Univerzita Palackého v Olomouci

Právnická fakulta

Ondřej Fiala

Ochrana osobních údajů v kontextu cloud computingu

Diplomová práce

Olomouc 2017

„Prohlašuji, že jsem diplomovou práci na téma Ochrana osobních údajů v kontextu cloud computingu vypracoval samostatně a citoval jsem všechny použité zdroje.“

V Olomouci dne 15. 3. 2017 .....

Ondřej Fiala

*Na tomto místě bych rád poděkoval **JUDr. Petru Prchalovi, Ph.D.** za jeho odborné vedení, cenné rady a konzultace pr□i pr□íprave□ této diplomové práce, a mým rodičům za podporu a trpělivost.*

Obsah

Seznam použitých zkratek

Právní předpisy

GDPR	Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES. Úř. věst. L 119, 4. května 2016, s. 1 a násl.
Listina	Listina základních práv a svobod, vyhlášená zákonem č. 23/1991 Sb., kterým se uvozuje LISTINA ZÁKLADNÍCH PRÁV A SVOBOD jako ústavní zákon Federálního shromáždění České a Slovenské Federativní Republiky, republikovaná usnesením předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky, ve znění ústavního zákona č. 162/1998 Sb., kterým se mění Listina základních práv a svobod
Listina EU	Listina základních práv Evropské unie. Úř. věst. C 326, 26. října 2012, s. 391 a násl.
MPOPP	Mezinárodní pakt o občanských a politických právech, vyhlášený pod č. 120/1976 Sb.
Nařízení Řím I	Nařízení Evropského parlamentu a Rady (ES) č. 593/2008 ze dne 17. června 2008 o právu rozhodném pro smluvní závazkové vztahy (Řím I). Úř. věst. L 177, 4. července 2008, s. 6 a násl.
OchOsÚ	Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů
o. z. *nebo* **občanský zákoník**	Zákon č. 89/2012 Sb., občanský zákoník, v platném znění
Rozhodnutí Komise	Rozhodnutí Komise 2016/1250 ze dne 12. července 2016, o odpovídající

2016/1250	úrovni ochrany poskytované štítem EU–USA na ochranu soukromí. Úř. věst. L 207, 1. srpna 2016, s. 1 a násl.
SEU	Smlouva o Evropské unii ze dne 7. února 1992, ve znění Lisabonské smlouvy ze dne 13. prosince 2007
SFEU	Smlouva o fungování Evropské unie ze dne 25. března 1957, ve znění Lisabonské smlouvy ze dne 13. prosince 2007
Směrnice 95/46/ES	Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto osob. Úř. věst. L 281, 23. listopadu 1995, s. 31 a násl.
Směrnice č. 58	Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací. Úř. věst. L 201, 31. července 2002, s. 37 a násl.
TZ	Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů
Úmluva	Úmluva o ochraně lidských páv a základních svobod, vyhlášená pod č. 209/1992 Sb.
Úmluva č. 108	Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat, ze dne 28. 1. 1981, vyhlášená pod č. 115/2011 Sb. m. s.
Ústava	Ústavní zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpisů
ZNSIS	Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů, ve znění pozdějších předpisů

Instituce

ESLP	Evropský soud pro lidská práva
EHP	Evropský hospodářský prostor
EU	Evropská Unie
Komise	Evropská komise
Nejvyšší správní soud	Nejvyšší správní soud České republiky
NIST	Národní ústav pro normalizace a technologie USA
PS 29	Pracovní skupina pro ochranu údajů, zřízená dle čl. 29 Směrnice 95/46/ES
SD EU *nebo* **Soudní dvůr**	Soudní dvůr Evropské Unie (*dříve Soudní dvůr Evropských společenství*)
Úřad	Úřad pro ochranu osobních údajů
Ústavní soud	Ústavní soud České republiky

Jiné

Sb.	Sbírka zákonů
Sb. m. s.	Sbírka mezinárodních smluv
USA *nebo* **Spojené státy**	Spojené státy americké

Úvod

V letech 1898 až 1901 byl vedoucím patentového úřadu Spojených států amerických Charles Holland Duell[1], který pronesl myšlenku: „*In my opinion, all previous advances in the various lines of invention will appear totally insignificant when compared with those which the present century will witness. I almost wish that I might live my life over again to see the wonders which are at the threshold.*".[2] Již víme, že Duell nemohl být svým vizionářským výrokem pravdě blíže. Když byl roku 1945 dokončen jeden z prvních elektronkových počítačů, nazvaný ENIAC, který je považován za jednoho z prapůvodních předchůdců dnešních počítačů[3], začala nová éra lidstva. Počítač se stal převratným vynálezem. Jeho význam se umocnil s příchodem internetové sítě. Ať již chceme nebo ne, počítače pro nás mají značné dopady – ekonomické i sociologické. Vždyť doba, ve které se nyní nacházíme, se označuje jako digitální věk.[4] S nárůstem terciárního sektoru hospodářství se počítačové technologie staly běžnou součástí pracovního života. Počítače, resp. moderní informační technologie, používá většina z nás v každodenním životě. Prohlížíme webové stránky, „konzumujeme" jejich obsah, komunikujeme na sociálních sítích. Nově na internetu i nakupujeme potraviny. Denně máme možnost navázat nové kontakty a nemusíme být ani fyzicky v blízkosti. Lze tak snadno získat iluzorní dojem anonymity a ztratit obezřetnost při opatrování svého soukromí. Užíváním moderních technologických nástrojů po sobě však zanecháváme digitální stopy. Jedná se např. o informace, které sdělují, jaké stránky jsme navštívili, které zboží jsme zakoupili, jaké fotografie jsme na sociálních sítích zveřejnili, apod. Možnosti nakládání s informacemi v dnešní době popisuje D. Goleman. Uvádí příklad programu, pomocí něhož byly po celém světě analyzovány vyhledávací požadavky uživatelů internetu. Po dobu pěti let bylo shromažďováno množství informací, přičemž čím více údajů bylo získáno, tím bylo dosaženo kvalitnějšího výsledku – jedná se o práci s tzv. *big data*. Zaměstnanci Googlu poté ve spolupráci s americkým Centrem pro kontrolu a prevenci

[1] Federal Judiciary Center. *History of the Federal Judiciary* [online]. fjc.gov, [cit. 20. října 2016]. Dostupné na <http://www.fjc.gov/servlet/nGetInfo?jid=654&cid=999&ctype=na&instate=na>.
[2] GRAFSGAARD, Brian. Portfolio, Program, and Project Management as Enablers of Innvation. In LEVIN, Ginger (ed). *Program Management: A Life Cycle Approach*. Auerbach Publications, 2012, s. 416.
[3] HAIGH, Thomas, PRIESTLEY, Mark. Where Codes Come From: Architectures of Automatic Control from Babbage to Algol. *Communications of the ACM*, 2016, roč. 59, č. 1, s. 41.
[4] TAPSCOTT, Don. *Digitální ekonomika: naděje a hrozby věku informační společnosti*. 1. vydání. Brno: Computer Press, 1999, s. 2.

nemocí (CDC)[5] vyvinuli aplikaci, která analyzovala výsledná data. Účelem bylo naučit se v budoucnu určit včasný výskyt chřipkové epidemie. Aplikace analyzovala dotazy typu zvýšená teplota nebo bolest zad, jako příznaky chřipky. Následně byl z výsledků aplikace vytvořen algoritmus, který nově určí propuknutí chřipky, a to s předstihem několika dní. Pouze na základě chování uživatelů internetu.[6] Uvedené je pouze zlomkem, jak lze zacházet s internetovými daty. Je to důkaz toho, jak se změnila práce s informacemi, a též jejich hodnota. Nemusí se vždy jednat o medicínské účely, ale např. marketingové či politické. Zde patrně cítíme, že už nejsme tak ochotni sdělovat o sobě údaje pro analyzování k obchodním účelům.

Bariéry, které byly budovány za účelem ochrany soukromí, tak mohou mít ohroženy své základy. Ostatně, bezdrátová síť internetu „prostupuje" opravdovými zdmi. Není pochyb o tom, že výpočetní technologie dnes usnadňují jednání, jímž dochází k narušení soukromí bez větších obtíží.[7] Pan profesor Telec uvádí, že internet neproměnil právo samotné, avšak „*nebývalou měrou zvýšil míru pokušení k porušování práv bližních a vůbec míru bezohlednosti veřejného projevu (...)*".[8] Do popředí se tak stále více dostává ochrana osobních údajů, jakožto nástroj realizace ústavně zaručeného práva před neoprávněným zasahováním do soukromí a osobního života a neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním osobních údajů.[9]

Předkládaná diplomová práce je zaměřena na koncepci ochrany osobních údajů jako součásti ochrany soukromí. Práce zkoumá ochranu osobních údajů v prostředí počítačového modelu užívání, jehož obliba je na vzestupu – *cloud computing*. Díky této službě dochází k využívání výpočetní techniky formou sdílení její kapacity. V řadě případů bývají cloudové služby používány jako datová úložiště, kde se koncentruje množství (osobních) údajů. Uživatelé svěřují svá data do rukou cizích osob, které s nimi dále nakládají. Přestože si to někteří neuvědomují, používají *cloud* běžně. Kupříkladu emailová schránka je na této bázi založena. V rámci cloudových služeb je častý mezinárodní prvek, kdy jsou služby provozovány z jednoho či více míst a nabízeny prostřednictvím internetové sítě uživatelům kdekoli na světě. Uživatelská data „cestují" do datového centra vzdáleného tisíce kilometrů.

---

[5] Centers for Disease Control and Prevention, www.cdc.gov.
[6] GOLEMAN, Daniel. *Pozornost: skrytá cesta k dokonalosti*. 1. vydání. Brno: Jan Melvil Publishing, 2014, s. 139 – 140.
[7] BARTOŇ, Michal. Ústavněprávní aspekty zveřejňování odposlechů: analýza kolize práva na soukromí, svobody šíření informací a práva na spravedlivý proces. In ŠIMÍČEK, Pavel (ed). *Právo na soukromí*. Brno: Masarykova univerzita, 2011, s. 63.
[8] TELEC, Ivo. Poznámky k internetu a proměnám práva. *Právní rozhledy*, 2013, roč. 21, č. 12, s. 448.
[9] Čl. 10 Listiny.

Tyto a další prvky mohou představovat prostředí umožňující narušení soukromí, případně ztěžovat zajištění jeho ochrany. Uvedeným výzvám by měla právní úprava čelit. Smyslem práce je zhodnotit, nakolik úspěšně se jí to daří.

Inspirací pro mě bylo uvědomění, že s rozvojem digitálních technologií získává ochrana soukromí novou dimenzi, kde se střetává svět právních norem s digitálními inovacemi. Zákonodárce se pochopitelně snaží reagovat na technologický pokrok a „nové" způsoby jednání lidí. Téma předložené práce považuji za důležité z hlediska jeho aktuálnosti, závažnosti dopadů a absence komplexního zpracování v literatuře. Ochraně osobních údajů při poskytování cloudových služeb se, v porovnání s tradičními tématy, odborná monografická literatura souhrnně nevěnuje, navzdory tomu, že dochází k nárůstu užívání těchto služeb. Domnívám se, že zmíněný stav je důsledkem relativně krátké doby, kdy cloudová „technologie" zaznamenala tak mohutné rozšíření. O něco příznivější situace je mezi odbornými články, a to jak cizojazyčnými, tak i českými. Samotná oblast internetových úložišť a jiných cloudových služeb není právním řádem specificky upravena. Zkoumána proto bude obecná úprava vztahující se k ochraně osobních údajů. Jedná se především o zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „OchOsÚ") a směrnici Evropského parlamentu a Rady 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto osob (dále jen „Směrnice 95/46/ES").

Cíl a hypotézy

Cílem práce je poukázání na rizikové situace z hlediska ochrany osobních údajů, vznikající při užívání cloudových služeb. Předkládaná práce není analýzou všech zákonných ustanovení upravujících danou problematiku. Vzhledem k tomu, že cloudové služby mají různé způsoby poskytování, zaměřím se v diplomové práci na užívání veřejných internetových úložišť a obdobných služeb ve formě *software jako služba*[10]. Přínosem práce je vyhodnocení používání cloudových služeb z hlediska ochrany osobních údajů a označení částí právní úpravy, která nedostatečně upravují užívání internetových úložišť a způsobují tak snížení ochrany osobních údajů. Na podkladě charakteru cloudové technologie označím rizikové situace, které nastávají při ukládání údajů do datových úložišť, aplikuji na ně příslušná zákonná ustanovení a tyto analyzuji. Získané poznatky budou následně vyhodnoceny tak, aby bylo možné opovědět na hlavní výzkumnou otázku:

[10] K pojmu software jako služba viz kapitola 2 předkládané práce.

1. **Zda právní úprava, dopadající na *cloud computing*, představuje riziko pro ochranu osobních údajů?**

Dílčí cíle této práce:

1. **Prokázat, že ochrana osobních údajů tvoří důležitou součást práva na ochranu soukromí.**
2. **Určit rizikové situace, při nichž vzniká hrozba snížení ochrany osobních údajů.**

Uvedené cíle korespondují s těmito hypotézami:

1. **Právní úprava obsahuje mezery, kdy absentuje úprava určitých situací, vznikajících při poskytování cloudových služeb.**
2. **Nedůsledná harmonizace evropsko-unijních předpisů a Úřadem zavádějící výklad má podíl na snížení ochrany osobních údajů.**
3. **Právní úprava vykazuje nedostatky při určování rozhodného práva regulující ochranu osobních údajů v EHP.**
4. **Právní úprava neobsahuje prostředky, které zajišťují efektivní výkon ochrany předávaných údajů do USA.**

Struktura práce

Diplomová práce je rozdělena do dvou hlavních částí – obecné a zvláštní. Obecná část obsahuje tři kapitoly a část zvláštní kapitoly dvě.

Práce se v první kapitole zabývá ochranou osobních údajů jako součásti základního lidského práva na soukromí. Zároveň je zde rozebrán charakter koncepce ochrany osobních údajů. Druhá kapitola se věnuje vymezení pojmu *cloud computing* a jeho smluvní povaze. Poslední kapitola obecné části popisuje základní právní úpravu regulující zkoumanou oblast a zároveň označuje základní prvky právního vztahu, které se stanou předmětem zkoumání ve zvláštní části.

Zvláštní část začíná ve čtvrté kapitole, kde se zkoumají vlivy zákonné úpravy závazkového poměru správce a zpracovatele a dále analyzují specifické situace, ke kterým při nakládání s osobními údaji u poskytování cloudových služeb dochází. Pátá kapitola je samostatně věnována přeshraničnímu transferu dat.

Závěr práce shrnuje poznatky získané z předchozích kapitol a ověřuje naplnění hypotéz.

Metodologie práce

V předkládané práci byla při výzkumu použita především metoda analyticko-deskriptivní. Deskripce je obsažena v obecné části, ve které zaujímá dominantní místo definice a klasifikace pojmu *cloud computing*, přičemž se jedná o nezbytnost pro kapitoly navazující. Popisný rámec následně pokračuje k vymezení základního okruhu právní úpravy, regulující vztahy vznikající při poskytování cloudových služeb. Právní úprava je řazena systematicky, a to od předpisů mezinárodní povahy, přes evropsko-unijní, k vnitrostátním předpisům České republiky. Analytickou část tvoří čtvrtá a pátá kapitola diplomové práce. V nich jsou vybraná ustanovení právní úpravy rozložena na jednotlivé části a tyto prvky následně aplikovány na reálné situace vznikající při užití cloudové technologie.[11] Výsledkem je poté na podkladě provedené analýzy spojení rozebraných prvků (syntéza)[12] a identifikace hrozeb pro zajištění náležité ochrany osobních údajů. Zároveň je v části páté kapitoly je metoda srovnávací.

Předkládaná práce se kombinací zmíněných metod snaží o souvislou posloupnost poznání, kdy je na počátku řetězce sběr relevantních dat (právní úprava, judikatura, výkladová stanoviska), která jsou následně podrobena analýze společně s dopady v praktických situacích. Ze získaných poznatků je provedeno zobecnění a závěr ověřující hypotézy a naplnění cíle předkládané práce.

[11] K analytické metodě viz KNAPP, Viktor, GERLOCH, Aleš. *Logika v právním myšlení*. 3. vydání. Praha: Eurolex Bohemia, 2000, s. 206.
[12] Tamtéž.

1 Právo na soukromí, ochrana osobních údajů a jejich ústavní rozměry

Množství údajů je shromažďováno o uživatelích internetu např. za účelem získání vzorce chování a jeho využití k marketingovým účelům.[13] Koncepce ochrany osobních údajů (dále jako „koncepce“) pak nabývá stále většího uplatnění. Je-li třeba řádně analyzovat ochranu osobních údajů v prostředí cloudových služeb, je nezbytné nevynechat otázku jejího postavení v rovině ústavní, neboť nejen porozumění toho, jaké skutečnosti právní úpravu ovlivňují, lze získat tam, kde vyvěrá její existenciální podstata.

1.1 Definice soukromí

Právo na soukromí se historicky začal vytvářet v USA, kde se v prosinci roku 1890 o první definici pokusili Samuel D. Warren a Louis D. Brandeis.[14] Jimi vymezené právo bylo užší, než jak ho chápeme dnes, když bylo vnímáno jako „právo být ponechán o samotě“ („*the righ to be let alone*“) a vyjadřovalo ochranu před nadměrným zájmem o osobu.[15] Odlišné pojetí nacházíme v evropském prostoru. Zde se právo na soukromí začalo vyvíjet v pozdější době, a to prostřednictvím lidskoprávních smluv.[16]

Maštalka definuje soukromí jako „*okruh skutečností osobního života*“.[17] Zdálo by se, že se jedná o dostačující vymezení, neboť každý dokážeme určit, které skutečnosti tvoří náš osobní život. Pokud se však nad uvedenou definicí zastavíme, pak zjistíme, že způsob, jak je uvedena, obsahuje základní problematický aspekt. Každý z nás totiž může chápat „osobní život“ odlišně. A skutečně chráníme soukromí jen ve sférách *osobního* života? Na pracovišti se mu ochrana neposkytuje? Nelze spatřit limity ochrany soukromí, obepínající *veřejný život* osoby, jako jednu ze sfér, jež je součástí jejího osobního života v širším smyslu?[18]

[13] MANTELERO, Alessandro. Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. *Computer Law & Security Review*, 2016, roč. 32, č. 2, s. 239 – 240.
[14] WARREN, Samuel, BRANDEIS, Louis. The Right to Privacy. *Harward Law Review*, 1890, roč. 4, č. 5, s. 194 – 197.
[15] SELTENREICH, Radim. Právo na soukromí v kontextu ústavního vývoje v USA. *Právník*, 2000, roč. 139, č. 1, s. 23.
[16] FILIP, Jan. Úvodní poznámky k problematice práva na soukromí. In ŠIMÍČEK, Pavel (ed). *Právo na soukromí*. Brno: Masarykova univerzita, 2011, s. 13.
[17] MAŠTALKA, Jiří. *Osobní údaje, právo a my*. 1. vydání. Praha: C. H. Beck, 2008, s. 3.
[18] Podobně viz nález Ústavního soudu ze dne 3. února 2015, sp. zn. II. ÚS 2051/14, bod 28.

Na předestřených otázkách ukazuji, že byť by se zdálo vhodné učinit jednotnou definici pojmu soukromí, jedná se o pojem široký, mající několik dimenzí. Zároveň je pojmem flexibilním a měnícím se v čase. Takové prvky brání vytvoření obecné definice.[19] Podat vyčerpávající vymezení se zdá být nesplnitelné. Nadto vše je soukromí vnímáno odlišně v jednotlivých kulturách, ale i na úrovni jednotlivců. Tvrzenou dynamičnost lze ilustrovat na faktu, že v minulosti byla ochrana soukromí spojena s prostorovou dimenzí, vázánou zejm. na obydlí.[20] Takové vnímání se vlivem technologických nástrojů změnilo, kdy se jeho ochrana rozšiřuje i do on-line prostředí.[21]

V České republice soukromí pojímá konstituční ochranu. Jeho definici však nenalezneme. O vyčerpávající popis se nesnaží ani judikatura. Přesto bylo v některých případech třeba vymezit, zda se okruh projednávaných skutečností pod pojem podřadí. Taková rozhodnutí nalezneme na vnitrostátním úrovni činností Ústavního soudu,[22] případně na evropské úrovni, kde se těmito otázkami zabýval ESLP, který zastává koncepci širokého pojetí soukromí. Plyne to např. z rozsudku Amann proti Švýcarsku, v němž je uvedeno, že soukromý život nesmí být vykládán restriktivně, neboť respektování soukromí zahrnuje i právo navazovat vztahy s jinými lidmi a tyto kontakty dále rozvíjet.[23] V jiném rozhodnutí ESLP vyslovil, že nepovažuje za možné ani nezbytné podat vyčerpávající definici pojmu „soukromý život“, neboť by jej tak limitoval na „vnitřní okruh“, ve kterém může každý žít osobní život, jak se rozhodne, a vyloučit vnější svět neobsáhnutý v tomto okruhu, přičemž respekt soukromí zahrnuje z části i právo tvořit a rozvíjet vztahy s ostatními.[24]

Než přiblížím pojetí v Listině, podívejme se nejdříve na zakotvení v mezinárodních smlouvách, které do našeho právního řádu prostupují skrze čl. 10 Ústavy. Úmluva obsahuje ochranu soukromí v čl. 8. Zde se každému zaručuje právo na respekt soukromého a rodinného života, obydlí a korespondence. Podobně MPOPP v čl. 17 zakazuje svévolné zásahy do soukromého života, rodiny, domova nebo korespondence, jakož i útoky na cti a pověsti. Jiné vymezení nalezneme na unijní úrovni, kde je ochrana zakotvena v Listině EU.

---

[19] Podobně i WAGNEROVÁ, Eliška. In WAGNEROVÁ, Eliška a kol. *Listina základních práv a svobod. Komentář*. 1. vydání. Praha: Wolters Kluwer ČR, 2012, s. 278 (čl. 10).

[20] KOKEŠ, Marian. K problematice konkrétních konfliktů mezi právem na informační sebeurčení a ochranou národní bezpečnosti v tzv. době internetové. In ŠIMÍČEK, Pavel (ed). *Právo na soukromí*…, s. 122.

[21] LONDON ECONOMICS. *Study on the economic benefits of privacy enhancing technologies* [on-line]. ec.europea.eu [cit. 22. října 2016]. Dostupné na <http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf>, s. 14 – 15.

[22] Viz např. nález Ústavního soudu ze dne 22. března 2011, sp. zn. Pl. ÚS 24/10, body 53 – 54.

[23] Evropský soud pro lidská práva: Rozsudek ze dne 16. února 2000, *Amann v Švýcarsko*, 27798/95, Sb. rozh. 6/2002, bod 65.

[24] Evropský soud pro lidská práva: Rozsudek ze dne 16. prosince 1992, *Niemietz v Německo*, 13710/88, Sb. rozh. 14/1996, bod 29.

Prostřednictvím čl. 8 je chráněno soukromí tak, jak známe z uvedených mezinárodních smluv. Nově se zde v čl. 9 vyděluje aspekt soukromí v podobě samostatné ochrany údajů osobního charakteru.

Listina obecnou koncepci ochrany soukromí, podobné Úmluvě či MPOPP, neobsahuje. Tvůrci Listiny zvolili způsob analogický s Listinou EU. Koncepci práva však systematicky rozpracovali. V Listině je právo na ochranu soukromí pojato komplexně, nicméně se skládá z jednotlivých práv, která jsou rozmístěna v několika dílčích ustanoveních. Kupříkladu právo na osobní integritu nalezneme v čl. 7, nedotknutelnost obydlí v čl. 12 a listovního tajemství v čl. 13. Pro tuto práci je klíčový čl. 10 Listiny, který garantuje ochranu soukromí v širším smyslu, a to před zásahy do soukromého a rodinného života, kde je následně v odst. 3 obsažena zvláštní úprava osobních údajů, v podobě ochrany před neoprávněným nakládáním. Přestože jsou uvedená ustanovení přímo aplikovatelná, je nezbytné, aby byla též provedena ve zvláštních zákonech.[25]

1.2 K postavení koncepce ochrany osobních údajů v rovině (pod)ústavní

Obecnou úpravu ochrany osobních údajů představuje OchOsÚ. Zákonodárce zde upravuje prostředky ochrany soukromí, také ve sféře práva veřejného, vedle tradičních soukromoprávních institucí jako např. ochrana osobnosti.

Dle Úřadu pro ochranu osobních údajů (dále jen „Úřad“) představuje koncepce ochrany osobních údajů nástroj, pomocí něhož se v České republice provádí ochrana osobnosti a soukromí před specifickými, zásahy, a to zejména v prostředí internetu.[26] Domnívám se, že takové tvrzení je nepřesné. Je třeba odlišit ochranu osobnosti a ochranu osobních údajů, neboť se jedná o rozdílné instituce, byť mají společný účel, jímž je ochrana soukromí. Soukromí je tak zastřešující pojem, jemuž je garantována ochrana pomocí dílčích složek, jako je ochrana osobnosti, ochrana osobních údajů či nedotknutelnost osoby, aj. Ostatně o právu na soukromí, jako právu složeného z určitých dílčích samostatných práv, požívajících ochranu, hovoří např. Wagnerová.[27] O tom, že nelze slučovat ochranu osobnosti a ochranu osobních údajů tak svědčí charakter právní úpravy, ale také její obsah. Ochrana osobnosti je soukromoprávní institucí, jejíž zakotvení nalézáme v § 81 a násl. o. z. Proti tomu stojí

[25] MATES, Pavel. K některým otázkám ochrany soukromí ve správním právu. *Právní rozhledy*, 2002, roč. 10, č. 8, s. 369.
[26] Stanovisko Úřadu pro ochranu osobních údajů – Zveřejňování osobních údajů na internetu, č. 13/2012, březen 2012 (aktualizace únor 2014), s. 1.
[27] WAGNEROVÁ, Eliška. In WAGNEROVÁ, Eliška a kol. *Listina základních práv a svobod*... s. 280 (čl. 10).

ochrana osobních údajů, jako veřejnoprávní ochrana upravena v samostatném zákoně OchOsÚ, prostřednictvím něhož zákonodárce reguluje určité poměry osob. OchOsÚ tak představuje prostředek správního práva, chránící garanci práva na soukromí.[28]

Výše uvedenou tezi Úřadu Maštalka dále rozvádí, když na příkladu střetu práva na soukromí a práva na informace, uvádí, že bude záležet na předpisech nižší právní síly, jak meze Listiny využijí, neboť „*realizace ochrany soukromí je vázána na další vymezení oprávněného a neoprávněného zásahu*“.[29] Takové pojetí chápe koncepci ochrany osobních údajů jako podmnožinu ochrany soukromí a její roli vnímá více v oblasti podústavní. Jiný pohled uvádí Komise, která považuje ochranu osobních údajů jako základní právo.[30]

Mám za to, že uvedené názory nejsou v rozporu, ale naopak se doplňují. Pokud bychom měli říci, jaké postavení má ochrana osobních údajů v ústavní a podústavní rovině, pak se domnívám, že koncepce ochrany osobních údajů požívá ústavní opory, neboť její úpravu nalézáme v čl. 10 odst. 3 Listiny. Jedná se tak o základní lidské právo, které vyžaduje zákonné upřesnění. Vlivem moderních technologií právo na ochranu osobních údajů nabývalo stále větší důležitosti, kdy je nyní garantováno jako samostatné lidské právo tvořící dílčí část v komplexu práva na ochranu soukromí. Takto je zakotveno v Listině. Podrobnější vymezení je však nezbytné na zákonné úrovni, kde nachází odraz v OchOsÚ.

[28] Podobně viz MATES, Pavel. K některým otázkám ochrany soukromí ve správním právu..., s. 369 – 371.
[29] MAŠTALKA, Jiří. *Osobní údaje, právo a my*..., s. 7.
[30] Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů – Komplexní přístup k ochraně osobních údajů v Evropské unii, KOM(2010) 609, listopad 2010, s. 2.

2 K pojmu cloud computing

Ochranu osobních údajů analyzuji v prostředí *cloud computingu*. Jedná se proto o klíčový pojem předkládané práce. Právní vymezení pojmu však absentuje. V literatuře jeho jednotnou definici nenalezneme. Naopak se setkáme s různými koncepty. Důvod je prostý, jedná se o široký pojem a existuje množství podob použití. Vzniku jednotné definice nepomáhá ani skutečnost, že vývoj cloudové technologie je natolik rychlý, že stále přibývají její nové modifikace.[31] Jednotná rigidní definice by v takovém případě mohla být časem zavádějící.

Kalifornská univerzita v Berkley ve studii vedené M. Armbrustem definuje *cloud* jako datové centrum zajišťující přístup k aplikacím na internetu skrze hardwarovou strukturu, která umožňuju takové poskytnutí služby, přičemž charakteristická je úhrada služby „*Pay-as-you-go*“, tj. uživatel hradí jen tolik, kolik reálně „spotřeboval“ kapacity výpočetní techniky.[32] Uvedené popisuje jen strukturu úložiště, nicméně se značně neliší např. od definice J. Svobody, který *cloud* vnímá jako poskytování IT služeb využívajících virtuální infrastrukturu dodavatele, a to prostřednictvím internetu a internetového prohlížeče. Svoboda však ve své definici, oproti studii M. Armbrusta, zdůrazňuje virtuální charakter infrastruktury poskytovatele služby.[33] Dalších vymezení bychom v literatuře vyhledali desítky. Lze však popsat základní obecné prvky, které jsou imanentní napříč různými definicemi. Pro základní představu o tom, co se skrývá pod pojmem *cloud computing* proto postačí jejich vymezení. NIST představil vlastní pojetí *cloudu*, které extrahuje charakteristické prvky a vytváří relativně ucelenou definici netrpící výše nastíněnými nedostatky.[34] *Cloud* bychom mohli v tomto pojetí charakterizovat jako model 5-3-4, tj. službu o pěti základních prvcích, třech druzích služeb a čtyřech modelech nasazení. Nicméně důkazem výše tvrzené dynamičnosti vývoje budiž fakt, že dnes se již běžně pracuje s více druhy služeb, než jen se třemi níže uvedenými.

[31] SVOBODA, Jiří. Cloud Computing. *Systémová integrace*, 2009, roč. 16, č. 2, s. 66.
[32] ARMBRUST, Michael et al. *Above the Clouds: A Berkley View of Cloud Computing* [online]. berkeley.edu, 10. února 2009 [cit. 8. listopadu 2016]. Dostupné na < https://www2.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf>, s. 4.
[33] SVOBODA, Jiří. *Cloud Computing*..., s. 67
[34] MELL, Peter, GRANCE, Timothy. *The NIST definition of cloud computing* [online]. nist.gov, září 2011 [cit. 8. listopadu 2016]. Dostupné na <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>.

2.1 Technické vymezení cloudu dle NIST

Organizace NIST považuje jako základní znaky cloudových služeb tyto následující:

2.1.1 Esenciální prvky

I. Samoobslužný systém (*On-demand),* tj. uživatel nezávisle na poskytovateli přistupuje k službě, využívá a disponuje kapacitou zdrojů. Reguluje velikost úložiště, a to bez přímé součinnosti poskytovatele.

II. Širokopásmový přístup (*Broad network access*) je permanentní síťový přístup služby z různých zařízení např. mobilní telefon, tablet, notebook.

III. Sdílení prostředků (*Resource pooling*), tj. počítačová infrastruktura poskytovatele je uspořádána, aby k ní přistupoval a využíval ji větší počet uživatelů nezávisle na sobě. Kapacita je dynamicky přidělována dle jednotlivých požadavků. Uživatel nad prostředky nevykonává správu. Často ani nemá povědomí, kde se technika nachází.

IV. Škálovatelnost (*Rapid elasticity*) je možnost uživatele operativně navyšovat nebo snižovat kapacitu dle jeho momentálních požadavků na výkon služby.

V. Měřená služba (*Measured service*) znamená, že zdroje jsou (kvalitativně i kvantitativně) měřitelné co do výkonu, kapacity, datového přesunu, dostupnosti apod. Zjištěná data se odrážejí zejm. při hrazení služby.

2.1.2 Servisní modely

Dalšími znaky jsou tři základní druhy služeb, přičemž *službou* se označuje možnost práce se znovu použitelnými a strukturovanými součástmi v síti poskytovatele *cloudu*. Obecně se tak vžilo označení „*as a service*“.[35]

I. Software jako služba (*Software as a Service*) je kompletní hostování a provozování softwaru. Uživateli se poskytuje služba, která je provozována na výpočetní infrastruktuře poskytovatele úložiště. Uživatel má k aplikacím přístup z různých zařízení např. pomocí internetového prohlížeče. Uživateli nemusí stahovat a instalovat softwaru do svého zařízení. Příkladem je balíček Google Apps (Gmail, Disk Google aj.).[36]

II. Platforma jako služba (*Platform as a Service*) je podstatou nasazení aplikace na úložišti, prostřednictvím které uživatele může sám vytvářet jiné (vlastní)

[35] VELTE, Anthony, VELTE Toby, ELSENPETER, Robert. *Cloud Computing*. 1. vydání. Brno: Computer Press, 2011, s. 32.
[36] RAŠKA, Ondřej. Obchodní modely Software as a Service. *Systémová integrace*, 2009, roč. 16, č. 2, s. 27.

aplikace. Často používané jako rozhraní pro další programování. Uživatel, oproti SaaS, získává částečnou kontrolu nad nasazenou aplikací a jejím nastavením (širší customizace). Příkladem PaaS je Microsoft Azure.

III. Infrastruktura jako služba (*Infrastrucutre as a Service*) je poskytování výpočetních prostředků pomocí sítě jako virtuální datové centrum. Provozovatel cloudové služby poskytuje výkon, datové úložiště a další základní zdroje. Uživateli může nasadit a spustit libovolný software, či celé operační systémy, ale nemá kontrolu nad výpočetní kapacitou infrastruktury. Pouze spravuje jím nahraný software. Příkladem IaaS může být Amazon Elastic Compute Cloud.

2.1.3 Modely nasazení

Způsob, jakým je cloudová služba poskytována, lze rozdělit na čtyři základní druhy: soukromý, komunitní, veřejný a hybridní nasazení.

I. Soukromé nasazení představuje služba, která je poskytována pro výhradní užití jediného subjektu, tvořeného více uživateli (např. zaměstnanci společnosti). Služba může být vlastněna a provozována jejím uživatelem či třetí osobou, ale i poskytovatelem. Lze kombinovat uvedené modely, kdy vlastník a správce spolu kooperují.

II. Komunitní *cloud* je též charakteristický svou uzavřeností, avšak uživatelská skupina bývá širší. Komunitní *cloud* je pro členy komunity tvořené organizacemi propojenými společnými zájmy. Infrastruktura může být provozována jednotlivou organizací v postavení uživatele, případně osobou odlišnou.

III. Veřejný *cloud* představuje infrastruktura poskytovaná veřejně. Výpočetní zdroje jsou v dispozici provozovatele. K nim má však prostřednictvím internetu přístup neomezený počet uživatelů.

IV. Hybridní cloudová infrastruktura je kombinací min. dvou předchozích typů, které jsou stále unikátní entitou, ale jsou propojené technologií, která umožňuje přenos dat či celé aplikace.

Na základě uvedené definice lze říci, že *cloud computing* je poskytování specifického druhu služeb, jejichž podstatou je sdílené využívání kapacity výpočetní technologie větším počtem uživatelů, a to za účelem efektivního využití jejího výkonu.[37] Nejedná se však

[37] DONÁT, Josef. Právní aspekty cloud computingu. *IT Systems*, 2011, roč. 13, č. 7-8, s. 42.

o novou technologii. Jedná se o nové pojetí zpřístupnění výpočetních služeb.[38] Dnešní svět je propojený na všech úrovních, a proto i takové pojetí služby, jakkoli v ní lze spatřovat ekonomické výhody (viz níže), s sebou zároveň přináší rizika. Z hlediska ochrany osobních údajů lze spatřovat největší rizika při poskytování veřejného *cloudu*. Ve své analýze se proto zaměřím na tento způsob poskytování cloudových služeb.

2.2 Právní pojetí

V souvislosti s poskytováním cloudových služeb je, pro prevenci vzniku možných budoucích sporů, nezbytné řádně smluvně určit práva a povinnosti mezi poskytovatelem služby a jeho zákazníkem. Jaká smlouva se však na daný právní vztah uplatní? A hovoříme o smlouvě typové, smíšené, nebo se bude jednat o *inominátní* závazkový vztah?

Pro zodpovězení si dané otázky je nezbytné určit obsah smlouvy, od kterého se bude dále odvíjet právní posouzení.[39] Na první pohled by se mohlo zdát, že předmětem cloudových služeb je poskytování výpočetní techniky. Takový výklad by pak mohl směřovat k tomu, že smluvní poměr má nájemní charakter. Předmětem nájemní smlouvy je však dle § 2201 o. z. závazek pronajímatele přenechat nájemci věc k dočasnému užití a závazek nájemce za to pronajímateli uhradit nájemné. Z cit. ustanovení plyne, že jedním z pojmových znaků nájmu je přenechání věci k užití jinému.[40] Domnívám se, že předmětem cloudových služeb není přenechání věci, byť i k tomu může dojít (viz níže). Podstatou cloudové služby tak je závazek k určité činnosti a nikoli věcné plnění.[41] Uvedené ostatně ontologicky vyjadřuje i obecně vžitý pojem cloudové „služby“. Takový přístup uvádí i Bednář, když jako podstatu cloudových služeb uvádí *multitenancy* charakter, tedy umožnění sdíleného používání výpočetních prostředků.[42] V odborné literatuře je tento prvek spojován s tzv. *virtualizací*, tj. zpřístupnění výpočetních zdrojů, přesněji jejich *výkonu*, ke kterému uživatel přistupuje prostřednictvím softwaru, prakticky odkudkoli prostřednictvím internetu na vyžádání (*on-demand*).[43] Charakteristické je také, že uživatel nemá k samotné výpočetní technice faktický přístup.

---

[38] Evropská agentura pro bezpečnost sítí a informací. *Security Cloud Computing: Benefits, risks and recommendation for information ecurity* [online]. enisa.europa.eu, 20. listopadu 2009 [cit. 16. listopadu 2016]. Dostupné na <https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment>, s. 4.

[39] HULMÁK, Milan. In HULMÁK, Milan a kol. *Občanský zákoník VI. Závazkové právo. Zvláštní část (§ 2055-3014). Komentář*. 1. vydání. Praha: C. H. Beck, 2014, s. 139 (§ 1746).

[40] HULMÁK: *Občanský zákoník VI. Závazkové právo. Zvláštní část…*, s. 216 (§ 2201).

[41] Podobně viz JANSA, Lukáš a kol. *Internetové právo*. 1. vydání. Brno: Computer Press, 2016, s. 130.

[42] BEDNÁŘ, Stanislav. Právní zajištění cloudových služeb a velkých dat. *IT Systems*, 2015, roč. 17, č. 2, s. 24.

[43] ALI, Mazhar, KHAN, Samee, VASILAKOS, Athanasios. Security in cloud computing: Opportunities and challenges. *Information Sciences*, 2015, roč. 305, s. 357.

Nenabývá k ní tak detenci a nevykonává nad ní žádnou jinou kontrolu. Domnívám se tak, že pro tyto případy nelze hovořit o přenechání výpočetní techniky, neboť ta zůstává zcela v dispozici poskytovatele. Mám naopak za to, že obsahem smlouvy o poskytnutí cloudových služeb je výkon činnosti, spočívající v síťovém zpřístupnění výkonu výpočetní techniky, resp. umožnění užití kapacity jejího paměťového prostoru. V takovém případě nemá smluvní ujednání charakter nájmu, ale smlouvy o dílo[44] či smlouvy příkazní[45]. Uvedené však platí pro veřejné modely nasazení. Jinak tomu může být v případě soukromého nasazení, kdy úložiště je fyzicky provozováno uvnitř organizace zákazníka. Uživatel vykonává fyzickou kontrolu nad technikou a nabývá tak detenci. V takovém případě lze hovořit o nájemním charakteru. Vzhledem k zaměření této práce na ochranu osobních údajů v prostředí internetových úložišť je však analýza věnována smluvním poměrům vznikajících v oblasti nasazení veřejného typu.

Součástí smlouvy bývá obvykle závazek provozovatele zajistit samotný chod aplikace na určité minimální úrovni tzv. *servis level agreement* (dále jen „SLA“) neboli servisní smlouva. Obsahem SLA je vymezení rozsahu, objemu a úrovně cloudových služeb.[46] Její podstatné náležitosti nejsou zákonem vymezeny a jedná se proto o smlouvu nepojmenovanou.[47] Ujednání servisních podmínek představuje obvyklou obsahovou část smlouvy při poskytování cloudových služeb.

V případě servisního modelu SaaS je obvyklé, že uživatel k přístupu na úložiště využívá aplikaci poskytovatele, kterou lze často i stáhnout a instalovat přímo do svého zařízení. K výše vymezenému obsahu pak ještě dále přistupují ustanovení o užívání aplikace (počítačového programu) v podobě licenčních ujednání.

Z uvedeného je zřejmé, že poskytování cloudových služeb je složitě právně uchopitelné. Domnívám se, že v případě veřejného nasazení modelu SaaS cloudových služeb se jedná o nepojmenovaný smluvní typ, který má svým charakterem nejblíže ke smlouvě o dílo. V případě smlouvy o dílo jde o činnost, na jejímž konci je určitý výsledek v podobě (i) zhotovení věci, (ii) údržbě a (iii) opravě nebo úpravě věci, případně (iv) činnosti s nehmotným výsledkem.[48] Jde-li o zajištění cloudových služeb, pak tato činnost splňuje podmínky činnosti s nehmotným výsledkem dle § 2631 o. z. Smlouva o dílo je v občanském zákoníku pojímána již ne pouze jako výsledek zachycený hmotně, ale i též jako nehmotný výsledek činnosti. Jedná se o proto o výsledek pouze hmotný, ale i o činnost s kterýmkoli

[44] § 2586 a násl. o. z.
[45] § 2430 a násl. o. z.
[46] UČEŇ, Pavel. Servis Level Agreement aplikačních služeb? *IT Systems*, 2002, roč. 4, č. 3, s. 70.
[47] ŠURMANOVÁ, Michaela, KNEBL, Ondřej. Service Level Agreements. *Revue pro právo a technologie: odborný recenzovaný časopis pro technologické obory práva a právní vědy*, 2011, roč. 3, č. 2, s. 23.
[48] § 2587 o. z.

jiným výsledkem.[49] Domnívám se, že činnost spočívající v provozování úložišť lze podřadit právě pod činnost s nehmotným výsledkem, neboť jejím výsledkem je zpřístupnění výpočetní kapacity a zároveň i závazek garance určité úrovně těchto služeb, resp. rychlosti odezvy a stability serveru (viz SLA apod.).

Přestože smlouva o poskytování cloudových služeb vykazuje dle mého názoru prvky díla, domnívám se, že s ohledem na všechna shora uvedená běžná ujednání v ní, se vytváří charakter služby, který je natolik svébytný, že lze hovořit o *inominátním* smlouvě. Může to být zapříčiněno relativně krátkou dobou užívání, kdy zákonodárce zatím ani neseznal, že je třeba upravit výslovně služby úložišť v právním řádu. Lze se také domnívat, že zákonodárce je odrazován složitostí, která se projevuje v množství způsobů poskytování služby, vzájemných kombinací apod.[50] Práva a povinnosti zde tvoří spletitý závazkový vztah. Stávající situace však na smluvní strany klade větší odpovědnost co do řádného ujednání obsahu smlouvy. Již s ohledem na dopady jejich správní odpovědnosti. Přestože je tak předmětem závazku moderní digitální technologie, uplatní se i zde klasická římskoprávní zásada *vigilantibus iura skripta sunt*.

2.3 Cloud computing v Evropské unii

Vzestupné tendence užívání *cloudu* zaznamenala i samotná Evropská unie, která ve Sdělení 2012/059 vyjádřila záměr využít příležitosti a zajisti si světovou vedoucí pozici ve využívání *cloud computingu*.[51] Sdělení 2012/059 vyzdvihuje především ekonomické výhody *cloudu* pro malé a střední podniky, jimž může jeho efektivní využití přinést rychlejší produktivitu, zvýšení konkurenceschopnosti, ale také možnost proniknout na vzdálené trhy, kde dosud působí velké nadnárodní společnosti. EU zároveň plánuje, že cloudové služby postupně aplikuje i do veřejné sféry, kde dojde k jejich nasazení při činnostech orgánů veřejné moci. Takovému záměru pomáhá další výhoda úložišť, spočívající ve znatelném snížení nákladů na provoz informačních a komunikačních technologií. Nelze ani opomenout pozitivní dopady na životní prostředí. Komise zároveň požádala o zpracování studie, ze které plyne, že více jak polovina podniků a uživatelů internetu určitým způsobem využila služeb *cloud computingu*. Při správném nastavení politiky podporující jeho užívání, se může ekonomika

[49] HORÁK, Pavel. In HULMÁK, Milan a kol. *Občanský zákoník VI. Závazkové právo. Zvláštní část (§ 2055-3014). Komentář*. 1. vydání. Praha: C. H. Beck, 2014, s. 1138 (§ 2631).
[50] Podobně OTEVŘEL, Petr. Vybraná úskalí uzavírání smluv typu SaaS. *IT Systems*, roč. 14, č. 4, s. 22.
[51] Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů – Uvolnění potenciálu cloud computingu v Evropě, KOM(2012) 059, září 2012, s. 2.

využívající *cloud* podílet na celkovém HDP EU až 250 miliardami EUR a zároveň vytvořit 3.8 milionu nových pracovních příležitostí. To vše do roku 2020.[52]

Je tak zřejmé, že fenomén *cloud computingu* přináší z ekonomického pohledu významné benefity, které EU lákají. Zároveň však jeho užívání přináší výzvy v podobě možného vzniku zásahů do soukromí jeho uživatelů. Podstata rizik vychází ze samotného charakteru služby, tj. ukládání vlastních dat na cizí výpočetní techniku. Dochází tak ke svěřování dat osobní povahy jinému subjektu. Uživatel pak spoléhá, že s nimi bude řádně nakládáno. *Cloud computing* přináší výzvy co do zajištění řádné ochrany osobních údajů. Sdělení 2012/059 některé výzvy konkrétně popsalo, když za ně považuje jednak nepřehlednost norem v oblasti ochrany osobních údajů, problematický výkon řádné kontroly subjektem údajů, komplikovanost právního rámce spočívající v prolínání se do více právních jurisdikcí a v neposlední řadě též obava ohledně přenositelnosti údajů. Tyto, ale i další výzvy spojené s ochranou osobních údajů v *cloud computingu* jsou právě předmětem zkoumání diplomové práce.

[52] Tamtéž.

3 Právní úprava ochrany osobních údajů

V předchozí kapitole jsem definoval koncepci ochrany osobních údajů, jako jednu ze složek práva na soukromí, vyvěrající z Listiny a mající veřejnoprávní charakter zákonného ukotvení. Nejširším základem ochrany osobních údajů je tak právní úprava ochrany soukromí osob. Účelem právní koncepce ochrany osobních údajů je zabránit, aby bylo zasahováno do práva na soukromí v podobě neoprávněného nakládání s osobními údaji. Hybným podnětem k vytvoření právního rámce koncepce bylo masové rozšíření počítačových technologií a umožnění nových zásahů do soukromí. Ty mají podobu intenzivního shromažďování dat, jejich snadného uchovávání a umožnění rozličných způsobů nakládání s nimi.[53] Cílem předpisů na ochranu osobních údajů je tedy vymezení podmínek, za nichž je zpracování osobních údajů přípustné.[54] Vzhledem k tomu, že se jedná o předpisy veřejnoprávního charakteru, mají normy kogentní charakter a nepřipouštějí možnost odchylných ujednání ve smyslu principu soukromoprávní autonomie vůle vyjádřené v čl. 2 odst. 3 Listiny. Na tomto podkladě lze uzavřít, že jednání, které nebude splňovat podmínky vymezené v předpisech na ochranu osobních údajů pro dovolené nakládání s nimi, narušuje soukromí osob nedovoleným způsobem.

3.1 Mezinárodní základy

V roce 1968 Parlamentní shromáždění Rady Evropy ve svém doporučení upozorňovalo na nové nástrahy soukromí v kontextu ochrany osobních údajů.[55] Prvotní pokusy o všeobecný základ pravidel ochrany osobních údajů vznikly na půdě OECD, která v roce 1980 vydala Pravidla ochrany soukromí a přeshraničních toků[56]. Další dokumenty na sebe nenechaly dlouho čekat. Byla to právě Rada Evropy, která položila základy evropské koncepce, když její členové přijali Úmluvu č. 108. Jedná se o základní evropský dokument, z něhož vycházejí evropsko-unijní a národní předpisy států EU. Mezinárodní Úmluva č. 108

[53] MATES, Pavel. *Ochrana soukromí ve správním právu*. 2. vydání. Praha: Linde, 2006. s. 187.
[54] MAŠTALKA, Jiří. *Osobní údaje, právo a my*..., s. 37.
[55] Rada Evropy. *Doporučení Parlamentního shromáždění Rady Evropy č. 509 (1968) na podkladě 16. zasedání Shromáždění ze dne 31. ledna 1968* [online]. assembley.coe.int, [cit. 19. listopadu 2016]. Dostupné na <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=14546&lang=en>.
[56] OECD. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* [online]. oecd.org, 2013 [cit. 19. listopadu 2016]. Dostupné na <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>.

dala směr, kterým se právní řád ubírá, a to zásluhou všeobecných principů, zakotvených v čl. 5 – 8 Úmluvy č. 108 a čl. 1 Dodatkového protokolu[57]. Úmluva č. 108 dále vymezuje základní pojmy, jakož i požadavky pro řádné zpracování osobních údajů a jejich přeshraniční transfer.

3.2 Prameny práva Evropské unie

Vstupem České republiky do Evropské unie došlo k provázání našeho právního řádu s evropsko-unijní legislativou. Do právního řádu tak vstoupily nové prameny práva. Pro oblast ochrany osobních údajů se jedná o dva nejčetnější druhy předpisů EU – směrnice a nařízení. V oblasti zajištění ochrany osobních údajů jsou dále použitelnými prameny práva soudní rozhodnutí SD EU, doporučení a stanoviska. Ačkoli doporučení a stanoviska nemají závaznou povahu, v oblasti ochrany osobních údajů se vyskytují často. Mohou být užita jako opora pro výklad a obsah práva.[58]

3.2.1 Směrnice 95/46/ES a další předpisy

V Evropské unii je pro ochranu osobních údajů stěžejní Směrnice 95/46/ES, která má působnost i v EHP. Vzhledem k tomu, že směrnice jakožto pramen práva s harmonizačním účelem, definujeme jako akt na cíl, kdy se závaznost směrnice týká jejího výsledku, nikoli celého rozsahu a doslovného znění,[59] pak cílem Směrnice 95/46/ES je ochrana práv a svobod osob v souvislosti se zpracováním osobních údajů. Při jeho naplňování vychází Směrnice 95/46/ES ze základních zásad, plynoucích z principů Úmluvy č. 108 a podstatně z ní čerpá. Úprava Směrnice 95/46/ES je však přísnější, neboť povinnosti členských států rozšiřuje a prohlubuje.[60] Jejím smyslem je nastolení rovnováhy mezi vysokou úrovní ochrany soukromí jednotlivce a zajištění volného pohybu osobních údajů mezi státy EHP.[61] Směrnice 95/46/ES dala vzniknout novému fenoménu pro členské země, když umožnila volný pohyb osobních údajů uvnitř své působnosti. Snaha EU v této oblasti je evidentní – prohlubovat

[57] Dodatkový protokol k Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat o orgánech dozoru a toku dat přes hranice ze dne 8. 11. 2001.
[58] BLAHOŽ, Josef, KLÍMA, Karel, SKÁLA, Josef a kol. *Ústavní právo Evropské unie*. 1. vydání. Dobrá Voda u Pelhřimova: Vydavatelství a nakladatelství Aleš Čeněk, 2003, s. 136 – 137.
[59] KLÍMA, Karel a kol. *Evropské právo*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2011, s. 119-120.
[60] DONÁT, Josef, TOMÍŠEK, Jan. *Právo v síti. Průvodce právem na internetu*. 1. vydání. Praha: C. H. Beck, 2016, s. 42.
[61] MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí.* 1. vydání. Praha: CZ.NIC, 2013, s. 62.

jednotný digitální trh.[62] Domnívám se, že pro internetová úložiště se jedná o zásadní skutečnost, neboť povaha cloudu, umožňující nahrávat data na servery lokalizované prakticky kdekoli, poté při odstranění hranic právních, tento volný pohyb umožnila v plném rozsahu. Jednotný vnitřní trh znamená propojení a sloučení národních trhů členských států EU do jednoho prostoru bez vnitřních hranic, který se řídí jednotnými pravidly a určitými zásadami.[63] Jedná se o prostor čtyř základních svobod.[64] Volný pohyb osobních údajů je komponentou, která rozvíjí svobodu pohybu osob. Osobní údaje, tak mohou být bez omezení převáděny uvnitř vnitřního trhu, mezi jednotlivými členskými státy.[65] Volný pohyb osobních údajů je umožněn díky harmonizaci právní úpravy. Od volného pohybu musíme odlišit transfer osobních údajů do tzv. třetích zemí, dle čl. 25 a násl. Směrnice 95/46/ES. Jedná se o přesun dat mimo EHP, který se řídí odlišnými pravidly.

Věcná působnost Směrnice 95/46/ES je vymezena v čl. 3 odst. 1 a odst. 2, dle něhož se úprava vztahuje na automatizované zpracování osobních údajů a na zpracování osobních údajů neautomatizované, pokud jsou údaje obsaženy v rejstříku nebo do něj mají být zařazeny. Vyloučena je z působnosti činnost spadající do oblasti společné zahraniční a bezpečností politiky, policejní a soudní spolupráce v trestních věcech, jakož i zpracování týkající se veřejné bezpečnosti, obrany bezpečnosti státu a jeho činnosti v oblasti trestního práva.[66] Poslední výjimkou je zpracování fyzickou osobou výlučně pro svou osobní potřebu. Nově se zde v čl. 8 odst. 1 vymezila zvláštní kategorie tzv. citlivých údajů.[67]

Mezi důležitá ustanovení Směrnice 95/46/ES patří povinnost správce a zpracovatele údajů informovat osobu, jíž se údaje týkají, o vymezených skutečnostech např. účel zpracování údajů, nebo sdělení příjemce údajů.[68] Subjekt údajů má pak právo na námitku proti zpracování údajů, stejně jako podrobit svou věc soudnímu přezkumu. Směrnice 95/46/ES zároveň vymezuje požadavky na zacházení s údaji, u něhož vyžaduje bezpečnostní standardy a zachování důvěrnosti. Členským státům nově vznikla povinnost zřídit ve smyslu čl. 28 Směrnice 95/46/ES dozorový orgán, jehož úkolem je výkon kontroly nad dodržováním předpisů, které směrnici provádí. V České republice je tímto orgánem Úřad se sídlem v Praze.

Evropsko-unijní legislativa v oblasti ochrany osobních údajů obsahuje i další předpisy. Tyto však netvoří obecný systematický rámec jako Směrnice 95/46/ES. Jedná se o zvláštní

[62] Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů – Uvolnění potenciálu cloud computingu v Evropě, KOM(2012) 059, září 2012, s. 6.
[63] ŠIŠKOVÁ, Naděžda a kol. *Evropské právo 2 – Jednotný vnitřní trh*. Praha: Wolters Kluwer ČR, 2012, s. 18.
[64] Čl. 26 odst. 2 SFEU.
[65] Bod (3) preambule Směrnice 95/46/ES.
[66] Hlava V. a VI. SEU.
[67] § 4 písm. b) OchOsÚ.
[68] Čl. 10 Směrnice 95/46/ES.

úpravu pro specifické oblasti, např. Směrnice č. 58. Členské státy však stále pomalu a někdy nesprávně transponují unijní směrnice. To se nevyhnulo ani oblasti ochrany osobních údajů, kde se objevují kritické hlasy ohledně nedůsledné harmonizace.[69] Chybějící harmonizaci označila samotná Komise za hlavní problém evropského rámce ochrany osobních údajů.[70] Pokud je zájem na rychlém překonání nedůsledné harmonizace, pak by tento problém mohl být vyřešen jediným způsobem – nařízením, jakožto unifikační formou pramene práva. Na podkladě reformy ochrany osobních údajů navržené Komisí byly zahájeny legislativní přípravy. Ty vyústily v přijetí GDPR, které zcela nahradí Směrnici 95/46/ES a v důsledku unifikačního charakteru též národní předpisy. S účinností od 25. 5. 2018 bude v celé EU účinný jeden obecný předpis pro ochranu osobních údajů. Předkládaná práce se však zaměřuje na současný stav účinné právní úpravy. Pro rozbor GDPR tak v této práci není prostor.

3.3 Vnitrostátní úprava České republiky

Vzhledem k tomu, že směrnice jsou primárně závazné toliko pro členské státy, je důležitá jejich řádná implementace v národních právních předpisech. V České republice je pro oblast ochrany osobních údajů základním předpisem OchOsÚ, který sic byl přijat v roce 2000, nicméně při jeho přípravách byly zapracovány evropské-unijní požadavky.[71] V oblasti ochrany osobních údajů se nicméně nerealizuje pouze OchOsÚ. Vyjma zmiňované Listiny, případně občanského zákoníku, dopadají na ochranu osobních údajů další předpisy. Jedná se však z větší části o úzce specializovanou materii. Z hlediska ochrany osobních údajů v informačním prostředí je významným předpisem ZNSIS, který upravuje podmínky při zasílání obchodních sdělení[72] a Úřadu zakládá v této oblasti působnost vykonávat dozor nad jeho dodržováním.[73] Dalšími předpisy, ve kterých nalezneme úpravu dotýkající se ochrany osobních údajů je např. zákon o policii České republiky[74], či zákon o občanských

[69] Např. KUNER, Christopher. *The „Internal Morality" of European Data Protection Law* [online]. SSRN.com, 24. listopadu 2008 [cit. 1. prosince 2016]. Dostupné na <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1443797>, s. 17.
[70] Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů – Komplexní přístup k ochraně osobních údajů v Evropské unii, KOM(2010) 609, listopad 2010, s. 10.
[71] Podobně i J. Matejka uvádí k OchOsÚ, že v dané oblasti se jedná o „*aplikačně nejvýznamnější právní předpis*". Viz MATEJKA: *Internet jako objekt práva*…, s.75.
[72] § 7 odst. 3 ZNSIS.
[73] § 10 odst. 1 písm. a) ZNSIS.
[74] § 65 odst. 5 zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.

průkazech[75]. Nesmíme taktéž zapomenout na skutkovou podstatu neoprávněného nakládání s osobními údaji ve smyslu § 180 TZ.

Je tak evidentní, že mimo obecný předpis OchOsÚ, je oblast ochrany osobních údajů po částech roztroušena do dalších zákonů. V tomto kontextu je nezbytné říct, že žádný z nich neupravuje otázky *cloud computingu*. Na tuto oblast tak nejvíce dopadají ustanovení OchOsÚ, u kterého v souvislosti s *cloudem* uvedu základní ustanovení dopadající na řešenou problematiku.

3.3.1 Zákon o ochraně osobních údajů

Ke správné aplikaci jeho ustanovení je vhodné si nejprve říci, k čemu z právního pohledu při poskytování cloudových služeb dochází. V podstatě se jedná o provozování služby, kdy uživatel svá data předává jiné osobě, která (běžně za úplatu) tyto údaje uchovává v datovém centru. Upozorňuji, že se jedná o zjednodušené vymezení, avšak na jeho podkladě lze snadno rozklíčovat hlavní komponenty daného vztahu, které je třeba analyzovat směrem k celé úpravě. Jedná se tedy o následující: předmět ochrany, jaké subjekty jsou oprávněny s osobními údaji nakládat; obsah práv a povinností, tj. především podmínky řádného nakládání s údaji; odpovědnostní vztahy a v neposlední řadě, určení rozhodného práva v případě mezinárodního transferu. Jedná se o klíčové aspekty celého právního vztahu. Podkapitola nemá sloužit jako souhrnný popis právní úpravy. Smyslem je přiblížit základní právní úpravu dopadající na nakládání s osobními údaji při užívání internetových úložišť a dalších služeb cloudové povahy. Podkapitola má představit základní právní vztahy vyskytujícími se při poskytování cloudových služeb.

Uživatel úložiště předává jeho provozovateli data různého druhu. Ne všechna jsou způsobilá právní ochrany. Dle § 4 písm. a) OchOsÚ je osobním údajem jen informace týkající se určeného nebo určitelného subjektu údajů, přičemž tento se považuje za určený nebo určitelný pokud ho lze „*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*“[76]. Je nezbytné říci, že osobou, k níž se osobní údaj váže, může být jen osoba fyzická. Taková osoba je označována jako subjekt údajů.[77] Z definice vyplývá, že k tomu, aby informace byla osobním údajem, musí vykazovat kvalifikovanou vlastnost, a to *určitelnost* ve vztahu k subjektu údajů. Určitelnost znamená, že

[75] § 16a odst. 1 písm. p) zákona č. 328/1999 Sb., o občanských průkazech, ve znění pozdějších předpisů.
[76] § 4 písm. a) OchOsÚ.
[77] § 4 písm. d) OchOsÚ.

na základě dané informace lze určit konkrétní osobu,[78] přičemž pro zhodnocení, zda na základě informace je osoba identifikovatelná, je nutné posuzovat všechny prostředky, které lze k identifikaci osoby rozumně využít.[79] V této souvislosti je mimořádně důležité zmínit, že určitelnost se neposuzuje objektivně, tj. optikou každého, zda na základě údaje může identifikovat člověka. Pro aplikace právní úpravy postačí, zda osoba určitelná pro toho, kdo s údaji disponuje.[80] Pokud tedy např. zaměstnavatel své zaměstnance označí zaměstnaneckým číslem, přičemž číslo následně zanese do své účetní databáze, a to spolu se jménem, bydlištěm a mzdovými údaji zaměstnance, pak se i ve vztahu k onomu číselnému označení zaměstnance jedná o osobní údaj. Zaměstnavatel má totiž možnost na základě takových údajů jednoznačně určit osobu vedenou pod daným číslem. Osobními údaji tedy může být i skupina informací, ve které sic každá jednotlivá informace sama o sobě k určení osoby nevede, avšak všechny informace ve svém souhrnu ano.[81]

Dostáváme se k dalšímu stěžejnímu prvku, a tím je určení subjektů, které jsou zapojeni v procesu zacházení s osobními údaji. Z pohledu § 4 písm. j) OchOsÚ se osoba stává *správcem* osobních údajů jestliže „*určuje účel a prostředky zpracování*“.[82] Správce je subjekt, který má primární odpovědnost za dodržování povinností z ochrany osobních údajů. Patří mezi hlavní subjekty problematiky. Jeho definičním znakem je schopnost určovat účel zpracování údajů, přičemž tímto účelem je třeba rozumět cíl (důvod), s jakým se zpracování údajů provádí.[83] Využijme uvedený příklad zaměstnavatele a osobních údajů zaměstnanců. Zaměstnavatel se stává správcem údajů, neboť určuje účel jejich zpracování, jímž je vedení účetní agendy. Správce je definován také tím, že určuje i prostředky zpracování, čímž se rozumí volba technického procesu, jakým budou údaje zpracovány.[84] Typickým prostředkem může být elektronické zpracovávání v podobě nahrávání databáze údajů na cloudové úložiště. Pokud správce provádí sám zpracování údajů, pak za tuto činnost nese plnou odpovědnost. Správce však není povinen zpracování činit pouze sám. OchOsÚ umožňuje, aby zpracování prováděla místo správce jiná osoba. Zde se pak přidává další subjekt, kterého OchOsÚ označuj za *zpracovatele*. Zpracovatel je dle § 4 písm. k) OchOsÚ každý subjekt, který buď dle zvláštního zákona nebo na základě pověření správce, zpracovává osobní údaje. Zpracování osobních údajů je vymezeno jako jakákoliv operace či soustava operací, které

[78] MATEJKA: *Internet jako objekt práva...,* s. 87.
[79] Bod (26) preambule Směrnice 95/46/ES.
[80] NONNEMANN, František. In KUČEROVÁ, Alena a kol. *Zákon o ochraně osobních údajů. Komentář*. 1. vydání. Praha: C. H. Beck, 2012, s. 52 (§ 4).
[81] MAŠTALKA: *Osobní údaje, právo a my*…, s. 15.
[82] Srov. § 4 písm. j) OchOsÚ.
[83] NONNEMANN, František. In KUČEROVÁ, Alena a kol. *Zákon o ochraně osobních údajů...,* s. 78 (§ 4).
[84] Tamtéž, s. 79.

správce nebo zpracovatel systematicky provádí s osobními údaji, a to automatizovaně nebo jinými prostředky. Automatizované zpracovaní je třeba chápat jako zpracování za pomocí výpočetní techniky.[85] Neautomatizované zpracování se pak *a contrario* provádí za pomocí jiných, než výpočetních prostředků, např. běžná papírová kartotéka. Demonstrativním výčtem zákon uvádí, které činnosti se považují za zpracování údajů. Jedná se typicky o jejich shromažďování, ukládání na nosiče informací či další dispozice v podobě předávání jiným subjektům.

V České republice vznikla zajímavá diskuze, zda se v případě poskytovatele *cloudu* vůbec jedná o zpracovatele osobních údajů. Úřad nejdříve zastával stanovisko, že pokud provozovatel svým zákazníkům jen „pronajímá" datové úložiště (poskytuje infrastrukturu) a nespadá pod definici zpracovatele.[86] Dle Úřadu v takovém případě chybí prvek nakládání s osobními údaji. Třeba dodat, že v evropském prostředí nebyl tento názor obecně sdílen jinými národními dozorovými orgány v oblasti ochrany osobních údajů.[87] Následně se k otázce vymezení pojmů správce a zpracovatele v prostředí *cloud computingu* vyjádřila PS 29 ve stanovisku, ze kterého plyne, že postavení provozovatele *cloud computingu* zásadně spadá pod definici zpracovatele, pouze s určitými výjimkami, kdy lze o poskytovateli hovořit jako o správci.[88] Patrně pod vlivem stanoviska PS 29 a v zájmu harmonizace, vydal posléze Úřad stanovisko, kde svůj dosavadní přístup změnil. Přiklonil se k výkladu sdíleného napříč členskými státy EU, tj. že poskytovatel cloudových služeb je zpracovatelem údajů. [89] Právní vztah správce a zpracovatele musí splňovat určité náležitosti. Správce je dle § 6 OchOsÚ povinen se zpracovatelem uzavřít smlouvu o zpracování osobních údajů (dále jen „zpracovatelská smlouva") přičemž se vyžaduje obligatorní splnění minimálních obsahových náležitostí.

V § 27 OchOsÚ je upraveno předávání osobních údajů do zahraničí. Vzhledem k celkovému charakteru cloudové technologie je běžné, že osobní údaje „cestují"

[85] Stanovisko Úřadu pro ochranu osobních údajů – Zveřejňování osobních údajů na internetu, č. 13/2012, březen 2012 (aktualizace únor 2014), s. 1.
[86] Úřad pro ochranu osobních údajů. *Zpracování osobních údajů na základě smluv zavíraných se zpracovateli (tzv. řetězení zpracovatelů osobních údajů)*. uoou.cz, [cit. 1. prosince 2016]. Dostupné na <https://www.uoou.cz/files/stanovisko_2009_1.pdf>, s. 2.
[87] KOLÁRIKOVÁ, Lenka. Největší záhada cloudu: jde o zpracování osobních údajů či nikoli? *Právní rádce*, 2012, roč. 20, č. 9, s. 27.
[88] Pracovní skupina pro ochranu údajů. *Stanovisko č. 05/2012 ke cloud computingu* [online]. uoou.cz, [cit. 15. prosince 2016]. Dostupné na <https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=16709>, s. 8.
[89] Úřad pro ochranu osobních údajů. *K právní ochraně osobních údajů při jejich předávání v rámci cloudových služeb* [online]. uoou.cz, [cit. 28. prosince 2016]. Dostupné na <https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=3002>, s. 3.

z domovského státu subjektu údajů na servery provozovatele služby, které jsou v zahraniční.[90] Poskytovatel *cloudu* může mít dokonce více datových center deponovaných různě po světě a údaje mezi nimi mohou tzv. „migrovat“. Zákonodárce si je patrně vědom, že při takovém nakládání s osobními údaji mohou vznikat nepřehledné situace, a proto problematiku výslovně upravil. Hlavní zásadou § 27 odst. 1 OchOsÚ je volný pohyb osobních údajů v rámci EHP. Ten je umožněn na základě skutečnosti, že členské státy implementovaly do národních právních řádů Směrnici 95/46/ES. V členských státech by tak měl být zajištěn jednotný standard ochrany.[91] Předávání osobních údajů mimo EHP se označuje jako předávání do tzv. *třetích* zemí. Režim předávání údajů do třetích zemí lze uskutečnit několika způsoby. Jedná se např. o předání (i) se souhlasem subjektu údajů, (ii) na základě mezinárodní smlouvy, (iii) na základě rozhodnutí orgánu EU nebo na základě povolení Úřadu, nebo (iv) jsou-li v třetí zemi dostatečné záruky pro ochranu osobních údajů.[92]

[90] KOPEČKOVÁ, Andrea. *K povinnostem souvisejícím se zpracováním osobních údajů v cloudu* [online]. epravo.cz, 20. listopadu 2015 [cit. 22. ledna 2017]. Dostupné na <http://www.epravo.cz/top/clanky/k-povinnostem-souvisejicim-se-zpracovavanim-osobnich-udaju-v-cloudu-98984.html>.
[91] Úřad pro ochranu osobních údajů. *Stanovisko č. 2/2010 – Předání osobních údajů do jiných států* [online]. uoou.cz, listopad 2010 [cit. 28. prosince 2016]. Dostupné na <https://www.uoou.cz/files/stanovisko_2010_2.pdf>, s. 2.
[92] § 27 odst. 2; odst. 3 OchOsÚ.

4 Analýza vybraných problémů

Za zajištění bezpečnosti osobních údajů při poskytování cloudových služeb odpovídá správce, případně pověřený zpracovatel.[93] Kapitola se věnuje právní úpravě regulující práva a povinnosti mezi těmito osobami.

4.1 Smluvní úprava poměru správce - zpracovatel

Pověří-li správce zpracováním osobních údajů zpracovatele, musí jejich právní poměr splňovat určité zákonné požadavky. Předně se jedná o povinnost uzavřít smlouvu o zpracování osobních údajů (tzv. zpracovatelská smlouva) dle § 6 OchOsÚ. Smlouva vymezí práva a povinnosti smluvních stran pro zpracování osobních údajů. Jde o základní právní dokument mezi správcem a zpracovatelem.[94] Mimo požadavek na písemnou formu, určuje zákon minimální obsahové náležitosti. Zpracovatelská smlouva musí vymezit rozsah a účel zpracování, časové období na jak dlouho se uzavírá. Dále musí obsahovat prohlášení zpracovatele o zárukách technického a organizačního zabezpečení osobních údajů. Zákon v § 6 OchOsÚ uvádí, že smlouva obsahuje *„zejména“* uvedené náležitosti. Jedná se o demonstrativní výčet. Je proto na smluvních stranách, zda si ujednají další práva a povinnosti např. proces migrace dat při případném přechodu správce na jiný informační systém.

Ve druhé kapitole jsem hovořil o vzájemném vztahu ochrany osobních údajů a ochrany osobnosti. Přestože jsem zmínil, že nelze tyto dvě koncepce zaměňovat, je třeba brát v potaz, že uvedené se vztahuje pro oblasti, na které každá z uvedených institucí dopadá. Neznamená to však, že by ustanovení občanského zákoníku byla vyloučena pro subsidiární aplikaci na právní vztahy vznikající v procesu nakládání s osobními údaji. Domnívám se totiž, že ačkoli je OchOsÚ veřejnoprávním předpisem, pak v otázkách zde neupravených, se subsidiárně užijí ustanovení občanského zákoníku, neboť OchOsÚ dopadá do soukromoprávních vztahů a otevírá zde jisté otázky, které je možné vyřešit toliko aplikací norem občanského zákoníku.

[93] § 13 OchOsÚ.
[94] FOLDOVÁ, Vanda. In KUČEROVÁ, Alena a kol. *Zákon o ochraně osobních údajů*…, s. 175 (§ 6).

4.1.1 Platnost zpracovatelské smlouvy

Zpracovatelskou smlouvu lze označit jako smlouvu typovou ve smyslu § 1746 o. z., neboť její podstatné náležitosti jsou stanoveny zákonem. Pokud by snad strany v domnění, že uzavřely zpracovatelskou smlouvu, neujednaly některou z uvedených náležitostí, nejednalo by se o neplatnou smlouvu, když takový následek není v OchOsÚ uveden a nevyplývá ani z podpůrného užití ustanovení[95] občanského zákoníku o neplatnosti právních jednání. Mám za to, že by se v takovém případě jednalo o smlouvu nepojmenovanou. Smlouva by strany zavazovala z hlediska jejich soukromoprávního závazku. Kterákoli strana by tak mohla při porušení smluvní povinnosti uplatnit nárok na náhradu škody dle § 2913 o. z. Zároveň by ale správce mohl nést správní odpovědnost za porušení povinnosti stanovené v § 13 OchOsÚ, dle něhož je povinen přijmout nezbytná bezpečnostní opatření.[96]

OchOsÚ však neupravuje následky situace, kdy smluvní strany nedodrží předepsanou písemnou formu zpracovatelské smlouvy. Nedodržení zákonné formy je ve smyslu § 582 odst. 1 o. z. sankcionováno neplatností. Doktrína tradičně rozlišuje mezi neplatností relativní a absolutní.[97] Je nezbytné se proto dále zabývat otázkou, o jaký druh neplatnosti se při nedodržení formy zpracovatelské smlouvy jedná. Handlar uvádí, že není možné, v závislosti na nedodržení zákonné formy, jednoznačně stanovit, zda se vždy jedná pouze o neplatnost relativní či absolutní. K určení druhu neplatnosti je totiž nezbytné zkoumat smysl a účel porušené normy.[98] Ustanovení § 582 o. z. bylo zároveň v nedávné době podrobeno soudnímu přezkumu. Nejvyšší soud se zabýval otázkou, v jaké formě má být udělena plná moc v případě zmocnění osoby pro zastoupení k založení obchodní společnosti. V rámci svého odůvodnění soud mj. uvedl, že „*Právní jednání odporující zákonu je neplatné pouze tehdy, vyžaduje-li to smysl a účel zákona (§ 580 odst. 1 OZ). Uvedené omezení platí i pro posouzení důsledků nedodržení formy právního jednání vyžadované zákonem (§ 582 odst. 1 OZ).*".[99] Nejvyšší soud tak při výkladu zákona šel ještě dále, když jinými slovy řekl, že v případě, kdy právní jednání není učiněno v zákonné formě, je otázkou, zda vůbec se jedná o neplatnost, a to v závislosti na zkoumání smyslu a účelu porušené normy. Uvedené závěry lze aplikovat na § 6 OchOsÚ. Zda byla zpracovatelská smlouva uzavřena platně, případně, o jaký druh neplatnosti se jedná, jsou otázky důležité pro subjekt údajů, neboť zpracovatelská

[95] Viz § 580 a násl. o. z.
[96] FOLDOVÁ, Vanda. In KUČEROVÁ, Alena a kol. *Zákon o ochraně osobních údajů*…, s. 176 (§ 6).
[97] K rozlišení relativní a absolutní neplatností blíže viz např. SPÁČIL, Jiří. Některé sporné otázky relativní neplatnosti v novém občanském zákoníku. *Právní rozhledy*, 2014, roč. 22, č. 5, s. 172 – 177.
[98] HANDLAR, Jiří. In LAVICKÝ, Petr a kol. *Občanský zákoník I. Obecná část (§ 1−654). Komentář.* 1. vydání. Praha: C. H. Beck, 2014, s. 2097 (§ 582).
[99] Usnesení Nejvyššího soudu ze dne 27. listopadu 2014, sp. zn. 29 Cdo 3919/2014.

smlouva může převést některé povinnosti na zpracovatele, které je zpracovatel povinen vůči subjektu údajů splnit. Přesto však OchOsÚ odpověď neposkytuje. Problematika je o to závažnější, neboť pokud by snad došlo k neplatnému uzavření zpracovatelské smlouvy, mohl by být subjekt údajů v nejistotě o tom, kdo je vůči němu povinen řádně plnit povinnosti[100] stanovené v OchOsÚ, příp. vůči komu má směřovat své požadavky[101].

Důvodová zpráva k § 6 OchOsÚ uvádí, že písemná forma zpracovatelské smlouvy je zavedena „*V zájmu právní jistoty nejen správce a zpracovatele, ale i subjektů údajů a dalších osob (...)*.“[102]. Mám za to, že samotná povinnost uzavřít zpracovatelskou smlouvu tak má za cíl ochranu subjektu údajů. Pokud je totiž dána možnost, aby se souhlasem správce nakládala s osobními údaji další osoba, pak je třeba tento vztah zprůhlednit, a to za účelem zřetelného rozložení práv a povinností, vymezení mantinelů pro zákonné zpracování a určení odpovědnostních vztahů. Transparentnosti lze dosáhnout pokud se právní poměr mezi správcem a zpracovatelem bude uskutečňovat jen na podkladě písemné smlouvy. Takový závěr podporuje i stanovisko PS 29, která ve vztahu k čl. 17 Směrnice 95/46/ES (z něhož požadavek uzavřít zpracovatelskou smlouvu vyvěrá) uvádí, že zpracovatelská smlouva se požaduje s ohledem na zajištění bezpečnosti zpracování a zachování důkazů pro případ porušení zákonných povinností.[103] Požadavek uzavřít zpracovatelskou smlouvu resp. požadavek přísnější formy jejího uzavření tak má zabránit situacím, které D. Novák popisuje jako „(…) *optimalizace procesů zpracování údajů tak, že se sníží riziko, že bude vůbec někdo volán k odpovědnosti (pokud není možné spolehlivě stanovit, kdo je správce a kdo zpracovatel, pak logicky nelze ani stanovit, kdo nese jaké povinnosti).*“[104] Lze uzavřít, že účelem požadavku písemné formy ve smyslu § 6 OchOsÚ je zajištění právní jistoty a ochrany subjektu údajů. Na základě uvedeného se tak domnívám, že nedodržení písemné formy má s ohledem na smysl a účel § 6 OchOsÚ za následek neplatnost zpracovatelské smlouvy. Je nezbytné vyřešit otázku, o jaký druh neplatnosti se jedná. Připomeňme, že relativní neplatnost je třeba namítnout. V opačném případě se právní jednání považuje za platné.[105] Relativní neplatnost je oprávněna namítat *jen* osoba, které je neplatnost právního

[100] Příkladem povinnosti vůči subjektu údajů je poskytnutí informací dle § 11 OchOsÚ. Povinnost může dle § 11 odst. 7 OchOsÚ splnit i zpracovatel.
[101] Viz práva stanovená v § 21 OchOsÚ – např. právo požadovat vysvětlení.
[102] Důvodová zpráva k návrhu zákona o ochraně osobních údajů a o změně některých zákonů ze dne 22. 9. 1999.
[103] Pracovní skupina pro ochranu údajů. *Stanovisko č. 1/2010 k pojmům „správce“ a „zpracovatel“* [online]. ec.europa.eu, [cit. 3. ledna 2017]. Dostupné na <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_cs.pdf>, s. 25.
[104] NOVÁK, Daniel. In NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související. Komentář*. 1. vydání. Praha: Wolters Kluwer ČR, 2014, s. 174 (§ 6).
[105] § 588 odst. 2 o. z.

jednání stanovena na ochranu jejích zájmů.[106] Ze zvláštní povahy § 6 OchOsÚ resp. povahy cloudové služby a s přihlédnutím ke smyslu koncepce ochrany osobních údajů, plyne, že v takovém případě mohou namítat neplatnost tři subjekty – správce, zpracovatel a subjekt údajů, když lze dovodit, že požadavek písemné formy zpracovatelské smlouvy může být k ochraně všech těchto subjektů. Na tom nic nemění fakt, že z charakteru koncepce ochrany osobních údajů je evidentní, že hlavním „beneficientem" je subjekt údajů. Správce a zpracovatel mohou namítat neplatnost z titulu svého postavení smluvní strany. Problém však spatřuji ve skutečnosti, že subjekt údajů mnohdy nemá přístup ke znění zpracovatelské smlouvy. Občanský zákoník by tak subjektu údajů přiznával právo namítat neplatnost smlouvy z důvodu nedodržení její formy, avšak předpisy na ochranu osobních údajů, ani subsidiárně občanský zákoník, by neobsahovaly úpravu, která by poskytovala subjektu údajů nástroj, jímž by mohl ověřit, zda správce splnil povinnost mu plynoucí z § 6 OchOsÚ. Správce je toliko povinen informovat subjekt údajů o tom, kdo a jakým způsobem osobní údaje zpracovává.[107] Povinnost je však formulována tak, že nelze dovodit oprávnění subjektu údajů nahlížet do zpracovatelské smlouvy. Domnívám se tak, že relativní neplatnost by popřela smysl a účel povinnosti uzavřít zpracovatelskou smlouvy v písemné formě, neboť jaký smysl by mělo chránit subjekt údajů nástrojem relativní neplatnosti smlouvy, pokud by právní úprava subjektu údajů neposkytovala žádný prostředek, jakým by mohl takovou povinnost správce kontrolovat? Naopak pro tvrzení, že jde o neplatnost absolutní svědčí fakt, že smyslem celé koncepce je ochrana soukromí. Jedná se tak o ochranu základního lidského práva, potažmo osobnostních práv přirozené povahy. Jakýkoliv zásah do takovýchto práv je poté v rozporu s veřejným pořádkem. Podobně se k intenzitě zásahu do práva na soukromí vyjádřil také P. Mates.[108] Pokud zásah naplňuje intenzitu porušení veřejného pořádku, pak je naplněna skutková podstata § 588 o. z., v němž je zakotvena absolutní neplatnost právního jednání. Domnívám se proto, že s ohledem na výše popsaný smysl a účel normy plynoucí z § 6 OchOsÚ a intenzity zásahu při jejím porušení, je nedodržení písemné formy zpracovatelské smlouvy stiženo absolutní neplatností.

Na tomto místě bych zároveň rád poukázal na nedůslednou transpozici evropsko-unijní legislativy. Jak bylo shora uvedeno, zpracovatelská smlouva dle § 6 OchOsÚ má původ v čl. 17 Směrnice 95/46/ES. Zmíněný článek v odstavci 3 oproti OchOsÚ navíc výslovně určuje, že zpracovatelská smlouva musí obsahovat závazek zpracovatel jednat pouze

[106] § 588 odst. 1 o. z.
[107] § 11 odst. 1 OchOsÚ.
[108] Viz MATES: *K některým otázkám ochrany soukromí...*, s. 369.

dle pokynů správce. Absence takovéto úpravy pak může mít za následek další oslabení ochrany subjektu údajů, když zejména v prostředí poskytovatelů služeb, nabízených prostřednictvím internetu, dochází k využívání cloudové technologie, kdy za účelem efektivního hospodaření nezřídka dochází k participaci více zpracovatelů na zpracování údajů (k řetězení zpracovatelů viz níže). Pokud správce údajů nemá zákonnou povinnost zavázat zpracovatelské subjekty, aby jednaly pouze na základě jeho pokynů, může ve složitějších řetězcích docházet při procesu zpracování údajů k nejasnostem ohledně vázanosti pokyny a z toho plynoucí nejistoty odpovědnosti pro případ porušení předpisů na ochranu osobních údajů. Mám za to, že výslovné stanovení povinnosti vázanosti pokynů správce může přinejmenším působit preventivně a předcházet porušování ujednaných bezpečnostních opatření. Nyní tak zůstává zcela dobrovolně na správci, zda takovouto povinnost zanese do zpracovatelské smlouvy. Pokud tak ale neučiní, nelze mu jeho chybějící iniciativu klást k tíži. V tomto ohledu je česká právní úprava méně přísná, než unijní, což v konkrétním případě může opět vést k nižší úrovni ochrany subjektů údajů.

4.1.2 Záruky zpracovatele

V § 6 OchOsÚ je vznesen požadavek, aby zpracovatelská smlouva obsahovala záruky zpracovatele o technickém a organizačním zabezpečení osobních údajů. Zákon, ani jeho prováděcí předpisy, ale blíže neurčují, jaké záruky mají být zajištěny. Terminologická neurčitost je o to více problematická, když správce a zpracovatel mají odpovědnost za přijetí bezpečnostních opatření dle § 13 OchOsÚ. Jediným vodítkem může být toliko konstatování v cit. ustanovení, že opatření mají zamezit neoprávněnému nebo nahodilému přístupu k osobním údajům či jejich zneužití. Nastíněný problém byl řešen i před Nejvyšším správním soudem, který podpořil následující tvrzení: *„(...) v oblasti bezpečnostních opatření k ochraně majetku obecně a při nakládání s osobními údaji, resp. jejich ochraně zvláště, určitý soubor bezpečnostních opatření považovaný za standard, aniž by musel být v zákoně výslovně vymezen“* a dále dodal, že *„Jisté skouposti zákonodárce při formulaci tohoto ustanovení* (§ 13 OchOsÚ, pozn. aut.) *zákona ve srovnání s textem směrnice lze jistě litovat a Nejvyšší správní soud připouští, že užitá dikce klade na správce a zpracovatele v jistém smyslu vyšší nároky, když způsob a prostředky zabezpečení osobních údajů ponechává na jednu stranu jejich vlastní úvaze, na druhou stranu za nesplnění předmětné povinnosti hrozí poměrně vysokými sankcemi.*[109] Pokud se Nejvyšší správní soud odvolává na „běžné standardy“, pak

[109] Rozsudek Nejvyššího správního soudu ze dne 10. května 2006, sp. zn. 3 As 21/2005.

mu sic lze dát zapravdu, že některé, zejm. nadnárodní, společnosti vytváří v daném segmentu bezpečnostní standard, který se díky konkurenčnímu prostředí udržuje i v jiných obchodních společnostech, nicméně takovéto „standardy“ nemají právní závaznost.[110] Navíc hranice uvedených standardů se logicky v čase posunuje stále výše, když prostředí technologických společností je silně inovativní a bezpečnostní opatření se kontinuálně posunují ve prospěch uživatelů. Pokud bychom přistoupili na argumentaci rozhodnutí, pak se s technologickým vývojem zároveň posouvá i hranice odpovědnosti za dodržení bezpečnostních opatření. Je tedy otázkou, zda takto nastavené prostředí právní nejistoty, vedeno sic snahou zajistit subjektům údajů, co největší ochranu, nepovede paradoxně ke snížení míry ochrany, když se poskytovatelé budou snažit „optimalizovat“ postupy a vyhnout se případné odpovědnosti. Nejvyšší správní soud hájí absenci určení standardů v liteře zákona s odůvodněním, že prostředí výpočetních technologií je velmi rychle se měnící oblastí a nové sofistikovanější hrozby překonávající dosavadní bezpečnostní opatření se zde objevují prakticky denně. Nejvyšší správní soud se tak snaží přimět poskytovatele služeb dodržovat bdělost, stále prověřovat možné hrozby a přizpůsobovat zabezpečení. Takovému postupu nelze upřít ratio, nicméně druhým protipólem je, pokud právní úprava zůstane na slovo zcela skoupá a nechá tak adresáty zákonné normy v nepřiměřené právní nejistotě. Domnívám se, že vhodným řešením by mohl být kompromis, kdy se určí obecné prvky, které je nezbytné zabezpečit, zanesou do právní úpravy. Samotné prostředky poté již budou na správcích či zpracovatelích. Uvedené řešení na jedné straně neponechává správce v právní nejistotě, jaké povinnosti vůbec má plnit, ale zároveň se nejedná o rigidní úpravu, která by se časem stala obsoletní. Takovýto postup můžeme vidět např. v úpravě německého Spolkového zákona na ochranu dat.[111] [112]

Ačkoli by zpracovatelská smlouva měla sloužit jako nástroj transparentnosti a zajištění náležitého zacházení s osobními údaji s cílem chránit subjekty osobních údajů, je s ohledem na výše řečené zřejmé, že její zakotvení v OchOsÚ uvedený účel nedosahuje v plném rozsahu. Výsledkem může být naopak oslabení postavení subjektů údajů.

4.2 Řetězení zpracovatelů

V případě zpracování osobních údajů v cloudovém prostředí vyvstává další otázka, a sice zda je přípustné v řetězci osob nakládajících s osobními údaji, aby na straně

[110] Např. standardy Mezinárodní organizace pro normalizaci ISO/IEC 27017:2015.
[111] § 9 a příloha k § 9 věta 1. Spolkového zákona na ochranu dat z 20. prosince 1990 (BGBl I 1990, s. 2954). Úplné znění zákona je dostupné též na adrese https://www.gesetze-im-internet.de/bdsg_1990/.
[112] NOVÁK, Daniel. In NOVÁK, Daniel. *Zákon o ochraně osobních údajů...,* s. 222 (§ 13).

zpracovatelů působilo více subjektů. Nejedná se o situaci v praxi nijak ojedinělou. Je běžné, že cloudová služba poskytována jedním dodavatelem, se skládá z kombinace služeb od většího počtu různých dodavatelů (subdodavatelů).[113] Zmíněný problém řetězení subjektů a absence jeho právní úpravy kritizuje i Kuner. Ten uvádí, že zpracovatel běžně poskytuje údaje jinému zpracovateli, např. v situaci, kdy další subjekt provádí pro zpracovatele servisní údržbu jeho databází. Pokud právní řád na tuto situaci nepamatuje (viz níže analyzovaná situace), pak násobné předávání údajů zůstává v právním vakuu.[114] Takový případ nastává i v prostředí české právní úpravy. Domnívám se však, že je možné takovou neúplnost zákona překlenout pomocí *analogie legis*, tj. nástrojem pro dotváření práva[115].

Úřad se k otázce násobného zapojení zpracovatelů staví negativně a jakékoli jejich řetězení nepřipouští.[116] V literatuře se zato můžeme setkat s o něco smířlivějším postojem, kdy řetězení zpracovatelů není považováno za zakázané, ale toliko za „*nežádoucí*".[117] Proti těmto názorům naopak stojí stanovisko PS 29, dle něhož řetězení zpracovatelů je připuštěno.[118] PS 29 upozorňuje, že takové řetězení je náročné z hlediska určení odpovědnosti jednotlivých článků. Je tak nezbytné řádně upravit povinnosti těchto subdodavatelů ve vztahu ke zpracovateli a správci údajů.[119]

Za povšimnutí stojí, že Úřad vylučuje jakékoli řetězení zpracovatelů, dodává ale, že může dojít ke zpracování osobních údajů dalšími osobami (odlišnými od správce a zpracovatele). Přesto se dle jeho názoru bude jednat o činnost v souladu s OchOsÚ. Úřad zde vychází z § 14 OchOsÚ, které připouští zpracování údajů zaměstnanci správce či zpracovatele, nebo třetími osobami na základě smlouvy.[120] Výklad Úřadu má však negativní důsledky. Pokud totiž není možné řetězení zpracovatelů, avšak je zároveň připuštěno, aby se jiné osoby podílely na zpracování osobních údajů, je evidentní, že tyto

---

[113] Pracovní skupina pro ochranu údajů. *Stanovisko č. 05/2012 ke cloud computingu* [online]. uoou.cz, [cit. 6. ledna 2017]. Dostupné na <https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=16709>, s. 6.

[114] KUNER, Christopher. *The „Internal Morality" of European Data Protection Law* [online]. SSRN.com, 24. listopadu 2008 [cit. 6. ledna 2017]. Dostupné na <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1443797>, s. 11.

[115] K metodám nalézání práva viz MELZER, Filip. *Metodologie nalézání práva. Úvod do právní argumentace*. 2. vydání. Praha: C. H. Beck, 2011, s. 223 – 230.

[116] Úřad pro ochranu osobních údajů. *Zpracování osobních údajů na základě smluv zavíraných se zpracovateli (tzv. řetězení zpracovatelů osobních údajů)*. uoou.cz, [cit. 1. prosince 2016]. Dostupné na <https://www.uoou.cz/files/stanovisko_2009_1.pdf>, s. 2.

[117] KUČEROVÁ, Alena, NONNEMANN, František. *Ochrana osobních údajů v praktických příkladech*. 1. vydání. Praha: BOVA POLYGON, 2013, s. 35.

[118] Pracovní skupina pro ochranu údajů. *Stanovisko č. 05/2012 ke cloud computingu* [online]. uoou.cz, [cit. 15. prosince 2016]. Dostupné na <https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=16709>, s. 13.

[119] Tamtéž.

[120] § 14 OchOsÚ.

osoby nemají postavení zpracovatele. Úřad se zde patrně snaží zamezit „dělení“ odpovědnosti na další osoby se záměrem ponechat odpovědnost na správci a zpracovateli. Co se však stane v případě, kdy onen další quasi-zpracovatel v řetězci zapříčiní neoprávněný únik osobních údajů?

Mám za to, že Úřad si je problematiky řetězení zpracovatelů vědom, avšak pro její řešení zvolil nešťastnou metodu, a sice považovat takové jednání za zakázané. Nevhodnost řešení spatřuji v tom, že pokud by naopak Úřad quasi-zpracovatelským subjektům přiznal, v souladu s výkladem PS 29, postavení zpracovatele, nesl by pak ex lege odpovědnost za zajištění bezpečnosti údajů. Výklad Úřadu se jeví nesystematický s ohledem na samotný § 14 OchOsÚ, který připouští další osoby v řetězci zpracování osobních údajů. Zákon však již k těmto osobám neuvádí, jaké mají postavení z hlediska nakládání s osobními údaji a za jaké jednání, nebo zda vůbec, jsou odpovědny. Vzniká tak mezera v právní úpravě. Domnívám se, že zmíněnou neúplnost zákona lze překlenout pomocí analogie, když na jednání takovýchto osob užijeme pravidla vztahující se na zpracovatele. Pokud takový subjekt zpracovává osobní údaje, splňuje totiž podmínky § 4 písm. k) OchOsÚ, vymezující osobu zpracovatele, a to s jedinou odlišností týkající se pověření správce. Z § 14 OchOsÚ totiž plyne, že pověření quasi-zpracovatele může vycházet i jen od zpracovatele. Správce údajů v tomto ohledu tak nemusí mít vědomost o činnosti subdodavatelů. Pokud tedy zpracovatel zajišťuje plnění pro správce formou subdodavatelských dodávek od dalšího subjektu, pak se na činnost této třetí osoby analogicky použijí zákonná ustanovení zpracovatele pro dodržování náležité ochrany údajů. Jsem si vědom, že nastíněné řešení rozšiřuje odpovědnost na další subjekty, a to v rozporu s textem OchOsÚ, avšak se domnívám, že takové dotváření práva je plně v souladu se smyslem a účelem právní úpravy a je přiléhavější, než Úřadem zvolený způsob řešení.

Je zřejmé, že § 14 OchOsÚ reflektuje praxi při zpracovávání osobních údajů, kdy se za účelem snížení nákladů dělí služby na menší celky, které se zajišťují subdodavatelsky. Nicméně § 14 OchOsÚ neupravuje povinnosti subdodavatelů. Domnívám se, že problém nastává ve chvíli, kdy OchOsÚ staví naroveň zaměstnance zpracovatele a osoby, které vykonávají subdodavatelské práce na základě jiné, než pracovněprávní smlouvy[121]. Úřad se snaží uvedenou mezeru zákona vyplnit přenesením odpovědnosti za jednání quasi-zpracovatele na správce a zpracovatele. Problém však nastane, pokud se správce či zpracovatel liberují dle § 46 OchOsÚ. Může tak dojít k nežádoucí situaci, kdy je prokázáno

[121] Případně na základě dohod konaných mimo pracovní poměr viz § 74 a násl. zákona č. 262/2006 Sb., zákoník práce, v platném znění.

porušení OchOsÚ, je znám i odpovědný subjekt, avšak osoby, které mají odpovědnost za zajištění bezpečnosti, se liberovaly. Správce a zpracovatel, ani původce narušení bezpečnosti údajů by tak nenesl správní odpovědnost.

Ustanovení § 14 OchOsÚ vykazuje nesystematičnost v celkovém zasazení zákona, když se zde povoluje osobám odlišným od správce a zpracovatele nakládat s osobními údaji, avšak již neurčuje, zda a v jakém rozsahu mají odpovědnost, pokud způsobí např. ohrožení bezpečnosti údajů.[122] Taková zákonná mezera by mohla být napravena pomocí nastíněné *analogie*.

Lze též předejít komplikacím, pokud správce ve zpracovatelské smlouvě zakáže zpracovateli další přenos povinností na subdodavatele. Takové jednání je představitelné, pokud jsou smluvní strany v rovnocenném postavení. Praxe je však taková, že smluvní podmínky cloudových služeb vč. ustanovení zpracovatelské smlouvy, určuje jednostranně poskytovatel úložiště a jedná se tak o smlouvy uzavírané *adhézním* způsobem.[123] Poskytovatel smluvní ujednání formuluje logicky zásadně ve svůj prospěch. Je málo představitelné, že správce, jakožto běžný zákazník cloudových služeb, bude mít dostatek vlivu na prosazení vlastních klauzulí do zpracovatelské smlouvy, kterou uzavírá s poskytovateli typu Amazon či Microsoft.

Domnívám se, že velkou měrou k nepřehlednosti v pravidlech přispívá fakt, že Směrnice 95/46/ES, jejíž výklad je zprostředkován PS 29, směřuje k opačným závěrům, než ke kterým se přiklání Úřad. Ve výsledku vzniká rozpor, kdy OchOsÚ, jako stěžejní předpis oblasti ochrany osobních údajů, je vykládán vnitrostátním dozorovým orgánem v rozporu se závěry PS 29, která zprostředkovává výklad unijních předpisů v oblasti ochrany osobních údajů. V této, jakož i v kapitole 3.3.1. popsaný přístup Úřadu, jsou příklady, kdy mezi vnitrostátními dozorovými orgány ochrany osobních údajů a unijními orgány, dochází k nejednotnosti při aplikaci předpisů. Přestože stanoviska PS 29 ani Úřadu nemají normotvorný charakter, v praxi je běžné, že správci i zpracovatelé tato stanoviska sledují a snaží se jim přizpůsobit svou činnost. Stanoviska tak mají faktický vliv. Ostatně, Úřad je jediným orgánem, který kontroluje plnění povinností z OchOsÚ. V této práci je věnována pozornost stanoviskám právě z důvodu, že se správci a zpracovatelé snaží sledovat názory

[122] Obdobně uvádí Novák, že pro případy porušení § 14 OchOsÚ zákon nestanoví žádný následek. Autor uzavírá, že odpovědnost osob tak může plynout z předpisů pracovněprávních, případně trestněprávních. Viz NOVÁK, Daniel. In NOVÁK, Daniel. *Zákon o ochraně osobních údajů...,* s. 237 (§ 14). Tomu lze namítat, že tyto druhy odpovědnosti jsou založeny na subjektivním zavinění. Prokázat tedy formu jejich zavinění je mnohem složitější, než odpovědnost dle OchOsÚ, která má objektivní charakter. Z uvedeného důvodu by odpovědnost dalších zpracovatelů měla být založena dle OchOsÚ, aby bylo dosaženo smyslu a účelu právní úpravy.
[123] § 1798 a násl. o. z.

Úřadu, aby jejich činnost byla v případném kontrolním řízení vyhodnocena jako nezávadná. Stanoviska mohou zároveň citovat soudy v rámci svých odůvodnění. Negativně tak hodnotím aplikační nejednotnost a nedůslednou harmonizaci, neboť zvyšuje celkovou nepřehlednost v již tak složité právní úpravě. Tyto skutečnosti mají nepříznivý vliv na správce a zpracovatele, kteří pod vlivem zmatečné situace a právní nejistoty spojené s nejasnými výklady předpisů, mohou volit raději nižší míru dodržování zákonných ustanovení na ochranu osobních údajů.[124] Takové jednání má opět za následek snížení úrovně ochrany osobních údajů.

V této práci navrhovaný přístup povolit řetězení zpracovatelů a učinit tak celé zpracování transparentní, podporuje i právní úprava *de lege ferenda*. Dosud neúčinné GDPR totiž ve svém čl. 28 odst. 2 řetězení zpracovatelů připouští. Oproti dnešnímu stavu se tak dalším osobám zúčastněným na zpracování zpřísní povinnosti, které mají vůči subjektům údajů.

[124] MATEJKA: *Internet jako objekt práva*…, s. 66.

5 Přeshraniční předávání osobních údajů

Výše je zmíněno, že předávání osobních údajů ve vnitřním trhu EU je umožněno bez jakýchkoli složitých překážek. Myšleny byly zásadně administrativněprávní bariéry. K tomu přistupuje skutečnost, že ani samotná faktická proveditelnost takového transferu není složitá. Troufám si tvrdit, že při užití běžných internetových služeb zvládne transfer i osoba s elementárními znalostmi zacházení s počítači. Připojí-li se další prvek, a to nižší cena, než provoz vlastní serverové struktury, pak rázem vzniká celosvětový fenomén. Z těchto důvodů si přeshraniční transfer zasluhuju vyšší pozornost.

5.1 Určení použitelného práva uvnitř EHP

Přestože vnitřní trh EU je prostorem jednotného trhu, není tomu v případě legislativy. Jednotlivé státy si v určité míře zachovaly zákonodárnou autonomii. Nakládání s osobními údaji se tak v členských státech řídí sic harmonizovanou, avšak stále do určité míry odchylnou, národní úpravou. V závazkovém vztahu s mezinárodním prvkem proto vyvstává otázka, jakým právním řádem se budou strany řídit? V případě cloudových úložišť pak může být zodpovězení otázky komplikovanější, neboť *potenciální ubikvita* cloudových služeb *on-demand* umožňuje, aby v jednom čase zasahovaly do několika právních jurisdikcí.

Pravidla určování rozhodného práva upravuje čl. 4 Směrnice 95/46/ES. V něm je určeno, že na činnost správce usazeného v členském státě EU se použije vnitrostátní právo daného státu, budou-li splněny další podmínky uvedené v cit. článku. Rozhodné právo takového přeshraničního transferu údajů se bude pro veřejná datová úložiště určovat na základě čl. 4 odst. 1 písm. a), který uvádí, že „*zpracování je prováděno v rámci činností provozovny správce na území členského státu; pokud je stejný správce usazen na území několika členských států, musí přijmout opatření nezbytná pro dodržování povinností stanovených použitelným vnitrostátním právem každou ze svých provozoven*“. Je tak nezbytné vyložit pojmy „provozovna“ a zpracování prováděné „v rámci činností“ takové provozovny.

5.1.1 Pojem „provozovna“

Směrnice 95/46/ES vymezení pojmu provozovna neobsahuje. Určité vodítko poskytl SD EU, když uvedl, že pojem je třeba vykládat ve světle 19. bodu odůvodnění Směrnice

95/46/ES, ze kterého plyne, že provozovna vyžaduje „*efektivní a skutečný výkon činnosti prostřednictvím stálého zařízení*“[125] přičemž není rozhodná právní forma takového subjektu.[126] V jiné věci zároveň SD EU uvedl, že je nezbytné, aby byly „*trvale dostupné lidské i technické zdroje potřebné pro poskytování příslušných služeb*“[127].

Na základě těchto rozhodnutí je možné určit, že provozovna ve smyslu čl. 4 Směrnice 95/46/ES představuje, bez ohledu na právní subjektivitu, organizační prvek správce, který určitým způsobem participuje na zpracování osobních údajů, a to s přihlédnutím k povaze a způsobu výkonu poskytovaných služeb. Unijní legislativa pojímá provozovnu jako flexibilní pojem, který nelze vykládat formalistickým způsobem, že provozovna je pouze tam, kde má správce své sídlo.[128] Uvedené je důležité zejm. pro správce údajů, kteří své služby poskytují mezinárodně, využívajíce internetových úložišť. Při určování rozhodného práva pro takové zpracování údajů nebude rozhodným kritériem místo, kde jsou osobní údaje dislokovány. Pro určení bude nezbytné zkoumat samotnou povahu a místo činností správce s jednotlivými údaji, odkud je tato vykonávána. Pojem provozovny tak bude slučitelný s pojmy známými v českém právním řádě, a to obchodní závod[129] či pobočka[130], avšak v případě zpracování osobních údajů je třeba splnit další podmínku viz dále.

5.1.2 Zpracování prováděné „v rámci činností“ provozovny

K výše uvedenému pojmu provozovna musí být kumulativně splněna další podmínka, kterou je provádění zpracování údajů *v rámci činností* provozovny. K aplikaci rozhodného práva tak není určující místo usazení správce či umístění údajů, ale užije se práva členského státu, ve kterém provozovna správce participuje na zpracování osobních údajů. Rámec činností je znovu pojmem nedefinovaným ve Směrnici 95/46/ES. Z rozsudku SD EU ve věci Google Spain proti AEPD, Mario C. González plyne, že je nezbytné v jednotlivých případech posuzovat, jakou faktickou úlohu při zpracování provozovna vykazuje. Zda zpracování probíhá v rámci provozovny správce se bude zkoumat na základě rozsahu a způsobu jejího zapojení. V citovaném rozsudku k aplikaci daného právního řádu vedla skutečnost, že provozovna sloužila k zajištění podpory odbytu služeb, při nichž docházelo ke zpracování

[125] Soudní dvůr: Rozsudek ze dne 1. října 2015, *Weltimo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*, C-230/14, bod 28.
[126] Tamtéž.
[127] Soudní dvůr: Rozsudek ze dne 4. července 1985, *Berkholz v Finanzamt Hamburg-Mitte-Altstadt*, C-168/84, Sb. rozh. s. 2251, bod 14.
[128] Stanovisko Generálního advokáta ze dne 25. června 2015 ve věci C-230/14, bod 28.
[129] § 502 o. z.
[130] § 503 o. z.

osobních údajů.[131] Pokud tedy dochází k propojení činností mezi jednotlivou provozovnou a zpracovatelskou činností, pak je naplněna podmínka, že se zpracování provádí také v rámci dané provozovny.

5.1.3 Aplikace článku 4 Směrnice 95/46/ES na činnost cloudových úložišť

V případě používání cloudových úložišť může dojít k následující situaci. Provozovatel internetové služby, správce údajů, je umístěn v členském státě A, kde má svou hlavní provozovnu. Správce má zároveň provozovny v dalších členských státech EU (B a C), přičemž jím provozovaná internetová služba shromažďuje údaje subjektů z členského státu B a C. Osobní údaje jsou však ukládány na serverech datového centra v členském státě D. Právní režim vztahující se na zacházení s údaji ve státě D se bude aplikovat na základě čl. 4 odst. 1 písm. a) Směrnice 95/46/ES.

Shora bylo rozebráno, že rozhodným prvkem pro určení, kterého členského státu se použije právní řád, bude umístění provozovny, v jejímž rámci se zpracování provádí, resp. která se na zpracování podílí. Do tohoto rozhodujícího klíče však vstupuje cloudová technologie. Ta svým charakterem užití může zapříčinit kolizi právních řádů. Shora namodelovanou situaci totiž lze doplnit následovně. K úložišti ve státě D přistupují zaměstnanci provozovny ze státu C, kteří sem přistupují za účelem vyřizování reklamací a obdobných zákaznických služeb. Zároveň ke shromažďovaným osobním údajům přistupuje ústředí společnosti ve státě A, a to za účelem jejich analýzy a plánování marketingových kampaní. Do centrální databáze mohou navíc přistupovat i zaměstnanci provozovny ve státě B, kteří na úložiště nahrávají údaje zpracovávané v rámci činnosti jejich provozovny, avšak při obsluhování databáze mají přístup k neanonymizovaným osobním údajům z členského státu C.

Zaměříme-li se na právní režim, dopadající na osobní údaje z členského státu C, poté dle shora uvedeného rozboru lze dovodit, že při aplikaci čl. 4 odst. 1 písm. a) nastane kolize právních řádů členských států A, B a C. V rámci činnosti provozoven z těchto států totiž dochází k nakládání s osobními údaji, které lze považovat za zpracování ve smyslu čl. 2 písm. b) Směrnice 95/46/ES, neboť popsané činnosti naplňují znaky zpřístupňování

[131] Soudní dvůr: Rozsudek ze dne 13. května 2014, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja GonzálezI*, C-131/12, body 54 – 57.

osobních údajů či umožnění jejich vyhledávání v databázi.[132] Tím dochází k naplnění hypotézy normy, že zpracování se uskutečňuje „v rámci činností" provozovny resp. provozoven správce, které jsou umístěné v rozdílných členských státech, a proto na základě čl. 4 odst. 1 písm. a) Směrnice 95/46/ES dochází k aplikaci uvedených právních řádů. Vzniká tak problematická situace, kdy na konkrétní osobní údaje z jednoho členského státu lze v reálném čase aplikovat právní řády několika členských států EU. Směrnice 95/46/ES takový konflikt však nepředvídá a neobsahuje pravidla pro jeho řešení.

Mohlo by se zdát, že kolize právních řádů členských států by neměla činit potíže, neboť jejich harmonizace zajišťuje jednotné podmínky ochrany osobních údajů. Bygravee k tomu však uvádí, že autoři Směrnice 95/46/ES v takovou harmonizaci jen doufají. Ve skutečnosti jí není náležitě dosaženo, neboť směrnice ponechává prostor členským státům, aby si v jednotlivých oblastech upravily své právní řády dle vlastního uvážení, viz čl. 5 Směrnice 95/46/ES.[133] Příkladem takovéto nejednotné úpravy může být povinnost plynoucí z čl. 4 odst. 2 Směrnice 95/46/ES, kdy správce musí určit svého zástupce na území členského státu EU, pokud je správce usazen v tzv. třetí zemi. Podíváme-li se do české úpravy, pak OchOsÚ nikterak nepřebírá uvedenou povinnost.[134] Naopak řecká úprava nejenže povinnost ustanovit zástupce převzala, ale zároveň pro případ porušení povinnosti sankcionuje správce pokutou od 300 000 do 50 000 000 drachem.[135] Dojde-li ke shora uvedenému konfliktu právních řádů a budou-li to předpisy České a Řecké republiky, pak vzniká situace, kdy proti sobě stojí právní řády nejen s neharmonizovanými, ale dokonce s odporujícími si normami. Přesto je dle Směrnice 95/46/ES povinnost je všechny aplikovat. Je tak zřejmé, že kritika nedodržení řádné harmonizace je namístě. Domnívám se, že s ohledem na bod č. 18 recitálu Směrnice 95/46/ES, ve kterém se uvádí jako jeden z cílů směrnice zamezit situacím, kdy jednotlivcům nebude poskytnuta ochrana, by se mělo užít přednostně řecké úpravy, neboť tato s ohledem na řádnou transpozici čl. 4 odst. 2 Směrnice 95/46/ES poskytuje vyšší míru ochrany subjektům údajů. Tento závěr

[132] Podobně viz Pracovní skupina pro ochranu údajů. *Stanovisko č. 8/2010 k použitelnému právu* [online]. ec.europea.eu, [cit. 28. února 2017]. Dostupné na <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_cs.pdf >, s. 13 – 17.

[133] BYGRAVE, Lee. Determining Applicable Law pursuant to European Data Protection Legislation. *Computer Law & Security Review*, 2000, roč. 16, č. 4, s. 255.

[134] Ostatně, kritika nevymáhání povinnosti čl. 4 odst. 2 Směrnice 95/46/ES národními právními řády se v literatuře již objevila viz KUNER, Christopher. *The „Internal Morality" of European Data Protection Law* [online]. SSRN.com, 24. listopadu 2008 [cit. 1. března 2017]. Dostupné na <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1443797>, s. 5.

[135] § 3 odst. 3 písm. b) a § 21 odst. 1 zákona řecké republiky č. 2472/1997 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů – dostupný též na internetových stránkách řeckého úřadu pro ochranu osobních údajů http://www.dpa.gr/portal/page?_pageid=33,19052&_dad=portal&_schema=PORTAL#21.

mě však vede ke zmínce dalšího problému, který je spojen s nejednotnou harmonizací. Domnívám se, že v případě, kdy v rámci členských států EU jsou v národních právních řádech zásadní rozdíly, pak je zde hrozba, že správci mohou své provozovny záměrně umístit do zemí, kde je pro ně příznivější právní prostředí, tj. kladeny menší nároky na technické a organizační zabezpečení osobních údajů. Charakter cloudové technologie takové jednání umožňuje. Správce tak může zvolit umístění provozovny, která bude zpracování provádět tak, aby ovlivnil aplikaci použitelného práva dle čl. 4 odst. 1 písm. a) ve svůj prospěch. Pokud by bylo v EU dosaženo jednotného standardu ochrany osobních údajů a řádné harmonizace, zamezilo by se takovému jednání správců. To však stávající právní úprava nesplňuje.

Domnívám se, že hlavní příčinou vzniku kolize právních řádů je pravidlo, jakým se určuje použitelný právní řád. Stávající určení na základě zpracování „v rámci činností provozovny správce“ je nevyhovující, neboť v případě užívání cloudovách služeb, kdy se na zpracování provozovnou v jednom členském státě, může podílet i více provozoven z jiných členských států, má za následek výše analyzovanou situaci konfliktu právních řádů. Domnívám se, že určení použitelného vnitrostátního práva by mělo být uskutečněno na základě prvků, které jsou více spjaty s původem osobních údajů – např. bydliště subjektu údajů nebo národní trh, na který bylo zpracování zaměřeno (vodítkem může být jazyková mutace internetových stránek či úhrada za přední pozice ve vyhledávačích v dané zemi). Zároveň pro případy, kdy by takové určení nebylo možné, by bylo užito stávajícího kritéria čl. 4 odst. 1 písm. a) Směrnice 95/46/ES, které by mělo subsidiární povahu.

Zde bych se rád pozastavit nad konstrukcí kritéria pro určení použitelného právního řádu. Určující prvek totiž následuje právní úpravu provozovny správce, a to bez ohledu, zda je ve stejné zemi usazen subjekt údajů. Výsledkem je tak situace, kdy ve velké většině případů se na zpracovávání údajů použije právní řád, jemuž subjekt údajů ani nemusí jazykově rozumět. Domnívám se, že již samotná ztráta ochrany vlastního právního řádu, je určitým způsobem snížením právní jistoty subjektů údajů, neboť tito musí v případě sporu složitě zjišťovat jaká mají práva vůči správci a zpracovateli dle cizího právního řádu. V opačné pozici a ve výhodě je správce (příp. i zpracovatel), kteří budou operovat s „domovským“ právním řádem. Můžeme srovnat situaci s principem uplatňujícím se v soukromoprávních závazkových vztazích, kde je-li zájem na ochraně určité (slabší) strany, jsou zvolena kritéria pro určení použitelného právního řádu tak, aby v prvé řadě byl aplikován

právní řád slabší strany, v němž je usazena, neboť se zde zcela logicky předpokládá, že osoba je znalá takového právního řádu.[136]

Na základě analyzovaných ustanovení jsem tak ověřil a následně potvrdil hypotézu stanovenou v úvodu předkládané práce, že náležitou ochranu osobních údajů snižuje nedůsledná harmonizace evropsko-unijních předpisů členských států EU. Příkladem budiž odlišnost řecké a české úpravy u povinnosti stanovené čl. 4 odst. 2 Směrnice 95/46/ES. Zároveň byla potvrzena hypotéza, že právní úprava dopadající do oblasti ochrany osobních údajů vykazuje nedostatky při určování použitelného práva, kdy v případě konfliktu více právních řádů se musí tyto souběžně aplikovat, avšak nedůsledná harmonizace národních právních řádů má za následek, že v některých situacích se obsah norem souběžně aplikovaných právních řádů vylučují. Pro takové případy však právní úprava neobsahuje kolizní normy.

5.2 Předávání osobních údajů do USA

Evropská unie a Spojené státy americké spolu udržují významné obchodní vztahy. Součástí transakcí, v nichž má velký podíl digitální ekonomika, je přenos osobních údajů.[137] Jejich velká část proudí z EHP technologickým společnostem do USA. Spojené státy americké jsou však dle čl. 25 a násl. Směrnice 95/46/ES tzv. třetí zemí, vůči níž není uplatněn volný pohyb osobních údajů.

V první kapitole byly popsány historické rozdíly vzniku práva na soukromí mezi USA a zeměmi EU. Právo na soukromí není v ústavě Spojených států explicitně vyjádřeno. Postupně se začalo dovozovat výkladem, když se v průlomovém případě Olmstead v. Spojené státy[138] vyjádřil disentním stanoviskem L. Brandeis pro uznání práva na soukromí.[139] Zároveň bylo uvedeno, že ochrana osobních údajů vyvěrá z práva na soukromí. Není-li tedy právo na soukromí v ústavě Spojených států zakotveno, marně v ní budeme hledat právo na ochranu osobních údajů. Absence ústavního zakotvení není jediným rozdílem mezi právními řády členských států EHP a USA. Spojené státy nedisponují propracovanou systematickou úpravou ochrany osobních údajů. Pokud jsem výše zmiňoval nedostatečnou harmonizaci na úrovni členských států EHP, pak v USA je situace odlišná. Hovořit o jakékoli systematické

[136] Např. čl. 5 odst. 2, čl. 6 odst. 1, čl. 8 odst. 1 Nařízení Řím I.
[137] Evropská komise. *Guide to the EU-U.S. Privacy Shield* [online]. ec.europa.eu, 2016 [cit. 4. března 2017]. Dostupné na <http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_en.pdf>, s. 7.
[138] Nejvyšší soud USA: Rozhodnutí ze dne 4. června 1928, *Olmstead v. United States*, 277 U.S. 438.
[139] Nález Ústavního soudu ze dne 22. března 2011, sp. zn. Pl. ÚS 24/10, bod 27.

harmonizaci, je vyloučeno. Jednotlivé státy mají odlišné zákonodárství a není neobvyklé, že jejich normy jsou navzájem protichůdné.[140] Výsledkem je absence obecného předpisu, který by jednotně reguloval problematiku osobních údajů. Ochrana soukromí a osobních údajů je rozmístěna nesystematicky v různých částech právního řádu. Na úrovni států lze např. uvést Kalifornský právní řád, v němž nalezneme regulaci shromažďování údajů prostřednictvím systému rozpoznávání poznávacích značek automobilů v civilním kodexu[141] či úpravu o soukromí elektronických komunikací, jako součásti trestního zákoníku[142]. Na federální úrovni nakládání s osobními údaji normuje např. zákon o soukromí elektronických komunikací[143]. Ve Spojených státech nenalezneme též systematický dohled nad dodržováním předpisů na ochranu osobních údajů v podobě centrálního dozorového orgánu. Přeshraniční transfer osobních údajů z EHP do USA je tak procesně komplikovaný z důvodu zajištění jejich náležité ochrany. Význam obchodních vztahů a objem předávaných údajů však byl důvodem, proč Komise přistoupila k aplikaci čl. 25 odst. 6 Směrnice 95/46/ES, dle kterého je oprávněna rozhodnout, že třetí země zajišťuje odpovídající úroveň ochrany. Na základě takového rozhodnutí a za podmínek v něm uvedených je umožněno zjednodušené předávání osobních údajů.

5.2.1 Od Bezpečného přístavu k Štítu soukromí

Komise využila své oprávnění a rozhodnutím ze dne 26. července 2000 určila, že při splnění tzv. „zásad bezpečného přístavu“ se USA považují za zemi s odpovídající úrovní ochrany, jako v prostoru EHP zajištěné Směrnicí 95/46/ES.[144] Podstatou tzv. „Bezpečného přístavu“ je zjednodušené předávání osobních údajů společnostem, která sídlí v USA. Těm je povoleno předávání pouze za podmínky, že jsou na základě certifikace vedeny v seznamu tzv. *Safe Harbor list*. Certifikaci obdrží jen v případě, zaváží-li se, že budou dodržovat obdobné bezpečnostní standardy osobních údajů, jako v EHP.

[140] SZABÓ, Anna. The European Union And The United States Of America From Perspective Of Data Privacy. *Acta Technica Corviniensis – Bulletin of Engineering*, 2016, roč. 9, č. 1, s. 102.
[141] Cal. Civ. Code § 1798.90.5, Stats. 2015, Ch. 532, Sec. 3.
[142] Cal. Pen. Code § 1546, Stats. 2015, Ch. 651, Sec. 1.
[143] § 2510 a násl. zákona o soukromí elektronických komunikací ze dne z roku 1986, Pub. L. No. 99-508, 100 Stat. 1849, 1873.
[144] Čl. 1 Rozhodnutí Komise 2000/520/ES ze dne 26. července 2000, o odpovídající ochraně poskytované podle zásad „bezpečného přístavu“ a s tím souvisejících „často kladených otázek“ vydaných Ministerstvem obchodu Spojených států. Úř. věst. L 215, 25. srpna 2000, s. 7.

Do tohoto stavu však zasáhl SD EU, když svým rozhodnutím ve věci Schrems v. Data Protection Commissioner[145] zrušil rozhodnutí zakládající Bezpečný přístav. Soud naznal, že ochrana osobních údajů v USA nesplňuje podmínky pro odpovídající úroveň ochrany, neboť k jejich dodržení nejsou vytvořeny účinné kontrolní mechanismy a dále bylo možné omezit zásady Bezpečného přístavu pro „*splnění požadavků bezpečnosti státu, veřejného zájmu nebo prosazování zákonů*“[146] Spojených států. Soudní dvůr k tomu výslovně uvedl, že „*Konkrétně právní úprava, která veřejným orgánům umožňuje globální přístup k obsahu elektronických komunikací, musí být považována za zasahující do podstaty základního práva na respektování soukromého života zaručeného článkem 7 Listiny*“[147] Jinými slovy nedotknutelnost osobních údajů, zaručená Bezpečným přístavem, mohla být *derogována* zákonodárstvím USA, které zásadám Bezpečného přístavu odporuje. Soud tak zamezil předávání údajů v rámci Bezpečného přístavu.

V reakci na zrušující rozsudek SD EU bylo vydáno Rozhodnutí Komise 2016/1250, jímž se zakotvuje tzv. *Privacy Shield*. Jedná se o totožný princip jako u Bezpečného přístavu, avšak s novými prvky. Snahou bylo reagovat na kritiku SD EU a zajistit efektivní kontrolu dodržování bezpečnostních standardů.[148] Komplexní analýza institutu *Privacy Shield* daleko přesahuje rozsah předkládané práce. Z tohoto důvodu jsem se zaměřil na prostředky ochrany osobních údajů, které mohou být při aplikaci Rozhodnutí Komise 2016/1250 v prostředí internetových úložišť použity subjektem údajů.

5.2.2 Prostředky ochrany v konceptu Privacy Shield

V případě, že se subjekt údajů domnívá, že správce údajů usazený v USA nakládá s osobními údaji v rozporu se zásadami *Privacy Shield*, pak je mu Rozhodnutím Komise 2016/1250 poskytnuto několik možností, jak se bránit takovému jednání. Prostředky ochrany jsou upraveny v čl. III odst. 11 Přílohy II Rozhodnutí Komise 2016/1250. Subjekt údajů má na výběr několik možností. Mimo žádosti u samotné správce, se mohou subjekty údajů dovolávat ochrany u (i) poskytovatele alternativních řešení sporů, (ii) národního orgánu pro ochranu osobních údajů, (iii) Ministerstva obchodu USA, Federální obchodní komise (dále jen „FTC“) a u (iv) tzv. „Panelu“ štítu na ochranu soukromí.

[145] Soudní dvůr: Rozsudek ze dne 6. října 2015, Maximillian Schrems v Data Protection Commissioner, C-362/14.
[146] Příloha I odst. 4 Rozhodnutí Komise 2000/520/ES ze dne 26. července 2000..., s. 10.
[147] Soudní dvůr: Rozsudek ze dne 6. října 2015, Maximillian Schrems v Data Protection Commissioner, C-362/14, bod 94.
[148] Body 9 – 12 odůvodnění Rozhodnutí Komise 2016/1250.

Výběr alternativního řešení sporů je na dobrovolném rozhodnutí správce údajů, zda bude stížnosti řešit takovou formou. Rozhodne-li se pro takovou možnost, má zároveň právo určit, zda tento postup bude učiněn v EU či v USA. Subjekt údajů tak nemá žádnou možnost ovlivnit, zda se stížnost bude řešit tímto způsobem, ani zda bude jednání probíhat v EU.[149] Domnívám se, že takovýto prostředek ochrany nezajišťuje s ohledem na jeho fakultativnost efektivní výkon ochrany. Možnost, aby si správce zvolil orgán řešení sporů se sídlem v USA, může být skutečností, která subjekt údajů odradí k podávání stížností, neboť případné jednání by probíhalo v USA.

Výše uvedené body (ii) a (iii) spolu úzce souvisí. Národní orgány na ochranu osobních údajů sic vykonávají určitou dozorovou činnost, nicméně jejich působnost je dle Směrnice 95/46/ES omezena na území EU. Subjekt údajů k nim má však snazší přístup, než k orgánům se sídlem v USA. V případě volby této možnosti je problematické, že dozorové orgány EU mají pomocnou funkci. Nemohou totiž ukládat povinnosti subjektům v jurisdikci práva USA. Jejich prostřednictvím však lze podat stížnost Ministerstvu obchodu USA.[150]

Subjekty údajů mají taktéž možnost podat stížnost přímo Federální obchodní komisi Spojených států.[151] Pokud poskytovatel cloudových služeb poruší zásady uvedené v Příloze II Rozhodnutí Komise 2016/1250, ke kterým se přihlásil prostřednictvím žádosti o získání autorizace, pak FTC přezkoumává, zda takovým jednáním nedošlo k porušení skutkové podstaty zakazující nekalou soutěž, klamavé jednání či praktiky v obchodní činnosti.[152] Samotné Rozhodnutí Komise 2016/1250 však upozorňuje, že FTC nemá pravomoci vykonávat kontroly na místě v oblasti ochrany soukromí. Může pouze požádat poskytovatele služeb, aby se ke stížnosti vyjádřil a předložil relevantní důkazy.[153] Jedinou možností v takovém případě je obrátit se na příslušný soud, aby vymohl příkazy FTC k dodržování programu na ochranu soukromí.[154]

V případě, že se subjekt údajů rozhodne podat stížnost proti poskytovateli internetových služeb, který je provozuje z USA, pak má subjekt údajů výše uvedené možnosti, jak stížnost učinit. Přestože Rozhodnutí Komise 2016/1250 dává na výběr několik možností, jakými prostředky se bude subjekt údajů bránit, jejich společným rysem je skutečnost, že veškerá jednání budou činěna před orgány USA a dle místních právních

[149] Čl. II odst. 1 písm. a) bod ix. Přílohy II Rozhodnutí Komise 2016/1250.
[150] Čl. III odst. 11 písm. g) bod iii. Přílohy II Rozhodnutí Komise 2016/1250.
[151] Čl. III odst. 11 písm. f) Přílohy II Rozhodnutí Komise 2016/1250.
[152] § 45 Zákona o Federální obchodní komisy z roku 1914, Federal Trade Commission Act, Část 15 Zákoníku USA (U.S. Code).
[153] Bod 55 odůvodnění Rozhodnutí Komise 2016/1250.
[154] § 56 Zákona o Federální obchodní komisy z roku 1914, Federal Trade Commission Act, Část 15 Zákoníku USA (U.S. Code).

předpisů. Výjimkou je stížnost podána poskytovateli alternativních řešení sporů, kde je však na volném uvážení poskytovatele služby, zda tento způsob zvolí a zda řízení bude vedeno subjektem z USA či EU. Subjekt údajů tak bude v drtivé většině případů muset komunikovat s orgány Spojených států a mít povědomí o tamní právní systému. Domnívám se, že takové prostředky pak ztrácí svou efektivitu, neboť jejich využití je komplikované a povinnosti, které musí poskytovatel služby splnit se nebudou posuzovat ani právní úpravou v EHP[155], přestože z nich tyto povinnosti poskytovatelů v USA vychází.

V této subkapitole jsem potvrdil hypotézu, že právní řád při zjednodušeném předávání osobních údajů do USA neobsahuje efektivní prostředky ochrany. Pokud poskytovatel služby poruší zásady dodržování náležité bezpečnosti, pak Rozhodnutí Komise 2016/1250 sice poskytuju několik možností, jak subjekt údajů může postupovat a podat stížnost na takové jednání, nicméně k projednání stížností jsou příslušné orgány USA. Zároveň porušení povinností plynoucích z Rozhodnutí Komise 2016/1250 se bude posuzovat dle právního řádu Spojených států. Mám tedy za to, že se nejedná o efektivní prostředky ochrany, neboť na subjekty údajů jsou kladeny nepřiměřené nároky, co do znalosti amerického právního systému. Výsledkem takto komplikovaných postupů může být, že subjekt údajů nebude ochoten domáhat se ochrany prostřednictvím těchto nástrojů. Prostředky ochrany by měly naopak zvyšovat důvěryhodnost právní úpravy a v případě negativního zásahu posilnit práva subjektu údajů, čehož není dosaženo.

Závěrem je nezbytné připomenout, že jedním z důvodů pro zrušení systému *Safe Harbor* v případu Schrems v. Data Protection Commissioner, bylo umožnění omezení zásad Bezpečného přístavu právním řádem USA. Takové omezení se neslučovalo s principy ochrany soukromí dle Směrnice 95/46/ES. Příloha II Rozhodnutí Komise 2016/1250 však obsahuje shodné ustanovení, umožňující opět *derogování* zásad ochrany osobních údajů.[156] Navzdory tomu Komise stále prosazuje, že právní řád USA splňuje podmínky odpovídající úrovně ochrany osobních údajů.[157] Je tak otázkou, zda v případném soudním přezkumu systém *Privacy Shield* obstojí.

[155] Čl. I odst. 2, odst. 7 Přílohy II Rozhodnutí Komise 2016/1250.
[156] Čl. I odst. 5 Přílohy II Rozhodnutí Komise 2016/1250.
[157] Bod 13 odůvodnění Rozhodnutí Komise 2016/1250.

Závěr

Koncepce ochrany osobních údajů tvoří důležitou část práva na soukromí, které je zároveň základním lidským právem. Moderní informační technologie umožňují nové způsoby, jakými je možné soukromí narušit. Takovouto technologií může být i *cloud computing*. Jedná se dnes o běžně užívaný způsob práce s počítači, který spočívá na principu sdílení výkonu výpočetní techniky, k níž uživatel přistupuje prostřednictvím internetové sítě. Oblíbeným druhem cloudových služeb jsou internetová úložiště, která lze používat pro soukromé nebo pracovní účely. V předložené diplomové práci jsem se proto zabýval stavem právní úpravy a zajištěním náležité úrovně ochrany osobních údajů při jejich používání. Analyzována byla česká právní úprava společně se stěžejními předpisy harmonizujícími úpravu členských států EHP, v němž evropsko-unijní předpisy ochrany osobních údajů působí. Zároveň byla v části práce zkoumána i právní úprava USA.

Základní výzkumnou otázku jsem určil, **zda právní úprava, dopadající na provozování internetových úložišť, představuje riziko pro ochranu osobních údajů z hlediska zajištění jejich náležité ochrany**. Cílem předkládané práce tak bylo určení, zda při využívání *cloud computingu* existují rizikové situace, při nichž není dostatečně zajištěna ochrana osobních údajů. Dílčími cíli práce bylo prokázání, že ochrana osobních údajů tvoří důležitou součást práva na ochranu soukromí a dále určit situace, při nichž vzniká hrozba snížení ochrany osobních údajů. K ověření základní výzkumné otázky jsem stanovil následující hypotézy:

1. Právní úprava obsahuje mezery, kdy absentuje úprava určitých situací, vznikajících při poskytování *cloudových* služeb.
2. Nedůsledná harmonizace evropsko-unijních předpisů a Úřadem zavádějící výklad má podíl na snížení ochrany osobních údajů.
3. Právní úprava vykazuje nedostatky při určování použitelného práva regulující ochranu osobních údajů v EU.
4. Právní úprava neobsahuje prostředky, které zajišťují efektivní výkon ochrany předávaných údajů do USA.

První hypotézu, že právní úprava ochrany osobních údajů neupravuje určité situace vznikající při využívání internetových úložišť, a tudíž obsahuje tzv. „slepá místa“, jsem potvrdil v případě řetězení zpracovatelů. V této situaci byla zároveň potvrzena i druhá hypotéza, týkající se nedůsledné transpozice Směrnice 95/46/ES do českého právního řádu

a nejednotnosti výkladu mezi národními a unijními orgány ochrany osobních údajů. Na rozdíl od PS 29 totiž Úřad nepřipouští řetězení zpracovatelů. Zároveň ale povoluje případy, kdy se na zpracování údajů mohou mimo správce a zpracovatele podílet i jiné osoby. Z OchOsÚ však již není patrná odpovědnost těchto dalších osob např. v situacích, kdy se správce a zpracovatel své odpovědnosti zprostí. Může tedy dojít k nežádoucí situaci, kdy osoba, která zapříčinila ohrožení osobních údajů či jiný zásah, není právně odpovědná. Taková právní úprava nemotivuje osoby participující na zpracování údajů k dodržování stanovených povinností, neboť za jejich porušení nehrozí ze strany Úřadu postih. Je zde proto riziko poklesu zajištění řádné ochrany osobních údajů. Charakter *cloudových* služeb, tj. přístup k úložišti odkudkoli prostřednictvím sítě, často umožňuje, aby nakládání s osobními údaji zasahovalo do právních jurisdikcí více států najednou. Vzniká tak situace, kdy na osobní údaje z jednoho členského státu EHP lze aplikovat právní řády několika členských států. To by nemělo činit potíže s ohledem na deklarovanou harmonizaci právních řádů v oblasti ochrany osobních údajů. Na příkladu srovnání české a řecké právní úpravy transpozice povinnosti správce, plynoucí ze Směrnice 95/46/ES, určit zástupce na území členského státu, jsem však prokázal, že řádné harmonizace není vždy dosaženo. V případě konfliktů právních řádů pak může nastat stav, kdy se užije více právních řádů, které se svým obsahem mohou dokonce i vylučovat. Dalším negativním důsledkem neharmonizované úpravy může být situace, kdy správce osobních údajů bude činnost spojenou s internetovým úložištěm provozovat záměrně v členském státě, v němž na něj nejsou kladeny takové nároky na zajištění bezpečnosti osobních údajů. Diplomová práce proto potvrdila třetí hypotézu ohledně nedostatků při určování rozhodného práva a též v tomto případě právní úprava vykazuje nedostatky z hlediska zajištění náležité ochrany osobních údajů. Práce potvrdila i poslední hypotézu, a sice že při mezinárodním předávání osobních údajů do USA absentují v právní úpravě efektivní prostředky nápravy, jimiž by se subjekt údajů mohl dovolávat nápravy pro případ, že správce údajů, umístěný v USA, nakládá s osobními údaji v rozporu se závaznými zásadami bezpečnosti. Právní úprava sice zakotvuje několik možností, které má subjekt údajů k dispozici, nicméně tyto nelze považovat za efektivní z hlediska vymáhání běžného standardu ochrany osobních údajů, neboť výslednou kontrolu a rozhodování provádí úřady se sídlem v USA a dle tamního právního řádu, který byl již Soudním dvorem podroben přezkumu z hlediska odpovídající úrovně ochrany bezpečnosti osobních údajů a byl shledán jako nevyhovující.

Předkládaná práce měla za cíl zhodnocení právní úpravy regulující ochranu osobních údajů při používání internetových úložišť, zda ve všech případech zajišťuje řádnou ochranu

údajů. Na podkladě provedeného výzkumu jsem tak došel k závěru, že analyzovaná právní úprava řádnou ochranu nezajišťuje, když lze nalézt problematické situace, při nichž může dojít ke snížení ochrany oproti běžnému standardu. V práci jsem vždy určil, které situace by mohly být takto závadné. Jako příklad lze uvést absenci řádné transpozice povinnosti plynoucí ze Směrnice 95/46/ES zpracovatele osobních údajů, a to být vázán výhradně pokyny správce údajů. Další příklady krizových situací jsou popsány v příslušných kapitolách věnujících se vymezeným oblastem. Souhrnně však lze rozklíčovat několik oblastí, při nichž není ochrana osobních údajů při využívání internetových úložišť zajištěna na náležité úrovni. Jedná se o vícenásobné zpracování osobních údajů (tzv. řetězení zpracovatelů) a rozložení odpovědnosti mezi subjekty participujícími na zpracování údajů, dále určování použitelného práva v případě konfliktů právních řádů členských států EHP a s ohledem na neefektivní prostředky ochrany je rizikovou oblastí i mezinárodní transfer osobních údajů do USA. Hlavními příčinami nedostatečné úrovně ochrany ve zkoumaných případech jsou mezery právní úpravy, kdy některé situace nejsou upraveny a dále nedůsledná transpozice unijních předpisů, jakož i nedůsledná harmonizace národních právních řádů mezi sebou. Při předávání osobních údajů do USA je příčinou závěru o nízké úrovni ochrany fakt, že na základě Rozhodnutí Komise 2016/1250 se tyto případy posuzují dle právního řádu Spojených států, který však již v minulosti byl Soudním dvorem vyhodnocen jako neodpovídající náležité ochraně, jaká je zajištěna v prostředí členských zemí EHP. Je evidentní, že i zákonodárce si je těchto negativních skutečností vědom a celou záležitost se snaží napravit. Pokud jde o zmiňovanou nedůslednou harmonizaci národních právních řádů, či nejisté rozložení odpovědnosti v případě řetězení zpracovatelů, tak tyto problémy jsou částečně řešeny *de lege ferenda* v nařízení GDPR. V případě dalších nedostatků lze toliko apelovat na zákonodárce, aby i zde pokračoval v úsilí o zkvalitnění právní úpravy.

Přínosem diplomové práce tak je nalezení a označení částí právní úpravy, která nedostatečně upravují užívání internetových úložišť a způsobují tak snížení ochrany osobních údajů. Uvedené rizikové oblasti jsou přitom běžné při využívání *cloudových* služeb. Uživatelé by tak měli být opatrní, neboť prostřednictvím takovýchto služeb svěřují třetím osobám osobní údaje, nad kterými lze snadno ztratit kontrolu, neboť internetová úložiště umožňují celosvětový transfer údajů. V situacích, ve kterých právní úprava není dostatečná, je proto na samotných subjektech údajů, aby pro ochranu soukromí řádně zvažovaly, komu budou údaje poskytovat, za jakých podmínek a zda si zjistí veškeré náležité informace o službách, které hodlají využít.

Seznam použitých zdrojů

Monografie

- BLAHOŽ, Josef, KLÍMA, Karel, SKÁLA, Josef a kol. *Ústavní právo Evropské unie*. 1. vydání. Dobrá Voda u Pelhřimova: Vydavatelství a nakladatelství Aleš Čeněk, 2003. 939 s.
- DONÁT, Josef, TOMÍŠEK, Jan. *Právo v síti. Průvodce právem na internetu*. 1. vydání. Praha: C. H. Beck, 2016. 350 s.
- GOLEMAN, Daniel. *Pozornost: skrytá cesta k dokonalosti*. 1. vydání. Brno: Jan Melvil Publishing, 2014. 312 s.
- JANSA, Lukáš a kol. *Internetové právo*. 1. vydání. Brno: Computer Press, 2016, 432 s.
- KLÍMA, Karel a kol. *Evropské právo*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2011. 579 s.
- KNAPP, Viktor, GERLOCH, Aleš. *Logika v právním myšlení*. 3. vydání. Praha: Eurolex Bohemia, 2000. 230 s.
- KUČEROVÁ, Alena, NONNEMANN, František. *Ochrana osobních údajů v praktických příkladech*. 1. vydání. Praha: BOVA POLYGON, 2013. 167 s.
- MAŠTALKA, Jiří. *Osobní údaje, právo a my*. 1. vydání. Praha: C. H. Beck, 2008. 212 s.
- MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí.* 1. vydání. Praha: CZ.NIC, 2013. 256 s.
- MATES, Pavel. *Ochrana soukromí ve správním právu*. 2. vydání. Praha: Linde, 2006. 313 s.
- MELZER, Filip. *Metodologie nalézání práva. Úvod do právní argumentace*. 2. vydání. Praha: C. H. Beck, 2011. 296 s.
- ŠIŠKOVÁ, Naděžda a kol. *Evropské právo 2 – Jednotný vnitřní trh*. Praha: Wolters Kluwer ČR, 2012. 264 s.
- TAPSCOTT, Don. *Digitální ekonomika: naděje a hrozby věku informační společnosti*. 1. vydání. Brno: Computer Press, 1999, 348 s.
- VELTE, Anthony, VELTE Toby, ELSENPETER, Robert. *Cloud Computing*. 1. vydání. Brno: Computer Press, 2011. 344 s.

Příspěvky ve sborníku

- BARTOŇ, Michal. Ústavněprávní aspekty zveřejňování odposlechů: analýza kolize práva na soukromí, svobody šíření informací a práva na spravedlivý proces. In ŠIMÍČEK, Pavel (ed). *Právo na soukromí*. Brno: Masarykova univerzita, 2011, s. 63 – 78.
- FILIP, Jan. Úvodní poznámky k problematice práva na soukromí. In ŠIMÍČEK, Pavel (ed). *Právo na soukromí*. Brno: Masarykova univerzita, 2011, s. 9 – 19.
- KOKEŠ, Marian. K problematice konkrétních konfliktů mezi právem na informační sebeurčení a ochranou národní bezpečnosti v tzv. době internetové. In ŠIMÍČEK, Pavel (ed). *Právo na soukromí*. Brno: Masarykova univerzita, 2011, s. 119 – 143.
- GRAFSGAARD, Brian. Portfolio, Program, and Project Management as Enablers of Innvation. In LEVIN, Ginger (ed). *Program Management: A Life Cycle Approach*. Auerbach Publications, 2012. s. 413 – 416.

Komentáře

- HULMÁK, Milan a kol. *Občanský zákoník VI. Závazkové právo. Zvláštní část (§ 2055-3014). Komentář*. 1. vydání. Praha: C. H. Beck, 2014. 2072 s.
- KUČEROVÁ, Alena a kol. *Zákon o ochraně osobních údajů. Komentář*. 1. vydání. Praha: C. H. Beck, 2012. 536 s.
- LAVICKÝ, Petr a kol. *Občanský zákoník I. Obecná část (§ 1−654). Komentář*. 1. vydání. Praha: C. H. Beck, 2014. 2380 s.
- NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související. Komentář*. 1. vydání. Praha: Wolters Kluwer ČR, 2014. 504 s.
- WAGNEROVÁ, Eliška a kol. *Listina základních práv a svobod. Komentář*. 1. vydání. Praha: Wolters Kluwer ČR, 2012. 931 s.

Odborné časopisy

- ALI, Mazhar, KHAN, Samee, VASILAKOS, Athanasios. Security in cloud computing: Opportunities and challenges. *Information Sciences*, 2015, roč. 305, s. 357 – 383.
- BEDNÁŘ, Stanislav. Právní zajištění cloudových služeb a velkých dat. *IT Systems*, 2015, roč. 17, č. 2, s. 24.
- BYGRAVE, Lee. Determining Applicable Law pursuant to European Data Protection Legislation. *Computer Law & Security Review*, 2000, roč. 16, č. 4, s. 252 – 257.
- DONÁT, Josef. Právní aspekty cloud computingu. *IT Systems*, 2011, roč. 13, č. 7-8, s. 42 – 43.
- HAIGH, Thomas, PRIESTLEY, Mark. Where Codes Come From: Architectures of Automatic Control from Babbage to Algol. *Communications of the ACM*, 2016, roč. 59, č. 1, s. 39 – 44.

- KOLÁRIKOVÁ, Lenka. Největší záhada cloudu: jde o zpracování osobních údajů či nikoli? *Právní rádce*, 2012, roč. 20, č. 9, s. 27.
- MANTELERO, Alessandro. Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. *Computer Law & Security Review*, 2016, roč. 32, č. 2, s. 238-255.
- MATES, Pavel. K některým otázkám ochrany soukromí ve správním právu. *Právní rozhledy*, 2002, roč. 10, č. 8, s. 367 – 371.
- OTEVŘEL, Petr. Vybraná úskalí uzavírání smluv typu SaaS. *IT Systems*, roč. 14, č. 4, s. 22 – 24.
- RAŠKA, Ondřej. Obchodní modely Software as a Service. *Systémová integrace*, 2009, roč. 16, č. 2, s. 27 – 47.
- SELTENREICH, Radim. Právo na soukromí v kontextu ústavního vývoje v USA. *Právník*, 2000, roč. 139, č. 1, s. 23 – 36.
- SVOBODA, Jiří. Cloud Computing. *Systémová integrace*, 2009, roč. 16, č. 2, s. 66 – 87.
- SZABÓ, Anna. The European Union And The United States Of America From Perspective Of Data Privacy. *Acta Technica Corviniensis – Bulletin of Engineering*, 2016, roč. 9, č. 1, s. 101 – 104.
- ŠURMANOVÁ, Michaela, KNEBL, Ondřej. Service Level Agreements. *Revue pro právo a technologie: odborný recenzovaný časopis pro technologické obory práva a právní vědy*. 2011, roč. 3, č. 2, s. 22 – 28.
- TELEC, Ivo. Poznámky k internetu a proměnám práva. *Právní rozhledy*, 2013, roč. 21, č. 12, s. 448 – 450.
- UČEŇ, Pavel. Servis Level Agreement aplikačních služeb? *IT Systems*, 2002, roč. 4, č. 3, s. 70 – 74.
- WARREN, Samuel, BRANDEIS, Louis. The Right to Privacy. *Harward Law Review*, 1890, roč. 4, č. 5, s. 193 – 202.

Internetové zdroje

- Federal Judiciary Center. *History of the Federal Judiciary* [online]. fjc.gov, [cit. 20. října 2016]. Dostupné na <http://www.fjc.gov/servlet/nGetInfo?jid=654&cid=999&ctype=na&instate=na>.
- LONDON ECONOMICS. *Study on the economic benefits of privacy enhancing technologies* [on-line]. ec.europea.eu [cit. 22. října 2016]. Dostupné na <http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf>. 238 s.

- ARMBRUST, Michael et al. *Above the Clouds: A Berkley View of Cloud Computing* [online]. berkeley.edu, 10. února 2009 [cit. 8. listopadu 2016]. Dostupné na <https://www2.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf>. 23 s.
- MELL, Peter, GRANCE, Timothy. *The NIST definition of cloud computing* [online]. nist.gov, září 2011 [cit. 8. listopadu 2016]. Dostupné na <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>.
- Evropská agentura pro bezpečnost sítí a informací. *Security Cloud Computing: Benefits, risks and recommendation for information ecurity* [online]. enisa.europa.eu, 20. listopadu 2009 [cit. 16. listopadu 2016]. Dostupné na <https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment>. 125 s.
- Rada Evropy. *Doporučení Parlamentního shromáždění Rady Evropy č. 509 (1968) na podkladě 16. zasedání Shromáždění ze dne 31. ledna 1968* [online]. assembley.coe.int, [cit. 19. listopadu 2016]. Dostupné na <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=14546&lang=en>.
- OECD. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* [online]. oecd.org, 2013 [cit. 19. listopadu 2016]. Dostupné na <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>.
- KUNER, Christopher. *The „Internal Morality" of European Data Protection Law* [online]. SSRN.com, 24. listopadu 2008 [cit. 1. března 2017]. Dostupné na <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1443797>. 19 s.
- Úřad pro ochranu osobních údajů. *Zpracování osobních údajů na základě smluv zavíraných se zpracovateli (tzv. řetězení zpracovatelů osobních údajů)*. uoou.cz, [cit. 1. prosince 2016]. Dostupné na <https://www.uoou.cz/files/stanovisko_2009_1.pdf>. 3 s.
- Pracovní skupina pro ochranu údajů. *Stanovisko č. 05/2012 ke cloud computingu* [online]. uoou.cz, [cit. 15. prosince 2016]. Dostupné na <https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=16709>. 27 s.
- Úřad pro ochranu osobních údajů. *K právní ochraně osobních údajů při jejich předávání v rámci cloudových služeb* [online]. uoou.cz, [cit. 28. prosince 2016]. Dostupné na <https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=3002>. 9 s.
- KOPEČKOVÁ, Andrea. *K povinnostem souvisejícím se zpracováním osobních údajů v cloudu* [online]. epravo.cz, 20. listopadu 2015 [cit. 22. ledna 2017]. Dostupné na

<http://www.epravo.cz/top/clanky/k-povinnostem-souvisejicim-se-zpracovavanim-osobnich-udaju-v-cloudu-98984.html>.

- Úřadu pro ochranu osobních údajů. *Stanovisko č. 2/2010 – Předání osobních údajů do jiných států* [online]. uoou.cz, listopad 2010 [cit. 28. prosince 2016]. Dostupné na <https://www.uoou.cz/files/stanovisko_2010_2.pdf>. 6 s.
- Pracovní skupina pro ochranu údajů. *Stanovisko č. 1/2010 k pojmům „správce" a „zpracovatel"* [online]. ec.europa.eu, [cit. 3. ledna 2017]. Dostupné na <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_cs.pdf>. 32 s.
- Pracovní skupina pro ochranu údajů. *Stanovisko č. 8/2010 k použitelnému právu* [online]. ec.europea.eu, [cit. 28. února 2017]. Dostupné na <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_cs.pdf >. 33 s.
- Evropská komise. *Guide to the EU-U.S. Privacy Shield* [online]. ec.europa.eu, 2016 [cit. 4. března 2017]. Dostupné na <http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_en.pdf>. 21 s.

Právní předpisy

Mezinárodní smlouvy

- Smlouva o fungování Evropské unie ze dne 25. března 1957, ve znění Lisabonské smlouvy ze dne 13. prosince 2007.
- Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat, ze dne 28. 1. 1981, vyhlášená pod č. 115/2011 Sb. m. s.
- Dodatkový protokol k Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat o orgánech dozoru a toku dat přes hranice ze dne 8. 11. 2001.
- Mezinárodní pakt o občanských a politických právech, vyhlášený pod č. 120/1976 Sb.
- Úmluva o ochraně lidských páv a základních svobod, vyhlášená pod č. 209/1992 Sb.
- Smlouva o Evropské unii ze dne 7. února 1992, ve znění Lisabonské smlouvy ze dne 13. prosince 2007.

Evropská unie

- Listina základních práv Evropské unie. Úř. věst. C 326, 26. října 2012, s. 391 a násl.
- Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto osob. Úř. věst. L 281, 23. listopadu 1995, s. 31 a násl.

- Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací. Úř. věst. L 201, 31. července 2002, s. 37 a násl.
- Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES. Úř. věst. L 119, 4. května 2016, s. 1 a násl.
- Nařízení Evropského parlamentu a Rady (ES) č. 593/2008 ze dne 17. června 2008 o právu rozhodném pro smluvní závazkové vztahy (Řím I). Úř. věst. L 177, 4. července 2008, s. 6 a násl.
- Nařízení Evropského parlamentu a Rady (ES) č. 593/2008 ze dne 17. června 2008 o právu rozhodném pro smluvní závazkové vztahy (Řím I). Úř. věst. L 177, 4. července 2008, s. 6 a násl.
- Rozhodnutí Komise 2000/520/ES ze dne 26. července 2000, o odpovídající ochraně poskytované podle zásad „bezpečného přístavu“ a s tím souvisejících „často kladených otázek“ vydaných Ministerstvem obchodu Spojených států. Úř. věst. L 215, 25. srpna 2000, s. 7 a násl.
- Rozhodnutí Komise 2016/1250 ze dne 12. července 2016, o odpovídající úrovni ochrany poskytované štítem EU–USA na ochranu soukromí. Úř. věst. L 207, 1. srpna 2016, s. 1 a násl.

Česká republika

- Ústavní zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpisů.
- Listina základních práv a svobod, vyhlášená zákonem č. 23/1991 Sb., kterým se uvozuje LISTINA ZÁKLADNÍCH PRÁV A SVOBOD jako ústavní zákon Federálního shromáždění České a Slovenské Federativní Republiky, republikovaná usnesením předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky, ve znění ústavního zákona č. 162/1998 Sb., kterým se mění Listina základních práv a svobod.
- Zákon č. 328/1999 Sb., o občanských průkazech, ve znění pozdějších předpisů.
- Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.
- Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů, ve znění pozdějších předpisů.
- Zákon č. 262/2006 Sb., zákoník práce, v platném znění.

- Zákon č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.
- Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.
- Zákon č. 89/2012 Sb., občanský zákoník, v platném znění.

Spolková republika Německo

- Spolkový zákon na ochranu dat z 20. prosince 1990 (Bundesdatenschutzgesetz, BGBl. I, s. 2954).

Spojené státy americké

- Civilní kodex Kalifornie (California Civil Code) z roku 1872.
- Trestní zákoník Kalifornie (California Penal Code) z roku 1872.
- Zákon o soukromí elektronických komunikací (Electronic Communications Privacy Act) ze dne 21. října 1986, Pub. L. No. 99-508, 100 Stat. 1849, 1873.
- Zákon o Federální obchodní komisy z roku 1914, Federal Trade Commission Act, Část 15 Zákoníku USA (U.S. Code), § 41 – § 71.

Řecká republika

- Zákon č. 2472 z roku 1997 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů.

Použitá judikatura

Evropský soud pro lidská práva

- Evropský soud pro lidská práva: Rozsudek ze dne 16. prosince 1992, *Niemietz v Německo*, 13710/88, Sb. rozh. 14/1996, bod 29.
- Evropský soud pro lidská práva: Rozsudek ze dne 16. ledna 2000, *Amann v Švýcarsko*, 27798/95, Sb. rozh. 6/2002.

Evropská unie

- Soudní dvůr: Rozsudek ze dne 4. července 1985, *Berkholz v Finanzamt Hamburg-Mitte-Altstadt*, C-168/84, Sb. rozh. s. 2251, bod 14.
- Soudní dvůr: Rozsudek ze dne 13. května 2014, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja GonzálezI*, C-131/12, body 54 – 57.

- Soudní dvůr: Rozsudek ze dne 1. října 2015, *Weltimo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*, C-230/14, bod. 14.
- Soudní dvůr: Rozsudek ze dne 6. října 2015, Maximillian Schrems v Data Protection Commissioner, C-362/14, bod 94.

Česká republika

- Nález Ústavního soudu ze dne 22. března 2011, sp. zn. Pl. ÚS 24/10, body 53 – 54.
- Nález Ústavního soudu ze dne 3. února 2015, sp. zn. II. ÚS 2051/14, bod 28.
- Rozsudek Nejvyššího správního soudu ze dne 10. května 2006, sp. zn. 3 As 21/2005.
- Usnesení Nejvyššího soudu ze dne 27. listopadu 2014, sp. zn. 29 Cdo 3919/2014.

Spojené státy americké

- Nejvyšší soud USA: Rozhodnutí ze dne 4. června 1928, *Olmstead v. United States*, 277 U.S. 438.

Úřední dokumenty

- Stanovisko Úřadu pro ochranu osobních údajů – Zveřejňování osobních údajů na internetu, č. 13/2012, březen 2012 (aktualizace únor 2014).
- Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů – Komplexní přístup k ochraně osobních údajů v Evropské unii, KOM(2010) 609, listopad 2010. 19 s.
- Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů – Uvolnění potenciálu cloud computingu v Evropě, KOM(2012) 059, září 2012. 17 s.
- Důvodová zpráva k návrhu zákona o ochraně osobních údajů a o změně některých zákonů ze dne 22. 9. 1999.
- Stanovisko Generálního advokáta ze dne 25. června 2015 ve věci C-230/14, bod 28.

Abstrakt

Ochrana osobních údajů je součástí souboru práv, které mají ve svém souhrnu za cíl ochranu soukromí člověka. Ochrana osobních údajů nabývá stále větší důležitosti s ohledem na rozšiřující se technologické možnosti. Internet a nové komunikační způsoby umožňují další zásahy do soukromí. Často užívaným způsobem práce s počítači je dnes i *cloud computing*. Principem je sdílení výkonu výpočetní techniky, k níž uživatel přistupuje prostřednictvím internetové sítě. Oblíbeným druhem cloudových služeb jsou internetová úložiště, jejichž prostřednictvím uživatelé svěřují své osobní údaje třetím osobám. V předložené diplomové práci jsem se zabýval stavem právní úpravy a zajištěním náležité úrovně ochrany osobních údajů v prostředí *cloud computingu*.

Cílem předkládané práce tak je určení, zda při využívání *cloud computingu* existují rizikové situace, při nichž není dostatečně zajištěna ochrana osobních údajů. Dílčími cíli práce je prokázání, že ochrana osobních údajů tvoří důležitou součást práva na ochranu soukromí a dále určit situace, při nichž vzniká hrozba snížení ochrany osobních údajů. Základní výzkumná otázka zní „Představuje právní úprava, dopadající na provozování internetových úložišť, riziko pro ochranu osobních údajů z hlediska zajištění jejich náležité ochrany?**“.**

Diplomová práce je rozdělena do dvou hlavních částí – obecné a zvláštní. V první kapitole je rozebrána ochrana osobních údajů jako součást základního lidského práva na soukromí. Druhá kapitola se věnuje vymezení pojmu *cloud computing*. Poslední kapitola obecné části popisuje základní právní úpravu regulující ochranu osobních údajů. Zvláštní část začíná ve čtvrté kapitole, kde se zkoumají vlivy zákonné úpravy závazkového poměru správce a zpracovatele a dále analyzují specifické situace, ke kterým při nakládání s osobními údaji u poskytování cloudových služeb dochází. Pátá kapitola je samostatně věnována mezinárodnímu předávání osobních údajů. Závěr práce shrnuje poznatky získané z předchozích kapitol a ověřuje naplnění hypotéz. Závěr potvrzuje následující hypotézy:

1. Právní úprava obsahuje mezery, kdy absentuje úprava určitých situací, vznikajících při poskytování cloudových služeb.
2. Nedůsledná harmonizace evropsko-unijních předpisů a Úřadem zavádějící výklad má podíl na snížení ochrany osobních údajů.
3. Právní úprava vykazuje nedostatky při určování použitelného práva regulující ochranu osobních údajů v EU.

4. Právní úprava neobsahuje prostředky, které zajišťují efektivní výkon ochrany předávaných údajů do USA.

Summary

Personal data protection is among those laws that exist to protect one's privacy. Personal data protection is gaining more importance the more technology advances; the internet and new ways of communicating also offer wider possibilities to invade one's privacy. Today, *cloud computing* is very popular among computer users. Its purpose is the ability to share the available performance via the internet. A popular branch of cloud services are online internet storages that allow users to store their data with the help of a third party. In this thesis I analyzed the current legal background and the proper level of personal data protection in the *cloud computing* environment.

The objective of this thesis is therefore to state whether *cloud computing* contains risks concerning inefficient personal data protection. The main focus is on proving that personal data protection is a large portion of the law on protection of privacy, and on determining the situations leading to higher risk of personal data protection violation. The basis for the research is the following question: Does the current statutory regulation of personal data protection law pose a threat to its enforcement in the environment of internet data storages?

The thesis consists of two main parts – the general part, and the specialized part. The first chapter of the general part discusses personal data protection as a basic human right for privacy. The second chapter focuses on defining *cloud computing*. The last chapter of the general part describes the basic statutory regulation of controlling personal data protection. The fourth chapter opens up the specialized part of the thesis, with an examination of the influence of the contractual relationship statutory regulation between the administrator and practitioner, and a deeper analysis of the specific situations that arise while treating personal data in cloud services. The fifth chapter is solely focused on international handling of personal data. The last part of the thesis summarizes the resulting data from the previous chapters and verifies the correctness of proposed hypotheses. The outcome is as follows:

1. The statutory regulation is incomplete, omitting certain situations that arise in providing cloud services.
2. Inconsistent harmonization of European Union legislation and misleading interpretation by personal data officer has contribute to a reduction of privacy protection.

3. The statutory regulation is not reliable for determining the correct legislative to regulate personal data protection in the European Union.
4. The statutory regulation does not contain the means to effectively protect data transferred to the USA.

Klíčová slova

Právo informačních technologií; Právo na soukromí; ochrana osobních údajů; Cloud Computing; Cloudová úložiště; Kybernetická bezpečnost

Keywords

Information technology law; Right to privacy; Personal data protection; Cloud computing; Cloud storage; Cyber security