

SOUHLAS SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ ZA ČASŮ INTERNETU

JAKUB MÍŠEK*

ABSTRAKT

Studie Souhlas se zpracováním osobních údajů za časů Internetu analyzuje právní podstatu souhlasu se zpracováním osobních údajů a zkoumá jeho roli v systému práva ochrany osobních údajů. Následně upozorňuje na nedostatky v současné právní úpravě i faktickém stavu, které jsou zapříčiněny, mimo jiné, masivním rozvojem informačních a komunikačních technologií a lpění na starých myšlenkových modelech. Zvláštní kapitola je věnována cookies a obdobným technologiím. Je zkoumán jejich vztah k právu ochrany osobních údajů a adekvátnost současné právní úpravy. Součástí studie jsou také návrhy na možná řešení diskutovaných problémů.

KLÍČOVÁ SLOVA

Ochrana osobních údajů, Ochrana soukromí, Souhlas se zpracováním osobních údajů, Cookies, Internet, Informační a komunikační technologie, Fetišismus

ABSTRACT

Study Consent to personal data processing in the Time of Internet analyses legal grounds of consent to personal data processing. The role of consent in the system of personal data protection is examined. The thesis draws attention to defections of current legal regulation as well as to problems of everyday situations, which are caused among other things by massive development of information and

* Jakub Míšek získal roku 2013 titul magistr umění v oboru Hudební teorie na Hudební a taneční fakultně Akademie múzických umění v Praze, roku 2014 pak získal magisterský titul v oboru Právo a právní věda na Právnické fakultě Masarykovy univerzity. Od roku 2012 působí jako externista na Odboru legislativy a zahraničních vztahů Úřadu pro ochranu osobních údajů, kde se zabývá primárně posuzováním vlivu nových technologií na ochranu osobních údajů. Kontaktní e-mail: jkb.misek@gmail.com

communication technologies. The study offers proposals of possible solutions for discussed problems. A specific chapter is dedicated for cookies and similar technologies. Their relationship with personal data protection is examined.

KEYWORDS

Personal Data Protection, Privacy Protection, Consent to Personal Data Processing, Cookies, Internet, Information and Communication Technologies, Fetishism

1. ÚVOD

Ochrana osobních údajů představuje jednu z klíčových oblastí ochrany soukromí. Zásady, na kterých je postavena, byly poprvé formulovány v osmdesátých letech¹ a jsou dodnes platné. V průběhu desetiletí se tato oblast postupně formalizovala a její ustanovení se přesouvala do dokumentů se stále vyšší právní silou. Dnes najdeme ochranu osobních údajů ve stupních nejvyšších, v Listině základních práv Evropské unie² i v ústavních dokumentech.³ S masivním rozvojem informačních a komunikačních technologií došlo přirozeně k nárůstu možností jak a v jakém rozsahu osobní údaje zpracovávat, stejně tak jako k navýšení počtu zpracování, která jsou prováděna.⁴ Paradigma ochrany osobních údajů se za poslední roky působením nových technologií zásadně změnilo. Cloudové technologie, Internet of Things nebo další služby informační společnosti, představují pro ochranu osobních údajů zásadní výzvy, se kterými se doposud zákonodárci, výkladové orgány ani akademická obec

¹ Srovnej *Thirty years after, The OECD privacy guidelines*. OECD, © 2011 [cit. 10. 6. 2014]. Dostupné z: <http://www.oecd.org/sti/ieconomy/49710223.pdf>.

² 2012/C 326/02, Listina základních práv Evropské unie. In: *CODEXIS* [právní informační systém]. ATLAS consulting [vid. 10. 6. 2014]. Čl. 8.

³ Usnesení 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. In: *CODEXIS* [právní informační systém]. ATLAS consulting [vid. 10. 6. 2014]. Čl. 10 odst. 3.

⁴ Srovnej například: SOLOVE, Daniel J. Privacy Self-Management and the Consent Dilemmas. *Harvard Law Review* [online]. 2013, vol. 126, no. 7, pp. 1880-1903. [cit. 10. 6. 2014] Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018.

WOLF, Christopher; POLONETSKY, Jules. An Updated Privacy Paradigm for the "Internet of Things". *Future of Privacy Forum* [online]. Future of privacy, 2013, 12 s. [cit. 10. 6. 2014]. Dostupné z: <http://www.futureofprivacy.org/wp-content/uploads/Wolf-and-Polonetsky-An-Updated-Privacy-Paradigm-for-the-%E2%80%9CInternet-of-Things-%E2%80%9D-11-19-2013.pdf>.

nedokázali plně vyrovnat. Tato studie se zaměřuje na jeden z klíčových institutů systému ochrany osobních údajů – souhlas se sběrem a zpracováním osobních údajů. Jejím cílem je posoudit jeho současnou právní úpravu a její praktické použití a dopad na adresáty právních norem. Zabývá se právní povahou souhlasu se zpracováním osobních údajů, zda se jedná o jednostranné nebo vícestranné právní jednání, jaký je vztah souhlasu a smlouvy a jaké jsou následky nevhodného použití tohoto institutu.

Nové technologie přinesly nečekané výzvy pro koncept ochrany osobních údajů, jak jej známe dnes, a souhlas není výjimkou. Současný systém je postaven na principu svobody vůle a schopnosti člověka (subjektu údajů) určit si, pro jaké příležitosti chce své údaje poskytnout a v jakých případech je neposkytne. Navýšení počtu zpracování, k nimž je souhlas vyžadován, však vede k rutinizaci udělování souhlasu, nepřehlednosti a v konečném důsledku k naprosté neefektivnosti tohoto právního institutu jako celku. Jak uvádí například Daniel J. Solove,⁵ nebo Frederik Borgesius,⁶ další překážkou bránící efektivnímu fungování souhlasu je psychologie lidského rozhodování, které rozhodně není tak racionální, jak zákonodárce předpokládá. Když se ke zmiňovaným problémům přidá ještě fakt, že lidé osobním údajům přikládají jen nízkou hodnotu,⁷ je evidentní, že rozdíl mezi tím, jak by institut souhlasu měl fungovat a jak opravdu funguje, je vpravdě propastný. O těchto a dalších problémech souhlasu, stejně jako o jejich možných řešeních, pojednává třetí kapitola.

Souhlas je důležitým konceptem i v právní úpravě cookies a podobných technologií, které spadají pod věcnou působnost článku 5 odst. 3 Směrnice

⁵ SOLOVE, Daniel J. Privacy Self-Management and the Consent Dilemmas. *Harvard Law Review* [online]. 2013, vol. 126, no. 7, pp. 1880-1903. [cit. 10. 6. 2014] Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018.

⁶ BORGESIOUS, Frederik. *Consent to behavioural targeting in European Law: What are the policy implications of insights from behavioural economics?* [online]. Amsterdam: Institute for Information Law, 2013, 58 s. [cit. 10. 6. 2014]. Dostupné z: <http://www.ivir.nl/staff/borgesius.html>.

⁷ Srovnej např. ACQUISTI, Alessandro; GROSSKLAGS, Jens. When 25 Cents is Enough: Willingness to Pay and Willingness to Accept for Personal Information [online]. *Workshop on the Economics of Information Security*. 2007, 22s. In: Carnegie Mellon University [online]. [cit. 10. 6. 2014]. Dostupné z: <http://weis2007.econinfosec.org/papers/66.pdf>, nebo KUMPOŠT, Marek; MATYÁŠ, Václav. Jak si lidé cení soukromí? *Zpravodaj ÚVT MU* [online]. Brno: Masarykova univerzita, 2009, roč. 20, č. 1, s. 13-20. [cit. 10. 6. 2014]. ISSN 1212-0901. Dostupné z: <http://www.ics.muni.cz/zpravodaj/articles/626.html>.

2002/58/ES,⁸ případně § 89 odst. 3 Zákona č. 127/2005 Sb., o elektronických komunikacích.⁹ Zákonodárce pomocí analyzovaného ustanovení vytváří další vrstvu ochrany soukromí. Metoda, kterou zvolil, tedy že souhlas s použitím technologie cookies přímo váže na souhlas se zpracováním osobních údajů, je však zcela nesystematická a poněkud nešťastná, protože dále prohlubuje problémy, o kterých pojednává třetí kapitola této práce. Silný tlak na omezování cookies využívaných k cílené reklamě navíc vede k zapojování technologií, které plní stejný účel, ale jsou ze strany uživatele hůře detekovatelné. Tím se snižuje jeho schopnost bránit se proti nim a dochází tedy ke zhoršení jeho pozice. Těmto otázkám se věnuje kapitola čtvrtá.

Cílem studie je více otevřít téma souhlasu se zpracováním osobních údajů v českém odborném prostředí. Zatímco ve světovém diskurzu už proběhl celý cyklus od pozice „Souhlas se zpracováním údajů je skvělý“, přes „Role souhlasu se nesmí přeceňovat“ a „Souhlas je mrtvý“, až po návrat k pozici „Souhlas má v systému ochrany osobních údajů své místo“, v Čechách diskuze zaostala na prvním kroku „Souhlas je skvělý“. Studie si klade za cíl zpochybnit tuto tezi, upozornit na nedostatky, které současná právní úprava má, navrhnout některá možná řešení a hlavně otevřít v českém diskurzu prostor pro diskusi o roli a budoucnosti souhlasu se zpracováním v systému ochrany osobních údajů.

Tato studie je založena na mé diplomové práci. Její dílčí část byla přijata k publikaci jako studie „*Consent to personal data processing – The Panacea or The dead end?*“ časopisem Masaryk University Journal of Law and Technology.¹⁰ V nyní publikované práci byl text zásadně přepracován a rozšířen.

⁸ Směrnice Evropského parlamentu a Rady č. 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích). In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

⁹ Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích). In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

¹⁰ Studie bude publikována v čísle 1/2014.

2. SOUHLAS V PRÁVU A OCHRANA OSOBNÍCH ÚDAJŮ

Souhlas se zpracováním osobních údajů je jedním ze zástupců právního institutu souhlasu, specifický svými zákonnými požadavky a příležitostmi, při které se používá. První kapitola tohoto textu slouží jako vhled do problematiky. V první podkapitole se zabývám charakterem souhlasu v jeho nejobecnější možné podobě, Hohfeldovskou analýzou právního vztahu a vlivem souhlasu na změnu právního vztahu z pohledu této analýzy. Druhá podkapitola je stručným představením právního rámce ochrany osobních údajů a to jak v Evropské unii, tak v České republice. Poslední podkapitola propojuje předchozí, pojednává o souhlasu se zpracováním osobních údajů z pohledu Hohfeldovy teorie a zabývá se otázkou, zda je souhlas se zpracováním jednostranným nebo dvoustranným právním jednáním.

2.1 SOUHLAS V PRÁVU

Vezměme si pro začátek výkladu o souhlasu v právu několik příkladů z českého právního řádu, které stanoví možnost souhlas použít. První je z oblasti soukromého práva a souvisí s ochranou absolutního majetkového práva. Dle § 1042 občanského zákoníku¹¹ se může vlastník věci domáhat ochrany proti každému, kdo neprávem do jeho vlastnického práva zasahuje. Pokud však vlastník udělí jiné osobě souhlas, že do vlastnického práva zasáhnout může,¹² nejedná se již o neoprávněný zásah. Jako druhý příklad jsem vybral § 30 trestního zákoníku,¹³ který jako jednu z okolností vylučujících protiprávnost činu jinak trestného uvádí svolení, tedy souhlas, poškozeného. Třetím příkladem je informovaný souhlas dle zákona o zdravotnických prostředcích,¹⁴ který působí jako způsob legitimizace provedení klinických zkoušek na pacientovi. Bez tohoto souhlasu, případně bez jiného důvodu ospravedlňujícího zásah, by byl takovýto postup

¹¹ Zákon č. 89/2012 Sb., občanský zákoník. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

¹² Takovým zásahem může být například zřízení věcného břemene na nemovité věci, nebo to, že jiná osoba věc zcizí.

¹³ Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

¹⁴ § 10 odst. 1 písm. b) zákona č. 123/2000 Sb., o zdravotnických prostředcích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

protiprávní vzhledem k zákonné ochraně osobnosti a tělesné integrity člověka. Ta je zakotvena v šestém oddílu druhé hlavy první části občanského zákoníku,¹⁵ který se věnuje ochraně osobnosti člověka. Zde zákonodárce stanoví, že s výjimkou v zákoně uvedených důvodů, může být do osobní integrity zasaženo jen se souhlasem daného člověka.

Z výše uvedených příkladů můžeme formulovat tezi, že souhlas slouží jako oprávnění k činnosti jinak zákonem nedovolené. Deryck Beyleveld a Roger Brownsword ve své monografii *Consent in the Law* tvrdí, že se jedná o procesní oprávnění.¹⁶ Zatímco totiž osoba, která souhlas dává, může vykonávat předmětná práva na základě hmotně právního zákonného zmocnění, osoba, které byl souhlas udělen, je může vykonávat toliko na základě daného souhlasu. V okamžik udělení souhlasu se navíc souhlasící vzdává části svých práv, nebo minimálně jejich ochrany, ve prospěch toho, komu svůj souhlas udělil.

U Beylevelda s Brownswordem ještě zůstaneme. Ve své práci velmi zajímavě navázali na tradiční Hohfeldovu analýzu právních vztahů, kterou rozpracovali o vliv souhlasu na předmětné kategorie právních vztahů.¹⁷ Wesley Newcomb Hohfeld ve studii *Fundamental Legal Conceptions*¹⁸ poukazuje na terminologickou nepřesnost, kdy termín „právo“ („right“) nese najednou hned několik vnitřních významů a tím označuje několik úrovní vztahu mezi subjekty práva. Těmito významy jsou právo v úzkém slova smyslu (nárok) („right“, nebo „claim“), privilegium („privilege“), pravomoc („power“) a imunita („immunity“),¹⁹ k nimž se korelativně řadí povinnost („duty“), absence práva („no-right“), podřízení se²⁰ („liability“)

¹⁵ Zákon č. 89/2012 Sb., občanský zákoník. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014]. § 81 a následující.

¹⁶ BEYLEVELD, Deryck; BROWNSWORD, Roger. *Consent in the Law*. Oxford and Portland: Hart Publishing, 2007, 388 s. ISBN 978-1-84113-679-4. s. 81.

¹⁷ *Ibid*, s. 64 – 85.

¹⁸ HOHFELD, Wesley, Newcomb. *Fundamental Legal Conceptions*. In: COOK, Walter, Wheeler. *Fundamental legal conceptions as applied in judicial reasoning and other legal essays*. New Haven: Yale University Press, 1923, s. 23-144.

¹⁹ Používám českou terminologii, kterou užil Hubert Smekal. SMEKAL, Hubert. *Lidská práva*. 1. vyd. Brno: Masarykova univerzita, 2013, s. 22.

²⁰ V případě tohoto termínu se jedná o můj překlad, protože Smekal českou variantu nenabízí. Zvolil jsem tento termín jako překlad Hohfeldova „liability“ proto, že přímý překlad „odpovědnost“ by byl vzhledem k zažitému kontextu zavádějící. Pro termín „podřízení se“ navíc hovoří následující Hohfeldův citát: „Perhaps the nearest synonym of ‘liability’ is ‘subjection’ or ‘responsibility’.“ In: HOHFELD, Wesley, Newcomb. *Fundamental Legal Conceptions*. In: COOK, Walter, Wheeler. *Fundamental legal conceptions as applied in judicial reasoning and other legal essays*. New Haven: Yale University Press, 1923, s. 59.

a nezpůsobilost („disability“). Následující tabulka přehledně ukazuje vztahy mezi uvedenými pojmy:

Právní Opozita	Právo	Privilegium	Pravomoc	Imunita
	Absence práva	Povinnost	Nezpůsobilost	Podřízení se
Právní Korelace	Právo	Privilegium	Pravomoc	Imunita
	Povinnost	Absence práva	Podřízení se	Nezpůsobilost

Tabulka 1 Hohfeldovo schéma²¹

První dva sloupce obsahují pojmy, které se zabývají obsahem právního vztahu. Druhé dva obsahují termíny, jejichž předmětem je možnost nakládání s daným právním vztahem. Pod sebou zařazená právní opozita se vztahují k jedné osobě, jedné straně právního vztahu.²² Pod sebou zařazené právní korelace se vztahují ke dvěma osobám, které pojí právní vztah. První z uvedených právních vztahů je nejklassičtější dvojice právo (nárok) a tomu odpovídající povinnost druhého něco dle tohoto práva činit či nečinit. Termín privilegium představuje možnost vykonávat určité právo, jemu přiřazená absence práva představuje nemožnost druhého do tohoto vykonávání zasáhnout. Jak připomínají Beyleveld s Brownswordem,²³ tyto charakteristiky jsou oddělené a samostatné. Mějme následující příklad: „A“ je vlastníkem pozemku, „B“ má tedy povinnost nezasahovat do jeho vlastnického práva. „A“ má privilegium, že může své vlastnické právo vykonávat a „B“ nemá možnost do tohoto privilegia zasáhnout.²⁴ Za předpokladu, že by „A“ s „B“ uzavřeli dohodu, že výhradně „B“ bude na pozemku sbírat jablka, „A“ by se připravil o privilegium vykonávat sběr jablek, a do doby, než by se tato dohoda změnila, neměl by právo do sběru

²¹ HOHFELD, Wesley, Newcomb. *Fundamental Legal Conceptions*. In: COOK, Walter, Wheeler. *Fundamental legal conceptions as applied in judicial reasoning and other legal essays*. New Haven: Yale University Press, 1923, s. 36.

²² SMEKAL, Hubert. *Lidská práva*. 1. vyd. Brno: Masarykova univerzita, 2013, 195 s. ISBN 978-80-210-6388-4. s. 23.

²³ BEYLEVELD, Deryck; BROWNSWORD, Roger. *Consent in the Law*. Oxford and Portland: Hart Publishing, 2007, s. 66.

²⁴ Za předpokladu, že „A“ nebude své právo vykonávat způsobem, kterým by narušil sousedská práva „B“.

„B“ zasáhnout. Ruku v ruce s tím jde implicitní souhlas „A“, že se „B“ může v době sběru pohybovat po pozemku „A“.

Podívejme se na druhé dva sloupce tabulky. Pravomoc znamená možnost osoby rozhodnout, co se s daným právním vztahem stane. Podřízení se je povinnost druhého toto rozhodnutí přijmout, snést takový zásah. Imunita značí ochranu proti zásahu do právního vztahu a konečně nezpůsobilost je absence pravomoci se vztahem nakládat. Hohfeld s mírnou nadsázkou těchto osm pojmů označuje za „nejnižší společný dělitel práva“²⁵ a celý systém přehledně shrnuje takto:

*“A right is one's affirmative claim against another, and a privilege is one's freedom from the right or claim of another. Similarly, a power is one's affirmative "control" over a given legal relation as against another; whereas an immunity is one's freedom from the legal power or "control" of another as regards same legal relation.”*²⁶

Beyleveld s Brownswordem do Hohfeldovy čtveřice korelujících vztahů výslovně zakomponovali souhlas²⁷ a došli k poznatku, že souhlas může v případě první dvojice vztahů působit dvěma způsoby. První z nich je, že souhlas je výkonem pravomoci, kterou má jedna strana nad právním vztahem, a dojde ke změně vztahu z právo/povinnost ve prospěch „A“ na nový vztah privilegium/absence práva ve prospěch „B“, případně naopak. Druhým způsobem je zachování původního vztahu mezi „A“ a „B“, s tím, že změna (právoplatnost počínání „B“, které by jinak bylo porušením povinnosti vůči právu „A“, kterou souhlas způsobí, proběhne uvnitř daného vztahu. Efektem samozřejmě bude omezení silnější strany a posílení slabší strany adekvátně k prvnímu případu.²⁸

Pro ilustraci se vraťme ještě na okamžik k příkladu se sběrem jablek. Mějme subjekt „A“, vlastníka pozemku s ovocnými stromy, který má právo erga omnes, aby do jeho vlastnického práva nebylo zasahováno. Jedná se

²⁵ HOHFELD, Wesley, Newcomb. Fundamental Legal Conceptions. In: COOK, Walter, Wheeler. *Fundamental legal conceptions as applied in judicial reasoning and other legal essays*. New Haven: Yale University Press, 1923, s. 64.

²⁶ Ibid, s. 60. „Právo je pozitivní nárok, který má jeho vykonavatel vůči jinému a privilegium je svoboda, na právu (nároku) jiného. Podobně, pravomoc je pozitivní kontrola nad právním vztahem, kdežto imunita je svoboda na právní moci jiného týkající se stejného právního vztahu.“

²⁷ BEYLEVELD, Deryck; BROWNSWORD, Roger. *Consent in the Law*. Oxford and Portland: Hart Publishing, 2007, s. 75 a n.

²⁸ Viz Ibid. S. 81-82.

tedy o modus právo a k němu odpovídající povinnost. „A“ udělí souhlas „B“, že se stane oprávněným ke sběru jablek. Tato situace se dle Beylevelda²⁹ dá vykládat buď jako využití pravomoci nad právním vztahem, kterou „A“ má, a změny vztahu na modus privilegium sběru jablek pro „B“ a absence práva do tohoto privilegia bez dalšího zasáhnout na straně „A“. Druhou variantou je, že zůstane zachován modus právo / povinnost do práva nezasáhnout, ale dojde k sebeomezení „A“ a oprávnění „B“, díky čemuž nebude sběr jablek považován za porušení vlastnického práva „A“. Tato změna však může proběhnout i v opačném směru. Jiným případem by bylo, kdyby se „A“, který má na své zahradě privilegium sběru jablek, zavázal „B“, že nebude jablka sbírat. „B“ doposud neměl žádné právo, jak by mohl zasáhnout do privilegia „A“. Opět se zde dle Beylevelda³⁰ nabízí použít dvojí interpretace dané situace. První možnost je, že vznikne nový vztah povinnosti neshbírat jablka na straně „A“ a tomu odpovídající právo aby tato povinnost nebyla porušena na straně „B“. Druhou možností je, že zůstane zachován vztah privilegium / absence práva s tím rozdílem, že se „A“ části svého práva vzdá ve prospěch „B“.

Zde uvedené poznatky Beyleveld s Brownswordem správně shrnují tak, že základní funkcí souhlasu v právu je poskytnout procesní oprávnění příjemci souhlasu něco činit na základě toho, že:³¹

- I) poskytovatel souhlasu udělí pravomoc příjemci souhlasu něco činit,
- II) poskytovatel souhlasu se vzdá svého práva, a nebo
- III) poskytovatel souhlasu se vzdá svého práva nebo udělí pravomoc příjemci souhlasu něco činit tím, že změní právní vztah mezi nimi.

Z uvedeného jasně vyplývá, že souhlas působí jako prostředek vzniku, změny, nebo zániku právního vztahu. Jelikož se jedná o jev závislý na vůli

²⁹ Ibid. S. 75.

³⁰ Ibid. S. 76.

³¹ Ibid. S. 83.

subjektu, můžeme, za předpokladu že nepůjde o individuální právní akt,³² celkem bezpečně říci, že souhlas je právním jednáním.³³

2.2 STRUČNÉ POJEDNÁNÍ O OBECNÉ ÚPRAVĚ OCHRANY OSOBNÍCH ÚDAJŮ

Účelem této podkapitoly je stručné uvedení do problematiky ochrany osobních údajů a seznámení s aktuální právní úpravou jak na půdě Evropské unie, které se věnuje první oddíl, tak na území České republiky, které je věnován oddíl druhý. Zaměřuji se zejména na postavení, jaké v právní úpravě zastává institut souhlasu se zpracováním údajů.

2.2.1 OCHRANA OSOBNÍCH ÚDAJŮ V EVROPSKÉ UNII

Budeme-li postupovat dle právní síly, prvním předpisem, ve kterém se s ochranou osobních údajů setkáme, je Listina základních práv Evropské unie.³⁴ Ochrana osobních údajů, zakotvená v článku 8, je systematicky zařazena k dalším článkům garantujícím respektování soukromého života. Listina základních práv EU rozpracovává a dovádí do detailu ochranu soukromí dle čl. 8 Evropské úmluvy o ochraně lidských práv, ze které vychází.³⁵ Na rozdíl od ní již obsahuje samostatné právo člověka na ochranu osobních údajů. Článek 8 Listiny základních práv EU zakládá každému právo na ochranu osobních údajů, které se ho týkají. Druhý odstavec je destilátem směrnice 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen Směrnice o ochraně osobních údajů),³⁶ z níž toto ustanovení ideově vychází. Stanoví totiž následující:

³² Souhlas může být samozřejmě výsledkem činnosti správního orgánu, jako příklad můžeme uvést územní souhlas. Tento aspekt souhlasu však stojí mimo záběr předkládaného textu a dále se jím proto nebudu zabývat.

³³ Srovnej například: ŠKOP, Martin; MACHÁČ, Petr. *Základy právní nauky*. Praha: Wolters Kluwer ČR, 2011, 196 s. ISBN 978-80-7357-709-4. s. 136.

³⁴ 2012/C 326/02, Listina základních práv Evropské unie. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

³⁵ Sdělení federálního ministerstva zahraničních věcí č. 209/1992 Sb., o sjednání Úmluvy o ochraně lidských práv a základních svobod ve znění protokolů č. 3, 5 a 8. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

³⁶ Směrnice Evropského parlamentu a Rady č. 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

„[Osobní, JM.] údaje musí být zpracovány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem. Každý má právo na přístup k údajům, které o něm byly shromážděny, a má právo na jejich opravu.“³⁷

Již jen z textu tohoto odstavce můžeme vyvodit základní modus práva ochrany osobních údajů na území Evropské unie. Je jím obecný zákaz zpracovávat osobní údaje,³⁸ který je překonatelný, má-li správce údajů nějaký zákonem stanovený důvod pro zpracování. Povšimněme si také privilegované role, kterou v evropské legislativě souhlas mezi těmito zákonem stanovenými důvody zaujímá. Jako jediný je zde uvedený výslovně, veškeré ostatní důvody jsou ukryty pod obecnou množinou „jiné oprávněné důvody stanovené zákonem“. Je to tedy jediný legitimizační důvod, který je podepírán právní silou předpisu stojícího na úrovni primárních smluv.³⁹

Připomeňme krátce, jaké je místo a aplikace Listiny základních práv EU v evropském právu. Dle čl. 6 odst. 1 Smlouvy o Evropské unii ve znění Lisabonské smlouvy,⁴⁰ Evropská unie uznává práva, svobody a zásady obsažené v Listině základních práv EU. Čl. 6 zároveň Listině základních práv EU uděluje stejnou právní sílu, jakou mají primární smlouvy.⁴¹ Dle článku 51 Listiny základních práv EU jsou její ustanovení určena orgánům, institucím a jiným subjektům Unie a členskými státy, výhradně pokud uplatňují právo Unie.

Sekundárním předpisem, který konkrétně upravuje právo na ochranu osobních údajů při zpracování osobních údajů orgány a institucemi Unie, je

³⁷ Článek 8, odst.2, 2012/C 326/02, Listina základních práv Evropské unie. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

³⁸ Subjektem údajů je osoba, o kterou dané údaje identifikují. Viz čl. 2 písm. a) Směrnice o ochraně osobních údajů. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

³⁹ Uvědomuji si, že možná v tomto místě přikládám textu Listiny a výskytu souhlasu v něm větší význam, než v dané souvislosti ve skutečnosti má. Na druhou stranu, kdyby zde souhlas zákonodárce uvést nechtěl, nemusel by tak činit. Souhlas se totiž perfektně vejde do množiny „oprávněných důvodů stanovených zákonem“.

⁴⁰ 2007/C 306/01, Lisabonská smlouva pozměňující Smlouvu o Evropské unii a Smlouvu o založení Evropského společenství. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

⁴¹ Srovnej: CHMEL, Marek; SYLLOVÁ, Jindřiška. *Listina základních práv Evropské unie a česká „výjimka“ z Listiny* [online]. Praha: Parlamentní institut, 2009 [cit. 10. 6. 2014]. Dostupné z: <http://www.psp.cz/sqw/text/text2.sqw?idd=59998>

Nařízení Evropského parlamentu a Rady č. 45/2001.⁴² Tento předpis rovněž ideově vychází ze Směrnice o ochraně osobních údajů. Souhlas je zde uveden jako zákonný důvod pro zpracování údajů v čl. 5, písm. d).⁴³ Je zajímavé, že na rozdíl od Směrnice o ochraně osobních údajů souhlas není mezi dalšími důvody pro zpracování umístěn na prvním místě, ale téměř až na samém konci taxativního výčtu. Důvodová zpráva k tomu říká následující:

„The criteria have been listed in the order of practical importance that can reasonably be expected in the case of public authorities such as Community institutions and bodies. In particular, it is only logical to place at the top of the list the performance of the task carried out by those institutions and bodies. By the same token, ... the data subject's consent or vital interests should not in practice be the criteria most often applied in order to make processing legitimate.“⁴⁴

Díky tomuto citátu se poprvé v tomto textu setkáváme s problémem, který zůstane aktuální až do jeho konce. Tím je otázka, kdy legitimizovat zpracování osobních údajů pomocí souhlasu, a kdy některým jiným zákonným důvodem. V případě Nařízení Komise a Rady č. 45/2001 je převládajícím principem zásada legality, která říká, že orgány státní správy mohou činit jen to, co je jim zákonem dovoleno. Z toho důvodu jsou v tomto nařízení legitimační důvody spočívající v plnění zákonných povinností předrženy svobodné vůli, kterou souhlas představuje. Způsob, jakým je zde tato otázka upravena, je dle mého názoru velmi vhodný, jelikož jasně vyznačuje priority pro konkrétní situaci zpracování údajů veřejnou institucí.

⁴² Nařízení Evropského parlamentu a Rady č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

⁴³ *Ibid.*, čl. 5 písm. d).

⁴⁴ Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data, COM(1999) 337 final, s. 39. In: *EUR-Lex* [právní informační systém]. Úřad pro publikace Evropské unie [cit. 10. 6. 2014]. Dostupné z: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:1999:0337:FIN:EN:PDF>. „Kritéria byla uvedena v pořadí, které odpovídá jejich předpokládané praktické důležitosti pro případy jejich použití institucemi a orgány Společenství. Konkrétně, je zcela logické umístit na začátek seznamu zpracování nezbytné pro výkon činnosti daných institucí a orgánů. Zároveň, ... souhlas subjektu údajů, nebo zachování jeho životně nezbytných zájmů, by neměly být nejčastěji používané důvody pro legitimizaci zpracování osobních údajů.“

Směrnice o ochraně osobních údajů 95/46/ES tvoří základní právní rámec ochrany osobních údajů v Evropské unii a díky jejím implementacím i ve členských státech. Jak jsem již naznačil v předchozích odstavcích, základní modus nakládání s osobními údaji je vyloučení jejich zpracování správcem nebo zpracovatelem,⁴⁵ ledaže existuje zákonný důvod pro zpracování. Toto pravidlo stanoví první věta článku 7 Směrnice o ochraně osobních údajů.⁴⁶ Důvody, které zpracování legitimizují, jsou taxativně vypsány v témže článku. Hned na prvním místě (čl. 7, písm. a)) je nezpochybnitelný souhlas subjektu údajů, který je jinak zákonně definován článkem 2 písm. h) Směrnice o ochraně osobních údajů jako

„jakýkoli svobodný, výslovný a vědomý projev vůle, kterým subjekt údajů dává své svolení k tomu, aby osobní údaje, které se jej týkají, byly předmětem zpracování.“⁴⁷

Souhlas se zpracováním patří mezi klíčové prvky Směrnice a objevil se již v jejím prvním návrhu z roku 1990.⁴⁸ Mezi další zákonné důvody, které umožňují zpracování i bez souhlasu subjektu údajů, patří:

- je-li zpracování nezbytné pro splnění smlouvy, kde je subjekt údajů jednou ze stran, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu (čl. 7, písm. b)),
- je-li zpracování nezbytné pro splnění právní povinnosti, které správce podléhá (čl. 7, písm. c)),
- je-li zpracování nezbytné pro zachování životně důležitých zájmů subjektu údajů (čl. 7, písm. d)),
- je-li zpracování nezbytné pro vykonání úkolu ve veřejném zájmu nebo při výkonu veřejné moci (čl. 7, písm. e)), nebo
- je-li zpracování nezbytné pro uskutečnění oprávněných zájmů správce nebo třetí osoby či osob, kterým jsou údaje sdělovány, za podmínky, že tento zájem vyjde pozitivně z testu proporcionality,

⁴⁵ Vzhledem k tomu, že není předmětem této práce zabývat se rozdíly a vztahem správce a zpracovatele osobních údajů, a také proto, že oprávnění zpracovatele zpracovávat údaje je odvozeno od oprávnění správce, budu nadále hovořit toliko o správci.

⁴⁶ Směrnice o ochraně osobních údajů. In: CODEXIS [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

⁴⁷ Ibid. Čl. 2, písm. h).

⁴⁸ Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data, COM (90), 314 final, SYN 287 and 288, Brussels, 13 September 1990. In: *Archive of European Integration* [online]. University of Pittsburgh [cit. 10. 6. 2014]. Dostupné z: <http://aei.pitt.edu/3768/1/3768.pdf>.

při kterém je vážen vůči právům a právem chráněným zájmům, které může narušit (čl. 7, písm. f)).

Zvláštní kategorie osobních údajů, jako jsou například údaje o etnickém původu, politických názorech a náboženském přesvědčení, jsou článkem 8 Směrnice o ochraně osobních údajů zařazeny do přísnějšího režimu ochrany, který některé legitimizační důvody článku 7 vylučuje (například plnění smlouvy) a ostatní zpřísňuje. Zpřísněná podoba souhlasu⁴⁹ předpokládá výslovný souhlas subjektu údajů.

Posledním případem, kdy se ve Směrnici objevuje institut souhlasu, je čl. 26, který souhlas stanoví jako způsob legitimizace předávání osobních údajů do zahraničí. Účel tohoto souhlasu je sice jiný, než je v případě souhlasu se shromažďováním a zpracováním údajů, formální požadavky jsou však na něj kladeny stejné. Směrnice je v tomto směru nikterak nerozlišuje a pro jeho platnost musí být splněny stejné podmínky, jaké jsou kladeny na souhlas se zpracováním.

Jako *lex specialis* vůči Směrnici o ochraně osobních údajů působí v oblasti elektronických komunikací Směrnice o soukromí a elektronických komunikacích.⁵⁰ To je založeno čl. 1 odst. 2, který stanoví, že „ustanovení této směrnice upřesňují a doplňují směrnici 95/46/ES“. Článek 2, který definuje podstatné právní termíny pro tuto směrnici, dále v písm. f) stanoví, že „souhlas“ uživatele či účastníka odpovídá souhlasu subjektu údajů dle Směrnice o ochraně osobních údajů. To se projevuje zejména v třetím odstavci článku 5 Směrnice o soukromí a elektronických komunikacích, který upravuje cookies a podobné technologie. Původně bylo použití cookies v režimu opt-out, tedy že se jich mohlo použít, pokud uživatel neprojevil s jejich použitím nesouhlas. Evropská Směrnice č. 2009/136/ES⁵¹ změnila úpravou zmíněného článku režim použití cookies

⁴⁹ Ibid. čl. 8, odst. 2, písm. a).

⁵⁰ Směrnice Evropského parlamentu a Rady č. 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích). In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

⁵¹ Směrnice Evropského parlamentu a Rady č. 2009/136/ES ze dne 25. listopadu 2009, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

na opt-in. Uživatel tedy nyní musí předem udělit poskytovateli služby souhlas s jejich použitím, jinak k němu nemůže dojít. Tento souhlas navíc musí splňovat požadavky na souhlas se zpracováním osobních údajů dle Směrnice o ochraně osobních údajů. Detailnímu rozboru uvedených ustanovení včetně výjimek z povinnosti souhlasit, je čtvrtá kapitola této práce.

Závěrem tohoto přehledového oddílu jen velmi stručně pojednám o připravovaném obecném nařízení o ochraně osobních údajů (dále „GDPR“).⁵² Od 25. ledna 2012, kdy byl návrh nařízení na půdě Evropské komise zveřejněn, došlo vzhledem k tisícům připomínek k nepočítaně úprav.⁵³ 12. března 2014 prošel návrh s vybranými připomínkami prvním čtením na půdě Evropského parlamentu.⁵⁴ S touto poměrně aktuální verzí pracuji. Stále však platí, že před dokumentem ještě stojí dlouhá legislativní cesta, během níž se může dojít k jeho změně. Jakkoli blíže analyzovat text GDPR, stále znamená stát na velmi kluzké a velmi pohyblivé ploše, a je proto dle mého názoru na místě určitá zdrženlivost. Jelikož věštění z čajových lístků nikdy nepatřilo do oblasti mé odbornosti, nebudu se pokoušet předvídat budoucnost, ale na základě aktuálního znění GDPR komentuji tendence, které jsou z něj znatelné.

Jednou z těchto tendencí je vědomé posílení role souhlasu se zpracováním. Čl. 4 odst. 8 návrhu GDPR uvádí, že souhlas musí být výslovný a nebude tedy již možné souhlasit konkludentně.⁵⁵ To potvrzuje i upravená verze recitálu č. 31 GDPR,⁵⁶ která rovněž výslovně uvádí zmíněný požadavek. Stejně jako v dnešní úpravě, dle čl. 6 návrhu GDPR je souhlas se zpracováním jedním z důvodů, které umožňují zpracování

⁵² Návrh Nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů), COM(2012) 11 final, 2012/0011. In: *EUR-Lex* [právní informační systém]. Úřad pro publikace Evropské unie [cit. 10. 6. 2014]. Dostupné z: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_cs.pdf.

⁵³ Spisu s návrhem nařízení se na odboru legislativy a zahraničních vztahů Úřadu pro ochranu osobních údajů přezdívá familiárně „Tlustoch“.

⁵⁴ Progress on EU data protection reform now irreversible following European Parliament vote. *Press releases database* [online]. Europa.eu, [cit. 10. 6. 2014]. Dostupné z: http://europa.eu/rapid/press-release_MEMO-14-186_en.htm.

⁵⁵ Návrh Nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů), COM(2012) 11 final, 2012/0011. In: *EUR-Lex* [právní informační systém]. Úřad pro publikace Evropské unie [cit. 10. 6. 2014]. Dostupné z: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_cs.pdf. Čl. 4 odst. 8.

osobních údajů. Velmi podstatný je čl. 7 návrhu GDPR, který upravuje podmínky nezbytné pro vyjádření platného souhlasu. Velice zajímavé je ustanovení upraveného čl. 7 odst. 4 b),⁵⁷ které zakazuje podmiňovat poskytování služeb udělením souhlasu, pokud pro jejich funkčnost není nezbytně nutný.

2.2.2 OCHRANA OSOBNÍCH ÚDAJŮ V ČESKÉ REPUBLICE

V tomto oddílu budeme postupovat analogicky k předchozímu, od předpisů nejvyšší právní síly k předpisům s nižší právní silou a od obecných ke speciálním. Na ústavní úrovni je právo na ochranu osobních údajů součástí práva na soukromí v širším smyslu,⁵⁸ které garantuje článek 10 Listiny základních práv a svobod (dále „LZPS“).⁵⁹ Tento článek stanoví ve třetím odstavci, který Eliška Wagnerová v komentáři k LZPS označuje jako „Informační sebeurčení“,⁶⁰ že každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.

Je celkem bez diskuze, a výše zmíněné ustanovení LZPS to potvrzuje, že ochrana osobních údajů je specifickou oblastí práva ochrany soukromí, a tedy ochrany osobnosti, což zase například dokládá systematické zařazení pododdílu „Podoba a soukromí“ do oddílu „Osobnost člověka“ v občanském zákoníku.⁶¹ Občanský zákoník představuje obecnou úpravu ochrany soukromí na úrovni běžného zákona. Jak správně poznamenává Nonnemann,⁶² je poněkud nešťastné, že byt' došlo k detailnějšímu rozpracování ochrany soukromí oproti starému občanskému zákoníku,

⁵⁶ Draft report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM (2012)0011–C7-0025/2012-2012/0011(COD)). *Evropský parlament* [online]. Europarl.europa.eu [cit. 10. 6. 2014]. Dostupné z: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf. s. 17.

⁵⁷ *Ibid.*, s. 76.

⁵⁸ WAGNEROVÁ, Eliška et al. *Listina základních práv a svobod. Komentář*. Praha: Wolters Kluwer ČR, a.s., 2012, 931 s. ISBN 978-80-7357-750-6. s. 277.

⁵⁹ Usnesení 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. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

⁶⁰ WAGNEROVÁ, Eliška et al. *Listina základních práv a svobod. Komentář*. Praha: Wolters Kluwer ČR, a.s., 2012, s. 284.

⁶¹ § 81 a následující zákona č. 89/2012 Sb., občanský zákoník. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

zákonodárce nikterak nezohlednil platnou právní úpravu ochrany osobních údajů a nejen, že nesjednotil terminologii mezi předpisy, ale nikterak výslovně nevyjasnil, jaký vztah mezi sebou občanský zákoník a Zákon o ochraně osobních údajů mají.

Nezbývá než vycházet z obecných právních zásad a řídit se pravidlem *lex specialis derogat legi generali*. Zákon o ochraně osobních údajů je pro předmětnou oblast ochrany soukromí zvláštním zákonem, a má proto interpretační přednost před občanským zákoníkem.

V Občanském zákoníku je souhlas - v jeho terminologii „svolení“, hlavním legitimačním důvodem pro zásah do soukromí člověka.⁶³ Stojí za zmínku, že § 87 výslovně umožňuje udělený souhlas odvolat a to i v případě, že byl dán na dobu určitou. Svědčí to o tom, že zákonodárce akcentuje právo člověka spravovat a hlídat si své soukromí.

Zákon o ochraně osobních údajů je implementací evropské Směrnice o ochraně osobních údajů a analogicky tak tvoří základní rámec právní úpravy ochrany osobních údajů v českém právním řádu. Souhlas se zpracováním je v něm upraven velmi obdobně jako ve zmíněné směrnici, stejně je na tom i výčet dalších legitimizačních důvodů pro zpracování. Detailní analýze právních náležitostí souhlasu je věnována následující kapitola, na tomto místě se však zastavme u některých dalších povinností, které musí správce splnit, aby mohl osobní údaje zpracovávat. Základní povinností správce je stanovit účel zpracování⁶⁴ a tomuto účelu zpracování podřídit.⁶⁵ Účel musí být vyjádřen dostatečně konkrétně, jelikož se dle něj posuzuje, který z legitimizačních důvodů bude použit.⁶⁶ Další povinnosti, které na tuto přímo navazují, jsou povinnost shromažďovat jen údaje odpovídající účelu a to v nezbytném rozsahu⁶⁷ a povinnost zpracovávat

⁶² Srovnej NONNEMANN, František. Právní úprava ochrany osobnosti v novém občanském zákoníku a její vztah k ochraně osobních údajů. *Právní rozhledy*. 2012, roč. 20, č. 13-14, s. 505-509. ISSN 1210-6410.

⁶³ § 84 zákona č. 89/2012 Sb., občanský zákoník. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

⁶⁴ § 5 odst.1 písm. a) zákona č. 101/2000 Sb o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

⁶⁵ *Ibid* § 5 odst. 1 písm. d).

⁶⁶ Srovnej MATOUŠOVÁ, Miroslava; HEJLÍK, Ladislav. *Osobní údaje a jejich ochrana*. 2. Vyd. Praha: ASPI, Wolters Kluwer, 2002, 468 s. ISBN 978-80-7357-322-5. s. 202.

⁶⁷ § 5 odst.1 písm. d) Zákona o ochraně osobních údajů. [cit. 10. 6. 2014].

údaje pouze v souladu s účelem, k němuž byly shromážděny.⁶⁸ Zatímco první ze jmenovaných chrání subjekt údajů, aby nebyly shromažďovány údaje, které jsou pro splnění daného účelu nadbytečné, druhá zamezuje správci, aby měnil účel v průběhu zpracování, což zajišťuje právní jistotu subjektu údajů. Té napomáhá i povinnost správce uchovávat osobní údaje jen po dobu nezbytnou vzhledem k účelu zpracování.⁶⁹ Tato povinnost je vlastně základem pro, v poslední době tolik citované, „právo na zapomenutí“, které se objevilo v GDPR, jelikož po uplynutí doby nezbytné účelu zpracování, která by navíc měla být správcem předem stanovena, má správce povinnost zpracovávané osobní údaje zlikvidovat.⁷⁰ Poslední z povinností správce, kterou na tomto místě zmíním, je informační povinnost. První odstavec § 11 stanoví:

„Správce je při shromažďování osobních údajů povinen subjekt údajů informovat o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny, nejsou-li subjektu údajů tyto informace již známy.“⁷¹

Toto ustanovení dává povinnost správci údajů informovat subjekt poměrně detailně o všech podstatných náležitostech zpracování. Rovněž časově specifikuje, že k informování má dojít při shromažďování údajů, tedy, jak uvádí Alena Kučerová:

„... nejpozději v okamžiku, kdy správce od subjektu údaje požaduje, žádá o jejich sdělení, případně předložení dokladu, nebo dokumentu, který údaje obsahuje. Aby byl naplněn účel tohoto ustanovení, musí být subjekt údajů v okamžiku předání svých údajů ... již informován, proto se jako přesnější (resp. jako jediný možný výklad tohoto časového určení) jeví formulace, že správce je povinen informační povinnost splnit již před samotným získáváním osobních údajů.“⁷²

⁶⁸ Ibid. § 5 odst.1 písm. f).

⁶⁹ Ibid. § 5 odst.1 písm. e).

⁷⁰ Ibid. § 20 odst. 1.

⁷¹ Ibid. § 11 odst. 1.

⁷² KUČEROVÁ, Alena et al. *Zákon o ochraně osobních údajů, Komentář*. 1. Vyd. Praha: C. H. Beck, 2012, 536 s. ISBN 978-80-7179-226-0. s. 211.

Vzhledem k tomu, správce musí plnit uvedené povinnosti při každém zpracování nehledě na jeho legitimizaci, můžeme vyslovit hypotézu, že souhlas se zpracováním se od ostatních legitimizačních důvodů liší toliko tím, že umožňuje zpracování údajů pro účely a v situacích, na které jiné legitimizační důvody nestačí.

Posledním právním předpisem, o kterém se v této části zmíním, je Zákon o elektronických komunikacích,⁷³ jehož pátá hlava je implementací výše zmiňované směrnice o soukromí a elektronických komunikacích. A podobně jako směrnice, i tento zákon je *lex specialis*⁷⁴ vůči zákonu o ochraně osobních údajů pro oblast elektronických komunikací. Cookies a podobné technologie jsou právně upraveny ve třetím odstavci § 89. Dopodrobna se tomuto předpisu věnuji ve zvláštní části této práce.

Touto stručnou zmínkou o Zákonu o elektronických komunikacích uzavíráme část, jejímž účelem bylo vytvořit obraz vztahů a spojitostí mezi jednotlivými předpisy upravujícími ochranu osobních údajů. Zároveň s tím byly představeny klíčové právní instituty a máme tak připraven základ pro další text práce.

2.3 HOHFELDOVSKÁ ANALÝZA VZTAHU SUBJEKT – SPRÁVCE A VLIV SOUHLASU NA TENTO VZTAH

V poslední podkapitole první kapitoly propojují poznatky z podkapitol předchozích a analyzují vztah subjekt údajů – správce údajů za pomoci Hohfeldových kritérií. Závěrem pak argumentují, zda je souhlas se zpracováním jednostranným, nebo dvoustranným právním jednáním.

Subjekt údajů má ústavně garantované právo na ochranu soukromí a osobních údajů. To můžeme přeformulovat tak, že má právo, aby nebylo zasahováno do jeho soukromí tím, že by bylo neoprávněně nakládáno s jeho osobními údaji.⁷⁵ Toto právo má subjekt údajů *erga omnes*.

⁷³ Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích). In: CODEXIS [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

⁷⁴ Viz *ibid.* § 87.

⁷⁵ Povšimněme si určitého oddělení soukromí a osobních údajů. Předmětem Zákona o ochraně osobních údajů jsou právě osobní údaje, soukromí je chráněno nepřímo skrze jejich ochranu. Tuto tezi podporuje například systematika Listiny základních práv a svobod EU, která výslovně uvádí právo na ochranu osobních údajů v samostatném článku.

Zákon potenciálnímu správci údajů zakazuje shromažďovat a zpracovávat údaje, nemá-li k tomu zákonný důvod.

Podívejme se na stav právního vztahu dle Hohfelda před udělením souhlasu:

- Subjekt má právo, aby s jeho údaji nebylo nakládáno, a potenciální správce má povinnost zdržet se nakládání s nimi (zpracování).
- Subjekt má privilegium vykonávat právo, aby s jeho údaji nebylo nakládáno,⁷⁶ a potenciální správce postrádá právo do výkonu tohoto práva jakkoli zasáhnout.
- Subjekt údajů má pravomoc změnit vztah mezi ním a potenciálním správcem,⁷⁷ který má povinnost se této změně podřídit.
- Subjekt údajů má imunitu chránící ho před změnou vztahu a potenciální správce není způsobilý takovou změnu provést.

Udělením souhlasu se zpracováním údajů se subjekt v jeho rozsahu vzdá zákonné ochrany a dojde k následující změně:

- Správce údajů má právo prolomit zákonnou ochranu subjektu údajů a subjekt údajů má povinnost zdržet se zásahu do tohoto práva.⁷⁸
- Správce má právo vykonávat právo prolomit zákonnou ochranu subjektu údajů, tedy zpracovávat osobní údaje subjektu. Subjekt postrádá právo do tohoto práva zasáhnout.

Co se týče třetí a čtvrté kategorie, zdánlivě je možných více variant změny vztahu.

Varianta A) předpokládá, že se souhlas se zpracováním na tyto kategorie nevztahuje, pravomoc nad tímto právním vztahem zůstává v rukou subjektu údajů a ten tak může jednou daný souhlas kdykoli odvolat. Vypadá následovně:

- Subjekt údajů má pravomoc změnit vztah mezi ním a správcem,⁷⁹ který má povinnost se této změně podřídit.

⁷⁶ To znamená, že se může zpracování údajů bránit.

⁷⁷ Tj. udělit souhlas se zpracováním a umožnit tak zpracování údajů.

⁷⁸ To znamená, že se nemůže bez dalšího zpracování údajů bránit. Pokud bychom vyjmuli pouze tuto dílčí část, tak by souhlas subjektu zněl „Souhlasím s tím, že nebudu se bránit zpracování těchto údajů.“

Srovnej: BEYLEVELD, Deryck; BROWNSWORD, Roger. *Consent in the Law*. Oxford and Portland: Hart Publishing, 2007, s. 76.

⁷⁹ Tj. odvolat souhlas se zpracováním údajů a znemožnit tak jejich zpracování.

- Subjekt údajů má imunitu chránící ho před změnou vztahu a správce tak není způsobilý takovou změnu provést.

Tato varianta odpovídá tezi, že souhlas se zpracováním je jednostranné právní jednání. Problém varianty A) spočívá v tom, že správce zdánlivě nemá možnost vztah ukončit. Domnívám se, že možné řešení spočívá v povinnostech, které jsou nezbytné pro zpracování údajů, zejména v povinnosti uchovávat osobní údaje jen po dobu nezbytnou vzhledem k účelu zpracování. Ve chvíli, kdy účelnost zpracování pomine, má správce povinnost zpracování ukončit, a tím skončí i souhlas daný pro to konkrétní zpracování. Toto řešení možné je, není však příliš elegantní.

Podívejme se nyní na variantu B). Ta předpokládá, že souhlas se zpracováním mění i tyto kategorie. V takovém případě ke změně dojde a vztah bude vypadat takto:

- Správce údajů má pravomoc změnit vztah mezi ním a subjektem,⁸⁰ který má povinnost se této změně podřídit.
- Správce údajů má imunitu chránící ho před změnou vztahu a subjekt není způsobilý takovou změnu provést.⁸¹

Z této varianty však vyplývá, že do vztahu může zasáhnout toliko správce. Subjekt do něj nemůže nikterak zasáhnout a nakládat s ním, nemá tedy ani možnost jednou daný souhlas odvolat. Ačkoli existují autoři, kteří tvrdí, že právě tak tomu je,⁸² podpořen studiemi Františka Nonnemanna⁸³ a Iva Telce,⁸⁴ českou judikaturou⁸⁵ a stanoviskem⁸⁶ Pracovní skupiny pro

⁸⁰ Pokud bychom opět vyjmuli pouze tuto dílčí část, souhlas by zněl takto „Souhlasím s omezením imunity, a proto mají akce správce efekt na náš právní vztah.“

Srovnej: BEYLEVELD, Deryck; BROWNSWORD, Roger. *Consent in the Law*. Oxford and Portland: Hart Publishing, 2007, s. 80.

⁸¹ Zde by dílčí souhlas subjektu zněl: „Souhlasím, že se vzdávám pravomoci nakládat s daným právním vztahem.“ Kauzálně správně by tedy nové vyjádření vztahu mělo znít „Správce údajů má imunitu chránící ho před změnou vztahu, protože subjekt není způsobilý takovou změnu provést.“

⁸² Srovnej CURREN, Liam; KAYE, Jane. Revoking consent: A 'blind spot' in data protection law? *Computer Law & Security Review* [online]. 2010, vol. 26, no. 3, pp. 273-283. [cit. 10. 6. 2014]. Dostupné z: <http://www.publichealth.ox.ac.uk/helex/publications/Curren2010273>.

⁸³ NONNEMANN, František. Odvolání souhlasu se zpracováním osobních údajů. *Právní rozhledy*. 2011, roč. 19, č. 24, s. 871-877. ISSN 1210-6410.

⁸⁴ Studie je věnována obecně ochraně osobnosti dle starého občanského zákoníku, ve kterém podobně jako v zákoně o ochraně osobních údajů nebylo odvolání výslovně uvedeno. Při použití analogie je aplikovatelná i na ochranu osobních údajů. Viz TELEČEK, Ivo. Svolení, nebo zákonné licence v právu osobnostním. *Právní rozhledy*. 2007, roč. 15, č. 24, s. 879-883. ISSN 1210-6410.

ochranu údajů zřízené podle článku 29⁸⁷ (dále „WP29“) tvrdícím, že souhlas, který nejde efektivně odvolat je nedostatečný, se domnívám, že jednostranné odvolání souhlasu se zpracováním subjektem údajů je, a musí být, možné. Z toho důvodu varianta B) není přijatelná.

Do úvahy tak přichází varianta C), která předchozí dvě kombinuje:

- Subjekt údajů má pravomoc změnit vztah mezi ním a správcem, který má povinnost se této změně podřídit.⁸⁸
- Správce údajů má pravomoc změnit vztah mezi ním a subjektem, který má povinnost se této změně podřídit.

Výsledkem je situace, kdy obě strany mohou svým jednostranným právním jednáním rovnou změnit vzájemný právní vztah a ani jedna z nich nepoživá imunity. Prakticky to tedy znamená, že subjekt údajů může souhlas odvolat, a tím i připravit správce údajů o právo osobní údaje zpracovávat. Zároveň s tím se může správce údajů svobodně vzdát uděleného práva zpracovávat osobní údaje.

Spojíme-li předchozí úvahy v jeden celek, schéma vztahu mezi subjektem a správcem údajů je následující:

Před udělením souhlasu:

- Subjekt má právo, aby s jeho údaji nebylo nakládáno a potenciální správce má povinnost zdržet se nakládání s nimi (zpracování).
- Subjekt má privilegium vykonávat právo, aby s jeho údaji nebylo nakládáno, a potenciální správce postrádá právo do výkonu tohoto práva jakkoli zasáhnout.
- Subjekt údajů má pravomoc změnit vztah mezi ním a potenciálním správcem, který má povinnost se této změně podřídit.

⁸⁵ Městský soud v Praze na straně 8 rozsudku ve věci žaloby proti rozhodnutí předsedy Úřadu pro ochranu osobních údajů s odvoláním souhlasu operuje a nikterak jej nerozporuje. Srovnej: Rozsudek Městského soudu v Praze ze dne 23. května 2013, sp. zn. 8Ca 95/2009. *Úřad pro ochranu osobních údajů* [online]. Úřad pro ochranu osobních údajů [cit. 10. 6. 2014]. Dostupné z: http://www.uouu.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=6558.

⁸⁶ Pracovní skupina pro ochranu údajů zřízená podle článku 29. Stanovisko č. 15/2011 k definici souhlasu. WP 187. *Evropská komise* [online]. [cit. 10. 6. 2014]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_cs.pdf, s. 13.

⁸⁷ WP 29 je nezávislý evropský poradní orgán zabývající se ochranou osobních údajů, jehož kompetence jsou popsány v článku 30 Směrnice o ochraně osobních údajů.

⁸⁸ To znamená, že subjekt údajů nesouhlasí se změnou této části vztahu.

- Subjekt údajů má imunitu chránící ho před změnou vztahu a potenciální správce není způsobilý takovou změnu provést.

Po udělení souhlasu:

- Správce údajů má právo prolomit zákonnou ochranu subjektu údajů a subjekt údajů má povinnost zdržet se zásahu do tohoto práva.
- Správce má právo vykonávat právo prolomit zákonnou ochranu subjektu údajů, tedy zpracovávat osobní údaje subjektu. Subjekt postrádá právo do tohoto práva zasáhnout.
- Subjekt údajů má pravomoc změnit vztah mezi ním a správcem, který má povinnost se této změně podřídit.
- Správce údajů má pravomoc změnit vztah mezi ním a subjektem, který má povinnost se této změně podřídit.

Takto popsaný souhlas je jednostranným právním jednáním. V literatuře a teoretickém diskurzu však nevyřešenou otázkou zůstává, zda je souhlas se zpracováním jednostranným, nebo dvoustranným právním jednáním mezi subjektem a správcem.⁸⁹ Jedním z autorů, kteří argumentují pro variantu, že se jedná o jednání dvoustranné je Nonnemann. Ve své studii uvádí:

„Povinnosti správce a práva subjektu údajů při probíhajících zpracováních jsou sice předmětem veřejnoprávní regulace, ale samotný jejich vztah, pokud vznikl na základě souhlasu subjektu údajů, je spíše soukromoprávní povahy. ... V oblasti soukromého práva můžeme ... nalézt jistou analogii pro postup před vyjádřením souhlasu se zpracováním osobních údajů. Informace o parametrech zamýšleného zpracování, které je správce před získáním souhlasu povinen poskytnout, lze spolu s dalšími skutečnostmi, které ... subjektu sdělí (např. jaké protiplnění mu za souhlas se zpracováním jeho osobních údajů nabízí), považovat za svého druhu

⁸⁹ Domnívám se, že není nutné na tomto místě podrobovat eventualitu dvoustranného právního jednání stejně detailní Hohfeldovské analýze. Stručně řečeno, první dvě kategorie jsou odpovídající jednostrannému právnímu jednání (jak před souhlasem, tak po souhlasu). Druhé dvě kategorie jsou však pouze v pozici imunity pro obě strany a to jak před souhlasem, tak po jeho udělení. Dá-li jedna strana ofertu, zároveň tím dává druhé straně pravomoc nad právním vztahem a na sebe ukládá odpovídající povinnost podřídit se této pravomoci. Srovnej: HOHFELD, Wesley, Newcomb. *Fundamental Legal Conceptions*. In: COOK, Walter, Wheeler. *Fundamental legal conceptions as applied in judicial reasoning and other legal essays*. New Haven: Yale University Press, 1923, s. 55-56.

nabídku, ofertu, a poskytnutí souhlasu za její přijetí. ... Lze říci, že mezi nimi vzniká inominátní smlouva sui generis.“⁹⁰

Argumenty, které Nonnemann uvádí, jsou bez pochyby platné. Poměrně hezky navíc ilustrují povahu souhlasu, jak by měl fungovat. Měl by být užíván tehdy, když správce údajů něco po subjektu žádá a iniciuje vznik právního vztahu. Pokud žádá něco subjekt po správci, nebude v naprosté většině případů souhlasu potřeba, protože se jako legitimizace zpracování použije důvod nutnosti zpracování údajů pro plnění smlouvy, jíž je subjekt stranou.

Dvoustranný pohled na souhlas však rozhodně není univerzálně přijímán. Opačnou interpretaci podporuje například stanovisko Úřadu pro ochranu osobních údajů (dále jen „UOOU“) č. 2/2012,⁹¹ které na 2. straně výslovně uvádí, že souhlas je jednostranným právním úkonem. Tuto doktrínu potvrzuje i ve své rozhodovací činnosti.⁹² Jako „jednoznačně jednostranný“ právní úkon jej označuje i Václav Bartík⁹³ a Ivo Telec, který ve své studii,⁹⁴ byť věnované souhlasu v právu duševního vlastnictví, popisuje situaci, o které jsem přesvědčen, že dobře odpovídá souhlasu se zpracováním osobních údajů. Blízkost těchto institutů je dána tím, že oba chrání osobnostní práva.⁹⁵ Telec píše, že souhlas je jednostranné právní jednání, které nezavazuje jiného, ale působí jako okolnost vylučující protiprávnost zásahu druhé strany. Toto schéma je zcela totožné s působením souhlasu se zpracováním, jak jasně vyplynulo z Hohfeldovské analýzy.

⁹⁰ NONNEMANN, František. Odvolání souhlasu se zpracováním osobních údajů. *Právní rozhledy*. 2011, roč. 19, č. 24, s. 873.

⁹¹ Stanovisko Úřadu pro ochranu osobních údajů č. 2/2011, Zpracování osobních údajů na základě souhlasu ve smlouvě nebo Všeobecných obchodních podmínkách a s tím související problémy. *Úřad pro ochranu osobních údajů* [online]. [cit. 10. 6. 2014]. Dostupné z: http://www.uouu.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=9185

⁹² Rozhodnutí Úřadu pro ochranu osobních údajů čj. SPR-5685/09. Náležitosti souhlasu se zpracováním osobních údajů. *Úřad pro ochranu osobních údajů* [online]. Úřad pro ochranu osobních údajů [cit. 10. 6. 2014]. Dostupné z: <http://www.uouu.cz/nalezitosti-souhlasu-se-zpracovanim-osobnich-udaju/d-1768>.

⁹³ BARTÍK, Václav; JANEČKOVÁ, Eva. Souhlas se zpracováním osobních údajů jako součást smlouvy. *Daně a právo v Praxi*. 2012, č. 11, s. 49. In: *ASPI* [právní informační systém]. Wolters Kluwer ČR [cit. 10. 6. 2014].

⁹⁴ TELEC, Ivo. Souhlas, nebo licenční závazek? *Právní rozhledy*. 2013, roč. 21, č. 13–14, s. 457–462. ISSN 1210-6410.

⁹⁵ Srovnej ibid s. 458.

Já se stavím spíše za variantu, že se jedná o jednostranné právní jednání. Utvrzuje mě v tom i existence plnění smlouvy jako samostatného legitimizačního důvodu pro zpracování osobních údajů.⁹⁶ Pokud by byl souhlas dvoustranným právním jednáním, tedy quasi smlouvou, bylo by zpracování na základě této smlouvy legitimizovatelné smlouvou samotnou dle § 5 odst. 2 písm. b) Zákona o ochraně osobních údajů, a nebylo by potřeba souhlasu jako takového. Existence těchto dvou institutů vedle sebe by za takového stavu postrádala smysl, proto je dle mého názoru tento stav možné a nutné vyloučit.

Často je variantě „jednostranné jednání“ vytýkáno, že nese málo jistoty pro správce údajů, který si nikdy nemůže být jistý, jestli jeho model podnikání nebude poškozen svévolným odvoláním souhlasu subjektem údajů. Jak uvádí Nonnemann,⁹⁷ tento problém je alespoň částečně ošetřen obecným požadavkem dobrých mravů a zákonnosti,⁹⁸ který je kladen na právní jednání. Jednání přičící se dobrým mravům, kterým šikanózní odvolání souhlasu zřejmě je, je dle § 580 občanského zákoníku neplatné.

Není ambicí této práce definitivně vyřešit otázku, zda je poskytnutí souhlasu jednostranným nebo dvoustranným právním jednáním. Cílem posledních odstavců bylo upozornit na tento převážně akademický problém a uvést některé zaznívající argumenty.

3. ANALÝZA SOUHLASU SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ

V této kapitole podrobíme souhlas se zpracováním osobních údajů detailnější praktické analýze. Jelikož je účelem souhlasu zajištění kontroly subjektu údajů nad svými daty,⁹⁹ jsou krom běžných požadavků na právní jednání¹⁰⁰ na souhlas se zpracováním kladeny ještě požadavky další, specifické pro tento právní institut. Evropská a česká zákonná úprava jsou

⁹⁶ § 5 odst. 2 písm. b) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů. In: CODEXIS [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

⁹⁷ NONNEMANN, František. Odvolání souhlasu se zpracováním osobních údajů. *Právní rozhledy*. 2011, roč. 19, č. 24, s. 874.

⁹⁸ § 545 Zákona č. 89/2012 Sb., občanský zákoník. In: CODEXIS [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

⁹⁹ Pracovní skupina pro ochranu údajů zřízená podle článku 29. Stanovisko č. 15/2011 k definici souhlasu. WP 187. *Evropská komise* [online]. [cit. 10. 6. 2014]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_cs.pdf. s. 8.

vzhledem k vysoké míře harmonizace velmi podobné. Můžeme proto vycházet zároveň z obou pramenů, přičemž v případě odlišností je rozdílům věnována pozornost. Poslední podkapitola je věnována otázce souhlasu jako součásti smlouvy.

3.1 ROLE SOUHLASU SE ZPRACOVÁNÍM V SYSTÉMU PRÁVA NA OCHRANU OSOBNÍCH ÚDAJŮ

Alena Kučerová v komentáři k Zákonu o ochraně osobních údajů uvádí, že souhlas je dle systematiky Zákonu o ochraně osobních údajů i Směrnice o ochraně osobních údajů základním legitimizačním prostředkem.¹⁰¹ S tímto názorem nemohu zcela souhlasit. Porovnejme znění konkrétních ustanovení. § 5 odst. 2 Zákonu o ochraně osobních údajů říká:

„(2) Správce může zpracovávat osobní údaje pouze se souhlasem subjektu údajů. Bez tohoto souhlasu je může zpracovávat,

a) jestliže provádí zpracování nezbytné pro dodržení právní povinnosti správce,

b) jestliže je zpracování nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro jednání o uzavření nebo změně smlouvy uskutečněné na návrh subjektu údajů,

c) pokud je to nezbytně třeba k ochraně životně důležitých zájmů subjektu údajů. V tomto případě je třeba bez zbytečného odkladu získat jeho souhlas. Pokud souhlas není dán, musí správce ukončit zpracování a údaje zlikvidovat, ...“¹⁰²

Oproti tomu článek 7 Směrnice o ochraně osobních údajů uvádí:

¹⁰⁰ Ty se řídí ustanoveními občanského zákoníku. Obecně můžeme říci, že se jedná o otázky právní osobnosti, svéprávnosti a náležitosti platného právního jednání dle prvního dílu hlavy páté první části občanského zákoníku. Více se jimi v této studii nezabývám. Dále viz například: DVORÁK, Jan; ŠVESTKA, Jirí; ZUKLÍNOVÁ, Michaela et al. *Občanské právo hmotné. Svazek I. Díl první: Obecná část*. Praha: Wolters Kluwer ČR, 2012, 432 s. ISBN 978-80-7478-326-5, MELZER, Filip. Právní skutečnosti (právní jednání, právní události). In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014], nebo BEZOUSKA, Petr; PIECHOWICZOVÁ, Lucie. *Nový občanský zákoník: Nejdůležitější změny*. Olomouc: Nakladatelství ANAG, 2013, 369 s. ISBN 978-80-7263-819-2.

¹⁰¹ Srovnej: KUČEROVÁ, Alena et al. *Zákon o ochraně osobních údajů, Komentář*. 1. Vyd. Praha: C. H. Beck, 2012, s. 89.

¹⁰² § 5 odst. 2 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

„Členské státy stanoví, že zpracování osobních údajů může být provedeno pouze pokud:

a) subjekt údajů nezpochybnitelně uděлил souhlas; nebo

b) je zpracování nezbytné pro splnění smlouvy, kde je subjekt údajů jednou ze stran, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu; nebo

c) je nezbytné pro splnění právní povinnosti, které podléhá správce; nebo

d) je nezbytné pro zachování životně důležitých zájmů subjektu údajů; ...“¹⁰³

Z citovaných textů vyplývá, že tvrzení Kučerové je platné pouze pro českou úpravu, přičemž v ní je použita stejná konstrukce, jako v případě ochrany osobnosti v občanském zákoníku.¹⁰⁴ V evropské Směrnici je však souhlas jen jedním z mnoha legitimizačních důvodů, což potvrzuje i WP29 ve svém stanovisku, když uvádí, že je třeba si uvědomit, že souhlas není vždy hlavním nebo nejvhodnějším legitimizačním prostředkem, a že je třeba ho užívat ve správném kontextu.¹⁰⁵

Domnívám se, že zařazením souhlasu se zpracováním osobních údajů do privilegované pozice oproti ostatním legitimizačním důvodům, se český zákonodárce dopustil značné chyby, která může v konečném důsledku vést ke zhoršení právního postavení subjektu údajů a snížení jeho právní jistoty. Příčinu této chyby lze hledat v převzetí konstrukce ochrany osobnosti dle občanského zákoníku,¹⁰⁶ protože ani ve Směrnici o ochraně osobních údajů,

¹⁰³ Čl. 7 Směrnice Evropského parlamentu a Rady č. 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. In: CODEXIS [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

¹⁰⁴ § 84 zákona č. 89/2012 Sb., občanský zákoník. In: CODEXIS [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014], stejně jako § 12 zákon č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů. In: CODEXIS [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

¹⁰⁵ Pracovní skupina pro ochranu údajů zřízená podle článku 29. Stanovisko č. 15/2011 k definici souhlasu. WP 187. Evropská komise [online]. [cit. 10. 6. 2014]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_cs.pdf. s. 10.

¹⁰⁶ § 12 odst. 1 zákona č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů. In: CODEXIS [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

ani ve starém zákonu zákon o ochraně údajů v informačních systémech¹⁰⁷ v této podobě není.

Znění, které nyní v zákoně je, akcentuje souhlas a navádí k tomu, že správce údajů používá pro legitimizaci zpracování tento institut i tehdy, má-li k dispozici jiné legitimizační důvody. Subjekt údajů se tak může dostat do situace, kdy udělí souhlas se zpracováním, později se třeba rozhodne, že ho odvolá, ale správce mu oznámí, že údaje bude zpracovávat dál, protože má další legitimizační důvod. Efektem této praxe je krom nadužívání institutu souhlasu¹⁰⁸ i zmiňované snížení právní jistoty subjektu.

Tvrdím proto, že souhlas se zpracováním osobních údajů má být ultima ratio legitimizace zpracování údajů v systému ochrany osobních údajů. Má nastoupit až tehdy, kdy žádné jiné možnosti umožňující zpracování nejsou k dispozici, protože ostatní důvody upravují speciální případy, pro které mají přirozeně přednost. Správce má povinnost posoudit, zda jeho plánované zpracování osobních údajů není takovým zákonem předpokládaným speciálním případem, a teprve až zjistí, že není, musí žádat subjekt údajů o souhlas. Není-li tato posloupnost dodržena, dostávají se nežádoucí efekty popsané výše. Toto tvrzení je dopodrobna rozebráno v následující kapitole.

Obecně můžeme říci, že souhlasu bude třeba v případech, kdy má o zpracování zájem primárně správce. Pokud má o službu, jejíž součástí je zpracování údajů, zájem subjekt údajů, může se jako legitimizační prostředek použít například plnění smlouvy, jíž je subjekt stranou. Takové údaje může však správce zpracovávat pouze za účelem plnění této smlouvy, ne za žádným jiným. Pokud by měl zájem zpracovávat údaje i jinak, musí získat souhlas subjektu, byť by za to nabízel nějakou přidanou hodnotu.

3.2 POŽADAVKY NA PLATNÝ SOUHLAS DLE SMĚRNICE A ZÁKONA O OCHRANĚ OSOBNÍCH ÚDAJŮ

Nyní se postupně budeme zabývat jednotlivými požadavky, které musí být splněny, aby byl souhlas platný. Směrnice o ochraně osobních údajů uvádí,

¹⁰⁷ Zákon č. 256/1992 Sb., o ochraně údajů v informačních systémech. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

¹⁰⁸ Které je samo o sobě fatálním problémem institutu souhlasu se zpracováním, jak je podrobně projednáno dále v této práci.

že souhlas má být jakýkoli svobodný, výslovný, vědomý¹⁰⁹ projev vůle udělený nezpochybnitelným způsobem¹¹⁰ a ve stejném smyslu hovoří i Zákon o ochraně osobních údajů. Domnívám se však, že při překladu Směrnice do českého jazyka došlo v tomto místě k chybě. Anglická verze Směrnice v článku 2 písm. h) uvádí, že souhlas má být „*freely given specific and informed*“. Slovo „*specific*“ se sice dá přeložit jako „výslovný“, pro tento význam je však v čl. 8 odst. 2 písm. a), kde česká verze používá rovněž termín „výslovný“, užito slova „*explicit*“. Smyslu, v jakém je slovo „*specific*“ použito, více odpovídá český termín „určitý“, čemuž odpovídá i výkladové stanovisko WP29 k definici souhlasu.¹¹¹ Zajímavostí je, že ač český překlad zmiňovaného stanoviska zachovává znění oficiálního překladu směrnice a uvádí rovněž slovo „výslovný“, pokaždé bezprostředně následuje v závorkách původní anglická varianta, což vzhledem k tomu, že se jedná o jediný případ, kdy se tak děje, samo o sobě nasvědčuje existenci překladového problému. V zájmu srozumitelnosti této práce se odchyluji od oficiálního překladu Směrnice a hovořím-li o tom, že souhlas má být „*specific*“, používám slovo „určitý“. Pojem „výslovný“ užívám ve smyslu „*explicit*“ v souvislosti se souhlasem ke zpracování citlivých osobních údajů.

První podmínkou souhlasu je svoboda jeho udělení. Kučerová uvádí:

„Svobodný je ten souhlas se zpracováním osobních údajů, který subjekt údajů udělil ze své vlastní vůle bez působení takových vnějších vlivů, které by omezovaly jeho možnost samostatně se rozhodnout, zda souhlas udělí či ne.“¹¹²

Aby byl souhlas svobodný, musí mít subjekt údajů k dispozici skutečnou volbu, zda souhlas udělí nebo ne, a nesmí při jeho rozhodování hrát roli riziko vzniku významných negativních následků v případě neudělení.¹¹³ To je ostatně pravidlo každého právního jednání. Pokud subjekt údajů nemá

¹⁰⁹ Čl. 2 písm. h) směrnice Evropského parlamentu a Rady č. 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. In: CODEXIS [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

¹¹⁰ Ibid. čl. 7 písm. a).

¹¹¹ Srovnej Pracovní skupina pro ochranu údajů zřízená podle článku 29. Stanovisko č. 15/2011 k definici souhlasu. WP 187. *Evropská komise* [online]. [cit. 10. 6. 2014]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_cs.pdf. s 17 – 18.

¹¹² KUČEROVÁ, Alena et al. *Zákon o ochraně osobních údajů, Komentář*. 1. Vyd. Praha: C. H. Beck, 2012, s. 90.

možnost výběru, nemůžeme souhlas považovat za platný. Často to je důvod pro zvážení, zda není jiný způsob legitimizace zpracování vhodnější. Příkladem takové situace je vytvoření bankovního účtu. Banka má zákonem danou povinnost zpracovávat o svých klientech určitá data. Důvodem pro zpracování tak nemůže být souhlas, ale splnění zákonem daných povinností správce dle § 5 odst. 2 písm. a).¹¹⁴ Souhlas, i kdyby ho subjekt udělil, by nebyl platný, protože by nebyl dán svobodně, neboť subjekt nemá reálnou možnost volby, chce-li využívat jakékoliv bankovní služby.¹¹⁵ Mohlo by se zdát, že podobným příkladem je například i registrace do on-line služeb, jako je například Facebook, která probíhá způsobem Ber nebo nech být. V tomto případě by však souhlas byl z hlediska svobodnosti v pořádku, protože subjekt údajů má reálnou možnost danou službu nepoužívat. Mohla by zaznít námitka, že nevyužívání služby by vzhledem k jejímu významnému zastoupení na trhu mohlo přinést negativní následky, a tudíž je situace obdobná ke zmiňovanému prvnímu příkladu. Dle mého názoru však takové následky mohou těžko dosáhnout stupně „významných negativních následků“, o jakých hovoří ve výkladovém stanovisku WP29.¹¹⁶ Můžeme však v závislosti na konkrétní situaci říci, že pokud poskytovatel služby odmítne subjektu údajů službu poskytnout, protože mu odmítl dát souhlas ke zpracování osobních údajů se službou nesouvisející, může se jednat o diskriminační praktiku a celý případ může mít přesah do spotřebitelského práva.¹¹⁷

Požadavek na určitost souhlasu se zpracováním není v českém zákoně o ochraně osobních údajů, na rozdíl od evropské Směrnice, výslovně uveden. Je však obsažen v základních podmínkách platnosti právního

¹¹³ Pracovní skupina pro ochranu údajů zřízená podle článku 29. Stanovisko č. 15/2011 k definici souhlasu. WP 187. *Evropská komise* [online]. [cit. 10. 6. 2014]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_cs.pdf. s 13.

¹¹⁴ Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

¹¹⁵ Samozřejmě toto platí pouze pro zpracování údajů, které jsou nezbytné k dosažení účelu stanoveného zvláštním zákonem. Pokud banka nabízí doplňkové služby nad tento rámec, souhlas už by byl vhodný způsob legitimizace.

¹¹⁶ Pracovní skupina pro ochranu údajů zřízená podle článku 29. Stanovisko č. 15/2011 k definici souhlasu. WP 187. *Evropská komise* [online]. [cit. 10. 6. 2014]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_cs.pdf. s 13.

¹¹⁷ Viz NONNEMANN, František. Ochrana spotřebitele a ochrana osobních údajů. *Právní rozhledy*. 2010, roč. 18, č. 22, s. 807-810. ISSN 1210-6410. S. 808.

jednání, jak bylo řečeno v první kapitole této práce. Určitost souhlasu se zpracováním souvisí s povinností správce určit účel a způsob zpracování a informovat o něm subjekt údajů. Můžeme dobře vidět, že určitost souhlasu je jedním z projevů zásady účelové limitace zpracování osobních údajů. Souhlas je tedy dáván právě a pouze k určenému účelu a ke zpracování nezbytnému pro tento účel, protože blanketový souhlas není přípustný. Pokud chce správce údajů data zpracovávat mimo účel vymezený v uděleném souhlasu, musí požádat o souhlas nový. Jako příklad můžeme uvést situaci, kdy uživatel mobilní aplikace sloužící k recenzování navštívených restaurací udělí souhlas provozovateli služby ke zpracování zeměpisných údajů za účelem zobrazení restaurací v uživatelově okolí na mapě v mobilním zařízení. Pokud by však chtěl provozovatel služby používat informace o uživatelově poloze i k jinému účelu, jako například zobrazení polohy účastníkům služby, které má uživatel označené jako přátele, musel by obdržet nový souhlas.

Třetí podmínkou platného souhlasu je, že musí být vědomý a informovaný. Aby mohl subjekt údajů svoji vůli vědomě vyjádřit, musí být informován o všech náležitostech, které se zpracováním údajů souvisejí. Pro platnost souhlasu musí být subjekt údajů schopen chápat a zhodnotit jeho důsledky.¹¹⁸ Informování subjektu údajů musí proběhnout před samotným udělením souhlasu, jak potvrzuje i česká judikatura.¹¹⁹ V českém Zákoně o ochraně osobních údajů je informační povinnost správce upravena na dvou místech. Za prvé, obecná povinnost informovat subjekt při shromažďování údajů je dle § 11 závazná pro všechny způsoby legitimizace zpracování. Stanoví povinnost informovat o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny. Zároveň toto ustanovení povazuje správce informovat subjekt o právu přístupu k osobním údajům, právu na opravu osobních údajů, jakož i o dalších právech stanovených v § 21. Za druhé, § 5 odst. 4 je zvláštní ustanovení, které upravuje informování v průběhu procesu udělení souhlasu. Zakládá povinnost informovat o tom, pro jaký účel zpracování

¹¹⁸ Srovnej ibid s. 19.

¹¹⁹ Rozsudek Nejvyššího správního soudu ze dne 23. srpna 2013, sp. zn. 5 As 158/2012 – 49. In: CODEXIS [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

a k jakým osobním údajům je souhlas dáván, jakému správci a na jaké období.¹²⁰

Nonnemann upozorňuje na fakt, že pro platný souhlas stačí, když jsou splněny podmínky § 5 odst. 4.¹²¹ S tímto tvrzením souhlasím. Důvodem však dle mého názoru není jen časové odlišení shromažďování údajů a počátek zpracování, jak tvrdí, ale i to, že informace, které jsou uvedené v § 11 navíc oproti § 5 odst. 4, jsou zákonem zaručená práva subjektu údajů, která nepředstavují proměnnou hodnotu konkrétního zpracování. Rovněž se ztotožňuji s názorem, že pokud subjekt není informován o skutečnostech uvedených v § 5 odst. 4, nemůže být souhlas považován za platný. Výjimku tvoří informace o období zpracování, která není dle Nonnemanna natolik zásadní, aby její absence způsobila neplatnost souhlasu.¹²² Tuto tezi podporuje, že zmíněná informace není přímo vyžadována Směrnicí o ochraně osobních údajů. Dále by subjektu údajů mělo být zdůrazněno, jaké má možnosti vlastního rozhodování ve věci toho, jaké údaje může poskytnout. Jinými slovy, jaký je rozsah povinných a nepovinných osobních údajů pro dané zpracování.¹²³ Obecně tak platí, že by správci údajů měli udržovat vysokou kvalitu poskytovaných informací. Jak uvádí WP29:

„Čím složitější je zpracování údajů, tím větší nároky jsou kladeny na správce údajů. Čím obtížnější je pro průměrného občana dohlížet na všechny složky zpracování údajů a porozumět jim, tím větší úsilí by měl správce údajů vynaložit, aby prokázal, že byl souhlas získán na základě konkrétních a srozumitelných informací.“¹²⁴

¹²⁰ Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů. In: CODEXIS [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

¹²¹ NONNEMANN, František. Náležitosti souhlasu se zpracováním osobních údajů. *Právní rozhledy*. 2011, roč. 19, č. 14, s. 520-522. ISSN 1210-6410. S. 521.

¹²² *Ibid*, s. 522.

¹²³ § 11 odst. 2 Zákona o ochraně osobních údajů.

Stanovisko Úřadu pro ochranu osobních údajů č. 5/2012, Poskytnutí informací a získání souhlasu subjektu údajů v elektronické komunikaci. *Úřad pro ochranu osobních údajů* [online]. [cit. 10. 6. 2014]. Dostupné z: http://www.uoou.cz/files/stanovisko_2012_5.pdf. S. 2

Jedná se o situaci, kdy jsou zároveň zpracovány údaje nezbytné pro daný účel (ty mohou být obvykle zpracovány na základě jiného důvodu, než je souhlas) a údaje volitelné, které umožní např. rozšíření funkcionality služby (pro ty je souhlas nutný). Více o této problematice v poslední části této kapitoly.

Jak je tato podmínka důležitá, tak je problematická. V době Internetu je pro subjekt údajů nesmírně obtížné představit si, pochopit a vyhodnotit možné důsledky souhlasu se zpracováním. Jak budu demonstrovat v následující kapitole, je takřka nemožné předvídat budoucí dopady současného rozhodnutí. Z tohoto důvodu je na místě se tázat, zda je subjekt údajů vůbec schopen informovaného souhlasu ve smyslu a rozsahu, v jakém si zákon představuje, že by měl být.

Poslední z výše uvedených základních podmínek platného souhlasu je jeho nezpochybnitelnost. Směrnice o ochraně osobních údajů tento požadavek uvádí v čl. 7 písm. a). V českém zákoně tento požadavek není sice výslovně uveden, účinně ho však zastupuje povinnost správce mít schopnost prokázat udělený souhlas po celou dobu zpracování.¹²⁵ Ačkoli, jak již bylo uvedeno v první kapitole, není předepsaná žádná forma souhlasu se zpracováním osobních údajů, nesmí být pochybností o tom, zda souhlas byl nebo nebyl udělen. V případě sporu, zda subjekt souhlas udělil či ne, bude důkazní břemeno prokázání zákonnosti zpracování spočívat na straně správce.¹²⁶ Z tohoto důvodu je problematický souhlas udělený konkludentně, ačkoli tento způsob není zákonem vyloučen. Pro příklad, pop-up notifikace s textem „Užíváním naší stránky souhlasíte se zpracováním osobních údajů“ je hraniční, dle mého názoru však stále platné ustanovení.¹²⁷ Naprostá absence projevu nemůže sloužit jako souhlas za žádných okolností.¹²⁸

Jak evropská, tak česká úprava zavádí přísnější režim pro souhlas s některými zvláštními kategoriemi osobních údajů, které jsou souhrnně označovány jako citlivé osobní údaje. § 4 písm. b)¹²⁹ zahrnuje do této skupiny například údaje vypovídající o národnostním, rasovém nebo

¹²⁴ Pracovní skupina pro ochranu údajů zřízená podle článku 29. Stanovisko č. 15/2011 k definici souhlasu. WP 187. *Evropská komise* [online]. [cit. 10. 6. 2014]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_cs.pdf. s 21.

¹²⁵ § 5 odst. 4, druhá věta zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

¹²⁶ Stanovisko Úřadu pro ochranu osobních údajů č. 2/2008, *Souhlas se zpracováním osobních údajů. Úřad pro ochranu osobních údajů* [online]. [cit. 10. 6. 2014]. Dostupné z: http://www.uouu.cz/files/stanovisko_2008_2.pdf. S. 3.

¹²⁷ Předpokládáme, že všechny ostatní náležitosti pro platný souhlas jsou splněny, subjekt byl řádně informován atd.

¹²⁸ Srovnej DVOŘÁK, Jan; ŠVESTKA, Jiří; ZUKLÍNOVÁ, Michaela et al. *Občanské právo hmotné. Svazek I. Díl první: Obecná část*. Praha: Wolters Kluwer ČR, 2012, s. 158.

etnickém původu, politických postojích, členství v odborové organizaci, náboženství, zdravotním stavu, biometrických a dalších údajích, o kterých zákonodárce předpokládá, že jejich zneužití by pro subjekt údajů mohlo mít vážný dopad. Dle § 9 Zákona o ochraně osobních údajů je citlivé údaje možné zpracovávat na základě souhlasu pouze tehdy, když je daný souhlas výslovný.

3.3 SOUHLAS JAKO SOUČÁST JINÉ SMLOUVY

Jednostranný souhlas se zpracováním osobních údajů je svojí podstatou podobný institutu legitimizace zpracování osobních údajů, z důvodu jejich nezbytnosti pro plnění smlouvy, jíž je subjekt údajů účastníkem dle § 5 odst. 2 písm. b) Zákona o ochraně osobních údajů.¹³⁰ Vztahuje se na veškeré zpracování údajů nezbytné pro plnění smluvního vztahu jak v jeho průběhu, tak v přípravné fázi směřující k jeho uzavření.¹³¹ Podmínkou je, že subjekt údajů musí být smluvní stranou. Tak jako v případě jednostranného souhlasu subjekt údajů dává svým jednáním najevo, že mu nevádí, budou-li jeho osobní údaje zpracovány.

Myslím, že je klidně možné s mírnou nadsázkou považovat poskytnutí souhlasu se zpracováním údajů výměnou za nějakou protihodnotu za obchod svého druhu. Rozdíl mezi souhlasem a zpracováním pro plnění smlouvy spočívá v tom, že v případě smlouvy protihodnota, kterou subjekt za poskytnutí osobních údajů obdrží, přímo souvisí s tímto zpracováním osobních údajů. Bez zpracování osobních údajů by nebylo plnění smlouvy možné. Naopak, v případě pouhého jednostranného souhlasu nemusí subjekt údajů obdržet za jeho poskytnutí žádnou protihodnotu, a pokud ji obdrží, pak ta získaná hodnota přímo nesouvisí se zpracováním údajů.

Příkladem zpracování nezbytného pro plnění smlouvy je webová služba, jejímž účelem je zaznamenávání, sledování a analýza fyzické aktivity uživatele za účelem sportovního tréninku. K údajům, které pro tento účel uživatel poskytuje, již nemusí dávat zvláštní souhlas, protože jejich

¹²⁹ Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

¹³⁰ *Ibid.*

¹³¹ KUCEROVÁ, Alena et al. *Zákon o ochraně osobních údajů, Komentář*. 1. Vyd. Praha: C. H. Beck, 2012, s. 138. ISBN 978-80-7179-226-0.

zpracování je nezbytné pro to, aby služba plnila svoji funkci, pro kterou ji uživatel využívá. Druhým příkladem jsou věrnostní karty obchodních řetězců, kdy uživatel výměnou za své osobní údaje poskytnuté za účelem marketingu obdrží slevu. V tomto případě je třeba uživatele jednostranného souhlasu se zpracováním osobních údajů za daným účelem. Samotné poskytnutí slevy na zboží se zpracováním a jeho účelem nikterak nesouvisí. Do třetice, v případě poněkud absurdního scénáře, kdy subjekt údajů uzavře se správcem smlouvu, jejímž účelem bude na základě chování vytvoření profilu subjektu pro cílení reklamy, bude platným titulem pro zpracování údajů plnění smlouvy a jednostranný souhlas nebude třeba.

Často se stává, že do textu smlouvy je přímo vložen souhlas se zpracováním osobních údajů, které není pro plnění dané smlouvy nezbytné. Tato praxe je velmi problematická hned z několika důvodů.¹³² V takovém textu se totiž kombinuje jednostranné právní jednání, kterým je souhlas se zpracováním údajů, s dvoustranným jednáním, kterým je samotná smlouva. Může to vést k značenému zmatení subjektu údajů, který může nabýt dojmu, že bez poskytnutí a zpracování údajů by nebylo možné danou smlouvu splnit.¹³³ To však není pravda. Domnívám se rovněž, že dle aktuálního znění GDPR je tento způsob navíc přímo zapovězen čl. 7 odst. 4 b),¹³⁴ který, jak jsem již uváděl výše, zakazuje podmiňovat poskytování služeb udělením souhlasu, jenž není pro jejich funkčnost nezbytně nutný. Možný je i druhý chybný výsledek, zmiňovaný již dříve v této kapitole, a to, že subjekt zbytečně poskytne souhlas i ke zpracování, které lze legitimizovat přímo smlouvou a jejím plněním. Takový souhlas je neplatný pro absenci reálné možnosti rozhodnout se.

¹³² Srovnej Stanovisko Úřadu pro ochranu osobních údajů č. 2/2011, Zpracování osobních údajů na základě souhlasu ve smlouvě nebo Všeobecných obchodních podmínkách a s tím související problémy. *Úřad pro ochranu osobních údajů* [online]. [cit. 10. 6. 2014]. Dostupné z: http://www.uouu.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=9185.

¹³³ Srovnej BARTÍK, Václav; JANEČKOVÁ, Eva. Souhlas se zpracováním osobních údajů jako součást smlouvy. *Daně a právo v Praxi*. 2012, č. 11, s. 49. In: *ASPI* [právní informační systém]. Wolters Kluwer ČR [cit. 10. 6. 2014].

¹³⁴ Draft report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM (2012)0011–C7-0025/2012-2012/0011(COD)). *Evropský parlament* [online]. http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf. s. 76. Dostupné z: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf. s. 76.

Aby se předešlo podobným nedorozuměním, je výrazně zvýšen nárok na splnění informační povinnosti ze strany správce. Subjekt by měl vědět, že má možnost souhlas neposkytnout, případně ho odvolat, aniž by to narušilo právní vztah, který je smlouvou založen. Je třeba nezapomínat, a správce údajů by to měl dle mého názoru subjektu výslovně připomenout, že souhlas se zpracováním údajů je na zbytku smlouvy nezávislý.

4. PROBLÉMY A MOŽNÁ ŘEŠENÍ

Jak jsme zjistili v předchozí kapitole, právní institut informovaného souhlasu se zpracováním osobních údajů je propracovaný nástroj, který má zajistit subjektu údajů kontrolu nad jeho osobními daty. Bohužel, jak ukážu v průběhu této kapitoly, lidská povaha ve skutečnosti mnohdy neodpovídá představě, kterou o ní má zákonodárce. Souhlas se zpracováním je jedním z těch institutů, které, byť na papíře vypadají skvěle, v realitě všedního dne se při jejich užití objevují problémy, se kterými zákonodárce nepočítal, a které nemají vždy snadné řešení. V této kapitole se jednotlivými otázkami aplikace souhlasu zabývám a v její poslední části navrhuji možná řešení, která by dle mého názoru mohla situaci pomoci.

4.1 NESCHOPNOST UDĚLIT INFORMOVANÝ SOUHLAS

První z obtíží, kterou jsem již naznačil v předchozí kapitole v části věnované požadavkům na platný souhlas, je neschopnost člověka udělit informovaný souhlas, který by splnil požadavky dané zákonem. Daniel Solove ve své studii¹³⁵ označuje několik dílčích problémů, které znemožňují efektivní rozhodování o ochraně údajů. Ty dále rozřadil do dvou skupin. První označil *kognitivní problémy*.¹³⁶ Zahrnuje subjektivní problémy, jako jsou znalosti a psychologie subjektu údajů. Druhá skupina obsahuje problémy označené *strukturální*,¹³⁷ které souvisí s povahou souhlasu se zpracováním a s jeho užíváním.

¹³⁵ SOLOVE, Daniel J. Privacy Self-Management and the Consent Dilemmas. *Harvard Law Review* [online]. 2013, vol. 126, no. 7, pp. 1880-1903. [cit. 10. 6. 2014] Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018.

¹³⁶ *Ibid*, s. 1883.

¹³⁷ *Ibid*, s. 1888.

4.1.1 KOGNITIVNÍ PROBLÉMY

Ačkoli lidé tvrdí, že se o své soukromí zajímají,¹³⁸ jen málokdo ve skutečnosti čte informace, které jim správci údajů před zpracováním poskytují, a udělují souhlas bez potřebných znalostí. Správci údajů nadarmo investují prostředky, aby splnili zákonné povinnosti, efekt na subjekt údajů je však malý. Informační dokumenty jsou totiž příliš dlouhé, aby obsáhly veškeré zákonem požadované informace, a tak se jim lidé vyhýbají. Frederik Borgesius uvádí,¹³⁹ že průměrný Američan by měl strávit 244 hodin ročně čtením dokumentů informujících o zpracování údajů službami (dále také „privacy policies“ či „podmínky ochrany soukromí“), které online využívá. Tento čas můžeme chápat jako transakční náklady, které by subjekt údajů musel investovat. Vzhledem k tomu, že lidé obecně nepřikládají svým osobním údajům příliš vysokou hodnotu, jak rozebereme dále, je to cena příliš vysoká, kterou subjekt údajů není ochoten investovat. Problémem je rovněž ohromné množství podmínek ochrany soukromí, které by měl subjekt číst. Tento fakt vtipně glosuje Lawrence Lessig:

“If you Google “privacy policy”, you’ll get close to 2.5 billion hits on the Web. And if you click through to the vast majority of them (not that you could do that in this lifetime), you will find that they are among the most incomprehensible legal texts around (and that’s saying a lot). These policies are the product of pre-Internet thinking about how to deal with a policy problem. The government was pushed to “solve” the problem of Internet privacy. Its solution was to require “privacy policies” be posted everywhere. But does anybody read these policies? And if they do, do they remember them from one site to another? Do you know the difference between Amazon’s policies and Google’s?”¹⁴⁰

¹³⁸ Srovnej ACQUISTI, Alessandro; GROSSKLAGS, Jens. Privacy and Rationality in Individual Decision Making. *IEEE Security and Privacy*. 2005, vol. 3, no. 1, pp- 26 – 33. ISSN 1540-7993. In: *Carnegie Mellon University* [online]. [cit. 10. 6. 2014]. Dostupné z: <http://www.heinz.cmu.edu/~acquisti/papers/acquisti.pdf>. s. 4.

¹³⁹ BORGESIOUS, Frederik. *Consent to behavioural targeting in European Law: What are the policy implications of insights from behavioural economics?* [online]. Amsterdam: Institute for Information Law, 2013, 58 s. [cit. 10. 6. 2014]. Dostupné z: <http://www.ivir.nl/staff/borgesius.html>. S. 32.

Lessig má pravdu, když zpochybňuje, zda je člověk schopný zapamatovat si rozdíl mezi jednotlivými službami. Zároveň upozorňuje na druhý problém, kterým je složitost předkládaných textů.

Dle výzkumu, na který odkazuje Borgesius,¹⁴¹ byla více než polovina podmínek ochrany soukromí, zařazených v daném výzkumu, pro většinu amerických uživatelů internetu příliš složitá. Podobné výsledky byly vykázaný i v případě Evropanů.¹⁴² Dilema, které se v tomto případě objevuje, je, jak upřednostnit srozumitelnost a usnadnit tak čtení, a zároveň zachovat dostatečnou informační hodnotu, aby byly splněny zákonné podmínky.¹⁴³

Třetím problémem je, že subjekt údajů často postrádá dostatečné prvotní znalosti, aby mohl posoudit obdržené informace v potřebném kontextu a mohl se tak opravdu informovaně rozhodnout, zda je pro něj zpracování údajů výhodné, nebo alespoň zda pro něj není nebezpečné. Výsledek průzkumu Chrise Hoofnagla ukazuje, že jen 25% z 974 účastníků dokázalo zodpovědět správně tři nebo více z pěti snadných otázek týkajících se ochrany soukromí online.¹⁴⁴ Jako další příklady můžeme uvést situace popisované Alessandrem Acquistim. Ten uvádí, že ačkoli si lidé obecně uvědomují rizika spojená s propojováním různých informací do jednoho celku, jen málo si skutečně připouští efekt, jaký taková propojení mohou být. Pro příklad na otázku jaká je pravděpodobnost jedinečné

¹⁴⁰ LESSIG, Lawrence. *Code version 2.0*. [online]. New York: Basic Books, 2006, 424 s. [cit. 10. 6. 2014]. ISBN 0-465-03914-6. Dostupné z: <http://codev2.cc/download+remix/Lessig-Codev2.pdf>. S. 226. "Když zadáte do Google "privacy policy", dostanete 2,5 miliardy výsledků na Webu. A pokud se většinou z nich proberete (ne že by to bylo možné v tomto životě), zjistíte, že patří mezi nejhůře srozumitelné právní texty vůbec (a to o něčem vypovídá). Tyto informační dokumenty jsou produktem „předinternetového“ způsobu přemýšlení a snahy o vyřešení problému soukromí. Vláda byla donucena "vyřešit" tento problém se soukromím na Internetu. Řešením byl požadavek, aby informační dokumenty byly umístěny takřka všude. Ale čte je vůbec někdo? A pokud ano, vybaví si lidé rozdíly mezi jednotlivými stránkami? Dokáží rozlišit podmínky ochrany soukromí Amazonu a Google?"

¹⁴¹ BORGESIUS, Frederik. *Consent to behavioural targeting in European Law: What are the policy implications of insights from behavioural economics?* [online]. Amsterdam: Institute for Information Law, 2013, s. 32. [cit. 10. 6. 2014]. Dostupné z: <http://www.ivir.nl/staff/borgesius.html>.

¹⁴² Ibid. Jednalo se o více než 25% evropských respondentů.

¹⁴³ VIZ SOLOVE, Daniel J. *Privacy Self-Management and the Consent Dilemmas*. *Harvard Law Review* [online]. 2013, vol. 126, no. 7, s. 1885. [cit. 10. 6. 2014] Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018.

¹⁴⁴ HOOFNAGLE, Chris Jay et al. *How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?* [online]. 2010, 20 s. [cit. 10. 6. 2014]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864. S. 19.

identifikace člověka na základě informace o jeho datu narození, pohlaví a ZIP kódu¹⁴⁵ 68.6 procenta dotázaných odpovědělo, že 50% nebo méně a 45.5 procenta dotázaných odpovědělo, že šance na takovou identifikaci je menší jak 25%. Pravděpodobnost takové identifikace však dosahuje až na 87%.¹⁴⁶ Dalším příkladem je, že ve chvíli kdy informaci, kterou jinak zná, nemá subjekt přímo na očích, zapomene na ní a nebere ji v potaz. To je důvod, proč 34,5% dotázaných zapomnělo na to, že při použití platební karty bude mít informaci o provedeném obchodu nejen obchodník, ale i banka. Tato informace, byť je jinak respondentovi známá, nebyla vůbec zahrnuta do jeho úvahy. Acquisti takovou situaci nazývá „zjednodušený myšlenkový model“.¹⁴⁷ Dalším příkladem zjednodušeného myšlenkového modelu je situace, kdy lidé věří více stránce, na které stojí, že obdržela „pečeť soukromí“, aniž by si již dále zjišťovali detaily o tomto ocenění.¹⁴⁸

Čtvrtý problém Solove nazývá „Problém zkresleného rozhodování“.¹⁴⁹ Ten je popisem situace, kdy se člověk, přestože by byl dokonale informovaný a dovedl si představit následky svých činů, rozhodne proti svému zájmu. Souvisí to se sklony v lidském chování, které vedou k upřednostnění jedné volby před jinou. Borgesius uvádí principy chování původně popsané behaviorální ekonomii, které se takto do oblasti ochrany osobních údajů promítají.¹⁵⁰ Prvním z nich je „krátkozrakost“ – jev, kdy lidé mají tendenci soustředit se spíše na okamžité uspokojení a nehlídají na budoucí náklady. To je důvod, proč lidé i přes předchozí proklamace, že jim na soukromí záleží, dají k dispozici své osobní údaje výměnou za slevovou kartu. Podobně působí v neprospěch subjektu údajů sklon udržet

¹⁴⁵ Americký ekvivalent poštovního směrovacího čísla.

¹⁴⁶ ACQUISTI, Alessandro; GROSSKLAGS, Jens. Privacy and Rationality in Individual Decision Making. *IEEE Security and Privacy*. 2005, vol. 3, no. 1, s. 7. ISSN 1540-7993. In: *Carnegie Mellon University* [online]. [cit. 10. 6. 2014]. Dostupné z: <http://www.heinz.cmu.edu/~acquisti/papers/acquisti.pdf>.

¹⁴⁷ *Ibid.*, s. 8.

¹⁴⁸ Viz BORGESIOUS, Frederik. *Consent to behavioural targeting in European Law: What are the policy implications of insights from behavioural economics?* [online]. Amsterdam: Institute for Information Law, 2013, 58 s. 39. [cit. 10. 6. 2014]. Dostupné z: <http://www.ivir.nl/staff/borgesius.html>.

¹⁴⁹ Viz SOLOVE, Daniel J. Privacy Self-Management and the Consent Dilemmas. *Harvard Law Review* [online]. 2013, vol. 126, no. 7, s. 1886. [cit. 10. 6. 2014] Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018.

¹⁵⁰ BORGESIOUS, Frederik. *Consent to behavioural targeting in European Law: What are the policy implications of insights from behavioural economics?* [online]. Amsterdam: Institute for Information Law, 2013, 58 s. 40 a následující. [cit. 10. 6. 2014]. Dostupné z: <http://www.ivir.nl/staff/borgesius.html>.

status quo.¹⁵¹ Lidé obvykle nechtějí investovat transakční náklady a tak nemění primární nastavení služby, i když z dlouhodobého hlediska by to pro ně bylo výhodnější.

Hovoříme-li o nákladech, je bezpochyby zajímavé zastavit se u otázky, jak si lidé opravdu cení svých osobních údajů a tedy svého soukromí. Marek Kumpošt s Václavem Matyášem se zabývali cenou, za jakou by respondenti jejich průzkumu byli ochotni poskytnout údaje o provozu svého mobilního zařízení a o online komunikaci v závislosti na tom, jaké entitě jsou údaje poskytovány.¹⁵² Jakkoli je ta studie zajímavá, zkoumá jen jednu stranu problému a to hodnotu soukromí při snížení míry jeho ochrany. Jak upozorňuje Acquisti, odpověď na otázku „Jaká je hodnota soukromí?“ závisí nejen na tom, koho se výzkumník zeptá, ale i jak se zeptá.¹⁵³ Jak totiž ukazují výsledky další Acquistiho studie, lidé mají výrazně vyšší tendenci vzdávat se svého soukromí za úplatu, než své soukromí za úplatu posilovat.¹⁵⁴ Tento výsledek jen dokazuje sklony ke krátkozrakosti a zachování statusu quo, o kterých jsem hovořil v minulém odstavci.

Soloveho slovy,¹⁵⁵ kognitivní problémy staví subjekt údajů do obdobné pozice, v jaké se nachází hrdina Kafkovy povídky Před zákonem, který stál před otevřenými dveřmi strážnými sérií hlídačů, každým dalším mocnějším než byl ten předchozí. Lidé nečtou podmínky ochrany soukromí. Pokud je čtou, nerozumí jim. Pokud je čtou a rozumí jim, často postrádají dostatečné znalosti, aby dokázali dát přečtený text do souvislostí a dokázali pochopit následky svého rozhodnutí. A konečně pokud všechny tyto obtíže překonají, rozhodnou se vlivem zkresleného rozhodování proti svému

¹⁵¹ Ibid, s. 41.

¹⁵² KUMPOŠT, Marek; MATYÁŠ, Václav. Jak si lidé cení soukromí? *Zpravodaj ÚVT MU* [online]. Brno: Masarykova univerzita, 2009, roč. 20, č. 1, s. 13-20. [cit. 10. 6. 2014]. ISSN 1212-0901. Dostupné z: <http://www.ics.muni.cz/zpravodaj/articles/626.html>.

¹⁵³ ACQUISTI, Alessandro; JOHN, Leslie; LOEWENSTEIN George. *What is Privacy Worth?* [online]. Carnegie Mellon University, 2010, 45 s. [cit. 10. 6. 2014]. Dostupné z: <http://www.heinz.cmu.edu/~acquisti/papers/acquisti-ISR-worth.pdf>. S. 33.

¹⁵⁴ ACQUISTI, Alessandro; GROSSKLAGS, Jens. When 25 Cents is Enough: Willingness to Pay and Willingness to Accept for Personal Information [online]. *Workshop on the Economics of Information Security*. 2007, 22s. In: Carnegie Mellon University [online]. [cit. 10. 6. 2014]. Dostupné z: <http://weis2007.econinfosec.org/papers/66.pdf>. S. 1.

¹⁵⁵ Viz SOLOVE, Daniel J. Privacy Self-Management and the Consent Dilemmas. *Harvard Law Review* [online]. 2013, vol. 126, no. 7, s. 1888. [cit. 10. 6. 2014] Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018.

racionálnímu zájmu. Již z těchto podkladů je zřejmé, že funkčnost modelu informovaného souhlasu je značně podkopána.

4.1.2 STRUKTURÁLNÍ PROBLÉMY

Tyto problémy se týkají vlastností souhlasu se zpracováním osobních údajů a jsou pokračováním problémů kognitivních. Prvním z nich je *problém rozsahu*,¹⁵⁶ který pomáhá osvětlit, proč lidé podmínky ochrany soukromí spíše nečtou. Subjekt údajů by teoreticky mohl dokázat vědomě hlídat a kontrolovat, jaké souhlasy k jakým účelům a v jakém rozsahu dává, pokud by takových souhlasů nebylo mnoho. V současné situaci, kdy je třeba podobných rozhodnutí dělat řádově stovky, není kontrola nad svými osobními údaji v lidských silách. Solove tento stav přirovnává¹⁵⁷ k situaci studenta, který dostane od několika učitelů text k přečtení do druhého dne. Ač samy o sobě jsou to úkoly snadno splnitelné, jsou-li zadány takto hromadně, student je splnit prostě nemůže. Naopak je určitá šance, že celý proces bude zcela kontraproduktivní, jelikož takto přetížený člověk na plnění nejspíše rezignuje.

Druhý strukturální problém je *problém agregace*.¹⁵⁸ Je povahou osobních údajů, že jejich efekt se umocňuje, pokud jsou shromážděny na jednom místě ve větším množství. Není v možnostech průměrného člověka pamatovat si při množství udělených souhlasů se zpracováním jejich konkrétní podmínky. Může tak nastat situace, že ačkoli samostatně jsou data nezávadná a k jejich zpracování je dán platný souhlas, spojí se nějakým způsobem s jinými údaji a dohromady vytvoří informaci, k jejímuž zpracování by subjekt údajů souhlas nedal. K tomu navíc může dojít až po velice dlouhé době. Tento problém se může obrátit i proti správci údajů. Pokud totiž ze spojení dat vyplynou informace spadající do kategorie citlivých osobních údajů, potřeboval by k jejich zpracování výslovný souhlas subjektu. Bez něj nemůže ke zpracování dojít. Proti *problému agregace* působí zásada limitace zpracování účelem. Nemělo by docházet k náhodnému spojování údajů, jelikož by se zřejmě jednalo o zpracování v rozporu s původním účelem, k jakému byly údaje poskytnuty. Na druhou

¹⁵⁶ Ibid.

¹⁵⁷ Ibid, s. 1889.

¹⁵⁸ Ibid.

stranu, je-li účel dostatečně široký, ale stále dle zákona přijatelný, k agregaci dojít může. Výsledkem je, že vzhledem k tomu, že průměrný člověk spíše neví, jaké údaje kdy poskytnul, nedokáže řádně vyhodnotit, jaký důsledek bude mít souhlas s poskytnutím dalších údajů. Tím je narušen předpoklad informovanosti při udělení souhlasu.

Třetí strukturální problém je *problém odhadnutí možné budoucí újmy*.¹⁵⁹ Vzhledem k tomu, že újma způsobená narušením ochrany osobních údajů se může projevit až za značně dlouhou dobu, jak ukazuje *problém agregace*, lidé mají obecně tendenci podceňovat možné negativní následky, které poskytnutí údajů může mít. Je to projev přílišného optimismu, co se budoucnosti týče. Tak jako lidé podceňují riziko dopravní nehody nebo nemoci, nebo přeceňují své šance na výhře v loterii, tak podceňují rizika spojená s poskytnutím osobních údajů.¹⁶⁰ Zároveň se s tím pojí, že lidé obecně více podceňují rizika, která jsou pro ně hůře představitelná, než rizika, která si představit dokáží.¹⁶¹ Hezký příklad takového jednání uvádí Acquisti. Dle jeho výzkumu¹⁶² značné procento lidí učinilo kroky proti nechtěnému nabízení obchodních produktů přes telefon, zatímco 82,3% respondentů nikdy neaktivovalo výstrahu pro případ zneužití kreditní karty, ačkoli možné následky jsou mnohonásobně závažnější. Acquisti to odůvodňuje tím, že je budoucí možné riziko vzdálené a poplatky za zřízení výstrahy jsou přítomné v okamžik rozhodnutí. Dle mého názoru s tím souvisí i naznačená abstraktnost možné škody oproti reálné a známé zkušenosti s nepříjemným a obtěžujícím telefonním marketingem.

Strukturální problémy souvisejí s těmi kognitivními. Některé jim předchází, jiné následují. Společně pak tvoří účinnou překážku zamezující subjektu údajů efektivně rozhodovat o tom, jak se svými údaji naloží.

¹⁵⁹ Ibid, s. 1891.

¹⁶⁰ Srovnej BORGESIOUS, Frederik. *Consent to behavioural targeting in European Law: What are the policy implications of insights from behavioural economics?* [online]. Amsterdam: Institute for Information Law, 2013, 58 s. 40 a následující. [cit. 10. 6. 2014]. Dostupné z: <http://www.ivir.nl/staff/borgesius.html>.

¹⁶¹ Člověk obvykle začne pečlivě zálohovat data až poté, co se zničí disk s daty nezalohovanými.

¹⁶² ACQUISTI, Alessandro; GROSSKLAGS, Jens. *Privacy and Rationality in Individual Decision Making. IEEE Security and Privacy*. 2005, vol. 3, no. 1, s. 9. ISSN 1540-7993. In: Carnegie Mellon University [online]. [cit. 10. 6. 2014]. Dostupné z: <http://www.heinz.cmu.edu/~acquisti/papers/acquisti.pdf>.

4.2 SOUHLAS JAKO FETIŠ

Výše nastíněné problémy mají jeden společný prvek, který některé vytváří a jiné „jen“ umocňuje. Je jím nadužívání institutu souhlasu v každodenním životě. Subjekt údajů je vystavován nutnosti souhlasit, a tedy v ideálním případě zvažovat důsledky své akce na své soukromí, až příliš často. Správci údajů, notně podporováni i zákonodárci a výkladovými orgány, na tento institut neadekvátně spoléhají. Souhlas je používán i v situacích, kdy ho není třeba. Je-li správce v pochybnostech, zda je možné údaje zpracovávat na základě některého z dalších důvodů, žádá subjekt o souhlas „jen tak pro jistotu“. Souhlas je vzýván jako univerzální důvod pro zpracování a je s ním tak i nakládáno. Tento stav nazývám *fetišismus souhlasu*.

Jak jsem již argumentoval v předchozích kapitolách, souhlas je jen jedním z možných zákonných důvodů pro legitimizaci zpracování údajů. Pokud je tento nástroj použit špatně, nemůže sloužit svému účelu, kterým je umožnit subjektu údajů rozhodnout se, jak naloží se svým soukromím. Nadužívání souhlasu způsobuje přetížení uživatele a ten pak přestane přikládat tomuto aktu jakoukoliv důležitost. Jak uvádí Beyleveld s Brownswordem:

“A recurring theme ... is that the lifeline offered by consent as a justification should not be abused. If we are to take consent seriously, at a practical level, we must guard against the ‘routinisation’ of consent; it will not do simply to direct a would-be consenting agent ‘to sign here and here’ or ‘just to tick the box’. Steps should be taken to ensure that the standards governing the adequacy of consent are fully articulated and stringently applied. The collection of consent, however commonplace, should not be approached in a mechanical or a perfunctory manner. ... Where substantive justification is called for, we should settle for nothing less; in particular, we should not be satisfied with artificial procedural justifications that are tendered in their place.”¹⁶³

¹⁶³ BEYLEVELD, Deryck; BROWNSWORD, Roger. *Consent in the Law*. Oxford and Portland: Hart Publishing, 2007, s. 63.

To, před čím autoři uvedeného citátu varují, se v případě souhlasu se zpracováním osobních údajů přesně stalo. Je to rutinní záležitost, které nikdo nepřikládá dostatečnou pozornost a důležitost. Zákonodárce a interpretační autority se však stále tváří, že je vše zcela v pořádku a v rámci udržení této překrásné fikce dále podnikají kroky, které roli souhlasu zvyšují. Zavedení režimu opt-in v případě cookies a podobných technologií, o kterých budu dále hovořit v příští kapitole, je takovým případem. Úplně stejným způsobem vyznívá i návrh nového Nařízení Rady o ochraně osobních údajů (GDPR), které například v článku 4 odst. 8 hovoří o výslovnosti jako povinné náležitosti souhlasu.¹⁶⁴

Pokud nedojde k nějaké zásadní změně v přístupu, bude institut souhlasu se zpracováním údajů stále více a více ztrácet svůj smysl, kvůli praktické nepoužitelnosti.

4.3 JE SOUHLAS MRTVÝ?

V nedávné době se začaly šířit hlasy, že koncept ochrany soukromí a osobních údajů tak jak ho známe v dnešní podobě je překonán vlivem nových technologií a novým nakládáním s osobními údaji, jako je například Internet of things,¹⁶⁵ big data¹⁶⁶ a další. Tyto hlasy tvrdí, že souhlas je mrtvý. Podobné názory silně rezonovaly v listopadu 2013 na workshopu *Internet of Things* pořádaným americkou Federal Trade Commission.¹⁶⁷ Text

„Opakujícím se tématem ... je, že záchranné lano ospravedlnění akce, poskytované souhlasem, nesmí být zneužito. Pokud máme brát souhlas v každodenním životě vážně, musíme se chránit před jeho "rutinizací". Nemůže stačit jednoduše navést subjekt, aby "zde podepsal" a "pouze zaškrtnl políčko". Měli by být učiněny kroky, které zajistí, že pravidla určující adekvátnost souhlasu budou striktně dodržována. Jakkoli je užití požadování souhlasu běžné, nesmí být mechanické nebo ledabylé. Když je třeba oprávnění založené hmotným právem, neměli bychom se spokojit s ničím menším; konkrétně bychom neměli být uspokojeni umělou procesní legitimizací nabízenou na jeho místě.“

¹⁶⁴ Návrh Nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů), COM(2012) 11 final, 2012/0011. In: *EUR-Lex* [právní informační systém]. Úřad pro publikace Evropské unie [cit. 10. 6. 2014]. Dostupné z: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_cs.pdf.

¹⁶⁵ Fenomén samostatných zařízení připojených a komunikujících přes Web bez přítomného lidského faktoru.

¹⁶⁶ Automatické zpracování velkého množství dat, soustředící se převážně na odchylky od normálního stavu.

¹⁶⁷ Viz JACOBS, David. Reports of the Death of Consent Have Been Greatly Exaggerated. *Privacy Rights Blog@epic.org* [online]. Electronic Privacy information Center, publikováno 28. 1. 2014 [cit. 10. 6. 2014]. Dostupné z: <http://epic.org/blog/2014/01/reports-of-the-death-of-consent-have-been-greatly-exaggerated-1.html>.

Christophera Wolfa,¹⁶⁸ zveřejněný před zmiňovaným workshopem, popisuje, dle jeho slov, nezbytnou změnu paradigma. Wolf doslova píše:

„The Internet of Things relies on frequent, often continuous, data inputs and transmissions from a broad array of connected devices. If the only way to authorize the collection of personal data were based on traditional notice and choice, individuals would be prompted to consent to data collection and use each time they bumped into new connected devices. That could occur hundreds or thousands of times a day. Not only would that substantially slow the data transmissions underlying the Internet of Things, it would be incredibly burdensome for individuals and could hinder the development of innovative new technologies.

It is unrealistic to expect that individuals will be willing or able to effectively register their informed preferences in a world where they are regularly prompted to read and accept notices of complex data collection, use, and sharing practices. Individuals may end up blindly accepting data practices rather than having to endure reading yet one more privacy disclosure. Instead of protecting privacy, strict adherence to traditional notice and choice principles may drive individuals to give up.“¹⁶⁹

Na Wolfův článek navázali další autoři. Stenley Crosley otevřeně říká „Soukromí a jeho ochrana, jak je známe dnes, je mrtvé.“¹⁷⁰ Eduardo Ustaran jde ve vyjádření ještě dál a tvrdí, že nejen, že je souhlas mrtvý, ale že je

¹⁶⁸ WOLF, Christopher; POLONETSKY, Jules. An Updated Privacy Paradigm for the “Internet of Things”. Future of Privacy Forum [online]. Future of privacy, 2013, 12 s. [cit. 10. 6. 2014]. Dostupné z: <http://www.futureofprivacy.org/wp-content/uploads/Wolf-and-Polonetsky-An-Updated-Privacy-Paradigm-for-the-%E2%80%9CInternet-of-Things-%E2%80%9D-11-19-2013.pdf>.

¹⁶⁹ Ibid, s. 4-5. „Internet of Things spoléhá na časté, obvykle nepřetržité, datové stopy a přenosy ze široké množiny připojených zařízení. Pokud by jediná možnost autorizace sběru osobních údajů byla založena na tradičním principu upozornění a volby, jednotlivci by byli nuceni souhlasit se sběrem údajů pokaždé, když vrazí do nových připojených zařízení. To se může stát stokrát nebo tisíckrát denně. Nehen, že by tato povinnost získat souhlas významně zpomalila přenos dat v Internet of Things, byla by zároveň neuvěřitelně zatěžující pro subjekty údajů a mohla by představovat překážku vývoje nových technologií.

Je nerealistické očekávat, že by jednotlivci byli ochotni nebo schopni efektivně udělovat informované souhlasy ve světě, kde by byli pravidelně nuceni číst a přijímat oznámení o komplexním zpracování osobních údajů. Nakonec jednotlivci mohou jen slepě přijímat podmínky ochrany soukromí, než aby se donutili k přečtení dalšího dokumentu. Místo ochrany soukromí může lpění na tradičním konceptu upozornění a volby subjekty údajů o soukromí připravit.“

nebezpečné, budeme-li mu nadále přikládat klíčovou úlohu v ochraně soukromí,¹⁷¹ protože možná kontrola subjektu nad jeho soukromím se reálně snižuje. Pokud zákonodárce bude trvat na používání souhlasu, dává tak plané naděje, že s tímto právním institutem subjekt něco zmůže.

Jak správně poznamenává David Jacobs,¹⁷² tato tvrzení jsou do značné míry založena na nepochopení institutu souhlasu. Dle mého názoru toto nepochopení souvisí právě s étosem fetiše, který kolem sebe souhlas má. Výše zmínění autoři totiž zapomněli, že souhlas není a nikdy neměl být univerzální prostředek k legitimizaci zpracování. To, že je tak v současné době mnohými vnímán, je nešťastné, ale není to vina tohoto právního institutu.

Domnívám se, že souhlas se zpracováním údajů není mrtvý. Jeho role jako prostředku vyjádření vůle subjektu údajů bude zachována. Určitou míru významu mu nakonec zachovávají i autoři, kteří jeho smrt hlásají. Důležitým faktorem myslím je i to, že citovaní autoři pocházejí z oblasti amerického práva, které má, oproti právu evropskému, v oblasti ochrany osobních údajů výrazně méně paternalistický přístup a více spoléhá na souhlas jako prostředek managementu soukromí.¹⁷³ „Smrt souhlasu“ má tak v americkém případě poněkud jiné konotace, než v případě evropském. Je však jisté, že současný přístup k ochraně osobních údajů a zapojení souhlasu do tohoto konceptu je třeba aktualizovat a přizpůsobit realitě 21. století.

¹⁷⁰ CROSLY, Stanley W. Old School Privacy is Dead, But Don't Go Privacy Crazy. *Privacy Perspectives* [online]. IAPP, publikováno 20. ledna 2014. [cit. 10. 6. 2014]. Dostupné z: https://www.privacyassociation.org/privacy_perspectives/post/old_school_privacy_is_dead_but_dont_go_privacy_crazy.

¹⁷¹ USTARAN, Eduardo. Yes, Consent Is Dead. Further, Continuing To Give It A Central Role Is Dangerous. *Privacy Perspectives* [online]. IAPP, publikováno 18. prosince 2013. [cit. 10. 6. 2014]. Dostupné z: https://www.privacyassociation.org/privacy_perspectives/post/yes_consent_is_dead_further_continuing_to_give_it_a_central_role_is_dangerous.

¹⁷² Viz JACOBS, David. Reports of the Death of Consent Have Been Greatly Exaggerated. *Privacy Rights Blog@epic.org* [online]. Electronic Privacy information Center, publikováno 28. 1. 2014 [cit. 10. 6. 2014]. Dostupné z: <http://epic.org/blog/2014/01/reports-of-the-death-of-consent-have-been-greatly-exaggerated-1.html>.

¹⁷³ Srovnej SOLOVE, Daniel J. Privacy Self-Management and the Consent Dilemmas. *Harvard Law Review* [online]. 2013, vol. 126, no. 7, s. 1897. [cit. 10. 6. 2014] Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018.

4.4 MOŽNÁ ŘEŠENÍ

Lessig tvrdí, že opravdovou výzvou pro digitální dobu je vytvoření možnosti smysluplné volby spotřebitele ohledně jeho soukromí.¹⁷⁴ S tím nelze než souhlasit. Řada autorů navrhla různé varianty řešení a více či méně se dobírali obdobných výsledků. Zachování možnosti subjektu údajů efektivně rozhodovat o svých osobních údajích, či snad lépe její znovuvytvoření, je zcela klíčové. V této části představuji několik dle mého názoru možných konceptů, které by mohly k takovému cíli vést. Jejich společným znakem je snížení transakčních nákladů, tedy času, který subjekt údajů musí vložit do procesu rozhodování o svých údajích. Možná řešení jsou řazena vzestupně dle jejich legislativní a praktické náročnosti. Byť je probírám postupně, nemyslím si, že jsou izolované. Je samozřejmé, že lepšího celkového efektu by bylo dosaženo, kdyby byly kombinovány.

4.4.1 AKCENTOVÁNÍ SPRÁVNÉHO UŽITÍ SOUHLASU

Nejjednodušším způsobem je za pomoci soustavného mírného tlaku a informování veřejnosti opustit souhlasový fetišismus a změnit paradigma nahlížení na souhlas se zpracováním osobních údajů. Postupným procesem by se tak dalo docílit toho, že nebude vnímán jako univerzální řešení vhodné pro všechny situace, ale bude užíván opravdu jen tehdy, kdy ho bude třeba. Je proto třeba změnit i rétoriku zákonodárce, výkladových orgánů a odborníků na ochranu osobních údajů. Dokud budou experti nadále tvrdit, že „povinnost správce získat souhlas subjektu údajů je jedním z klíčových principů ochrany osobních údajů,¹⁷⁵ bez toho, aby dodali, že je pouze jedním z několika důvodů ke zpracování,¹⁷⁶ bude obtížné náhled veřejnosti změnit.

Jsem přesvědčen o tom, že ve většině případů každodenního života není i za zachování současného právního režimu souhlasu ke zpracování osobních údajů potřeba. Valnou většinu zpracování, jak offline tak online, je možné legitimizovat jinými zákonnými důvody, jako je zpracování z důvodu plnění smlouvy, zpracování z důvodu plnění právní povinnosti

¹⁷⁴ LESSIG, Lawrence. *Code version 2.0*. [online]. New York: Basic Books, 2006, s. 228 [cit. 10. 6. 2014]. Dostupné z: <http://codev2.cc/download+remix/Lessig-Codev2.pdf>.

¹⁷⁵ MATOUŠOVÁ, Miroslava; HEJLÍK, Ladislav. *Osobní údaje a jejich ochrana*. 2. Vyd. Praha: ASPI, Wolters Kluwer, 2002, s. 224.

¹⁷⁶ Byť uvedený na prvním místě.

správce, nebo zpracování z důvodu ochrany chráněného zájmu správce. Jak jsem již jednou uváděl v předchozí kapitole, institutu souhlasu je třeba jako ultima ratio tehdy, když jiný důvod pro zpracování není k dispozici. Aby bylo možné tohoto stavu dosáhnout, bylo by zřejmě třeba i pečlivějšího dozoru ze strany státního orgánu ochrany osobních údajů.

V případě, že by bylo souhlasu důsledně používáno jen tehdy, když je nezbytný, pokleslo by množství požadavků na souhlas, které jsou kladeny na subjekt údajů, čímž by narostla subjektivní pocitová důležitost takové situace. Když už by se nějaký takový požadavek objevil, byl by to pro subjekt znamením, že se toto zpracování nějak liší od ostatních zpracování, o kterých je jen informován.¹⁷⁷ V tu chvíli by byl subjekt údajů ostražitější a význam, který by danému zpracování přikládal, by byl vyšší. Díky tomu by byla i větší šance, že se bude rozhodování více věnovat a nebude se jednat jen o rutinní záležitost.

4.4.2 ZAJIŠTĚNÍ SROZUMITELNOSTI SDĚLENÍ

Další problém, který je třeba vyřešit, je, že daným textům nikdo nerozumí. Stejně jako se dá apelovat na správce údajů, aby o souhlas žádali jen tehdy, když je nezbytně nutný, dá se na ně apelovat, aby psali své informační dokumenty příznivěji pro běžného uživatele. Na druhou stranu, složitost těchto dokumentů je často dána právě snahou správců splnit zákonné požadavky informování subjektu.¹⁷⁸

Možným řešením je inspirovat se Creative Commons – vytvořit a používat pro indikaci zpracování osobních údajů podobný systém grafických značek. Myslím, že je možné vytvořit seznam nejčastějších účelů zpracování a dalších jevů jako předávání údajů do zahraničí nebo třetím osobám. Názorné značky mohou pomoci subjektu údajů v orientaci. Navíc, pokud by uživatelé mohli udělovat značky přímo sami,¹⁷⁹ byl by naplněn i požadavek granularity souhlasu údajů. Tím je myšlen ideální stav, kdy má subjekt údajů v rukou možnost přesně určit, které údaje chce správci jak

¹⁷⁷ Nesmíme zapomenout, že informační povinnost správce se vztahuje na všechna zpracování s výjimkou případů uvedených v §11 odst. 3 Zákona o ochraně osobních údajů.

¹⁷⁸ Srovnej MYŠKA, Matěj et al. Creative Commons and Grand Challenge to Make Legal Language Simple. *AICOL Workshops* [online]. Berlin, Heidelberg, 2011, pp. 271 – 285. [cit. 10. 6. 2014] Dostupné z: http://link.springer.com/chapter/10.1007/978-3-642-35731-2_19. S. 276.

¹⁷⁹ Nebyli by tedy postaveni před volbu Ber nebo nech být, ale museli by aktivně určit, jaká oprávnění správci udělí.

poskytnout. Granularita souhlasu v současné době není příliš využívána pro přílišnou komplikovanost a nároky jak na správce (příprava), tak na subjekt údajů (pochopení textu).

Podobným způsobem jako grafické značky může ještě snadněji fungovat systém barevných indikací. Uživatel by v okamžiku udělování souhlasu viděl barevně označenou rizikovost daného zpracování. Například zelená by mohla znamenat bezpečné zpracování správcem a jeho přímými zpracovateli bez předávání údajů do zahraničí, nebo jen v rámci Evropské unie, oranžová zpracování údajů třetími stranami pro komerční účely a předávání údajů do mimoevropských zemí s vysokými standardy na ochranu osobních dat a červená rizikové zpracování, při kterém jsou data předávána do zemí s nízkou kvalitou ochrany osobních údajů, nebo kde hrozí velké riziko zneužití. Aby měly takové barvy opravdu vypovídající hodnotu, bylo by zapotřebí nezávislé autority, která by barevná pásma určovala. Možné řešení nabízí GDPR, které v čl. 33 předpokládá povinnost správce vypracovat posouzení dopadu zpracování na ochranu údajů.¹⁸⁰ Na základě tohoto posouzení by mohlo být chystané zpracování údajů zařazeno do některé z barevných zón. Určování, do jaké barevné zóny daný správce spadá, však nemusí být jen na úřední moci. Mohou existovat nezávislé soukromé subjekty zabývající se takovou činností, kterým by úřad jen dával oprávnění, že takovou činnost mohou provádět, a následně je kontroloval a zaručoval jejich důvěryhodnost.¹⁸¹ Kredibilita těchto společností by tak byla garantována státem a subjekt údajů by nemusel investovat čas do ověřování zdroje hodnocení.

4.4.3 AUTOMATIZOVANÝ SOUHLAS

Lessig uvádí, že problém spočívající v zajištění ochrany údajů uživatele v kyberprostoru a zároveň zachování jeho reálné možnosti ovlivnit, jak bude s jeho údaji nakládáno, může být vyřešen programovým nastavením

¹⁸⁰ Čl. 33. návrhu Nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů), COM(2012) 11 final, 2012/0011. In: *EUR-Lex* [právní informační systém]. Úřad pro publikace Evropské unie [cit. 10. 6. 2014]. Dostupné z: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_cs.pdf. Tuto problematiku řeší také recitály 70 a následující.

¹⁸¹ Viz BORGESIUŠ, Frederik. *Consent to behavioural targeting in European Law: What are the policy implications of insights from behavioural economics?* [online]. Amsterdam: Institute for Information Law, 2013, s. 49 [cit. 10. 6. 2014]. Dostupné z: <http://www.ivir.nl/staff/borgesius.html>.

služeb, jejich kódem. Prostředkem, kterým toho lze dosáhnout je PET („private enhancing technology“, neboli „technologie podpory soukromí“),¹⁸² která na jedné úrovni automaticky sděluje vnějším službám jen ty informace, které potřebují zpracovávat ke svému správnému fungování. Na druhé úrovni se nachází protokol zvaný Platforma pro preference soukromí („P3P“, „Platform for Privacy Preferences“), která by umožnila strojově čitelné vyjádření přání uživatele týkající se soukromí a sdělování údajů. Lessig pokračuje:

“It would enable an automatic way for an individual to recognize when a site does not comply with his privacy preferences. If you surf to a site that expresses its privacy policy using P3P, and its policy is inconsistent with your preferences, then depending upon the implementation, either the site or you are made aware of the problem created by this conflict. The technology thus could make clear a conflict in preferences. And recognizing that conflict is the first step to protecting preferences.”¹⁸³

Lessig předpokládá, že technologie umožní snížit transakční náklady natolik, že nebude pro subjekt údajů překážkou věnovat se plně rozhodnutí, zda svá data poskytne, či nikoli.

Daniel Le Metayer uvažuje podobně. Pokud technologie způsobila obtíže na poli ochrany soukromí a osobních údajů, proč by nám tyto problémy opět technologie nepomohla vyřešit?¹⁸⁴ Oproti Lessigovi jde ve svých úvahách ještě dál. Předpokládá existenci systému automatického elektronického zástupce – programu, skrz který může subjekt údajů vyjádřit svá přání na zpracování. Le Metayer předpokládá propojenou strukturu složenou ze tří částí. První částí je klient běžící na koncovém zařízení subjektu údajů. Do něj subjekt údajů zadá, jaká data chce poskytnout pro jaké účely zpracování. Druhá část běží v systému správce, se kterým subjekt

¹⁸² LESSIG, Lawrence. *Code version 2.0*. [online]. New York: Basic Books, 2006, s. 226 [cit. 10. 6. 2014]. Dostupné z: <http://codev2.cc/download+remix/Lessig-Codev2.pdf>.

¹⁸³ Ibid. „Umožnilo by to automatický způsob, jak může jednotlivec rozpoznat, kdy stránka neodpovídá jeho představám o soukromí. Pokud surfujete na stránce, která má vyjádřené své podmínky ochrany soukromí za pomoci protokolu P3P, a tyto podmínky nejsou v souladu s vaším nastavením, potom dle nastavení služby, buď stránka, nebo vy budete upozorněni na problém, který konfliktem vzniknul. Tato technologie tak jasně ukazuje na konflikt mezi požadavkem stránky a zákazníka. A rozpoznání takového konfliktu je prvním krokem k ochraně těchto požadavků.“

¹⁸⁴ MÉTAYER, Daniel Le; MONTELEONE, Shara. Automated consent through privacy agents: Legal requirements and technical architecture. *Computer law & Security review*. 2009, vol. 25, no. 2, pp. 136-144. ISSN 0267-3649. S. 137.

komunikuje. Správce zde zadá, jaká data potřebuje a chce zpracovávat pro jaké účely. Pokud tomu odpovídají přání subjektu údajů, která před tím vyjádřil ve svém klientu, data se automaticky předají. Třetí část je představována nezávislým dozorovým agentem, jehož úlohou je certifikovat pravdivost a identitu správce a hlídat vykonání transferu. Podmínky na určení účelu zpracování a informování předem jsou splněny, jelikož je subjekt údajů vlastně určuje sám.

Ačkoli tento způsob přináší otázky, na které Le Meayer ostatně sám upozorňuje, jako například, kdo bude odpovědný za nezákonné zpracování údajů v případě pochybení systému, představuje, myslím, poměrně zajímavou možnost vyřešení přítomného problému.

4.4.4 KOMPLEXNÍ ZMĚNA OCHRANY OSOBNÍCH ÚDAJŮ

Jak mnozí autoři tvrdí, je možné, že současný model ochrany soukromí, a konkrétně osobních údajů, vyžaduje hlubší změny. Ukazuje se totiž, že může být výhodné jak pro subjekt údajů, tak pro celou společnost, zpracovávat získané údaje i jinými způsoby a za jinými účely, než pro které byly původně sbírány. V případě velkého množství dat je nesmírně náročné a ekonomicky nevýhodné získávat nový souhlas ke zpracování a praktické využití umožňující odhalení hodnotných poznatků by tak bylo znemožněno. V tomto oddílu uvádím několik konceptů, které mohou napomoci v řešení panujícího problému.

Možnou cestou je postupovat obdobně jako v případě pracovního práva, nebo práva na ochranu spotřebitele, jak uvádí Lessig,¹⁸⁵ a přesněji ohraničit svobodu volby správců i subjektů. Solove píše,¹⁸⁶ že je třeba sejmout ze subjektu údajů břímě povinnosti znát problematiku ochrany soukromí natolik, aby byl schopen se správně rozhodovat. Veřejná moc by měla zajistit určitou míru bezpečnosti zpracování údajů, tak jako je zajištěna určitá kvalita spotřebitelských výrobků. Tento názor rezonuje i texty autorů tvrdících, že souhlas se zpracováním je mrtvý. Ustaran tvrdí, že právo by mělo přestat tolik regulovat subjekty údajů, ale soustředit se více na

¹⁸⁵ LESSIG, Lawrence. *Code version 2.0*. [online]. New York: Basic Books, 2006, s. 227 [cit. 10. 6. 2014]. ISBN 0-465-03914-6. Dostupné z: <http://codev2.cc/download+remix/Lessig-Codev2.pdf>.

¹⁸⁶ SOLOVE, Daniel J. Privacy Self-Management and the Consent Dilemmas. *Harvard Law Review* [online]. 2013, vol. 126, no. 7, s. 1901. [cit. 10. 6. 2014] Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018.

správce.¹⁸⁷ Je třeba změnit zaměření z otázky „Jak jsou osobní údaje sbírány?“ na otázku „Jak jsou osobní údaje používány?“.

Jako dobré řešení se nabízí širší využívání anonymizace a pseudonymizace údajů. Tato metoda, kterou hojně prosazuje například Wolf,¹⁸⁸ umožňuje zpracovávat údaje bez nutnosti souhlasu subjektů údajů, jelikož díky procesu pseudonymizace data přestávají mít schopnost identifikovat konkrétní subjekt, přestávají spadat do definice osobních údajů a dostávají se tak mimo záběr právní úpravy chránící osobní údaje. Ač tento způsob určitě dokáže pomoci ochraně soukromí, má jisté limity, které je třeba mít na zřeteli.¹⁸⁹ Základní problém, se kterým se anonymizace potýká, je nepřímá úměra mezi užitečností údajů a mírou anonymity subjektů. Neexistuje nic jako dokonalá anonymizace, a pokud ano, bude zcela neúčinná. Vždy hrozí riziko zpětné identifikace, čímž by se zpracovávaná data opět dostala pod věcnou působnost legislativy chránící osobní údaje. Tyto problémy jsou však do značné míry překonatelné a tento postup je dobrou možností, jak zvýšit ochranu soukromí subjektů údajů.¹⁹⁰ Jsem ale přesvědčen, že by bylo velkou chybou, učinit z anonymizace univerzální nástroj, který by jen nahradil v současné době univerzálně používaný souhlas.

Solve dále navrhuje opustit princip technologické neutrality právní úpravy souhlasu.¹⁹¹ Cílem je soustředit se více na obsah konkrétního zpracování osobních údajů a přestat používat souhlas univerzálně. Již současná evropská a česká úprava to do určité míry splňuje, je však možné v této linii pokračovat. Vznik pravidel, která by podrobněji rozpracovala

¹⁸⁷ USTARAN, Eduardo. Yes, Consent Is Dead. Further, Continuing To Give It A Central Role Is Dangerous. *Privacy Perspectives* [online]. IAPP, publikováno 18. prosince 2013. [cit. 10. 6. 2014]. Dostupné z: https://www.privacyassociation.org/privacy_perspectives/post/yes_consent_is_dead_further_continuing_to_give_it_a_central_role_is_dangerous.

¹⁸⁸ WOLF, Christopher; POLONETSKY, Jules. An Updated Privacy Paradigm for the “Internet of Things”. *Future of Privacy Forum* [online]. *Future of privacy*, 2013, s. 7 – 8. [cit. 10. 6. 2014]. Dostupné z: <http://www.futureofprivacy.org/wp-content/uploads/Wolf-and-Polonetsky-An-Updated-Privacy-Paradigm-for-the-%E2%80%9CInternet-of-Things%E2%80%9D-11-19-2013.pdf>.

¹⁸⁹ Srovnej OHM, Paul. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*. [online]. 2010, vol. 57, no. 6, pp. 1701 – 1777. [cit. 10. 6. 2014] Dostupné z: <http://www.uclalawreview.org/?p=1353>.

¹⁹⁰ Řadu zajímavých řešení nabízí Paul Ohm ve výše uvedené studii.

¹⁹¹ SOLOVE, Daniel J. Privacy Self-Management and the Consent Dilemmas. *Harvard Law Review* [online]. 2013, vol. 126, no. 7, s. 1903. [cit. 10. 6. 2014] Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018.

různé účely a způsoby zpracování osobních údajů a jejich dopady na subjekty údajů by vedl k vytvoření skupiny zpracování, pro jejichž nízký zásah do soukromí subjektů údajů nebude předchodit souhlas vůbec třeba.¹⁹² Tím pádem by byl požadavek souhlasu pro subjekt údajů opět výraznější výstrahou, že zpracování údajů, se kterým se právě chystá souhlasit, může nějak významně zasáhnout do jeho soukromí.

Vyvážení práva jedince na soukromí a potřeby společnosti získávat podstatné informace na základě analýzy osobních údajů představuje pro právo ochrany soukromí a osobních údajů velikou výzvu do budoucna. Navržené způsoby řešení nejsou jedinými možnými a ideální podoba právní úpravy ochrany osobních údajů bude tvořena kombinací různých dílčích řešení. Jisté je, že současný stav má k dobrému řešení daleko a čím dříve budou potřebné změny provedeny, tím lépe.

5. COOKIES A PODOBNÉ TECHNOLOGIE

V této kapitole se budeme věnovat specifické oblasti ochrany osobních údajů, kterou jsou cookies a podobné technologie, které spadají pod úpravu článku 5 odst. 3 Směrnice o soukromí a elektronických komunikacích.¹⁹³ Jedná se o problematiku téma a stejně problematickou právní úpravu, o čemž svědčí i množství oficiálních materiálů, které jí byly věnovány.¹⁹⁴ Stanovisko WP29 cookie popisuje jako:

„Krátký alfanumerický text, který poskytovatel sítě ukládá do koncového zařízení subjektu údajů a později jej odtud znovu získává. Tento alfanumerický text lze využívat pro celou řadu účelů, jako je zapamatování preferencí, ukládání informací o relaci nebo stanovení totožnosti subjektu údajů prostřednictvím jedinečného označení.“¹⁹⁵

¹⁹² Po tom, aby nebyl souhlas používán jako jednoduchá cesta procesního povolení, v případech, kdy je možné danou činnost povolit na hmotně právním základě, ostatně volají i Beyleveld s Brownswordem, jak je vidno z citace v podkapitole 3.2 této práce.

¹⁹³ Směrnice Evropského parlamentu a Rady č. 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích). In: CODEXIS [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

¹⁹⁴ Čtyři stanoviska a jedno vyjádření WP29, stanovisko českého Úřadu pro ochranu osobních údajů by mělo vyjít v relativně krátké době. Jak bude probráno dále, do právní úpravy článku 5 odst. 3 směrnice 2002/58/ES však spadá celá řada dalších moderních technologií z oblasti komunikací a IT, například mobilní aplikace.

V první podkapitole se seznámíme detailněji s právní úpravou tohoto fenoménu a jejím vývojem jak v právu Evropské unie, tak v českém právním řádu. Druhá podkapitola se věnuje obecnější otázce vztahu právní úpravy cookies a ochrany osobních údajů. Třetí část je zaměřena na možné řešení diskutovaného problému.

5.1 PRÁVNÍ ÚPRAVA

Základní právní úpravu v této oblasti, jak již vyplývá z úvodu kapitoly, představuje článek 5 odst. 3 Směrnice o soukromí a elektronických komunikacích. Ten v původní verzi zněl takto:

„Členské státy zajistí, aby užívání sítí elektronických komunikací k uchování informací nebo získávání přístupu k informacím uchovávaným v koncovém zařízení účastníka nebo uživatele bylo povoleno pouze za podmínky, že dotčený účastník či uživatel byl jasně a úplně informován v souladu se směrnicí 95/46/ES, mimo jiné o účelech zpracování, a že je mu správcem údajů nabídnuto právo odmítnout takové zpracování. To nebrání technickému ukládání nebo takovému přístupu, jehož jediným účelem je provedení nebo usnadnění přenosu sdělení prostřednictvím sítí elektronických komunikací nebo, je-li to nezbytně nutné pro poskytování služeb informační společnosti, které si účastník nebo uživatel výslovně vyžádal.“¹⁹⁶

Věcná působnost uvedeného článku spadá na veškeré informace, které provozovatel služby ukládá do koncového zařízení uživatele, nebo informace již v koncovém zařízení uložené, ke kterým má provozovatel služby přístup a může je číst.¹⁹⁷ Směrnice mlčí v otázce, o jaké informace se přesně má jednat. Vzhledem k tomu je věcná působnost sama o sobě

¹⁹⁵ Pracovní skupina pro ochranu údajů zřízená podle článku 29. Stanovisko č. 2/2010 k internetové reklamě zaměřené na chování. WP 171. *Evropská komise* [online]. [cit. 10. 6. 2014]. Dostupné z: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_cs.pdf. S. 6.

¹⁹⁶ Směrnice Evropského parlamentu a Rady č. 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích). In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

¹⁹⁷ Srovnej Pracovní skupina pro ochranu údajů zřízená podle článku 29. Stanovisko č. 2/2010 k internetové reklamě zaměřené na chování. WP 171. *Evropská komise* [online]. [cit. 10. 6. 2014]. Dostupné z: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_cs.pdf.

překvapivě široká. Krom cookies tak ustanovení bez pochyby dopadá i na mobilní aplikace,¹⁹⁸ internetové obchody typu iTunes a Steam, nebo používání zaručeného elektronického podpisu. Extenzivním výkladem by bylo možné rozšiřovat působnost tohoto ustanovení až do pozice, kdy pod něj bude spadat veškerá síťová komunikace, protože pro její funkčnost vždy budou nějaká data v koncovém zařízení zpřístupňována a nějaká do něj zpět ukládána.¹⁹⁹

Analyzovaný článek zakládá povinnost informovat koncového uživatele v souladu se Směrnicí o ochraně osobních údajů.²⁰⁰ Poskytovatel služby tedy musí splnit stejnou informační povinnost, jako správce osobních údajů a to i v případě, že informace, se kterými služba pracuje, nejsou osobní údaje. Je nezbytné si uvědomit, že pro použití ustanovení čl. 5 odst. 3 není nutné, aby informace byly osobními údaji dle Směrnice o ochraně osobních údajů. Stačí, když splní požadavky uvedené v minulém odstavci. Smyslem, který zákonodárce sledoval je, že informace obsažené v koncových zařízeních tvoří součást soukromí uživatelů, které je třeba chránit.²⁰¹ Z toho vyplývá, že i v případě, že k žádnému zpracování osobních údajů nedochází, provozovatel služby má povinnost na tento fakt uživatele upozornit. Na textu ustanovení a příslušných recitálů Směrnice je jasně viditelné, že tento text byl psán v určité době za účelem limitace rizika, které představuje například spyware.²⁰² Působí na mě dojmem, že si zákonodárce plně neuvědomil šíři materie, kterou tímto ustanovením upravil.

¹⁹⁸ Viz Pracovní skupina pro ochranu údajů zřízená podle článku 29. Stanovisko č. 2/2013 k aplikacím v inteligentních zařízeních. WP 202. *Evropská komise* [online]. [cit. 10. 6. 2014]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_cs.pdf.

¹⁹⁹ WP29 v doposud nepublikovaném návrhu stanoviska k fingerprinting (identifikace počítače na základě meta informací, které odesílá) takto širokou interpretaci s odkazem na recitál 66 směrnice 2009/136/ES odmítá. Argument, jak k tomu na základě tohoto recitálu dospěla, je sice poněkud záhadný (odkazuje se na úmysl zákonodárce, když recitál 66 hovoří o „neodůvodněném narušení soukromé sféry“, nebylo úmyslem postihnout veškerou komunikaci), závěr je však přesto vítaný.

²⁰⁰ Směrnice o ochraně soukromí a elektronických komunikacích je, jak již bylo uvedeno v první kapitole práce, v oblasti elektronických komunikací lex specialis vůči Směrnicí o ochraně osobních údajů.

²⁰¹ Srovnej Pracovní skupina pro ochranu údajů zřízená podle článku 29. Stanovisko č. 2/2010 k internetové reklamě zaměřené na chování. WP 171. *Evropská komise* [online]. [cit. 10. 6. 2014]. Dostupné z: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_cs.pdf. s. 9.

²⁰² Viz recitál 24 Směrnice o soukromí a elektronických komunikacích.

V původním znění Směrnice o soukromí a elektronických komunikacích bylo navazující povinností provozovatele služby poskytnout uživateli možnost odmítnout takové zpracování.²⁰³ Zákodárce zde nastavil režim opt-out, který předpokládá souhlas s použitím technologie, ledaže se uživatel vyjádří opačně. Vzhledem k působení sklonu uživatelů držet status quo a neinvestovat transakční náklady v podobě času na změnu základního nastavení, tímto způsobem zákonodárce umožnil snadnější provoz zmíněných technologií a zdánlivě tak rameno pomyslné váhy vychýlil směrem k provozovateli služby.²⁰⁴

Čl. 5 odst. 3 rovněž zakládal výjimku z výše uvedených povinností informovat a dát možnost zpracování odmítnout. Poskytovatel služby nebyl touto povinností vázán, pokud jediným účelem činnosti spadající do věcné působnosti tohoto článku bylo technické ukládání – přístup, jehož jediným účelem bylo provedení nebo usnadnění přenosu sdělení, nebo bylo-li to nezbytně nutné pro poskytnutí služeb, které uživatel výslovně vyžádal. Můžeme si všimnout, že tato třetí možnost je variantou legitimizace zpracování osobních údajů na základě nezbytnosti zpracování pro plnění smlouvy, které je subjekt údajů stranou.

V českém právním řádu byl tento článek implementován do § 89 odst. 3 zákona o elektronických komunikacích.²⁰⁵ Převedení do českého práva bylo provedeno takřka doslovně, proto i zde platí, co bylo řečeno k evropské úpravě. Jedinou změnou je, že se český zákonodárce nespokojil s odkazem na informační povinnost dle Zákona o ochraně osobních údajů a výslovně stanovil povinnost informovat o rozsahu a účelu zpracování.

Evropská Směrnice 2009/136/ES přinesla novelu rozebíraného článku 5 odst. 3. Nové znění je následující:

„Členské státy zajistí, aby uchovávání informací nebo získávání přístupu k již uchovávaným informacím bylo v koncovém zařízení účastníka nebo uživatele povoleno pouze pod podmínkou, že dotčený

²⁰³ Teď již čistě teoretickou otázkou zůstává, jak se tato povinnost aplikovala (měla aplikovat) na situace, kdy k žádnému zpracování nedocházelo.

²⁰⁴ Srovnej DREIER, Thomas. „Opt in“ and „opt out“ mechanisms in the internet era – towards a common theory. *Computer law & Security review*. 2010, vol. 26, no. 2, pp. 144-150. ISSN 0267-3649.

²⁰⁵ Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích). In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

*účastník či uživatel poskytl svůj souhlas poté, co mu byly poskytnuty jasné a úplné informace v souladu se směrnicí 95/46/ES, mimo jiné o účelu zpracování. To nebrání technickému ukládání nebo takovému přístupu, jehož jediným účelem je provedení přenosu sdělení prostřednictvím sítě elektronických komunikací, nebo je-li to nezbytně nutné k tomu, aby mohl poskytovatel služeb informační společnosti poskytovat služby, které si účastník nebo uživatel výslovně vyžádal.*²⁰⁶

Věcná působnost a informační povinnost provozovatele služby zůstaly beze změny. Výkladový recitál 66 této směrnice uvádí, že je „nanejvýš důležité, aby měli uživatelé, kteří zahajují jakoukoli činnost, která by mohla vést k takovému uchovávání údajů nebo přístupu k nim [dle článku 5 odst. 3, JM.], k dispozici jasné a srozumitelné informace.“ Došlo však ke zcela zásadnímu otočení v oblasti toho, kdy je možné dotčené technologie používat. Legislativce opustil režim opt-out a přistoupil na režim opt-in, který vyžaduje předchozí informovaný souhlas uživatele.²⁰⁷ Tímto krokem nastavil základní pozici tak, že není možné dané technologie používat a zdánlivě tím vychýlil vztah mezi poskytovatelem a uživatelem služby ve prospěch uživatele. Jedná se o evidentní projev přehnané důvěry ve schopnosti institutu informovaného souhlasu, o které jsem hovořil v předchozí kapitole. Nutnost souhlasit před každým prvním použitím dotčené technologie dále přispívá k rutinizaci udělování, a tím i devalvací významu informovaného souhlasu v oblasti ochrany soukromí jako celku. Krok, který se na první pohled může zdát jako posílení pozice uživatele, tak ve skutečnosti působí spíše proti němu.

Druhou změnou, kterou novelizace přinesla, je zúžení výjimky, umožňující použití dotčené technologie i bez souhlasu. Toho bylo docíleno vypuštěním slova „usnadňující“. Výjimka se tedy již vztahuje jen na

²⁰⁶ Čl. 2 odst. 5 Směrnice Evropského parlamentu a Rady č. 2009/136/ES ze dne 25. listopadu 2009, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele. In: CODEXIS [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

²⁰⁷ Souhlas dle čl. 2 písm. f) Směrnice o soukromí a elektronických komunikacích odpovídá souhlasu subjektu údajů dle Směrnice o ochraně osobních údajů.

technologie, bez kterých se přenos nemůže uskutečnit a na ty, které jsou nezbytně nutné k poskytnutí služby výslovně vyžádané uživatelem.²⁰⁸

Implementace novelizující směrnice 2009/136/ES do Zákona o elektronických komunikacích byla provedena zákonem č. 468/2011 Sb.,²⁰⁹ který novelizoval § 89 odst. 3 Zákona o elektronických komunikacích. Došlo však k zajímavé situaci, nová směrnice byla implementována jen částečně. Legislativní úprava upravila pravidla pro výjimky, aby odpovídala evropskému předpisu,²¹⁰ zbytek ustanovení však zůstal beze změny, tedy ve znění původní směrnice 2002/58/ES. Zůstal tak zachován režim opt-out. Matoucí však zůstává text důvodové zprávy k zákonu 468/2011 Sb. V té stojí následující:

„Ukládání údajů, nebo získání přístupu k údajům uloženým v koncových zařízeních účastníků nebo uživatelů, je možné pouze se souhlasem těchto účastníků nebo uživatelů. Tato povinnost neplatí pro technické ukládání nebo přístup výhradně pro potřeby (již nikoliv pro usnadnění přenosu) přenosu zprávy prostřednictvím sítě elektronických komunikací nebo je-li to nezbytné pro potřeby poskytování služby informační společnosti, která je výslovně vyžádána účastníkem nebo uživatelem.“²¹¹

Věta „je možné pouze se souhlasem“ naznačuje přechod na opt-in režim. To však nemá oporu v zákoně. Výsledkem tak je naprosté zmatení adresátů této právní normy, a krom toho i nesplnění povinnosti České republiky implementovat evropskou Směrnici.²¹²

²⁰⁸ O jaké technologii cookies se jedná, velmi podrobně referuje stanovisko WP29. Viz Pracovní skupina pro ochranu údajů zřízená podle článku 29. Stanovisko č. 4/2012 k výjimce z požadavku na souhlas s cookies. WP 194. *Evropská komise* [online]. [cit. 10. 6. 2014]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_cs.pdf.

²⁰⁹ Čl. 1 odst. 211 zákona č. 468/2011 Sb. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

²¹⁰ To znamená, že vypustil slova „provedení nebo usnadnění“.

²¹¹ 347/0, Vládní návrh na vydání zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a některé další zákony. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

²¹² Je však třeba dodat, že v tom zdaleka není sama. Viz Cookie ‘Consent’ Rule: EEA Implementation Table. *International association of privacy professionals* [online]. Field Fisher Waterhouse, publikováno 4. 2. 2013. [cit. 10. 6. 2014]. Dostupné z: https://www.privacyassociation.org/resource_center/cookie_consent_rule_eea_implementation_table.

Na tomto místě by mohl být výklad o cookies a podobných technologiích ukončen, jelikož, jak vyplývá z textu zákona, není v České republice třeba předchozího souhlasu k tomu, aby mohly být cookies v koncovém zařízení uživatele použity. Domnívám se ale, že zůstaly nevyřešeny některé zajímavé otázky, které však předpokládají, že je v působení režim opt-in. Pro potřeby této práce tak budu nadále vykládat daná ustanovení eurokonformně a budu předpokládat, že souhlasu je třeba.

5.2 JSOU COOKIES OSOBNÍMI ÚDAJI?

Předchozí podkapitola se věnovala právní úpravě cookies a podobných technologií. Cílem této podkapitoly je blíže analyzovat podstatu vztahu mezi prvním dílem páté hlavy Zákona o elektronických komunikacích²¹³ a Zákonem o ochraně osobních údajů. Budu postupovat od konkrétního příkladu k abstraktnější obecné rovině.

Petr Krčmář v článku na root.cz cituje Kateřinu Hruběšovou, ředitelku Sdružení pro internetovou reklamu, která tvrdí, že cookies nejsou osobním údajem.²¹⁴ Tato teze není pravdivá, jelikož cookies mohou být osobním údajem. Vzhledem k tomu, jak je široká zákonná definice osobních údajů, může se snadno stát, že cookies zaznamenávající pohyb uživatele po Internetu bude mít dostatek informací, aby bylo možné na jejich základě identifikovat subjekt údajů. Ostatně dle Krčmáře i sama Hruběšová přiznává, že se uživatel dříve či později při užití cookies identifikuje. Na co ovšem Hruběšová zapomíná je, že se ustanovení o souhlasu dle zákona o ochraně osobních údajů budou aplikovat, i za předpokladu, že by cookies a podobné technologie opravdu osobními údaji nebyly. Souhlas se sběrem a zpracováním osobních údajů a souhlas k využití technologie cookies²¹⁵ jsou dva odlišné právní instituty, byť se řídí stejnými pravidly pro udělení a platnost souhlasu. Jak tvrdí recitál 24,²¹⁶ koncové zařízení uživatele

²¹³ Ochrana osobních, provozních a lokalizačních údajů a důvěrnost komunikací.

²¹⁴ KRČMÁŘ, Petr. Cookies umírají, reklamní branže si ale najde náhradu. *Root.cz* [online]. Internet Info, s.r.o., publikováno 13. 2. 2014. [cit. 10. 6. 2014]. Dostupné z: <http://www.root.cz/clanky/cookies-umiraji-reklamni-branze-si-ale-najde-nahradu/>.

²¹⁵ Nadále budu v rámci zjednodušení hovořit jen o cookies, byť tam, jak bylo pojednáno, spadá celá řada dalších technologií.

²¹⁶ Směrnice Evropského parlamentu a Rady č. 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích). In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

a informace na něm uložené jsou součástí soukromí uživatele, funkce souhlasu s použitím cookies je tedy analogická se souhlasem se zpracováním osobních údajů. Tento souhlas je jednostranným právním jednáním, které umožňuje třetí osobě, jinak právem zapovězený, zásah do soukromí souhlasícího.

Rozeberme si nyní pro přehlednost dvě varianty aplikace ustanovení.

Varianta A) spočívá v použití cookies nebo podobných technologií, které jsou zároveň osobními údaji. V takovém případě se plně aplikuje jak § 89 odst. 3 Zákona o elektronických komunikacích,²¹⁷ tak Zákon o ochraně osobních údajů.²¹⁸ Provozovatel služby, který je zároveň správcem údajů, musí nejprve obdržet od uživatele (subjektu údajů) souhlas s použitím cookies, a to i tehdy, je-li pro zpracování osobních údajů per se aplikovatelný jiný legitimizační důvod. Souhlas s užitím technologie cookies musí splňovat všechny podmínky, jako souhlas se zpracováním osobních údajů, jak jsou pojednány ve druhé kapitole této práce.²¹⁹ Musí tedy být svobodný, určitý, vědomý a jednoznačný. Rovněž nemá předepsanou formu, jelikož ani Zákon o elektronických komunikacích ani evropská Směrnice o soukromí a elektronických komunikacích z pozice *lex specialis* tuto otázku konkrétně nespecifikují. Subjekt údajů může tedy udělit platný souhlas s užitím cookies i konkludentně.

Protože ve variantě A) se opravdu jedná o zpracování osobních údajů, má provozovatel dále povinnost splnit všechny závazky správce údajů dle Zákona o ochraně osobních údajů. Musí tak splnit informační povinnost, na kterou výslovně odkazuje § 89 odst. 3²²⁰ a upozornit uživatele na účel a způsob zpracování. Dále musí splnit také například registrační povinnost, povinnost určení účelu a prostředků zpracování, povinnost prokázání udělení souhlasu se zpracováním po celou dobu zpracování a další ze Zákona o ochraně osobních údajů vyplývající.

²¹⁷ Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích). In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

²¹⁸ S výjimkou náležitostí upravených v Zákoně o elektronických komunikacích jinak. Viz § 87 odst. 1 Zákona o elektronických komunikacích.

²¹⁹ Viz § 87 odst. 2 Zákona o elektronických komunikacích a Čl. 2 písm. f) evropské Směrnice o soukromí a elektronických komunikacích.

²²⁰ Zákon o elektronických komunikacích.

Správce také musí mít zákonný důvod pro zpracování. V případě, že je tímto důvodem souhlas dle § 5 odst. 2 Zákona o ochraně osobních údajů, můžeme za takový souhlas považovat již svolení k použití cookies. Pokud je však použit jiný legitimizační důvod než souhlas,²²¹ pro subjekt údajů dochází k nepřehledné situaci. Je totiž nejprve žádán o souhlas, následně je však postaven do pozice, kdy dochází ke zpracování jeho údajů bez možnosti jeho zásahu. Správce má jednoznačnou povinnost subjekt o podstatě této situace poučit.

Domnívám se, že v případě, kdy je zpracování cookies - osobních údajů založeno jiným právním důvodem než souhlasem, můžeme se poměrně úspěšně tázat, zda je udělení souhlasu s použitím cookies platné. Pokud je například toto zpracování odůvodněné plněním právní povinnosti správce údajů, subjekt není v pozici, kdy by stál před svobodnou volbou, zda souhlas udělí, nebo ne. Takové zpracování proběhnout musí a případný souhlas se zpracováním není platný, protože postrádá podmínku svobodnosti.²²² Zákon o ochraně osobních údajů takové situace umožňuje řešit alternativními legitimizačními důvody ke zpracování. Ty však nelze aplikovat pro případ souhlasu s použitím cookies. Právní úprava nedává možnost výběru a její nutný výklad hovoří jasně: „K použití této technologie je třeba předchozí souhlas, který odpovídá souhlasu dle Směrnice o ochraně osobních údajů. Tento souhlas tedy musí být svobodný, určitý, vědomý a jednoznačný.“ Jelikož je zpracování na základě zákonné povinnosti nezbytné, nemůže být souhlas s použitím cookies udělen svobodně, a proto není platný. Bez platného souhlasu však nemůže být technologie cookies použita a to i přes to, že je takové zpracování nezbytné. Nacházíme se tak v logické pasti, z níž není úniku.

Varianta B) spočívá v použití cookies nebo podobných technologií, které zároveň osobními údaji nejsou. V tomto případě se bude aplikovat toliko ustanovení § 89 odst. 3 Zákona o elektronické komunikaci a k použití technologie cookies bude mít provozovatel povinnost uživatele informovat o zpracování²²³ a získat od něj souhlas s použitím cookies, jenž naplní požadavky na souhlas dle Zákona o ochraně osobních údajů. Takový

²²¹ Jak bylo dovozeno v předchozí kapitole, pokud taková možnost existuje, měla by být upřednostněna.

²²² Viz kapitola 2 této práce.

²²³ Tedy že žádné neprobíhá.

souhlas tedy musí být svobodný, určitý, vědomý a jednoznačný, a může být udělen i konkludentně.²²⁴ Žádné další povinnosti na provozovatele však kladeny nejsou. Dle mého názoru není možné interpretačně rozšířit termín „zpracování“²²⁵ tak, aby zahrnoval pouhé použití cookies a Zákon o ochraně osobních údajů byl tak bez dalšího aplikovatelný.

Po uvedené detailní analýze vztahu souhlasu s použitím cookies a ochrany osobních údajů se domnívám, že probíraný institut, tak jak jej zavádí Čl. 5 odst. 3 Směrnice o soukromí a elektronických komunikacích je nesmírně problematický a poněkud zbytečný. Pokud jsou za pomoci cookies zpracovány osobní údaje, stačí k jejich ochraně obecný předpis k jejich ochraně určený. Pokud zpracovávány nejsou, a účelem daného ustanovení je pouze přímá ochrana soukromí uživatele, pak není třeba složitě odkazovat na jiný samostatný právní předpis, jelikož ve výsledku dochází k naprostému zmatení všech zúčastněných. Současný způsob ochrany, kdy je ustanovení předpisu o elektronických komunikacích masivně využíváno v diskurzu ochrany osobních údajů, je zcela nesystémový. Pokud už by zákonodárce chtěl použít princip souhlasu, jakkoli by jiný způsob byl dle mého názoru přiměřenější, výrazně vhodnějším způsobem by bylo zavedení autonomního institutu souhlasu se zásahem do koncového zařízení uživatele.

5.3 DALŠÍ VÝVOJ

Ze staré i nové úpravy čl. 5 odst. 3 Směrnice o soukromí a elektronických komunikacích je patrný jasný akcent na informování uživatele. To je, myslím, zcela v pořádku a na tomto principu by dle mého názoru měla právní úprava cookies a podobných technologií být postavena. Souhlasím s tím, že průnik do koncového zařízení uživatele je zásahem do jeho soukromého prostoru, jak tvrdí recitál 24 Směrnice o soukromí a elektronických komunikacích. Z toho důvodu je zajištění informovanosti uživatele i nadále klíčové, protože každý by měl mít možnost zjistit, za jakým účelem je software, umístěný v jeho zařízení, používán. Toto informování nemusí probíhat jen pomocí dlouhých složitých textů, ale je

²²⁴ Jelikož určitě nejsou zpracovávány žádné citlivé údaje, je jisté, že nebude třeba výslovného souhlasu.

²²⁵ Který má jasný význam pocházející ze Směrnice a Zákona na ochranu osobních údajů.

možné využít i dalších metod, o kterých jsem podrobně referoval na konci třetí kapitoly této práce. Nutné použití souhlasu je však dle mého názoru kontraproduktivní z mnoha již uvedených důvodů.²²⁶ Pokud už však existuje povinnost užívat institut souhlasu, mělo by být jeho udělení možné co nejjednodušším způsobem.

Jako vhodné řešení se tak jeví souhlas s použitím cookies daný pomocí nastavení webového prohlížeče, o kterém se přímo zmiňuje recitál 66 směrnice č. 2009/136/ES. Tímto způsobem může uživatel předem vyjádřit jasný souhlas či nesouhlas s použitím cookies. WP29 však ve svém stanovisku správně upozorňuje, že aby se dalo nastavení prohlížeče považovat za projev vůle, musí existovat jistota, že uživatel je o této možnosti obeznámen.²²⁷ Toho je nejlépe dosaženo tehdy, když nastavení prohlížeče provede uživatel sám. Pokud prohlížeč přijímá cookies v základním „továrním“ nastavení, je velmi problematické považovat to za souhlas uživatele s použitím cookies. Větším problémem tohoto jinak elegantního řešení je, že uživatel dává nastavením cookies souhlas s jejich použitím dopředu blanketově, bez znalosti účelů zpracování. Takový souhlas tedy není dostatečně vědomý a informovaný, a proto by mohl být neplatný. Třetím problémem je, že i pokud by bylo nastavení webového prohlížeče dostatečným souhlasem pro použití technologie cookies, nestačilo by už jako souhlas se zpracováním osobních údajů tehdy, bude-li se jednat o osobní údaje a souhlas ke zpracování bude potřeba. Subjekt údajů by tak stejně musel ještě jednou souhlas se zpracováním udělit.

Dle mého názoru by dobrou cestou bylo zachování původního znění Směrnice o soukromí a elektronických komunikacích a nechat tak užití cookies v režimu opt-out. Zachování informační povinnosti a výslovně uvedená možnost od zpracování údajů odstoupit, jakkoli je sama o sobě implicitně daná, představuje dle mého názoru dostatečnou ochranu subjektu údajů bez zbytečného zatěžování obou zúčastněných stran. Toto řešení je navíc zcela kompatibilní se současnou úpravou ochrany osobních

²²⁶ Např. zvýšená zátěž na uživatele, snížení rychlosti datového toku, devalvace hodnoty souhlasu a jeho automatizace atd.

²²⁷ Pracovní skupina pro ochranu údajů zřízená podle článku 29. Stanovisko č. 2/2010 k internetové reklamě zaměřené na chování. WP 171. *Evropská komise* [online]. [cit. 10. 6. 2014]. Dostupné z: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_cs.pdf. S. 16 – 15.

údajů, která konkludentní souhlas umožňuje. Silnou ochranu osobních údajů tvoří již legislativa zaměřující se na tuto oblast a není třeba ji takto externě uměle zesilovat.

Tlak, který je ze strany legislativy na poskytovatele služeb ohledně získání souhlasu s použitím cookies vyvíjen, vede ke snižování použití této technologie, což nemusí být nutně prospěšný efekt. Jedním z účelů, k jakým jsou cookies používány, je získávání informací o uživateli pro potřeby behaviorální reklamy. Je naivní domnívat se, že přísnou regulací cookies sledování uživatelů ustane. Pokud k tomu nebudou využívány cookies, které jsou uživatelem poměrně dobře detekovatelné a případně snadno odstranitelné, budou k tomu použity jiné technologie, nad kterými uživatel nebude mít takovou míru kontroly.²²⁸ To by vedlo ke zhoršení pozice uživatele.

Myslím, že závěrem této kapitoly je vhodné připomenout, že ač po celou dobu zmiňuji pouze cookies, § 89 odst. 3 Zákona o elektronických komunikacích dopadá na celou řadu dalších technologií. To, co bylo uvedeno v průběhu této kapitoly, se tak týká například také aplikací do chytrých mobilních zařízení, on-line obchodů typu iTunes nebo Steam, služeb jako Dropbox a celé řady dalších. Vždy, když služba ukládá do koncového zařízení nějaká data, nebo má přístup k datům v koncovém zařízení, § 89 odst. 3 vyžaduje, aby uživatel s tímto procesem souhlasil, přičemž souhlas musí splňovat podmínky kladené na souhlas se zpracováním Zákonem o ochraně osobních údajů. Pokud přímým účelem dané služby není zpracování osobních údajů dle Zákona o ochraně osobních údajů, a takových případů je, myslím, většina, bude taková služba příkladem varianty B), jak jsem ji uvedl v předchozí podkapitole. Krom získání souhlasu s použitím technologie zasahující do koncového zařízení uživatele tak nebude mít poskytovatel služby žádné další povinnosti vyplývající ze Zákona o ochraně osobních údajů.

²²⁸ Srovnej KRČMÁŘ, Petr. Cookies umírají, reklamní branže si ale najde náhradu. Root.cz [online]. Internet Info, s.r.o., publikováno 13. 2. 2014. [cit. 10. 6. 2014]. Dostupné z: <http://www.root.cz/clanky/cookies-umiraji-reklamni-branze-si-ale-najde-nahradu/>.

6. ZÁVĚR

Tato studie představila souhlas se zpracováním osobních údajů jako jednostranné právní jednání, které je prostředkem ospravedlnění zásahu jedné osoby (správce údajů) do právem chráněné oblasti soukromí osoby druhé (subjektu údajů). Subjekt údajů může dát svým souhlasem najevo, že mu případný zásah ze strany správce údajů nevádí, díky čemuž se zpracování údajů stane legitimním. Bylo mnohokrát zdůrazněno, že je třeba, aby správce údajů souhlas po subjektu požadoval ve správném kontextu, tedy pouze tehdy, nemá-li k dispozici pro zpracování osobních údajů jiný zákonný důvod. Typickým příkladem, kdy se důvody pro zpracování často zaměňují a dochází tak k němu na základě špatného důvodu, jsou vícestanné smlouvy, do nichž je souhlas se zpracováním osobních údajů inkorporován.

S nástupem informačních a komunikačních technologií došlo k masivnímu nárůstu zpracování osobních údajů, a to jak po kvalitativní, tak kvantitativní stránce. Studie poukázala na nedostatky v současné právní úpravě a jejich praktický dopad na adresáty právních norem. Víra v univerzální použitelnost institutu souhlasu, která dle mého názoru až hraničí s fetišismem, vede k používání tohoto institutu i v případech, pro které se nehodí. To je jeden z faktorů, který přispívá k současnému stavu, kdy je subjekt údajů přehlčen různými požadavky na souhlas. Tento stav je velmi nežádoucí, neboť spouští škodlivou spirálu, která vede ke zhoršení právní pozice subjektu údajů.

Nejjednodušším řešením, jak tento stav zlepšit, je používat souhlas jen v takových případech, pro které je vhodný. To klade na správce údajů nároky, aby pečlivě analyzoval plánované zpracování osobních údajů a o souhlas žádal subjekt pouze tehdy, nemůže-li použít pro plánovaný účel jiný zákonný legitimizační důvod. Je-li jiná možnost, jak údaje zpracovávat, než souhlas, měla by být preferovaná. Dalším způsobem, jak zlepšit právní postavení subjektu, je zajistit větší srozumitelnost informačních dokumentů. Například použití grafických symbolů podobných Creative Commons, nebo barevných označení, které by na první pohled prozradily rizikovost zpracování osobních údajů, by mohlo k dosažení tohoto cíle pomoci.

Typickým příkladem chybného použití institutu souhlasu se zpracováním osobních údajů je jeho zahrnutí do právního režimu ochrany soukromí při použití technologie cookies a jí podobných. Zákodárce v tomto případě ve snaze o zvýšení bezpečnosti všech uživatelů těchto technologií vytvořil další vrstvu ochrany v podobě nového institutu souhlasu s použitím cookies a podobných technologií. Pro platnost tohoto souhlasu musí být splněny všechny náležitosti jako v případě souhlasu se zpracováním osobních údajů. Taková konstrukce je však vpravdě problematická. Nejen, že jsou na provozovatele služeb využívajících cookies kladeny vysoké požadavky pro splnění zákonné povinnosti, zároveň v určitých případech může dojít k situaci, kdy uživatel (subjekt údajů) nemůže udělit takový souhlas, který by dle zákona platný. Jako vhodné řešení pro cookies a podobné technologie jsem navrhl návrat k opt-out systému se silným principem informování uživatele a možností snadného odmítnutí použití cookies.

Jedním z cílů této studie bylo také pomoci otevřít v českém diskurzu prostor pro diskuzi o problémech a možných řešeních, které jsou v jejím textu zpracovány. Zatímco ve světové literatuře a odborných diskuzích je na institut souhlasu se zpracováním osobních údajů nahlíženo kriticky, a mnoho autorů upozorňuje na jeho nedostatky, v českém právním prostředí je až příliš často chápán jako takřka univerzální lék. Je glorifikován jako ideální způsob, jak může jedinec určit, kdo bude jeho osobní údaje zpracovávat a tak zajistit jejich ochranu. V mnoha případech tomu tak ale není. Pokud by však byl současný postoj odborné veřejnosti zachován, je jen malá naděje na zlepšení stávající situace. Nezbyvá mi, než doufat, že se ledy pohnou a dojde k otevření odborné diskuze, díky které se přiblíží nezbytná modernizace systému ochrany osobních údajů tak, aby odpovídal požadavkům moderní informační společnosti.

7. LITERATURA A DALŠÍ POUŽITÉ ZDROJE

7.1 MONOGRAFIE, PUBLIKACE, SBORNÍKY, ODBORNÉ ČLÁNKY

[1] BEYLEVELD, Deryck; BROWNSWORD, Roger. *Consent in the Law*. Oxford and Portland: Hart Publishing, 2007, 388 s. ISBN 978-1-84113-679-4.

[2] BEZOUŠKA, Petr; PIECHOWICZOVÁ, Lucie. *Nový občanský zákoník: Nejdůležitější změny*. Olomouc: Nakladatelství ANAG, 2013, 369 s. ISBN 978-80-7263-819-2.

- [3] DVORÁK, Jan; ŠVESTKA, Jiří; ZUKLÍNOVÁ, Michaela et al. *Občanské právo hmotné. Svazek I. Díl první: Obecná část*. Praha: Wolters Kluwer ČR, 2012, 432 s. ISBN 978-80-7478-326-5.
- [4] DREIER, Thomas. „Opt in“ and „opt out“ mechanisms in the internet era – towards a common theory. *Computer law & Security review*. 2010, vol. 26, no. 2, pp. 144-150. ISSN 0267-3649.
- [5] HOHFELD, Wesley, Newcomb. Fundamental Legal Conceptions. In: COOK, Walter, Wheeler. *Fundamental legal conceptions as applied in judicial reasoning and other legal essays*. New Haven: Yale University Press, 1923, s. 23-144.
- [6] KUČEROVÁ, Alena et al. *Zákon o ochraně osobních údajů, Komentář*. 1. Vyd. Praha: C. H. Beck, 2012, 536 s. ISBN 978-80-7179-226-0.
- [7] MATOUŠOVÁ, Miroslava; HEJLÍK, Ladislav. *Osobní údaje a jejich ochrana*. 2. Vyd. Praha: ASPI, Wolters Kluwer, 2002, 468 s. ISBN 978-80-7357-322-5.
- [8] MÉTAYER, Daniel Le; MONTELEONE, Shara. Automated consent through privacy agents: Legal requirements and technical architecture. *Computer law & Security review*. 2009, vol. 25, no. 2, pp. 136-144. ISSN 0267-3649.
- [9] NONNEMANN, František. Ochrana spotřebitele a ochrana osobních údajů. *Právní rozhledy*. 2010, roč. 18, č. 22, s. 807-810. ISSN 1210-6410.
- [10] NONNEMANN, František. Náležitosti souhlasu se zpracováním osobních údajů. *Právní rozhledy*. 2011, roč. 19, č. 14, s. 520-522. ISSN 1210-6410.
- [11] NONNEMANN, František. Odvolání souhlasu se zpracováním osobních údajů. *Právní rozhledy*. 2011, roč. 19, č. 24, s. 871-877. ISSN 1210-6410.
- [12] NONNEMANN, František. Právní úprava ochrany osobnosti v novém občanském zákoníku a její vztah k ochraně osobních údajů. *Právní rozhledy*. 2012, roč. 20, č. 13-14, s. 505-509. ISSN 1210-6410.
- [13] SMEKAL, Hubert. *Lidská práva*. 1. vyd. Brno: Masarykova univerzita, 2013, 195 s. ISBN 978-80-210-6388-4.
- [14] ŠKOP, Martin; MACHÁČ, Petr. *Základy právní nauky*. Praha: Wolters Kluwer ČR, 2011, 196 s. ISBN 978-80-7357-709-4.
- [15] TELEC, Ivo. Svolení, nebo zákonné licence v právu osobnostním. *Právní rozhledy*. 2007, roč. 15, č. 24, s. 879-883. ISSN 1210-6410.
- [16] TELEC, Ivo. Souhlas, nebo licenční závazek? *Právní rozhledy*. 2013, roč. 21, č. 13-14, s. 457-462. ISSN 1210-6410.
- [17] WAGNEROVÁ, Eliška et al. *Listina základních práv a svobod. Komentář*. Praha: Wolters Kluwer ČR, a.s., 2012, 931 s. ISBN 978-80-7357-750-6.

7.2 DOKUMENTY A PRÁVNÍ PŘEDPISY

- [18] 2007/C 306/01, Lisabonská smlouva pozměňující Smlouvu o Evropské unii a Smlouvu o založení Evropského společenství. In: CODEXIS [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].
- [19] 2012/C 326/02, Listina základních práv Evropské unie. In: CODEXIS [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

- [20] Nařízení Evropského parlamentu a Rady č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].
- [21] Směrnice Evropského parlamentu a Rady č. 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].
- [22] Směrnice Evropského parlamentu a Rady č. 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích). In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].
- [23] Směrnice Evropského parlamentu a Rady č. 2009/136/ES ze dne 25. listopadu 2009, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].
- [24] Usnesení 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. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].
- [25] Zákon č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].
- [26] Zákon č. 256/1992 Sb., o ochraně údajů v informačních systémech. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].
- [27] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].
- [28] Zákon č. 123/2000 Sb., o zdravotnických prostředcích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].
- [29] Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti). In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].
- [30] Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích). In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].
- [31] Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].
- [32] Zákon č. 468/2011 Sb. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].
- [33] Zákon č. 89/2012 Sb., občanský zákoník. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

[34] Sdělení federálního ministerstva zahraničních věcí č. 209/1992 Sb., o sjednání Úmluvy o ochraně lidských práv a základních svobod ve znění protokolů č. 3, 5 a 8. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

[35] Pracovní skupina pro ochranu údajů zřízená podle článku 29. Stanovisko č. 2/2010 k internetové reklamě zaměřené na chování. WP 171. *Evropská komise* [online]. [cit. 10. 6. 2014]. Dostupné z: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_cs.pdf.

[36] Pracovní skupina pro ochranu údajů zřízená podle článku 29. Stanovisko č. 15/2011 k definici souhlasu. WP 187. *Evropská komise* [online]. [cit. 10. 6. 2014]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_cs.pdf.

[37] Pracovní skupina pro ochranu údajů zřízená podle článku 29. Stanovisko č. 4/2012 k výjimce z požadavku na souhlas s cookies. WP 194. *Evropská komise* [online]. [cit. 10. 6. 2014]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_cs.pdf.

[38] Pracovní skupina pro ochranu údajů zřízená podle článku 29. Stanovisko č. 2/2013 k aplikacím v inteligentních zařízeních. WP 202. *Evropská komise* [online]. [cit. 10. 6. 2014]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_cs.pdf.

[39] Stanovisko Úřadu pro ochranu osobních údajů č. 2/2008, Souhlas se zpracováním osobních údajů. *Úřad pro ochranu osobních údajů* [online]. [cit. 10. 6. 2014]. Dostupné z: http://www.uouu.cz/files/stanovisko_2008_2.pdf.

[40] Stanovisko Úřadu pro ochranu osobních údajů č. 2/2011, Zpracování osobních údajů na základě souhlasu ve smlouvě nebo Všeobecných obchodních podmínkách a s tím související problémy. *Úřad pro ochranu osobních údajů* [online]. [cit. 10. 6. 2014]. Dostupné z: http://www.uouu.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=9185.

[41] Stanovisko Úřadu pro ochranu osobních údajů č. 5/2012, Poskytnutí informací a získání souhlasu subjektu údajů v elektronické komunikaci. *Úřad pro ochranu osobních údajů* [online]. [cit. 10. 6. 2014]. Dostupné z: http://www.uouu.cz/files/stanovisko_2012_5.pdf.

[42] Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data, COM (90), 314 final, SYN 287 and 288, Brussels, 13 September 1990. In: *Archive of European Integration* [online]. University of Pittsburgh [cit. 10. 6. 2014]. Dostupné z: <http://aei.pitt.edu/3768/1/3768.pdf>.

[43] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data, COM(1999) 337 final, s. 39. In: *EUR-Lex* [právní informační systém]. Úřad pro publikace Evropské unie [cit. 10. 6. 2014]. Dostupné z: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:1999:0337:FIN:EN:PDF>.

[44] Návrh Nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů), COM(2012) 11 final, 2012/0011. In: *EUR-Lex* [právní informační systém]. Úřad pro publikace Evropské unie [cit. 10. 6. 2014]. Dostupné z: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_cs.pdf.

[45] Draft report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM (2012)0011–C7-0025/2012-2012/0011(COD)). *Evropský parlament* [online]. Europarl.europa.eu [cit. 10. 6. 2014]. Dostupné z: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf.

[46] 347/0, Vládní návrh na vydání zákona, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a některé další zákony. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

[47] Rozhodnutí Úřadu pro ochranu osobních údajů čj. SPR-5685/09. Náležitosti souhlasu se zpracováním osobních údajů. *Úřad pro ochranu osobních údajů* [online]. Úřad pro ochranu osobních údajů [cit. 10. 6. 2014]. Dostupné z: <http://www.uouu.cz/nalezitosti-souhlasu-se-zpracovanim-osobnich-udaju/d-1768>.

7.3 SOUDNÍ ROZHODNUTÍ

[48] Rozsudek Nejvyššího správního soudu ze dne 23. srpna 2013, sp. zn. 5 As 158/2012 – 49. In: *CODEXIS* [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].

[49] Rozsudek Městského soudu v Praze ze dne 23. května 2013, sp. zn. 8Ca 95/2009. *Úřad pro ochranu osobních údajů* [online]. Úřad pro ochranu osobních údajů [cit. 10. 6. 2014]. Dostupné z: http://www.uouu.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=6558.

7.4 ELEKTRONICKÉ PRAMENY

[50] ACQUISTI, Alessandro; GROSSKLAGS, Jens. Privacy and Rationality in Individual Decision Making. *IEEE Security and Privacy*. 2005, vol. 3, no. 1, pp- 26 – 33. ISSN 1540-7993. In: Carnegie Mellon University [online]. [cit. 10. 6. 2014]. Dostupné z: <http://www.heinz.cmu.edu/~acquisti/papers/acquisti.pdf>.

[51] ACQUISTI, Alessandro; GROSSKLAGS, Jens. When 25 Cents is Enough: Willingness to Pay and Willingness to Accept for Personal Information [online]. *Workshop on the Economics of Information Security*. 2007, 22s. In: Carnegie Mellon University [online]. [cit. 10. 6. 2014]. Dostupné z: <http://weis2007.econinfosec.org/papers/66.pdf>.

[52] ACQUISTI, Alessandro; JOHN, Leslie; LOEWENSTEIN George. *What is Privacy Worth?* [online]. Carnegie Mellon University, 2010, 45 s. [cit. 10. 6. 2014]. Dostupné z: <http://www.heinz.cmu.edu/~acquisti/papers/acquisti-ISR-worth.pdf>.

[53] BARTÍK, Václav; JANEČKOVÁ, Eva. Souhlas se zpracováním osobních údajů jako součást smlouvy. *Daně a právo v Praxi*. 2012, č. 11, s. 49. In: *ASPI* [právní informační systém]. Wolters Kluwer ČR [cit. 10. 6. 2014].

[54] BORGESIOUS, Frederik. *Consent to behavioural targeting in European Law: What are the policy implications of insights from behavioural economics?* [online]. Amsterdam: Institute for Information Law, 2013, 58 s. [cit. 10. 6. 2014]. Dostupné z: <http://www.ivir.nl/staff/borgesius.html>.

- [55] CROSLEY, Stanley W. Old School Privacy is Dead, But Don't Go Privacy Crazy. *Privacy Perspectives* [online]. IAPP, publikováno 20. ledna 2014. [cit. 10. 6. 2014]. Dostupné z: https://www.privacyassociation.org/privacy_perspectives/post/old_school_privacy_is_dead_but_dont_go_privacy_crazy.
- [56] CURREN, Liam; KAYE, Jane. Revoking consent: A 'blind spot' in data protection law? *Computer Law & Security Review* [online]. 2010, vol. 26, no. 3, pp. 273-283. [cit. 10. 6. 2014]. Dostupné z: <http://www.publichealth.ox.ac.uk/helex/publications/Curren2010273>.
- [57] HOOFNAGLE, Chris Jay et al. *How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?* [online]. 2010, 20 s. [cit. 10. 6. 2014]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864.
- [58] CHMEL, Marek; SYLLOVÁ, Jindřiška. *Listina základních práv Evropské unie a česká „výjimka“ z Listiny* [online]. Praha: Parlamentní institut, 2009 [cit. 10. 6. 2014]. Dostupné z: <http://www.psp.cz/sqw/text/text2.sqw?idd=59998>.
- [59] JACOBS, David. Reports of the Death of Consent Have Been Greatly Exaggerated. *Privacy Rights Blog@epic.org* [online]. Electronic Privacy information Center, publikováno 28. 1. 2014 [cit. 10. 6. 2014]. Dostupné z: <http://epic.org/blog/2014/01/reports-of-the-death-of-consent-have-been-greatly-exaggerated-1.html>.
- [60] KUMPOŠT, Marek; MATYÁŠ, Václav. Jak si lidé cení soukromí? *Zpravodaj ÚVT MU* [online]. Brno: Masarykova univerzita, 2009, roč. 20, č. 1, s. 13-20. [cit. 10. 6. 2014]. ISSN 1212-0901. Dostupné z: <http://www.ics.muni.cz/zpravodaj/articles/626.html>.
- [61] KRČMÁŘ, Petr. Cookies umírají, reklamní branže si ale najde náhradu. *Root.cz* [online]. Internet Info, s.r.o., publikováno 13. 2. 2014. [cit. 10. 6. 2014]. Dostupné z: <http://www.root.cz/clanky/cookies-umiraji-reklamni-branze-si-ale-najde-nahradu/>.
- [62] LESSIG, Lawrence. *Code version 2.0.* [online]. New York: Basic Books, 2006, 424 s. [cit. 10. 6. 2014]. ISBN 0-465-03914-6. Dostupné z: <http://codev2.cc/download+remix/Lessig-Codev2.pdf>.
- [63] MELZER, Filip. Právní skutečnosti (právní jednání, právní události). In: CODEXIS [právní informační systém]. ATLAS consulting [cit. 10. 6. 2014].
- [64] MÝŠKA, Matěj et al. Creative Commons and Grand Challenge to Make Legal Language Simple. *AICOL Workshops* [online]. Berlin, Heidelberg, 2011, pp. 271 – 285. [cit. 10. 6. 2014] Dostupné z: http://link.springer.com/chapter/10.1007/978-3-642-35731-2_19.
- [65] OHM, Paul. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*. [online]. 2010, vol. 57, no. 6, pp. 1701 – 1777. [cit. 10. 6. 2014] Dostupné z: <http://www.uclalawreview.org/?p=1353>.
- [66] SOLOVE, Daniel J. Privacy Self-Management and the Consent Dilemmas. *Harvard Law Review* [online]. 2013, vol. 126, no. 7, pp. 1880-1903. [cit. 10. 6. 2014] Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018.
- [67] USTARAN, Eduardo. Yes, Consent Is Dead. Further, Continuing To Give It A Central Role Is Dangerous. *Privacy Perspectives* [online]. IAPP, publikováno 18. prosince 2013. [cit. 10. 6. 2014]. Dostupné z: https://www.privacyassociation.org/privacy_perspectives/post/yes_consent_is_dead_further_continuing_to_give_it_a_central_role_is_danger.

[68] WOLF, Christopher; POLONETSKY, Jules. An Updated Privacy Paradigm for the “Internet of Things”. *Future of Privacy Forum* [online]. *Future of privacy*, 2013, 12 s. [cit. 10. 6. 2014]. Dostupné z: <http://www.futureofprivacy.org/wp-content/uploads/Wolf-and-Polonetsky-An-Updated-Privacy-Paradigm-for-the-%E2%80%9CInternet-of-Things%E2%80%9D-11-19-2013.pdf>.

[69] Cookie ‘Consent’ Rule: EEA Implementation Table. *International association of privacy professionals* [online]. Field Fisher Waterhouse, publikováno 4. 2. 2013. [cit. 10. 6. 2014]. Dostupné z: https://www.privacyassociation.org/resource_center/cookie_consent_rule_eea_implementation_table.

[70] Progress on EU data protection reform now irreversible following European Parliament vote. *Press releases database* [online]. Europa.eu, [cit. 10. 6. 2014]. Dostupné z: http://europa.eu/rapid/press-release_MEMO-14-186_en.htm.

[71] *Thirty years after, The OECD privacy guidelines*. OECD, © 2011 [cit. 10. 6. 2014]. Dostupné z: <http://www.oecd.org/sti/ieconomy/49710223.pdf>.