozornit, že v tomto případě nejde jen o „pouhé“ zpřístupnění osobních údajů cestujících (především občanů členských států EU), neboť tyto osobní údaje budou ze strany amerických orgánů *„uchovávány po dobu patnácti let a mohou být předávány dalším orgánům“*[123]. Údaje *„vztahující se ke konkrétnímu případu nebo vyšetřování lze uchovávat i déle, dokud případ nebo vyšetřování nejsou zarchivovány.“*[124] Zároveň není

[122] Spojené věci C-317/04 a C-318/04: Rozsudek Soudního dvora (velkého senátu) ze dne 30. května 2006 – Evropský parlament v. Rada Evropské unie (*„Rozhodnutí Rady 2004/496/ES ze dne 17. května 2004 o uzavření dohody mezi Evropským společenstvím a Spojenými státy americkými o zpracování a předávání údajů jmenné evidence cestujících (PNR) Úřadu pro cla a ochranu hranic ministerstva vnitřní bezpečnosti Spojených států a rozhodnutí Komise 2004/535/ES ze dne 14. května 2004 o odpovídající úrovni ochrany osobních údajů obsažených v záznamech o knihování cestujících v letecké dopravě, které se předávají Úřadu USA pro cla a ochranu hranic, se zrušují*“

[123] Stanovisko č.2/2007 k informování cestujících o předávání údajů jmenné evidence cestujících (PNR) orgánům Spojených států, Příloha 1.

[124] Tamtéž.

zcela jisté, zda všechny zpřístupňované osobní údaje skutečně americké orgány potřebují ve svém širokém rozsahu k tomu, aby naplňovaly svůj cíl – tedy zajištění bezpečnosti. Mezi příklady osobních údajů, které mají být předávány, patří: informace o platbě, objednání jídla nebo rezervace invalidního vozíku[125]. Dle tohoto stanoviska by cestující měli být informováni o tom, že by nemělo docházet k předávání jejich citlivých osobních údajů, a to za pomocí instalace automatického filtračního programu. Nicméně je otázkou, zda to mnohdy nejsou právě citlivé osobní údaje, které by americké státní orgány nejvíce zajímaly (např. údaje o náboženském vyznání či zdravotním stavu). Další zajímavou skutečností je, že některé z uvedených osobních údajů jsou americkým orgánům předávány již před přicestováním dané osoby do USA.

Poněkud problematické je rovněž stanovení doby, po kterou budou americké orgány zpřístupněné osobní údaje uchovávat. Přestože v citaci ze stanoviska uvedené výše je přesně stanovena tato doba na patnáct let, nelze vyloučit, že získané osobní údaje budou uchovávány po dobu ještě delší. Tyto úvahy nutně vyplývají přímo z textu mezinárodní dohody mezi USA a Evropskými společenstvími z roku 2007[126] „*DHS uchovává údaje EU PNR v aktivní analytické databázi po dobu sedmi let, po jejímž uplynutí budou údaje převedeny do nečinného, nepoužitelného stavu. Údaje v nečinném stavu budou uchovávány po dobu osmi let a přístup k nim lze získat pouze se schválením vysokého úředníka DHS určeného ministrem vnitřní bezpečnosti a pouze v reakci na konkrétní případ, hrozbu nebo riziko.* ***Očekáváme, že na konci tohoto období budou údaje EU PNR vymazány****; otázkou, zda a kdy zničit údaje PNR shromážděné v souladu s tímto dopisem se budou DHS a EU zabývat v rámci budoucích jednání*.“. Spojené státy se v této dohodě nezavazují po uplynutí doby 15 let osobní údaje zlikvidovat, ale pouze „očekávají“ tento postup.

V této souvislosti je ze strany Evropské unie zajímavá snaha sladit mezi různými správci údajů (nejčastěji leteckými společnostmi) postup, v jaké podobě a jakým způsobem by měli být o zpracování osobních údajů ve jmenné evidenci cestujících a jejím zpřístupnění orgánům USA informováni samotní cestující. V této souvislosti Pracovní skupina WP29

[125] Příloha 2 Stanoviska č.2/2007 k informování cestujících o předávání údajů jmenné evidence cestujících (PNR) orgánům Spojených států, s.2

[126] Rozhodnutí Rady 2007/551/SZBP/SVV ze dne 23. července 2007 o podpisu, jménem Evropské unie, Dohody mezi Evropskou unií a Spojenými státy americkými o zpracovávání údajů jmenné evidence cestujících (PNR) leteckými dopravci a o jejich předávání Ministerstvu vnitřní bezpečnosti Spojených států (Dohoda PNR 2007)

vydala v roce 2007 stanovisko, dle kterého by v roli správců osobních údajů, kteří mají povinnost informovat cestující, byly letecké společnosti, ale též cestovní kanceláře (které zprostředkovávají nákup letenky) nebo provozovatelé počítačových rezervačních systémů k nákupu letenek.[127] S ohledem na to, že „*se předávání údajů PNR [jmenná evidence cestujících] v praxi stalo podmínkou pro vycestování do Spojených států…*“[128] bylo doporučováno o tomto typu zpracování osobních údajů informovat cestující v souvislosti s koupí letenky a jejím následným potvrzením. Součástí tohoto stanoviska byly i vzorové informace, jakým způsobem bylo možné cestující informovat.

Na jedné straně zde tedy dochází ke střetu veřejného zájmu (zájmu na bezpečnosti občanů Spojených států amerických) a na straně druhé požadavkům na ochranu osobních údajů cestujících, a práva na jejich soukromí. Požadavky plynoucí z uzavřených mezinárodních dohod o předávání osobních údajů osob cestujících letecky do USA je potřeba vidět komplexně, ve světle dalších souvisejících opatření: (i) velké množství osob z jiných kontinentů se do USA přepravuje právě letecky, (ii) v případě České republiky existovala ještě do nedávné doby značná možnost americké administrativy ovlivnit možnost příjezdu osob na americké území formou vízové povinnosti a jistá omezení přetrvávají i po zrušení vízové povinnosti a (iii) kromě předávaných osobních údajů cestujících americké státní orgány pořizují záznamy biometrických osobních údajů (například otisk palce nebo informace o oku) osob vstupujících na území USA.[129] Ukazuje se, že Spojené státy americké mají přinejmenším možnost získávat osobní údaje velkého množství osob z jiných států a to bez skutečné možnosti ovlivnit nakládání takovými získanými osobními údaji. V případě osob, které do USA cestují kupříkladu z pracovních důvodů, neexistuje skutečná možnost se poskytování a předávání svých osobních údajů vyhnout.

3.3.2 Zpracování osobních údajů studentů škol

Ochrana osobních údajů studentů je další oblastí, která je již delší dobu diskutována a ve které se objevují nové a nové nejasné otázky a problémy. V souvislosti se vzrůstajícími problémy s chováním některých studentů (a s problémy takové chování zvládat ze strany

[127] Stanovisko č.2/2007k informování cestujících o předávání údajů jmenné evidence cestujících (PNR) orgánům Spojených států
[128] Tamtéž, s. 5
[129] Úřad pro ochranu osobních údajů. *Kde jsou hranice nových možností biometriky*?

učitelů) se objevily občasné snahy zavádět do škol namátkové kontroly požití návykových látek studenty.[130]

Posléze, v souvislosti obecným fenoménem rozvoje kamerových systémů, se ukázala snaha zavést monitorovací systémy nejen na chodby škol, ale následně i do tříd, a to nejen během přestávek mezi vyučovacími hodinami, ale i během samotné výuky.[131]

V této souvislosti se objevuje hned několik problematických aspektů těchto forem zpracování osobních údajů – ani jeden z uvedených způsobů zásahů do soukromí studentů není podřazen pod zákonnou výjimku, kdy by bylo možné zpracovávat osobní údaje studentů, bez jejich souhlasu (respektive bez souhlasu jejich zákonných zástupců). Školy jsou si této skutečnosti zpravidla vědomy a postupují formou generálních nebo ad hoc souhlasů zákonných zástupců studentů. Nicméně již není zcela jasné, zda v případě uchovávání získaných osobních údajů, splňují další povinnosti, kterým jako správci osobních údajů podléhají. Takové školy by měly zcela jasné uvádět, jaké osobní údaje, v jakém rozsahu a jakým způsobem zpracovávají. Praxe není v tomto směru jednotná, a tak existují školy, které používají kamerové systémy, z nichž nejsou pořizovány záznamy, ale i školy, které záznamy ze systémů uchovávají jeden den nebo až dva týdny.[132] V tomto směru není zcela jasné, zda takové školy své studenty a jejich zákonné zástupce dostatečným způsobem informují nejen o samotném zpracování osobních údajů, ale také o jejich právech, které vyplývají ze Zákona (včetně práva být informován o tom, jaké osobní údaje jsou o osobě daného studenta zpracovávány, a práva obrátit se v případě pochybností na Úřad).

V současné do médií rovněž pronikly informace o databázích, které jsou o studentech vedeny státními orgány a o kterých studenti zpravidla mají jen velmi malé a zkreslené údaje. Dle informací uveřejněných v Hospodářských novinách v článku „*Ministerstvo toho ví o studentech až příliš*“ existují o všech studentech (tedy o studentech od základní až po vysoké školy) dvě základní databáze – první obsahuje informace o studentech vysokých škol, druhá o zbylé skupině studentů. V této souvislosti vznikly pochybnosti

[130] Více viz. Mladá fronta Dnes. Školy získají testy na drogy, rodiče musí se zkouškou souhlasit ze dne 27.4.2009
[131] Více viz. KOTEK, P. Kamerové systémy používá 28 procent škol, některé porušují práva žáků a studentů ze dne 10.11.2009
[132] Tamtéž.

jednak o rozsahu zpracovávaných osobních údajů a také o způsobu jejich zpracování, respektive o možnosti jejich zneužití ke komerčním účelům. Osobní údaje studentů jsou v těchto databázích údajně evidovány na podkladě rodného čísla, jako klíčového identifikátoru.[133] Domnívám se, že navzdory skutečnosti, že rozsah osobních údajů (v případě studentů jiných než vysokých škol) je stanoven právním předpisem (konkrétně vyhláškou č. 364/2005 Sb. o vedení dokumentace škol a školských zařízení a školní matriky o předávání údajů z dokumentace škol) a nevyžaduje tedy souhlas se zpracováním osobních údajů studentů, měli by studenti (popřípadě zákonní zástupci studentů) být o rozsahu a způsobu zpracování osobních údajů informováni – není totiž zcela jasné, zda rozsah a způsoby zpracování osobních údajů poskytují dostatečné záruky ochrany poskytovaných osobních údajů před zneužitím. Dále není zcela jasné, z jakého důvodu jsou kupříkladu požadovány informace o způsobu financování studia daného studenta nebo není zcela jisté, že anonymizované osobní údaje o zdravotním stavu (a zdravotním postižení) studenta není možné nějakým způsobem propojit a identifikovat tak osobu konkrétního studenta.

V souvislosti se zaváděním kamerových systémů do škol a s opatřováním souhlasu k takové formě zpracování osobních údajů se nabízí další zajímavá teoretická otázka – totiž otázka zda u studentů, jejichž věk nedosahuje 18 let, ale již nejde o malé děti, mohou souhlas poskytnout výhradně rodiče (zákonní zástupci) studenta anebo zda již může takový souhlas (ne)poskytnout student sám. Dle § 9 občanského zákoníku mají nezletilí způsobilost jen k takovým právním úkonům, které jsou svojí povahou přiměřené rozumové a volní vyspělosti odpovídající jejich věku. Je nepochybné, že poskytnutí (či odmítnutí poskytnutí) souhlasu ke zpracování osobních údajů je právním úkonem ve smyslu zákona.[134] Můžeme si klást otázku, zda takový téměř dospělý (zletilý) student stále není oprávněn souhlas ke zpracování osobních údajů formou pořizování záznamů z kamerového systému udělit, zvláště když si uvědomíme, že stejně starý student si může zřídit přístup do nejrůznějších internetových sociálních sítí (včetně poskytnutí souhlasu se zpracováním osobních údajů) nebo může uzavírat nejrůznější kupní smlouvy, nebo (za splnění určitých podmínek) může být účastníkem silničního provozu. Zvláště pikantní

[133] Rodné číslo je velmi často používáno jako velmi oblíbeného identifikátor fyzických osob, a to nejen ze strany státních institucí. Takový způsob zpracování osobních údajů je nicméně často a oprávněně velmi kritizován, neboť existují obavy z možného propojování databází a jejich zneužívání.
[134] Právním úkonem je projev vůle směřující zejména ke vzniku, změně nebo zániku těch práv nebo povinností, které právní předpisy s takovým projevem spojují (§ 34 občanského zákoníku).

příchuť tato otázka dostává v momentě, kdy si představíme střet zájmů zákonného zástupce studenta a rodiče. Lze si velmi snadno představit situaci, kdy kupříkladu rodič bude stále mít zájem, aby jeho takřka zletilé dítko bylo podrobováno testům na požití návykových látek nebo prostě, aby bylo snímáno během výuky kamerovým systémem (čímž by si mohl ověřovat jeho fyzickou přítomnost na výuce) a zcela opačné mínění studenta. V těchto případech se zdá být na první pohled zcela nepochybné, že souhlas se zpracováním osobních údajů je, až do dosažení zletilosti, oprávněn udělit pouze zákonný zástupce. Ale je tomu skutečně tak?

3.3.3 Státní ústav pro kontrolu léčiv a Centrální úložiště receptů

Další aktuálně sledovaný případ v souvislosti s ochranou osobních údajů se dotýká provozování tzv. Centrálního úložiště elektronických receptů – tedy elektronického systému (databáze) provozovaného Státním ústavem pro kontrolu léčiv (dále jen „**SÚKL**“), ve kterém jsou shromažďovány a zpracovávány osobní údaje velmi citlivé povahy.

Zákon o léčivech č. 378/2007 Sb. § 13, odst. 3, písm. n) stanoví, že SÚKL „*zřizuje a provozuje centrální datové úložiště pro sběr a zpracování elektronicky předepisovaných léčivých přípravků* (dále jen "centrální úložiště elektronických receptů")“. Smyslem zprovoznění uvedené databáze bylo, podle zahraničních vzorů, usnadnit komunikaci mezi lékaři, lékárnami a pacienty a přispět tak, kromě jiného, k efektivnějšímu využívání léků na elektronický předpis. Z § 80 zákona o léčivech plyne, že lékař může po dohodě s pacientem vydat předpis na lék (recept) jak v „klasické“ listinné podobě, tak v elektronické podobě (označovaný jako „**elektronický recept**“). Tyto elektronické recepty by měly být předávány elektronickou cestou do centrálního úložiště elektronických receptů (dále jen „**centrální úložiště**“), odkud by měl být daný elektronický recept zpřístupněn k nahlédnutí příslušné lékárně (elektronický recept je opatřen tzv. identifikačním znakem, který sdělí lékař pacientovi a kterým se pacient v lékárně „přihlásí“ ke svému receptu). Na podkladě uvedeného pak lékárna pacientovi předepsaný lék vydá a provede o tom záznam v centrálním úložišti.

Z podstaty věci je zřejmé, že jak v elektronickém receptu, tak v centrálním úložišti jsou zpracovávány, shromažďovány a zpřístupňovány citlivé osobní údaje osob – pacientů.

Konkrétně jsou předmětem evidence tyto osobní údaje: *jméno, příjmení, datum narození, označení zdravotní pojišťovny, označení diagnózy, identifikace léčivého přípravku předepsaného a vydaného pacientovi.*[135] Podobně rozporné reakce budí další evidence SÚKL v souvislosti s vydáváním léčivých přípravků obsahujících pseudoefedrin – dle stávající úpravy je možné zakoupit léky obsahující tuto látku jen v omezeném množství, a po registraci osobních údajů a údajů o zakoupeném léčivu a jeho množství v elektronickém systému.[136]

Jde tedy především o citlivé osobní údaje o zdravotním stavu. Povinnosti SÚKL v souvislosti s provozováním centrálního úložiště jsou uvedeny v § 81 zákona o léčivech a pod písmenem e) je SÚKL uloženo „*zajistit ochranu a bezpečnost v databázi uložených elektronických receptů před jejich poškozením, zneužitím a ztrátou podle Zákona na ochranu osobních údajů.*“ Již od počátku přípravy spuštění tohoto nového systému vyvstávaly otázky, zda a jak bude zajištěno, že uvedené citlivé osobní údaje budou dostatečně chráněny před neoprávněným nakládáním. Jako spornou se ukázala otázka, zda je vůbec a z jakého titulu SÚKL (respektive jeho zaměstnanci) oprávněn zpracovávat citlivé osobní údaje – údaje o zdravotním stavu a léčbě pacienta (a nahlížet tak do zdravotnické dokumentace).[137] V této souvislosti bylo naznačeno, že povinnostem kladeným na lékárny v souvislosti s hlášením vydání léčivých přípravků na elektronický recept by bylo možné učinit za dost i v anonymizované podobě, tedy aniž by byly do centrálního úložiště zasílány informace umožňující identifikovat pacienty. Jedním z velmi kritizovaných prvků tohoto systému bylo i to, že osobní údaje, které jsou při evidenci vydaných receptů ukládány do centrálního úložiště, jsou stanoveny informačním pokynem SÚKL[138] – tedy nikoliv zákonem a navíc se tato požadovaná data mohou měnit. Na jednu stranu je pochopitelné, že SÚKL zabezpečuje velmi důležité úkoly, zejména v souvislosti s ochranou zdraví pacientů užívajících léčivé přípravky (zejména s ohledem na monitoring a hlášení nežádoucích účinků), nicméně je potřebné, aby byla zabezpečena ochrana osobních údajů v dostatečné míře. Domnívám se, že pouhý odkaz na to, že s danými osobními údaji je nakládáno v souladu se zákonem na ochranu

[135] § 6 a § 7 Vyhlášky č. 54/2008 Sb. o způsobu předepisování léčivých přípravků, údajích uváděných na lékařském předpisu a o pravidlech používání lékařských předpisů
[136] Toto opatření je platné, dle tiskové zprávy Státního ústavu pro kontrolu léčiv ze dne 23.3.2009 uveřejněného na internetových stránkách SÚKL, počínaje 1.5.2009.
[137] Dopis České lékařské komory ze dne 21.4.2009 řediteli SÚKL, panu PharmDr. Martinu Benešovi na stránkách SÚKL (www.sukl.cz), sekce Komunikace s médii.
[138] § 82, odst. 3, písm. d) zákona o léčivech

osobních údajů, není postačující, vzhledem k tomu, že jde o osobní údaje pacientů a jiných fyzických osob. Tyto osoby, jakožto subjekty údajů by měly být přesně informovány o tom, s jakými osobními údaji a jak je v uvedených souvislostech nakládáno, a to výslovně. Na internetových stránkách SÚKL se nicméně pacient tyto informace nedozví, není informován ani o tom, na koho se v této souvislosti má obrátit.

Podobně se ukázalo, že není zcela jasné, jak naložit s citlivými osobními údaji pacienta v případě vydávání léčiv s omezením (tedy léčivých přípravků zpravidla s obsahem pseudoefedrynu), když se uvažovalo nad zavedením on-line systému monitorujícího vydávání konkrétního léčivého přípravku konkrétním osobám.[139] Podle informací SÚKL, které adresoval lékárnám ve svém sdělení ze dne 5.8.2009, bylo provedeno kontrolní šetření ze strany Úřadu a SÚKL byl předán kontrolní protokol, vůči kterému je možné se bránit námitkami. Jak bylo zdůrazněno, Úřad se zaměřil na kontrolu nakládání osobními údaji v SÚKL, v této souvislosti nevydal ani žádné rozhodnutí. Přestože uvedený kontrolní protokol nebyl zveřejněn, „*v rámci kontroly Centrálního úložiště receptů bylo zjištěno, že SÚKL koná nad rámec pravomocí ukládaných mu zákonem a v rozporu se zákonem o ochraně osobních údajů.*“[140] Na tiskové konferenci Úřadu dne 21. října 2009 bylo potvrzeno, že „*kontrola zjistila, že vydávání elektronických předpisů, jejichž zavedení bylo důvodem pro zřízení centrálního úložiště, dosud nebylo zahájeno, nicméně že SÚKL v rámci centrálního úložiště zpracovává osobní údaje získané z jednotlivých lékáren prostřednictvím hlášení o lécích vydaných na základě písemného předpisu a o výdeji léků, které se vydávají bez předpisu, ale vztahuje se na ně omezení, co do množství účinné látky vydané jedné osobě v rámci určité doby. Kontrola konstatovala, že k uvedenému shromažďování osobních údajů nemá SÚKL žádné zákonné zmocnění, které je - zejména s ohledem na zpracování citlivých údajů - nezbytným předpokladem. Znamená to, že SÚKL nadále tyto údaje nesmí shromažďovat a takto pořízené osobní údaje je povinen smazat. Námitkám vzneseným SÚKL proti kontrolnímu protokolu předseda Úřadu nevyhověl.*“[141] V návaznosti na šetření a zjištění Úřadu byl SÚKL nucen

[139] Žádost o posouzení souladu zpracování citlivých osobních údajů se zákonem adresované ze stravy Grémia majitelů lékáren Úřadu, ze dne 20. Listopadu 2008
[140] Tisková zpráva Úřadu ze dne 4. srpna 2009 dostupná na http://www.uoou.cz/uoou.aspx?menu=15
[141] Tisková zpráva Úřadu ze dne 21. října 2009 dostupná na http://www.uoou.cz/uoou.aspx?menu=15&loc=651

přistoupit k likvidaci získaných osobních údajů a změnit podmínky pro prodej léčivých přípravků s omezením.[142]

I v tomto případě můžeme vidět střet zájmu veřejného a zájmu na ochranu osobních údajů, tedy práva na soukromí. Zastánci provozování dotčené databáze SÚKL argumentují tím, že je zde potřeba monitorovat veškeré léky, které daný pacient užívá na základě lékařského předpisu a předcházet tak nebezpečí z možných nežádoucích interakcí léků současně užívaných. Dalším argumentem je volání po omezení zbytečně předepisovaných léků. Můžeme se tedy ptát, pokud dotčený systém měl evidovat léky vydávané na předpis – jaká je možnost, že zmiňované nežádoucí interakci způsobí léky, které si pacient opatří bez předpisu v rámci volného prodeje[143]?

V současné době se také začalo hovořit o modernizaci a spolupráci lékařů v rámci implementace elektronického propojení pracovišť lékařů a zavádění elektronicky vedené zdravotní dokumentaci.[144] V tomto případě bychom se mohli ptát, proč by měl SÚKL shromažďovat osobní údaje pacientů, když nahlédnutím do záznamů pacienta by možné riziko z interakcí léků mohl odstranit sám lékař? Domnívám se, že na místě jsou rovněž obavy z toho, že pokud už jednou dojde k oprávněnému vytvoření a provozování podobných databází, bude velmi obtížné přesvědčit provozovatele jiných souvisejících databází o jejich zrušení, nebo omezení. Kromě toho není zcela jasné, zda by zde neměl být nastaven daleko přísnější režim kontroly nakládání takovými zpracovávanými citlivými osobními údaji, když jde o centrální databázi obsahující velmi citlivé osobní údaje, o jejímž fungování samotní pacienti (subjekty údajů) nemají dostatek informací.

[142] Tisková zpráva SÚKL ze dne 21. října 2009 dostupná na http://www.sukl.cz/tiskova-zprave-ze-dne-21-10-2009 a Tisková zpráva SÚKL ze dne 21. října 2009 II. dostupná na http://www.sukl.cz/uploads/TIO/TZ_21.10.2009/TZ_Meni_se_zpusob_vydeje_PSE_1021_final_verze_MZ.pdf

[143] Je zcela jasné, že z hlediska svých účinků jsou léky předepisované na recept v porovnání s léky volně prodejnými daleko nebezpečnější. Nicméně nelze opomenout ani onu hypotetickou možnost, že k interakcím může docházet i u volně prodejných léků.

[144] Například tzv. Elektronická zdravotní knížka. Více informací viz. http://www.izip.cz/

Závěr

Na závěr této diplomové práce můžeme shrnout, že otázka ochrany osobních údajů je velmi úzce spjata se základními lidskými právy – s ochranou soukromí a rodinného života.

Kořeny právního zakotvení ochrany osobních údajů nacházíme v celé řadě mezinárodních právních dokumentů různé právní síly a různého zaměření – počínaje Všeobecnou deklarací základních lidských práv a svobod a Evropskou úmluvou o ochraně lidských práv a svobod počínaje, a konče specifickými dokumenty věnujícími se již přímo a výhradě ochraně osobních údajů – zejména Úmluvou na ochranu osob se zřetelem na automatické zpracování osobních dat a evropskou směrnicí z roku 1995 konče. Přestože o lidsko-právních kořenech ochrany osobních údajů nejsou pochyby, dochází v současné době stále častěji ke střetu tohoto práva s jinými druhy lidských práv a zejména s právy, která mají chránit většinovou společnosti (oproti právům zaměřeným na ochranu jednotlivce). Otázka, která lidská práva a zda vůbec mají přednost před právem na ochranu osobních údajů, není stále zodpovězena a zůstává výzvou do budoucnosti.

Právní základy úpravy ochrany osobních údajů v českém právním řádu koncentruje především zákon o ochraně osobních údajů. Vedle tohoto zákona existuje celá řada právních předpisů, které se ve své dílčí části věnují rovněž problematice ochrany osobních údajů. S ohledem na členství České republiky v Evropské unii je nutné zohledňovat též evropské normy v oblasti ochrany osobních údajů – zejména Směrnici (ang. označovanou jako „*Data Protection Directive*“). Současný text zákona o ochraně osobních údajů z velké části přebírá formulace užité ve Směrnici.

Na tomto místě je potřeba podotknout, že text Směrnice se od roku 1995, kdy byla přijata, příliš nezměnil. Vzhledem k rostoucí mezeře mezi současnou praxí v oblasti ochrany osobních údajů a právní úpravou se stále častěji objevují požadavky na revizi Směrnice (tomuto tématu se věnuje například dokument nazvaný „*Review of the Data Protection Directive*“ – tedy „Revize Směrnice o ochraně osobních údajů“ z května

2009). Přestože obecně řečeno bývá evropský přístup k problematice ochrany osobních údajů hodnocen lépe než americký, objevují, dle mého názoru, se v souvislosti s revizí některé návrhy zavádět prvky typické pro americký systém, jako odklon od principu oznamovacího. Přestože celkově nemůžeme popřít, že současná právní úprava je v mnoha ohledech nedostatečná a nevyhovující, nelze proces revize právní úpravy v této oblasti naprosto obrátit a stavět na úplně nových základech. Další otázkou, kterou si v této souvislosti musíme položit je, zda v současné době vůbec existuje prostor pro jakoukoliv zásadnější změnu úpravy a zda se nemůže naopak stát, že namísto zefektivnění ochrany subjektu údajů, jakožto slabší strany, bude situace využita k prosazení větší míry kontroly nad občany jednotlivých států (například ve jménu boje proti zločinu a terorismu). Na tomto místě si dovolím připomenout, že právě tato hesla stála v pozadí dohod, na jejichž podkladě dochází k předávání osobních údajů osob cestujících letadly do Spojených států amerických. O tom, že tu existuje snaha tato „politická témata“ využít k monitoringu osob svědčí i námitky Úřadu pro ochranu osobních údajů k tzv. *SWIFT Agreement*, na jejímž vyjednávání se podílí za Českou republiku ministerstvo financí.[145]

Právní rámec oblasti ochrany osobních údajů se vyznačuje specifickým pojmoslovím a právní úpravou, která by měla být natolik obecná, aby mohla být aplikována v stávajícím, stále se rozvíjejícím světě moderních technologií a rostoucí výměny informací. Ústředním pojmem jsou osobní údaj (informace vztahující se k určitelné fyzické osobě) a subjekt údajů (fyzická osoba, jíž se zpracování osobních údajů týká). Osobní údaje mohou být členěny z celé řady pohledů, nicméně zvláštní kategorii mezi osobními údaji představují osobní údaje citlivé. V případě citlivých osobních údajů nejde o „citlivost“ vnímanou subjektivně konkrétním subjektem údajů, ale o kategorii taxativně vymezenou zákonem. Termín zpracování osobních údajů označuje nejrůznější způsoby nakládání a operací s osobními údaji konkrétních fyzických osob a v obecné rovině téměř vždy vyžaduje souhlas ze strany dotčeného subjektu údajů. Mezi osoby, které operace zpracování osobních údajů provádějí, patří nejčastěji správce osobních údajů (osoba, která určuje účel, pro který osobní údaje zpracovává) a zpracovatel osobních údajů (osoba odlišná od správce, která mu v určité rovině se zpracováním osobních údajů

[145] Informace o námitkách Úřadu pro ochranu osobních údajů je možné najít na webových stránkách Úřadu na adrese: http://www.uoou.cz/uoou.aspx?menu=14&loc=328 (článek nazvaný Zásadní námitky ke „Swift agreement“ uplatněné vůči gestorovi - MF - v průběhu sjednávání ze dne 3. prosince 2009

pomáhá, a to na základě smluvního vztahu). Nicméně musíme podotknout, že daleko častější jsou situace, kdy jedna a tatáž osoba vystupuje v obou zmíněných pozicích.

Při ochraně osobních údajů se uplatňuje celá řada principů – zásad ochrany osobních údajů. Mezi tři nejzákladnější patří (i) princip informovanosti o zpracování osobních údajů, (ii) informování o právech subjektů údajů v souvislosti se zpracováním osobních údajů a možnosti tato práva realizovat a (iii) právo na ochranu poskytnutých osobních údajů před jejich zneužitím. Některé z těchto principů jsou výslovně zmíněny, jiné z právních předpisů vyplývají implicitně. Základním stavebním prvkem, na kterém je právní úprava ochrany osobních údajů postavena, je souhlas subjektu údaje s jejich zpracováváním. Ukazuje se, že osoby zpracovávající osobní údaje směšují požadavky na získávání souhlasu s povinností o zpracování osobních údajů informovat formou podání oznámení. Jak již bylo zmíněno, terminologie používaná Zákonem je mnohdy pro laiky natolik nejasná, že dává prostor pro nejrůznější formy výkladu, často na úkor subjektů údajů.

Na realizaci práva na ochranu osobních údajů se podílejí instituce na národní úrovni (Úřad pro ochranu osobních údajů v případě České republiky), instituce evropské (Evropská komise, Evropský inspektor ochrany údajů) či mezinárodní (mezivládní či mezinárodní organizace nebo nevládní organizace). S ohledem na probíhající procesy globalizace se můžeme stále častěji setkat s tím, že aktivity správce osobních údajů jsou mezinárodní (občas doslova globální). Takové aktivity je poměrně těžké sledovat, právě proto, že národní dozorové orgány se zpravidla více věnují „domácím“ problémům, a už méně těm zahraničním. Právě zde, dle mého názoru, vzniká prostor pro působení různých nadnárodních organizací, které prostřednictvím internetu takovéto aktivity monitorují a upozorňují na ně. Svojí činností tak přispívají nejen k informovanosti široké veřejnosti o potenciálních rizicích, ale usnadňují i činnost dozorovým orgánům. V rámci požadavků na revizi právní úpravy bylo zmíněno, že je potřeba, aby formalizované dozorové orgány spolupracovaly přímo s adresáty právní úpravy na ochranu osobních údajů – se správci, zpracovateli i subjekty údajů. Návrh aktivizovat veřejnost, spolupracovat s nevládními organizacemi a sdruženími (jako jsou profesní svazy a spotřebitelské organizace) je, dle mého názoru, správnou cestou k přiblížení právní úpravy skutečnému životu.

Zmíněné mezinárodní aktivity správců osobních údajů jsou velmi často úzce spjaty s problematikou předávání osobních údajů do zahraničí – tedy situací, kdy osobní údaje „putují“ od správce osobního údaje v jednom státě k příjemci těchto údajů ve státě jiném. Z hlediska terminologie zařadíme předávání osobních údajů mezi formy zpracování osobních údajů. Přestože zde mohou existovat obavy z takového předávání osobních údajů do zahraničí, nelze tyto činnosti úplně eliminovat, zejména z hospodářských důvodů. Realizace mezinárodního obchodu je z velké části neoddělitelně spjata s předáváním osobních údajů do zahraničí. Z tohoto důvodu byla hledána cesta, jakým způsobem umožnit předávání osobních údajů do zahraničí a zároveň zabezpečit, že tato data nebudou zneužita. Díky implementaci Směrnici nevznikají problémy při intra-komunitárním pohybu osobních údajů, ale jak je tomu v případě pohybu osobních údajů ven z EU? Současná právní úprava nabízí hned několik možností, které lze pro předávání osobních údajů vně Evropské unie zvolit.

Jako první je možné zmínit předávání na základě rozhodnutí Evropské komise, které je vydáváno na základě detailního posuzování záruk, které skýtá daný právní řád k ochraně osobních údajů. Na této bázi je možné předávat osobní údaje na britský ostrov Guernsey či do Kanady.

Velmi oblíbeným způsobem je též začlenění tzv. „standardních smluvních doložek“ do smlouvy nebo uzavření samostatné smlouvy o předávání osobních údajů. V souvislosti se standardními smluvními doložkami je možné upozornit na zajímavý teoretický problém, který prozatím není uspokojivě řešen – a totiž na smluvní ukotvování vztahů správce – správce, správce – zpracovatel a dokonce zpracovatel-zpracovatel. Přestože není možné pochybovat o tom, že praxe všechny tyto typy vztahů zná (a že dochází mezi osobami v takovémto postavení k výměně osobních údajů), zejména česká právní úprava na toto dostatečně nereflektuje. Dle mého názoru je možné některé diskrepance překonat extensivním výkladem, nicméně je evidentní, že jde i zde prostor pro změnu právní úpravy.

Jako další, velmi zajímavou metodu jsme si představili Zásady bezpečného přístavu. Jde o formu, která je založena na vůli a ochotě společností ze Spojených států amerických poskytnout záruky odpovídající těm evropským (za účelem umožnění vývozu osobních údajů z EU do USA). V tomto nástroji pro předávání osobních údajů do USA se zrcadlí,

do jisté míry princip americké volnosti a svobody – jde totiž o systém založený na dobrovolnosti a „sebe-regulace“. Právě z této jeho charakteristické vlastnosti vyplývají i rizika – skutečná míra dodržování těchto pravidel a jejich vymahatelnost. Dalším problémem je i jejich omezení jen na některé druhy společností.

Poměrně specifickým nástrojem, který není v České republice příliš rozšířen, jsou Závazná podniková pravidla, jako nástroj intra-skupinového předávání osobních údajů. Podobně, jako v případě Zásad bezpečného přístavu, je tento systém do určité míry charakterizován „sebe-regulací“. Tyto zásady si z velké části vytvářejí samotné společnosti a jsou jim doslova „šité na míru“. Odlišností od amerického modelu je prvek dozoru – pravidla podléhají konzultacím a schvalování některým z národních orgánů dozoru a jsou i striktně vymahatelná. Přesto jde stále o nástroj poměrně málo rozšířený. To nicméně neznamená, že do budoucna nemůžeme očekávat větší použití tohoto instrumentu (v rámci revize Směrnice se dokonce ozývají volání, že tato cesta je ta správná).

Poslední variantu představuje předávání osobních údajů na principu povolení Úřadu pro ochranu osobních údajů. Jak již bylo zmíněno, jde o poměrně silný nástroj Úřadu, kterým může omezovat předávání osobních údajů do třetích států. Na tomto místě je možné podotknout, že český Úřad má v Evropě dobrou a poměrně přísnou pověst. Při posuzování, zda Úřad takové předávání povolí či nikoliv posuzuje celou řadu kritérií. S ohledem na výše uvedené proto nebude překvapením, že na poskytnutí povolení k předávání osobních údajů do zahraničí není právní nárok.

Poslední část této diplomové práce představila několik málo příkladů, které byly v nedávné době diskutovány veřejností v souvislosti s ochranou osobních údajů. Z uvedených aktuálních otázek můžeme potvrdit, že ke zpracování našich osobních údajů dochází stále častěji. Na jedné straně, zdá se vzniká nebezpečný trend upřednostňovat veřejné zájmy (a zájmy státu) před zájmem jednotlivců a před jejich lidskými právy. Na druhé straně je význam pojmů „soukromí“ a „ochrany osobních údajů“ snižován dobrovolnou aktivitou samotných subjektů údajů. V této souvislosti si můžeme klást nové otázky – můžeme se spoléhat na uvědomění a rozum subjektů údajů, na jejich schopnost správně hodnotit rizika spojená s poskytováním osobních údajů, nebo zde vzniká potřeba zásahů státu v podobě přísnější regulace, která by měla tyto lidi chránit

před jimi-samými? Ve světle obav z terorismu, které jsou stále diskutovány, totiž vzniká nejen prostor pro zneužití osobních údajů jinými osobami. Můžeme se ptát, zda do určité míry není takovéto oslabení ochrany osobních údajů pro stát v některých aspektech výhodné. Na tyto otázky není lehké odpovědět. Taková odpověď totiž bude závislá na okolnostech, na politické situaci i na tom, zájmy které skupiny jsou upřednostňovány. Vzhledem k stále rostoucímu technologickému rozvoji není pochyb o tom, že na tyto otázky časem bude dána odpověď.

Na závěr si dovolím vyslovit přání, aby se lidé více zajímali o to, co se s jejich osobními údaji děje, komu je dávají k dispozici a především, aby se nebáli svá práva hájit. Můžeme doufat, že budoucnost přinese změny k lepšímu i v této právní oblasti a na otázku, kterou jsme zmínili v úvodu této práce - *Je dnes ještě možné tvrdit, že ochrana osobních údajů je stále důležitá* – budeme moci dál odpovídat: *Ano je a i nadále bude*.

Seznam použité literatury

- **Literatura klasická i dostupná na internetu**

1. COMMISSION OF THE EUROPEAN COMMUNITIES. *Commission Staff Working Document - The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce SEC(2004)1323*. 20.10.2004. Dostupné na *http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm* [cit. dne19.9. 2009]

2. COMMISSION OF THE EUROPEAN COMMUNITIES. *Commission Start Working Paper. The application of the Commission decision 520/2000/EC of 26 July 2000 pursuant to the Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Policy Principles and Related Frequently Asked Queastions issued by the US Department of Commerce 14.2.2002.* Dostupné na *http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm* [cit. dne19.9. 2009]

3. CONOLLY, CHRIS. *The US Safe Harbor – Fact or fiction (2008).* Galexia. 12.12.2008 Dostupné na http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf [cit. dne19.9. 2009]

4. COUNCIL OF EUROPE. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; CETS No.: 108; Status as of: 15/2/2009.* Dostupné na: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=8&DF=2/15/2009&CL=ENG [cit. dne: 5.2.2009]

5. ČLÁNEK 29 - PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Stanovisko č.2/2007 k informování cestujících o předávání údajů jmenné evidence cestujících (PNR) orgánům Spojených států*. Dostupné na http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_en.htm [cit. dne: 24.10.2009]

6. ELECTRONIC PRIVACY INFORMATION CENTER. *Social Networking Privacy.* Dostupné na http://epic.org/privacy/socialnet/ cit. dne: 24.8.2009]

7. EUROPEAN COMMISSION, DG FREEDOM, JUSTICE AND SECURITY. *Tasks of the Article 29 Data Protection Working Party* dostupné na http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/tasks-art-29_en.pdf [cit. dne: 24.8.2009]

8. EUROPEAN COURT OF HUMAN RIGHTS. *Key case law-issues. The concepts of „private and family life“* ze dne 24.ledna 2007, dostupné na: http://www.echr.coe.int/NR/rdonlyres/F6DC7D2E-1668-491E-817A-

D0E29F094E14/0/COURT_n1883413_v1_Key_caselaw_issues__Art_8__The_Concepts_of_Private_and_Family_Life.pdf [cit. dne: 5.2.2009]

9. EUROPEAN COURT OF HUMAN RIGHTS. *Key case law-issues. The concepts of „home and correspondence“* ze dne 31. ledna 2007, dostupné na: http://www.echr.coe.int/NR/rdonlyres/F6DC7D2E-1668-491E-817A-D0E29F094E14/0/COURT_n1883413_v1_Key_caselaw_issues__Art_8__The_Concepts_of_Private_and_Family_Life.pdf [cit. dne: 5.2.2009]

10. FOLDA, J. *Nejste náhodou terorista?* Článek z července 2007 uveřejněný na http://www.uoou.cz/uoou.aspx?menu=287&submenu=288&loc=324 [cit. dne: 15.10.2009]

11. HOSPODÁŘSKÉ NOVINY. WEIKERT, P. *Ministerstvo toho ví o studentech až příliš.* 2.9.2009 Dostupné na http://hn.ihned.cz/c1-38199590-ministerstvo-toho-vi-o-studentech-az-prilis [cit. dne: 16.11.2009]

12. *Hyatt signs up to EU binding corporate rules for data transfers*. Dostupné na http://www.theregister.co.uk/2009/09/22/hyatt_bcr/ [cit. dne: 20.11.2009]

13. KRŮPA, B. *Regulace ochrany osobních údajů v právu EU*. Diplomová práce. Právnická fakulta Masarykovy university. Katedra mezinárodního a evropského práva. 2006/2007.

14. KUČEROVÁ A., BARTÍK V., PECA J., NEWIRT K., NEJEDLÝ J., *Zákon o ochraně osobních údajů. Komentář.* 1.vyd., Praha: C.H. Beck, 2003

15. KUNER, Ch. a kol.. *ICC report on binding corporate rules for international transfer of personal data.* International Chamber of Commerce, Paris, 24.10.2004 dostupné na http://www.iccwbo.org/id5108/index.html [cit. dne: 5.2.2009]

16. LEWIS, N. Right for privacy in the age of Facebook. http://www.spiked-online.com/index.php/site/article/7686/ [cit. dne: 24.11.2009]

17. MATOUŠOVÁ M., HEJLÍK L., *Osobní údaje a jejich ochrana.* 2. vyd., Praha, ASPI, Wolters Kluwer, 2008

18. MLADÁ FRONTA DNES. *Školy získají testy na drogy, rodiče musí se zkouškou souhlasit*. 27.4.2009. Dostupné na http://zpravy.idnes.cz/skoly-ziskaji-testy-na-drogy-se-zkouskou-musi-rodice-souhlasit-pwo-/brno.asp?c=A090427_192112_brno_dmk [cit. dne: 16.11.2009]

19. OECD. *Privacy and Personal Data Protection*. Dostupné na http://www.oecd.org/dataoecd/30/32/37626097.pdf [cit. dne: 24.8.2009]

20. PALEKAR, N.S. *Privacy Protection“ When is „adequate actually adequate?* Dostupné na http://www.law.duke.edu/shell/cite.pl?18+Duke+J.+Comp.+&+Int'l+L.+549 [cit. dne: 5.2.2009]

21. PAN AMERICAN HEALTH ORGANIZATION. *The regulation of privacy and data protection in the use of electronic health information*. Washington. 2001. Vybrané části dostupné na http://books.google.com [cit. dne: 15.11.2009]

22. PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Stanovisko č. 3/2009 k předloze rozhodnutí Komise o standardních smluvních doložkách pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích podle směrnice 95/46/ES (od správce údajů k zpracovateli údajů.* Dostupné na http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp161_cs.pdf [cit. dne: 24.9.2009]

23. PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Stanovisko č. 2/2007 k informování cestujících o předávání údajů jmenné evidence cestujících (PNR) orgánům Spojených států přijaté dne 15. února 2007 a revidované a aktualizované dne 24. června 2008.* Dostupné na http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp151_cs.pdf [cit. dne: 11.11.2009]

24. PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Stanovisko č. 5/2009 k internetovým sociálním sítím.* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_cs.pdf [cit. dne: 11.11.2009]

25. PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Stanovisko č. 1/2008 k otázkám ochrany osobních údajů v souvislosti s vyhledávači*. Dostupné na http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_cs.pdf [cit. dne: 11.11.2009]

26. PRACOVNÍ SKUPINA PRO OCHRANU OSOBNÍCH ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29. *Working Document setting up a table with elements and principles to be found in Binding Corporate Rules* ze dne 24.6.2008 Dostupné na http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/bcr_table_wp153.pdf [cit. dne: 11.11.2009]

27. PRÁVO. KOTEK, P. *Kamerové systémy používá 28 procent škol, některé porušují práva žáků a studentů.* 10.11.2009 Dostupné na http://www.novinky.cz/veda-skoly/183864-kamerove-systemy-pouziva-28-procent-skol-nektere-porusuji-prava-zaku-a-studentu.html [cit. dne: 16.11.2009]

28. PRÁVO. PŘIBYL, M.. *Školství sbírá statisíce citlivých dat o žácích.* 16.1.2009 Dostupné na http://www.novinky.cz/domaci/158864-skolstvi-sbira-statisice-citlivych-dat-o-zacich.html [cit. dne: 16.11.2009]

29. PRIVACY INTERNATIONAL. *The 2007 International Privacy Ranking.* Dostupné na http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559597[cit. dne: 24.10.2009]

30. RAMASASTRY, A. *The EU-US Safe Harbor Does Not Protect US Companies with Unsafe Privacy Practices.* 17.11.2009 Dostupné na http://writ.news.findlaw.com/ramasastry/20091117.html [cit. dne: 20.11.2009]

31. RAND Corporation. *Review of the European Data Protection Directive*. Květen 2009. Dostupné na http://www.rand.org/pubs/technical_reports/TR710/ [cit. dne: 15.11.2009]

32. RICE, DENIS T. *Jurisdiction over privacy issues on the internet.* http://www.howardrice.com/uploads/content/JurisdictionOverPrivacyIssuesRice2004.pdf (*vybrané aspekty).*

33. Stanovisko č. 1/2008 k otázkám ochrany osobních údajů v souvislosti s vyhledávači, s. 10 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_cs.pdf

[cit. dne: 18.11.2009]

34. STÁTNÍ ÚSTAV PRO KONTROLU LÉČIV. *Tisková zpráva ze dne 23.3.2009., dále ze dne 4.8.2009 a 21.10.2009* Dostupné na http://www.sukl.cz/tiskove-zpravy-k-cinnosti-sukl [cit. dne: 11.11.2009]

35. Tisková zpráva SÚKL ze dne 21. října 2009 dostupná na http://www.sukl.cz/tiskova-zprave-ze-dne-21-10-2009 a Tisková zpráva SÚKL ze dne 21. října 2009 II. dostupná na http://www.sukl.cz/uploads/TIO/TZ_21.10.2009/TZ_Meni_se_zpusob_vydeje_PSE_1021_final_verze_MZ.pdf

36. TN.CZ *Trestní oznámení na šéfku Fondu ohrožených dětí. Kvůli fotkám.* Dostupné na http://tn.nova.cz/zpravy/domaci/trestni-oznameni-na-fond-ohrozenych-deti-zverejnuje-fotky-deti.html [cit. dne: 15.11.2009]

37. ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ . *Tisková zpráva ze dne 21. října 2009*. Dostupná na http://www.uoou.cz/uoou.aspx?menu=15&loc=651 [cit. dne: 10.11.2009]

38. ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *K problémům z praxe – č. 1. K pojmu osobní údaj*. Dostupné na http://www.uoou.cz/uoou.aspx?menu=14&loc=330 [cit. dne: 15.11.2009]

39. ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Kde jsou hranice nových možností biometriky*? Dostupné na http://www.uoou.cz/printer.aspx?id=183 [cit. dne: 10.11.2009]

40. ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Stanovisko č. 1/2009 Úřadu pro ochranu osobních údajů - Zpracování osobních údajů na základě smluv uzavíraných se zpracovateli (tzv. řetězení zpracovatelů osobních údajů*. Dostupné na http://www.uoou.cz/files/stanovisko_2009_1.pdf [cit. dne: 24.8.2009]

41. VEŘEJNÝ OCHRÁNCE PRÁV. *Práva osob při ochraně osobních údajů*. 11. listopadu 2009. Dostupné na http://www.ochrance.cz/dokumenty/dokument.php?doc=1556 [cit. dne: 11.11.2009]

- **Právní předpisy a mezinárodní dohody**

1. Evropská Úmluva o ochraně lidských práv a základních svobod ze dne 4.listopadu 1950, Rada Evropy, dostupné na: http://www.helcom.cz/view.php?cisloclanku=2005020107&PHPSESSID=1f7063f0566fda2874b56d5da5958fed [cit. dne: 5.2.2009]

2. Směrnice Evropského parlamentu a Rady č. 95/46/ES, ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů

3. Úmluva č. 108 – na ochranu osob se zřetelem na automatické zpracování osobních dat ze dne 28. ledna 1981

4. Všeobecná deklarace lidských práv a svobod, čl. 12

5. Zákon č. 101/2000 Sb.o ochraně osobních údajů a o změně některých zákonů (zákon o ochraně osobních údajů), v aktuálním znění

6. Zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech.

7. Zákon č. 262/2006 Sb. – vybraná ustanovení.

8. Zákon č. č. 378/2007 Sb. o léčivech – vybraná ustanovení.

9. Rozhodnutí Komise ze dne ze dne 26. července 2000 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně poskytované podle zásad bezpečného přístavu a s tím souvisejících často kladených otázek vydaných Ministerstvem obchodu Spojených států (2000/500/ES)

10. Rozhodnutí Komise ze dne 20. prosince 2001 o odpovídající ochraně osobních údajů, kterou poskytuje kanadský zákon o ochraně osobních informací a elektronických dokumentech (Personal Information Protection and Electronic Documents Act) (2002/2/ES)

11. Rozhodnutí Komise ze dne 30. června 2003 podle Směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně osobních údajů v Argentině (2003/490/ES)

12. Rozhodnutí Komise ze dne 21. listopadu 2003 o odpovídající ochraně osobních údajů v Guernsey (2003/821/ES)

13. Rozhodnutí Komise ze dne 28. dubna 2004 o odpovídající ochraně osobních údajů na Ostrově Man (2004/411/ES)

14. Rozhodnutí Rady 2007/551/SZBP/SVV ze dne 23. července 2007 o podpisu, jménem Evropské unie, Dohody mezi Evropskou unií a Spojenými státy americkými o zpracovávání údajů jmenné evidence cestujících (PNR) leteckými dopravci a o jejich předávání Ministerstvu vnitřní bezpečnosti Spojených států (Dohoda PNR 2007). Dostupná na http://eur-lex.europa.eu/Notice.do?val=453550:cs&lang=cs&list=476932:cs,476933:cs,476809:cs,469524:cs,453652:cs,453653:cs,453550:cs,478912:cs,435269:cs,435270:cs,&pos=7&page=1&nbl=30&pgs=10&hwords=passenger~data~&checktexte=checkbox&visu=#texte [cit. dne: 10.11.2009]

15. VYHLÁŠKA č. 54/2008 ze dne 6. února 2008 o způsobu předepisování léčivých přípravků, údajích uváděných na lékařském předpisu a o pravidlech používání lékařských předpisů

16. Rozhodnutí Komise ze dne 8. května 2008 podle Směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně osobních údajů v Jersey (2008/393/ES)

- **Soudní a jiná rozhodnutí**

1. Rozhodnutí Nejvyššího správního soudu 9 As 34/2008 ze dne 12.2.2009 dostupné na www.uoou.cz, sekce Judikatura, česká.

2. SOUDNÍ DVŮR EVROPSKÝCH SPOLEČENSTVÍ. *Spojené věci C-317/04 a C-318/04: Rozsudek Soudního dvora (velkého senátu) ze dne 30. května 2006 – Evropský parlament v. Rada Evropské unie.* Dostupné na http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2006:178:0001:0002:CS:PDF [cit. dne 29.10. 2009]

3. Rozhodnutí evropského soudního dvora C-101/01 ze dne 6.11.2003 dostupné na http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=en&newform=newform&Submit=Submit&alljur=alljur&jurcdj=jurcdj&jurtpi=jurtpi&jurtfp=jurtfp&alldocrec=alldocrec&docj=docj&docor=docor&docop=docop&docav=docav&docsom=docsom&docinf=docinf&alldocnorec=alldocnorec&docnoj=docnoj&docnoor=docnoor&radtypeord=on&typeord=ALL&docnodecision=docnodecision&allcommjo=allcommjo&affint=affint&affclose=affclose&numaff=&ddatefs=&mdatefs=&ydatefs=&ddatefe=&mdatefe=&ydatefe=&nomusuel=&domaine=&mots=privacy+%22data+subject%22&resmax=100 [cit. dne 29.9. 2009]

4. Rozsudek Soudního dvora C-553/07 ze dne 7.5.2009 dostupné na http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:153:0010:0010:CS:PDF [cit. dne 15.10. 2009]

- **Internetové stránky**

1.	http://epic.org/	Webové stránky Electronic Privac Information Center
2.	http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm	Webové stránky Evropské komise věnované ochraně osobních údajů
3.	http://www.edps.europa.eu/EDPSWEB/edps/pid/1?lang=cs	Webové stránky Evropského inspektora ochrany údajů
4.	http://www.export.gov/safeharbor/index.asp	Webové stránky Ministerstva obchodu Spojených států amerických věnované problematice exportu a Safe Harbor pravidlům
5.	http://www.uoou.cz/uoou.aspx	Webové stránky Úřadu pro ochranu osobních údajů

Resumé – Personal Data Protection

Norman Lewis, the author of an article entitled “Right for Privacy in the Age of Facebook”, points out an important divergence related to personal data protection: “It is common to encounter people who are concerned about data collection and the potential abuse of power by the state, but who are at the same time willing to reveal deeply personal thoughts on social networking sites”. In his article, N.Lewis poses a question “can one seriously argue that privacy is generally regarded as important today?” In my opinion, the issue of personal data protection is becoming increasingly important.

An interest in the topic of personal data protection is connected to the modern era and mainly to the development of modern technologies. Personal data processing, the possible misuse of such data and personal data theft are phrases often to be heard nowadays. In addition, another related issue has recently been gaining considerable attention – personal data transfer to foreign countries.

Outlining the structure of this thesis in greater detail, the first chapter introduces the basic historical sources of corresponding international and European legislation (such as international agreements, OECD Guidelines on protection of privacy and trans-border flows of personal data or Personal Data Protection Directive). It also mentions the most important statutes regulating the personal data protection in the Czech Republic. Having made the reader acquainted with the personal data protection topic, an introduction to terminology and basic personal data principles follows. The last part of chapter one deals with institutions in this field such as the European Commission, Article 29 Working Party of Personal Data Protection Commissioner or in case of the Czech Republic – Office for Personal Data Protection; the most well-known international non-governmental organizations are also mentioned.

Chapter 2 of this thesis introduces the topic of personal data transfer and outlines different means stated by legislation that enable transfer of personal data. The reader the reader finds out about personal data transfers based on “Standard Contractual Clauses”, European Commission’s Decisions, Safe Harbor Principles (applicable in case of personal data transfer to the USA) or Binding Corporate Rules enabling personal data to be transferred among different companies within a given corporate group. Personal data

transfer based on the approval of the Czech Office for Personal Data Protection forms the last part of this chapter.

The last chapter of this thesis points out three groups of actual cases or problems publically discussed, which are exemplified using a few illustrative examples. The first of the three categories of cases contains the ones where personal data processing is free and facultative. Secondly, we look at such types of personal data processing when the data subject provides consent to personal data protection, but not from his/her own free will. Instead, he/she is somehow "forced" to do so. Thirdly, the last group illustrates cases when people's personal data are processes obligatorily and there is no way to avoid it. The exceptionally contemporaneous nature of the topic addressed means new issues and developments as well as further cases arise on a daily basis. Therefore, given the limited scope of this work, these must be left for discussion to other authors.

The thesis is based on actual information provided mostly from the Internet as the corresponding literature in the Czech language is not so wide. The work is based on information provided until 1st December 2009.

Key words: **personal data, data transfer, actual cases**

Klíčová slova: **ochrana osobních údajů, předávání osobních údajů do zahraničí, aktuální otázky**