Univerzita Palackého v Olomouci

Právnická fakulta

Tereza Šnorová

Právo na informační sebeurčení v rámci práva na ochranu soukromí

Diplomová práce

Olomouc 2016

Prohlašuji, že jsem diplomovou práci na téma „*Právo na informační sebeurčení v rámci práva na ochranu soukromí*“ vypracovala samostatně a citovala jsem všechny použité zdroje.

V Horních Ředicích dne 25. listopadu 2016 ……

Tereza Šnorová

Na tomto místě bych ráda poděkovala za cenné rady, hodnotné poznámky, pomoc a odborné vedení při zpracování diplomové práce panu doc. JUDr. Michalovi Bartoňovi, PhD., vedoucímu mé diplomové práce. Díky patří i mým blízkým, kteří mě po celou dobu studia podporovali.

Obsah

Seznam použitých zkratek

ESLP – Evropský soud pro lidská práva

SDEU – Soudní dvůr Evropské unie

NSS – Nejvyšší správní soud

NS – Nejvyšší soud

Úmluva – Sdělení federálního ministerstva zahraničních věcí č. 209/1992 Sb., o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících

Listina - 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.

ČR – Česká republika

EU – Evropská unie

sp. zn. – spisová značka

např. - například

Úvod

Téma diplomové práce *„Právo na informační sebeurčení v rámci práva na ochranu soukromí"* jsem pro svou diplomovou práci zvolila zejména z důvodu, že právo na informační sebeurčení je institutem poměrně mladým, s kterým není dle mého názoru veřejnost dostatečně seznamována. Právo na informační sebeurčení je zároveň v souvislosti s vyvíjející se právní úpravou tématem nestálým. Hlavním cílem práce je proto představit institut práva na informační sebeurčení a objasnit jeho obsah.

Jelikož žijeme v hektické době 21. století, musíme si zvykat na neustálé změny, které nás provázejí každodenním životem, především na změny technologické. S technologickým vývojem vzniká otázka, jakým způsobem moderní technologie mohou zasahovat a jakým způsobem mohou ovlivňovat oblast práva na soukromí - právo na informační sebeurčení jedince. Cílem diplomové práce je vymezení souvislosti práva na informační sebeurčení a existence internetu, kamerových systémů a analýzy DNA.

Právo na soukromí prochází v souvislosti s rozvojem moderních technologií a v souvislosti s vývojem technických prostředků dynamickým rozvojem. V souvislosti s používáním moderních technologií a v souvislosti s tím, že žijeme ve společnosti, v níž jsou informace stěžejním prostředkem pro rozvoj osobnosti, dochází v poslední dekádě k významnému rozvoji jedné ze součástí práva na soukromí, kterou je právo na informační sebeurčení.

Jelikož technických prostředků, které jsou schopny do práva na informační sebeurčení zasáhnout, je velké množství, vybrala jsem si pro svou práci rozbor práva na informační sebeurčení z hlediska existence internetu, dále z hlediska kamerových systémů umístěných ve specifických prostorech a z hlediska analýzy DNA. Pro svou práci jsem si zvolila rozbor práva na informační sebeurčení v rámci práva na ochranu soukromí z hlediska existence internetu a z hlediska existence kamerových systémů z důvodu, že s těmito technologiemi přicházíme každodenně do styku. Proto je cílem mé práce přiblížit, jakým způsobem mohou tyto technologie do našich práv zasahovat. Myslím si, že mnozí si bohužel neuvědomují, že existence těchto technologií je schopna zasáhnout do našich základních práv a někteří lidé nedbají přílišné opatrnosti a své soukromí příliš nechrání. I z tohoto důvodu dochází k vytrácení tohoto práva z našich životů.

Informační sebeurčení jedince je právo každého rozhodnout o tom, jaké informace o své osobě poskytne. Je ale nutné s tímto právem nakládat opatrně a s rozmyslem, neboť právo na informační sebeurčení jedince v oblasti používání technologií ještě nepodléhá celkové upravenosti právními předpisy. Z toho důvodu může bohužel docházet ke zneužívání informací, které o sobě poskytujeme.

V diplomové práci se věnuji popisu právních předpisů, které se k daným institutům souvisejícím s právem na informační sebeurčení vztahují. Cílem práce je také uvést ke každému z témat příslušnou judikaturu. Tuto judikaturu podrobuji analýze a vytyčuji vztah rozhodnutí soudů k právu na informační sebeurčení.

Mezi zdroje této práce budou patřit zejména monografie, komentáře a soudní rozhodnutí a dále webové zdroje. Práce je členěna kromě úvodu a závěru na čtyři samostatné kapitoly, které jsou dále členěny na podkapitoly.

V první kapitole za účelem uvedení do problematiky práva na informační sebeurčení představuji právo na soukromí, uvádím stručný vývoj práva na ochranu soukromí a dále předpisy, které toto právo upravují. Součástí první kapitoly je představení institutu testu proporcionality, v souladu s kterým může být právo na soukromí omezeno. Dále rozebírám, ze kterých jednotlivých aspektů se právo na soukromí skládá. Pro účely diplomové práce používám dělení práva na ochranu soukromí dle Elišky Wagnerové, které použila ve svém komentáři k Listině základních práv a svobod[1] (dále jen Listina).

V druhé kapitole rozebírám právo na informační sebeurčení jedince ve vztahu k existenci internetu. Nejprve se zabývám charakteristikou internetu, dále jaký je charakter zásahů do informačního sebeurčení na internetu, přiblížím pojem data retention a problémy s tímto institutem spojené a rozeberu právo na informační sebeurčení z hlediska internetových sociálních sítí.

Ve třetí kapitole se věnuji právu na informační sebeurčení ve vztahu ke kamerovým systémům. Nejprve kamerové systémy charakterizuji z hlediska práva na informační sebeurčení a provádím analýzu kamerových systémů z hlediska jejich umístění v různých prostorech. Dále rozebírám, jaké aspekty souvisejí s jednotlivými místy, na kterých se kamerové systémy nacházejí a představuji službu Google Street View a problémy, kterými tento institut v souvislosti s právní úpravou prošel v ČR.

Ve čtvrté kapitole se věnuji právu na informační sebeurčení ve vztahu k institutu analýzy DNA. Rozbor tohoto institutu z hlediska práva na informační sebeurčení jsem pro účely své práce zvolila z důvodu, že nejde sice o institut úplně nový, ale v ČR není zcela zdařile právně upravený. Cílem kapitoly, ve které se tímto institutem zabývám, je uvést, s jakými problémy je analýza DNA a právo na informační sebeurčení spojeno. V této kapitole představuji Národní databázi DNA a problematiku právní úpravy tohoto institutu. Nakonec se zabývám genetickou diskriminací, což je druh diskriminace, který je v ČR téměř nepopsaný a začíná se o něm teprve otevírat diskuse.

[1] Usnesení předsednictva ČNR č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky.

1 Právo na soukromí a jeho charakteristika

1.1 Vývoj práva na soukromí a prameny práva na soukromí

V úvodní kapitole je představen stručně vývoj právní úpravy práva na ochranu soukromí na území ČR. Dále jsou uvedeny prameny práva na ochranu soukromí z hlediska vnitrostátního i mezinárodního. Kapitola pokračuje charakteristikou práva na soukromí jako práva základního, přirozeného a osobnostního. Navazuje úvaha o definici soukromí v rámci různých pojetí práva na soukromí. Právo na soukromí je rozčleněno na čtyři aspekty soukromí, hlavní pozornost je ale věnována právu na informační sebeurčení, v rámci kterého jsou definovány osobní údaje. Je také uvedeno, jakým způsobem lze omezit právo na soukromí.

1.1.1 Vývoj právní úpravy práva na soukromí

Obsah práva na soukromí prochází neustálým vývojem, který nabývá v posledních několika letech na dynamičnosti, což jistě souvisí i s rozvojem moderních technologií. Lze konstatovat, že mezi první zmínky právní úpravy práva na soukromí patří Zákon dvanácti desek. Právo na soukromí bylo upraveno pouze velmi okrajově, v rámci Zákona dvanácti desek bylo upraveno pouze ublížení na cti jako úmyslný projev neúcty urážlivým způsobem vůči jiné osobě.[2]

Mezníkem ve vývoji právní úpravy soukromí na našem území byl zákon ABGB[3] z roku 1811, který v rámci práva na soukromí upravoval ochranu jména. Později, v roce 1920 byl přijat ústavní zákon o ochraně svobody osobní, domovní a tajemství listovního,[4] ve kterém bylo upraveno právo na soukromí v patnácti paragrafech. V roce 1933 byla zákonem o ochraně cti[5] zakotvena ochrana cti v oblasti trestního práva. Ústava z roku 1948[6] upravovala právo na soukromí v rámci svobody domovní, tajemství listovního a tajemství dopravovaných zpráv a ochrany rodiny. Ústava z roku 1960[7] a její úprava z roku 1968[8] právní úpravu práva na soukromí neobsahovala. Státní totalitní režim totiž úpravě soukromého práva příliš nepřál, neboť idea práva na soukromí byla v té době spíše popírána. Zákon o ochraně cti byl zrušen občanským zákoníkem z roku 1950,[9] který již upravoval pouze ochranu jména a to v rámci jediného paragrafu. Další vývoj zaznamenalo právo

[2] Zákon dvanácti desek, deska VIII.
[3] Zákon č. 946/1811 Sb., rakouský všeobecný zákoník občanský, ve znění ze dne 1. června 1811.
[4] Zákon č. 293/1920 Sb., o ochraně svobody osobní, domovní a tajemství listovního, ve znění ze dne 9. dubna 1920.
[5] Zákon č. 108/1933 Sb., o ochraně cti, ve znění ze dne 28. června 1933.
[6] Zákon č. 150/1948 Sb., Ústava Československé republiky, ve znění ze dne 9. května 1948.
[7] Zákon č. 100/1960 Sb., Ústava Československé socialistické republiky, ve znění ze dne 11. července 1960.
[8] Zákon č. 143/1968 Sb., Ústavní zákon o československé federaci, ve znění ze dne 27. října 1968.
[9] Zákon č. 141/1950 Sb., občanský zákoník, ve znění ze dne 25. října 1950.

na soukromí až v občanském zákoníku z roku 1964,[10] který obsahoval samostatnou úpravu ochrany osobnosti. Z této právní úpravy vyplývalo právo jednotlivce rozhodovat se podle vlastního uvážení.[11] Samotný pojem soukromí se znovu objevuje ale až v novele občanského zákoníku z roku 1991[12] v demonstrativním výčtu mezi ostatními osobnostními právy. Právo na soukromí jako celek bylo v právním řádu tehdy České a Slovenské Federativní republiky zakotveno Listinou v roce 1991.

1.1.2 Prameny práva na soukromí

Právo na soukromí je upraveno řadou mezinárodních i vnitrostátních právních dokumentů. Z mezinárodních pramenů představuje právní úpravu práva na soukromí Evropská úmluva o ochraně lidských práv (dále jen Úmluva)[13] v čl. 8 odst. 1 jako *„právo každého na respektování svého soukromého a* rodinného *života, obydlí a korespondence"*. Čl. 8 odst. 2 Úmluvy stanoví možnost zásahu státního orgánu do práva na soukromí za podmínek, kdy je zásah v souladu se zákonem, pokud je nezbytný v demokratické společnosti a pokud splňuje legitimní cíl v podobě *„zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, ochrany pořádku a předcházení zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných"*. Právní úpravu práva na soukromí obsahuje dále Úmluva č. 108,[14] která má za cíl sjednotit terminologii pojmů týkajících se ochrany osobních údajů v mezinárodním hledisku. Dalším mezinárodním pramenem je Všeobecná deklarace lidských práv,[15] která v čl. 12 stanoví pravidlo, že *„nikdo nesmí být vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence, ani útokům na svou čest a pověst. Každý má právo na zákonnou ochranu proti takovým zásahům nebo útokům."* Ochranu před svévolným zásahem do soukromého práva upravuje také Mezinárodní pakt o občanských a politických právech v čl. 17.[16]

Vnitrostátním pramenem práva na ochranu soukromí je Listina. Obecným ustanovením ochrany práva na soukromí je čl. 7 Listiny, který zaručuje nedotknutelnost osoby a jejího soukromí. Právo na soukromí je dále specifikováno v čl. 10 Listiny, který upravuje právo na soukromí z hlediska ochrany lidské důstojnosti, osobní cti, dobré pověsti a ochrany jména (čl. 10 odst. 1), ochrany rodinného a soukromého života (čl. 10 odst. 2) a práva na informační sebeurčení jedince

[10] Zákon č. 40/1964 Sb., občanský zákoník, ve znění ze dne 26. února 1964.
[11] KRATOCHVÍL, Zdeněk. Nové občanské právo. 1. vydání. Praha: Orbis, 1965, s. 63.
[12] Zákon č. 509/1991 Sb., kterým se mění, doplňuje a upravuje občanský zákoník, ve znění ze dne 5. listopadu 1991.
[13] Sdělení federálního ministerstva zahraničních věcí č. 209/1992 Sb., o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících.
[14] Sdělení Ministerstva zahraničních věcí č. 115/2001 Sb., o sjednání Úmluvy Rady Evropy č. 108, o ochraně osob se zřetelem na automatizované zpracování osobních údajů.
[15] *Všeobecná deklarace lidských práv* [online]. un.org [cit. 28. října 2016]. Dostupné na <https://childrenandarmedconflict.un.org/keydocuments/czech/universaldeclara1.html>.
[16] Vyhláška ministra zahraničních věcí č. 120/1976 Sb., o Mezinárodním paktu o občanských a politických právech a Mezinárodním paktu o hospodářských, sociálních a kulturních právech.

v podobě práva každého *„na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě“* (čl. 10 odst. 3). V Čl. 12 Listiny je upravena ochrana soukromí v prostorové dimenzi a v čl. 13 Listiny je upravena ochrana soukromí v oblasti důvěrnosti komunikace.

Ochrana soukromí v rámci soukromého práva je vyjádřena i v občanském zákoníku,[17] zejména v § 3 odst. 2 písm. a) občanského zákoníku, který stanoví, že *„každý má právo na ochranu svého života a zdraví, jakož i svobody, cti, důstojnosti a soukromí“*.

Z hlediska veřejnoprávních předpisů je ochrana soukromí vyjádřena v ust. § 180 trestního zákoníku,[18] kde je stanovena ochrana práva na informační sebeurčení v rámci trestného činu neoprávněné nakládání s osobními údaji. Zásadní pramen práva na informační sebeurčení představuje zákon o ochraně osobních údajů.[19] Ten upravuje instituty související s ochranou osobních údajů a zřizuje Úřad pro ochranu osobních údajů, který působí jako dozorčí orgán pro ochranu osobních údajů dle § 2 odst. 2 zákona o ochraně osobních údajů. Se zákonem o ochraně osobních údajů souvisí směrnice o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.[20] Cílem této směrnice je sjednotit ochranu osobních údajů v zemích Evropské unie a dále také poskytnout právní rámec volnému pohybu osobních údajů mezi státy Evropské unie.

1.2 Charakter práva na soukromí

V této podkapitole uvedu charakteristické rysy práva na ochranu soukromí. Právo na soukromí nebo také právo na ochranu soukromí patří mezi základní lidská práva. Nositelem tohoto práva je každá fyzická osoba, tedy každý člověk. V některých oblastech toto právo náleží i osobám právnickým, mezi takové oblasti patří zejména dobré jméno právnické osoby, ochrana důvěrnosti komunikace nebo oblast ochrany domovní svobody. Právo na soukromí je charakteristické tím, že má přirozenoprávní povahu, to znamená, že každému člověku náleží již od narození a právnické osobě náleží od okamžiku jejího vzniku. Právo na soukromí je také charakteristické tím, že patří mezi práva osobnostní, to znamená, že je tímto právem chráněna osobnost člověka. Do osobnostních práv patří zejména ochrana jména, cti, pověsti a důstojnosti člověka.

Co se týče definice pojmu právo na soukromí, lze konstatovat, že jde o problematickou otázku, neboť pojem soukromí není zcela vyčerpávajícím způsobem vymezen v žádném právním

[17] Zákon č. 89/2012 Sb., občanský zákoník.
[18] Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.
[19] Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů.
[20] Rozhodnutí Rady 95/46/ES ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Úř. věst. L 281 ze dne 23. listopadu 1995.

dokumentu. Složitost vymezení pojmu souvisí s jeho neustálou dynamikou, vývojem a proměnlivostí. Za jednu z prvních studií, která byla v souvislosti s vymezením pojmu soukromí provedena, je považována studie dvou amerických právníků Samuela D. Warrena a Louise D. Brandeise z roku 1890 *„The Right to Privacy"*, kteří došli k vymezení práva na soukromí jako práva „*the right to be let alone,*" což můžeme přeložit jako právo být ponechán o samotě, nebo právo být ponechán sebou samým.[21] V tomto pojetí byl vyjádřen význam práva na soukromí jako práva oddělit se od ostatních nebo rozhodovat samostatně o svém životě. Soukromí lze chápat také jako možnost kontrolovat informace, čímž se již dostáváme k soukromí v oblasti informační sféry dle Alana F. Westina, který říká, že *„soukromí je nárok jednotlivců, skupin a institucí určovat kdy, jak a co bude o nich sdělováno ostatním"*[22].

Právo na soukromí je charakteristické tím, že na něho lze pohlížet jako na dva rozdílné závazky státu, kterými jsou právo na soukromí v negativním smyslu (status negativus) a právo na soukromí v pozitivním smyslu (status positivus). V negativním smyslu znamená právo na soukromí povinnost státu nezasahovat do soukromí jednotlivce, čímž je vyjádřen pasivní postoj státu vůči právu na soukromí, znamená také právo každého na nerušený výkon jeho práva. Právo na soukromí z pohledu negativního závazku státu je vyjádřen i v rozhodnutí ESPL ve věci *S. a Marper proti Spojenému království*. Na právo na soukromí se hledí jako na právo *„být nechán na pokoji"*[23]. V tomto slovním spojení je vyjádřen status negativus práva na soukromí, na základě kterého by do práva na soukromí nemělo být zasahováno jednak v prostorové dimenzi, tedy v oblasti fyzické a psychické integrity, ale i z hlediska rozhodování o vlastní identitě, tedy v oblasti rozhodování o jméně, pohlaví, sexuálním životu a šíření informací o sobě.[24]

Naopak právo na soukromí v pozitivním smyslu znamená, že stát je povinen *„přijmout rozumná a přiměřená opatření k zajištění a k ochraně práv jednotlivců na respektování jejích soukromého života"*[25]. To znamená, že stát je povinen zakotvit ochranu práva na soukromí do právního řádu a je povinen zajistit vynutitelnost tohoto práva státní mocí.[26] K hranici mezi pozitivním a negativním závazkem státu se vyjádřil ESLP v rozhodnutí *Von Hannover proti Německu,* v němž soud uvedl, že hranici mezi pozitivním a negativním závazkem státu není možné striktně vymezit.[27]

---

[21] WARREN, Samuel, BRANDEIS, Louis. The right to privacy. *Harward Law Review*, 1890, vol. IV. December, č. 5, s. 193-220.
[22] WESTIN, Alan F. *Freedom and Privacy*. New York: Athenum, 1967, s. 7.
[23] Rozsudek ESLP ve věci *S. a Marper proti Spojenému království* ze dne 4. prosince 2008, stížnost č. 30562/04, § 66.
[24] KRATOCHVÍL, Jan. In KMEC, Jiří (ed). *Evropská Úmluva o lidských právech: komentář*. 1. vydání Praha: C. H. Beck, 2012, s. 868.
[25] Rozsudek ESLP ve věci *Storcková proti Německu* ze dne 16. června 2005, stížnost č. 61603/00, §149.
[26] SVATOŇ, Jan. *Státověda*. 5. vydání. Praha: Wolters Kluwers, a. s., 2011, s. 189.
[27] Rozsudek ESLP ve věci *Von Hannover proti Německu* ze dne 24. června 2004, stížnost č. 59320/00, § 57.

1.3 Aspekty práva na soukromí

Právo na ochranu soukromí můžeme dělit podle určitých charakteristických rysů do několika oblastí. Dle mého názoru došla k logickému a přehlednému dělení práva na soukromí Eliška Wagnerová, která člení právo na soukromí do čtyř oblastí, a to na osobní soukromou sféru, kam je zahrnuto právo na informační sebeurčení, soukromí v rodinném životě, důvěrnost komunikace a soukromí v prostorové dimenzi.[28] V následující části práce představím jednotlivé oblasti práva na soukromí, blíže se budu věnovat právu na informační sebeurčení.

1.3.1 Ochrana rodinného života

Ochrana soukromí v oblasti rodinného života je upravena v čl. 10 odst. 2 Listiny. Předpokladem ochrany soukromí rodinného života je existence rodiny, ale soud při poskytování ochrany rodinnému životu nerozlišuje, zda rodina je tvořena formálně, tedy sezdaným párem, nebo neformálně nesezdaným párem.[29] Ochrana rodinného života se vztahuje zejména na otázky rodinných vztahů, rovnost manželství, ochranu intimity, ochranu sexuálních menšin nebo otázku interrupcí a adopcí.

1.3.2 Právo na soukromí v prostorové dimenzi

Právem na soukromí v prostorové dimenzi rozumíme ochranu domovní svobody, která souvisí s tím, že obydlí je nedotknutelné a není dovoleno do něj vstupovat bez souhlasu osoby, která v něm bydlí, což je stanoveno v čl. 12 odst. 1 Listiny. Toto právo vyjadřuje právo nebýt rušen v soukromé prostorové sféře. Tato sféra souvisí zejména se soukromím v oblasti rodinného života,[30] neboť obydlí často představuje místo, kde se střetávají osoby, mezi nimiž existují rodinné vazby.

Ochrana soukromí v oblasti prostorové dimenze je poskytována i v prostoru, který je užíván jen přechodně. Mezi tyto prostory patří například koleje nebo studentské byty využívané během školního semestru. Stejná ochrana jako domovním prostorám náleží i prostorám náležejícím k domu nebo bytu. Takovými prostory jsou garáže, zahrady, sklepy nebo terasy.[31]

---

[28] WAGNEROVÁ, Eliška. Právo na soukromí: Kde má být svoboda, tam musí být soukromí. In ŠIMÍČEK, Vojtěch (ed). *Právo na soukromí.* Brno: MUNI press, 2011, s. 54.
[29] Rozsudek ESLP ve věci *Marckx proti Belgii* ze dne 13. června 1979, stížnost č. 6833/74, § 31.
[30] WAGNEROVÁ, Eliška. In WAGNEROVÁ, Eliška (ed). *Listina základních práv a svobod komentář.* 1. vydání. Praha: Wolters Kluwer ČR, a. s., 2012, s. 330.
[31] WAGNEROVÁ: *Listina základní práv*…, s. 332.

1.3.3 Ochrana komunikace v soukromé sféře

Ochranu soukromí v oblasti důvěrnosti komunikace upravuje čl. 13 Listiny, toto právo je také označováno jako „*listovní tajemství*". Ochrana důvěrnosti komunikace jinými slovy znamená ochranu informací sdělených mezi konkrétními osobami bez možnosti zásahu třetí osoby do obsahu komunikace. Omezení práva v oblasti důvěrnosti komunikace bývá odůvodněno zejména instituty trestního práva, jako je zadržení a otevření poštovních zásilek nebo odposlech a záznam telekomunikačního zařízení.[32]

Pod tento pojem řadíme tajemství písemností a záznamů uchovávaných v soukromí, tajemství přepravovaných zpráv v jakékoli formě a také moderní formy komunikace jako jsou e - maily, SMS, chat, Skype a zprávy posílané prostřednictvím technických prostředků jako je osobní počítač, notebook, mobil nebo tablet. Původně toto právo vzniklo za účelem ochrany poštovních zpráv, ale v souvislosti s rozvojem technologií se ukázalo jako nutné, aby se vztahovalo i na další uvedené formy komunikací.[33]

Součástí práva v oblasti důvěrnosti komunikace je ochrana zpráv i před osobami, které se na přepravě zpráv samy podílejí. Judikatura vztáhla ochranu komunikace také na vnější projevy komunikace, mezi které patří okolnosti, za nichž komunikace probíhá, tedy okolnosti jako jsou čas, způsob komunikace, místo nebo účastníci komunikace.[34]

1.3.4 Informační sebeurčení jednotlivce

Co představuje pojem právo na informační sebeurčení? Takovou otázku si kladl Ústavní soud ve svém rozhodnutí ze dne 22. března 2011, sp. zn. Pl. ÚS 24/10, kde vymezil institut práva na informační sebeurčení jako součást práva na soukromí, na základě kterého *„právo na respekt k soukromému životu zahrnuje i garanci sebeurčení ve smyslu zásadního rozhodování jednotlivce o sobě samém. Jinými slovy, právo na soukromí garantuje rovněž právo jednotlivce rozhodnout podle vlastního uvážení, zda, popř. v jakém rozsahu, jakým způsobem a za jakých okolností mají být skutečnosti a informace z jeho osobního soukromí zpřístupněny jiným subjektům. Jde o aspekt práva na soukromí v podobě práva na informační sebeurčení, výslovně garantovaný čl. 10 odst. 3 Listiny.*"[35]

Čl. 10 odst. 3 Listiny výslovně upravuje ochranu práva na informační sebeurčení ve smyslu, že *„každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě"*. Z toho vyplývá, že právo na informační sebeurčení znamená právo každého se

[32] WAGNEROVÁ: *Listina základní práv*…, s. 219.
[33] WAGNEROVÁ: *Listina základní práv*…, s. 341.
[34] WAGNEROVÁ: *Listina základní práv*…, s. 341.
[35] Nález Ústavního soudu ze dne 22. března 2011, sp. zn. Pl. ÚS 24/10, bod 29.

rozhodnout, které informace o své osobě poskytne ostatním. Znamená to právo na ochranu před sledováním soukromí ze strany veřejné moci, zároveň ale nevylučuje například preventivní sledování osob na veřejnosti kamerovými systémy, pokud je takové sledování v souladu s testem proporcionality,[36] který přibližuji v následující podkapitole.

Poprvé byl pojem právo na informační sebeurčení použit a definován v rozhodnutí Německého Spolkového Ústavního soudu ze dne 15. prosince 1983 ve věci posouzení ústavnosti zákonné úpravy procesu sběru a uchování dat za účelem sčítání lidu, ve kterém bylo uvedeno, že „*v moderní společnosti charakterizované i obrovským nárůstem informací a dat musí být ochrana jednotlivce před neomezeným sběrem, uchováváním, užitím a zveřejňováním dat o její/jeho osobě a soukromí poskytována v rámci obecnějšího, ústavně garantovaného práva jednotlivce na soukromí. Pokud jednotlivci nebude garantována možnost hlídat a kontrolovat obsah i rozsah osobních dat a informací jím poskytnutých, jež mají být zveřejněny, uchovány či použity k jiným než původním účelům, nebude-li mít možnost rozpoznat a zhodnotit důvěryhodnost svého potenciálního komunikačního partnera a případně tomu uzpůsobit i své jednání, pak nutně dochází k omezení až potlačování jeho práv a svobod, a nelze tak již nadále hovořit o svobodné a demokratické společnosti. Právo na informační sebeurčení (informationelle Selbstbestimmung) je tak nezbytnou podmínkou nejen pro svobodný rozvoj a seberealizaci jednotlivce ve společnosti, nýbrž i pro ustavení svobodného a demokratického komunikačního řádu.*“[37]

K právu na informační sebeurčení lze doplnit zajímavý názor o existenci digitální nebo informační stopy, která souvisí s životem každé osoby. Pod tímto pojmem můžeme rozumět, že každá osoba vytváří informace o sobě na jednu stranu úmyslně, ale na druhou stranu i mimoděk. Tyto informace jsou s člověkem spojeny, a tím dochází k vytvoření informační stopy za každou osobou zejména v prostředí internetu.[38] K úmyslnému vytváření informační stopy může docházet aktivitou osob na sociálních sítích, nebo například interakcemi s ostatními na internetu. O informační stopě vytvořené mimoděk se jedná v případě informací, které jsou o osobě jako uživateli internetu shromažďovány prostřednictvím cookies – jsou to zejména informace ohledně délky navštívení internetové stránky, informace o adrese zařízení, ze kterého byla internetová stránka navštívena a podobně. Z důvodu nepochybné existence informační stopy, která je s jedincem spojena například v souvislosti se zveřejňováním fotografií na internetu nebo v novinách, na základě účasti osob v písemných diskusích nebo zobrazením osoby ve videích, je nutné regulovat právo na soukromí vytvořením institutu osobních údajů, kterému se věnuji v následující podkapitole.

[36] WAGNEROVÁ: *Listina základní práv*…, s. 284.
[37] Rozsudek Spolkového ústavního soudu SRN ze dne 15. prosince 1983, sp. zn. BVerfGE 65, 1.
[38] MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie práva a soukromí*. 1. vydání. Praha: CZ.NIC, 2013, s. 39.

Právo na informační sebeurčení může být pojato také jako právo osoby rozhodnout o tom, jakým způsobem bude žít svůj život. Tímto pojetím práva na informační sebeurčení se zabýval ve svém rozhodnutí ESLP ve věci *Pretty proti Spojenému království*. V této věci se ESPL zabýval právem stěžovatelky spáchat sebevraždu. Protože stěžovatelkou byla ale osoba, která vzhledem ke svému zdravotnímu stavu nebyla sebevraždu schopna vykonat samostatně, žádala o právo na spáchání sebevraždy s asistencí svého manžela, který za toto jednání podle jejího požadavku neměl být trestně stíhán. ESLP ale nakonec právo na asistovanou sebevraždu nedovodil, uvedl, že právo na život by nemělo být interpretováno tak, že zahrnuje i negativní aspekt tohoto práva.[39]

Právo osoby rozhodnout o tom, jak bude svůj život žít, tedy zahrnuje právo žít život i takovým způsobem, kdy člověk sám sobě ubližuje nebo se poškozuje. Toto právo ale zároveň znamená, že pokud se člověk rozhodne svůj život ukončit, nemá právo na to, aby mu k tomuto jednání jiná osoba beztrestně dopomohla. Výjimkou jsou některé státy EU, u kterých je asistovaná sebevražda legální.

1.4 Právo na informační sebeurčení a osobní údaje

Jak bylo již uvedeno, s právem na informační sebeurčení souvisí institut osobních údajů. Právní úpravou tohoto institutu je možné poskytnout ochranu před zneužitím informací, které souvisejí se soukromím osob. Dále je možné upravit nakládání, uchovávání, sběr či likvidaci těchto informací.

Ke shromažďování dat týkajících se člověka se vyjádřil ESLP ve věci *Rotaru proti Rumunsku*. ESLP ve svém rozhodnutí uvedl, že *„jsou osobní data shromažďována a využívána v souladu se zákonem, jen pokud existuje přehledná právní úprava této činnosti a pokud se mohou dotčené osoby účinně domoci, aby soudy přezkoumaly, zda nejsou tato data shromažďována nad míru, která je v demokratické společnosti nezbytná, a zda jsou využívána jen k legitimním účelům“*[40]. Dále uvedl, že shromažďování a uchovávání osobních údajů je zásahem do práva na informační sebeurčení a není zároveň rozhodné, zda jde o informace, které jsou získávány ze soukromého nebo z veřejného života jedince.[41]

Právní ukotvení osobních údajů je tedy podmínkou nakládání s osobními daty. Tento požadavek považuji za nezbytný už z hlediska toho, že žijeme v informační době a v informační společnosti a informace, osobní data a osobní údaje jsou od nás vyžadovány den co den při každém jednání.

[39] Rozsudek ESLP ve věci *Pretty proti Spojenému Království* ze dne 29. dubna 2002, stížnost č. 2346/02, § 61–62.
[40] Rozsudek ESLP ve věci *Rotaru proti Rumunsku* ze dne 4. května 2000, stížnost č. 28341/95, § 44.
[41] Rozsudek ESLP ve věci *Rotaru proti Rumunsku* ze dne 4. května 2000, stížnost č. 28341/95, § 44.

V ČR jsou osobní údaje upraveny v § 4 písm. a) zákona o ochraně osobních údajů. *„Osobním údajem je jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu."* Dle § 4 písm. d) zákona o ochraně osobních údajů je *„subjektem údajů osoba fyzická, k níž se osobní údaje vztahují"*. Subjektem osobních údajů může být tedy pouze člověk.

Pojem osobní údaje je uváděn i v jiných právních předpisech ČR. Kromě zákona o ochraně osobních údajů používá tento pojem i trestní zákoník, zákon o svobodném přístupu k informacím, zákoník práce nebo Listina. Podle mého názoru jsou osobní údaje touto právní úpravou v ČR dostatečně upraveny.

1.5 Omezení práva na soukromí

Právo na soukromí je právo relativní povahy, to znamená, že je to právo omezitelné. Možností omezení práva na ochranu soukromí se zabýval Ústavní soud ve svém nálezu ze dne 18. prosince 2006, sp. zn. I. ÚS 321/06, ve kterém je vyjádřeno, že za splnění určitých podmínek lze přikročit dle Listiny k omezení základních lidských práv, tedy i práva na soukromí. Podmínkou přípustnosti omezení základního práva je omezení *„za účelem ochrany základních práv jiných osob, nebo za účelem ochrany veřejného zájmu, který je v podobě principu či hodnoty obsažen v ústavním pořádku"*[42]. Právo na soukromí může být omezeno zásahem, pokud se dostane do kolize s jiným základním právem. V takovém případě je potřeba posoudit účel takového zásahu na základě testu proporcionality.

Test proporcionality slouží k prověření, zda byla dodržena ústavnost omezení základních práv. Zahrnuje v sobě tři kroky, na základě kterých je posuzována přípustnost zásahu do základního práva. Prvním krokem testu proporcionality je test vhodnosti. Na základě testu vhodnosti je zkoumána způsobilost naplnění účelu, podle kterého musí být použité opatření schopné dosáhnout předem určeného cíle, kterým je ochrana základních práv jiných osob nebo ochrana veřejného zájmu. Dalším krokem testu proporcionality je test potřebnosti, na základě kterého je možné k omezení práva použít prostředek, který je nejšetrnější k dotčeným základním právům. Třetím krokem je vlastní test proporcionality, na základě kterého nesmí být újma na základním právu nepřiměřená ve vztahu k zamýšlenému cíli. Pokud je zásah do práva na soukromí v souladu s testem proporcionality, je zároveň nutné, aby došlo k minimálnímu zásahu do tohoto práva. Test proporcionality tedy připouští pouze takový zásah do soukromí, který je nutný a který lze ještě

[42] Nález Ústavního soudu ze dne 18. prosince 2006, sp. zn. I. ÚS 321/06, bod 21.

požadovat pro naplnění účelu omezení tohoto práva. Test proporcionality je rozebrán například v rozhodnutí Ústavního soudu ze dne 20. června 2006, sp. zn. Pl. ÚS 38/04.[43]

Pokud srovnáme úpravu přípustnosti omezení práva na soukromí v Listině a v Úmluvě, dojdeme k závěru, že Úmluva obsahuje na rozdíl od Listiny limitační klauzuli zakotvenou v čl. 8 odst. 2, která stanoví legitimní cíle, na základě kterých lze omezit právo na soukromí. Mezi limity omezení práva na ochranu soukromí kromě případů, kdy je to v souladu se zákonem a nezbytné v demokratické společnosti, patří zájem národní bezpečnosti, veřejné bezpečnosti, hospodářský blahobyt země, ochrana pořádku a předcházení zločinnosti, ochrany zdraví, morálky, nebo ochrany práv a svobod jiných. Dle Úmluvy lze tedy připustit zásahy do práva na soukromí v rámci uvedených limitů, zároveň ale každý případ omezení práva na soukromí musí být posuzován samostatně a individuálně vzhledem k okolnostem jednotlivých případů.

Také zkoumání, zda došlo nebo nedošlo k porušení práva zaručeného Úmluvou, se liší. Při zjišťování, zda bylo porušeno právo na soukromí podle čl. 8 Úmluvy, ESPL postupuje podle pětistupňového testu. Tento test lze vyjádřit v pěti otázkách: „*1) spadá projednávaný případ pod rozsah namítaného článku Úmluvy?; 2) došlo k „zásahu" do namítaného práva stěžovatele?; 3) byl tento zásah „v souladu se zákonem"?; 4) sledoval tento zásah alespoň jeden z legitimních cílů?; a konečně 5) byl tento zásah „nezbytný v demokratické společnosti"?"*[44]

[43] Nález Ústavního soudu ze dne 20. června 2006, sp. zn. Pl. ÚS 38/04, bod 27.
[44] KOSAŘ, David. *Evropská Úmluva* …, s. 101.

2 Právo na informační sebeurčení a internet

2.1 Úvod do problematiky internetu

V této kapitole se zabývám vztahem internetu a práva na informační sebeurčení. Internetové spojení je nedílnou součástí této doby, dá se konstatovat, že se stalo nedílnou součástí našich životů. Mnozí si svět bez internetu, který by se dal označit jako hlavní zdroj lidského poznání 21. století, neumí představit. Je důležité si uvědomit, že internet přispěl i k rozvoji a uplatňování základních lidských práv, a to zejména práva na informace a práva na svobodu projevu.[45] Před vznikem internetu byli lidé odkázáni získávat informace jiným způsobem, který jistě nebyl tak rychlý a jednoduchý. Dříve lidé získávali informace zejména prostřednictvím knihoven, databází nebo úřadů. V dnešní době, kdy člověk na internet vložil informace z mnoha oblastí lidského poznání, může každý, kdo disponuje internetovým připojením, informace získávat rychle a jednoduše.

Vztah internetu s právem na informační sebeurčení je velmi úzký, vyplývá to například z pojmu *„internet privacy"* nebo také *„online privacy"*. Tyto pojmy vyjadřují, že soukromí a osobní údaje na internetu, je možné chránit a zabezpečovat právní regulací. Ochrana soukromí by logicky měla být pro uživatele internetu prvořadá, jelikož prostřednictvím internetu dochází k neustálému sběru osobních údajů, které jsou s osobou spojeny, jako již zmíněná informační stopa.[46] Při pohledu zejména na sociální sítě, kde uživatelé uveřejňují mnohdy i intimní soukromé informace ze svého života, lze polemizovat o tom, zda uživatelé internetu o ochranu soukromí stojí.

Proti možnosti využívat internet jako informační zdroj patří možnost jeho zneužití jako předmětu trestného činu. Trestná činnost spojená s existencí internetu se nazývá kybernetická kriminalita, zkráceně kyberkriminalita nebo kybernalita.[47] Tato trestná činnost je postupně začleňována do trestních předpisů, výjimkou nejsou ani trestní předpisy ČR, příkladem je trestný čin dle § 230 trestního zákoníku – neoprávněný přístup k počítačovému systému a nosiči informací nebo trestný čin dle § 231 trestního zákoníku – opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat. Dalším příkladem kybernality je činnost jako

[45] KOKEŠ, Marian. Několik poznatků k problematice konkrétních konfliktů mezi právem na informační sebeurčení a ochranou národní bezpečnosti v tzv. době internetové. In ŠIMÍČEK, Vojtěch (ed). *Právo na soukromí.* Brno: MUNI press, 2011, s. 127.

[46] *Internet privacy* [online]. techopedia.com, [cit. 4. ledna 2016]. Dostupné na <https://www.techopedia.com/definition/24954/internet-privacy>.

[47] JIROVSKÝ, Václav. *Kybernetická kriminalita*. 1. vydání. Praha: Grada, 2007, s. 25.

hacking, kybernetické výpalné, zneužití internetových stránek, spamming a mnoho dalších, které uvádím pouze jako příklad, jelikož rozbor kybernality není předmětem této práce.[48]

K účinné ochraně před zásahem do soukromí uživatele internetu by musela vést kontrola každého příspěvku na internetu před jeho zveřejněním, to by ale znamenalo cenzuru, která je v demokratické společnosti nepřijatelná.

2.2 Charakter zásahů do informačního sebeurčení na internetu a právo *„být zapomenut“*

Zásahy do práva na informační sebeurčení mají díky internetu odlišnou podobu ve srovnání se zásahy do tohoto práva před existencí internetu. Dříve měly zásahy do soukromí charakter více zhmotnělý v tom smyslu, že osoby zasahující do soukromí byly konkrétní a mnohem lépe dohledatelné. Do soukromí zasahovala například média v tištěné nebo zvukové podobě. Zásahy do soukromí byly snáze zjistitelné a dotčená osoba měla o zásahu do soukromí většinou povědomí. V souvislosti s internetem jsou ale zásahy velmi časté a zároveň málo intenzivní. To znamená, že osoba o zásahu do tohoto práva nemusí vůbec vědět, nemusí poznat, že jsou o ní shromažďovány osobní údaje a jiné informace. V internetové době jsou osoby, které zasahují do práva na informační sebeurčení velmi těžko zjistitelné.[49] To souvisí zejména s vysokou mírou anonymity osob, jelikož osoby při projevech na internetu mohou vystupovat pod smyšlenými jmény.

Zásahy do práva na informační sebeurčení prostřednictvím internetu jsou charakteristické také tím, že je nelze účinně kontrolovat a předcházet jim. Sbírání dat se z důvodu jeho množství a neustálých proměn vymyká právní regulaci a není možné ho podrobit spolehlivé právní kontrole. Tím se snižuje možnost jedince zachovat ochranu práva na informační sebeurčení.[50]

Zásahem do práva na informační sebeurčení je i to, že vše, co uživatel na internet vloží, je nesmazatelnou stopou spojeno s jeho osobou a je umístěno trvale v rámci internetové sítě, internet totiž *„nezapomíná“*.[51] Při pohledu na fakt, že s každodenním používáním internetu se rozšiřuje digitální stopa v podobě informací o aktivitě jedince, nás může napadnout otázka, zda by nemělo existovat i právo být na internetu *„zapomenut“*? Touto otázkou se zabýval SDEU v věci *Costeja proti Google Spain.* Soud uložil povinnost likvidace osobních údajů z internetového prohlížeče, pokud

[48] JIROVSKÝ, Václav. *Kybernetická kriminalita*. 1. vydání. Praha: Grada, 2007, s. 7.
[49] KÜHN, Zdeněk. Ochrana soukromí v internetové době. In ŠIMÍČEK, Vojtěch (ed). *Právo na soukromí.* Brno: MUNI press, 2011, s. 110-111.
[50] KOKEŠ, Marian. Několik poznatků k problematice konkrétních konfliktů mezi právem na informační sebeurčení a ochranou národní bezpečnosti v tzv. době internetové. In ŠIMÍČEK, Vojtěch (ed). *Právo na soukromí.* Brno: MUNI press, 2011, s. 127.
[51] SCHONBERGER, Viktor Mayer. *Delete – The Virtue of Forgetting in the Digital Age*, Princeton University Press, 2009, s. 1.

o to konkrétní osoba společnost provozující internetový prohlížeč požádá. Jedná se o přelomový rozsudek, který představuje jeden z prostředků ochrany práva na informační sebeurčení, ale pouze za podmínky, pokud o takovou ochranu osoba sama aktivně požádá. V této věci figuroval španělský občan Mario Costeja Gonzales, který neplatil příspěvky na sociální zabezpečení a v důsledku toho mu vznikl dluh. Následně byla v souvislosti s nezaplaceným dluhem prodána jeho nemovitost v rámci vykonávacího řízení. Problémem bylo, že prostřednictvím internetu bylo možné i po téměř dvou desítkách let od prodeje nemovitosti tuto skutečnost dohledat, protože internet tuto informaci stále uchovával. V souladu s existencí směrnice o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů[52] SDEU rozhodl o tom, že informace o prodeji nemovitosti nebude možné nadále vyhledat prostřednictvím internetového prohlížeče Google Spain, neboť zveřejněním uvedené skutečnosti po tak dlouhou dobu došlo k neoprávněnému zásahu do informačního sebeurčení jedince.[53] Jako důsledek tohoto rozhodnutí začala společnost Google poskytovat uživatelům internetu on-line formuláře označené jako *„žádosti o odstranění z vyhledávání na základě evropských předpisů o ochraně údajů"*[54]. Prostřednictvím vyplnění formuláře, který je dostupný na internetové stránce https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=cs, může uživatel internetového prohlížeče www.google.com požádat o odstranění údajů souvisejících s jeho osobou z výsledků vyhledávání prostřednictvím internetového prohlížeče. Po podání žádosti o odstranění osobních údajů probíhá analýza, zda právo na ochranu informačního sebeurčení jedince převažuje nad právem na informace. Pokud je shledáno, že právo na informační sebeurčení v rámci práva na ochranu soukromí převažuje, je výsledek vyhledávání z internetového prohlížeče odstraněn.

Otevření otázky ohledně práva být na internetu zapomenut považuji za velký přínos ochrany práva na soukromí. Zejména kladně hodnotím i přístup společnosti Google v tom, že sama navrhla řešení jako následek uvedeného rozhodnutí a sama poskytla prostředek možnosti případné ochrany práva na soukromí, pokud budou splněny nastavené podmínky.

2.3 Data retention na internetu

Pojem data retention je další problematikou, která je spojena s informačním sebeurčením jedince. Tento pojem znamená plošné shromažďování provozních a lokalizačních údajů poskytovatelů veřejné komunikační sítě o komunikaci uživatelů služeb elektronických komunikací

[52] Rozhodnutí Rady 95/46/ES ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Úř. věst. L 281, 23. listopadu 1995, čl. 22 – 28.
[53] Rozsudek SDEU ze dne 13. května 2014, *Google Spain proti Mario Costeja González*, C 131/12, § 21.
[54] *Žádost o odstranění z vyhledávání na základě evropských předpisů o ochraně údajů* [online]. google.com, [cit. 5. ledna 2016]. Dostupné na <https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=cs>.

bez výjimky a bez nutnosti podezření ze spáchání trestné činnosti. Prostřednictvím data retention dochází k zaznamenávání informací o proběhlých telefonních spojeních, emailech nebo textových zprávách, souhrnně o datových přenosech. Zároveň platí, že s takovým shromažďováním není současně shromažďován obsah takové komunikace. Pokud bychom se snažili pojem data retention dohledat v právním řádu ČR, nebyly bychom úspěšní, pojem data retention není v právním řádu ČR definován, jde spíše o technicky vykládaný pojem.[55]

Právní úpravu data retention na evropské úrovni tvořila kontroverzní směrnice č. 2006/24/ES o uchování dat,[56] která byla včleněna do českého právního řádu v podobě § 97 zákona č. 127/2005 Sb., o elektronických komunikacích[57] a prováděcí vyhláškou č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů o době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání.[58] Vyhláška upravovala dobu uchování provozních a lokalizačních údajů a formu a způsob jejich předávání orgánům oprávněným k jejich využívání. V této vyhlášce byly vymezeny podmínky uchovávání informací o poloze jedince. Právní regulace touto vyhláškou měla za účel zajištění bezpečnosti poskytování služeb, které získávají informace o lokalizaci osob.[59]

Tato právní úprava se ale dostala do řízení před Ústavním soudem. Podle rozhodnutí Ústavního soudu ze dne 22. března 2011, sp. zn. Pl. ÚS 24/10, se jevilo jako nežádoucí, aby subjekty jako poskytovatelé mobilních služeb měly oprávnění ke sběru a uchovávání lokalizačních a provozních informací o jejich uživatelích.[60] Bylo tomu z důvodu, že účel takového shromažďování nebyl v žádném zákoně specifikován, nebyl vymezen rozsah uchovávaných údajů, práv a povinností a nebylo stanoveno ani kontrolní opatření těchto shromažďovaných a uchovávaných informací. Ústavní soud v nálezu judikoval, že právní úprava data retention nebyla v souladu s ústavním principem předvídatelnosti rozhodnutí a legitimního očekávání, a byla tedy v rozporu s právní jistotou státu a úpravu data retention označil jako neústavní[61] a následně došlo ke zrušení ustanovení § 97 odst. 3 a 4 zákona č. 127/2005 Sb., o elektronických komunikacích, které se týkalo doby uchování údajů, kdy poskytovatelé služeb elektronických komunikací měli povinnost uchovávat provozní a lokalizační údaje po dobu šest až dvanáct měsíců.[62]

---

[55] MATEJKA, Ján. *Internet jako objekt*…, s. 129.
[56] Rozhodnutí Rady 2006/24/ES ze dne 15. března 2006, o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES. Úř. věst. L 105/54 ze dne 13. dubna 2006.
[57] Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.
[58] Vyhláška č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání, ve znění pozdějších předpisů.
[59] MATEJKA, Ján. *Internet jako objekt*…, s. 130.
[60] Nález Ústavního soudu ze dne 22. března 2011, sp. zn. Pl. ÚS 24/10, bod 41.
[61] MATEJKA, Ján. *Internet jako objekt práva*… s. 129-133.
[62] MATEJKA, Ján. *Internet jako objekt práva*…, s. 133-135.

Na rozhodnutí Ústavního soudu, sp. zn. Pl. ÚS 24/10 reagoval dalším rozhodnutím Ústavní soud, sp. zn. Pl. ÚS 24/11, na základě kterého bylo zrušeno jako neústavní ustanovení § 88a trestního řádu, které upravovalo institut zajištění důkazů prostřednictvím odposlechu a záznamu telekomunikačního provozu pro trestní řízení. Bylo to proto, že ustanovení § 88a trestního řádu představovalo nepřiměřený zásah do práva na informační sebeurčení jedince tím, že nebyl striktně vymezen účel a podmínky, za kterých bylo možné tento institut použít. Na základě uvedeného ustanovení bylo možné pro účely trestního řízení zpřístupnit osobám činným v trestním řízení údaje z telekomunikačního provozu osoby při prošetřování velkého množství trestných činů. Ústavní soud se zabýval otázkou, „*zda napadené ustanovení poskytuje z hlediska základního práva na informační sebeurčení dostatečné garance proti zneužití předmětných údajů během celého trvání trestního řízení. Těmito garancemi je přitom třeba rozumět jak stanovení podmínek, za nichž mají mít příslušné orgány přístup k údajům o uskutečněném telekomunikačním provozu, tak i existenci účinné kontroly jejich dodržování.*“ [63] V napadeném ustanovení nebylo vymezeno, na které trestné činy se tento prostředek vztahuje. *„Ústavní soud má za to, že tímto způsobem upravené meze základního práva na informační sebeurčení jsou formulovány velmi široce a neurčitě a ve své podstatě umožňují vyžádání a použití předmětných údajů ze strany orgánů činných v trestním řízení pokaždé, je-li jim možné přiznat nějakou souvislost s probíhajícím trestním řízením.“*[64] Ústavním soudem bylo shledáno, že ustanovení § 88a trestního řádu není v souladu s právem na ochranu tajemství zpráv ve smyslu čl. 13 Listiny a bylo zrušeno.[65]

Na uvedená rozhodnutí Ústavního soudu reagoval zákonodárce novelou zákona č. 273/2012 Sb., o elektronických komunikacích,[66] který sice obsahuje povinnost uchovávat provozní a lokalizační údaje po dobu maximálně 6 měsíců, ale zároveň reaguje na uvedená rozhodnutí Ústavního soudu. Byly vymezeny orgány, které mohou provozní a lokalizační údaje žádat, dále byly vymezeny trestné činy, u kterých lze tyto údaje žádat. Podrobnosti k tomuto zákonu upravuje vyhláška č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů.[67]

Na problematiku data retention reagoval i SDEU v řízení o předběžné otázce ve věci *Digital Rights Ireland a Kärntner Landesregierung*[68] a dne 8. dubna 2014 SDEU zrušil směrnici 2006/24/ES o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí z důvodu, že

[63] Nález Ústavního soudu ze dne 20. prosince 2011, sp. zn. Pl. ÚS 24/11, body 29-30.
[64] Tamtéž.
[65] Tamtéž.
[66] Zákon č. 273/2012 Sb., o elektronických komunikacích, ve znění pozdějších předpisů.
[67] Vyhláška č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů, ve znění pozdějších předpisů.
[68] Rozsudek SDEU ze dne 8. dubna 2014, *Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources a další a Kärntner Landesregierung a další*, C-293/12 a -594/12.

provedení této směrnice v členských státech EU nebylo bezproblémové, což lze usuzovat i z uvedených rozhodnutí Ústavního soudu, dle kterých byla ustanovení zákonů vycházející ze směrnice zrušena pro neústavnost a následně byla nahrazena směrnicí EU 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací.[69]

Plošné shromažďování provozních a lokalizačních údajů zůstává i po změně právní úpravy sporným institutem. Údaje, které se pomocí data retention získávají, mohou poskytovat o osobě informace, dle kterých je možné zjistit mnohé o jejím chování, o tom, s kým osoba komunikuje a na jakých místech se vyskytuje a na základě těchto informací dochází k prodloužení digitální stopy jedince. Ochrana soukromí bude zajištěna pouze za podmínky, pokud budou data retention využívána pouze pro stanovené trestné činy a v praxi bude kontrolováno využívání těchto údajů a bude zabezpečena možnost zneužití shromážděných údajů.

2.4 Internetové sociální sítě

V této podkapitole se zaměřuji na problémy, které se vyskytují v souvislosti s ochranou soukromí na sociálních sítích, které se staly prostředkem komunikace každodenního života. Sociální sítě nám umožňují sdílet informace s lidmi prostřednictvím celé šíře internetu. Umožňují nám přímo komunikovat s lidmi, kteří skryti pod svými přezdívkami pro nás mohou být v podstatě anonymní, můžeme také bez problémů komunikovat s lidmi, kteří jsou od nás vzdáleni tisíce kilometrů. Život lze díky sociálním sítím přenést do virtuální reality na internetu. Tato volnost v komunikaci ale přináší z hlediska práva na soukromí řadu nevýhod.

Problémem sociálních sítí je fakt, že jejím prostřednictvím jsou neustále shromažďovány informace o soukromí osob a jejich osobních údajích. Otázkou je, zda společnosti přináší neustálé poskytování informací, příběhů a nálad převážný užitek v porovnání s tím, že prostřednictvím sociálních sítí je zároveň výrazným způsobem zasahováno do informačního sebeurčení jedinců.

Při pohledu na sociální sítě lze stále častěji pozorovat, že uživatelé internetu o sobě zveřejňují nepoměrné množství osobních informací vzhledem ke skutečnosti, že uživatelům chybí prostředky kontroly ochrany soukromí na internetu.[70] Ne každý si uvědomuje, že nese odpovědnost za veškeré informace, které o sobě na sociální síti zveřejní a že veškeré informace ve vztahu k němu mohou být zneužity. Než o sobě osoba informace prostřednictvím sociální sítě zveřejní, měla by se zamyslet nad tím, zda ji zveřejněná informace nemůže nějakým způsobem ohrozit.

[69] Rozhodnutí Rady 2002/58/ES ze dne 31. července 2002, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací. Úř. věst. L 201 ze dne 31. července 2002.
[70] MATEJKA, Ján. *Internet jako objekt práva*… s. 114-117.

Informace nebo videa či fotografie, které o sobě zveřejníme na sociálních sítích jako Facebook, Instagram, Twiter, MySpace nebo Google+, mohou být použity jinou osobou a například zveřejněny jinde na jiné internetové stránce. To může být považováno jako páchání trestné činnosti proti právům na ochranu osobnosti, soukromí a listovního tajemství.

Ústavní soud se k problematice sociálních sítí vyjádřil v nálezu ze dne 30. října 2014, sp. zn. II. ÚS 3844/13, kde definoval sociální síť Facebook jako komunikační síť sloužící k vytváření vztahů mezi osobami online, k šíření informací a jako síť, která nemá jednoznačně soukromou nebo veřejnou povahu. Bylo shledáno, že při získávání dat ze sociálních sítí se nelze bez dalšího odvolávat na veřejnou povahu informací zveřejněných na sociální síti Facebook. V této věci bylo proti stěžovateli vedeno trestní řízení za přečin ohrožování mravní výchovy mládeže. Bylo zjištěno, že stěžovatel na svém Facebook profilu veřejně sdílí dehonestující a zesměšňující informace o osobě činné v trestním řízení, která přečin projednávala. Následně osoby činné v trestním řízení stěžovateli za toto jednání uložili pořádkovou pokutu. Ústavní soud shledal za problematický způsob, jakým byly získány informace orgánem činným v trestním řízení z profilové stránky Facebook stěžovatele, na základě kterých mu byla uložena pokuta. Usnesení o pořádkové pokutě totiž neobsahovalo, jak a proč se stala data zveřejněná na profilu Facebook stěžovatele předmětem zkoumání policejního orgánu a nebylo ani uvedeno, jakým způsobem policejní orgán získal informace, na kterých založil rozhodnutí uložit stěžovateli pořádkovou pokutu. Uložení pořádkové pokuty bez uvedení těchto informací není v souladu s trestním řádem. Ústavní soud se vyjádřil dále k charakteru sociální sítě Facebook. Sociální síť Facebook je charakterem veřejné povahy v případě profilů, u kterých uživatelé usilují o co nejvyšší známost, ale na druhé straně má síť Facebook charakter soukromé povahy v případě, že uživatel využívá sociální síť jako soukromý komunikační kanál.[71] Nelze však získávat informace s ohledem k právu na informační sebeurčení v rozporu s trestním řádem, jako se stalo v uvedeném případě.[72]

Dle mého názoru do budoucna bude toto rozhodnutí velice užitečné, jelikož internetové sociální sítě se i v budoucnu budou zřejmě dále rozvíjet. Ujasnění, co lze považovat za soukromé informace a které informace jsou již považovány za veřejné, by mohlo vést k rozvoji povědomí uživatelů sociálních sítí z hlediska zveřejňování soukromých intimních informací osob na sociálních sítích a předcházet tak případným nedorozuměním.

Podobnou otázkou ohledně charakteru informací, které jsou zveřejněny na internetové sociální síti, se zabýval také kalifornský soud ve věci *Moreno proti společnosti Hanford Sentinel Inc.* Paní

[71] Nález Ústavního soudu ze dne 30. října 2014, sp. zn. III. ÚS 3844/13, body 39 – 43.
[72] SUCHOMELOVÁ, Helena. *Při zjišťování dat ze sociálních sítí se nelze bez dalšího odvolávat na jejich veřejnou povahu* [online]. Pravniprostor.cz, 15. ledna 2015 [cit. 2. října 2016]. Dostupné na <http://www.pravniprostor.cz/clanky/trestni-pravo/pri-zjistovani-dat-ze-socialnich-siti-se-nelze-bez-dalsiho-odvolavat-na-jejich-verejnou-povahu>.

Moreno zveřejnila na sociální síti MySpace článek, ve kterém byl vyjádřen její kritický postoj k městu, ve kterém se narodila. Článek byl následně uveřejněn v novinách a paní Moreno žalovala noviny za porušení práva na soukromí. Kalifornský soud se zabýval problémem, zda lze informaci zveřejněnou prostřednictvím sociální sítě považovat za soukromou, pokud původně bylo úmyslem zveřejnit informaci pouze určitému okruhu lidí. Soud rozhodl o tom, že se o soukromou povahu v tomto případě nejednalo, protože věc, která již byla jednou zveřejněna nebo se stala veřejnou, nadále nemůže být považována za věc soukromou.[73]

Myslím si, že v tomto rozhodnutí přistupuje soud k právu na ochranu soukromí až příliš restriktivním způsobem. Pokud by soudní praxe pokračovala tímto směrem, lze očekávat, že právu na soukromí bude poskytována čím dál menší ochrana, až dojde k jeho úplnému vymizení. Jelikož sociální síť MySpace je založena na podobných principech jako Facebook, měla by se dle mého názoru i ochrana soukromí na těchto sociálních sítích ubírat podobným směrem. V případě rozhodnutí kalifornského soudu se ale jedná o zcela odlišné stanovisko, než jaké uvedl v podobné věci soud český. Přikláním se spíše k názoru soudu českého, jelikož pokud je na profilu osoby zobrazen určitý příspěvek, jehož účelem je jeho zobrazení lidem ve stejné komunitě, neměl by se bez vědomí osoby dostat do média jiného. Jen tak lze realizovat právo na ochranu soukromí alespoň v určité míře.

[73] *Moreno v. Hanford Sentinel, Inc.* ze dne 4. dubna 2009, 172 Cal. App. 4th 1125.

3 Kamerové systémy a právo na informační sebeurčení

3.1 Charakter kamerových systémů

V této kapitole se zaměřuji na vztah kamerových systémů a informačního sebeurčení jedince. Kamerové systémy jsou systémy sledování osob, věcí nebo situací. V poslední dekádě dochází k významnému rozvoji kamerových systémů a je běžné provozovat kamerové systémy na nejrůznějších místech. Kamerové systémy rozlišujeme na kamerové systémy se záznamem a kamerové systémy bez záznamu, které jsou nejčastěji provozované online. Za předpokladu, že je kamerový systém vybaven záznamem, považuje se provozování takového kamerového systému za zpracování osobních údajů. V ČR ale dosud není problematika provozování kamerových systémů se záznamem upravena zvláštním zákonem. Provozování kamerových systémů se záznamem tedy podléhá právní úpravě zákona o ochraně osobních údajů a při zpracování osobních údajů musí být dodržena ustanovení tohoto zákona. Ke zpracování osobních údajů dochází v situacích, kdy kamerovým systémem je zároveň prováděn obrazový či zvukový záznam za účelem pozdější identifikace zaznamenaných osob.[74]

Mezi základní povinnosti provozování kamerového systému se záznamem patří povinnost před tím, než dojde ke zpracování osobních údajů, oznámit provozování kamerového systému Úřadu pro ochranu osobních údajů, další povinností je registrace tohoto zařízení dle ustanovení § 16 odst. 1 zákona o ochraně osobních údajů. Oznamovací a registrační povinnost k Úřadu pro ochranu osobních údajů se nevztahuje na provozování kamerového systému se záznamem, který je prováděn pouze pro osobní potřebu. Také se nevztahuje na kamerové systémy bez záznamu, protože takové kamerové systémy nejsou považovány za zpracování osobních údajů.[75]

Zpracování osobních údajů prostřednictvím kamerových záznamů je možné provádět pouze za splnění dalších povinností, které jsou uvedeny v § 16 zákona o ochraně osobních údajů. Mezi takové povinnosti patří zejména uvést veškeré zákonem vyžadované informace v oznámení o provozování kamerového systému k Úřadu pro ochranu osobních údajů. Mezi ně patří zejména identifikace správce osobních údajů, stanovení účelu zpracování osobních údajů, popis způsobu zpracování osobních údajů, nebo místo zpracování osobních údajů.

---

[74] JANEČKOVÁ, Eva, BÁRTÍK, Václav. *Kamerové systémy v praxi: právní režim z pohledu ochrany osobních údajů a ochrany osobnosti.* 1. vydání. Praha: Linde, 2011, s. 19.

[75] *Provozování kamerových systémů: Metodika pro splnění základních povinností ukládaných zákonem o ochraně osobních údajů* [online]. uoou.cz, [cit. 2. října 2016]. Dostupné na <https://www.uoou.cz/files/metodika_provozovani_kamerovych_systemu.pdf>.

Zpracování osobních údajů prostřednictvím kamerového systému se záznamem může být odůvodněno účelem plnění povinností na základě ustanovení zvláštních zákonů, jako jsou zákon o Policii ČR, o obecní policii,[76] o ochraně utajovaných informací a bezpečnostní způsobilosti,[77] o Bezpečnostní informační službě,[78] o Vězeňské službě[79] a dalších. Zpracování osobních údajů provádí správce, který je vymezen v § 4 písm. j) zákona o ochraně osobních údajů jako *„každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak."* Zpracovávat osobních údaje je možné na základě poskytnutí souhlasu subjektu údajů, je ale zároveň nutné vymezit okruh osob, které jsou kamerovým systémem se záznamem monitorovány.[80] Zpracovávat osobní údaje prostřednictvím kamerových systémů se záznamem bez souhlasu subjektu údajů je možné v situaci podle § 5 odst. 2 zákona o ochraně osobních údajů, zejména pro ochrana života a zdraví osob, ochranu bezpečnosti a ochrana majetku. Kamerovými systémy lze zpracovávat osobní údaje pouze za předpokladu, že stanoveného účelu nelze dosáhnout jiným způsobem. Současně provozování kamerového systému nesmí nepřiměřeně zasahovat do práva na soukromí osob, které jsou monitorovány.[81]

Při zpracování osobních údajů musí být dodržována lhůta, po kterou mohou být záznamy kamerových systémů uchovány. Lhůta pro zpracování osobních údajů je stanovena jako doba nezbytná ke zpracování osobních údajů. Taková lhůta je dlouhá maximálně několik dní. Pokud vznikne spor ohledně toho, zda byla v konkrétním případě lhůta nepřiměřená, je přiměřenost lhůty předmětem posouzení Úřadu pro ochranu osobních údajů. Další podmínkou pro provozování kamerového systému se záznamem je informativní označení monitorovaného prostoru. Takové označení bývá prováděno nejčastěji umístěním tabulky, na které je vyobrazena kamera a na které je napsané například *„tento prostor je monitorován kamerovým systémem"*. Označení monitorovaného prostoru musí být umístěno na viditelném místě a zároveň před vstupem do tohoto prostoru.[82]

Dle mého názoru tímto způsobem označení není dostatečně splněna informativní povinnost o monitorování prostoru, ale v praxi je tento způsob označení běžný. Informativní tabulka totiž obsahuje údaj pouze o tom, že prostor je monitorovaný, neposkytuje další důležité

---

[76] Zákon č. 553/1991 Sb., o obecní policii, ve znění pozdějších předpisů.
[77] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.
[78] Zákon č. 154/1994 Sb., o Bezpečnostní informační službě, ve znění pozdějších předpisů.
[79] Zákon č. 555/1992 Sb., o Vězeňské službě a justiční stráži České republiky, ve znění pozdějších předpisů.
[80] Stanovisko č. 1/2006 Úřadu pro ochranu osobních údajů – provozování kamerového systému z hlediska zákona o ochraně osobních údajů (leden 2006).
[81] JANEČKOVÁ, Eva, BÁRTÍK, Václav. *Kamerové systémy v praxi* …, s. 11.
[82] *Provozování kamerových systémů: Metodika pro splnění základních povinností ukládaných zákonem o ochraně osobních údajů* [online]. uoou.cz, [cit. 2. října 2016]. Dostupné na <https://www.uoou.cz/files/metodika_provozovani_kamerovych_systemu.pdf>.

informace - za jakým účelem je prostor monitorován, jaká je lhůta uchování záznamů, nebo jak bude správce osobních údajů údaje zpracovávat. Nápravou tohoto problému by mohlo být alespoň doplnění informace do informativní tabulky o tom, kdo je správce kamerového systému a kde je možné dohledat uvedené informace o provozování kamerového systému.

Otázkou související s kamerovými systémy je, zda je možné použít záznamy z kamerového systému jako důkaz v řízení správním nebo trestním. Obecným východiskem je, že lze použít jen takové záběry, na základě kterých je možné identifikovat osobu, proti které je řízení vedeno. Záznam z kamerového systému tedy musí mít určitou kvalitu zaznamenaných údajů.[83] V rozhodnutí Ústavního soudu ze dne 8. února 2010, sp. zn. IV. ÚS 2425/09 byla řešena situace, kdy provozovatel kamerového systému zpracovával osobní údaje získané z kamerového systému se záznamem a nesplnil povinnost registrace kamerového systému u Úřadu pro ochranu osobních údajů. Přesto Ústavní soud judikoval, že záznamy z kamerového systému nejsou absolutně neplatným důkazním prostředkem pro trestní nebo správní řízení.[84]

Veřejný ochránce práv se k tomuto problému také vyjádřil a vydal stanovisko, ve kterém doplňuje, že je přípustné používat záznamy ze soukromých kamerových systémů jako důkaz v přestupkových sporech, pokud byl záznam pořízen jednou stranou sporu. Použití takového záznamu sice představuje zásah do práva na ochranu soukromí, ale je odůvodněn zájmem nezbytné ochrany práva na obhajobu strany sporu, která chce záznam v řízení použít. V každém individuálním případě je ale nutné posoudit, zda převažuje požadavek na řádné projednání věci nad právem na informační sebeurčení jedince. Veřejný ochránce práv uvedl, že v případě správního řízení se bude primárně postupovat podle ustanovení § 5 odst. 2 písm. e) zákona o ochraně osobních údajů. Toto ustanovení představuje jednu z výjimek z povinnosti souhlasu subjektu údajů se zpracováním osobních údajů.[85]

Tento názor je podpořen i rozhodnutím Nejvyššího správního soudu, sp. zn. 1 As 113/2012-133, dle kterého záznam kamerového systému, který obsahuje faktické informace o trestném činu, může provozovatel kamerového systému předat orgánům činným v trestním řízení. Použití kamerového záznamu bez souhlasu zaznamenané osoby pro účely trestního řízení zmocňuje ustanovení § 89 odst. 2 trestního řádu, dle kterého *„za důkaz může sloužit vše, co může přispět k objasnění věci“*[86].

---

[83] *Provozování kamerových systémů: Metodika pro splnění základních povinností ukládaných zákonem o ochraně osobních údajů* [online]. uoou.cz, [cit. 28. října 2016]. Dostupné na <https://www.uoou.cz/files/metodika_provozovani_kamerovych_systemu.pdf>.

[84] Usnesení Ústavního soudu ze dne 8. února 2010, sp. zn. IV. ÚS 2425/09.

[85] MOTEJL, Otakar. *Závěrečné stanovisko ve věci podnětu Mgr. E. a L., H.* [online]. ochrance.cz, 22. dubna 2010 [cit. 28. října 2016]. Dostupné na <http://www.ochrance.cz/fileadmin/user_upload/STANOVISKA/Prestupky/5432-09-IK-ZSO.pdf>.

[86] Usnesení Nejvyššího správního soudu ze dne 25. února 2015, sp. zn. 1 As 113/2012-133.

Otázka použitelnosti záznamů z kamerového systému v řízení správním a trestním i bez registrace takového systému se zdá být jako kontroverzní. Tato situace by mohla vést k nárůstu počtu provozovaných kamerových systémů, které nebudou u Úřadu pro ochranu osobních údajů registrovány. Myslím si, že by se registrace kamerových systémů mohla v důsledku tohoto stát v budoucnu do jisté míry bezpředmětnou.

3.2 Umístění kamerových systémů

3.2.1 Úvod do umístění kamerových systémů

Kamerové systémy lze dělit kromě kamerových systémů se záznamem nebo kamerových systémů bez záznamu také podle toho, na jakém místě se nacházejí. Podle umístění kamerových systémů je možné určit specifické legitimní cíle, které odůvodňují umístění jednotlivých kamerových systémů. Účelem umístění těchto systémů je sledování problematických prostor. Podle prostoru umístění kamerových systémů podléhají kamerové systémy právní úpravě dalších zákonů, které jsou ve vztahu k zákonu o ochraně osobních údajů právní úpravou subsidiární.

V dnešní době je téměř celý prostor, kde se setkávají lidé monitorovaný, právo na informační sebeurčení může být zasaženo na jakémkoli místě, kde se osoba nachází. V této části představím kamerové systémy se záznamem umístěné na veřejných prostranstvích, na místech veřejně přístupných, kamerové systémy sloužící soukromým účelům, kamerové systémy umístěné ve školních institucích, kamerové systémy umístěné na pracovišti a jejich vztah k právu na informační sebeurčení. Dále představím problematiku Google Street View provozovaného v ČR.

3.2.2 Kamerové systémy na veřejných prostranstvích

Veřejná prostranství jsou místa, která jsou určená k obecnému užívání podle ustanovení § 34 zákona o obcích.[87] Jsou to *„všechna náměstí, ulice, tržiště, chodníky, veřejná zeleň, parky a další prostory přístupné každému bez omezení, tedy sloužící obecnému užívání, a to bez ohledu na vlastnictví k tomuto prostoru“.*

Dohled nad místy veřejného prostranství je prováděn takzvaným obecním dohlížecím kamerovým systémem. Takový systém je provozovaný obecní policií, kterou zřizuje obec v rámci samostatné působnosti a obec je v tomto případě správcem osobních údajů při zpracování osobních údajů. Pokud obec nemá zřízenou obecní policii, nemůže tento druh kamerového systému provozovat. Kamerové systémy monitorující veřejná prostranství představují nejméně

[87] Zákon č. 128/2000 Sb., o obcích, ve znění pozdějších předpisů.

invazivní zásah do práva na informační sebeurčení ze všech typů umístění kamerových systémů se záznamem. Je tomu z důvodu, že při monitorování veřejného prostranství převažuje zájem veřejné bezpečnosti osob nad jejich soukromím, což je snad i pochopitelné a všeobecně akceptovatelné. Obecní policie je nadána zákonnou licencí, na základě které není třeba přechozího souhlasu osoby s pořízením záběrů.[88] Oprávnění obecní policie provozovat kamerové systémy je upraveno v ustanovení § 24a zákona o obecní policii, na základě kterého je obecní policie oprávněna zpracovávat osobní údaje, které potřebuje k plnění svých úkolů. Dle § 24b zákona o obecní policii je obecní policie oprávněna *„je-li to potřebné pro plnění jejích úkolů podle tohoto nebo jiného zákona, pořizovat zvukové, obrazové nebo jiné záznamy z míst veřejně přístupných, popřípadě též zvukové, obrazové nebo jiné záznamy o průběhu zákroku nebo úkonu"*. Zároveň je ale povinností obecní policie provozovat kamerové systémy tak, aby monitorovaly pouze veřejná prostranství a nemonitorovaly prostory, které nemají veřejný charakter.[89]

Problematikou sledování osob kamerovými systémy umístěnými na veřejných prostranstvích se zabýval ESLP ve věci *Peck proti Spojenému Království*. Z rozhodnutí vyplývá, že sledování osob na veřejném místě prostřednictvím zařízení, které zaznamenává pouze obrazová data, nemůže být zásahem do práva na soukromí dle čl. 8 Úmluvy. Zásahem do tohoto práva by bylo až zveřejnění záznamu ze zařízení široké veřejnosti.[90] Toto rozhodnutí je dle mého názoru dalším příkladem stále se zvětšující možnosti omezení práva na soukromí, které je prováděno v souladu se zákonem a je tedy legitimní a oprávněné.

3.2.3 Kamerové systémy na místech veřejně přístupných

Pod pojmem místa veřejně přístupná si můžeme představit místa kulturního, společenského nebo sportovního setkávání. Jsou to například divadla, kina, sportoviště, restaurace nebo obchody. Na veřejně přístupných místech osoby očekávají alespoň takovou míru soukromí, která odpovídá určitému charakteru konkrétního místa.[91] Pojmem místo veřejně přístupné se zabýval NS v usnesení ze dne 15. března 2012, sp. zn. 8 Tdo 682/2009, ve kterém uvedl, že *„místem veřejnosti přístupným je takové místo, kam má přístup široký okruh lidí individuálně neurčených a kde se také zpravidla více lidí zdržuje…"*[92]

Pro monitorování míst veřejně přístupných kamerovým systémem neexistuje v ČR speciální právní úprava, provoz kamerových systémů tedy podléhá plně ustanovením zákona

[88] JANEČKOVÁ, Eva, BÁRTÍK, Václav. *Kamerové systémy v praxi:*…, s. 129-130.
[89] JANEČKOVÁ, BÁRTÍK. *Kamerové systémy v praxi*…, s. 47-49.
[90] Rozsudek ESLP ve věci *Peck proti Spojenému Království* ze dne 28. ledna 2003, stížnost č. 44647/98, bod 59.
[91] JANEČKOVÁ, BÁRTÍK. *Kamerové systémy v praxi*…, s. 118.
[92] Rozsudek Nejvyššího soudu ze dne 8. prosince 2009, sp. zn. 8 Tdo 682/2009.

o ochraně osobních údajů, zejména ustanovení § 5 odst. 2 písm. e) zákona o ochraně osobních údajů, který představuje výjimku z udělení souhlasu se zpracováním osobních údajů z důvodu nezbytnosti pro ochranu práv a zájmů. Účelem provozování kamerových systémů je nejčastěji sledování prostor za účelem ochrany bezpečnosti osob a ochrany majetku.[93]

Pří monitorování veřejně přístupných míst platí stejná zásada jako při monitorování veřejných prostranství, tedy, že kamery mohou být umístěny takovým způsobem, aby sledovaly pouze prostor odůvodňující potřebu sledování. Ze sledování prostor veřejně přístupných jsou tak vyloučena místa, na kterých náleží každé osobě nutná míra soukromí. Jedná se zejména o toalety, šatny nebo diskrétní zóny před pokladnami v obchodech.[94] Zároveň musí být zohledněno, že sledované prostory mohou být i pracovištěm pro personál obsluhující místa veřejně přístupná, kamerové systémy musí být tedy umístěny v souladu s ustanovením § 316 odst. 2 zákoníku práce.[95] Umístění kamer na pracovišti se budu věnovat v této kapitole dále.

Otázkou monitorování míst veřejně přístupných se zabýval i NSS ve věci, kdy se dostalo do kolize právo na ochranu soukromí a právo na ochranu majetku. V rozhodnutí NSS ze dne 28. června 2013, sp. zn. 5 As 1/2011-156, byla přiznána právu na soukromí větší ochrana než právu na ochranu majetku a to z toho důvodu, že kamerové systémy monitorovaly i soukromé prostory hotelu, monitorování těchto prostor tedy nesplňovalo předem stanovený účel ochrany majetku. Sledováním soukromých prostor bylo porušeno také ustanovení zákona o ochraně osobních údajů upravující nezbytnou délku doby uchování záznamu, kdy doba uchování záznamu činila 7 dní, což byla doba vzhledem k vymezenému účelu nepřiměřeně dlouhá. Soud potvrdil, že za přiměřenou dobou uchování kamerových záznamů je ve většině případů třeba považovat 3 dny.[96]

3.2.4 Kamerové systémy sloužící soukromým účelům

Kamerové systémy sloužící k soukromým účelům jsou kamerové systémy umisťované nejčastěji v lidských obydlích. Účelem provozování těchto kamerových systémů je především ochrana vlastnictví. V prostorách okolo domu jeho obyvatelé očekávají jistou míru soukromí, byť ne tak vysokou jako v samotném bytě nebo domě. Právo na ochranu soukromí se vztahuje i na prostory okolo domů a bytů. To vyplývá z rozhodnutí Městského soudu v Brně sp. zn. 7 Ca 204/2005-49, ve kterém je uvedeno, že *„i prostory mimo obydlí se považují za soukromé prostory“*[97].

[93] JANEČKOVÁ, BÁRTÍK. *Kamerové systémy v praxi*…, s. 126.
[94] JANEČKOVÁ, BÁRTÍK. *Kamerové systémy v praxi*…, s. 118-119.
[95] Zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů.
[96] Rozsudek Nejvyššího správního soudu ze dne 28. června 2013, sp. zn. 5 As 1/2011-156.
[97] Rozsudek Městského soudu v Praze ze dne 28. února 2007, sp. zn. 7 Ca 204/2005-49.

S právní úpravou kamerových systémů v soukromých prostorech souvisí ustanovení § 1013 občanského zákoníku, ve kterém je stanoveno, že vlastník jednoho pozemku se má zdržet všeho, co v nepřiměřené míře místním poměrům vniká na sousední pozemek a podstatně omezuje obvyklé užívání sousedního pozemku. Mezi toto jednání lze zahrnout i instalaci kamery vlastníka pozemku takovým způsobem, že monitoruje i sousední pozemek. Pokud je tímto jednáním závažným způsobem, což je zejména neustálé nahlížení do sousední nemovitosti, narušeno soukromí vlastníka sousedního pozemku, jedná se o takzvané *„obtěžování pohledem"*, a toto jednání je dle rozhodnutí NS ze dne 15. března 2012, sp. zn. 22 Cdo 1150/99, protiprávní.[98]

S otázkou monitorování soukromých prostor souvisí i otázka charakteru prostor uvnitř bytového domu. Prostory uvnitř bytového domu se dají rozdělit na dva typy. Prvním typem jsou prostory, které neslouží k soukromému obývání osob. Jsou to sklepy, půdy, kolárny nebo prostory u schránek. Na umístění kamerových systémů do těchto prostor lze aplikovat ustanovení § 5 odst. 2 písm. e) zákona o ochraně osobních údajů, tedy výjimku z poskytování souhlasu se zpracováním osobních údajů. Druhým typem prostorů jsou takové, které se soukromým životem obyvatel bytového domu souvisí. Jde například o výtah, chodby nebo schodiště. Monitorováním takových prostor může dojít k zásahu do soukromí monitorovaných osob, a to například v případě obrazového monitorování návštěv nebo zaznamenávání času odchodu osob z bytu.[99] Aby byly kamerové systémy v takových prostorách provozovány v souladu se zákonem, je nutný předchozí souhlas se zpracováním osobních údajů od všech osob, které v bytovém domě bydlí. Tyto prostory nelze zařadit pod prostory, kde lze uplatnit výjimku neposkytnutí souhlasu jako v předchozím případě, což bylo potvrzeno i rozhodnutím Městského soudu v Praze ze dne 28. února 2007, sp. zn. 7 Ca 204/2005-49.[100]

3.2.5 Kamerové systémy umístěné ve školních institucích

Monitorování prostor ve školních institucích bývá odůvodněno ochranou majetku a zajištěním veřejné bezpečnosti studentů a zaměstnanců těchto institucí. Možnost použít kamerové systémy ve školském zařízení vyplývá z ustanovení školského zákona,[101] zejména jde o ustanovení § 29 odst. 2 školského zákona, které stanoví, že školy mají povinnost zajistit bezpečnost a ochranu zdraví osob při jejich vzdělávání a poskytují takovým osobám nezbytné informace k zajištění bezpečnosti a ochrany zdraví. Ke splnění této povinnosti školní institucí lze využít kamerové

[98] Usnesení Nejvyššího soudu ze dne 15. března 2012, sp. zn. 22 Cdo 1150/99.
[99] JANEČKOVÁ, BÁRTÍK. *Kamerové systémy v praxi*…, s. 79-83.
[100] Rozsudek Městského soudu v Praze ze dne 28. února 2007, sp. zn. 7 Ca 204/2005-49.
[101] Zákon č. 561/2004 Sb., o předškolním, základním, středním a vyšším odborném vzdělávání (školský zákon), ve znění pozdějších předpisů.

systémy, jejichž použití musí být uvedeno ve školním řádu dle § 30 odst. 1 písm. c) školského zákona.

Otázkou, zda je kamerový systém umístěny na chodbách školy provozován v souladu se zákonem, řešil Městský soud v Praze v rozhodnutí ze dne 23. března 2012, sp. zn. 11 Ca 298/2008-47. Kamerový systém se záznamem umístěný na chodbách školy monitoroval i byt školníka nacházející se v těchto místech. K umístění kamerového systému na chodby školy došlo kvůli krádežím v prostorách školy a také na základě faktu, že škola byla zpřístupněná i mimo dobu výuky k soukromým aktivitám. O umístění kamer byli zaměstnanci školy i žáci informováni. Kamerový systém ale nebyl registrován, takže byl provozován v rozporu se zákonem. Dalším problémem bylo, že kamerový systém snímal prostory po celý den, což bylo vyhodnoceno Městským soudem v Praze jako nepřiměřený zásah do soukromí, a zároveň soud vyjádřil, že ke sledovanému účelu, který byl stanoven jako ochrana života a zdraví studentů a zaměstnanců a ochrana majetku, by postačilo monitorování prostor v době, kdy se ve škole nenacházejí žádné osoby.[102]

S tímto závěrem lze souhlasit. Ochrana majetku, který byl stanoven jako účel provozování kamerového systému, by měl být zabezpečován zejména v době, kdy neprobíhá vyučovací činnost, protože si myslím, že při vyučování je ohrožení zcizení majetku minimální.

Do informačního sebeurčení osob bylo neoprávněně zasaženo z důvodu, že zaměstnanci školy i žáci školy byli sice o provozování kamerového systému informováni, nikde nebylo ale uvedeno, v jakém rozsahu a za jakým účelem budou osobní údaje zpracovány, kdo je bude zpracovávat a jakým způsobem a komu mohou být zpřístupněny. Za toto jednání byla uložena správci osobních údajů pokuta Úřadem pro ochranu osobních údajů a soud potvrdil, že byla uložena oprávněně. [103]

Toto rozhodnutí soudu uvádím jako příklad, že kamerové systémy se záznamem jsou mnohdy provozovány, i přestože nebyly registrovány u Úřadu pro ochranu osobních údajů, což stanoví zákon jako povinnost. Jelikož není nikde vymezena povinnost Úřadu pro ochranu osobních údajů aktivně odhalovat tyto systémy provozované bez registrace, nelze ani dost dobře vytvořit přehled takových systémů.

S tématem monitorování prostor ve školských zařízeních souvisí také otázka, v jaké míře má dítě právo na soukromí a zda existuje rozdíl v tom, v jaké míře do tohoto práva může být zasahováno ve srovnání se soukromím dospělé osoby. Dle čl. 16 Úmluvy o právech dítěte[104] musí respektovat právo na soukromí dítěte všichni, včetně jeho zákonných zástupců. Není nikde vymezeno, že dítě má menší míru práva na ochranu soukromí, tudíž lze dovodit, že dítě má právo

[102] Rozsudek Městského soudu v Praze ze dne 23. března 2012, sp. zn. 11 Ca 298/2008-47.
[103] Rozsudek Městského soudu v Praze ze dne 23. března 2012, sp. zn. 11 Ca 298/2008-47.
[104] Sdělení federálního ministerstva zahraničí č. 104/1991 Sb., o sjednání Úmluvy o právech dítěte.

na ochranu soukromí včetně ochrany osobních údajů ve stejné míře jako dospělá osoba a nelze tedy slevit z požadavku ochrany práva na soukromí v jakékoli podobě. Proto i mezi podmínky provozování kamerového systému ve školském zařízení patří seznámení studentů s jejich provozem. Úřad pro ochranu osobních údajů je toho názoru, že děti, které jsou starší 15 let, jsou natolik rozumově a mravně vyspělé, aby byly schopny posoudit, zda chtějí udělit souhlas se zpracováním osobních údajů. U dětí mladších 15 let udělují souhlas se zpracováním osobních údajů jejich zákonní zástupci.[105]

3.2.6 Kamerové systémy umístěné na pracovišti

Kamerové systémy umístěné na pracovišti mají zřejmě opodstatnění v možnosti kontroly efektivity vykonávané práce zaměstnance, nebo v ochraně majetku, který je zaměstnanci k výkonu zaměstnání svěřen. Při provozu kamerových systémů umístěných na pracovišti musí osoba provozující toto zařízení postupovat v souladu s ustanovením § 316 odst. 3 zákoníku práce,[106] který stanoví základní pravidlo, dle kterého při monitorování kamerovými systémy nesmí zaměstnance zaměstnavatel podrobovat sledování bez předchozího informování o způsobu a rozsahu monitorování a také nesmí zaměstnance podrobovat sledování bez závažného důvodu. Zároveň je zaměstnavatel povinen se zdržet skrytého monitorování zaměstnanců a nadměrného narušování soukromí sledováním zaměstnanců. Zaměstnavatel musí zároveň při provozování kamerového systému plnit všechny povinnosti stanovené podle zákona o ochraně osobních údajů.[107]

Uvedený postup zaměstnavatel musí dodržovat z důvodu, že zaměstnanec tráví na pracovišti nezanedbatelný čas a i na pracovišti má právo na ochranu soukromí. Právem na soukromí v souvislosti s kamerovými systémy umístěnými na pracovišti se zabýval ESLP ve věci *Niemietz proti Německu*. V této věci bylo namítáno stěžovatelem Niemietzem, že při prohlídce jeho pracoviště – advokátní kanceláře, bylo porušeno jeho právo na soukromí dle čl. 8 Úmluvy z důvodu, že byla provedena prohlídka jeho advokátní kanceláře orgány činnými v trestním řízení za účelem nalezení důkazů pro trestní řízení bez jakéhokoli omezení a byla odůvodněna pouze tím, že je advokát podezřelý na základě určitých domněnek, nikoli na základě faktů, ze spáchání trestné činnosti. Prohlídka jeho kanceláře ale nepřinesla v důsledku pro trestní stíhání žádné výsledky. ESPL dovodil, že ochrana práva na soukromí se vztahuje i na místa, ve kterých je vykonáváno zaměstnání. Dále soud uvedl, že ochrana práva na soukromí by se měla vztahovat i na vytváření vztahů s dalšími osobami z důvodu, že rozvoj vztahů s dalšími osobami mnohdy souvisí

[105] JANEČKOVÁ, BÁRTÍK. *Kamerové systémy v praxi*…, s. 112-115.
[106] Zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů.
[107] JANEČKOVÁ, BÁRTÍK. *Kamerové systémy v praxi*…, s. 63-66.

s pracovním procesem. Pokud by došlo k nezákonnému narušení těchto chráněných vztahů třetí osobou, došlo by i k porušení čl. 8 Úmluvy.[108]

Vliv rozhodnutí ve věci *Niemietz proti Německu* lze najít i v rozhodování Ústavního soudu v rozhodnutí ze dne 1. března 2000, sp. zn. II. ÚS 517/99, ve kterém je uvedeno, že právo na soukromí zahrnuje v určité míře i právo na vytváření vztahů s jinými lidmi a že povinností státu je zajistit, aby takové vztahy mohly osoby mezi sebou rozvíjet.[109]

Dle mého názoru se jedná o naprosto vhodnou myšlenku. Je potřeba poskytnout ochranu soukromí i vztahům osob v pracovním procesu. Člověk jako bytost žijící ve společnosti takovou ochranu potřebuje i v oblasti pracovních vztahů, protože v rámci pracovního procesu většinou rozvíjí vztahy s ostatními lidmi. Na druhou stranu je ale pochopitelné, že umístění kamerových systémů na pracoviště zlepšuje dodržování pracovní morálky.

3.2.7 Google Street View

S problematikou kamerových systémů a práva na informační sebeurčení souvisí i fenomén Google Street View. Google Street View představuje službu dostupnou na webové stránce www.google.com/streetview/, jejímž prostřednictvím lze virtuálně prohlížet oblasti na mapách, které byly zmonitorovány pomocí speciálně upravených aut s kamerovým systémem. Prohlížet lze pohledy s rozsahem 360° horizontálním pohledem a 290°vertikálním pohledem, na kterých je vidět pohled zachycený z komunikací. Google Street View je série fotografií, které jsou snímány auty s kamerovým systémem po zhruba 10 metrech a které jsou spojeny do jednoho celku. Google Street View funguje v ČR od 7. října 2009.[110]

Provoz služby Google Street View v ČR byl zpočátku spojen s několika problémy, které souvisejí s ochranou práva na soukromí osob. Jedním z problémů bylo uložení dočasného pozastavení pořizování snímků Google Street View Úřadem pro ochranu osobních údajů z důvodu, že snímací tyč na automobilu, na které byla umístěna kamera, byla umístěna ve výšce 2, 7 metru, takže často snímala oblasti ve výšce oken obydlí a tím pádem na snímcích byly zobrazeny interiéry lidských obydlí. Monitorováním tímto způsobem docházelo podle Úřadu pro ochranu osobních údajů k nadměrnému zásahu do práva na soukromí a důsledkem byl zákaz zpracovávat prostřednictvím služby Google Street View osobní údaje, což souviselo s nepovolením registrace kamerových systémů. Tento zákaz platil od 2. září 2010 do 23. května 2011. Výška, ze které jsou snímky pořizovány dnes, byla společností jako následek rozhodnutí snížena na výšku

[108] Rozsudek ESLP ve věci *Niemietz proti Německu* ze dne 16. prosince 1992, stížnost č. 13710/88, § 29.
[109] Usnesení Ústavního soudu ze dne 1. března 2000, sp. zn. II. ÚS 517/99.
[110] *Co je street view.* [online]. streetview.cz, [cit. 27. října 2016] Dostupné na <http://www.streetview.cz/>.

2, 3 – 2, 4 metru, což bylo v souladu s požadavkem Úřadu pro ochranu osobních údajů.[111] Na základě splnění uvedeného požadavku proběhla dne 23. května 2011 registrace služby Google Street View u Úřadu pro ochranu osobních údajů. Mezi další požadavky, na základě jejichž splnění bylo vydáno rozhodnutí o registraci kamerových systémů služby Google Street View, dále patřilo jmenování správce osobních údajů, kterým se stala společnost Google Ireland Ltd. Dále byla stanovena povinnost předem informovat o tom, že bude provedeno snímání určitého území, a byly vytvořeny zásady týkajících se práva na soukromí. Ty jsou dostupné na webových stránkách https://www.google.com/streetview/privacy/.[112]

Služba Google Street View deklaruje v uvedených zásadách ochranu soukromí snímaných osob také prohlášením, že na základě jimi vyvinuté technologie dochází po pořízení snímků automaticky k rozmazávání obličejů osob a státních poznávacích značek na automobilech, čímž mají být osoby a státní registrační značky neidentifikovatelné. Dále společnost Google Inc. dává každému v rámci těchto zásad možnost požádat o rozmazání snímků zobrazujících jejich obydlí, státní registrační značky nebo jiné oblasti, jejichž zobrazení zasahuje do jejich práva na soukromí.[113] To je dobrým krokem k tomu, aby se každý mohl aktivně domoci ochrany svého soukromí.

Provozování služby Google Street View je u Úřadu pro ochranu osobních údajů řádně registrováno a probíhá v souladu se zákonem o ochraně osobních údajů. Jak je ale odůvodněn účel provozování této služby? Domnívám se, že provozování této služby nelze zdůvodnit účelem ochrany zdraví, majetku nebo např. veřejného pořádku. Důvodem, proč lze na základě tohoto systému zpracovávat osobní údaje je tedy zřejmě celkový technologický vývoj společnosti, která vyžaduje prohlížení reálných fotografií a zároveň na úkor tohoto nechá zasáhnout do svého soukromí. Pokud je opravdu důsledně dodrženo rozmazávání obličejů osob, které jsou na snímku zobrazeny, nemělo by být možné zobrazenou osobu identifikovat a tím pádem by nemělo docházet ani ke zpracování osobních údajů.

I přesto služba představuje dle mého názoru celkem zřejmý zásah do práva na informační sebeurčení. Otázkou je, zda by služba obstála v testu proporcionality? Při provozování služby se dostávají do kolize právo na informace a právo na soukromí. Při aplikaci testu proporcionality by bylo nejprve zjišťováno, zda je služba Google Street View způsobilá dosáhnout určitého cíle. Cílem by bylo pravděpodobně šíření informací o určitých místech prostřednictvím jejich zobrazení. Můžeme konstatovat, že uvedeného cíle tímto prostředkem dosáhnout lze. Dalším krokem testu

---

[111] ZANDL, Patrik. *Google může opět snímkovat pro StreetView. Kde byl problém?* [online]. lupa.cz, 27. května 2011 [cit. 5. října 2016]. Dostupné na <http://www.lupa.cz/clanky/google-muze-opet-snimkovat-pro-streetview-kde-byl-problem/>.

[112] ŠTĚPÁNSKÁ, Hana. *Tisková zpráva.* [online]. uoou.cz, 23. května 2011 [cit. 12. října 2016]. Dostupné na <https://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=3105&n=tiskove%2Dzpravy%2D2011>.

[113] *Zásady přijímání snímků a ochrany soukromí.* [online]. google.com, [cit. 27. října 2016]. Dostupné na <https://www.google.com/streetview/privacy/#privacy-and-blurring>.

by byla otázka potřebnosti tohoto prostředku. Lze dosáhnout stanoveného cíle jinými prostředky? Zde bych se přikláněla k negativní odpovědi, protože k naplnění stanoveného cíle si neumím představit jiný prostředek. Dostáváme se k aplikaci třetího kroku testu, v němž by došlo k porovnání dvou práv stojících v kolizi. Přikláněla bych se spíše k tomu názoru, že u provozování služby Google Street View převažuje zásah do soukromí nad právem na informace. Provozováním služby dochází k oslabení práva na soukromí nedobrovolným snímáním osob, které jsou následně prostřednictvím této služby zobrazeny. Zásah do soukromí umocňuje právní rámec provozování této služby, který neposkytuje mnoho prostředků k ochraně soukromí.

Vzhledem k tomu, do jaké míry mohou kamerové systémy zasáhnout do soukromí, považuji za alarmující současný stav právní úpravy této technologie. Kamerové systémy by si zasloužily úpravu samostatným zákonem, který by současně zohledňoval problematiku umístění těchto systémů ve specifických prostorech a sjednotil tak právní úpravu, která je v současnosti roztroušena do mnoha zákonů.

Nová právní úprava by byla vhodná i z hlediska stále se nově objevujících kontroverzí v této oblasti. Podobná služba jako Google Street View byla zavedena na internetovém serveru www.mapy.cz. V poslední době je diskutovaným tématem např. provozování dronů, bezpilotních letadel s kamerovým systémem. I tyto přístroje jsou schopné zasáhnout do práva na soukromí, když přelétávají nad soukromými pozemky a pořizují snímky ze soukromí osob bez jejich souhlasu. Stále častěji si totiž přístroje pořizují osoby pro soukromé účely. Při provozu přístrojů existuje kromě možnosti zasáhnout do soukromí i možnost provozem někoho zranit nebo dokonce možnost střetu dronu s vrtulníkem nebo letadlem. Přístrojů, na kterých budou kamery umisťovány, bude jistě s přibývající dobou více, nová právní úprava, která by zohlednila celkovou problematiku, by tedy byla velice vhodná.

4 Analýza DNA a právo na informační sebeurčení

4.1 Právní úprava analýzy DNA

Analýza deoxyribonukleové kyseliny (dále jen DNA) je odběr lidských buněk, při němž dochází k identifikaci osob na základě kódu získaného výsledkem analýzy DNA. Analýza DNA je využívána jednak v soukromém právu například při určování otcovství, nebo ke zkoumání dědičných chorob či určování předků osob. Ve veřejném právu je analýza DNA využívána zejména v oblasti trestního práva při identifikaci pachatelů, kteří spáchali určitý delikt. Jedno mají ale způsoby využití analýzy DNA společné. S možnostmi využití tohoto institutu souvisí možnost zneužití získaných informací a možnost neoprávněného zásahu do informačního sebeurčení jedince.[114] Proto jsem toto téma zařadila do své práce.

V souvislosti s uvedeným je nutné, aby postup získávání vzorků DNA byl řádným způsobem právně upraven. Jaká je ale situace právní úpravy odběru vzorků DNA v ČR? Při pohledu do právního řádu ČR nenalezneme zákon, který by samostatně upravoval analýzu DNA. Určitou právní úpravu nalezneme v zákoně o ochraně osobních údajů.

Z § 4 písm. b) zákona o ochraně osobních údajů vyplývá, že identifikace osoby na základě vzorku DNA je citlivým údajem, jelikož jde o genetický údaj subjektu údajů. V § 4 písm. e) zákona o ochraně osobních údajů je upraveno, že jakákoli operace s osobním údajem je zpracováním osobních údajů. Podmínky zpracování citlivých údajů upravuje § 9 zákona o ochraně osobních údajů. Mezi ně patří např. výslovný souhlas subjektu údajů se zpracováním citlivých údajů, informace o účelu zpracování citlivého údaje, k jakým osobním údajům je souhlas dáván, komu je dáván a na jaké období. Účelem odběru vzorků DNA může být například vyšetřování trestných činů ohrožujících život lidí, zdraví nebo bezpečnost společnosti, předcházení trestné činnosti, zajišťování veřejného pořádku v ČR, nebo i recidiva pachatelů trestných činů.[115]

Další právní úpravu odběru vzorků DNA najdeme v zákoně o Policii České republiky.[116] V § 63 odst. 2 zákona o Policii České republiky je upraveno oprávnění policisty vyzvat osobu k prokázání totožnosti a dále v § 63 odst. 4 zákona o Policii České republiky je upraveno, jak postupovat, pokud nelze totožnost osoby zjistit. V takovém případě má možnost policista postupovat dle § 65 zákona o Policii České republiky. V ustanovení § 65 odst. 1 zákona o Policii

[114] *Proč potřebujeme novou právní úpravu využívání analýz DNA POLICIÍ?* [online]. epravo.cz, 9. července 2010 [cit. 10. října 2016]. Dostupné na <http://www.epravo.cz/top/clanky/proc-potrebujeme-novou-pravni-upravu-vyuzivani-analyz-dna-policii-63396.html>.
[115] Tamtéž.
[116] Zákon č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.

České republiky je policistům dáno oprávnění odebírat biologické vzorky umožňující získání informací o genetickém vybavení.[117]

Provést odběr vzorků DNA je ale možné za určitých podmínek i bez souhlasu subjektů údajů na základě zákona o Policii České republiky. Lze tak ale pouze u těch osob, u kterých nelze získat osobní údaje, na základě kterých by bylo možné provést identifikaci takové osoby. Pokud jsou osoby ve vazbě nebo ve výkonu trestu, je možné vzorky DNA odebrat a zpracovat bez souhlasu pouze u osoby, u které dosud nedošlo k identifikaci. Další podmínkou k odběru DNA bez souhlasu subjektu údajů také je, že vzorek DNA, který má být odebrán, musí být nezbytný pro již probíhající trestní řízení.[118]

Trestní řád upravuje možnost odběru vzorku DNA od osoby pouze za předpokladu, že je to nutné k provedení důkazu v trestním řízení dle § 114 odst. 2 trestního řádu. Pokud nastane situace, že osoba klade odpor s odebíráním vzorku DNA, má policie oprávnění takový odpor překonat na základě ustanovení § 114 odst. 4 trestního řádu. Způsob překonání odporu musí být ale dle tohoto ustanovení přiměřený intenzitě odporu.

Právní úprava tohoto institutu je tedy roztroušena do několika zákonů. Uvedené zákony upravují ale pouze možnost odebírat vzorky DNA. Jak je to ale s jejich dalším nakládáním? Uvedení do této problematiky je předmětem následující podkapitoly.

4.2 Národní databáze DNA

Vzorky získané analýzou DNA jsou v České republice uchovávány v Národní databázi DNA, v současné době obsahuje databáze zhruba 200 tisíc profilů DNA. Tato databáze vznikla v roce 2002. Je vedena Kriminalistickým ústavem a slouží k odhalování a zejména předcházení trestné činnosti.[119] Možnost odebírat vzorky DNA je upravena, jak již bylo uvedeno, v ustanovení trestního řádu a v ustanovení zákona o Policii České republiky. Institut Národní databáze DNA je ale založen pouze interním předpisem, kterým je závazný pokyn policejního prezidenta ČR č. 88/2002 k naplňování, provozování a využívání Národní databáze DNA.[120] To ale představuje zásadní problém, jelikož pokyn policejního prezidenta není zákonem.

---

[117] FOJDA, Jan. *Databáze DNA* [online]. uoou.cz, [cit. 30. října 2016]. Dostupné na <https://www.uoou.cz/databaze-dna/ds-2479/p1=2479>.

[118] *Odběry vzorků DNA byly v rozporu se zákonem* [online]. ochrance.cz, 27. února 2008 [cit. 10. října 2016]. Dostupné na <http://ochrance.cz/aktualne/tiskove-zpravy-2008/odbery-vzorku-dna-byly-v-rozporu-se-zakonem/>.

[119] *Ministerstvo chce usměrnit pravidla nakládání se vzorky DNA, policie by je mohla odebrat i dětem* [online]. aktualne.cz, 21. května 2016 [cit. 30. října 2016]. Dostupné na <http://zpravy.aktualne.cz/domaci/dna/r~09a3a22c1f8c11e6bc7c0025900fea04/>.

[120] Závazný pokyn policejního prezidenta č. 88/2002, k naplňování, provozování a využívání Národní databáze DNA.

V Národní databázi DNA přitom dochází ke zpracování citlivých údajů. Povinnost zákonné úpravy přitom vyžaduje už samotná Listina, která v čl. 7 odst. 1 stanoví, že omezit základní právo lze pouze v případech stanovených zákonem. Závazný pokyn policejního prezidenta je ale interním předpisem, který není veřejně přístupný. Osoby, kterým je provedena analýza DNA, nemají k tomuto předpisu přístup a nemohou tedy zjistit, jakým způsobem je nakládáno s odebranými vzorky DNA.[121]

Také v doporučení Rady Evropy č. R 92 1 Výboru ministrů členským státům o využívání DNA v rámci systému trestní justice,[122] kterým je ČR vázána, je uvedeno, že *„vytvoření a provozování jakéhokoli registru DNA pro účely vyšetřování a stíhání trestných činů by mělo být právně upraveno"*. Dále také Úmluva v čl. 8 odst. 2 upravuje, že *„státní orgán nemůže do výkonu tohoto práva zasahovat kromě případů, kdy je to v souladu se zákonem a nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, ochrany pořádku a předcházení zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných"*. Otázkou dostatečnosti právní úpravy Národní databáze DNA se zabýval ve svém šetření i veřejný ochránce práv a také dospěl k závěru, který potvrzuje vše uvedené, že nakládání se vzorky DNA v Národní databázi DNA není dostatečně právně upraveno.[123]

Právní úprava Národní databáze DNA byla napadena žalobou u Městského soudu v Praze. Soudní spor ohledně legálnosti provozování Národní databáze DNA trvá již sedm let. Žalobce Jiří Pivoda napadl u soudu, že mu byl odebrán vzorek DNA a následně uložen do Národní databáze DNA na základě plošného odebírání prováděného ve věznicích v roce 2007, ke kterému došlo pod určitou pohrůžkou přemístění do jiné věznice v případě odporu s odebráním vzorku DNA, tedy protiprávně, a proto žalobce požadoval, aby byl jeho vzorek byl z Národní databáze DNA vymazán. V rozhodnutí Městského soudu v Praze ze dne 3. ledna 2013, sp. zn. 31C 70/2012 - 116 bylo rozhodnuto o povinnosti odstranit profil DNA žalobce z Národní databáze DNA, jelikož právní úprava Národní databáze DNA je v rozporu s Úmluvou a Listinou, z důvodu, že je tato instituce je upravena pouze podzákonným předpisem. Soud také uvedl, že zákon pouze uvádí, jakým způsobem a za jakých podmínek lze odebrat vzorek DNA, ale již neuvádí, jak se bude s tímto vzorkem nakládat, kdo k němu bude mít přístup nebo jakým způsobem bude zlikvidován, což je také nepřípustné.[124] Jelikož ale později bylo zjištěno, že Městský soud v Praze nebyl k projednávání

[121] VOBOŘIL, Jan. *Proč potřebujeme novou právní úpravu využívání analýz DNA policií?* [online]. epravo.cz, 9. července 2010 [cit. 10. října 2016]. Dostupné na <http://www.epravo.cz/top/clanky/proc-potrebujeme-novou-pravni-upravu-vyuzivani-analyz-dna-policii-63396.html>.
[122] Doporučení Výboru ministrů Rady Evropy č. (92) 1 o využívání DNA v rámci systému trestní justice.
[123] MOTEJL, Otakar. *Závěrečné stanovisko ve věci postupu Policie ČR při odběru biologických vzorků odsouzeným a obviněným* [online]. ochrance.cz, 31. ledna 2008 [cit. 15. října 2016]. Dostupné na <http://www.ochrance.cz/fileadmin/user_upload/STANOVISKA/Policie/DNA-ZSO.pdf>.
[124] Rozsudek Městského soudu v Praze ze dne 3. ledna 2013, sp. zn. 31C 70/2012 – 116.

věci věcně příslušný, bylo rozhodnutí zrušeno a věc se bude projednávat znovu.[125] Plošné odběry DNA byly řešeny i v rámci šetření veřejného ochránce práv Otakara Motejla a byly také označeny jako protiprávní. Veřejný ochránce práv také upozornil na nutnost doplnění právní regulace této problematiky.[126]

Na základě uvedeného soudního sporu Ministerstvo vnitra začalo připravovat zákon o ochraně práv osob při nakládání s genetickými vzorky a profily v souvislosti s prováděním forenzní analýzy DNA (zákon o DNA). Zákon by měl upravovat dle 1§ „*fungování Databáze profilů DNA, jakož i pravidla zpracování genetických vzorků a profilů pro účely identifikační genetiky v rámci trestních řízení a plnění dalších úkolů Policie ČR*". Dále by měl stanovit taxativní výčet skupin osob, které budou podléhat odběru vzorků DNA a také stanovit lhůty, po jejichž uplynutí by měly být tyto profily DNA likvidovány. Poslanecké sněmovně byl návrh zákona (sněmovní tisk 635/0) předložen 23. října 2015. Vláda ale vyjádřila s tímto návrhem nesouhlas dne 23. listopadu 2015. V listopadu 2016 je zákon ve stádiu, kdy organizační výbor doporučil projednání zákona v Poslanecké sněmovně. Projednávání zákona v Poslanecké sněmovně by mělo proběhnout do konce roku 2016.[127]

K problematice odběru vzorků DNA se vyjádřil ESLP ve svém rozhodnutí ve věci *S. a Marper proti Spojenému Království,* ve kterém ESLP stanovil, že uchování informací, které se vztahují k soukromému životu, je zásahem do práva na soukromí bez ohledu, zda tyto informace jsou využity. Dále ESLP stanovil, že je nezákonné uchovávat DNA osob, které byly v trestním řízení zproštěny viny, neboť není splněna podmínka nezbytnosti tohoto opatření v demokratické společnosti podle čl. 8 odst. 2 Úmluvy.[128] Praxe v ČR je taková, že pokud je osoba, která byla trestně stíhána následně zproštěna viny, Národní databáze DNA obdrží požadavek na likvidaci vzorku DNA z databáze a likvidace takového vzorku je dle vyjádření Policie ČR[129] následně provedena. Neexistuje ale žádný právní předpis, který by takovou povinnost obsahoval.

Nezbývá než věřit, že se právní řád ČR co nejdříve rozšíří o právní úpravu tohoto institutu, jelikož je provozován ve zřejmém rozporu se zákonem. K problematice identifikace osob na základě odebraných vzorků DNA lze ještě doplnit informaci o existenci genetické diskriminace.

---

[125] *Vrchní soud v Praze: Rozsudek, podle nějž stojí policejní databáze DNA mimo zákon je správný. Vydal ho ale nesprávný soud. Zjistili jsme to po třech letech.* [online]. iure.org, [cit. 30. října 2016]. Dostupné na <http://www.iure.org/15/1210/vrchni-soud-v-praze-rozsudek-podle-nejz-stoji-policejni-databaze-dna-mimo-zakon-je-spravny-v>.

[126] *Odběry vzorků DNA byly v rozporu se zákonem* [online]. ochrance.cz, 27. února 2008 [cit. 10. října 2016]. Dostupné na <http://ochrance.cz/aktualne/tiskove-zpravy-2008/odbery-vzorku-dna-byly-v-rozporu-se-zakonem/>.

[127] *Sněmovní tisk 635 N. z. o DNA* [online]. psp.cz, [cit. 3. listopadu 2016]. Dostupné na <http://www.psp.cz/en/sqw/historie.sqw?o=7&t=635>.

[128] Rozsudek ESLP ve věci *S. a Marper proti Spojenému království* ze dne 4. prosince 2008, stížnost č. 30562/04, § 125.

[129] VANČO, Emil. *Policie ČR nezneužívá DNA* [online]. policie.cz, [cit. 4. listopadu 2016]. Dostupné na <http://www.policie.cz/clanek/informacni-servis-zpravodajstvi-policie-cr-nezneuziva-dna.aspx>.

4.3 Genetická diskriminace

V ČR jde zatím o pojem poměrně neznámý a v běžném životě se s ním lze setkat minimálně. Pojem genetická diskriminace znamená určité znevýhodňování osob při určité podobě profilu DNA zjištěného na základě analýzy DNA. Tento druh diskriminace je zejména ve Spojených státech amerických rozšířen například v oblasti neposkytnutí bankovního úvěru, ukončení zaměstnání nebo ztráty životního pojištění z důvodu genetických abnormalit, které vyplývají ze zjištěného profilu DNA. K tomuto druhu diskriminace dochází zejména z důvodu možnosti vyčíst z profilu DNA i informace o chorobách, ke kterým by osoby mohly mít predispozice. I tato oblast je tedy spojena s informačním sebeurčením jedince. Ke genetické diskriminaci dochází, i přestože ze zjištěného vzorku DNA není jisté, zda se předpoklady k chorobám v životě projeví, nebo zda zůstanou uchovány pouze v profilu DNA.[130] Tento typ diskriminace je tak diskriminací do jisté míry nepodloženou a zároveň neoprávněnou.

Ve Spojených státech amerických v důsledku rozšiřování genetické diskriminace bylo zavedeno pravidlo, podle něhož nelze hodnotit výši pojištění podle rasového původu člověka. V roce 2008 byl podepsán tehdejším prezidentem federální zákon *„The Genetic Information Nondiscrimination Act,"*[131] který měl pomoci zabránit genetické diskriminaci. Tento zákon upravuje zákaz diskriminace v oblasti zdravotního pojištění a v oblasti zaměstnání.[132]

Podobný postup bych očekávala i v legislativě ČR, jelikož otázka genetické diskriminace je i otázkou do jisté míry etickou. Lze totiž předpokládat, že informace zjistitelné z DNA osob budou stále kvalitnější a podrobnější. Proto by bylo vhodné problematiku nakládání se vzorky DNA právně zakotvit i z hlediska možného zneužití vzorků prostřednictvím genetické diskriminace.

---

[130] GERARDS Jannek. H., HERINGA, Aalt-Willem, JANSSEN Heleen L. *Genetic Discrimination and Genetic Privacy in a Comparative Parspective.* Mortsel: Intersentia, 2005, s. 146-149.

[131] *President Bush Signs H. R. 493, the Genetic Information Nondiscrimination Act of 2008* [online]. archives.gov, 21. května 2008 [cit. 21. října 2016]. Dostupné na <http://georgewbush-whitehouse.archives.gov/news/releases/2008/05/20080521-7.html>.

[132] *What is genetic discrimination?* [online] nih.gov, 25. října, 2016 [cit. 28. října 2016]. Dostupné na <https://ghr.nlm.nih.gov/primer/testing/discrimination>.

Závěr

V práci jsem si kladla za cíl poukázat, jak moderní technologie, se kterými přicházíme každý den do styku, mohou zasáhnout do práva na informační sebeurčení. Cílem práce bylo upozornit a věnovat se aktuálním problémům v oblasti kamerových systémů, internetu a analýzy DNA a uvést k problémům relevantní judikaturu ať už zahraniční nebo českou. Záměrem práce nebylo poskytnout celkový rozbor práva na informační sebeurčení ze všech možných hledisek vzhledem k rozsáhlosti tématu, které se dotýká mnoha dalších oblastí kromě výše uvedených.

Celkově považuji problematiku práva na informační sebeurčení za velmi roztříštěnou, ve které není snadné se orientovat. Hlavním problém dle mého názoru je, že právo na soukromí a jeho právní ochrana vznikala v době, kdy ještě neexistovaly instituty spojené s uvedenými moderními technologiemi. Po zpracování tohoto tématu docházím k závěru, že aktuální právní úprava práva na informační sebeurčení má mezery, které zapříčiňují, že např. nakládání a uchovávání vzorků DNA v Národní databázi DNA je nezákonné. Pokud se nic v nejbližší době nezmění, budou sporné oblasti předmětem stále se zvyšujícího počtu soudních sporů. Stav, ve kterém se právní úprava institutů souvisejících s uvedenými technologiemi nachází, je ale v podstatě logický, jelikož rychlý vývoj technologií nelze dost dobře ihned promítat do právní úpravy. Postupná aktualizace právní úpravy je ale velmi důležitým krokem z hlediska zachování garance ochrany práva na soukromí alespoň v míře již existující ochrany soukromí.

Z práce vyplynulo, že právo na soukromí není v žádném právním předpise vyčerpávajícím způsobem definované. To je ale paradoxně možné považovat za velký přínos, jelikož soudům je při rozhodování, co ještě lze podřadit pod právo na soukromí a jakému jednání poskytnout ochranu práva na soukromí, ponechána větší míra prostoru pro jeho uvážení. Samotný ESLP ve věci *Niemietz proti Německu* uvedl, že není nezbytné pojem soukromí podrobovat vyčerpávající definici.[133] Je tomu z důvodu propojenosti tohoto pojmu s vývojem společnosti, s dobou a dynamickým vývojem technologií. Vyčerpávající definice by tedy postrádala svůj smysl z hlediska dlouhodobějšího uchopení tohoto pojmu.

Při pokusu o odpověď na otázku, v jaké míře právo na informační sebeurčení existuje, se vraťme k výkladu tohoto pojmu. Tento pojem znamená právo svobodně se rozhodnout, jaké informace o sobě osoba poskytne okolí. Zároveň v sobě toto právo zahrnuje i ochranu před neoprávněným sledováním ze strany veřejné moci, s čímž souvisí povinnost státu poskytnout garanci ochrany tohoto práva a zajistit, aby nebylo do práva neoprávněně zasahováno. Míra

[133] Rozsudek ESLP ve věci *Niemietz proti Německu* ze dne 16. prosince 1992, stížnost č. 13710/88, § 28.

ochrany informačního sebeurčení jedince se zároveň odvíjí od způsobu života konkrétní osoby. Pokud osoba dobrovolně zveřejní soukromé informace, míra ochrany tohoto práva se v tomto rozsahu snižuje, snižuje se tak i povinnost státu poskytnout ochranu tomuto právu. Dále se míra práva na informační sebeurčení odvíjí od postavení osob ve společnosti. Pokud jde o osoby veřejně známé, např. politiky, umělce nebo sportovce, kteří vystupují na veřejnosti, míra poskytnutí ochrany práva na informační sebeurčení těchto osob je nižší. Je tomu z důvodu veřejného postavení těchto osob a toto východisko souvisí s možností veřejně známých osob své právo na soukromí lépe před veřejností obhajovat.[134] Míru ochrany práva na informační sebeurčení lze tedy do jisté míry ovlivnit vytvořením svého postavení ve společnosti a odhalováním svého soukromí v tomto postavení.

Pokud si položím otázku, co zbývá z práva na soukromí, lze se vrátit k charakteru zásahů do soukromí, které v souvislosti s vývojem technologií prošly změnou kvantitativní i kvalitativní. Ve smyslu zásahů kvantitativních lze jednoznačně dojít k závěru, že počet zásahů do práva se s vývojem technologií dramaticky zvýšil i v souladu s tím, že 21. století je označováno jako informační doba. Právo na informace zejména ve vztahu k existenci internetu nabralo významné postavení. Zásahy do práva na soukromí z hlediska kvalitativního lze charakterizovat v souvislosti s informační dobou jako takové zásahy, o kterých nemusí mít dotčená osoba vůbec povědomí. Dotčená osoba nemusí vůbec vědět, že její soukromí už nadále soukromím není.

S příchodem internetu výrazně stoupl počet informací. Informace je možné sdílet prostřednictvím sociálních sítí nebo jiných komunikačních prostředků bez ohledu na vzdálenost po celém světě. Hlavní problematikou ve vztahu k internetu je paměť internetu. Vše, co je na internetu zaznamenáno, na něm zůstane. Nemusí to být přímo ve vizuální podobě, ale vše zůstane zaznamenané v podobě kódu, na základě kterého internet technicky funguje. Vývoj práva na soukromí tudíž spočívá v tom, že v době před internetem informace zanikaly spolu s lidskou pamětí, na internetu však informace zůstávají zachovány. Správný směr ohledně této problematiky dle mého názoru představuje otevření otázky práva být na internetu zapomenut, kterou se zabýval ESLP ve věci *Costeja proti Google Spain*. V rozhodnutí ESLP je vyjádřeno právo být zapomenut na základě podané žádosti o odstranění z výsledků vyhledávání internetového prohlížeče. Zatím se ale jedná o otázku značně omezenou, protože právo být zapomenut z výsledků vyhledávání internetového prohlížeče podléhá vždy aktivnímu upozornění dotčené osoby na zásah do tohoto práva na základě podané žádosti o odstranění osobních údajů. Nově je právo být zapomenut upraveno v čl. 17 nařízení EU o ochraně fyzických osob v souvislosti se zpracováním osobních

[134] MATES, Pavel. *Ochrana soukromí ve správním právu,* 2. vydání. Praha: Linde, 2006, s. 15.

údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES,[135] které vstoupí v plnou účinnost 25. května 2018. Dotčená osoba by měla v souladu s tímto předpisem mít nárok na vymazání osobních údajů a také na to, aby její osobní údaje nebyly dále zpracovávány, pokud nejsou potřebné pro účel, za kterým byly shromážděny. V budoucnu bude ale tato otázka jistě ještě rozvinuta např. v tom směru, že nebude nutné informace přímo odstraňovat, ale alespoň ztížit určitý přístup k informacím vytvořením ochranných institutů.

Neustálý sběr informací o osobách a jejich možné zveřejňování a nemožnost efektivní kontroly právo na soukromí na internetu do jisté míry vylučuje. Myslím si, že na internetu by mělo více než kde jinde platit, že informace, které jsou uváděny za účelem soukromým, by soukromými zůstat měly. Jen tak lze zajistit ochranu v uspokojivé míře před neoprávněným sběrem informací, kterých se prostřednictvím tohoto institutu šíří obrovské množství.

V kapitole kamerové systémy a právo na informační sebeurčení jsem chtěla poukázat zejména na problém neexistence samostatného zákona, který by kamerové systémy upravoval. Zákon o ochraně osobních údajů upravuje problematiku osobních údajů, které jsou zpracovávány prostřednictvím kamerových systémů se záznamem. Tento zákon ale neobsahuje konkrétní právní úpravu směřující přímo k problematice kamerových systémů. Právní úprava kamerových systémů se záznamem podléhá zákonům, které jsou vzhledem k zákonu o ochraně osobních údajů právní úpravou speciální podle konkrétního prostoru, ve kterém jsou umístěny. Zákony, které jsou vzhledem k zákonu o ochraně osobních údajů speciální, jsou ale právně nejednotné, v právní úpravě tak vzniká zmatek. Tento problém by mohl být vyřešen zákonem, který by samostatně upravoval kamerové systémy a zároveň by zohlednil právní úpravu této technologie ve vztahu ke specifickým místům jejího umístění.

Problematika analýzy DNA v souvislosti s právem na informační sebeurčení jedince představuje v ČR problém z hlediska chybějící právní úpravy institutu Národní databáze DNA. Národní databáze DNA je upravena pouhým podzákonným právním aktem, kterým je pokyn policejního prezidenta. Právní úprava institutu je ale nedostatečná a v rozporu se zákonem, zejména s čl. 8 odst. 2 Úmluvy, který stanoví, že pokud má být právo na soukromí omezeno, musí být omezeno v souladu se zákonem. Provoz Národní databáze DNA je v rozporu se základním požadavkem ochrany práva na soukromí, provoz tohoto institutu se tedy nachází v rozporu se zákonem.

[135] Rozhodnutí Rady 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Úř. věst. L 119/1 ze dne 4. května 2016.

Relevantní právní úprava sporných otázek ohledně nakládání a uchování vzorků DNA se vyžaduje již delší dobu, ale při pohledu na legislativní proces nabývám dojmu, jakoby zákonodárce na úpravu tohoto institutu nijak nenaléhal. Přitom, jak bylo uvedeno v rozebíraném rozsudku žalobce Jiřího Pivody, soud uznal, že právní úprava tohoto institutu není v souladu se zákonem. K nezákonnosti právní úpravy tohoto institutu se vyjádřil již i veřejný ochránce práv. Do té doby, než bude vytvořena zákonná úprava, bude docházet k neoprávněným zásahům do práva na soukromí.

Závěrem lze dodat, že možnosti omezení práva na ochranu soukromí jsou stále větší. Do budoucna proto bude potřeba zajistit jeho větší ochranu vytvořením relevantní právní úpravy, aby mohlo být jako ústavní právo zachováno ve stejné míře jako dnes. Pokud zákonodárce přestane reagovat na technologický vývoj, vyjádří tak jasný postoj, že právo na informační sebeurčení není důležité chránit a toto právo se tak postupně z našich životů opravdu vytratí.

Bibliografie

Monografie, komentáře, odborné články

- FILIP, Jan. Úvodní poznámky k problematice práva na soukromí. In ŠIMÍČEK, Vojtěch (ed.). *Právo na soukromí*. Brno: MUNI press, 2011. 212 s.
- GERARDS Jannek. H., HERINGA, Aalt-Willem, JANSSEN Heleen L. *Genetic Discrimination and Genetic Privacy in a Comparative Parspective. Mortsel.* Intersentia, 2005. 241 s.
- JANEČKOVÁ, Eva, BÁRTÍK, Václav. *Kamerové systémy v praxi: právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. 1. vydání. Praha: Linde, 2011. 240 s.
- JIROVSKÝ, Václav. *Kybernetická kriminalita*. 1. vydání. Praha: Grada, 2007. 284 s.
- KMEC, Jiří (ed). *Evropská Úmluva o lidských právech: komentář*. 1. vydání. Praha: C. H. Beck, 2012. 1696 s.
- KOKEŠ, Marian. Několik poznatků k problematice konkrétních konfliktů mezi právem na informační sebeurčení a ochranou národní bezpečnosti v tzv. době internetové. In ŠIMÍČEK, Vojtěch (ed). *Právo na soukromí*. Brno: MUNI press, 2011. 212 s.
- KRATOCHVÍL, Zdeněk a kol. *Nové občanské právo.* 1. vydání. Praha: Orbis, 1965. 716 s.
- KÜHN, Zdeněk. Ochrana soukromí v internetové době. In ŠIMÍČEK, Vojtěch (ed). *Právo na soukromí.* Brno: MUNI press, 2011. 212 s.
- MATEJKA, *Ján. Internet jako objekt práva: hledání rovnováhy autonomie práva a soukromí.* 1. vydání. Praha: CZ.NIC, 2013. 256 s.
- MATES, Pavel. *Ochrana soukromí ve správním právu*, 2. vydání. Praha: Linde, 2006. 320 s.
- SVATOŇ, Jan. *Státověda*. 5. vydání. Praha: Wolters Kluwers, a. s., 2011. 400 s.
- SCHONBERGER, Viktor Mayer. *Delete – The Virtue of Forgetting in the Digital Age*, Princeton University Press, 2009. 256 s.
- WAGNEROVÁ, Eliška. In WAGNEROVÁ, Eliška (ed). *Listina základních práv a svobod komentář*. 1. vydání. Praha: Wolters Kluwer ČR, a. s., 2012. 931 s.

- WAGNEROVÁ, Eliška. Právo na soukromí: Kde má být svoboda, tam musí být soukromí. In ŠIMÍČEK, Vojtěch (ed). *Právo na soukromí*. Brno: MUNI press, 2011. 212 s.
- WARREN, Samuel, BRANDEIS, Louis. The right to privacy. *Harward Law Review*, 1890, vol. IV, December, č. 5, s. 193-220.
- WESTIN, Alan F. *Freedom and Privacy*. New York: Athenum, 1967. 487 s.

Judikatura soudů ČR

- Nález Ústavního soudu ze dne 22. března 2011, sp. zn. Pl. ÚS 24/10.
- Nález Ústavního soudu ze dne 18. prosince 2006, sp. zn. I. ÚS 321/06.
- Nález Ústavního soudu ze dne 20. června 2006, sp. zn. Pl. ÚS 38/04.
- Nález Ústavního soudu ze dne 20. prosince 2011, sp. zn. Pl. ÚS 24/11.
- Nález Ústavního soudu ze dne 30. října 2014, sp. zn. III. ÚS 3844/13.
- Nález Ústavního soudu ze dne 22. března 2015, sp. zn. Pl. ÚS 21/02.
- Usnesení Ústavního soudu ze dne 1. března 2000, sp. zn. II. ÚS 517/99.
- Usnesení Ústavního soudu ze dne 8. února 2010, sp. zn. IV. ÚS 2425/09.
- Rozsudek Nejvyššího správního soudu ze dne 28. června 2013, sp. zn. 5 As 1/2011-156.
- Usnesení Nejvyššího soudu ze dne 15. března 2012, sp. zn. 22 Cdo 1150/99.
- Usnesení Nejvyššího správního soudu ze dne 25. února 2015, sp. zn. 1 As 113/2012-133.
- Rozsudek Nejvyššího soudu ze dne 8. prosince 2009, sp. zn. 8 Tdo 682/2009.
- Rozsudek Městského soudu v Praze ze dne 3. ledna 2013, sp. zn. 31C 70/2012 – 116.
- Rozsudek Městského soudu v Praze ze dne 28. února 2007. sp. zn. 7 Ca 204/2005-49.
- Rozsudek Městského soudu v Praze ze dne 23. března 2012, sp. zn. 11 Ca 298/2008-47.

Zahraniční judikatura

- Rozsudek ESLP ve věci *Marckx proti Belgii* ze dne 13. června 1979, stížnost č. 6833/74.
- Rozsudek ESLP ve věci *S. a Marper proti Spojenému království* ze dne 4. prosince 2008, stížnost č. 30562/04.
- Rozsudek ESLP ve věci *Niemietz proti Německu* ze dne 16. prosince 1992, stížnost č. 13710/88.
- Rozsudek ESLP ve věci *Pretty proti spojenému království* rozsudek ze dne 29. dubna 2002, stížnost č. 2346/02.
- Rozsudek ESLP ve věci *Rotaru proti Rumunsku* ze dne 4. května 2000, stížnost č. 28341/95.
- Rozsudek ESLP ve věci *Storcková proti Německu* ze dne 16. června 2005, stížnost č. 61603/00.
- Rozsudek ESLP ve věci *Von Hannover proti Německu* ze dne 24. června 2004, stížnost č. 59320/00.
- Rozsudek Spolkového ústavního soudu SRN ze dne 15. prosince 1983, sp. zn. BVerfGE 65, 1.
- Rozsudek SDEU ze dne 13. května 2014, *Google Spain proti Mario Costeja González*, C 131/12.
- Rozsudek SDEU ze dne 8. dubna 2014, *Digital Rights Ireland Ltd proti Minister for Communications, Marine and Natural Resources a další a Kärntner Landesregierung a další*, C-293/12 a -594/12.
- *Moreno v. Hanford Sentinel, Inc.* ze dne 4. dubna 2009, 172 Cal. App. 4th 1125.

Právní Předpisy ČR

- Usnesení předsednictva ČNR č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky.
- Zákon č. 150/1948 Sb., Ústava Československé republiky, ve znění ze dne 9. května 1948.

- Zákon č. 100/1960 Sb., Ústava Československé socialistické republiky, ve znění ze dne 11. července 1960.
- Zákon č. 143/1968 Sb., Ústavní zákon o československé federace, ve znění ze dne 27. října 1968.
- Zákon č. 946/1811 Sb., rakouský všeobecný zákoník občanský, ve znění ze dne 1. června 1811.
- Zákon č. 293/1920 Sb., o ochraně svobody osobní, domovní a tajemství listovního, ve znění ze dne 9. dubna 1920.
- Zákon č. 108/1933 Sb., o ochraně cti, ve znění ze dne 28. června 1933.
- Zákon č. 141/1950 Sb., občanský zákoník, ve znění ze dne 25. října 1950.
- Zákon č. 40/1964 Sb., občanský zákoník, ve znění ze dne 26. února 1964.
- Zákon č. 509/1991 Sb., kterým se mění, doplňuje a upravuje občanský zákoník, ve znění ze dne 5. listopadu 1991.
- Zákon č. 89/2012 Sb., občanský zákoník.
- Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.
- Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů.
- Zákon č. 273/2012 Sb., o elektronických komunikacích, ve znění pozdějších předpisů.
- Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.
- Zákon č. 553/1991 Sb., o obecní policii, ve znění pozdějších předpisů.
- Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.
- Zákon č. 154/1994 Sb., o Bezpečnostní informační službě, ve znění pozdějších předpisů.

- Zákon č. 555/1992 Sb., o Vězeňské službě a justiční stráži České republiky, ve znění pozdějších předpisů.

- Zákon č. 128/2000 Sb., o obcích, ve znění pozdějších předpisů.

- Zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů.

- Zákon č. 561/2004 Sb., o předškolním, základním, středním a vyšším odborném vzdělávání (školský zákon), ve znění pozdějších předpisů.

- Zákon č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.

- Vyhláška č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání, ve znění pozdějších předpisů.

- Vyhláška č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů, ve znění pozdějších předpisů.

Právní předpisy EU

- Rozhodnutí Rady 95/46/ES ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Úř. věst. L 281 ze dne 23. listopadu 1995.

- Rozhodnutí Rady 2002/58/ES ze dne 31. července 2002, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací. Úř. věst. L 201 ze dne 31. července 2002.

- Rozhodnutí Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES. Úř. věst. L 105/54 ze dne 13. dubna 2006.

- Rozhodnutí Rady 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Úř. věst. L 119/1 ze dne 4. května 2016.

Internetové zdroje

- *Internet privacy* [online]. techopedia.com, [cit. 4. ledna 2016]. Dostupné na <https://www.techopedia.com/definition/24954/internet-privacy>.

- PAVLÁT, David. *Jak mohu postupovat v případě šíření hanlivých a dehonestujících informací na sociálních sítích, v internetových diskuzích apod. o mé osobě?* [online]. uoou.cz, 23. července 2014 [cit. 28. října 2016]. Dostupné na <https://www.uoou.cz/jak-mohu-postupovat-v-pripade-sireni-hanlivych-a-dehonestujicich-informaci-na-socialnich-sitich-v-internetovych-diskuzich-apod-o-me-osobe/d-11338>.

- *Žádost o odstranění z vyhledávání na základě evropských předpisů o ochraně údajů* [online]. google.com, [cit. 5. ledna 2016]. Dostupné na <https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=cs>.

- SUCHOMELOVÁ, Helena. *Při zjišťování dat ze sociálních sítí se nelze bez dalšího odvolávat na jejich veřejnou povahu* [online]. Pravniprostor.cz, 15. ledna 2015 [cit. 2. října 2016]. Dostupné na <http://www.pravniprostor.cz/clanky/trestni-pravo/pri-zjistovani-dat-ze-socialnich-siti-se-nelze-bez-dalsiho-odvolavat-na-jejich-verejnou-povahu>.

- *Provozování kamerových systémů: Metodika pro splnění základních povinností ukládaných zákonem o ochraně osobních údajů* [online]. uoou.cz, [cit. 2. října 2016]. Dostupné na <https://www.uoou.cz/files/metodika_provozovani_kamerovych_systemu.pdf>, s. 7-12

- MOTEJL, Otakar. *Závěrečné stanovisko ve věci podnětu Mgr. E. a L. H* [online]. ochrance.cz, 22. dubna 2010 [cit.28. října 2016]. Dostupné na <http://www.ochrance.cz/fileadmin/user_upload/STANOVISKA/Prestupky/5432-09-IK-ZSO.pdf>.

- *Co je street view.* [online], streetview.cz, [cit. 27. října 2016]. Dostupné na <http://www.streetview.cz/>.

- ZANDL, Patrik. *Google může opět snímkovat pro StreetView. Kde byl problém?* [online]. lupa.cz, 27. května 2011 [cit. 5. října 2016]. Dostupné na <http://www.lupa.cz/clanky/google-muze-opet-snimkovat-pro-streetview-kde-byl-problem/>.

- ŠTĚPÁNSKÁ, Hana. *Tisková zpráva*. [online]. uoou.cz, 23. května 2011 [cit. 12. října 2016]. Dostupné na <https://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=3105&n=tiskove%2Dzpravy%2D2011>.

- *Zásady přijímání snímků a ochrany soukromí.* [online]. google.com, [cit. 27. října 2016]. Dostupné na <https://www.google.com/streetview/privacy/#privacy-and-blurring>.

- VOBOŘIL, Jan. *Proč potřebujeme novou právní úpravu využívání analýz DNA policií?* [online]. epravo.cz, 9. července 2010 [cit. 10. října 2016]. Dostupné na <http://www.epravo.cz/top/clanky/proc-potrebujeme-novou-pravni-upravu-vyuzivani-analyz-dna-policii-63396.html>.

- *Odběry vzorků DNA byly v rozporu se zákonem* [online]. ochrance.cz, 27. února 2008 [cit. 10. října 2016]. Dostupné na <http://ochrance.cz/aktualne/tiskove-zpravy-2008/odbery-vzorku-dna-byly-v-rozporu-se-zakonem/>.

- MOTEJL, Otakar. *Závěrečné stanovisko ve věci postupu Policie ČR při odběru biologických vzorků odsouzeným a obviněným* [online]. ochrance.cz, 31. ledna 2008 [cit. 15. října 2016]. Dostupné na <http://www.ochrance.cz/fileadmin/user_upload/STANOVISKA/Policie/DNA-ZSO.pdf>.

- *President Bush Signs H.R. 493, the Genetic Information Nondiscrimination Act of 2008* [online]. archives.gov, 21. května 2008 [cit. 21. října 2016]. Dostupné na <http://georgewbush-whitehouse.archives.gov/news/releases/2008/05/20080521-7.html>.

- *What is genetic discrimination?* [online] nih.gov, 25. října, 2016 [cit. 28. října 2016]. Dostupné na <https://ghr.nlm.nih.gov/primer/testing/discrimination>.
- *Ministerstvo chce usměrnit pravidla nakládání se vzorky DNA, policie by je mohla odebrat i dětem* [online]. aktualne.cz, 21. května 2016 [cit. 30. října 2016]. Dostupné na <http://zpravy.aktualne.cz/domaci/dna/r~09a3a22c1f8c11e6bc7c0025900fea04/>.

- FRUMAROVÁ, Kateřina. *Ústavní stížnost pro nezákonnou nečinnost orgánů veřejné správy* [online]. ihned.cz, 22. září 2003 [cit. 30. října 2016]. Dostupné na <http://pravniradce.ihned.cz/c1-13385370-ustavni-stiznost-pro-nezakonnou-necinnost-organu-verejne-spravy>.

- FOJDA, Jan. *Databáze DNA* [online]. uoou.cz, [cit. 30. října 2016]. Dostupné na <https://www.uoou.cz/databaze-dna/ds-2479/p1=2479>.

- *Vrchní soud v Praze: Rozsudek, podle nějž stojí policejní databáze DNA mimo zákon je správný. Vydal ho ale nesprávný soud. Zjistili jsme to po třech letech.* [online]. iure.org, [cit. 30. října 2016]. Dostupné na <http://www.iure.org/15/1210/vrchni-soud-v-praze-rozsudek-podle-nejz-stoji-policejni-databaze-dna-mimo-zakon-je-spravny-v>.

- *Sněmovní tisk 635 N. z. o DNA* [online]. psp.cz, [cit. 3. listopadu 2016]. Dostupné na <http://www.psp.cz/en/sqw/historie.sqw?o=7&t=635>.

- VANČO, Emil. *Policie ČR nezneužívá DNA* [online]. policie.cz, [cit. 4. listopadu 2016]. Dostupné na <http://www.policie.cz/clanek/informacni-servis-zpravodajstvi-policie-cr-nezneuziva-dna.aspx>.

Další

- Sdělení federálního ministerstva zahraničí č. 104/1991 Sb., o sjednání Úmluvy o právech dítěte.

- Sdělení federálního ministerstva zahraničních věcí č. 209/1992 Sb., o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících.

- Vyhláška ministra zahraničních věcí č. 120/1976 Sb., o Mezinárodním paktu o občanských a politických právech a Mezinárodním paktu o hospodářských, sociálních a kulturních právech.

- Zákon dvanácti desek, deska VIII.

- *Všeobecná deklarace lidských práv* [online]. un.org [cit. 28. října 2016]. Dostupné na <https://childrenandarmedconflict.un.org/keydocuments/czech/universaldeclara1.html >.

- Sdělení Ministerstva zahraničních věcí č. 115/2001 Sb., o sjednání Úmluvy Rady Evropy č. 108, o ochraně osob se zřetelem na automatizované zpracování osobních údajů.

- Stanovisko č. 1/2006 Úřadu pro ochranu osobních údajů – provozování kamerového systému z hlediska zákona o ochraně osobních údajů (leden 2006).

- Závazný pokyn policejního prezidenta č. 88/2002 k naplňování, provozování a využívání Národní databáze DNA.

- Doporučení Výboru ministrů Rady Evropy č. (92) 1 o využívání DNA v rámci systému trestní justice.

Abstrakt

Tématem diplomové práce je *„Právo na informační sebeurčení v rámci práva na ochranu soukromí*". Hlavním cílem diplomové práce je představit právo na informační sebeurčení jako součást práva na ochranu soukromí. Dalším cílem je vymezit souvislost práva na informační sebeurčení v prostředí internetu, kamerových systémů a analýzy DNA. V diplomové práci jsou popsány právní předpisy a analyzována judikatura, která souvisí s uvedenými instituty a má určitou souvislost s právem na informační sebeurčení. Práce je členěna kromě úvodu a závěru do čtyř kapitol. Jednotlivé kapitoly jsou členěny na podkapitoly. První kapitola je úvodem do problematiky práva na soukromí a jeho součásti - práva na informační sebeurčení. Obsahuje stručný vývoj práva na soukromí, právní úpravu práva na soukromí, jednotlivé aspekty práva na soukromí a možnost omezení práva na soukromí prostřednictvím testu proporcionality. Druhá kapitola se věnuje vztahu práva na informační sebeurčení a internetu. Je v ní analyzován charakter zásahů do práva na informační sebeurčení, představen pojem data retention a problematika sociálních sítí. Třetí kapitola je věnována informačnímu sebeurčení ve vztahu k provozování kamerových systémů, zejména kamerovým systémům se záznamem, prostřednictvím kterých jsou zpracovávány osobní údaje. V rámci kapitoly jsou kamerové systémy rozděleny podle umístění do jednotlivých typů prostor a uvedeny problémy, které souvisejí s umístěním kamerových systémů ve specifických prostorech. Dále je představena služba Google Street View a jsou uvedeny problémy s tímto institutem spojené. Čtvrtá kapitola obsahuje problematiku analýzy DNA a práva na informační sebeurčení. V rámci kapitoly je představen institut Národní databáze DNA a je zde uvedena problematika genetické diskriminace.

Abstract

The topic of this master thesis is *"The right to informational self-determination within the right to privacy"*. The main goal of the master thesis is to introduce the right to informational self-determination as a part of the right to privacy. Another goal is to define the connection of this right in terms of the Internet, camera systems and DNA analysis existence. The thesis describes the legislation and analyzes case law connected with stated institutes and has a certain connection with the right to informational self-determination. The thesis is divided into four chapters, introduction and conclusion. Each chapter is divided into subchapters. The first chapter is an introduction to the right to privacy and its part - the right to informational self-determination. The chapter includes a brief history of the right to privacy, legislation of the right to privacy, individual aspects of the right to privacy and the possibility of limitation of the right to privacy via the proportionality test. The second chapter discusses the relationship of the right to informational self-determination and the Internet. The character of interventions into the right to informational self-determination is analyzed, data retention, the issues of social networks are introduced there. The third chapter is about informational self-determination in relation to operation of camera systems, especially camera systems with records by which personal data are processed. Camera systems are divided by location into different types of areas and the problems connected with camera systems location in specific areas are stated in the chapter. Furthermore, Google Street View is presented together with the problems associated with this institute. The fourth chapter includes the issue of DNA analysis and the right to informational self-determination. The National DNA database institute is introduced within this chapter; the defense against disagreement with DNA collection and genetic discrimination are stated there.

Klíčová slova

právo na informační sebeurčení, právo na soukromí, osobní údaj, analýza DNA, internet, kamerové systémy, zákon o ochraně osobních údajů, Úřad pro ochranu osobních údajů

Key words

right to informational self-determination, right to privacy, personal data, DNA analysis, internet, camera systems, Act on the Protection of Personal Data, The Office for Personal Data Protection