

Západočeská univerzita v Plzni

FAKULTA PRÁVNICKÁ

DIPLOMOVÁ PRÁCE

**KAMEROVÉ SYSTÉMY A JEJICH TRESTNĚ PRÁVNÍ A
PROCESNĚPRÁVNÍ ASPEKTY**

Lucie Majerová

Plzeň, 2013

Západočeská univerzita v Plzni

FAKULTA PRÁVNICKÁ

Katedra trestního práva

DIPLOMOVÁ PRÁCE

KAMEROVÉ SYSTÉMY A JEJICH TRESTNĚ PRÁVNÍ A

PROCESNĚPRÁVNÍ ASPEKTY

Lucie Majerová

Studijní program: Právo a právní věda

Studijní obor: Právo

Vedoucí práce: JUDr. Petr Kybic, Ph.D.,

katedra trestního práva,

Fakulta právnická Západočeské univerzity v Plzni

Plzeň, 2013

Prohlašuji, že jsem diplomovou práci vytvořila zcela samostatně s využitím literatury a zdrojů informací vyjmenovaných v níže uvedeném seznamu.

V Plzni dne 1. července 2013

.....
vlastnoruční podpis

PODĚKOVÁNÍ

Na tomto místě bych ráda poděkovala především vedoucímu mé diplomové práce JUDr. Petru Kybicovi, Ph.D. za jeho ochotu a vstřícný přístup, a to nejen při zpracování této diplomové práce, ale za celé mé studium. Velmi si vážím každé jeho rady a času, který mi v souvislosti s vypracováním této práce věnoval. Rovněž bych ráda poděkovala své rodině a přátelům, za jejich podporu. Protože bez své rodiny a přátel, bych teď nebyla tím, kým jsem. A těmto výjimečným lidem, kteří ve mě věřili vždy, když já sama jsem přestala, bych ráda věnovala svoji diplomovou práci.

Obsah

1.	Úvod.....	1
2.	Vymezení pojmů.....	3
2.1.	Kamerové systémy (CCTV).....	3
2.2.	Osobní údaj	4
2.3.	Citlivý údaj.....	7
2.4.	Zpracování osobních údajů	8
2.5.	Shromažďování osobních údajů.....	9
2.6.	Uchovávání osobních údajů	10
2.6.	Správce.....	10
2.8.	Zveřejněný osobní údaj	11
2.9.	Souhlas	11
2.10.	Soukromí.....	12
3.	Kamerové systémy.....	14
3.1.	Kamerové systémy bez záznamu	16
3.2.	Kamerové systémy se záznamem.....	19
3.2.1.	Zpracování osobních údajů provozováním kamerového systému	19
3.2.2.	Povinnosti správce osobních údajů.....	20
3.2.3.	Stanovení účelu.....	21
3.2.4.	Stanovení prostředků a způsobu	22
3.2.5.	Zpracovávat pouze přesné osobní údaje	23
3.2.6.	Shromažďovat osobní údaje pouze ke stanovenému účelu a v nezbytném rozsahu	23
3.2.7.	Uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování.....	24
3.2.8.	Zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny	25
3.2.9.	Shromažďovat osobní údaje pouze otevřeně	25
3.2.10.	Nesdružovat osobní údaje, které byly získány k rozdílným účelům	25
3.2.11.	Udělení souhlasu se zpracováním osobních údajů prostřednictvím kamerových systémů.....	26
3.2.12.	Informační povinnost.....	27
3.2.13.	Povinnost chránit záznamy	29
3.2.14.	Oznamovací povinnost	29
3.3.	Oblasti využití kamerových systémů	31
3.3.1.	Veřejná prostranství.....	31

3.3.2	Místo veřejně přístupné	37
3.3.3	Kamerové systémy ve školách.....	38
3.3.4	Kamerové systémy na pracovišti	42
3.3.5	Kamerové systémy instalované pro soukromý účel	43
4.	Trestněprávní aspekty kamerových systémů	46
4.1	Regulace trestním právem hmotným	46
4.2	Neoprávněné nakládání s osobními údaji	47
4.3	Příklad z praxe – Kauza Savoy	52
4.4	Trestněprocesní aspekty kamerových systémů	59
4.4.1	Důkaz a dokazování v trestním řízení.....	59
4.4.2	Použitelnost záznamu z kamerového systému jako důkazního prostředku v trestním řízení	62
5.	Úvahy de lege ferenda	73
6.	Závěr	82
	Resumé.....	84
	Seznam použitých zdrojů.....	85

Seznam použitých zkratek:

ČR	Česká Republika
ZOOÚ	Zákon o ochraně osobních údajů ve znění pozdějších předpisů, zákon č. 101/2000 Sb., ve znění pozdějších předpisů
FO	fyzická osoba
OZ	Občanský zákoník, zákon č. 40/1964 Sb. ve znění pozdějších předpisů
Listina	Listina základních práv a svobod, zákon č. 2/1993 Sb., ve znění pozdějších předpisů
Úmluva	Úmluva o ochraně lidských práv a základních svobod, zákon č. 209/1992 Sb., ve znění pozdějších předpisů
NSZ	nejvyšší státní zastupitelství
Ústav práva	Ústavu státu a práva Akademie věd ČR
PRF Brno	Právnická fakulta Masarykovy univerzity v Brně
Čl.	článek
MKDS	městské kamerové dohlížecí systémy
ZoOP	Zákon č. 553/1991 Sb., o obecní policii ve znění pozdějších předpisů
PČR	policie ČR
ZoPČR	Zákon č. 273/2008 Sb., o Policii ČR, ve znění pozdějších předpisů
Hl. m.	hlavní město Praha
KČ	korun českých
TČ	trestný čin
ZP	Zákon č. 262/2006 Sb., zákoník práce ve znění pozdějších předpisů
PO	právníké osoby
TŘ	Zákon č. 141/1961 Sb., trestní řád, ve znění pozdějších předpisů
TZ	Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů
OČVTŘ	orgány činné v trestním řízení
OS	okresní soud
NS	Nejvyšší soud ČR
ÚS	ústavní soud
NSS	nejvyšší správní soud
Směrnice	Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24.10.1995 o ochraně FO v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
EU	Evropská unie

1. Úvod

Cílem této práce není popsat detailně všechny možné oblasti využití kamerových systémů v návaznosti na jejich právní problematiku. Cílem této práce je alespoň nastínit problematiku kamerových systémů jako fenoménu dnešní doby a také upozornit na nepřehlednou a v mnoha ohledech nedostatečnou právní úpravu. Přestože název práce zní *Kamerové systémy a jejich trestněprávní a procesněprávní aspekty*, tato práce byla soustředěna především na důležité základní informace o kamerových systémech a na jejich trestněprávní aspekty (z hlediska hmotného i procesního práva trestního).

V první části této práce jsem nastínila základní pojmy, které upravuje zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů. Ve větší části své práce se věnuji kamerovým systémům se záznamem, na které se právě tento zákon vztahuje, a proto je nezbytné pochopit základní pojmy, se kterými se pak v celé problematice pracuje.

V druhé části jsem se zabývala oblastí využití kamerových systémů, jejich základnímu rozdělení a také právní úpravě. Ohledně oblasti využití je třeba říci hned na úvod, že jsem stručně nastínila jen některé z nich, jelikož oblastí pro využití je skutečně mnoho. Neměla jsem žádné zvláštní kritérium pro výběr konkrétních oblastí, vybírala jsem je tedy náhodně, podle svého momentálního uvážení nebo s ohledem na aktuální dění.

Třetí část této práce se pak věnuje trestněprávním aspektům kamerových systémů. Co se týká úpravy trestního práva hmotného, je poměrně skromná, nezdráhám se na tomto místě použít spojení „v podstatě žádná“. V praxi se jedná spíše o jediné ustanovení, a to ustanovení § 180, Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů (neoprávněné nakládání s osobními údaji). Ohledně ostatních to pak mohou být pouze domněnky, proto jsem zařadila pouze tento trestný čin. V trestně procesní části jsem se pak zaměřila především na problematiku záznamů z kamerového systému jako důkazu v trestním řízení, a to v návaznosti na § 89 odst. 2, zákona č. 40/1961 Sb., trestní řád, ve znění pozdějších předpisů.

Čtvrtá část práce se pak věnuje úvahám de lege ferenda, kde vyzdvihuji některé základní problémy a nutnost jednotné právní úpravy kamerových systémů. V této části

práce rovněž představuji navrhovanou novelu trestního zákona, která se dotýkala trestných činů vztahujících se ke kamerovým systémům, tedy nedovolenému sledování.

Během této práce jsem byla zapojena do projektu, který vedla katedra trestního a občanského práva, za což jsem velmi vděčná. Tento projekt obohatil mé vědomosti a rovněž jsem díky němu mohla pracovat s řadou knih, se kterými bych jinak mohla pracovat jen omezeně nebo vůbec.

Pevně věřím, že se mi podaří touto prací dosáhnout svého cíle, a to nastínit kamerové systémy v takovém světle, aby každý kdo si tuto práci přečte, viděl jejich dobrou i špatnou stránku. Nic není jen černé nebo bílé, ale pro využití kamerových systémů bohužel chybí dostatečné právní mantinely.

2. Vymezení pojmů

Pohled na kamerové systémy z právního hlediska, je velmi složitý a nejednoznačný, neboť kamerové systémy mohou velmi významně zasahovat do ústavně zaručených lidských práv a svobod. Když jsem se o toto téma začala hlouběji zajímat, uvědomila jsem si, z kolika úhlů je možné, ne-li dokonce nutné na něj nahlížet. Kamerové systémy jsou fenoménem naší doby. Mají nás především chránit. Chránit nás a naši bezpečnost, náš život, náš majetek. Mají být prevencí před neoprávněnými zásahy do našeho soukromí, nebo majetku (tedy prevencí a ochranou proti trestné činnosti). Přesto se sami na hranici neoprávněného zásahu do základních lidských práv a svobod pohybují. A to na hranici velmi tenké.

Jak už jsem předeslala, pohled na ně by měl být co nejkompexnější a pokud možno nezaujatý. Na začátek mé práce tedy předkládám základní pojmy, jejichž základní vysvětlení je podstatné pro pochopení dané problematiky, jelikož právě s těmito pojmy veškerá stanoviska a výklady ohledně kamerových systémů běžně pracují.

2.1. Kamerové systémy (CCTV)

Kamerový systém (angl. Closed Circuit TeleVision, nebo-li uzavřený televizní okruh), je z hlediska technického, užití kamer pro sledování určitých prostor a následné zobrazování těchto záznamů na monitorech a v případě kamerových systémů se záznamem (viz. dále) také jejich uchovávání a následné zpracování a využití. Tento systém se skládá z kamer, hardware a software vybavení, a v neposlední řadě může být (a často také je) doplněn o mikrofony, reproduktory nebo o zařízení pro ukládání nahraných dat. Tyto systémy mohou fungovat na základě otočných nebo statických kamer. Mohou pracovat automaticky nebo být ovládány k tomu oprávněnou osobou. Tato zařízení je možné rovněž ovládat a sledovat vzdáleně (např. majitel baru, který instaloval systém kamer do své provozovny, může vzdáleně sledovat a ovládat tento systém ze svého domova).

2.2 Osobní údaj

Osobní údaje jsou v ČR chráněny a regulovány Zákonem o ochraně osobních údajů ve znění pozdějších předpisů, zákon č. 101/2000 Sb., ve znění pozdějších předpisů (dále jen ZOOÚ) a dalšími právními předpisy. Nutno říci, že se vlastně jedná o transpozici Směrnice Evropského parlamentu a rady č. 95/46 ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Právní úprava ochrany osobních údajů je tedy následující:

Obecné předpisy:

Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů

Směrnice Evropského parlamentu a Rady 95/46/ES, o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů

Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat, (úmluva č. 108)

Speciální předpisy o ochraně osobních údajů:

Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti)

Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)

Směrnice Evropského parlamentu a Rady 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích)

Směrnice Evropského parlamentu a rady 2000/31/ES o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (Směrnice o elektronickém obchodu) ¹

Je třeba brát v úvahu, že pojem *osobní údaj* je z hlediska provozování kamerových systémů pojmem klíčovým a ani z pohledu ZOOÚ není vždy jednoduché definovat, co vlastně osobním údajem je či není. Tento pojem tedy není vždy jednoznačný a můžeme se setkat s mnoha judikáty, které na osobní údaj nahlížejí různě. V návaznosti na provozování kamerových systémů je nutné vědět, že je třeba rozlišovat, zda provozováním kamerových systémů dochází či nedochází ke zpracování osobních údajů. Pojem osobní údaj, je tedy vymezen v ZOOÚ následovně:

„...osobním údajem 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“²

Jak uvádí ZOOÚ, o osobní údaj se tedy jedná, pokud je na jeho základě možné identifikovat jeho subjekt (tedy subjekt osobního údaje). Subjektem může být pouze fyzická osoba.³ Vzhledem k době, ve které žijeme, tedy v době velmi rozvinutých moderních technologií, nemusí být osobním údajem jen např. číslo občanského průkazu, rodné číslo aj., ale jakákoliv informace, na základě které je možno subjekt osobního údaje přímo či nepřímo identifikovat (tedy např. záznam pořízený prostřednictvím kamerového systému), i když u některých údajů je možno tento subjekt identifikovat jen krátkodobě. Nejvyšší správní soud se ve svém rozhodnutí ze dne 12. února 2009, čj. 9 As 34/2008 – 68 k otázce osobního údaje vyjádřil následovně:

„ ... plná identita fyzické osoby v současných podmínkách technologicky vyspělé společnosti, tj. za vysokého stupně elektronických a jiných médiích, která jsou většině populace snadno dostupná, ve své podstatě neznámá nic jiného, než možnost tuto osobu určitým způsobem kontaktovat, aniž by bylo nutno znát místo jejího aktuálního

¹ Právní předpisy vztahující se k ochraně osobních údajů, 27.3.2013, dostupné z URL: http://www.oou.cz/index.php?file=personal_data_protection_law

² Zákon č. 101/2000 Sb., § 4, písm a), o ochraně osobních údajů ve znění pozdějších předpisů

³ KUČEROVÁ, Alena a kol. Zákon o ochraně osobních údajů komentář, Praha: nakladatelství C.H.Beck, 2012, 536 s. ISBN 978-80-7179-226-0. S. 47

pobytu. Proto se výklad pojmu osobní údaj nemůže striktně omezit jen na znalost např. rodného čísla, adresy či pracoviště subjektu údajů. Z tohoto důvodu je za osobní údaj nutno považovat i číslo mobilního telefonu určité osoby, jakkoliv může být takové číslo používáno jen dočasně, a zároveň nijak nespecifikuje jeho fyzickou, psychickou, ekonomickou či sociální identitu. Prostřednictvím tohoto údaje je však možno daný subjekt v určitém časovém úseku přímo kontaktovat a tento subjekt je tak dosažitelný a jistým způsobem určitelný, a to případně i bez znalosti jeho jména a dalších údajů, které již vazbu na jeho fyzickou, psychickou, ekonomickou či sociální identitu mají.⁴

Co se týká údajů pořízených kamerovými systémy, ÚOOÚ je ve svém stanovisku z roku 2006 shrnul následovně:

„...údaje uchovávané v záznamovém zařízení, ať obrazové či zvukové, jsou osobními údaji za předpokladu, že na základě těchto záznamů lze přímo či nepřímo identifikovat konkrétní fyzickou osobu (tedy: informace z obrazových či zvukových nahrávek umožňují, byť nepřímo, identifikaci osoby). Fyzická osoba je identifikovatelná, pokud ze snímku, na němž je zachycena, jsou patrné její charakteristické rozpoznávací znaky (zejména obličeje) a na základě propojení rozpoznávacích znaků s dalšími disponibilními údaji je možná plná identifikace osoby. Osobní údaj pak ve svém souhrnu tvoří ty identifikátory, které umožňují příslušnou osobu spojit s určitým, na snímku zachyceným, jednáním.“⁵

Vzhledem k výše uvedenému, však vyvstává otázka, zda provozování kamerových systému bez záznamu, skutečně není zpracováním osobních údajů (být zpracování Sui generis), jelikož osoba, která sedí na druhé straně, tedy před monitorem, může v danou chvíli daný subjekt identifikovat a kontaktovat (na základě vnímaného obrazu).

⁴ srov. podle rozsudku Nejvyššího správního soudu ze dne 12.02.2009, čj. 9 As 34/2008 – 68, [on-line] [cit. 27.3.2013], dostupné z URL: <http://www.stavebni-pravo.cz/9_As_34_2008-68_pojistovaci_agent-je_spravce_databaze.pdf>

⁵ Stanovisko č. 1/2006. Úřad pro ochranu osobních údajů. [on-line] [cit. 27.3.2013], dostupné z URL: <http://www.uouu.cz/files/stanovisko_2006_1.pdf>

2.3. Citlivý údaj

Pojem citlivý údaj byl vtělen do českého ZOOÚ na základě evropského vzoru (Směrnice 96/94, Úmluva 108⁶). Jedná se o odlišení osobních údajů zvláštního charakteru, jejichž zpracováním dochází k mnohem citelnějším zásahům do soukromí subjektů. V ZOOÚ je jeho výčet následující a citlivým údajem je tedy:

„...osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů.“⁷

Aby se jednalo o citlivý údaj, musí být současně splněny dvě podmínky. V první řadě, se musí jednat o informace k identifikované či identifikovatelné fyzické osobě (musí tedy obecně jít o osobní údaj), a současně s tím se musí jednat alespoň o jednu ze skutečností, které jsou uvedené ve výčtu skutečností v § 4, písm. b) ZOOÚ. Pro zpracování informací o citlivých údajích však platí přísnější režim a oprávnění k jejich zpracování se omezuje na specifické situace.⁸

Ohledně aplikace právních postupů je důležité, že výklad pojmu citlivý údaj nemůže být zužující a rovněž by neměl být rozšiřující. Jelikož špatný výklad (rozšiřující nebo zužující), by mohl mít v případě zúžení za následek nepatřičné omezení zvýšené ochrany osobních údajů, opačně pak v případě rozšíření výkladu by mohlo být následkem vtažení údajů, kterým se zvýšené ochrany souvislosti se soukromým fyzické osoby nedostává. V podstatě lze tento pojem rozdělit na čtyři skupiny: 1) *informace o původu člověka* (údaje o náboženství, národnostním, rasovém nebo etnickém původu), 2) *informace o jeho názorech a přesvědčení* (o politických postojích, členství v odborových organizacích, o náboženství nebo o filozofickém přesvědčení), 3) *o osobním životě* (odsouzení za trestný čin, zdravotní stav a sexuální život), 4) *genetické a*

⁶ Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat (ETS č.108, Štrasburk, 28 ledna 1981), sděl. Ministerstva č. zahr. věci č. 115/2001 Sb.

⁷ Zákon č. 101/2000 Sb., § 4, písm. b), o ochraně osobních údajů, ve znění pozdějších předpisů,

⁸ KUČEROVÁ, Alena a kol. Zákon o ochraně osobních údajů komentář, Praha: nakladatelství C.H.Beck, 2012, 536 s. ISBN 978-80-7179-226-0. S. 55.

biometrické údaje (resp. takové biometrické údaje, které umožňují přímou identifikaci osoby).⁹

Vzhledem ke kamerovým systémům se občas v praxi může jevit problematickou otázka, zda při zpracování osobních údajů prostřednictvím záznamového zařízení, při kterém lze ve většině případů identifikovat např. rasový původ, se bude jednat o zpracování citlivých údajů (informace o původu člověka). Je třeba říci, že ač by takový záznam obsahoval citlivé údaje, ve většině případů však jde o zpracování nahodilé (ve smyslu dikce § 3 odst. 4 ZOOÚ) a nejedná se o jejich zpracování, neboť ve většině případů je cílem instalování kamerového systému ochrana majetku před neoprávněnými zásahy a slouží tedy k identifikaci případného pachatele, nikoliv k identifikaci rasy příslušné osoby. Primárním hlediskem tady je hledisko nahodilosti, k zachycení těchto údajů nedochází cíleně a neslouží k identifikaci konkrétní rasy pachatele. Ovšem ke zpracování citlivých údajů by docházelo tehdy, pokud by provozovatel (resp. správce) kamerového systému zaznamenával a zpracovával tyto údaje cíleně, tedy např. by je třídil podle příslušnosti k určité rase nebo etniku. V případě že by tak správce skutečně činil cíleně, musí si být jist, že svým jednáním neporušuje právní normy, a to nikoliv pouze normy České republiky, ale rovněž normy Evropské unie, neboť by se jednalo o zpracování citlivých údajů o původu člověka. Případné neoprávněné zásahy pak mohou mít za následek trestní sankce.¹⁰

2.4 Zpracování osobních údajů

Pojem zpracování osobních údajů lze společně s definicí osobního údaje a správce osobních údajů, považovat za klíčový z hlediska právní úpravy osobních údajů.

11

„Zpracováním osobních údajů je jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo

⁹ KUČEROVÁ, Alena a kol. Zákon o ochraně osobních údajů komentář, Praha: nakladatelství C.H.Beck, 2012, 536 s. ISBN 978-80-7179-226-0. S 55 – 56.

¹⁰ Tamtéž

¹¹ Zákon č. 101/2000 Sb., § 4, písm. e), o ochraně osobních údajů ve znění pozdějších předpisů

pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace“¹²

Je tedy nepochybné, že pokud je kamerový systém vybaven zařízením, které provádí záznam snímaného objektu, popř. objektů, jedná se o zpracování osobních údajů se všemi povinnostmi vyplývajícími ze zákona. Zpracováním těchto údajů, může být jedna operace nebo soustava operací. Operací či úkonem je nutno rozumět takovou operaci, při které správce s údaji nakládá, pracuje s nimi nebo je ovlivňuje (in futuro). Podmínkou při zpracování osobních údajů je prvek systematickosti. Tento prvek se posuzuje u zpracování manuálního, neboť při automatizovaném nakládání (př. snímání, nahrávání, třídění, ukládání atd.) je tento prvek přítomen vždy. Prvek systematickosti u manuálního zpracování je při komplexním pohledu třeba vždy posuzovat i do budoucna (to co správce s osobními údaji zamýšlí).¹³

V druhé části ustanovení § 4 ZOOÚ je uveden následný výčet pojmů, které zákonodárce pokládá za zpracování osobních údajů. Pojmy, které pokládá za zpracování jsou následující:

2.5 Shromažďování osobních údajů

Jedná se o jeden ze způsobů zpracování osobních údajů. Platná definice je obsažena v § 4 ZOOÚ písm. f) a jedná se tedy o: „...*systematický postup nebo soubor postupů, jehož cílem je získání osobních údajů za účelem jejich dalšího uložení na nosič informací pro jejich okamžité nebo pozdější zpracování*“¹⁴

Lze tedy říci, že shromažďováním osobních údajů jsou takové úkony správce, na základě kterých se v souladu se svou vlastní vůlí rozhodne získat OÚ za účelem dalšího zpracování a tedy i v kontextu do budoucna se rozhodne je uložit na nosič informací.¹⁵

¹² KUČEROVÁ, Alena a kol. Zákon o ochraně osobních údajů komentář, Praha: nakladatelství C.H.Beck, 2012, 536 s. ISBN 978-80-7179-226-0. S 47.

¹³ KUČEROVÁ, Alena a kol. Zákon o ochraně osobních údajů komentář, Praha: nakladatelství C.H.Beck, 2012, 536 s. ISBN 978-80-7179-226-0. S. 68-71

¹⁴ Zákon č. 101/2000 Sb., § 4, písm. e), o ochraně osobních údajů ve znění pozdějších předpisů

¹⁵ KUČEROVÁ, Alena a kol. Zákon o ochraně osobních údajů komentář, Praha: nakladatelství C.H.Beck, 2012, 536 s. ISBN 978-80-7179-226-0. S. 72

2.6 Uchovávání osobních údajů

V ZOOÚ je uchovávání definováno v § 4 písm. g) následovně, a to jako:

„... udržování údajů v takové podobě, která je umožňuje dále zpracovávat“¹⁶

Uchovávání OÚ je jednou z nejčastějších operací, kterou správce s údaji nakládá. Už z logiky věci je jasné, že údaje shromažďuje (resp. uchovává) za cílem jejich následného využití, jinak by již jejich zpracování pozbývalo smysl (proč uchovávat údaje, které nepotřebuji a nic s nimi nezamýšlím). Uchovávání těchto údajů znamená jejich uložení na nosiče informací, nezáleží na tom, o jaké nosiče se jedná. Podstatnou je vždy doba jejich uchovávání, která je upravena v § 5 odst. 1) písm. e ZOOÚ. Tuto dobu je správce osobních údajů povinen respektovat, je to *doba nezbytně nutná k účelu zpracování osobních údajů*.

2.6 Správce

Pojem správce osobních údajů je hned po subjektu osobních údajů nejdůležitějším pojmem celé úpravy ochrany osobních údajů, jelikož právě správce rozhoduje o tom, jak budou osobní údaje zpracovány (případně odpovídá za výběr zpracovatele¹⁷), za jakým účelem, jakými prostředky a zároveň za toto zpracování odpovídá konkrétní fyzické osobě, která je daným zpracováním dotčena a také odpovídá státu na základě veřejnoprávní úpravy povinností správce, které stát jako nositel veřejné moci upravil v ZOOÚ.¹⁸ Správcem je tedy dle dikce § 4 písm. j) ZOOÚ: *„...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“¹⁹*

¹⁶ Zákon č. 101/2000 Sb., § 4, písm. e), o ochraně osobních údajů ve znění pozdějších předpisů

¹⁷ Každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle ZOOÚ. Oproti správci, neurčuje účel nebo prostředky zpracování osobních údajů. Zpracovatelem se rozumí také jakýkoli jiný subjekt, který provádí jen některou činnost (nebo některé činnosti) související se zpracováním. Nemusí tedy jít vždy o subjekt, který osobní údaje shromažďil.

¹⁸ KUČEROVÁ, Alena a kol. Zákon o ochraně osobních údajů komentář, Praha: nakladatelství C.H.Beck, 2012, 536 s. ISBN 978-80-7179-226-0. S. 72

¹⁹ Zákon č. 101/2000 Sb., § 4, písm. j), o ochraně osobních údajů ve znění pozdějších předpisů

2.8 Zveřejněný osobní údaj

Zveřejněný osobní údaj je dle dikce § 4 písm. l) ZOOÚ vymezen následovně:
*„...osobní údaj zpřístupněný zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu“*²⁰

Definice tohoto pojmu z hlediska ZOOÚ není zcela jasná, a to vzhledem k tomu, že § 4 písm. e) tohoto zákona je mezi operacemi s osobními údaji uvedeno jak jejich zpřístupnění tak jejich zveřejnění, nicméně v komentovaném znění tohoto zákona, je však zveřejnění osobních údajů definováno jako jejich zpřístupnění, což způsobuje, že dle zákonodárce se z těchto pojmů stávají téměř synonyma. Rozdíl lze spatřovat zejména v tom, že *zpřístupnění osobního údaje je proces, jehož výsledkem je zveřejnění OÚ bez omezení, či omezení jen určitému okruhu osob* (př. nahlížení osob do zdravotnické dokumentace § 65 Zákona o zdravotnických službách).²¹

Značně problematickou oblastí je z pohledu ochrany osobních údajů jejich zpřístupňování prostřednictvím médií. Většina lidí vnímá sdělení (obrazové i slovní) učiněné např. veřejnoprávní televizí za legitimní, ale často se může stát, že takováto sdělení se mohou velmi citelně a neoprávněně dotknout soukromí osob (kterých se týká daná reportáž). Zmiňuji se o tomto problému mj. také proto, že i právě potřeba upravit zveřejňování osobních údajů specifických skupin osob, vedla k přijetí novely trestního řádu (zákon č. 52/2009 Sb.), která se právě této problematice dotýká a nese označení *náhubkový zákon*.²²

2.9 Souhlas

Souhlas subjektu údajů se zpracováním jeho osobních údajů je obecným pravidlem v souladu s dikcí § 5 odst. 2 ZOOÚ. Tímto ustanovením, je deklarován základní princip nutnosti souhlasu subjektu údajů se zpracováním jeho osobních údajů.²³ Souhlas subjektu údajů je definován dle dikce § 4 písm. n) jako:

²⁰ Tamtéž, § 4, písm. l)

²¹ KUČEROVÁ, Alena a kol. Zákon o ochraně osobních údajů komentář, Praha: nakladatelství C.H.Beck, 2012, 536 s. ISBN 978-80-7179-226-0. S. 85-89

²² Jedná se o novelizaci trestního řádu, z roku 2009 (zákon č. 52/2009 Sb.), s jeho účinností od dubna 2009 novelizoval znění § 8a, zavedl nová ustanovení § 8 b a 8 c trestního řádu (zákon č.141/1961 Sb.). Šlo o novelizaci v oblasti poskytování informací o trestním řízení a o osobách na něm zúčastněných. Rovněž zavedl nový trestný čin a to §180, TČ Neoprávněné nakládání s osobními údaji

²³ BARTÍK V., JANEČKOVÁ E.: *Kamerové systémy v praxi. Právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. Praha, Linde 2011, 240 s. ISBN 978-80-7201-850-5. S. 29

„...svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů“²⁴

V problematice kamerových systémů je však toto pravidlo velmi těžko použitelné, a to jen v případech, kdy lze jednoznačně vymezit okruh osob, které se nacházejí v dosahu kamery. Souhlas subjektu s jeho nahráváním je v případě kamerových systémů tedy velmi diskutabilním a několikrát soudy projednávaným problémem. Pro případy, kdy souhlas není třeba, je tedy nutno hledat buď zákonné zmocnění (př. Policie ČR) nebo výjimku danou právě v již zmiňovaném § 5 odst. 2 ZOOÚ, na základě které je možné zpracovávat osobní údaje bez souhlasu subjektu údajů jen v případě, že je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce²⁵ či jiné dotčené osoby (pojem dotčená osoba není v ZOOÚ nijak dále vysvětlen, nejspíše se však jedná o FO již by se údaje zpracované v rámci této výjimky mohly dotknout).²⁶

Nicméně souhlas se zpracováním osobních údajů je *právním úkonem*, kterým konkrétní subjekt dává svou vůlí najevo, že souhlasí s jejich konkrétním zpracováním. Právní úkony všeobecně, jsou upraveny v Občanském zákoníku, zákon č. 40/1964 Sb. ve znění pozdějších předpisů, (dále jen OZ). Je tedy nutno souhlas vždy posuzovat s přihlédnutím k náležitostem právního úkonu uvedených v OZ. Tyto náležitosti jsou upraveny v § 34 až § 42a.²⁷ S ohledem na uvedené je třeba dodat, že aby byl souhlas se zpracováním osobních údajů byl platný, musí reflektovat podmínky obou dvou právních předpisů, tedy jak OZ, tak ZOOÚ.

2.10 Soukromí

Jedná se o pojem, který se ve svém výkladu neustále rozvíjí. *„Na pojem soukromí je možno nahlížet ze dvou rovin. Jednak je to ochrana proti úniku informací o intimní sféře člověka na veřejnost a jednak ochrana ve vztahu k veřejné kontrole státní*

²⁴ Zákon č. 101/2000 Sb., § 4, písm. n), o ochraně osobních údajů ve znění pozdějších předpisů

²⁵ Podle § 4 písm. o) ZOOÚ je příjemcem každý subjekt, kterému jsou osobní údaje zpřístupněny, za příjemce se nepovažuje subjekt, který zpracovává osobní údaje podle § 3 odst. 6 písm.g,

²⁶ BARTÍK V., JANEČKOVÁ E.: *Kamerové systémy v praxi. Právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. Praha, Linde 2011, 240 s. ISBN 978-80-7201-850-5. S. 29

²⁷ § 34 Právní úkon je projev vůle směřující zejména ke vzniku, změně nebo zániku těch práv nebo povinností, které právní předpisy s takovým projevem spojují, zák. č. 40/1964 Sb. ve znění pozdějších předpisů

*moci. Je to ona sféra života člověka, do které nikdo (ani stát) nesmí zasahovat bez výslovného svolení člověka, kterého by se takový zásah do soukromí týkal. Je to taková sféra, kterou může člověk před kýmkoliv (i před státem) utajit, s výjimkou případů v zákoně výslovně uvedených. Současně je to takový prostor každého z nás, do kterého nikdo nesmí bez svolení nahlížet, vstupovat nebo pořizovat obrazové či zvukové záznamy.*²⁸

Je však zřejmé, že právo na soukromí zcela jistě není právem abstraktním nebo absolutním. Zásahy do něj jsou v zákonných důvodech povoleny a zákon sám je, jak je zřejmé předvídá (když uvádí... *s výjimkou případů v zákoně výslovně uvedených*). Právo na ochranu soukromí však zahrnuje jak negativní tak pozitivní složku dispozitivního práva. V praxi to znamená že:

- a) **negativní složka** - oprávněné právo bránit se proti neoprávněnému získávání a následnému využívání získaných informací o soukromí člověka
- b) **pozitivní složka** – pak znamená dispoziční právo ve vztahu k využití skutečností o jeho soukromém životě²⁹

Právo na soukromí je tedy právo každého z nás rozhodovat o tom, zda a jak smí být do našeho soukromého života zasahováno. Toto právo je chráněno mj. Listinou základních práv a svobod (dále jen Listina) ve svém čl. 10 odst. 2. který říká že: „*Každý má právo na ochranu před neoprávněným zásahem do soukromého a rodinného života.*“³⁰ A také v Úmluvě o ochraně lidských práv a základních svobod (dále jen Úmluva) ve svém čl.8 který říká že: „*(1) Každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence. (2) 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,*

²⁸ BARTÍK V., JANEČKOVÁ E.: *Kamerové systémy v praxi. Právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. Praha, Linde 2011, 240 s. ISBN 978-80-7201-850-5. S. 43

²⁹ tamtéž

³⁰ Listina základních práv a svobod, zákon č. 2/1993 Sb., ve znění pozdějších předpisů, čl. 10 odst. 2

*hospodářského blahobytu země, předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných.*³¹

Ve své výroční zprávě z roku 2009 ÚOOÚ uvádí že: „...zpracování osobních údajů prostřednictvím kamerových systémů je využíváno téměř ve všech možných životních situacích a v očích mnohých občanů se stávají zcela běžnou součástí našeho života a staly se velkým problémem naší společnosti. Pořízené záznamy jsou využívány pro dokazování sousedských sporů, k dokázání kázeňského prohřešku dětí ve škole. Jsou často zneužívány ve firmách ke sledování docházky, plnění pracovních úkolů, a to s pracovněprávními následky pro sledované osoby.“³²

Každý rok ÚOOÚ zaznamenává velké množství stížností proti neoprávněnému zásahu do soukromí občanů prostřednictvím kamerových systémů. Je více než jasné, že soukromí není tedy respektováno v takovém rozsahu, v jakém by respektováno být mělo.

3. Kamerové systémy

V návaznosti na předešlou kapitolu, kde byly stručně vysvětleny základní pojmy, se kterými budu pracovat v celé své diplomové práci, se nyní pokusím předložit ucelenější pohled na kamerové systémy jako takové, tedy na rozdělení kamerových systémů se záznamem a bez záznamu, na jejich právní úpravu a oblast využití. Díky této práci a času, který jsem nad ní strávila, si stále více uvědomuji, o jak aktuální téma se jedná a jak důležitým krokem by byl ucelený právní předpis pro jejich využívání, protože do dnešního dne existuje v podstatě jen pár paragrafů, které jsou roztroušeny do více právních předpisů, které lze na právní úpravu kamerových systémů využít.

V dnešní době již jsou kamerové systémy zaváděny na všech možných místech, jsou zaváděny do škol, do metra, v tramvajích, hojně jsou využívány pro majitele vozů, jako prostředek ochrany na letištích, v supermarketech a např. ve třetích zemích, byly zřízeny systémy s funkcí rozpoznávání obličeje pro prevenci bigamie.³³ Kamerové

³¹Úmluva o ochraně lidských práv a základních svobod, zákon č. 209/1992 Sb., ve znění pozdějších předpisů

³² ÚOOÚ, výroční zpráva za rok 2009, [on-line] [cit. 27.3.2013], dostupné z URL: <http://www.uoou.cz/files/vz_2009.pdf>

³³ BARTÍK V., JANEČKOVÁ E.: *Kamerové systémy v praxi. Právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. Praha, Linde 2011, 240 s. ISBN 978-80-7201-850-5. S. 11

systemy jsou na každém kroku a stále více tak vlastně žijeme ve společnosti pod odhledem (angl. surveillance society).³⁴

Hlavní kategorie pro využití kamerových systémů:

- a) ochrana jednotlivců**
- b) ochrana majetku**
- c) veřejný zájem**
- d) odhalování, prevence a stíhání trestné činnosti**
- e) získávání důkazů**
- f) jiné legitimní zájmy³⁵**

Důvody instalace kamerových systémů mohou být, jak vidíme výše – různé. Někdy je instalace dobrovolná (tedy ponechána na vůli té či oné konkrétní osoby) a v některých případech je dokonce povinná, např. v kasinech (upravuje zákon č. 202/1990 Sb., ve znění pozdějších předpisů, v dikci § 37).³⁶

Za platnou legislativu, která se vztahuje na kamerové systémy lze označit:

- zákon. č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů
- zákon č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů (příslušná ustanovení k ochraně osobnosti)
- zákon č. 2/1990 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů
- zákon. č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů
- zákon č. 273/2008 Sb., o Policii ČR, ve znění pozdějších předpisů

³⁴ pojem označující rozšiřující se dohled nad veškerou populací

³⁵ Stanovisko č. 4/2004. Úřad pro ochranu osobních údajů. [on-line] [cit. 27.3.2013], dostupné z URL: <<http://www.uoou.cz/uoou.aspx?menu=50&submenu=52&loc=83>>

³⁶ § 37 Kasino musí být vybaveno zabezpečovacím zařízením a monitorovacím zařízením. Monitorovacím zařízením musí být obrazově a zvukově zaznamenán celý průběh všech provozovaných her, dále pak práce přípravné (výdej žetonů) a závěrečné (uzavírání stolů, počítání žetonů a hotovosti). Provozovatel je povinen uchovávat po dobu 90 kalendářních dnů záznamy pořízené monitorovacím zařízením a pracovníkům státního dozoru umožnit přístup k těmto záznamům včetně jejich zapůjčení mimo prostor kasina. Monitorování musí být prováděno v nezpomaleném a nepřerušovaném záznamu. Bližší podmínky pro monitorování a uchovávání záznamů stanoví ministerstvo právním předpisem, zákon č. 202/1990 Sb., o loteriích a jiných podobných hrách, ve znění pozdějších předpisů

- zákon č. 553/ 1991 Sb., o obecní policii, ve znění pozdějších předpisů
- zákon č. 202/1990 Sb., o loteriích a jiných podobných hrách, ve znění pozdějších předpisů
- vyhláška ministerstva financí č. 285/1998 Sb., o podmínkách monitorování a uchovávání záznamu v kasinu
- stanoviska vydávána Úřadem pro ochranu osobních údajů, stěžejně Stanovisko č. 4/2004 ke zpracování osobních údajů prostředky kamerového sledování

Za mezinárodní právní nástroje vztahující se k úpravě kamerových systémů lze považovat:

- Úmluva o ochraně lidských práv a základních lidských svobod, zákon č. 209/1992 Sb., ve znění pozdějších předpisů
- Úmluva Rady Evropy č. 108/1981, o ochraně jednotlivců se zřetelem na automatizované zpracování osobních dat
- Listina základních práv Evropské unie
- Směrnice Evropského parlamentu a rady, č. 95/46 ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů

3.1 Kamerové systémy bez záznamu

Pokud mluvíme o systémech bez záznamu, ZOOÚ se na tyto systémy nevztahuje. Je to způsobeno tím, že chybí podstata uvedená v dikci § 4 písm. e)³⁷. Tedy chybí ukládání a shromažďování dat (podstata pojmů vysvětlena v předešlé kapitole), jedná se totiž o pouhé přenosy či monitoring (kamerové monitorovací systémy). Zákon se na tento druh systémů nevztahuje ani tehdy, pokud je záznam přímo přenášen např. na internetové síť (což je dle mého názoru dosti diskutabilní, jelikož zaznamenávaná osoba je v některých případech velmi dobře identifikovatelná). Ohledně otázky legality těchto monitorovacích systémů je třeba zmínit, že v řadě případů je velmi obtížné na ni jednoznačně odpovědět.³⁸

³⁷ Zákon č. 101/2000 Sb., §4 písm. e) zpracováním osobních údajů jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace,

³⁸ BARTÍK V., JANEČKOVÁ E.: *Kamerové systémy v praxi. Právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. Praha, Linde 2011, 240 s. ISBN 978-80-7201-850-5. S. 42

Touto otázkou, tedy otázkou problematiky instalování monitorovacích kamerových systémů, se mj. zabýval Úřad veřejného ochránce práv v roce 2003, kdy se jednalo o problematiku umístění monitorovacích kamerových systémů ve školském zařízení. Shrnutí podává výkladové stanovisko Nejvyššího státního zastupitelství (dále jen NSZ) pořadové č. 10/2003³⁹, ve kterém je proveden rozbor problematiky na základě dvou stanovisek, a to stanoviska Ústavu státu a práva Akademie věd ČR (dále jen Ústav) a odborného stanoviska Právnické fakulty Masarykovy univerzity v Brně (dále jen PRF Brno), kde obě uvedená stanoviska dospěla k rozdílným závěrům. Ústav při svém hodnocení dospěl mj. k závěru že:

„pouhé zrakové a sluchové pozorování, které ani není zaznamenáváno, není právem upraveno a považuje se za samozřejmé, že v zařízeních s určitou koncentrací osob je nutné provádět sluchovou a zvukovou kontrolu chování osob, a to vždy s intenzitou odpovídající povaze věci, že z hlediska práva není žádný rozdíl v tom, je-li takto sledován cestující na pohyblivých schodech v metru, nebo dítě ve výchovném ústavu, že ani v jednom případě takové sledování samo osobě nenarušuje ani jeho obydlí, ani soukromí, ani dobré jméno atd., a zejména neporušuje míru jeho svobody pohybu nebo jiného počínání: "Ta totiž zůstává vždy stejná, jako kdyby zde sledování vůbec nebylo, protože míra svobody počínání jednotlivce v konkrétní situaci je věcí jen hmotného práva, a nikoliv věci intenzity kontroly."⁴⁰

K tomuto názoru se pak postavila nesouhlasně PRF Brno, která konstatovala: „... že stavění naroveň kamerového monitoringu ve výchovných ústavech a např. na nádražích, v obchodních domech, bankách, atp. svědčí o nepochopení zásadního rozdílu této činnosti na veřejně přístupných prostranstvích a v soukromí. Dovojuje se, že prostory ve výchovných ústavech nelze považovat za veřejné, že použití kamerového systému v tomto případě ve skutečnosti není zaměřeno neadresně a v podstatě náhodně (jak tomu je například v bankách, nádražích), nýbrž je jednoznačně orientováno na pozorování předem určené a velmi omezené skupiny osob, jejichž chování se sleduje a zaznamenává. Podle stanoviska se tedy nejedná o prostorové sledování, nýbrž o sledování osobní. Ve stanovisku se uvádí, že je nutno rozlišovat mezi

³⁹ Výkladové stanovisko pořadové č. 10/2003, K zákonnosti umístění audio - vizuálních prostředků ve školských zařízeních, kde se vykonává ústavní výchova a ochranná výchova, 17.4.2013, dostupné na URL: <http://www.nsz.cz/images/stories/PDF/Stavoviska_Proces/2003/stavovisko%2010-2003.pdf>

⁴⁰ Tamtéž, [on-line] [cit. 17.4.2013]

*ochranou chování osob na veřejnosti na straně jedné a soukromí na straně druhé, že v soukromí je osobní sféra chráněna daleko intenzivněji. Ve stanovisku se dovozuje, že ubytování osob ve výchovných ústavech a podobných zařízeních spadá pod garance čl. 12 Listiny, že tyto instituce představují ve vztahu k ubytovaným osobám obydlí."*⁴¹

Ohledně zmíněného stanoviska Ústavu k problematice on-line kamerových systémů, nutno dodat, že ač se jedná o názor renomované instituce, je to názor více než diskutabilní. Ve svém důsledku by totiž znamenal, že na základě absence právní úpravy on-line monitoringu, není možné zasáhnout do osobnostních práv člověka a do jeho soukromí. *Jenže ve vztahu ke KS, je právě pojem soukromí jedním z těch pojmů, které mohou přes chybějící dostatečnou právní úpravu vymezit, zda je kamerový monitorovací systém využíván v souladu s právem či nikoliv.* Porušení práva na soukromí neznamená jen to, že určitý subjekt získává vědomosti o soukromém životě jiné osoby, ale také to, že tyto vědomosti dále rozšiřuje, a to je přesně obsahem kamerových systémů. Získávat informace o jiných osobách za účelem dalšího využití.⁴²

Nicméně i v případě kamerových systémů bez záznamu (tedy monitorovacích systémů) je třeba respektovat jiné právní předpisy, které jako takové poskytují ochranu soukromí osob, které jsou kamerou snímány. Těmito právními předpisy jsou Zákon č. 40/1964 Sb., OZ, ve znění pozdějších předpisů, § 12, který jako takový upravuje v této souvislosti podmínky ochrany osobnosti a to tak že, *podobizny, obrazové snímky a obrazové a zvukové záznamy týkající se fyzické osoby nebo jejích projevů osobní povahy smějí být pořizeny nebo použity jen s jejím svolením*⁴³. Dále je v § 12 odst. 2) uvedeno že, *svolení není třeba, použijí-li se písemnosti osobní povahy, podobizny, obrazové snímky nebo obrazové a zvukové záznamy k účelům úředním a na základě zákona a v odst. 3) je dále uvedeno že, podobizny, obrazové snímky a obrazové a zvukové záznamy se mohou bez svolení fyzické osoby poříditi nebo použíti přiměřeným způsobem též pro vědecké a umělecké účely a pro tiskové, filmové, rozhlasové a televizní zpravodajství. Ani takové použití však nesmí být v rozporu s oprávněnými zájmy fyzické osoby.*⁴⁴

⁴¹ Tamtéž,[on-line][cit.17.4.2013]

⁴² BARTÍK V., JANEČKOVÁ E.: *Kamerové systémy v praxi.Právní režim z pohledu ochrany osobních údajů a ochrany osobnosti.* Praha, Linde 2011, 240 s. ISBN 978-80-7201-850-5. S. 43

⁴³ Občanský zákoník, § 12, zákon č. 40/1961 Sb., ve znění pozdějších předpisů

⁴⁴ Tamtéž, § 12 odst. 2

A dále je třeba brát v úvahu příslušná ustanovení Listiny a to čl. 10 odst 2⁴⁵ a Úmluvy čl. 8 odst. 1⁴⁶, která v případě monitorovacích kamerových systémů zajišťují ochranu dotčeným osobám před neoprávněným zásahem do jejich rodinného a soukromého života.

Ráda bych ovšem podotkla, že do dnešní chvíle nikdo netuší, jaké je vlastně oficiální číslo kamerových systémů, které nepodléhají registraci u ÚOOÚ. Avšak v některých odborných kruzích zaznívá ohromující číslo 800 000 provozovaných monitorovacích systémů (odhadem k roku 2011).⁴⁷

3.2 Kamerové systémy se záznamem

Provozování kamerových systémů se záznamem, je mnohem složitější z hlediska povinností subjektu, který je hodlá provozovat. Jak již bylo řečeno v první kapitole, v případě, že je tento systém používán k identifikaci FO při určitém jednání a k následnému uchování a zpracování nahraných záznamů, je nepochybné, že podle dikce ZOOÚ se jedná o zpracování osobních údajů se všemi povinnostmi, které takové jednání obnáší a je tedy nutné splnit podmínky pro toto provozování, které tento zákon klade.

3.2.1 Zpracování osobních údajů provozováním kamerového systému

Již v předešlé kapitole jsem vysvětlila základní pojmy, které se dotýkají celé problematiky kamerových systémů. Nyní bych se ráda blíže zaměřila na kamerové systémy se záznamem. O zpracování osobních údajů se tedy jedná v případě, kdy je kromě kamerového sledování prováděn také záznam pořízených záběrů a pokud účelem

⁴⁵ Listina základních práv a svobod, zákon č. 2/1993 Sb., ve znění pozdějších předpisů, čl. 10 odst. 2, *Každý má právo na ochranu před neoprávněným zásahem do soukromého a rodinného života*

⁴⁶ Úmluva o ochraně lidských práv a základních svobod, zákon č. 209/1992 Sb., ve znění pozdějších předpisů, čl. 8, *odst.(1) Každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence. odst.(2) 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, předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných*

⁴⁷ BARTÍK V., JANEČKOVÁ E.: *Kamerové systémy v praxi. Právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. Praha, Linde 2011, 240 s. ISBN 978-80-7201-850-5. S. 47

pořízení těchto záběrů je mj. identifikace určitých osob v souvislosti s jejich určitým jednáním.⁴⁸

Ohledně možnosti provozování kamerových systémů se záznamem lze říci, že je lze provozovat jen na základě několika právních důvodů:

- *Pokud je to nezbytně nutné pro ochranu práv a právem chráněných zájmů správce nebo jiného subjektu* (zpravidla nejčastější důvod, typicky ochrana majetku), v případě provozování na základě tohoto důvodu, vždy je nutné dbát, aby nadměrně nezasahoval do práva na soukromí dotčených subjektů.
- *Jestliže je to nezbytně nutné pro dodržení právní povinnosti správce.* Zde se jedná zejména o plnění úkolů stanovených zákonem (př. Zákon č.273/2008 Sb., o Policii ČR, ve znění pozdějších předpisů, zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, atd.)
- *Na základě souhlasu subjektů.* V praxi velmi omezená možnost.⁴⁹

Provozování kamerových systémů se záznamem, braného tedy podle dikce ZOOÚ předpokládá splnění celé řady základních povinností.

3.2.2 Povinnosti správce osobních údajů

Provozování kamerových systémů se záznamem podléhá oznamovací povinnosti ÚOOÚ podle dikce § 16 ZOOÚ. Pro naplnění registrační povinnosti podle dikce zmíněného ustanovení je třeba dodržet zákonné povinnosti a metodické pokyny ÚOOÚ uvedené v *Metodice pro splnění základních povinností ukládaných ZOOÚ*.⁵⁰

⁴⁸ Metodika k provozování kamerových systémů, ÚOOÚ, [on-line] [cit. 19.4.2013], dostupné z URL: <http://www.uouu.cz/files/metodika_provozovani_kamerovych_systemu.pdf>

⁴⁹ tamtéž

⁵⁰ ÚOOÚ, Metodika provozování kamerových systémů, 21.4.2013, dostupné na URL: <http://www.uouu.cz/files/metodika_provozovani_kamerovych_systemu.pdf>

ZOOÚ jasně stanovuje, které podmínky jsou ty, jež je správce povinen splnit. Tyto povinnosti jsou vymezeny v § 5 odst. 1, ZOOÚ. Především je třeba vždy dbát toho, aby kamerové systémy nadměrně nezasahovali do soukromí subjektu údajů. Nasazení kamerových systémů by mělo být, řečeno s nadsázkou až ultima ratio. Tedy jejich použití by mělo přicházet na řadu až ve chvíli, kdy nelze sledovaného účelu dosáhnout účinně jinou cestou. Kamerové systémy nesmí být použity na místech určených k ryze soukromým účelům (př. toalety, šatny, sprchy), ovšem určitou možností i v těchto případech je dosažení určitého kompromisu, např. prostřednictvím vyznačení místa k převlékání, na která kamerové systémy nedohlédnou.⁵¹

3.2.3 Stanovení účelu

První z povinností, která vyplývá z dikce ZOOÚ v § 5 odst. 1 písm. a), je povinnost *stanovit účel, k němuž mají být údaje zpracovány*.⁵² Správce je povinen vždy vědět k jakému účelu mají být osobní údaje pomocí kamerových systémů zpracovány a tento účel musí být také schopen obhájit, jak vyplývá z oznamovací povinnosti vůči ÚOOÚ dle ustanovení § 16 ZOOÚ a rovněž také z povinnosti informační vůči subjektu údajů dle dikce § 11 ZOOÚ. Je na správci údajů zajistit, aby sledovaný účel nebyl nejasný či nejednoznačný. Je třeba mít tedy jasné kritérium pro posuzování slučitelnosti sledovaných údajů s účelem. Další podstatnou informací je, že je třeba vyloučit použití nashromážděných údajů za jiným účelem, než pro ten, který byl prvotně správcem stanoven. Účel pořízení takových záznamů tedy musí jasně korespondovat se zájmy správce, jako je např. ochrana správcova majetku. Záznamy mohou být využity k jinému účelu jen v případě, že to vyžaduje veřejný zájem (př. boj proti kriminalitě aj.)⁵³

⁵¹ ÚOOÚ, stanovisko k provozování kamerových systémů z hlediska ochrany osobních údajů, č. 1/2006, [on-line] [cit. 21.4.2013], dostupné z URL: http://www.uoou.cz/files/stanovisko_2006_1.pdf

⁵² Zákon č. 101/2000 Sb., § 5 odst. 1 písm a), o ochraně osobních údajů ve znění pozdějších předpisů

⁵³ ÚOOÚ, stanovisko k provozování kamerových systémů z hlediska ochrany osobních údajů, č. 1/2006, [on-line] [cit. 21.4.2013], dostupné z URL: http://www.uoou.cz/files/stanovisko_2006_1.pdf

3.2.4 Stanovení prostředků a způsobu

Stejně tak jako stanovit účel, je správce povinen rovněž *stanovit prostředky a způsob zpracování osobních údajů*⁵⁴, obojí ještě před zahájením zpracování. Ovšem zákonodárce bohužel ve jmenovaném ustanovení příliš jasně nevymezil, co je prostředkem zpracování a co je způsobem, považují tedy za příhodné zde tento rozdíl nastínit.

Jako prostředek zpracování, se povětšinou označují především zařízení technického charakteru (čím je zpracování prováděno) a za způsob zpracování pak lze označit metodu pro vyhodnocení osobních údajů (jak zpracování probíhá, manuálně⁵⁵, automatizovaně aj.). Zvolené prostředky či způsob zpracování lze s ohledem na danou funkčnost a efektivitu kdykoliv změnit v průběhu zpracování (na rozdíl od účelu).⁵⁶

Základním omezením je zde však zásada přiměřenosti, tedy že jak způsob, tak prostředky by měly být adekvátní sledovanému účelu. Je třeba ještě dodat, že v případě *střetu dvou zájmů (myšleno např. zájmu na ochraně majetku a zájmu na ochraně soukromí) má pak větší váhu zájem na ochraně soukromí jako na jednom ze základních lidských práv*, (např. rozhodnutí Městského soudu v Praze č.j. 11 Ca 298/2008 – 47). Vždy je však třeba brát v potaz okolnosti jednotlivého případu, účelu instalace kamerového systému, prostředí, v němž je kamerový systém nainstalován atd.⁵⁷

⁵⁴ Zákon č. 101/2000 Sb., §5, odst. 1) písm. b) správce je povinen stanovit prostředky a způsob zpracování osobních údajů, ve znění pozdějších předpisů

⁵⁵ Manuálním zpracováním se rozumí např. nejručnější formuláře, které se v dnešní době využívají spíše jako první krok ke zpracování osobních údajů

⁵⁶ KUČEROVÁ, Alena a kol. Zákon o ochraně osobních údajů komentář, Praha: nakladatelství C.H.Beck, 2012, 536 s. ISBN 978-80-7179-226-0. S. 108-111.

⁵⁷ HORKÝ, Štěpán. Kamerové systémy, epravo.cz, [on-line] [cit. 23.4.2013], dostupné z URL:<<http://www.epravo.cz/top/clanky/kamerove-systemy-dobry-pomocnik-ale-88307.html>>

3.2.5 Zpracovávat pouze přesné osobní údaje

Povinnost uvedená v § 5 odst. 1 písm. c)⁵⁸ je v zásadě vyjádřena ve dvou bodech, a to zpracovávat pouze přesné údaje a rovněž údaje aktuální. Splnění požadavku aktuálnosti je však vzhledem ke kamerovým systémům v podstatě požadavkem ad absurdum. V případě rigidního výkladu by totiž tento požadavek znamenal, že veškeré neaktuální údaje by měl správce (popř. zpracovatel) smazat. Specifikace tohoto požadavku na přesné a aktuální údaje je vzhledem ke kamerovým systémům z mého pohledu poměrně svízelná a zůstává otázkou, zda výraz „přesné“ znamená stricto sensu také „stále aktuální“, protože některé kamerové systémy pořizují záznamy v historické posloupnosti a tudíž zpětně již nemusí být aktuálními. Těžko je pak správce bude také aktualizovat, jelikož principem kamerových systémů je, že zaznamenávají situace, které se již staly, proto je velmi těžké na ně neustále aplikovat obecné předpisy. Rovněž problematický se jeví požadavek na případné zlikvidování ve chvíli, kdy správce zjistí, že údaje nelze opravit či aktualizovat, v případě kamerových systémů by pak veškeré nahrávání pozbývalo smyslu.⁵⁹

3.2.6 Shromažďovat osobní údaje pouze ke stanovenému účelu a v nezbytném rozsahu

V dikci § 5 odst. 1 písm. d)⁶⁰ ZOOÚ, která se týká přiměřenosti zpracování osobních údajů, jsou sice na první pohled povinnosti dvě, ale jejich smysl je v podstatě shodný. Lze shrnout, že se jedná o povinnosti zpracovávat údaje přiměřené, podstatné a především také nepřesahující stanovený rámec (resp. míru) účelu zpracování (viz. čl. 6 odst. 1 písm. c) Směrnice 95/46 ES).⁶¹ Přiměřenost rozsahu je třeba vždy posuzovat

⁵⁸ Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, §5, odst. 1 písm. c) zpracovat pouze přesné osobní údaje, které získal v souladu s tímto zákonem. Je-li to nezbytné, osobní údaje aktualizuje. Zjistí-li správce, že jím zpracované osobní údaje nejsou s ohledem na stanovený účel přesné, provede bez zbytečného odkladu přiměřená opatření, zejména zpracování blokuje a osobní údaje opraví nebo doplní, jinak osobní údaje zlikviduje. Nepřesné osobní údaje lze zpracovat pouze v mezích uvedených v § 3 odst. 6. Nepřesné osobní údaje se musí označit. Informaci o blokování, opravě, doplnění nebo likvidaci osobních údajů je správce povinen bez zbytečného odkladu předat všem příjemcům, ve znění pozdějších předpisů

⁵⁹ BARTÍK V., JANEČKOVÁ E.: *Kamerové systémy v praxi. Právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. Praha, Linde 2011, 240 s. ISBN 978-80-7201-850-5. S. 25.

⁶⁰ Zákon č. 101/2000 Sb., §5, odst. 1 písm. c) shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu

⁶¹ Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, čl. 6 odst. 1 písm. c)

v souladu se stanoveným účelem, neboť ke každému účelu je třeba jiného rozsahu. Tuto povinnost je však správce rovněž povinen splnit ještě před zahájením zpracování osobních údajů.⁶²

3.2.7 Uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování

Požadavek uchovávání osobních údajů uvedený v § 5 odst. 1 písm. e)⁶³ je společně s předešlou povinností uvedenou v § 5 odst. 1 písm. d) v praxi při provozování kamerových systémů velmi těžko aplikovatelný. Zákon v tomto směru vyžaduje, aby existovala úzká souvislost mezi účelem a dobou uchovávání zpracovaných osobních údajů. Doba uchovávání těchto záznamů je vždy z hlediska ÚOOÚ posuzována s ohledem na dané okolnosti konkrétního zpracování a účelu.

Ve většině případů je správce povinen tuto dobu určit na základě ZOOÚ sám. Nicméně tato doba by měla být adekvátní, v praxi to znamená, že např. v případě trvale střeženého objektu by data neměla být uchovávána déle než 24 hodin a v zásadě by tato doba neměla přesáhnout několik dnů a po dosáhnutí stanovené doby, by tato data měla být vymazána (pokud není výjimka stanovena např. podle zvláštního zákona, při pořizování záznamů policejním orgánem).⁶⁴ Tato podmínka se ovšem nevztahuje na případy, kdy dojde k případnému incidentu a kopie těchto dat, by měla být zpřístupněna orgánům činným v trestním řízení, soudu popř. jiným oprávněným osobám.⁶⁵

Členské státy stanoví, že osobní údaje musejí být: přiměřené, podstatné a nepřesahující míru s ohledem na účely, pro které jsou shromažďovány a/nebo dále zpracovávány; [on-line] [cit. 25.4.2013], dostupné z URL: <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:CS:NOT>>

⁶² KUČEROVÁ, Alena a kol. Zákon o ochraně osobních údajů komentář, Praha: nakladatelství C.H.Beck, 2012, 536 s. ISBN 978-80-7179-226-0. S. 115-117.

⁶³ Zákon č. 101/2000 Sb., §5, odst. 1 písm. d) uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování. Po uplynutí této doby mohou být osobní údaje uchovávány pouze pro účely státní statistické služby, pro účely vědecké a pro účely archivnictví. Při použití pro tyto účely je třeba dbát práva na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů a osobní údaje anonymizovat, jakmile je to možné.

⁶⁴ BARTÍK V., JANEČKOVÁ E.: *Kamerové systémy v praxi. Právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. Praha, Linde 2011, 240 s. ISBN 978-80-7201-850-5. S. 25-27.

⁶⁵ Stanovisko ÚOOÚ, č.1/2006, [on-line] [cit. 25.4.2013], dostupné z URL: <http://www.uoou.cz/files/stanovisko_2006_1.pdf>

3.2.8 Zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny

Podle dikce § 5 odst. 1 písm. f)⁶⁶ je naprosto nepřipustné, aby správce údaje zpracované za konkrétním účelem následně použil za účelem jiným. Výkladem tohoto ustanovení se vylučuje možnost obcházení zákona a v souladu s tímto ustanovením je tak kladen limit pro správce, kteří si často myslí, že mají-li už nějaké údaje jednou ve své moci, mohou s nimi dle své libosti nakládat (např. ke komerčním účelům). Snahou zákonodárce zde je zamezení neoprávněnému nakládání s osobními údaji.⁶⁷

Nicméně v praxi je i toto ustanovení problematické a soudy se jim rovněž zabývaly, neboť pohled správce a ÚOOÚ se v mnoha ohledech značně rozchází.

3.2.9 Shromažďovat osobní údaje pouze otevřeně

Další z povinností správce vyjádřených v § 5 odst. 1 písm. g)⁶⁸ je shromažďovat osobní údaje pouze otevřeně. V praxi by tento výklad neměl činit zásadní potíže, lze říci, že v souladu se Směrnicí 95/46 ES je správce povinen jednat „korektně“ (v angl. verzích použit termín *fairly*). Cílem je zde především dosáhnout naprosté legality shromažďování osobních údajů.⁶⁹

3.2.10 Nesdružovat osobní údaje, které byly získány k rozdílným účelům

Poslední povinnost v § 5 vyjádřena v odst. 1 písm. h)⁷⁰ se v zásadě nese ve stejném duchu jako všechny předchozí, tedy jednat korektně v souladu s účelem a zároveň přiměřeně. Vzhledem ke snaze zákonodárce, tedy minimalizovat možný zásah

⁶⁶Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, § 5 odst. 1 písm. f) zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny. Zpracovávat k jinému účelu lze osobní údaje jen v mezích ustanovení § 3 odst. 6, nebo pokud k tomu dal subjekt údajů předem souhlas,

⁶⁷ BARTÍK V., JANEČKOVÁ E.: *Kamerové systémy v praxi. Právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. Praha, Linde 2011, 240 s. ISBN 978-80-7201-850-5. S. 25-27

⁶⁸Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, § 5 odst. 1 g) shromažďovat osobní údaje pouze otevřeně; je vyloučeno shromažďovat údaje pod záminkou jiného účelu nebo jiné činnosti,

⁶⁹ KUČEROVÁ, Alena a kol. *Zákon o ochraně osobních údajů komentář*, Praha: nakladatelství C.H.Beck, 2012, 536 s. ISBN 978-80-7179-226-0. S. 128-130.

⁷⁰ Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, § 5 odst. 2 písm. h) nesdružovat osobní údaje, které byly získány k rozdílným účelům.

do osobnostních práv, je zde možno spatřovat logiku věci v tom, že v případě sdružování údajů by mohlo docházet k nepřesnostem zpracovaných osobních údajů.

3.2.11 Udělení souhlasu se zpracováním osobních údajů prostřednictvím kamerových systémů

Definice souhlasu jako taková byla uvedena již v základních pojmech, následující text však předkládá spíše náležitosti takového souhlasu, který má být udělen k provozování kamerových systémů. Pokud se na zpracování osobních údajů kamerovým systémem nevztahuje výjimka uvedená v dikci § 5 odst. 2 písm. a) až g) ZOOÚ, podléhá toto zpracování povinnosti zpracovávat osobní údaje pouze se souhlasem subjektu údajů. Udělení souhlasu se týká pouze těch subjektů, které se v monitorovaném prostoru vyskytují pravidelně. Těmito subjekty mohou být např. v případě umístění kamerových systémů ve školách studenti, v obytných domech jejich obyvatelé aj. Pokud bude subjektem údajů nezletilá nebo nesvéprávná osoba, uděluje souhlas zákonný zástupce. U nezletilých se pak předpokládá, že souhlas je za ni zákonným zástupcem udělován do věku 15 let. Od tohoto věku je pak předpokládáno, že subjekt již dokáže posoudit rozsah případného zásahu do soukromí a je tedy schopen udělit ke zpracování souhlas. Udělení souhlasu se pak netýká subjektů vstupujících do monitorovaných prostor nepravidelně, resp. krátkodobě (návštěvy aj.).⁷¹

Jak již bylo uvedeno na začátku práce, souhlas musí být svobodný, vědomý a informovaný projev vůle. Správce musí být schopen doložit platný souhlas se zpracováním osobních údajů po celou dobu, kdy zpracování probíhá. Subjekt údajů, případně zákonný zástupce subjektu, musí být před nebo nejpozději při udělení souhlasu informován o všech podstatných skutečnostech týkajících se tohoto zpracování. Musí být tedy informován, jak již bylo uvedeno o účelu zpracování, rozsahu (umístění kamer), správci osobních údajů, o období, na které je souhlas udělen, o tom, kdo a jak bude osobní údaje zpracovávat, komu mohou být osobní údaje zpřístupněny. Dále je nutné subjekt údajů informovat o jeho právu na přístup k informacím o jeho zpracovaných osobních údajích (viz. § 12 ZOOÚ). Dále pak o případném právu na

⁷¹ ÚOOÚ, Metodika provozování kamerových systémů, [on-line] [25.4.2013], dostupné z URL: <http://www.uoou.cz/files/metodika_provozovani_kamerovych_systemu.pdf>

opravu osobních údajů (což v praxi kamerových systémů nelze v podstatě aplikovat), podání vysvětlení a o dalších právech plynoucích z § 21 ZOOÚ. V případě zásadních změn v rozmístění a nastavení kamer, je třeba subjekty údajů o těchto změnách informovat a získat rovněž souhlas subjektů s těmito změnami. Nicméně je třeba dodat, že i přesto že v praxi bývá sledování kamerovým systémem na základě souhlasu spíše výjimečné, institut souhlasu nesmí být zcela opomenut. Základem je ZOOÚ, kde je stanoveno ono obecné pravidlo, že správce může osobní údaje zpracovávat pouze se souhlasem, výjimky z tohoto pravidla jsou pak v ZOOÚ vyjmenovány. Bohužel i tak je na případné neudělení souhlasu v praxi velmi často naráženo, a to především ve chvíli, kdy je záznam např. použit jako důkaz (rozvedeno především v kapitole trestněprávních aspektů).⁷²

3.2.12 Informační povinnost

Další z povinností správce osobních údajů, je povinnost informační. Tato povinnost je zakotvena v dikci § 11 odst. 1) ZOOÚ.⁷³ Tato povinnost je velmi důležitá pro efektivní ochranu osobních údajů konkrétního subjektu, a to především proto, že na základě informací, které obdrží subjekt od správce, se může takový subjekt svobodně rozhodnout, zda bude za daných podmínek souhlasit se zpracováním svých údajů. Také se tak aktivně podílí na své ochraně a může se v případě nutnosti domáhat nápravy, pokud jeho osobní údaje nejsou zpracovány v souladu s právní úpravou.⁷⁴

Dále je třeba dodat, že ke splnění informační povinnosti nestačí pouze umístit do sledovaných prostor tabulku s nápisem „*Prostor sledován kamerovým systémem*“, jak se bohužel většina správců domnívá. Toto opatření je naprosto nedostačujícím, z hlediska ochrany subjektu údajů a to mj. i proto, že tato věta obsahuje pouze sdělení o tom, že osobní údaje budou zpracovány, nicméně nepodává žádné další informace o tom, kdo a jak tyto údaje bude zpracovávat nebo k jakým účelům a dále také neobsahuje

⁷² ÚOOÚ, Metodika provozování kamerových systémů, [on-line] [25.4.2013], dostupné z URL: <http://www.uoou.cz/files/metodika_provozovani_kamerovych_systemu.pdf>

⁷³ § 11 odst. (1) Správce je při shromažďování osobních údajů povinen subjekt údajů informovat o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny, nejsou-li subjektu údajů tyto informace již známy. Správce musí subjekt údajů informovat o jeho právu přístupu k osobním údajům, právu na opravu osobních údajů, jakož i o dalších právech stanovených v § 21. Zákon č. 101/2002 sb. o ochraně osobních údajů ve znění pozdějších předpisů

⁷⁴ BARTÍK V., JANEČKOVÁ E.: *Kamerové systémy v praxi. Právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. Praha, Linde 2011, 240 s. ISBN 978-80-7201-850-5. S. 30-32

informaci o tom, kde je případně možné mít přístup k těmto zpracovaným osobním údajům. Ohledně obsahu informačního sdělení je třeba říci, že není nutné, aby v tomto sdělení bylo definováno, kde je sledovací zařízení umístěno, je však nutné, aby informace o tom, že vůbec probíhá kamerové sledování, byly umístěny viditelně a také souhrnně s ostatními požadovanými údaji. Je dále vhodné, tyto informace např. doplnit vhodnými symboly, které již svou účinnost v souvislosti s kamerovým dohledem prokázaly (např. obrázek kamery aj.). Informace mají být uvedeny v odpovídající velikosti (s ohledem na místo, kde probíhá sledování). Na informační tabuli musí být vždy uveden účel sledování a správce příslušného systému. Rovněž je nutné brát v úvahu informovanost nevidomých osob, které se rovněž mohou nacházet v monitorovaných prostorech. Koncepti těchto požadavků lze pak označit jako tzv. *vícevrstevný systém*.⁷⁵

Nicméně v praxi to tak velmi často není, v mnoha provozovnách jsem zaznamenala, že informační tabule byla umístěna v rohu u dveří, její umístění tedy bylo více než nevyhovující, a předpokládám, že většina subjektů nacházejících se v této provozovně ani nevěděla, že nějaké kamerové sledování probíhá. Případné nesplnění informační povinnosti pak v podstatě vede k tomu, že by mohl být zpochybněn udělený souhlas subjektu údajů, jelikož v dikci ZOOÚ je předpokládáno, že subjektu údajů jsou před souhlasem sděleny všechny potřebné informace, na základě kterých se může svobodně rozhodnout, zda souhlas udělí či nikoliv. Případná nedostatečnost informovanosti subjektu, může tedy zakládat neplatnost uděleného souhlasu, neboť tento právní úkon může být považován za platný jedině v případě, že byly subjektu dány všechny potřebné informace týkající se zamýšleného zpracování.⁷⁶

Rovněž je nutné na tomto místě zmínit, že podle dikce § 21 ZOOÚ⁷⁷, je informovanost subjektu důležitá také proto, že subjektu údajů plynou z tohoto

⁷⁵ Stanovisko pracovní skupiny WP 29, č. 4/2004 ke zpracování osobních údajů prostředky kamerového sledování, [on-line] [27.4.2013], dostupné z URL:

<<http://www.uoou.cz/uoou.aspx?menu=50&submenu=52&loc=83#pp25>>

⁷⁶ BARTÍK V., JANEČKOVÁ E.: *Kamerové systémy v praxi. Právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. Praha, Linde 2011, 240 s. ISBN 978-80-7201-850-5. S. 30-32

⁷⁷ § 21, (1) Každý subjekt údajů, který zjistí nebo se domnívá, že správce nebo zpracovatel provádí zpracování jeho osobních údajů, které je v rozporu s ochranou soukromého a osobního života subjektu údajů nebo v rozporu se zákonem, zejména jsou-li osobní údaje nepřesné s ohledem na účel jejich zpracování, může a) požádat správce nebo zpracovatele o vysvětlení, b) požadovat, aby správce nebo zpracovatel odstranil takto vzniklý stav. Zejména se může jednat o blokování, provedení opravy, doplnění nebo likvidaci osobních údajů. (2) Je-li žádost subjektu údajů podle odstavce 1 shledána oprávněnou, správce nebo zpracovatel odstraní neprodleně závadný stav. (3) Pokud vznikla v důsledku zpracování

ustanovení práva na vysvětlení, opravu a další práva uvedená v tomto ustanovení. Nicméně ohledně zpracování osobních údajů pomocí kamerových systémů, jsou tyto požadavky velmi těžko aplikovatelné, jelikož není možné zaznamenané údaje např. opravit či doplnit. Jediná možnost pak v případě jakýchkoliv problémů je zničení těchto nahraných údajů.⁷⁸

3.2.13 Povinnost chránit záznamy

Další z povinností, která platí pro správce i pro zpracovatele, je povinnost uvedená v § 13 ZOOÚ a to povinnost ochrany záznamů. Podle dikce tohoto ustanovení, jsou jak zpracovatel, tak správce povinni přijmout taková opatření, která zajistí dostatečnou ochranu zpracovaným osobním údajům. Především jsou povinni, zajistit takovou ochranu, která bude dostatečná před neoprávněnými zásahy, tedy před neoprávněným nebo nahodilým přístupem k osobním údajům, k jejich změně, zničení nebo ztrátě. Rovněž jsou povinni je chránit před případným zneužitím. Stricto sensu lze říci, že jde o povinnost, přijmout ta nejvhodnější bezpečnostní opatření vzhledem k účelu a způsobu zpracování osobních údajů. Podle ZOOÚ je tedy správce povinen vyhodnotit všechna případná rizika ještě před začátkem zpracování osobních údajů a na základě tohoto vyhodnocení přijmout a provést odpovídající opatření. Konkrétní podobu ochrany však ponechává zákonodárce právě na správci či zpracovateli.⁷⁹

3.2.14 Oznamovací povinnost

Podle dikce § 16 ZOOÚ je správce osobních údajů provozováním kamerového systému se záznamem povinen dostát oznamovací povinnosti a to vždy ještě před zahájením provozování samotného kamerového systému, za předpokladu, že se na něj nevztahuje některá ze zvláštních výjimek uvedená v § 18 téhož zákona. Ke splnění této

osobních údajů subjektu údajů jiná než majetková újma, postupuje se při uplatňování jejího nároku podle zvláštního zákona.(4) Došlo-li při zpracování osobních údajů k porušení povinností uložených zákonem u správce nebo u zpracovatele, odpovídají za ně společně a nerozdílně.(5) Správce je povinen bez zbytečného odkladu informovat příjemce o žádosti subjektu údajů podle odstavce 1 a o blokování, opravě, doplnění nebo likvidaci osobních údajů. To neplatí, pokud je informování příjemce nemožné nebo by vyžadovalo neúměrné úsilí. Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů

⁷⁸ BARTÍK V., JANEČKOVÁ E.: *Kamerové systémy v praxi. Právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. Praha, Linde 2011, 240 s. ISBN 978-80-7201-850-5. S.30-32

⁷⁹ tamtéž

povinnosti je možné využít registrační formulář, který se nachází na stránkách ÚOOÚ, kde jsou rovněž obsaženy podrobné informace k plnění oznamovací povinnosti. ÚOOÚ má po provedení oznámení lhůtu 30 dnů na zapsání oznámení do registru. Po zápisu do tohoto registru vzniká správci právo zahájit zpracování osobních údajů prostřednictvím kamerových systémů se záznamem.⁸⁰

Jak je již uvedeno výše, na některé případy se oznamovací povinnost nevztahuje, těmito případy jsou:

a) Provozování kamerových systémů se záznamem pro osobní potřebu:

Pokud se FO rozhodne prostřednictvím těchto systémů chránit svůj majetek (např. monitorování soukromého pozemku), pak se na toto zpracování ZOOÚ nebude vztahovat (viz. § 3 odst. 3 ZOOÚ⁸¹). V tomto případě pak tedy ani není nutné podávat ÚOOÚ oznámení o zpracování. Vždy je však třeba důkladně vyhodnotit, zda provozování těchto kamerových systémů nebude zasahovat do jiných práv subjektů. Jak již bylo řečeno, je důležité, aby nedocházelo k nadměrnému zasahování do soukromí jiných osob, jelikož právě toto právo je velmi významně chráněno.

b) Provozování kamerového systému se záznamem, na základě zvláštního zákona:

Oprávnění na základě dílky § 18 ZOOÚ, jako příkladný výčet lze uvést následující:

- zákon č. 273/2008 sb., o Policii ČR, 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. 59/2006 Sb., o prevenci závažných havárií, ve znění pozdějších předpisů

⁸⁰ Metodika k provozování kamerových systémů, ÚOOÚ, [on-line] [29.4.2013], dostupné z URL: <http://www.uoou.cz/files/metodika_provozovani_kamerovych_systemu.pdf>

⁸¹ Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, § 3 odst. (3) Tento zákon se nevztahuje na zpracování osobních údajů, které provádí fyzická osoba výlučně pro osobní potřebu.

- zákon č. 18/1997 sb., o mírovém využívání jaderné energie a ionizujícího záření a o změně a doplnění některých zákonů, ve znění pozdějších předpisů
- zákon č. 109/2002 Sb., o výkonu ústavní výchovy nebo ochranné výchovy ve školských zařízeních a o preventivně výchovné péči ve školských zařízeních a o změně dalších zákonů, ve znění pozdějších předpisů
- zákon č. 129/2008 Sb., o výkonu zabezpečovací detence, ve znění pozdějších předpisů
- Zákon č. 326/1999 Sb., o pobytu cizinců na území ČR, ve znění pozdějších předpisů
- Zákon č. 555/1992 Sb., o vězeňské službě a justiční strážní ČR, ve znění pozdějších předpisů
- Zákon č. 17/1992 Sb., o celní správě, ve znění pozdějších předpisů⁸²

3.3 Oblasti využití kamerových systémů

Kamerové systémy se dnes využívají již prakticky všude a ke všem možným účelům. Velmi rozšířeným trendem jsou především kamerové systémy na pracovišti, v obytných domech, ve školách, ve zdravotnických zařízeních aj. Oblast využití je tedy opravdu velmi široká. I když bych skutečně ráda předložila všechny oblasti využití, musím na následujících stránkách zvolit jen některé z nich, jelikož pokusit se o komplexní vysvětlení všech oblastí využití, by bylo nejspíše v rozsahu několika diplomových prací.

3.3.1 Veřejná prostranství

Definice veřejných prostranství je následující: „*Veřejným prostranstvím jsou 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.*“⁸³

⁸² Metodika k provozování kamerových systémů, ÚOOÚ, [on-line] [29.4.2013], dostupné z URL: <http://www.uoou.cz/files/metodika_provozovani_kamerovych_systemu.pdf>

⁸³ Zákon č. 128/2008 Sb., Zákon o obcích (obecní zřízení), § 34, ve znění pozdějších předpisů.

Pokud se bude jednat o využití kamerových systémů bez záznamu, dalo by se říci, že se v podstatě jedná o ten nejnižší možný zásah do soukromí jednotlivce. Nicméně je pravdou, že subjekty, které jsou v těchto případech nadáni právem zřídit kamerové systémy se záznamem, mohou provozovat rovněž kamerové systémy bez záznamu, právo volby pak spočívá na tom kterém subjektu. Ve většině těchto případů, se jedná o zákonem uloženou možnost, nikoliv povinnost provozovat kamerový systém (i když lze nalézt případy, kdy se bude jednat o zákonem uloženou povinnost).

Typem kamerových systémů, které jsou využívány na veřejném prostranství, jsou Městské kamerové dohlížecí systémy (dále jen MKDS). Oprávnění k jejich provozování má pak Policie ČR a obecní policie v rámci zákonného zmocnění.⁸⁴

Zákon č. 553/1991 Sb., o obecní policii ve znění pozdějších předpisů

Obecní policie jakožto orgán obce, je zřízena (popř. rušena) obecně závaznou vyhláškou obecního zastupitelstva. Mezi úkoly obecní policie podle dikce zákona č. 553/1991 Sb. o obecní policii (dále jen ZoOP), patří především ochrana bezpečnosti osob a majetku, dohlížení nad dodržováním pravidel občanského soužití, obecně závazných vyhlášek a nařízení, rovněž se dále podílí na dohledu nad bezpečností a plynulostí provozu na pozemních komunikacích, podílí se nad dodržováním právních předpisů, na prevenci kriminality, odhaluje přestupky a jiné správní delikty, jejichž projednávání je v působnosti obce atd.⁸⁵

Logicky vzato, je nasazení kamerových systémů běžným prostředkem k dosahování zmíněných úkolů. Oprávnění k provozování kamerových systémů je zakotveno v § 24 písm. b) odst. 1 ZoOP, ve kterém je stanoveno že „... *obecní policie je 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.*“⁸⁶ K otázce kdo je v tomto případě správcem, který je odpovědný za zpracování osobních údajů je pak nutno dodat, že tímto správcem je obec, která obecní policii zřizuje. V případě obce, která obecní policii nezřídí pak platí, že legálně kamerové systémy provozovat

⁸⁴ BARTÍK V., JANEČKOVÁ E.: *Kamerové systémy v praxi. Právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. Praha, Linde 2011, 240 s. ISBN 978-80-7201-850-5. S. 47-49

⁸⁵ Srov. zákon č. 553/1991 Sb., o obecní policii, § 2, ve znění pozdějších předpisů

⁸⁶ tamtéž

nemůže.⁸⁷ Z pohledu požadavků ZOOÚ se pak v podstatě jedná o zvláštní úpravu k požadavkům § 4 tohoto zákona, které byly dopodrobna rozebrány v kapitole právní úprava. A na základní otázky je pak odpovězeno následovně: *kdo zpracovává osobní údaje?* (obecní policie), *pro jaký účel?* (monitorování zabezpečovaných míst, průběhu zákroků, předcházení kriminality), *z jakých míst?* (veřejná prostranství). Ke způsobu informování veřejnosti je pak nutno říct, že není nikterak definováno, jakým způsobem má být veřejnost informována o umístění kamerových systémů. V § 24 b odst. 2) je pouze uvedeno, že policie je povinna informace o zřízení těchto systémů vhodným způsobem uveřejnit, tato podmínka však není dále definována. Na zveřejnění těchto informací o provozu kamerových systémů je několik názorů, velmi často se tak stane zveřejněním na webových stránkách či prostřednictvím místních periodik, tento názor je možno vysledovat i v odborné literatuře. Ohledně plnění této informační povinnosti však existují i přísnější názory, jako např. ve stanovisku ministerstva vnitra ČR⁸⁸, které uvádí, že by občané města měli být dostatečně informováni o tom, že je veřejné prostranství monitorováno, a to např. informační tabulí s textem, nicméně toto bude v praxi spíše výjimkou. Podstatnou informací pro hledisko nasazení kamerových systémů obecní policií pak je určení, která místa vlastně mohou být pod dohledem těchto kamer. Bohužel, ZoOP v tomto směru není moc konkrétní. V § 2 ZoOP je uvedeno, že *policie provádí dohled nad dodržováním čistoty na veřejných prostranstvích a odhaluje přestupky a jiné správní delikty*⁸⁹, v této dikci tedy nutno hledat základní oprávnění pro umístění kamerových systémů a dále pak v již zmíněném § 24b ZoOP, kde je uvedeno, že *je oprávněna pořizovat obrazové a zvukové záznamy z míst veřejně přístupných*⁹⁰. Nicméně úkolem obecní policie také je, aby dodržovala i další obecné podmínky pro zpracování osobních údajů. Jednou z podmínek je pak např. doba uchovávání pořízených záznamů, kterou ZoOP vůbec neupravuje, proto je tedy nutné vycházet z podmínek ZOOÚ. Platí tedy i zde, uchovávat zpracované údaje (v tomto případě obecní policií) pouze pro nezbytně nutnou dobu pro účel zpracování. Z praxe úřadu vyplývá, že touto přiměřenou dobou je zpravidla doba třech dní.

⁸⁷ KUČEROVÁ, Alena a kol. Zákon o ochraně osobních údajů komentář, Praha: nakladatelství C.H.Beck, 2012, 536 s. ISBN 978-80-7179-226-0. S. 152-159

⁸⁸ Stanovisko Ministerstva vnitra ČR, [on-line] [30.4.2013], dostupné z URL: <http://www.uoou.cz/files/info_mvcr_kamery.pdf>

⁸⁹ Srov. zákon č. 553/1991 Sb., o obecní policii, § 2, ve znění pozdějších předpisů

⁹⁰ Srov. zákon č. 553/1991 Sb., o obecní policii, § 24 b), ve znění pozdějších předpisů

V případě delšího uchovávání nějakých záznamů, musí být tato doba řádně odůvodněná a přiměřená. Další častou otázkou pak je zveřejňování zaznamenaných údajů, k tomu třeba dodat, že zveřejňovat tyto zpracované osobní údaje nelze. Podrobně se touto otázkou zabývá např. stanovisko⁹¹ odboru prevence kriminality ministerstva vnitra, které tento problém podrobně zpracovalo.⁹²

Zákon č. 273/2008 Sb., o Policii ČR, ve znění pozdějších předpisů

Úkoly Police ČR (dále jen PČR) jsou vymezeny v § 2 zákona o Policii ČR (dále jen ZoPČR), těmito úkoly jsou především služba veřejnosti, ochrana osob, majetku a veřejného pořádku. Mezi další hlavní úkoly patří předcházení trestné činnosti a plnění úkolů podle trestního řádu. Dále pak další úkoly v rámci udržování pořádku a bezpečnosti. Z uvedeného vyplývá, že PČR provozuje kamerové systémy v podstatě za obdobných podmínek jako obecní policie. ZoPČR sice ve své hlavě X obsahuje celou část, která se vztahuje k nakládání s osobními údaji, avšak na kamerové systémy se vztahuje v podstatě pouze § 62 odst. 1 a 2, a § 2, který vymezuje rozsah činnosti PČR zákona č. 273/2008, o Policii ČR, ve znění pozdějších předpisů.⁹³ Ohledně ustanovení, která se vztahují na nakládání s osobními údaji je ještě třeba poznamenat, že tato ustanovení jsou předpisem *lex specialis* vůči ZOOÚ. Oblasti, které však neupravuje ZoPČR pak samozřejmě upravuje ZOOÚ. Je tedy zřejmé, že PČR i obecní Policie mohou provozovat kamerové systémy se záznamem, která monitorují veřejná prostranství za stejných podmínek.⁹⁴

V rámci výše uvedených zmocnění je tedy umožněno obecní (resp. městské) policii nebo PČR monitorování veřejných prostranství. Ovšem i pro tyto subjekty platí, že zásah do soukromí osob v rámci monitorování by měl být co nejmenší. Kamery by tedy neměly zabírat jiná místa, než původně určené, zejména by kamery neměly mířit

⁹¹ Stanovisko Ministerstva vnitra ČR, [on-line] [30.4.2013], dostupné z URL: <http://www.uouu.cz/files/info_mvcr_kamery.pdf>

⁹² KUČEROVÁ, Alena a kol. Zákon o ochraně osobních údajů komentář, Praha: nakladatelství C.H.Beck, 2012, 536 s. ISBN 978-80-7179-226-0. S. 152-159

⁹³ § 62, odst. 1) Policie může, je-li to nezbytné pro plnění jejich úkolů, pořizovat zvukové, obrazové nebo jiné záznamy osob a věcí nacházejících se na místech veřejně přístupných a zvukové, obrazové nebo jiné záznamy o průběhu úkonu. Odst. 2) Jsou-li k pořizování záznamů podle odstavce 1 zřízeny stálé automatické technické systémy, policie informace o zřízení takových systémů vhodným způsobem uveřejní, Zákon č. 273/2008 Sb., o Policii ČR, ve znění pozdějších předpisů

⁹⁴ BARTÍK V., JANEČKOVÁ E.: *Kamerové systémy v praxi. Právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. Praha, Linde 2011, 240 s. ISBN 978-80-7201-850-5. S. 159-160

do oken okolo stojících domů, nebo zabírat jiná místa, které již nejsou veřejným prostranstvím.⁹⁵

3.3.1.1 Městské kamerové dohlížecí systémy (MKDS)

MKDS jsou specifickým nástrojem prevence kriminality, na které jsou uvolňovány státní finanční prostředky. Jak již bylo uvedeno, provozuje je obecní (resp. městská) police a PČR. Nejdůležitější funkcí je tedy jejich funkce preventivní, tedy vytváření bezpečných zón v exponovaných lokalitách. MKDS bývají instalovány na místech, kde je největší pohyb obyvatel, případně návštěvníků těchto obcí a měst, dále pak na místech, kde jsou soustředěny různé instituce (jako např. komerční, sportovní a kulturní), na náměstích, pěších a obchodních zónách, parkovištích, nádražích, na frekventovaných sídlištích a také na místech kde je třeba monitorovat silniční dopravu (kontrola dopravních přestupků aj.). Jejich umístění by tedy mělo přispívat k ochraně osob a majetku, k dodržování vyhlášek, odhalování přestupků a také k ochraně veřejného pořádku. Významnou funkcí je tedy zaznamenávání protiprávních jednání všech typů pachatelů. Jak vyplývá již z výše uvedeného, jejich provozování musí být v souladu se ZoPČR, zákon č. 283/1991 Sb., ve znění pozdějších předpisů, se ZoOP, zákon č. 553/1991 Sb., o obecní Policii, ve znění pozdějších předpisů a v neposlední řadě se ZOOÚ, zákon č. 101/200 Sb., ve znění pozdějších předpisů. Nutno připomenout, že MKDS musí monitorovat pouze a jedině veřejná prostranství ve smyslu již zmíněné dikce § 34 zákona. č.128/2000 Sb., o obcích, ve znění pozdějších předpisů. Všechna riziková místa vhodná k případnému umístění MKDS se stanovují na základě podrobných analýz PČR.⁹⁶

K výše zmíněnému je dobré uvést jeden dobrý příklad za všechny. Ona totiž teorie a praxe co se týká kamerových systémů jsou diametrálně odlišné. Velmi dobrým příkladem, je případ, který se stal v roce 2007 v Plzni.

Městská bezpečnostní kamera, která měla sledovat provoz na křižovatce, konkrétně Na Belánce, místo provozu sledovala rozsvícené okno jednoho z bytů

⁹⁵ BARTÍK V., JANEČKOVÁ E.: *Kamerové systémy v praxi. Právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. Praha, Linde 2011, 240 s. ISBN 978-80-7201-850-5. S. 49-50

⁹⁶ Stanovisko Ministerstva vnitra ČR, [on-line] [2.5.2013], dostupné z URL: <http://www.uoou.cz/files/info_mvcr_kamery.pdf>

protějššího domu. Kamera přiblížila záběr natolik, že byla patrná kuchyňská linka a ostatní zařízení kuchyně. Tento obraz se objevil v noci na oficiálních stránkách Magistrátu města Plzně, který byl také jeho správcem, tudíž každý, kdo se v tu chvíli připojil na web magistrátu, mohl pokojně sledovat, co se v onom bytě děje. Ve dne tento systém obsluhovala PČR a večer a v noci městská policie.

Magistrát tehdy prostřednictvím k tomu pověřené osoby uvedl, že tyto kamery jsou nastaveny na dva možné pohyby, a to automatický (naprogramovaný) nebo ruční. Podle názoru magistrátu se jednalo o přiblížení kamery ruční manipulací a na vině údajně tedy byla městská policie. Majitel bytu se obrátil se stížností na ÚOOÚ. Nakonec byl skutečně shledán vinným strážník městské Policie, který měl prý kameru odpojit od webu. Tento strážník byl za tento prohřešek také sankcionován. Poškozený majitel bytu se tehdy vyjádřil k celé situaci tak, že si již nemůže být v budoucnu vůbec jist svým soukromím, a rovněž také vyjádřil obavu, aby někdo v budoucnu tyto systémy nezneužil.⁹⁷ Není se čemu divit. Tento případ je velmi mediálně známý, a v neposlední řadě je třeba dodat, že plzeňskému magistrátu bylo v rámci Big brother awards⁹⁸ tehdy právě i díky tomuto případu uděleno „ocenění“ pro největšího úředního slídila roku 2007.

Závěrem k MKDS bych ještě ráda dodala, že jejich rozvoj je skutečně alarmující. V roce 2005 obdrželo hl.m. Praha rovněž ocenění největšího úředního slídila v rámci Big brother Awards, a to za masivní podporu rozvoje kamerových systémů. Kamerové systémy jsou v Praze budovány od roku 1998 a do roku 2005 byla investice do těchto systémů okolo 400 milionů Kč a to aniž by existovala jasná zákonná pravidla pro využívání a uchovávání záznamů z těchto systémů. V roce 2008 šlo o cca 300 kamer. Dnes, v roce 2013 jde o cca 1000 kamer na území hl.m. Prahy.⁹⁹ Nutno dodat, že původním cílem bylo dosáhnout do roku 2010 integrace cca 2000 kamer pro MKDS.¹⁰⁰

⁹⁷ Plzeňská městská kamera sledoval byt,článek IDNES. cz, [on-line] [3.5.2013], dostupne z URL: <http://zpravy.idnes.cz/plzenska-mestska-kamera-sledovala-byt-ne-krizovatku-pcf-domaci.aspx?c=A070801_144158_domaci_hos>

⁹⁸ Big Brother Awards (ceny velkého bratra), jedná se o anticeny pro nejvzlejší firmy, úřady nebo technologie. Tyto ceny uděluje občanské sdružení Iuridicum Remedium, které se aktivně věnuje ochraně soukromí, které je porušováno v souvislosti s rozvojem nových technologií

⁹⁹ Mapa kamer, [on-line] [3.5.2013],dostupné z URL: < <http://www.mapakamer.cz/mapakamer/>>

¹⁰⁰ POSPÍŠIL, Filip, prezentace, Vývoj dosavadních snah o novou úpravu kamerových systémů, [on-line] [3.5.2013], dostupné z URL: <http://www.slidilove.cz/content/vyvoj-dosavadnich-snah-o-novou-upravu-kamerovych-systemu>

Co se tedy týká účinnosti MKDS, pro příklad a možná i pro pobavení zde uvádím *Murphyho kamerové zákony*, které shrnul na semináři Ministerstva vnitra v roce 2004 velitel Městské policie Zlín Ing. Jan Suchoň, podle jeho Murphyho zákonů platí, že: „... protiprávní jednání se děje mimo dosah MKDS, pokud dojde k protiprávnímu jednání pod MKDS, je kamera nastavena jinak, i když je však kamera MKDS nastavena na místo protiprávního jednání, je v poruše, pokud dojde k tomu, že je funkční kamera MKDS nastavena na místo protiprávního jednání, je v poruše záznam, je-li funkční kamera MKDS nastavena na místo protiprávního jednání a je funkční záznam dojde k jeho automatickému vymazání nebo jinému znehodnocení, zaznamená-li MKDS protiprávní jednání jsou telemetrické parametry pohledu nastaveny tak, že záznam neposkytuje dostatečné důkazní prostředky, jsou-li důkazní prostředky zaznamenané MKDS dostatečné, nejsou efektivně využity v trestním řízení. Technika sice rychle spěje kupředu, ale výše uvedené překážky nemůže nikdy úplně vyřešit. Některé z nich totiž nejsou čistě „technické“. Jsou spíše projevem různých zájmů těch, kterým mají kamery sloužit.¹⁰¹

Z výše uvedeného je tedy zřejmé, že skutečná účinnost kamerových systémů v rámci boje s kriminalitou je velmi diskutabilní. V mnoha studiích je navíc uváděno, že jejich účinnost je často průkazná pouze u majetkových zločinů, jako je např. vykrádání vozů na parkovištích. Zatímco na násilné TČ, nemají kamerové systémy vůbec žádný vliv.¹⁰²

3.3.2 Místo veřejně přístupné

Místo veřejně přístupné je velmi důležité z hlediska trestního práva a to vzhledem k § 358, zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů (TČ výtržnictví). Jedná se tedy o takové místo „...kam má přístup široký okruh lidí individuálně neurčených, a kde se také zpravidla více lidí zdržuje, takže hrubá neslušnost nebo výtržnost by mohla být postřehnutá více lidmi. Takové místo nemusí být přípustné bez omezení komukoli a kdykoli. Postačí, že je přístupné jen některým osobám

¹⁰¹Kamerové systémy v ČR - opravdu dlouhý sumarizační článek z roku 2007, [on-line] [cit.3.5.2013], dostupné z URL:< <http://www.slidilove.cz/content/kamerov%C3%A9-syst%C3%A9my-v-%C4%8Dr-opravdu-dlouh%C3%BD-sumariza%C4%8Dn%C3%AD-%C4%8Dl%C3%A1nek-z-roku-2007>>

¹⁰²GILL, Martin, SPRIGGS, Angela, *Vyhodnocení účinku kamerových systémů*, Praha:Institut pro kriminologii a sociální prevenci, vydavatelství KUFR, 2007, 141 s. ISBN 978-80-7338-061-8. S. 15

za určitých okolností a určitou dobu (např. čekárna zdravotnického zařízení, viz k tomu usnesení Nejvyššího soudu ze dne 28. 11. 2002, sp. zn. 3 Tdo 969/2002, uveřejněné v Souboru rozhodnutí Nejvyššího soudu, svazek 23, roč. 2003, T-522).¹⁰³

Vzhledem k uvedenému lze říci, že míst veřejně přístupných na základě této definice je tedy značné množství. Těmito místy mohou být např. supermarkety, běžné obchody, banky, čekárny autobusových nebo vlakových nádraží, zdravotnické zařízení, bary, restaurace, hotely, plovárny atd. Tato místa mohou být sledována monitorovacími systémy a rovněž kamerovými systémy se záznamem (v případě kamerových systémů se záznamem je však nutné respektovat požadavky ZOOÚ). Důvodem monitoringu těchto míst pak bývá ochrana majetku a osob, které se na těchto místech vyskytují. Na všech těchto místech budou osoby, které je navštíví požívat omezeného práva na soukromí, nicméně i monitoring těchto míst musí mít hranice. Neměla by být tedy monitorována místa, kde člověk očekává zvýšenou míru soukromí (př. šatna, toalety, sprcha aj.).¹⁰⁴

Nicméně většina (ne-li) každý z uvedených příkladů míst veřejně přístupných vyžaduje z hlediska aplikace ZOOÚ specifický přístup, pokud se jedná o kamerové systémy se záznamem a v případě, že se jedná pouze o monitorovací kamerové systémy, naráží stejně tak na právo na soukromí, jehož porušování musí být vždy důsledně odůvodněno. K této problematice se velmi významně vyjadřuje ÚOOÚ ve své výroční zprávě¹⁰⁵ z roku 2008 kde uvádí i mnoho popisů konkrétních příkladů.

3.3.3 Kamerové systémy ve školách

V dnešní době se stává rovněž velmi rozšířenou praxe umístování kamerových systémů do škol. V této části budu pojednávat o kamerových systémech se záznamem, jelikož tak jako u ostatních, právě ten naplňuje podmínky ochrany osobních údajů podle ZOOÚ. Ohledně kamerových systémů ve školách lze říci, že jde o téma více než aktuální, neboť se dotýká práva na soukromí dětí (samozřejmě nejen jich, ale i jiných subjektů, jako rodičů, zaměstnanců a rovněž třetích osob, které do prostor škol

¹⁰³ Usnesení Nejvyššího soudu ze dne 24.6.2009, sp.zn.8 Tdo 682/2009, [on-line] [11.5.2013], dostupné z URL: <<http://pravo4u.cz/judikatura/nejvyssi-soud-cr/8-tdo-682-2009/>>

¹⁰⁴ BARTÍK V., JANEČKOVÁ E.: *Kamerové systémy v praxi. Právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. Praha, Linde 2011, 240 s. ISBN 978-80-7201-850-5. S. 49-50

¹⁰⁵ Výroční zpráva ÚOOÚ za rok 2008, [on-line] [12.5.2013], dostupné z URL: <http://www.uoou.cz/files/vz_2008.pdf>

vstupují), nicméně problematika práva na soukromí dětí vyžaduje mnohem specifičtější přístup, vzhledem k vývoji osobnosti dítěte. Ohledně legitimity instalování kamerových systémů do škol, je třeba uvést, že tak jako v jiných případech zde dochází ke střetu dvou zájmů, a to zájmu na ochranu soukromí (dětí, zaměstnanců, třetích osob) a zájmu správce (v tomto případě např. ředitel školy) na ochranu majetku.

Problematickou otázkou se zde tedy může jevit, na jakou míru ochrany soukromí má právo dítě. Dítětem je každá lidská bytost mladší 18 let, pokud nedosáhne zletilosti dříve (podle právního řádu, jenž se na něj vztahuje).¹⁰⁶ Dítě je tedy úplnou lidskou bytostí a jako takovému je mu přiznáno plné právo na ochranu jeho soukromí, tedy rovněž i na ochranu osobních údajů. Ovšem vždy je třeba mít na zřeteli, že dítě je osobou, která se teprve rozvíjí, aby se stala dospělou bytostí (ať už psychicky či fyzicky), z tohoto důvodu je třeba dbát zvláštní ochrany (nejen) jeho soukromí. Hlavní zásady jsou obsaženy v základních mezinárodních dokumentech.¹⁰⁷ Některé z těchto dokumentů se dotýkají lidských práv a současně obsahují zvláštní pravidla, která se dotýkají dětí.¹⁰⁸

Základním problémem se zde pak může jevit souhlas subjektu údajů, vyplývající z dikce ZOOÚ a rovněž z mezinárodních směrnic (tj. 95/46/ES a 2002/58/ES). Tyto dokumenty sice samostatně nepojednávají o dětech, nicméně se vztahují na každou FO, tedy i na děti. Instalaci kamerových systémů se záznamem ve školách naprosto nepochybně dochází ke zpracování OÚ, ve smyslu dikce §4 písm. a) ZOOÚ. Dále pak shromažďování a pozdější využití naplňuje znaky pro zpracování osobních údajů uvedených v § 4 písm. e) téhož zákona. Tento zákon se tedy na provoz kamerových systémů ve školách plně vztahuje. Jak již však bylo řečeno v předešlých kapitolách, ZOOÚ stanovuje pro zpracování osobních údajů podmínku souhlasu subjektu údajů a to v § 5 odst. 2, výjimka z udělení souhlasu je možná jen na základě důvodů uvedených v § 5 odst. 2 písm. a) až g) tohoto zákona.¹⁰⁹

Ohledně kamerových systémů ve školách je často diskutována výjimka uvedená v dikci § 5 odst. 2 písm. e), který uvádí, že souhlasu není třeba, pokud je to třeba

¹⁰⁶ Čl. 1 Úmluvy OSN o právech dítěte

¹⁰⁷ Těmito dokumenty jsou: Všeobecná deklarace lidských práv, čl. 25, čl. 26 odst. 3, Evropská úmluva o ochraně lidských práv a základních svobod, čl. 8, Listina zákl. práv EU, čl. 242, Úmluva OSN o právech dítěte

¹⁰⁸ BARTÍK V., JANEČKOVÁ E.: *Kamerové systémy v praxi. Právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. Praha, Linde 2011, 240 s. ISBN 978-80-7201-850-5. S. 100-116

¹⁰⁹ Tamtéž

k ochraně práv a právem chráněných zájmů správce, či jiné dotčené osoby, nicméně vždy platí, že takové zpracování nesmí být v rozporu s právem subjektů na ochranu soukromého a rodinného života. Je tedy více než zřejmé, že této ochrany požívají jak děti tak mladiství a to vzhledem k jejich vývoji se zvýšenou ochranou. Jelikož opět tak jako u většiny (resp. každé části této problematiky) chybí pozitivní právní úprava, je třeba vše posuzovat proporcionalně ve vztahu práva na soukromí a na ochranu majetku. Ve velké míře zde záleží na přesném umístění kamerových systémů. Je zřejmé, že v případě, že budou kamerové systémy umístěny na místech, kde se pohybují zaměstnanci v rámci své pracovní doby a rovněž studenti v rámci výuky, popř. i během přestávky, dochází pak k porušení § 10 ZOOÚ.¹¹⁰

Východiskem pro tuto úvahu může být rovněž judikatura ESLP, když ve svém rozhodnutí ve věci *Niemietz vs. Německo* (velmi důležitý judikát rovněž pro oblast kamerových systémů na pracovišti) konstatoval, že neshledává nezbytným pokoušet se o vyčerpávající definici pojmu soukromý život a judikoval že: „*Respektování soukromého života musí do určité míry zahrnovat právo na vytváření a rozvíjení vztahů s dalšími lidskými bytostmi. Dále se pak zdá, že neexistuje důvod pro to, aby tento způsob chápání pojmu "soukromý život" vylučoval aktivitu profesní nebo obchodní povahy, protože právě během své pracovní činnosti má většina lidí značnou, ne-li největší příležitost rozvíjet vztahy s vnějším světem.*“¹¹¹

Stricto sensu lze konstatovat, že tento názor je možné aplikovat rovněž na žáky či studenty škol a samozřejmě i zaměstnance školy, kteří se nacházejí v jejich vnitřních prostorách. Pokud tedy nelze uplatnit výjimku pro zpracování bez souhlasu, musí být správci udělen souhlas, který musí splňovat podmínky právního úkonu tak, jak je uvedeno v OZ (svobodný a vědomý projev vůle) také musí splňovat podmínky uvedené v § 5 odst. 4 ZOOÚ (souhlas musí být informovaný). S ohledem na souhlas subjektů je třeba zvážit základní otázku a to, čím souhlas je v tomto případě (kdy subjektem zpracování je dítě) je vlastně třeba, zda přímo souhlas dětí či jejich zákonných zástupců. K této otázce se velmi podrobně vyjádřil ÚOOÚ a to následovně: „*Vedle obecného rámce podmínek souhlasu subjektu údajů je nezbytné odkázat na úzkou souvislost*

¹¹⁰ Při zpracování osobních údajů správce a zpracovatel dbá, aby subjekt údajů neutrpěl újmu na svých právech, zejména na právu na zachování lidské důstojnosti, a také dbá na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů.

¹¹¹ *Niemietz vs. Německo*, rozsudek z 16.12.1992, [on-line] [cit.17.5.2013], dostupne z URL: <<http://spcp.prf.cuni.cz/judikat/es27-96.htm>>

*tohoto ustanovení s ustanovením § 8 ObčZ., který upravuje obecné podmínky pro posuzování zákonnosti projevů vůle, a to s ohledem na právní subjektivitu (způsobilost k právům a povinnostem) FO, která má souhlas se zpracováním svých osobních údajů učinit. Obecně by měla platit zásada uplatňovaná v občanském právu, která vychází z předpokladu, že tento souhlas poskytuje subjekt údajů, jehož se zpracování týká, přičemž se jedná o právní úkon, na který je nutné ve vztahu k žákům a studentům školy nahlížet ve smyslu ustanovení § 9 zákona č. 40/1964 Sb., ObčZ., ve znění pozdějších předpisů. Podle tohoto ustanovení mají nezletilí způsobilost pouze k takovým právním úkonům, které jsou svou povahou přiměřené rozumové a volní vyspělosti odpovídající jejich věku. Úřad je v této souvislosti přesvědčen, že dnešní studenti jsou od dosažení hranice 15 let věku již dostatečně rozumově a volně vyspělí, aby po řádném poučení dokázali s náležitou odpovědností posoudit, zda chtějí, aby jejich osobní údaje byly ve škole, ve které tráví většinu dne, zpracovávány prostřednictvím kamerového systému, a že by proto v tomto případě měl správce (škola) získávat souhlasy přímo od těchto studentů a nikoliv od jejich zákonných zástupců. Přičemž se však nedá vyloučit ani ta možnost, že rovněž rodiče náctiletých studentů budou náležitě informováni o nasazení kamerového sledování, o jeho účelu, době provozu a dalších skutečnostech, které školu k instalaci kamerového systému vedly. Závěrem však lze konstatovat, že i toto zpracování by bylo v rozporu se zákonem v případě, pokud by všichni studenti nebo všichni rodiče nebo zákonní zástupci žáků neposkytli škole souhlas s tímto zpracováním. Pro školu by tak vznikl těžko řešitelný problém, jak zajistit, aby v případě provozu kamerového systému byly zpracovávány osobní údaje jen těch osob, které souhlas poskytl.*¹¹²

Faktem však zůstává, že forma souhlasu není stanovena, nicméně tento souhlas by měl být zpětně dohledatelný, tudíž jako nejlepší se pak jeví forma písemná. Ohledně třetích osob vstupujících do prostor monitorovaných školou pak lze uplatnit onu výjimku § 5 odst. 2 písm. e) ZOOÚ, jelikož tyto osoby se v těchto prostorách nezdržují soustavně. Dále pak je třeba pamatovat na dikci § 316 odst. 2 Zákoníku práce, zákon č. 262/2006 Sb., ve znění pozdějších předpisů (dále jen ZP), která zaměstnavateli zakazuje

¹¹² Praktické otázky provozování kamerových systémů ve školách a školských zařízeních, ÚOOÚ, [online] [cit. 17.5.2013], dostupné na URL: <<http://www.uoou.cz/uoou.aspx?menu=14&loc=383#kamery>>

bez zvláštních důvodů narušovat soukromí zaměstnanců (tato problematika bude nastíněna v další části, kamerové systémy na pracovišti).¹¹³

Závěrem k nastínění této problematiky lze dodat, že vždy musí být splněny obecné požadavky ZOOÚ, které rozhodně nelze obcházet (všechny tyto požadavky jsou uvedeny v kapitole povinnosti správce). Tedy musí být stanoven účel zpracování osobních údajů. Tímto účelem může být pouze ochrana majetku, nikoliv sledování osob. Při instalaci kamerových systémů musí být dán závažný důvod, který musí správce při registraci u ÚOOÚ dostatečně obhájit. Doba zpracování by neměla přesáhnout dobu několika dnů, jako ideální se jeví doba 3 dnů, během kterých by jistě mělo případné nežádoucí chování vyjít najevo. Musí být dána pevná pravidla pro přístup ke kamerovému systému a tedy i osobním údajům, které jsou jejich prostřednictvím zpracovány. Rovněž musí být zajištěna dostatečná ochrana těchto záznamů před jejich zneužitím. Umístění kamerových systémů ve školách by mělo tedy reflektovat především právo na soukromí (obzvláště dětí) a to i s ohledem na výše zmíněný judikát ESLP, nemělo by tedy do soukromí nadměrně zasahovat.¹¹⁴

3.3.4 Kamerové systémy na pracovišti

Rovněž v problematice kamerových systémů na pracovišti, se střetávají dva zájmy, zájem zaměstnavatele na ochraně majetku (a efektivitě práce zaměstnance) a zájem zaměstnance na ochraně soukromí (zahrnuje rovněž ochranu cti, projevů osobní povahy aj.). Tak jako u jiných oblastí i zde je nutno hledisko práva na ochranu soukromí posuzovat jako právo esenciální, které je základem každého právního státu a požívá rovněž mezinárodní ochrany. Základem pro provoz kamerových systémů na pracovišti je zde dikce § 316, Zákon č. 262/2006 Sb., zákoník práce ve znění pozdějších předpisů (dále jen ZP) a to především odst. 1) až 3).¹¹⁵

¹¹³ BARTÍK V., JANEČKOVÁ E.: *Kamerové systémy v praxi. Právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. Praha, Linde 2011, 240 s. ISBN 978-80-7201-850-5. S. 100-117.

¹¹⁴ Tamtéž

¹¹⁵ § 316, Zákon č. 262/2006 Sb., zákoník práce ve znění pozdějších předpisů: (1) Zaměstnanci nesmějí bez souhlasu zaměstnavatele užívat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele včetně výpočetní techniky ani jeho telekomunikační zařízení. Dodržování zákazu podle věty první je zaměstnavatel oprávněn přiměřeným způsobem kontrolovat. (2) Zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci. (3) Jestliže je u

Jak lze vyčíst ze zmíněného ustanovení § 316 odst. 1) ZP, zaměstnavatel je oprávněn kontrolovat dodržování zákazů uvedených v tomto odstavci a to přiměřeným způsobem, zaměstnavatel se tedy může domnívat, že lze tuto kontrolu provádět pomocí kamerových systémů. Nicméně odst. 2) § 316 ZP pak stanovuje mantinely pro onu kontrolu, a to tak, že zaměstnavatel smí narušovat soukromí zaměstnance uvedeným způsobem pouze za předpokladu, že důvod k tomuto spočívá ve zvláštní povaze činnosti zaměstnavatele. Bohužel však ZP v tomto směru není více konkrétní, tedy určení toho co je či není zvláštní povahou činnosti zaměstnavatele je pak ponecháno na budoucí praxi soudů, tedy tomu, jak tento pojem vyloží. Lze však říci, že se nejspíše bude jednat o činnosti hodné zvláštní ochrany, např. práce s utajovanými informacemi, práce s penězi, know-how aj.¹¹⁶

Soukromí na pracovišti tedy není zcela nedotknutelné a jsou připuštěny určité výjimky. Pokud by povaha činnosti zaměstnavatele skutečně spadala pod uvedenou výjimku, bylo by chybou se domnívat, že naplnění této dikce postačí pro provozování kamerových systémů. I zde musí zaměstnavatel (tedy správce) splnit veškeré povinnosti, které mu ukládá ZOOÚ. Jako např. stanovení účelu, souhlas subjektu údajů, povinnost registrace u ÚOOÚ aj. Zároveň je nutno brát stále v úvahu ochranu soukromí (viz. již zmiňovaný judikát ESLP *Niemietz vs. Německo*). Navíc rozhodně i zde platí, že nesmí být monitorována místa, kde je předpokládána větší míra soukromí (šatny, toalety aj.). Musí být tedy stále respektována příslušná ustanovení na ochranu osobnosti, která jsou zakotvena v OZ. Závěrem lze dodat, že v případě, kdy by měl zaměstnanec pocit, že bylo porušeno jeho právo na soukromí a je do něj nadměrně zasahováno, může se obrátit na ÚOOÚ.¹¹⁷

3.3.5 Kamerové systémy instalované pro soukromý účel

Kamerové systémy instalované pro soukromý účel se ve společnosti objevují stále častěji. Důvodem bývá především získání důkazů pro případné dokázání protiprávního jednání. Stručně tedy lze shrnout, tak jako ve většině případů instalování

zaměstnavatele dán závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele, který odůvodňuje zavedení kontrolních mechanismů podle odstavce 2, je zaměstnavatel povinen přímo informovat zaměstnance o rozsahu kontroly a o způsobech jejího provádění.

¹¹⁶ BARTÍK V., JANEČKOVÁ E.: *Kamerové systémy v praxi. Právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. Praha, Linde 2011, 240 s. ISBN 978-80-7201-850-5. S. 63-78.

¹¹⁷ Tamtéž

kamerových systémů, že účelem je ochrana majetku, popř. jiných lidských hodnot před neoprávněnými zásahy.

Ve většině případů však bývá velmi problematické určit, zda je kamerový systém využíván v souladu s právem či nikoliv. Povětšinou se toto stanovuje podle míry zásahu do soukromí monitorovaných osob. K určení vhodnosti, nebo oprávněnosti se užívá testu proporcionality. Jde tedy o velmi specifickou oblast využití kamerových systémů.

S ohledem na výše uvedené lze rovněž konstatovat, že kamerové systémy instalované pro soukromý účel velmi často figurují v sousedských sporech (resp. nahrávky z těchto systémů). V dnešní době velmi rozvinuté techniky nepředstavuje žádný problém si takový kamerový systém pro svou vlastní potřebu pořídit, navíc tyto systémy jsou poměrně cenově dostupné, mohou být instalovány v podstatě kdekoli, na zahradě, na domě, ve společných prostorách bytových domů, mohou být skryté, nebo viditelné pouhým okem.

Právě při psaní této části vydal Nejvyšší soud ČR na svém květnovém zasedání sjednocující stanovisko, které se dotýká závažného porušování soukromí vlastníka nemovitosti (jde o rozsudek Nejvyššího soudu ze dne 30.10.2012, sp. zn. 22 Cdo 583/2011). Vzhledem k aktuálnosti jsem se tedy rozhodla toto stanovisko zařadit právě do této části. Zmiňované stanovisko se totiž dotýká tzv. imateriální imise.¹¹⁸

Zásahy do vlastnických práv upravuje § 127 odst. 1 OZ, jedná se v podstatě o generální klauzuli sousedských práv, které ukládá vlastníkům věci povinnost zdržet se zásahů do vlastnických práv jiného vlastníka, kterým by nad míru přiměřenou poměrům obtěžoval jiného. Nejvyšší soud již v minulosti ve svých stanoviscích konstatoval, že tzv. imateriální imise mohou být právně podstatně významné. Imisi tedy v tomto smyslu může být rovněž *obtěžování pohledem*.

Pro možnost nahlížet na obtěžování pohledem jako na imisi, musí daná situace splňovat podmínku mimořádnosti. Tedy, musí se jednat o takovou mimořádnou situaci, při které je závažným způsobem narušováno soukromí vlastníka, nebo v druhém případě pak uživatele sousední nemovitosti. Zpravidla se pak jedná o případy, kdy je vlastnické právo zneužíváno např. k nahlížení do sousedních nemovitostí, a to za účelem narušování soukromí. Jak také uvedl Nejvyšší soud, při posuzování věci je třeba

¹¹⁸ Imise jsou zásahy do vlastnického práva, dají se dělit na imise materiální a imateriální.

přihlížet k oprávněným zájmům všech účastníků řízení. Uvedené platí tím spíše pro fotografování či filmování osob, v tomto směru se totiž v jistém smyslu jedná o „obtěžování pohledem“, a toto je navíc umocněno právě tím, že tento pohled je zachycen technickými prostředky (např. kamerovým systémem).¹¹⁹

S ohledem na výše uvedené tedy Nejvyšší soud ČR zveřejnil dne 17.5.2013 tuto právní větu: „*Soustavné a závažné narušování soukromí vlastníka nebo uživatele nemovitosti fotografováním nebo pořizováním jiného obrazového záznamu může být imisí ve smyslu § 127 odst. 1 obč. zák.*“¹²⁰

Jako účinnou ochranu proti takovému jednání pak lze použít žalobu na ochranu osobnosti. Nicméně bohužel nutno konstatovat, že v některých případech se pak tato ochrana může částečně překrývat s ochranou poskytovanou právě ustanovením § 127 odst. 1 OZ., proti jednání vlastníka věci (fotoaparátu, kamery či jiného podobného zařízení). I s ohledem na to že jde o otázku, na kterou jsou v různých kruzích vyslovovány různé názory, je nutno vycházet z toho, že v pochybnostech je třeba dát přednost takovému výkladu, který chrání především „obtěžovaného“ účastníka oproti výkladu, který by poskytoval ochranu tomu, kdo jako vlastník věci jiného obtěžuje či ohrožuje výkon jeho vlastních práv (právo na soukromí, nerušené užívání vlastní nemovitosti).¹²¹

¹¹⁹ Stanovisko NS k závažnému narušování soukromí, [on-line] [cit. 17.5.2013], dostupné z URL: <http://www.nsoud.cz/JudikaturaNS_new/ns_web.nsf/web/Proverejnostamedia~Tiskovezpravy~Stanovisko_NS_k_zavaznemu_narusovani_soukromi~?openDocument&lng=CZ>

¹²⁰ tamtéž

¹²¹ tamtéž

4. Trestněprávní aspekty kamerových systémů

Kamerové systémy jsou ve většině případů zaváděny jako prevence kriminality, ochrana před neoprávněnými zásahy do práv FO a také velmi často mohou sloužit jako důkazní prostředek k prokázání viny pachatelů trestné činnosti. Vzhledem k výše uvedenému je následující část této práce věnována jejich trestněprávním aspektům, jelikož dle mého je pohled z hlediska trestního práva naprosto neopomenutelným. Přesto že moderní technika neochvějně postupuje vpřed, bohužel právo v této oblasti, dá se říci, stagnuje. Vývoj moderních technologií je bohužel tak rychlý, že právní úprava na tuto problematiku nestačí dostatečně rychle a flexibilně reagovat. Právě i díky tomuto je pohled na kamerové systémy z hlediska trestního práva značně omezený. Následující text se tedy bude ubírat přes úpravu hmotně právní a volně naváže na procesní úpravu.

Ohledně sankcí za nakládání s osobními údaji v rozporu se zákonem, lze říci hned na úvod, že tato právní úprava postihů v rámci trestního práva není dostatečná (vzhledem ke kamerovým systémům). Pokud je takové nakládání s osobními údaji v rozporu se zákonem, FO se pak mohou dopustit přestupku nebo TČ, právnické osoby (dále jen PO) a nebo podnikající FO pak jiného správního deliktu. Jak již bylo několikrát zmíněno, při nezákonném nakládání s osobními údaji dochází k porušování práva na ochranu osobnosti člověka. Náprava porušení těchto práv je v praxi poměrně obtížná (*stricto sensu* nemožná). Zmíněné přestupky a správní delikty jsou pak stanoveny v ZOOÚ. Obrátila jsem se ohledně trestní a sankční praxe s dotazem na organizaci Iuridicum Remedium, která se zabývá ochranou lidských práv v souvislosti (nejen) s moderními technologiemi. Bylo mi sděleno, že v praxi se prakticky neseťkávají s trestněprávními postihy při využívání kamerových systémů. Většina postihů je tak činěna ve sféře správního trestání ze strany ÚOOÚ. Teoreticky tedy připadá v úvahu postih podle § 180 zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů (dále jen TZ), a to například při masivnějších únicích záznamů z kamerových systémů.

4.1 Regulace trestním právem hmotným

Bohužel, v současné legislativě chybí dostatečná právní úprava TČ, které by reflektovali jednotlivé možnosti zneužití osobních údajů prostřednictvím kamerových

systemů, tedy např. sledování, utajené sledování aj., přesto, že takové TČ byli navrhované v novele TZ. K těmto úvahám se ale dostanu v závěrečné části své práce (Úvahy de lege ferenda). Nicméně TČ které by se mohli (nebo se vztahují) ke kamerovým systémům je třeba hledat ve zvláštní části TZ, a to v jeho hlavě II., TČ proti svobodě a právům na ochranu osobnosti.

V návaznosti na to, že zatím není dostatek literatury či odborných názorů na tuto problematiku a současně také není dostatečná praxe soudů, která by dané TČ přiřadila k problematice kamerových systémů, uvádím tedy pouze stěžejní § 180 TZ, který se vztahuje k osobním údajům, byť jen v souvislosti s výkonem veřejné moci a pro podrobnější představu uvádím případ z praxe, vztahující se ke kamerovým systémům a současně ke zmíněnému § 180 TZ, jedná se o mediálně velmi známou *Kauzu Savoy*.

4.2 Neoprávněné nakládání s osobními údaji

Jak je zřejmé z celé právní úpravy, která byla vylíčena v předchozích kapitolách, v případě kamerových systémů se záznamem se nepochybně jedná o zpracování osobních údajů. Tento TČ, vymezený v dikci § 180 TZ, byl vtělen již zákoníkem z roku 1961, následně byl doplněn v roce 1993 a upraven novelou z roku 2000. Dále byl pak pozměněn novelou TZ z roku 2009. Objektem TČ je zde zájem na ochraně dat před neoprávněným nakládáním (zveřejňováním a jiným zneužitím). Tato ochrana vyplývá z již několikrát zmiňovaného čl. 10 Listiny. Zvýšená potřeba trestněprávní ochrany je pak logickým důsledkem vývoje současné techniky a s tím související možností případného zneužití získaných údajů o konkrétní osobě. Avšak toto ustanovení se vztahuje pouze na neoprávněné nakládání s osobními údaji v souvislosti s výkonem veřejné moci.¹²²

Dikce § 180 TZ obsahuje dvě samostatné skutkové podstaty. První z nich je vymezena v odst. 1 následovně: „*Kdo, byť i z nedbalosti, neoprávněně zveřejní, sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje, které byly o jiném shromážděné v souvislosti s výkonem veřejné moci, a způsobí tím vážnou újmu na právech nebo oprávněných*

¹²² JELÍNEK, J. a kol.: Trestní právo hmotné. 2. vydání. Praha: Leges, 904 s. ISBN 978-80-87212-49-3. S. 539-540

*zájmech osoby, již se osobní údaje týkají, bude potrestán odnětím svobody až na tři léta nebo zákazem činnosti.*¹²³

První skutková podstata tedy chrání každý subjekt, před neoprávněným zveřejněním, sdělením, zpřístupněním či jiným zpracováním nebo přisvojením si osobních údajů, které byly o jiném shromážděny *v souvislosti s výkonem veřejné moci*. Veřejnou mocí se pak rozumí taková moc, která přímo či zprostředkovaně rozhoduje o právech a povinnostech jiných subjektů. Co je či není osobním údajem, bylo vysvětleno již v první kapitole této práce. Pokud pak jde tedy o pojem *osobní údaje shromážděné v souvislosti s výkonem veřejné moci*, může se jednat o údaje získané v souvislosti s přípravou voleb, údaje ze soudních a jiných statistik, údaje z databází vytvořených na základě údajů, které jsou občané povinni sdělovat aj.¹²⁴

Pojem *zveřejněný osobní údaj* podle dikce § 4 písm. f) ZOOÚ byl rovněž vymezen v první kapitole, nutno však dodat, že ono zveřejnění může být provedeno způsoby uvedenými v dikci § 180 odst. 3 písm. b) tedy *tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí či jiným obdobně účinným způsobem*. Naplnění této skutkové podstaty však již podmiňuje užití vyšší trestní sazby. Jedná se tak o doplnění znaku zveřejnění a způsobu provedení.¹²⁵

K naplnění dalšího znaku, tedy sdělení *osobních údajů* o jiném pak postačí neoprávněné sdělení o nashromážděných údajích alespoň jedné osobě vyjma poškozeného. Toto sdělení pak může být ústní, písemné, může být předáno na různých nosičích informací atd. Znakem zpřístupnění pak je, že pachatel z nedbalosti či úmyslně zpřístupní údaje o jiném jedné nebo více osobám, nejedná se však o zveřejnění. Pojem zpracování *osobních údajů*, který je rovněž uveden v dikci § 180 je také podrobně zpracován v první kapitole této práce.

Dalším bodem pak je pojem *přisvojení si osobních údajů*, což znamená získání takové možnosti, která ve svém důsledku znamená možnost s těmito údaji trvale pracovat (resp. disponovat). K naplnění tohoto znaku je třeba, aby šlo o přisvojení neoprávněné (př. nedovolené odnesení úložiště dat, které obsahuje osobní údaje, odeslání přes počítačovou síť na domácí počítač s účelem pozdějšího soukromého využití těchto údajů). Pro naplnění skutkové podstaty uvedené v § 180 pak nepostačuje

¹²³ § 180 odst. 1), Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů

¹²⁴ Šámal, P. a kol. Trestní zákoník II. § 140 až 421. Komentář. 2. vydání. Praha : C.H.Beck 2012, 2150 s. ISBN 978-80-7400-428-5. S. 1790-1798

¹²⁵ tamtéž

způsobení újmy na právech nebo oprávněných zájmech osoby, naopak je třeba, aby šlo o způsobení *vážné újmy*. Vážnou újmu tedy může být újma majetková i nemajetková. Pod majetkovou újmu je pak možno si představit ztráty v oblasti podnikání, snížení příjmu poškozeného, aj. Pod újmu nemajetkovou se může jednat o újmu na dobré pověsti, v rodinném životě, poškození dobrého jména aj. Vzhledem k okolnostem každého konkrétního případu je tedy velmi důležité dostatečně posoudit danou způsobenou újmu. Zvláště se zřetelem o jaký chráněný zájem či právo se jedná a jaká byla intenzita způsobené újmy. Rovněž je důležité se zabývat otázkou, jaké následky to mělo pro poškozeného, zda šlo o odstranitelný či neodstranitelný následek (nebo pouze částečně odstranitelný).¹²⁶

Z hlediska subjektivní stránky tohoto TČ lze dodat, že formulace „*byť i z nedbalosti*“ pak určuje, že je možné tento TČ spáchat jak úmyslně tak nedbalostně. Vždy je tedy třeba se zabývat formou konkrétního zavinění. Pachatelem tohoto TČ nemůže být PO (srov. § 7 TOPO¹²⁷), může jim být tedy kterákoli FO, která v rámci svého povolání přichází do styku s *osobními údaji* shromažďovanými v souvislosti s výkonem veřejné moci. Rovněž se pak může jednat o FO, která k daným údajům přišla náhodně (např. omylem zaslány na soukromý počítač) a nebo se k těmto údajům dostala záměrně (např. je koupí od jiného, rovněž přichází v úvahu hackerství).¹²⁸

Druhá skutková podstata se pak liší od první v tom, že se jedná o zveřejnění údajů získaných v souvislosti s výkonem povolání, zaměstnání, nebo funkce, jestliže tím pachatel porušil povinnost mlčenlivosti.

„Stejně bude potrestán, kdo, byť i z nedbalosti, poruší státem uloženou nebo uznanou povinnost mlčenlivosti tím, že neoprávněně zveřejní, sdělí nebo zpřístupní třetí osobě osobní údaje získané v souvislosti s výkonem svého povolání, zaměstnání nebo funkce, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají.“¹²⁹

Objektivní stránkou § 180 odst. 2 je, že osoba, která spáchá tento TČ je vázána státem uznanou či uloženou povinností mlčenlivosti, neoprávněně sdělí, zveřejní nebo jinak zpřístupní *osobní údaje* třetí osobě, které byly získané v souvislosti s výkonem

¹²⁶ Šámal, P. a kol. Trestní zákoník II. § 140 až 421. Komentář. 2. vydání. Praha : C.H.Beck 2012, 2150 s. ISBN 978-80-7400-428-5. S. 1790-1798

¹²⁷ Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, ve znění pozdějších předpisů

¹²⁸ Šámal, P. a kol. Trestní zákoník II. § 140 až 421. Komentář. 2. vydání. Praha : C.H.Beck 2012, 2150 s. ISBN 978-80-7400-428-5. S. 1790-1798

¹²⁹ § 180, odst. 2, Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů

svého povolání (zaměstnání či funkce) a tímto způsobí *vážnou újmu* na právech či oprávněných zájmech poškozené osoby, které se tyto údaje týkají. Státem uložená a uznaná povinnost mlčenlivosti, je pak definována v dikci § 124 TZ, je to taková mlčenlivost, která je uložena nebo uznána jiným právním předpisem. Za tuto státem uznanou mlčenlivost se podle TZ pak ale nepovažuje taková povinnost, jejíž rozsah není vymezen jiným právním předpisem, ale vyplývá z právního úkonu učiněného na základě jiného právního předpisu.¹³⁰

V případě druhého odstavce tedy platí, že osoba, která by případně *osobní údaje*, které byly nashromážděné v souvislosti s výkonem veřejné moci, bude trestně odpovědná, pokud by tím porušila státem uloženou nebo uznanou povinnost mlčenlivosti (např. advokáti, notáři, zdravotničtí pracovníci aj.). Ohledně zveřejnění, sdělení a zpřístupnění *osobních údajů* a vážné újmy na právech, se výklad shoduje s výkladem pro první odstavec tohoto paragrafu. Tento TČ může být rovněž spáchán jak nedbalostně, tak úmyslně. Pachatelem TČ může být rovněž pouze FO (srov. §7 TOPO). Podrobný popis možného pachatele rovněž shodný s prvním odstavcem.¹³¹

V odst. 3 je pak uvedena okolnost podmiňující vyšší trestní sazbu. Touto okolností je, že pachatel spáchá čin uvedený v odst. 1 a 2 jako člen organizované skupiny. Zde se pak již zvyšuje trestní sazba od jednoho roku do pěti let.

„Odnětím svobody na jeden rok až pět let, peněžitým trestem nebo zákazem činnosti bude pachatel potrestán,

- a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny,*
- b) spáchá-li takový čin tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem,*
- c) způsobí-li takovým činem značnou škodu, nebo*
- d) spáchá-li takový čin v úmyslu získat pro sebe nebo pro jiného značný prospěch“¹³²*

Organizovanou skupinou se zde rozumí sdružení více osob, které se vyznačuje určitou dělbou úkolů a činnost této skupiny se pak vyznačuje koordinovaností a

¹³⁰ § 124, Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů

¹³¹ Šámal, P. a kol. Trestní zákoník II. § 140 až 421. Komentář. 2. vydání. Praha : C.H.Beck 2012, 2150 s. ISBN 978-80-7400-428-5. S. 1790-1798

¹³² § 180, odst. 3, Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů

plánovitostí, čímž se rovněž zvyšuje možnost úspěšného provedení TČ. Organizovaná skupina nemusí mít trvalý charakter. Tímto způsobem lze spáchat TČ i jednorázově. Pro charakterizaci člena organizované skupiny není nutné, aby do ní vstoupil výslovně, postačí, že se do ní pachatel včlení a aktivně se tak podílí na její činnosti.¹³³

Tiskem se zde rozumí jak periodické (noviny, časopisy, bulletiny), tak neperiodické publikace (knihy, sborníky aj.). Jedná se o tiskoviny, jimiž se rozumí jakékoliv vyhotovení textu, znaku nebo obrazu vyhotoveného tiskem. Podstatnou náležitostí je vyhotovení tiskařským strojem, nebo jiným obdobným způsobem, tiskovinou tedy není například přepis na psacím stroji. Pod pojem film, lze zařadit všechny filmy určené k veřejné produkci. Nepatří sem pak televizní inscenace a televizní filmy, ty se vztahují k pojmu televize. Televizí se rozumí veřejnoprávní televize, soukromé televizní společnosti a rovněž společnosti satelitní a kabelové. Rozhlasem je zde vyjádřeno rozhlasové vysílání na všech vlnových frekvencích, rovněž rozhlas po drátě. Není směrodatnou informací, kdo je či není provozovatelem. Veřejně přístupnou počítačovou sítí je nutno rozumět určité funkční propojení počítačů do sítí s cílem vytvořit informační systém, který pracuje s tzv. dálkovým přístupem. Nejdůležitější veřejně přístupnou sítí je Internet, zahrnující i službu WWW (World Wide Web). Pokud se bude jednat o jiný obdobně účinný způsob, může jim být např. neoprávněné rozšiřování, zveřejňování, sdělování aj. za podmínky, že daný rozsah šíření *osobních údajů* je podobný jako u ostatních způsobů uvedených v § 180 odst. 3 písm. b).¹³⁴

Výkladové pravidlo pro značnou škodu je pak uvedeno v § 138 odst. 1) TZ, a jedná se o škodu, která dosahuje částky nejméně 500 000 Kč, z hlediska zavinění škody postačí zavinění nedbalostní (srov. § 17 písm. a) TZ. K úmyslu získat pro sebe či pro jiného značný prospěch, pak opět platí výklad § 138 odst. 1) a 2), tedy jedná se o prospěch dosahující částky nejméně 500 000 Kč. Značný prospěch může pachatel získat jak pro sebe, tak pro jiného. Z hlediska zavinění je nutný úmysl, k dokonání TČ však postačí jednání pachatele tento značný prospěch získat, není tedy třeba, aby byl TČ dokonán.¹³⁵

¹³³ Šámal, P. a kol. Trestní zákoník II. § 140 až 421. Komentář. 2. vydání. Praha : C.H.Beck 2012, 2150 s. ISBN 978-80-7400-428-5. S. 1790-1798

¹³⁴ Tamtéž

¹³⁵ Šámal, P. a kol. Trestní zákoník II. § 140 až 421. Komentář. 2. vydání. Praha : C.H.Beck 2012, 2150 s. ISBN 978-80-7400-428-5. S. 1790-1798

„Odnětím svobody na tři léta až osm let bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 1 nebo 2 škodu velkého rozsahu, nebo b) spáchá-li takový čin v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu“¹³⁶

V posledním odstavci § 180 je opět vyšší trestní sazba, která je podmíněna způsobením škody velkého rozsahu. Jedná se o nejvyšší možnou hranici škody uvedenou v TZ. Určení výše škody nutno hledat opět v dikci § 138 odst. 1), podle výkladu je tedy tato škoda v rozsahu nejméně 5 000 000 Kč. Z hlediska zavinění zde postačí zavinění nedbalostní. Pokud jde o prospěch velkého rozsahu, znovu se použije výklad § 138 TZ, tedy jedná se o prospěch v rozsahu nejméně 5 000 000 Kč. Prospěch může pachatel chtít získat jak pro sebe, tak pro jiného. Z hlediska zavinění je třeba úmysl (§ 17 písm. a TZ). K dokonání tohoto TČ však pachatel nemusí tohoto TČ dosáhnout, stačí, že jednal v úmyslu, tento prospěch velkého rozsahu pro sebe či pro jiného získat. Ohledně vztahu k jiným ustanovením, je možný jednočinný souběh s TČ pomluvy (§ 184 TZ) a TČ zneužití pravomoci úřední osoby (§ 329 TZ). Rovněž se zde pak zakládá trestní odpovědnost podle § 367 TZ, tedy za nepřekážení TČ ve smyslu § 180 odst. 4) TZ. Související ustanovení s tímto TČ, které se dle mého názoru mohou případně vztahovat i na oblast kamerových systémů (resp. osobních údajů těmito systémy zpracovanými) jsou dále ustanovení § 182 TZ porušení dopravovaných zpráv a § 183 TZ porušení tajemství listin a jiných dokumentů uchovávaných v soukromí.¹³⁷

4.3 Příklad z praxe – Kauza Savoy

Jedná se o poměrně mediálně velmi známou kauzu z roku 2008. Tento případ je zajímavý jak z hlediska trestního práva (§ 180 TZ), tak z hlediska provozování kamerových systémů a v neposledním případě také vzhledem ke svému politickému podtextu.

Případ se odehrál v lednu roku 2008. Centrem dění byl pražský hotel *Savoy*, který v té době nahrál prostřednictvím svých kamerových systémů setkání PhDr. Ing. J. Weigla, CSc. (člen Národní ekonomické rady vlády NERV, 2003–2013 vedoucí

¹³⁶ § 180, odst. 4, Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů

¹³⁷ Šámal, P. a kol. Trestní zákoník II. § 140 až 421. Komentář. 2. vydání. Praha : C.H.Beck 2012, 2150 s. ISBN 978-80-7400-428-5. S. 1790-1798

Kanceláře prezidenta republiky V. K.) s Ing. J. Šloufem (politický lobbista, bývalý poslanec KSČ, do roku 2009 vlivná postava ČSSD, působil např. jako vedoucí poradců bývalého premiéra, dnešního prezidenta ČR Miloše Zemana, jeho jméno figuruje v celé řadě politických skandálů). Nahrávka této schůzky se dostala do médií čtyři dny před prezidentskou volbou.

Toto zveřejnění pak mělo např. vliv na rozhodnutí o veřejné volbě prezidenta. Zároveň se tehdy spekulovalo o tom, že na jednání J. Weigla s J.Šloufem se diskutovalo o možnosti získat hlasy pro tehdejšího kandidáta ODS (Václava Klause) od sociálních demokratů. Z hotelu *Savoy* unikl videozáznam údajně díky P. Bakešovi (bývalý pracovník rozvědky) a J. Dvořákovi (bývalý policista). Bakeš údajně požádal Dvořáka o opatření záznamu z kamerového systému hotelu *Savoy* (23. ledna 2008). Druhý den policista záznam na DVD získal od marketingového ředitele hotelu, a to aniž by počkal na upřesňující písemnou žádost. Záznam získal díky smyšlené legendě o údajném zájmu policie na hledaných osobách. Toto DVD se záznamem z kamerových systémů hotelu *Savoy* následně pracovníkovi rozvědky Bakeš také předal. Kromě médií, se samozřejmě tento případ dostal také před soud. Následně tedy v prosinci roku 2009 se začal proces tzv. *kauzy Savoy* projednávat před Obvodním soudem pro Prahu 1. Dění v jednací síni však tehdy bylo neveřejné, jelikož státní zastupitelství předalo soudu obžalobu v režimu utajení. Do jednací síně tedy vcházeli pouze obvinění Bakeš a Dvořák, společně se svými obhájci. Oba muži čelili obžalobě z TČ zneužívání pravomoci veřejného činitele (dnes zneužití pravomoci úřední osoby § 329 TZ) a TČ neoprávněné nakládání s osobními údaji (§ 180 TZ, tento TČ podrobně rozebrán v předešlé kapitole).¹³⁸

Oběma mužům hrozil až pětiletý trest vězení. Verdikt však nepadl a jednání bylo odročeno na 11. února 2009. Oba muži byli však potrestáni již v červnu trestním příkazem, který Bakešovi uložil peněžitý trest 100 000 Kč a Dvořákovi 40 000 Kč. Navíc obviněný Bakeš dostal dvouletý zákaz činnosti. Dvořák pak roční zákaz činnosti. Oba obvinění však podali odpor. Definitivní konec této kauzy však byl potvrzen až v lednu 2012 před Městským soudem v Praze, kdy se Městský soud ztotožnil s obvodním soudem pouze v případě obviněného Bakeše, kterému potvrdil peněžitý

¹³⁸ Kauza hotelu Savoy, centrum.cz, [on-line] [cit. 1.6.2013], dostupné z URL: <http://aktualne.centrum.cz/tema/savoy-hotel_57010/?offset=1>

trest i zákaz činnosti a bývalého policistu Dvořáka obžaloby zprostil. Podle Městského soudu v Praze totiž Dvořák nevěděl, že Bakeš nahrávku nepoužije ke služebním účelům.¹³⁹

V neposlední řadě měla tato kauza rovněž dohru pro novinářku, která odmítla státnímu zástupci prozradit s odkazem na tiskový zákon (zákon č. 46/2000 Sb., o právech a povinnostech při vydávání periodického tisku a o změně některých dalších zákonů, ve znění pozdějších předpisů) zdroj, který ji poskytl danou nahrávku, kterou následně zveřejnila. Byla potrestána pokutou ve výši 20 000 Kč.

Tato poměrně zajímavá kauza hotelu *Savoy*, však měla dohru i pro samotný hotel. Právě medializace tohoto případu odstartovala kontrolu ÚOOÚ z hlediska zákonnosti provozování kamerových systémů. Přesto, že zde již nejsou patrné trestněprávní aspekty, zařazují spor ohledně oprávněnosti kamerových systémů rovněž na toto místo a to především z důvodu návaznosti.

Oprávněnost kamerových systémů hotelu *Savoy* se tedy následně stala předmětem soudního sporu, rovněž před Městským soudem v Praze. Žalobce (na rozsudku začerněn, nicméně jednalo se o majitele hotelu, tedy případného správce osobních údajů) se domáhal žalobou zrušení rozhodnutí předsedy ÚOOÚ, na základě svého přesvědčení, že byl tímto rozhodnutím zkrácen na svých právech. Rozhodnutím předsedy ÚOOÚ, byl totiž zamítnut rozklad žalobce, kterým nebylo povoleno zpracování osobních údajů prostřednictvím kamerových systémů. Důvodem pro zamítnutí bylo, že nespĺňoval podmínky stanovené ZOOÚ a tím by došlo k porušení již zmiňovaného ustanovení § 5 odst. 1 písm. e) a odst. 2 a § 10 tohoto zákona.

Žalobce ve své žalobě nejprve uváděl, že je provozovatelem hotelu s nabídkou služeb té nejvyšší úrovně a z důvodu minimálního zásahu do soukromí a zachování základní míry bezpečnosti zvolil složený kamerový systém a toto zpracování oznámil ÚOOÚ dne 22. února 2008. Dále pak žalobce tvrdil, že provoz kamerového systému sám o sobě nevede ke shromažďování osobních údajů, k nakládání s nimi a jeho provoz tedy automaticky nespádá pod režim ZOOÚ. A to ani v případě, že je pořizován zvukový nebo obrazový záznam. Dále upozornil, že přístup do hotelu není podmíněn žádným dalším identifikováním návštěvníků.

¹³⁹ Kauza hotelu *Savoy*, [on-line] [cit. 1.6.2013], dostupne z URL: <http://aktualne.centrum.cz/tema/savoy-hotel_57010/?offset=1>

Žalobce (majitel hotelu) ve své žalobě proti žalovanému (ÚOOÚ) dále namítal, že ÚOOÚ odmítá vnímat specifika provozu takového hotelu, a důvody pro zamítnutí zpracování osobních údajů prostřednictvím kamerového systému dostatečně nezdůvodnil. Žalobce poukazoval rovněž na to, že nesouhlasí se závěry ÚOOÚ uvedených v rozkladu, neboť se domnívá, že souhlasu subjektu údajů není třeba, a to na základě zákonných výjimek uvedených v dikci § 5 odst. 2 písm. a), b) a c) ZOOÚ, jelikož provoz kamerového systému je naprosto nezbytný pro ochranu práv a právem chráněných zájmů správce, příjemce a jiných dotčených osob. Dále pak namítal, že doba uchovávání záznamu je zcela přiměřená (8-12 dní) a nikoliv nepřiměřená, jak uvedl ÚOOÚ. Majitel hotelu sice souhlasil s tím, že zde jde o střet zájmů dvou základních lidských práv (práva na soukromí, práva vlastnit majetek a chránit ho). Nicméně také uvedl, že je přesvědčen že ÚOOÚ nesprávně uchopil svou diskreční pravomoc, když v případě hotelu *Savoy* významně zpřísnil vlastní výklady k podmínkám provozování kamerových systémů. Dále pak uváděl, že hosté o provozu kamerového systému vědí a nevnímají tyto systémy jako zásah do jejich soukromí.

ÚOOÚ jako žalovaný, pak k tomuto uvedl, že kamerový systém hotelu *Savoy* se nachází jak v prostorách hotelu, tak mimo ně. Kamerový systém tedy monitoroval vchod, vstupní halu recepce, vstupy do výtahů, vozovku před hotelem a to včetně zastávky MHD. Tyto údaje byly zpracovány na základě provozu kamerového systému, který pracuje v nepřetržitém provozu, záznam byl aktivován při detekci pohybu a zpracované údaje byly uchovávány po dobu 8-12 dní, a po té vymazány. ÚOOÚ konstatoval, že tyto záznamy byly pořizovány bez souhlasu subjektu údajů a rovněž bez splnění informační povinnosti správce vyplývající ze ZOOÚ.

ÚOOÚ konstatoval, že s námitkami majitele hotelu se vypořádal již v kontrolním protokolu a znovu odkázal majitele hotelu na dikci § 4 písm. a) ZOOÚ, tedy na definici pojmu osobní údaj. Zároveň konstatoval, že záznam lidské podoby resp. lidské tváře, umožňuje jasně určit lidskou identitu na základě jejích fyziologických znaků a to je také účelem, za kterým se kamerové systémy pořizují – tedy identifikace osob. Bez ohledu na to, zda je třeba pro identifikaci v souhrnu více údajů, jedná se o osobní údaj a ZOOÚ se na tento případ vztahuje a dále poukazoval na to, že základní identifikační znak lidské bytosti je její vzhled. Dále poukazoval na to, že záznamy z hotelu *Savoy* byli tak kvalitní, že snímané osoby lze nepochybně určit a krom toho, ze

záznamů bylo možné určit řadu známých osobností a osoby majiteli hotelu blízké a je tedy postaveno na jisto, že lze tak shromažďovat jejich citlivé údaje.

Dále pak ÚOOÚ nesouhlasil s názorem majitele hotelu v tom, že na něj nedopadá § 5 odst. 2 písm. e) a není tedy třeba souhlasu subjektu údajů se zpracováním osobních údajů. Dále konstatoval, že souhlas se zpracováním osobních údajů je podmíněn poskytnutím všech relevantních informací o předmětném zpracování subjektu údajů a to včetně práva na námitku proti jejich zpracování, což praxe hotelu *Savoy* rozhodně nesplňovala.

Majitel hotelu dále pak odkazoval na § 433 OZ¹⁴⁰, nicméně ÚOOÚ v souvislosti s tímto ustanovením konstatoval, že toto ustanovení by opravňovalo žalobce pouze na sledování těch míst, kam by byly věci případně uloženy (místa k tomu určená) a nikoliv ke sledování hostů, návštěvníků, zaměstnanců, navíc v restauraci, chodbách, baru či navíc místa mimo hotel. ÚOOÚ majitele dále upozornil, že v souladu s dikcí § 316 ZP, nesmí být zaměstnanci cílem sledování.

Městský soud v Praze tedy přezkoumal žalobou napadené rozhodnutí a rovněž jemu předcházející řízení před správním úřadem (ÚOOÚ), z hlediska všech žalobních námitek a dospěl k závěru, že žaloba majitele hotelu proti ÚOOÚ není důvodná.

Stěžejní námitkou žalobce namítal, že kamerový systém se záznamem tak jak byl navržen, nevedl ke shromažďování osobních údajů, není nakládáním s nimi a to ani když je pořizován a uchováván zvukový či obrazový záznam a teprve kombinace s jiným systémem by vedla k tomu, že z podobizen se stává osobní údaj. Této námitce soud nepřisvědčil, neboť o osobní údaje se v daném případě jednalo, jak také uvedly i správní orgány ve svých rozhodnutích. Soud tedy odkázal na znění § 4 písm. a) ZOOÚ na vysvětlení pojmu co je vlastně osobní údaj a dále na § 4 písm. e) téhož zákona, co je zpracováním osobních údajů.

¹⁴⁰ § 433 (1) Provozovatel poskytující ubytovací služby odpovídá za škodu na věcech, které byly ubytovanými fyzickými osobami nebo pro ně vneseny, ledaže by ke škodě došlo i jinak. Vnesené jsou věci, které byly přineseny do prostor, které byly vyhrazeny k ubytování nebo k uložení věcí, anebo které byly za tím účelem odevzdány provozovateli nebo některému z pracovníků provozovatele. (2) Je-li s provozováním nějaké činnosti zpravidla spojeno odkládání věcí, odpovídá ten, kdo ji provozuje, fyzické osobě za škodu na věcech odložených na místě k tomu určenému nebo na místě, kam se obvykle odkládají, ledaže by ke škodě došlo i jinak. (3) Odpovědnosti podle odstavců 1 a 2 se nelze zprostit jednostranným prohlášením ani dohodou. Zákon č. 262/2006 Sb., zákoník práce ve znění pozdějších předpisů

Soud při hodnocení důvodnosti námitky vycházel z toho, že žalobce nainstaloval kamery se záznamem, a to jak sám žalobce uvedl za účelem zpracování osobních údajů. Pokud tedy dochází k záznamu určitého prostoru a v důsledku toho i k záznamu pohybu jednotlivých osob (resp. jejich podoby), jde jednoznačně o shromažďování osobních údajů, neboť osoby zachycené na záznamu mohou být následně identifikovány. Soud nesohlasil ani s námitkou žalobce, že záznam podobizny se stává osobním údajem až v kombinaci kamerového systému s jiným systémem (př. písemná evidence, čipová karta), neboť osobu lze jistě identifikovat jen na základě jejího vzhledu. Režim kamerového systému tak, jak jej provozoval žalobce tedy režimu dle ZOOÚ podléhá.

Rovněž soud neshledal důvodnou námitku žalobce, že v tomto případě výslovný souhlas subjektu údajů se zpracováním osobních údajů není potřeba a aplikace výjimek uvedených v dikci § 5 odst. 2 ZOOÚ je vyloučena. Nicméně žalobce tento souhlas po subjektech údajů vůbec nepožadoval, a toto jednání odůvodňoval, jak bylo uvedeno již výše tím, že na něj dopadá výjimka dle dikce § 5 odst. 2 písm. a), b), c) a e) ZOOÚ. Ani s jednou z uvedených výjimek se soud neztotožnil a uvedl následující.

Pokud jde o výjimku dle písm. b), dospěl soud k závěru, že není žádná konkrétní smlouva, která by nasvědčovala, že zpracování osobních údajů subjektu údajů je nezbytné pro její plnění. Ohledně písm. a) se soud ztotožnil se závěry správního orgánu, tedy že odpovědnost žalobce za vnesené věci dle § 433 a násl. OZ, se vztahuje pouze na věci, které se nacházejí na místech určených k odkládání věcí, tedy např. v šatně. Dále soud uvedl, že na daný případ se nevztahuje ani výjimka dle písm. a). K námitce žalobce o výjimce dle písm. e), soud nepřisvědčil námitce žalobce, že provozování kamerového systému je nezbytné pro ochranu majetkových zájmů žalobce, ale i dalších práv a právem chráněných zájmů třetích osob, včetně samotných subjektů údajů, v důsledku čehož není třeba jejich souhlasu.

Dále soud uvedl, že Listina zaručuje všem jak nedotknutelnost osoby a jejího soukromí a právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě (čl. 7 a čl. 10 odst. 3), tak právo vlastnit majetek a právo na jeho ochranu (čl. 11 odst. 1). Soud již dříve judikoval, že při střetu dvou zájmů (zájem na ochraně soukromí a ochraně majetku), je nutné větší váhu přiznat zájmu na ochraně soukromí, jak jednomu ze základních lidských práv (př. rozsudek ze dne 28.2.2007, sp. zn. 7 Ca 204/2005 a ze dne 30.11.2009, č.j. 11 Ca 298/2008-47).

Postup žalobce, který v podstatě nadřadil zájem na ochraně před drobnými krádežemi, vandalstvím a případným excesem některého z návštěvníků nad právo na ochranu soukromí a osobního života, je podle soudu naprosto nepřipustný a neproporcionální ve vztahu k veřejnému zájmu, který žalobce údajně prosazoval.

Po zvážení všech podstatných okolností dopěl Městský soud v Praze k závěru, že v tomto případě byla naprosto bezdůvodně dána přednost právu na ochraně majetku před ochranou soukromí a práva na ochranu před neoprávněným shromažďováním, zveřejňováním, nebo jiným zneužíváním údajů o své osobě (viz. též rozhodnutí Ústavního soudu ČR, č.j. IV ÚS 154/97).

Soud dále poukazoval na argument žalobce, že v tomto případě postačí pouze souhlas konkludentní, který subjekt údajů dá tím, že do hotelu vstoupí a rovněž v tomto případě se s argumenty žalobce neztotožnil. Kamerovým systémem se záznamem instalovaným v hotelu, může dojít k zásadnímu zásahu do soukromý monitorovaných osob, a proto jistě nemůže postačovat jako souhlas ve smyslu ZOOÚ pouhé konkludentní jednání, čili srozumění se stavem, který žalobce instalováním zmíněného kamerového systému nastolil.

K námitce žalobce, že doba uchovávání záznamů po 7 dní je zcela přiměřená, a naopak doba 3 dnů navrhovaná žalovaným není dostatečná soud uvedl následující. To že neobsahuje ZOOÚ ani jiný právní předpis přímo popisná pravidla pro použití kamerových systémů, neznamená to, že si každý může stanovit vlastní pravidla zcela libovolně, ale bezpodmínečně musí vyhovět obecným podmínkám, kladeným na uchovávání záznamů obecně a to dle ustanovení § 5 odst. 1 písm. e) ZOOÚ. Tedy uchovávat osobní údaje pouze po dobu přiměřenou účelu. Pokud tedy žalobce uvedl, že účelem bylo zamezení protiprávních jednání v hotelu (krádeže, ostatní delikty), soud se přiklonil k názoru ÚOOÚ, tedy že doba 7 dnů je nepřiměřená a zvyšuje nebezpečí zneužití uchovávaných záznamů. Městský soud tedy posoudil všechny námitky žalobce a žalobu proti rozhodnutí ÚOOÚ zamítl jako nedůvodnou.¹⁴¹

Kauzou *Savoy* jsem chtěla především manifestovat komplikovanost právní úpravy kamerových systémů, a jejich velmi snadné zneužití. V případě hotelu *Savoy*, kontrolu hotelu odstartovala až medializace úniku nahrávek, což názorně předkládá momentální nedostatečnou kontrolu nad provozem kamerových systémů.

¹⁴¹ Rozsudek Městského soudu v Praze, č.j. 11 Ca 433/2008, [on-line] [cit. 10.6.2013], dostupné z URL: <http://www.uouu.cz/files/judik_rozsudek_ms_-_hotel.pdf>

4.4 Trestněprocesní aspekty kamerových systémů

Tato část práce, je věnována trestněprocesním aspektům kamerových systémů a to především jejich roli při dokazování trestné činnosti. Jedná se o aspekt velmi problematický, neboť tak jako v ostatních případech, je vždy naráženo na právo na soukromí (pachatele) a právo vlastnit majetek a také ho chránit. Úvod k této kapitole pak tvoří shrnutí základních zásad dokazování v trestním řízení a volně přechází k příkladům z praxe, které se týkají kamerových systémů.

4.4.1 Důkaz a dokazování v trestním řízení

Dokazování v trestním právu procesním je postup orgánů činných v trestním řízení (dále jen OČVTŘ), upravený TŘ, který směřuje k poznání všech skutečností, které jsou důležité pro rozhodnutí ve věci samé. Jde tedy o opatření důkazů o skutečnostech, které jsou důležité pro trestní řízení. Dále jde o provedení (zachycení a zhodnocení) těchto potřebných důkazů, a to v hlavním líčení a veřejném zasedání soudu, a to zásadně za aktivní role stran obžaloby (státního zástupce) a obhajoby (obviněný zpravidla zastoupený obhájcem). Postup je upraven příslušnými normami TŘ, které tak tvoří důkazní právo. Pod pojmem důkazní právo chápeme souhrn norem trestního práva procesního, které se vztahují k samotnému dokazování. V procesním slova smyslu začíná dokazování již v přípravném řízení. Účelem dokazování je tedy dostatečně zjistit skutkový stav věci, a to v rozsahu, který je nezbytný pro rozhodnutí OČVTŘ. *Důkazními prostředky* pak rozumíme např. výslech obviněného, svědka nebo znalce, rovněž znalecké posudky, ohledání osob nebo věcí, aj., z čehož OČVTŘ čerpají poznatky a dále je zachycují (resp. fixují) sepsáním protokolu nebo jiným vhodným prostředkem, kterým může být např. audiozáznam nebo videozáznam. Pramenem důkazů pak rozumíme nositele informací, z nichž se čerpá poznatek, který je důležitý pro předmět dokazování. Tímto pramenem dokazování pak mohou být *osoby* (obviněný, svědek, znalec aj.) nebo *věci* (listiny, předměty aj.). Důkazem se pak rozumí přímý poznatek, nebo výsledek činnosti OČVTŘ při dokazování. Jedná se o takový přímý poznatek, či výsledek, který byl získán procesním dokazováním OČVTŘ o skutkové okolnosti, která se stala v minulosti a je třeba ji dokázat. Z hlediska vymezení pojmu *důkaz* pak nutno uvést, že i nepravdivý, nezávažný, nebo dokonce nezákonný důkaz je v procesním slova smyslu důkazem a příslušný OČVTŘ se s tímto důkazem musí

v souladu s TŘ vypořádat. Z hlediska rozlišení *důkazních prostředků* a *důkazu*, je pak důkazní prostředek trestněprocesní formou poznávání a *důkaz* je obsahem tohoto poznávání a je tedy základem skutkového zjištění OČVTŘ. Vzhledem k uvedenému je třeba konstatovat, že je zde velmi úzká souvislost, která velmi často vede k tomu, že mezi těmito pojmy není rozlišováno a pro oba dva pojmy se užívá pojmu *důkaz*. S ohledem na fakt, že každý procesní důkaz je velmi úzce spojen s určitou osobou či věcí, je termín důkaz užíván dokonce i ve smyslu pramene (nositele) důkazu, a to jak v literatuře, tak v legislativě i praxi. Což ve svém významu nemá negativní dopad, neboť z kontextu je zřejmé, zda se tak činí ve smyslu důkazního prostředku, pramene důkazu či důkazu v užším slova smyslu.¹⁴²

Z hlediska ústavního zakotvení základních zásad dokazování, je třeba zmínit Listinu, Úmluvu a Mezinárodní pakt o občanských a politických právech (vyhláška Ministerstva zahraničních věcí č. 120/1976 Sb.

Základní zásadami dokazování jsou:

- **Zásada presumpce nevinny (§ 2 odst. 2)** – vyjadřuje, že vina obviněného, resp. obžalovaného má být úplně a nepochybně prokázána v průběhu dokazování během hlavního líčení
- **Zásada vyhledávací (§ 2 odst. 5)** – OČVTŘ jsou povinny zjišťovat důkazy důležité pro trestní řízení, a to ať už svědčí v prospěch nebo neprospěch obviněného (i bez návrhu stran)
- **Zásada ústnosti (§ 2 odst. 11)** – vychází z toho, že důkazy v hlavním líčení a ve veřejném zasedání se zpravidla provádějí ústně (formou výpovědí). Listiny a protokoly o úkonech, kterými se provádí dokazování musí být přečteny. Důvodem je, že ústním provedením se vytvářejí ty nejlepší předpoklady pro náležité zjištění skutkového stavu věci. TŘ připouští i výjimky (§ 102 odst. 2 aj.)
- **Zásada bezprostřednosti (§2 odst. 12)** - požadavek, aby soudce v hlavním líčení přímo vnímal dokazované skutečnosti (zásadní význam pro naplnění zásady volného hodnocení důkazů a zjištění skutkového stavu věci), souvisí s naplněním pravidla, že *soud má čerpat důkazy z pramene pokud možno*

¹⁴² Musil, J., Kratochvíl, V., Šámal, P., a kol. Kurs trestního práva. Trestní právo procesní, 3. přepracované a doplněné vydání. Praha C.H.Beck, 2007, 1211 s. ISBN 978-80-7179-72-8. S. 373-379.

nejbližšího dokazované skutečnosti, (pravidlo nezměnitelnosti složení soudu, neporušitelnosti soudního jednání)

- **Zásada volného hodnocení důkazů (§ 2 odst. 6)** – protiklad dříve uznávané důkazní teorie, OČVTŘ hodnotí jednotlivé důkazy na základě svého vnitřního přesvědčení, založeného na pečlivém zvážení všech okolností daného případu, nejsou vázáni ničím jiným než zákonem a vlastním přesvědčením
- **Zásada zjištění skutkového stavu bez důvodných pochybností (§ 2 odst. 5)** – OČVTŘ provádějí dokazování jen v takovém rozsahu, který je nezbytný z hlediska zjištění skutkového stavu věci pro konkrétní rozhodnutí (zásada materiální pravdy)

Předmět a rozsah dokazování:

V dikci § 89 odst. 1 TŘ je pak vymezen předmět dokazování. Tímto předmětem se rozumí okruh skutečností, které je nutno dokázat, a které jsou přímo či nepřímo důležité pro rozhodnutí. Podle zmíněné dikce je tedy třeba dokazovat zejména:

- zda se stal skutek, v němž je spatřován trestný čin
- zda tento skutek spáchal obviněný, případně z jakých pohnutek
- podstatné okolnosti mající vliv na posouzení povahy a závažnosti činu
- podstatné okolnosti k posouzení osobních poměrů pachatele
- podstatné okolnosti umožňující stanovení následku, výše škody způsobené TČ a bezdůvodné obohacení
- okolnosti, které vedly k trestné činnosti nebo umožnily její spáchání

Důkazní prostředky

Jak je uvedeno v dikci § 89 odst. 2 TŘ, **platí, že za důkaz může sloužit vše, co může přispět k objasnění věci.**¹⁴³ Obecně lze říci, že TŘ nepovažuje určitý druh důkazních prostředků za průkaznější než jiný. Význam každého důkazního prostředku tedy závisí na povaze, druhu nebo důkazní hodnotě ostatních získaných důkazních

¹⁴³ § 89, odst. 2) Za důkaz může sloužit vše, co může přispět k objasnění věci, zejména výpovědi obviněného a svědků, znalecké posudky, věci a listiny důležité pro trestní řízení a ohledání. Každá ze stran může důkaz vyhledat, předložit nebo jeho provedení navrhnout. Skutečnost, že důkaz nevyhledal nebo nevyžádal orgán činný v trestním řízení, není důvodem k odmítnutí takového důkazu. Zákon č. 141/1961 Sb., trestní řád, ve znění pozdějších předpisů

prostředků. Je třeba důkazní prostředky také vždy posuzovat ve vztahu ke konkrétní věci a také jak společně s ostatními důkazy potvrzuje či vyvrací dokazovanou skutečnost. Lze tedy shrnout, že k dokázání jakékoliv skutečnosti, lze použít každého důkazního prostředku, TŘ totiž nespecifikuje, kterým důkazním prostředkem by měla či neměla být dokázána konkrétní skutečnost (s výjimkou některých případů, např. § 105 odst.)¹⁴⁴

4.4.2 Použitelnost záznamu z kamerového systému jako důkazního prostředku v trestním řízení

Koncepce celé mé diplomové práce je pojata tak, aby bylo patrné, že právní úprava kamerových systémů je v celkovém pojetí značně nedostatečná a rozkolísaná. Zákonodárce není schopen s dostatečnou rychlostí reagovat na stále rychlejší vývoj techniky a její stále častější použití pro soukromé využití. Nepochybně lze říci, že cílem instalace soukromých kamerových systémů je ve většině případů (když vynechám úvahy nad jejich účinností v prevenci kriminality), opatření důkazů o protiprávním jednání pachatele. Cílem je tedy zaznamenání pachatele při protiprávním jednání, kdy např. neoprávněně poškozuje cizí majetek. Ve chvíli kdy se podaří takové nezákonné jednání onoho pachatele zaznamenat, přichází na řadu otázka, zda je vůbec možné takový důkaz použít a zda je tento důkaz vůbec schopný obstát. Pochybnosti je možno spatřovat zejména již v několikrát zmiňované ústavní rovině práva na ochranu soukromí. V občanskoprávní rovině pak nutno znovu zmínit § 12 OZ s odkazem na ochranu osobnosti.

V případě užití důkazu formou nahrávky z kamerového systému pak dochází ke kolizi několika práv, s právem na ochranu osobnosti a soukromí v kontrapozici k právu vlastnit majetek a také ho chránit. Rovněž může být často namítáno právo na spravedlivý proces (jak ze strany poškozeného, tak ze strany pachatele). Na možnost použití těchto záznamů lze nahlížet z hlediska správního nebo soudního (ať trestního či občanského). Já se v této části zaměřím stěžejně na důkaz nahrávkou v trestním řízení. Nicméně vzhledem k poměrně rozkolísané judikatuře se často odvětví mohou prolínat.

¹⁴⁴ Musil, J., Kratochvíl, V., Šámal, P., a kol. Kurs trestního práva. Trestní právo procesní, 3. přepracované a doplněné vydání. Praha C.H.Beck, 2007, 1211 s. ISBN 978-80-7179-72-8, S. 417-419

Jsem toho názoru, že závěry soudů vzhledem ke každému odvětví mohou být přínosné, a tak ani zde (i s ohledem na mé téma), nevylučuji, že se pro srovnání zmíním o stavu např. s ohledem na správní právo, směřem k prokazování přestupků aj., jelikož se domnívám, že správní trestání má k trestnímu právu podstatně blízko.

Jak bylo uvedeno již ve stručném shrnutí základů trestního práva procesního, resp. základů dokazování v trestním řízení, pro případy trestního práva procesního platí dikce ustanovení § 89 odst. 2 (srov. § 125 OSŘ), tedy že *za důkaz může sloužit vše, co může přispět k objasnění věci*. Poměrně jasná zásada, kdy si každý může nepochybně říci, že s ohledem na toto ustanovení, je jistě zajištění důkazu prostřednictvím kamerových systémů v pořádku a není třeba nad tím více uvažovat. Proč by takový důkaz neměl být také proveden. Když samotná nahrávka může být v řadě ohledů nejprůkaznějším materiálem pro dokázání protiprávního jednání. To jistě může, ale jen do chvíle, kdy pachatel namítne, že daný záznam, kterým má být prokázána vina, zasahuje do jeho práva na soukromí. Případně může namítat (a velmi často také namítá) že onen případný záznam byl použit (resp. získán) bez jeho souhlasu, tedy záznam byl získán v rozporu se zákonem a je tedy pro trestní řízení nepoužitelný.

Pak zůstává na moci zákonodárny, jak se s tímto argumentem vypořádá. Z hlediska zdravého rozumu, se pak zdá tato námitka skutečně námitkou ad absurdum. Případný pachatel TČ porušuje práva jiných svým protiprávním jednáním a v případě možného usvědčení záznamem z kamerového systému se pak dovolává ochrany svého nezákonného jednání, neboť by tím bylo porušeno jeho právo na soukromí. V praxi by to tedy podle některých pachatelů (někdy i praxe soudů) mohlo vypadat tak, že v případě kdy zjistím, že dochází k neoprávněnému zásahu do mého majetku, rychle přispěchám k onomu pachateli a slušně se ho dotážu, zda by souhlasil se zaznamenáním jeho protiprávního jednání. Pro případnou platnost souhlasu pak bude lepší, když nám pachatel udělí souhlas písemný. Logicky je to nesmysl, samozřejmě. Ne v každém případě se k tomu tak soudy ovšem staví, nicméně se stoupajícími případy, vztahujícími se k této problematice, i judikatura v tomto směru spěje vpřed, především tedy v trestním a správním řízení.

I když může výše uvedené znít sebevíc absurdně, jedná se bohužel o běžnou praxi. Přesně takovým případem, o kterém bylo pojednáno výše, kdy se pachatel TČ domáhá ochrany svého soukromí, je případ z roku 2007. Pachatel TČ byl uznán vinným

TČ poškozování cizí věci, podle § 257 odst. 1 TZ na skutkovém základě, že záměrně vpravil neznámou hmotu, o které věděl, že zatuhne a způsobí tak nevrtané znehybnění a nefunkčnost do celkem sedmi zámků (vstupních dveří domů, prodejny) a rovněž do dvou zámků osobního automobilu. Jediným přímým důkazem zde byl záznam z průmyslové kamery poškozeného. Rozsudkem Okresního soudu v Přerově (dále jen OS Přerov) byl tedy pachatel uznán vinným a byl mu uložen trest odnětí svobody ve výši osmi měsíců. Obviněný se proti rozsudku odvolal a Krajský soud v Brně napadený rozsudek zrušil ve výroku o trestu a způsobu jeho výkonu a pachatele odsoudil k výkonu trestu v trvání čtyř měsíců. Načež pachatel reagoval dovoláním podaným k Nejvyššímu soudu (dále jen NS). Záměrně zde vynechám nepodstatné argumentace onoho pachatele (jako např. podjatost soudů) a zaměřím se přímo na použití záznamu z kamerového systému jako důkazu.

V odvolání k NS opřel dovolatel svou argumentaci na námitce procesní neúčinnosti důkazu, neboť kamerový systém, ze kterého pocházel záznam, měl poškozený nainstalovaný bez povolení ÚOOÚ (nezákonný důkaz opatřený přestupkem) a bez tohoto záznamu by tedy nebyl k dispozici žádný přímý důkaz. NS dospěl k závěru, že soudům nelze po procesní stránce nic vytknout a k poslední otázce, tedy týkající se záznamu z kamerových systémů jako důkazu soud uvedl v právní větě následující: „ *S ohledem na ustanovení § 89 odst. 2 tr. ř. lze za důkaz použitelný v trestním řízení pokládat též obsah obrazového záznamu z kamerového systému, který poškozený nainstaloval za účelem zjištění identity osoby poškozující jeho majetek (např. jeho obydlí, jeho automobil). V takovém případě zpravidla nepředstavuje jednání poškozeného nepřijatelný zásah do soukromí zaznamenané osoby, který by znamenal neúčinnost takového důkazu, i když instalaci záznamového zařízení a jeho provoz neoznámil Úřadu pro ochranu osobních údajů podle § 16 odst. 1 odst. 2 zák. č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů. Přípustnost takového důkazu je však nezbytné vždy posuzovat i s přihlédnutím k právu na soukromí zakotvenému v čl. 8 Úmluvy o ochraně lidských práv a základních svobod a na nedotknutelnost osoby a jejího soukromí ve smyslu čl. 7 a čl. 10 odst. 2 Listiny základních práv a svobod.*“¹⁴⁵

¹⁴⁵ usnesení Nejvyššího soudu ze dne 03. 06. 2009, sp. zn. 3 Tdo 593/2009, uveřejněný pod č. 22/2010 Sbírky soudních rozhodnutí a stanovisek, [on-line] [cit.14.6.2013], dostupné na URL:

NS dovolání odmítl na základě podání z jiného důvodu, než je uvedeno v zákoně. Nicméně výše zmíněný pachatel trestného činu podal ústavní stížnost, ve které se rovněž domáhal zrušení výše uvedených rozsudků obecných soudů s tím, že bylo dotčeno jeho právo na spravedlivý proces (čl. 36 listiny), dále že byl porušen zákaz stíhání a zbavení osobní svobody jinak než z důvodů a způsobem, který stanoví zákon, (článek 8 odst. 2 Listiny), a konečně *bylo zasaženo do stěžovatelova práva na soukromí zaručeného články 7 a 10 Listiny*. Stěžovatel opět namítal, že jediným přímým důkazem, který jej měl usvědčovat ze spáchání trestného činu, je videozáznam pořízený kamerovým systémem poškozeného u jedněch vstupních dveří. Stěžovatel byl toho názoru, že tento videozáznam byl získán v rozporu se zákonem, neboť byl pořízen bez jeho souhlasu, čímž bylo navíc *zasaženo do jeho práva na soukromí*, a dále pak proto, že poškozený nesplnil oznamovací povinnost dle ustanovení § 16 ZOOÚ, v důsledku čehož kamerový systém provozoval v rozporu se zákonem. Důkazní prostředek byl získán nelegálně, a tudíž byl v trestním řízení nepoužitelný. I pro případ, že by takový důkazní prostředek byl přípustný, nelze z něj dovodit, že stěžovatel všechny zámky poškodil, poněvadž je na něm zachycena pouze přítomnost stěžovatele u jednoho z poškozených zámků, aniž by bylo patrné, jakou činnost zde vykonává. Konečně stěžovatel uváděl, že obecné soudy dosud nerozhodly o jeho námitce podjatosti. Dále stěžovatel žádal, aby Ústavní soud (dále jen ÚS) přikázal OS v Přerově zničit videozáznam a fotografie pořízené kamerovým systémem poškozeného, které se nacházejí ve spise tohoto soudu, případně v souvisejících spisech PČR nebo okresního státního zastupitelství.

Po zvážení okolností předložené věci však ÚS dospěl k závěru, že podaná ústavní stížnost byla zjevně neopodstatněná. Dále však uvedl, že jako takový je oprávněn zjišťovat, zda byla či nebyla zachována procesní čistota řízení, která je jako podmínka zvláště výrazná v *trestním procesu*, který musí dostát všem zákonným požadavkům, aby bylo možné shledat jeho výsledek, k němuž se vedení trestního řízení upíná, zákonným a ústavně souladným. Podmínka procesní čistoty jako taková se uplatňuje i při dokazování. K tomuto se ÚS vyjádřil následovně: „*Jestliže při vyhledávání, opatřování nebo provádění důkazu došlo k porušení právního předpisu,*

<http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/BA7591FBECEBAC75C1257A4E00650559?openDocument&Highlight=0,3,tdo,593/2009>

kteře mělo povahu podstatné vady řízení, jedná se o důkaz absolutně neúčinný, a tedy nepoužitelný. Protože trestní řád neobsahuje žádnou kategorizaci takových vad (vyjma získání důkazu nezákonným donucením nebo hrozbou takového donucení), je nutné nepoužitelnost důkazů dovozovat výkladem v každém konkrétním případě zvlášť, a to především s ohledem na charakter vady řízení, vliv na konkrétní důkaz a význam tohoto důkazu pro řízení (srov. Šámal/Král/Baxa/Púry: Trestní řád - komentář, díl. I., 4. vydání. C. H. Beck 2002, s. 583-584). Ačkoli nesplnění oznamovací povinnosti dle ustanovení § 16 zákona o ochraně osobních údajů je přestupkem [srov. § 44 odst. 2 písm. i) citovaného zákona], nelze jej hodnotit jako porušení právního předpisu takové závažnosti, která by měla za následek absolutní neúčinnost důkazu získaného průmyslovou kamerou. Jedná se o formální pochybení v záležitosti administrativního charakteru ve vztahu ke správnímu orgánu, které však nutně neimplikuje neoprávněnost instalace záznamového zařízení či nepřípustnost důkazního prostředku takto pořízeného. Při posuzování námitky porušení práva na soukromí pořízením uvedeného záznamu lze dát za pravdu stěžovateli, že monitorování veřejného místa kamerou a následné pořízení trvalého záznamu spadá pod ochranu poskytovanou článkem 10 Listiny a článkem 8 odst. 1 Úmluvy o ochraně lidských práv a základních svobod (dále jen "Úmluva"). Obecně je pro účely hodnocení, zda došlo k nedovolenému zásahu do soukromí ze strany orgánů veřejné moci, nutno zkoumat, zda byla zaznamenána soukromá záležitost či veřejná událost a zda byl získaný materiál určen pro omezené použití či měl být dostupný široké veřejnosti (srov. odst. 58 rozsudku Evropského soudu pro lidská práva P. G. a J. H. proti Spojenému království ze dne 25. 9. 2001, č. 44787/98, dostupný na <http://echr.coe.int>). Běžné použití bezpečnostních kamer samo o sobě, ať na ulici nebo v prostorách jako nákupní centrum nebo policejní stanice, kde slouží legitimnímu a předvídatelnému účelu, není problematické z pohledu článku 8 odst. 1 Úmluvy (srov. odst. 40 rozsudku Perry proti Spojenému království ze dne 17. 7. 2003, č. 63737/00). Uvedené závěry jsou plně aplikovatelné na stěžovatelovu věc, neboť poškozený instalováním průmyslové kamery na veřejném místě sledoval legitimní cíl, tj. ochranu svého majetku a odhalení pachatele trestného činu, který by se jej osobně dotýkal. Pořízený záznam byl pak využit jen pro nezbytně nutný účel (prokázání viny stěžovatele v trestním řízení) a nebyl nijak zneužit, např. veřejným zpřístupněním záznamu, znevažováním stěžovatele ve sdělovacích prostředcích apod. Lze tedy uzavřít,

*že instalace průmyslové kamery a záznam jejím prostřednictvím získaný nenaplnuje znaky porušení stěžovatelova ústavně zaručeného práva na ochranu soukromí.*¹⁴⁶

V uvedených závěrech je tedy možno spatřovat jistý pozitivní přístup, v případě provádění důkazů prostřednictvím záznamů z kamerových systémů v trestním řízení. Dokonce jak uvedl NS ve své právní větě, podle § 89 odst. 2 TRŘ je možné, použít důkaz záznamem z kamerového systému v trestním řízení. Domnívám se, že je to v tomto směru velmi přínosný judikát, neboť pachatelů TČ dožadujících se ochrany soukromí stále přibývá. Nicméně v každém případě bude jistě soud používat jistého principu proporcionality, kdy se právo na ochranu soukromí nepovažuje za absolutně nedotknutelné, a budou mu směle konkurovat práva jiná (např. ochrana majetku). V praxi se rovněž objevuje názor, že takové případné odepření důkazu nahrávkou za kamerových systémů, je jistým druhem šikanózního výkonu práva, popř. lze takovéto odmítnutí považovat za rozpor s dobrými mravy. Možných argumentací je jistě mnoho a opět je jen na orgánech veřejné moci, jak k nim budou přistupovat.

Tuto problematiku zde doplním usnesením Nejvyššího správního soudu (dále jen NSS), sp.zn. 1 As 113/2012, kde bylo mj. odkazováno na výše zmíněná rozhodnutí a v souvislosti s problematikou instalace kamerových systémů byla tímto usnesením položena Soudnímu dvoru Evropské unie předběžná otázka. Na toto místo zařazuji zmíněné usnesení mj. proto, že na začátku sporu bylo pořízení záznamu za účelem získání případných důkazů pro trestní řízení proti pachatelům trestné činnosti. V tomto usnesení se jedná o žalobě proti rozhodnutí žalovaného ÚOOÚ, kdy žalobcem je FO.

Skutkový základ sporu v původním řízení spočíval v tom, že žalobce instaloval na rodinný dům ve výlučném vlastnictví své manželky v říjnu 2007 kamerový systém. K tomuto kroku přistoupil až poté, co neznámé osoby opakovaně několik let útočily na něj osobně, členy jeho rodiny a na výše zmíněný rodinný dům. Pachatele trestné činnosti se nikdy nepodařilo vypátrat. Je nesporné, že jediným důvodem pro instalaci kamerového systému byla ochrana majetku, zdraví a života žalobce a jeho rodiny. Tímto systémem byl snímán vstup do domu, veřejná ulice a vstup do protějšího domu. Systém umožňoval obrazový záznam, který byl ukládán do nahrávacího zařízení.

¹⁴⁶ K přípustnosti důkazu získaného bezpečnostním kamerovým systémem pro účely trestního řízení ve vztahu k právu na ochranu soukromí, usnesení ústavního soudu, IV.ÚS 2425/09 ze dne 8. 2. 2010, [online] [cit. 14.6.2013], dostupné z URL: <<http://nalus.usoud.cz/Search/GetText.aspx?sz=4-2425-09>>

K systému a jeho datům měl přístup pouze žalobce. V noci z 6.10 na 7.10. 2007 došlo k dalšímu útoku, který spočíval v rozbití okna rodinného domu výstřelem z praku. Díky kamerovému systému se podařilo identifikovat dvě podezřelé osoby. Následně jeden z podezřelých podal podnět k prověření kamerového systému žalobce. Tímto podnětem upozorňoval na to, že provoz systému nejspíše porušuje ZOOÚ.

ÚOOÚ následně ve svém rozhodnutí ze dne 4.8.2008 dospěl k závěru, že žalobce skutečně spáchal přestupky dle díkce § 44 odst. 2 písm. e), f) a i)¹⁴⁷ ZOOÚ. Těchto přestupků se dopustil tím, že jako správce osobních údajů shromažďoval pomocí kamerového systému instalovaného na svém domě osobní údaje osob pohybujících se po ulici před domem a vstupujících do domu na protější straně ulice, a to bez jejich souhlasu. Tyto osoby o prováděném zpracování neinformoval a ani jinak nesplnil informační povinnost správce osobních údajů uvedenou v § 11 odst. 1 ZOOÚ (pro jaký účel budou údaje zpracovány, kdo a jakým způsobem jejich zpracování provede, v jakém rozsahu a komu mohou být tyto údaje zpřístupněny). Dále pak jako správce osobních údajů nesplnil informační povinnost vůči ÚOOÚ podle § 16 odst. 1 téhož zákona. Na základě těchto skutečností byla žalobci uložena pokuta ve výši 1.500 Kč. Proti tomuto rozhodnutí podal žalobce rozklad. Předseda ÚOOÚ však uvedené rozhodnutí potvrdil.

Žalobce napadl výše uvedené rozhodnutí ÚOOÚ žalobou u Městského soudu v Praze, ten však žalobu jako nedůvodnou zamítl. V odůvodnění se plně ztotožnil s ÚOOÚ. Záznamy z předmětného kamerového systému obsahovaly informace týkající se určitelných subjektů údajů. Tímto způsobem tedy dochází ke ztotožnění zaznamenaných osob a jedná se tedy o osobní údaje. Uvedl, že v daném případě se nejedná o výjimku ze ZOOÚ dle § 3 odst. 3 (zpracování osobních údajů výlučně pro vlastní potřebu). Argumentoval tím, že dle soudu tento záznam *neměl sloužit pouze pro vlastní potřebu žalobce, ale naopak měl být předán policejnímu orgánu a následně tedy využit jako důkaz v trestním řízení.*

¹⁴⁷ § 44 odst. (2) Fyzická osoba se jako správce nebo zpracovatel dopustí přestupku tím, že při zpracování osobních údajů e) zpracovává osobní údaje bez souhlasu subjektu údajů mimo případy uvedené v zákoně (§ 5 odst. 2 a § 9), f) neposkytne subjektu údajů informace v rozsahu nebo zákonem stanoveným způsobem (§ 11), i) nesplní oznamovací povinnost podle tohoto zákona (§ 16 a § 27), Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů

Žalobce rozsudek městského soudu napadl včas podanou kasační stížností. V této stížnosti kromě mnoha jiných argumentů namítl, že na jeho případ se uvedená výjimka § 3 odst. 3 ZOOÚ vztahuje. Podle této výjimky, se ZOOÚ nevztahuje na případy, kdy zpracování osobních údajů provádí FO čistě pro vlastní potřebu. NSS dospěl k závěru, že předmětem sporu je mj. aplikovatelnost ZOOÚ na kauzu žalobce. Tedy zda dopadá na případ monitorování veřejného prostranství za účelem ochrany majetku a zdraví. Sporným je tedy výklad ustanovení § 3 odst. 3 téhož zákona, který dle práva EU dále provádí čl.3 odst.2¹⁴⁸ Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24.10.1995 o ochraně FO v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen směrnice).

K problematice předběžné otázky bylo uvedeno následující. Žalobce od počátku sporu tvrdí, že monitorování veřejného prostranství spadá v případě žalobce pod § 3 odst. 3 ZOOÚ, tedy že jde o zpracování výlučně pro vlastní potřebu žalobce, k souvztažnosti s čl. 3 odst. 2 směrnice 95/46/ES, kdy *tato směrnice se nevztahuje na zpracování osobních údajů prováděné FO pro výkon výlučně osobních či domácích činností*.¹⁴⁹ Proto podle žalobce neměl být ZOOÚ vůbec aplikován.

NSS uvedl, že je nepochybné, že žalobce pořizoval videozáznam dění před rodinným domem nikoliv za účelem jeho dalšího šíření, ale jen a pouze za účelem získání případných důkazů v trestním řízení proti pachatelům trestné činnosti, kteří na něj opakovaně léta útočili a policie nebyla schopna zjednat jakoukoliv nápravu. Podle české judikatury lze takový videozáznam použít jako důkaz v trestním řízení (viz. předcházející případ, usnesení Nejvyššího soudu ze dne 3.6.2009 sp.zn. 3 Tdo 593/2009).

NSS tedy v tomto případě zvážil, zda může vyložit čl. 3 odst. 2 Směrnice bez položení předběžné otázky. Z dostupné judikatury a praxe členských států EU zjistil, že řada z nich monitorování veřejného prostranství majitelem rodinného domu za účelem ochrany před trestnou činností nepodřazuje pod výjimku čl. 3 odst. 2 Směrnice

¹⁴⁸ Článek 3. Odst. 2 „Tato směrnice se nevztahuje na zpracování osobních údajů: (...) - prováděné fyzickou osobou pro výkon výlučně osobních či domácích činností, Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24.10.1995 o ochraně FO v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů

¹⁴⁹ (12) vzhledem k tomu, že zásady ochrany se musí vztahovat na veškerá zpracování osobních údajů kteroukoli osobou, jejíž činnosti spadají do oblasti působnosti práva Společenství; že je třeba vyloučit zpracování údajů fyzickou osobou při výkonu činností, které mají výlučně osobní povahu, jako je korespondence nebo vedení adresáře; Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24.10.1995 o ochraně FO v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů

(Rakousko, Španělsko, Belgie). Tedy právní úprava ochrany osobních údajů na takovéto monitorování plně dopadá. V některých dalších členských zemích je však praxe odlišná, např. v Irsku a Velké Británii (Velká Británie je mj. průkopníkem masového nasazení kamer na veřejná prostranství, Londýn s cca 10 500 kamerami je považován za nejsledovanější město světa). Podle britského Úřadu komisaře pro informace (The Information Commissioner's Office)¹⁵⁰, se britský zákon na ochranu údajů¹⁵¹ nevztahuje na potřeby osobního sběru a užití dat, pod což spadá i instalace kamer pro ochranu domu před loupeží.

Otázka tedy zní, zda je možné provozování kamerového systému za účelem ochrany majetku, osob, života a zdraví žalobce a jeho rodiny podřadit pod zpracování osobních údajů prováděné FO pro výkon výlučně osobních či domácích činností (čl. 3 odst. 2 Směrnice). NSS se v tomto případě přiklonil k názoru, že text této směrnice daný výklad umožňuje.

NSS tedy položil Soudnímu dvoru EU následující otázku: „Lze provozování kamerového systému umístěného na rodinném domě za účelem ochrany majetku, zdraví a života majitelů domu podřadit pod zpracování osobních údajů „*prováděné FO pro výkon výlučně osobních či domácích činností*“ ve smyslu čl. 3 odst. 2 směrnice 95/46/ES, třebaže takovýto systém zabírá též veřejné prostranství.“¹⁵²

Toto usnesení jsem zařadila také proto, že mi přijde absurdní, že osoby, které páchají trestnou činnost a ohrožují jeho život, zdraví či majetek upozorňují na přestupky poškozeného. Stejně tak mi přijde absurdní, když se takové osoby dovolávají ochrany jejich soukromí. Je zajímavé, že v podstatě banální případ vyústil až k položení předběžné otázky Soudnímu dvoru EU. Myslím, že mnoho z těchto problémů by vyřešila dostatečná právní regulace kamerových systémů.

K použití nahrávek z kamerových systémů v trestním řízení, se ve své podstatě vztahuje rovněž usnesení ÚS, sp. zn. IV.ÚS 449/03. Zde se jednalo o prokázání trestného činu výtržnictví, ke kterému došlo při zápase na fotbalovém stadionu. Záznam z kamerových systémů pak byl použit jako prostředek pro identifikaci pachatele, přičemž v předmětném řízení jako důkaz nefiguroval. Pachatel byl rozsudkem

¹⁵⁰ Nezávislý orgán zabývající se ochranou osobních údajů

¹⁵¹ Data Protection Act 1988, zkr. DPA

¹⁵² Usnesení NSS, č.j. 1 As 113/2012-59, [on-line] [cit.20.6.2013], dostupné z URL:

<http://www.nssoud.cz/files/SOUDNI_VYKON/2012/0113_1As__120_20130415081244_prevedeno.pdf>

Městského soudu v Brně odsouzen pro trestný čin výtržnictví podle § 202 odst. 1 TZ a k peněžitému trestu ve výši 15.000 Kč. Proti tomuto rozsudku se pachatel odvolal, Krajský soud v Brně však odvolání zamítl jako nedůvodné. Pachatel pak následně podal dovolání k NS ČR, přičemž toto dovolání bylo rovněž odmítnuto. Zmíněný pachatel však neváhal a podal ústavní stížnost pro porušení ústavně zaručených práv a svobod, které spatřoval hned v několika skutečnostech.

Jednou z těchto skutečností byl podle stěžovatele postup PČR, díky kterému došlo k porušení jeho osobnostních práv podle § 11 a 12 OZ, neboť bez jeho vědomí byly prostřednictvím kamerových systémů pořízeny jeho obrazové záznamy, které byly následně využity v trestním řízení, což je podle stěžovatele rovněž v rozporu s § 158d odst. 2 TŘ, tímto postupem došlo k zásahu do jeho ústavně zaručených práv podle čl. 2 odst. 2, čl. 7 odst. 1 a čl. 10 Listiny. V této souvislosti stěžovatel tedy zpochybňoval tvrzení odvolacího soudu, že policie jednala na základě § 42f odst. 1 a 2 zákona o PČR, neboť nebylo zjištěno, kdo monitorování prováděl, zda policie, pořadatel nebo bezpečnostní agentura, ani kdo je vlastníkem monitorovacího zařízení. Použití monitorovacího zařízení policií je přitom řazeno mezi operativní techniku, která je však použitelná pouze pro pátrací potřeby policie, nikoliv jako důkaz v trestním řízení; jako důkaz rovněž nejsou použitelné úkony učiněné před zahájením trestního stíhání.

K tomuto ÚS uvedl následující: „*Lze přisvědčit tvrzení stěžovatele, že z obsahu trestního spisu nevyplývá, zda monitorování zápasu prováděla policie, pořadatel či jiný subjekt, z tohoto důvodu se závěr odvolacího soudu, že policie pořizovala obrazový záznam ve smyslu ustanovení § 42f zákona o Policii České republiky, neopírá o provedené důkazy, a tedy není odůvodněný. Rozhodující skutečností nicméně zůstává, že záznam z tohoto monitorovacího zařízení nebyl v předmětném trestním řízení vůbec použit jako důkaz, přičemž úkolem trestního řízení není posuzovat porušování osobnostních práv občanů podle § 11 a 12 obč. zák. (srov. § 1 odst. 1 tr. ř), proto v ústavní stížnosti směřující proti závěrům trestního řízení nelze porušení těchto práv namítat.*“¹⁵³

Nepochybně lze souhlasit s tím, že úkolem trestního řízení skutečně není posuzovat porušování osobnostních práv občanů. Úkolem trestního řízení především je, zajišťovat důkazy, které vedou k usvědčení pachatele, tedy naplnit účel trestního řízení,

¹⁵³ Usnesení ÚS ze dne 15.4.2004, sp.zn. IV. ÚS 449/03, [on-line] [cit. 24.5.2013], dostupné z URL: <<http://nalus.usoud.cz/Search/ResultDetail.aspx?id=45756&pos=1&cnt=1&typ=result>>

nikoliv posuzovat zásah do soukromí občanů. Trestněprávní aspekty bych tedy ukončila v duchu toho, že *účelem trestního řízení není jenom spravedlivé potrestání pachatele, nýbrž i "fair" proces, který je nevyhnutelnou podmínkou existence demokratického právního státu* (Ústavní soud ČR, II. ÚS 268/03) a v rámci *fair* procesu by nahrávky z kamerových systémů dle mého, měly být připouštěny jako důkaz v trestním řízení. Jak je uvedeno v § 1 odst. 1 TŘ, trestní řízení musí působit k upevnování zákonnosti, k předcházení a zamezování trestné činnosti a k výchově občanů v duchu důsledného zachování zákonů a pravidel občanského soužití. To mě vede k myšlence, že pokud by byly důkazy z kamerových systémů odmítány pro ochranu soukromí pachatele trestné činnosti, účel trestního řízení v demokratické společnosti by pak pozbýval smyslu.

5. Úvahy de lege ferenda

„Každý zvuk, který Winston vydal a jenž byl hlasitější než velmi tiché šeptání, obrazovka zachycovala; a co víc, pokud zůstával v zorném poli kovové desky, bylo ho vidět a slyšet. Samozřejmě, člověk si nikdy nebyl jist, zda ho v daném okamžiku sledují. Jak často a podle jakého systému Ideopolicie zapínala jednotlivá zařízení, bylo hádankou. Předpokládalo se, že sledují každého neustále. A rozhodně mohli zapnout vaše zařízení, kdy se jim chtělo. Člověk musel žít – a žil, ve zvyku, který se stal pudovým, – v předpokladu, že každý zvuk, který vydá, je zaslechnut, a každý pohyb, pokud není tma, zaznamenán“. (George Orwell, 1984)

Jako úvod k poslední kapitole své diplomové práce, která se věnuje kamerovým systémům, jsem použila po vzoru ÚOOÚ¹⁵⁴ výňatek z románu G.Orwella, kde byl rovněž poprvé použit výrok Velký bratr Tě sleduje!. Orwell by se dnes asi hodně divil, pokud by dostal možnost vidět, kam až dnešní technika dospěla a kolik různých bratříčků velkého bratra nás dnes sleduje na každém kroku. V současné době stále více dochází k rozmachu kamerových systémů. Lze to přičítat především jejich snadné cenové dostupnosti. K jejich pořízení většinou vede snaha zabezpečit ochranu sobě, svým blízkým a svému majetku. Jako po nejefektivnějším způsobu této ochrany většinou lidé sahají především po kamerovém systému se záznamem, který na rozdíl od on-line monitoringu spadá pod ochranu osobních údajů. Je tedy patrné, že pro oba druhy kamerových systémů platí naprosto rozdílný právní režim. Zůstává tedy otázkou, zda je nejednotnost této rozdílné regulace důvodná a zda právní režim, který se vztahuje na systémy se záznamem, tedy režim pod ZOOÚ je dostačující. Po přečtení mnoha judikátů, článků a stanovisek úřadů, musím konstatovat, že podle mého názoru nikoliv.

Současný právní stav tedy vypadá následovně. Pokud je instalován kamerový systém, který nemá záznamové zařízení, tedy jeho prostřednictvím nedochází ke zpracování osobních údajů, ZOOÚ se na tento systém nebude vztahovat. Otázka zní, existuje nějaká speciální právní úprava, která by se na tyto systémy vztahovala? Musím konstatovat, že bohužel ne. Domnívám se však, že to není právě šťastný krok. Jistě, žijeme ve společnosti, která si víceméně zvykla, že je sledována. Málokdo se dnes pozastaví nad kamerou, která ho sleduje v krámu, na ulici, v čekárně u lékaře a na mnoha jiných místech. Žijeme ve společnosti pod dohledem a nijak se tomu ve své podstatě nebráníme. Lze pochopit, pokud se někdo domnívá, že on-line kamerové

¹⁵⁴ Bulletin ÚOOÚ 2/2011, [on-line] [cit. 27.5.2013], dostupné z URL:<http://www.uoou.cz/files/zpravodaj/bulletin_2011_02.pdf>

systemy nemohou do soukromí nějak zasáhnout. Velmi často je však opak pravdou, protože právě i pouhé monitorování může mít v konkrétních případech vliv např. na psychiku či vývoj monitorovaného jedince. Ve své diplomové práci jsem se zmiňovala o případu, kdy byly tyto on-line kamerové systémy využívány v zařízeních, kde se vykonává ústavní výchova. Podnětem pro zkoumání tohoto případu bylo zjištění Úřadu veřejného ochránce práv o umístění kamerových systémů ve školském zařízení. Nejednalo se o nějak výjimečný případ, je to dnes běžná praxe. V souvislosti s tímto případem bylo vysloveno několik názorů několika renomovaných institucí. Jádrem problému bylo, zda pouhým monitorováním dochází či nedochází k porušení práv zakotvených v čl. 8 odst. 1 Úmluvy, čl. 16 ve spojení se čl. 20 odst. 1) Úmluvy o právech dítěte a s čl. 7 odst. 1, čl. 10 odst. 2 a čl. 12 odst. 1 Listiny.

K problematice se vyslovily dvě renomované instituce, Ústav a PRF Brno. Obě však došly k rozdílným závěrům. Závěrem Ústavu práva bylo, že není rozdíl, zda jsou takto sledováni např. cestující v metru, nebo dítě které je umístěno ve výchovném ústavu. Bylo konstatováno, že ani v jednom případě nedochází k narušení soukromí aj. V kontrapozici pak byl názor PRF Brno, který konstatoval, že stavění naroveň kamerového monitoringu ve výchovných ústavech a např. na nádražích, svědčí o nepochopení pojmu soukromí. Bylo konstatováno, že je nutno rozlišovat mezi ochranou chování osob na veřejnosti a v soukromí. V soukromí je totiž osobní sféra chráněna mnohem intenzivněji. Podle stanoviska PRF Brno, umístění a využívání kamer ve výchovných ústavech a jiných podobných zařízeních podléhá ústavním garancím ukotvených v Listině. Závěrem bylo, že se jedná o opatření protiústavní. V závěrečném stanovisku zástupkyně ochránce práv pak bylo konstatováno, že se ztotožňuje se závěrem PRF Brno a jednoznačně odmítá argumentaci Ústavu práva. Umístění kamer bylo posouzeno jako neoprávněný a svévolný zásah do práva na soukromí umístěných osob. Nemluvě pak o negativních dopadech na psychický stav, který byl rovněž několikrát konstatován v odborných kruzích při posuzování této problematiky. Poměrně jasné je pak i vyjádření ombudsmana, JUDr. Pavla Varvařovského v jeho úvaze nad nejednotnou právní regulací kamerových systémů. Konstatoval, že během jeho návštěv v zařízeních, kde se nacházejí nebo mohou nacházet osoby omezené na svobodě (např. dětské domovy, psychiatrické léčebny), bylo v řadě případů shledáno, že soustavným monitorováním těchto osob může docházet k porušení jejich práva na soukromí.

V souvislosti s těmito případy se tedy obrátil na ÚOOÚ, který sice vykonal své dozorové pravomoci, ale v okamžiku kdy zjistil, že není prováděn záznam a neexistují důkazy o tom, že by v minulosti byl, konstatoval, že zde není dána jeho působnost. V těchto případech bylo nepochybné, že docházelo jak k zásahům do práva na soukromí tak do práva na zachování lidské důstojnosti. Ve své podstatě byly údaje o těchto osobách jistým způsobem shromažďovány a po té co byly zachyceny kamerou, mohly být následně přeneseny na obrazovku, kde se s nimi mohl kdokoliv seznámit. V neposlední řadě je třeba brát v úvahu, že v dnešní době existují také analogové digitální systémy, které mohou osobní údaje digitalizovat, a v této podobě pak mohou být přenášeny a ukládány kdekoli jinde než na koncovém zařízení. Ombudsman k tomuto dále konstatoval, že žít pod drobnohledem kamer není normální, a je jedno zda pořizují záznam či nikoliv.¹⁵⁵ S tímto názorem se naprosto ztotožňuji. Bohužel však konkrétní povinnosti, které požaduje po správcích kamerových systémů ZOOÚ ve svém § 5, jako je např. povinnost stanovit účel, způsob, poskytnout informace sledovaným osobám aj., platí *de lege lata* pouze na kamerové systémy se záznamem.

Shora uvedeným jsem chtěla manifestovat, že i kamerové systémy bez záznamu mohou být v mnoha ohledech nebezpečné pro sledované subjekty. Mohou významně narušit soukromí i důstojnost sledovaných osob a rovněž mohou mít v případě umístění těchto systémů např. ve výchovných zařízeních velmi nepříznivý vliv na psychický stav umístěných osob. Nejen v tomto případě musím konstatovat, že velmi citelně postrádám konkrétní právní úpravu kamerových systémů, která by se vztahovala na obě dvě možnosti a to jak na kamerové systémy se záznamem tak bez záznamu a dostatečně regulovala tuto problematiku. Obojí totiž sebou nese velmi podstatná rizika pro demokratickou společnost.

Stejnou míru absence právní úpravy kamerových systémů postrádám v trestním právu. Jsem toho názoru, že postihy v rámci správních deliktů nemají dostatečnou preventivní funkci. Praxe ukázala, že jako jediný možný postih v rámci trestního řízení přichází postih podle § 180 TZ (neoprávněné nakládání s osobními údaji). Bohužel skutková podstata tohoto TČ spočívá pouze v neoprávněném nakládání s osobními údaji, které byly o jiném shromážděny s výkonem veřejné moci. Toto omezení mi přijde poměrně nešťastné, neboť k podstatnému zneužití osobních údajů zaznamenaných

¹⁵⁵ Bulletin ÚOOÚ 2/2011, [on-line] [cit. 27.5.2013], dostupné z URL:<http://www.uoou.cz/files/zpravodaj/bulletin_2011_02.pdf>

prostřednictvím kamerových systémů může docházet (a často také dochází) i v běžném životě. Tedy nemusí se jednat pouze o zneužití údajů, které byly o jiném shromážděny s výkonem veřejné moci. V tomto případě bych se přikláněla k novele zákona č. 40/2009 Sb., trestního zákona, ve znění pozdějších předpisů. Domnívám se, že by to byl logický krok, vzhledem k rychlému vývoji kamerových systémů. Dnes už nemáme jen obyčejné kamery, které nás „pouze“ nahrávají. Na trh přichází kamery s mnoha novými funkcemi, které mohou být nebezpečné. Existují např. kamery se systémem rozpoznávání lidských tváří (angl. facial recognition system), které umožňují rozpoznávat lidské obličeje bez jejich vědomí a stávají se tak nebezpečným nástrojem pro masové sledování lidí. Jedním z varovných signálů rychlého vývoje těchto systémů je rovněž nově testovaná schopnost kamerových systémů, která spočívá v *rozpoznávání zločinu dříve než se stane*. Tyto systémy fungují na základě speciálního softwaru, který je schopen měřit srdeční puls v reálném čase. Ke změření stačí pouhých pět vteřin. Na základě změření tepové frekvence subjektu, pak dokáže kamerový systém odhalit v jeho tepové frekvenci výkyvy a odhalit tak subjekt, který se chová podezřele. V případě, že tento výkyv systém odhalí, je schopen upozornit ostrahu a ta může subjekt podrobit kontrole ještě dříve, než skutečně dojde k případnému protiprávnímu jednání. Tento systém vyvíjí společnost Fujistu a hodlá ho v několika málo letech nabídnout jak soukromým společnostem, tak státním institucím.¹⁵⁶ Podle mého názoru se jedná o další z mnoha varovných signálů, který implikuje nutnost potřebu ucelenější právní úpravy.

V rámci novelizace trestního práva je pak možno již dnes vysledovat konkrétní snahy o novelizaci trestních sankcí, které by postihovaly např. právě sledování prostřednictvím kamerových systémů. Právě tento nedostatek, kdy dostatečné sankce chybí, se totiž stává nástrojem k invazivnímu narušení soukromý sledovaných osob a to povětšinou s cílem je poškodit popř. vysledované informace jinak zneužít.

Jednou z těchto snah bylo předložení návrhu do připomínkového řízení skupiny poslanců J. Tejce, B. Sobotky a dalších. Tato navrhovaná novela byla předložena v roce 2011 a spočívala v následujících změnách, které se v první řadě dotýkaly již zmiňovaného § 180 TZ, za který měl být vložen § 180 a který zněl následovně:

¹⁵⁶ Kamerový systém dokáže odhalit zločin dříve než se stane, [on-line] [cit. 29.5.2013], dostupné z URL: <<http://www.novinky.cz/internet-a-pc/298262-novy-kamerovy-system-dokaze-odhalit-zlocin-drive-nez-se-stane.html>>

„§ 180a

Nedovolené sledování

(1) Kdo neoprávněně a v rozporu s veřejným zájmem o jiném nebo o jeho věcech utajovaným způsobem získává poznatky s použitím elektronického nebo jiného technického zařízení sloužícího k pořizování, záznamu nebo přenosu zvuku nebo obrazu, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti.

(2) Stejně bude potrestán, kdo čin uvedený v odstavci 1 sjedná nebo o něj požádá nebo jej zajistí.

(3) Odnětím svobody na jeden rok až tři léta bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1

a) jako člen organizované skupiny,

b) ačkoliv byl za takový čin v posledních třech letech odsouzen nebo potrestán,

c) na osobě mladší osmnácti let,

d) na svědkovi, znalci nebo tlumočnickovi v souvislosti s výkonem jejich povinnosti,

e) jako osoba, která má zvláštní povinnost zajišťovat ostrahu osob a majetku, nebo

f) s cílem umožnit spáchání další trestné činnosti na sledované osobě,

g) v obydlí.¹⁵⁷

Další změna se měla dotýkat § 354 (nebezpečné pronásledování, tzv. stalking), odst. 1 písm. b) TZ kde za slovo „jej“ měla být vložena slova „neutajovaným způsobem“. Tento zákona měl nabýt účinnosti 1. ledna 2012.

Při zhodnocení platného právního stavu, bylo v důvodové zprávě uvedeno, že problematika, která se dotýká nedovoleného sledování osob nebo jejich věcí, zejm. prostřednictvím odposlechů, zaznamenávání pohybu a pobytu osob aj., není v platném trestním právu náležitě upravena. S ohledem na to, že se může jednat o činnost, která vykazuje vysoký stupeň škodlivosti pro společnost by však měla být postihována trestněprávní sankcí. V dikci § 354 TZ je upraven pouze TČ nebezpečné

¹⁵⁷ Navrhovaná novela zákona, trestní zákoník, sněmovní tisk 428/0, [on-line] [cit. 29.5.2013], dostupné na URL: <<http://www.psp.cz/sqw/text/tiskt.sqw?O=6&CT=428&CT1=0>>

pronásledování, kterého se dopustí ta osoba, která *a) jiného dlouhodobě pronásleduje tím, že jinému vyhrožuje ublížením na zdraví nebo jinou újmu jemu nebo jeho blízkým osobám, b) vyhledává jeho osobní blízkost nebo jej sleduje, c) vytrvale jej prostřednictvím prostředků el. komunikací, písemně nebo jinak kontaktuje, d) omezuje jej v jeho obvyklém způsobu života nebo e) zneužije jeho osobních údajů za účelem získání osobního nebo jiného kontaktu, a toto jednání je způsobilé vzbudit v něm důvodnou obavu o jeho život nebo zdraví nebo o život a zdraví osob jemu blízkých, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti.*¹⁵⁸ Touto skutkovou podstatou však není postihnuto sledování osob, které je prováděno utajovaným způsobem za použití technických nebo jiných prostředků. Cílem takového jednání pak je především získávat informace o životě sledované osoby, tj. o jejím pobytu nebo pohybu, o jejích stycích a komunikaci s jinými osobami aj. Znakem TČ uvedeného v § 354 TZ je pronásledování dlouhodobého charakteru. Podle odst. 1 písm. b) se sice tohoto TČ dopustí i ten, kdo jiného sleduje, ale musí jít o sledování neutajované, o němž sledovaná osoba ví, jelikož toto sledování musí být způsobilé v jiném vzbudit důvodnou obavu o její život, zdraví nebo o život a zdraví jejích blízkých.

S nedovoleným sledováním dále souvisí TČ uvedený v § 180 TZ (neoprávněné nakládání s osobními údaji). Tento TČ byl podrobně rozebrán v předchozích kapitolách mé práce, nicméně znovu uvádím, že neoprávněného nakládání s osobními údaji se týká pouze těch údajů, které byly o jiném shromážděny v souvislosti s výkonem veřejné moci a nebo byly zpřístupněny tak, že tím byla porušena státem uznaná povinnost mlčenlivosti. Ani zde uvedené skutkové podstaty tedy neřeší problém sledování osob a věcí pomocí elektronických či jiných technických zařízení v takovém rozsahu, v jakém je to v dnešní době třeba (resp. neřeší jej vůbec). Z výše uvedeného je tedy zřejmé, že současná platná právní úprava náležitě neupravuje tuto problematiku (myšleno např. utajované sledování osob pomocí kamerových systémů).

Vzhledem k výše uvedenému bylo tedy připravovanou novelou navrhováno zařazení nového TČ nedovoleného sledování (§ 180 a) a zařadit jej do oddílu o trestných činech proti právům na ochranu osobnosti, soukromí a listovního tajemství, konkrétně za stávající TČ neoprávněného nakládání s osobními údaji. Toto zařazení je podle mého naprosto logické. Podle této navrhované novely by však byl trestný pouze

¹⁵⁸ § 354, Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů

ten, kdo by neoprávněně *v rozporu s veřejným zájmem* o jiném či o jeho věcech utajovaným způsobem získával poznatky a to s použitím elektronických či jiných technických zařízení sloužících k pořizování záznamů či přenosů zvuku nebo obrazů. Skutková podstata byla inspirována zněním ustanovené § 158d odst. 1 TŘ, které vymezuje pojem sledování osob a věcí, a to jako získávání poznatků o osobách a věcech prováděné utajovaným způsobem technickými nebo jinými prostředky a dále § 120 TZ, který zavedl pojem elektronické nebo jiné technického zařízení. Potrestána by byla nejen osoba, která provádí nedovolené sledování, ale rovněž ta osoba, která by si toto sledování vyžádala nebo jej pro jiného zajistila. Základní skutková podstata navrženého § 180a odst. 1) by tedy postihovala nedovolené sledování prováděné elektronickým nebo jiným technickým zařízením sloužícím k pořizování, záznamu nebo přenosu zvuku nebo obrazu. Další skutkové podstaty by pak přísněji postihovaly pachatele, který by se utajovaného sledování dopustil jako člen organizované skupiny, pokud by byl pachatel za takový čin v posledních třech letech odsouzen nebo potrestán, dopustil by se tohoto činu na osobě mladší osmnácti let, nebo by se takového sledování dopustil na svědkovi, znalci nebo tlumočnickovi v souvislosti s výkonem jejich povinnosti, nebo jako osoba která má zvláštní povinnost zajišťovat ostrahu osob a majetku a nebo s cílem, umožnit spáchání další trestné činnosti na sledované osobě, nebo v obydlí.¹⁵⁹

Vláda však k této navrhované novele zaujala negativní stanovisko¹⁶⁰ a to z následujících důvodů. Předložený návrh se údajně pokoušel zajistit ochranu zájmům, které již v platném právním řádu ČR chráněny jsou. Za prvé v rovině občanskoprávní a to příslušnými normami na ochranu osobnosti (s čímž souhlasit lze). Za druhé jsou částečně chráněny v TZ (podle mého názoru, bych slovo částečně nahradila slovním spojením spíše vůbec). V tomto stanovisku vlády bylo uvedeno, že navrhovaná novela je zcela nevhodná, neboť užívá nejednoznačných pojmů, jako je *neoprávněně* a *v rozporu s veřejným zájmem*. Pokud jde o pojem neoprávněně, osobně ho neshledávám tak nejednoznačným, že by představoval takovou vadu, která by měla za následek nepřijetí této novely. Pokud pak jde o pojem *veřejný zájem*, v souvislosti s tímto ustanovením ho také shledávám poměrně nešťastným. Neboť tento pojem není

¹⁵⁹ Navrhovaná novela zákona, trestní zákoník, sněmovní tisk 428/0, [on-line] [cit. 29.5.2013], dostupné na URL: <<http://www.psp.cz/sqw/text/tiskt.sqw?O=6&CT=428&CT1=0>>

¹⁶⁰ Stanovisko vlády k návrhu zákona, kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění zákona č. 306/2009 Sb., [on-line] [cit. 29.5.2013], dostupné na URL:<<http://www.psp.cz/sqw/text/tiskt.sqw?o=6&ct=428&ct1=1>>

jednoznačně definován a právě jeho definice a uplatnění může být zdrojem problémů. Veřejný zájem se totiž může významně různit s ohledem na konkrétní situace a ani Lippmannova definice, totiž že: „*Veřejný zájem je zřejmě tím, co by si lidé vybrali, kdyby viděli jasně a racionálně, a jednali nezaujatě a benevolentně.*“, mě nijak neuklidňuje, neboť situace kdy lidé jednají nezaujatě a racionálně nebývá častá (zvláště v právním světě). Lze tedy souhlasit s tím, že v předloženém návrhu by byl TČ odkázán na naprosto neurčitý veřejný zájem, což by jistě neposílilo právní jistotu. Dle mého názoru by stačilo v navrhovaném § 180a vypustit spojení „*v rozporu s veřejným zájmem*“ a zůstalo by tedy pak tedy znění: *Kdo neoprávněně o jiném nebo o jeho věcech utajovaným způsobem získává poznatky s použitím elektronického nebo jiného technického zařízení sloužícího k pořizování, záznamu nebo přenosu zvuku nebo obrazu, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti.*

Za problematické byly mj. označeny pojmy jako *poznatky* (navrhované v § 180a odst. 1), pojem *zajistí* (navrhovaný § 180a odst. 2) a pojem *v obydlí* (navrhovaný § 180a odst. 3). S tímto názorem se neztotožňuji, neboť v platném právu je mnohem více nejasných pojmů a domnívám se, že chvíle, kdy budou všechny právní pojmy jasné nikdy nepřijde. Mým názorem ohledně pojmu *obydlí* je, že tento pojem je již dostatečně definován v § 133 TZ, podle nějž je obydlím dům, byt nebo jiný prostor sloužící k bydlení a příslušenství k němu náležející. Nemyslím tedy že, pojem „v obydlí“ se nějak významně liší od pojmu „obydlí“, které mj. rovněž upravuje ustanovení § 82 odst. 1 in fine zákon č. 141/1961 TR, ve znění pozdějších předpisů.

Podle mého názoru se však lze ztotožnit s tím, že navrhovaná změna, která se dotýká § 354 odst. 1 písm. b) TZ, na základě které by TČ nebezpečného pronásledování byl zúžen pouze na sledování neutajovaným způsobem, mám rovněž postaveno za jisto, že forma utajeného sledování může být mnohem škodlivější než sledování neutajované. Totiž dle mého uvážení, podstata *neutajovaného sledování* je totiž *stricto sensu* vyjádřena již v podmínce § 354 odst. 1 písm. e), tedy že toto jednání je způsobilé vzbudit v jiném důvodnou obavu o jeho život nebo zdraví. Navrhovala bych tedy v tomto případě zařadit do § 354 TZ další odstavce, a to mezi původní odst. 1) a 2) který by zněl např. následovně: *Kdo jiného dlouhodobě pronásleduje tím, že jej sleduje s použitím elektronického nebo jiného technického zařízení sloužícího k pořizování, záznamu nebo přenosu zvuku nebo obrazu, a zpracovává tak neoprávněně jeho osobní*

údaje, bude potrestán etc. Jistě by bylo nutné tyto úvahy podrobně rozpracovat, ale takové pronásledování by dle mého mělo být v souvislosti s kamerovým systémem a možným zneužitím osobních údajů trestné a to nikoliv jen v souvislosti, kdy je toto jednání schopno vzbudit v druhém důvodné obavy a jeho život nebo zdraví. Prostřednictvím nedovoleného sledování se totiž škodlivé důsledky pro společnost mohou pohybovat i v mnoha jiných rovinách. Mohou významně poškozovat základní lidská práva zaručená Listinou.

Úvahy o navrhované novele TZ lze uzavřít následovně, s některými připomínkami vlády lze souhlasit, s jinými méně, ale jistě by to nemělo mít za následek konec veškerých snah o trestněprávní novelizaci této oblasti. I když je pravdou, že navrhovaná novela mířila pouze na ty největší excesy při používání sledovacích systémů. Z hlediska soukromých provozovatelů kamerových systémů dochází rovněž velmi často k porušování ZOOÚ. Příčinou je bohužel obecná, nejasná a v praxi velmi často neproveditelná formulace ZOOÚ.

Úvahy *de lege ferenda* tedy uzavírám tím, že celková právní úprava kamerových systémů je nedostatečná, vzhledem k možnému nebezpečí zneužití těchto systémů s úmyslem jiného poškodit. Uvědomuji si, že vypracovat takový právní předpis, který by upravoval tuto oblast by bylo těžkým úkolem, nicméně v dnešní době by to byl velký krok kupředu.

6. Závěr

Nad koncepcí této diplomové práce jsem strávila opravdu hodně času. Přečetla jsem mnoho soudních rozhodnutí, stanovisek ÚOOÚ a čerpala z mnoha různých zdrojů. Doufám, že se mi podařilo do této práce vtělit to nejdůležitější ohledně kamerových systémů.

Během psaní této práce jsem si několikrát ověřila, že právní úprava kamerových systémů je skutečně nedostatečná. Je tak možné poměrně snadno tyto systémy zneužít a často tak končí mnoho sporů, kde tyto systémy figurují před soudem. Znepokojujícím faktem je rovněž úplná absence v podstatě jakékoliv právní úpravy kamerových systémů bez záznamu, které nemusí být nikde registrovány a tak vlastně nikdo neví, kolik těchto systémů v naší společnosti je. Skutečností k zamyšlení je mj. i to, že pokud kamerový systém v jednu dobu postrádá záznamové zařízení, neznamena to, že toto zařízení neměl v minulosti či nebude mít v budoucnu. I proto si tedy myslím, že právní úprava vztahující se pouze na kamerové systémy se záznamem je chybná. Oba druhy kamerových systémů nabízejí svým majitelům mnoho možností pro práci s osobními údaji.

Postrádám tedy v návaznosti na výše uvedené rozsáhlejší kontrolu ÚOOÚ a rovněž důslednější postihy v rámci správního práva. S ohledem na trestněprávní úpravu postrádám právní úpravu celkově. Jsem toho názoru, že zavedení TČ které by dopadaly na kamerové systémy je v současné společnosti třeba. Co se týká úpravy např. v ZoPČR, úprava využití kamerových systémů PČR mi přijde rovněž nedostatečná, jelikož neposkytuje dostatečné mantinely pro práci s těmito systémy.

Bohužel, žijeme skutečně ve společnosti pod dohledem a čísla kamerových systémů se budou stále jen zvyšovat a tyto systémy budou mít stále více nových funkcí, které budou schopny stále více ohrožovat soukromí každého z nás. Během psaní této práce, jsem mj. zaznamenala mnoho nových informací, které se dotýkaly kamerových systémů. Jednou z těchto informací byla ta, že vznikají nové kamerové systémy s názvem *Facedeals*, které v propojení s účtem na *Facebooku* využívají funkce rozpoznávání obličeje. V praxi fungují tak, že na svém účtu uživatel zaškrtně souhlas s touto aplikací, a kamery mohou tyto uživatele pak podle tváře rozpoznávat. Nejčastěji by tyto kamery měly být využívány např. v krámech či barech a jejich výhoda prý spočívá v tom, že na základě identifikace subjektu jsou schopny nabídnout slevu na

oblíbené produkty aj. Tento systém je zatím ve vývoji, ale mohu za sebe říci, že představa něčeho takového v praxi mi nahání strach. Kamerové systémy na každém kroku, propojení s účty na internetu, chytré telefony, GPS v autech a hodinkách, chytré televize, to všechno nabízí výhody moderní doby, které nám mají usnadnit život. Usnadnit ano, ale za jakou cenu, za cenu totální ztráty tolik důležitého a ústavně chráněného práva na soukromí.

Závěrem bych tedy chtěla jen dodat, že vzhledem k velmi rychlému vývoji kamerových systémů, jak dokazují např. i výše zmíněné nové funkce, je potřeba konkrétní právní úpravy naprosto nepochybná. Svobody a soukromí by si měl každý vážit, a ne se těchto práv vzdávat jen z toho důvodu, že to tak jde ruku v ruce s moderní dobou.

Resumé

The master's thesis discusses the using of camera systems and its legal aspects. The thesis is divided into four chapters. The first chapter is dedicated to the explanation of the basic terms that are used in the whole thesis. The second chapter deals with camera systems in detail, defines the basic categories, the legislation and the areas of utilization.

The third chapter focuses on the criminal law aspects of camera systems from two different perspectives – from the viewpoint of the property criminal law and the viewpoint of the procedural criminal law. The considerations *de lege ferenda* are worked out in the last chapter of the thesis. This part is based on the knowledge acquired during writing of the thesis. The thesis includes both theoretical and practical knowledge of camera systems, mainly from the area of utilization, with regard to the legislation.

Seznam použitých zdrojů

Literatura:

- BARTÍK V., JANEČKOVÁ E.: *Kamerové systémy v praxi. Právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. Praha, Linde 2011, 240 s. ISBN 978-80-7201-850-5.
- GILL, Martin, SPRIGGS, Angela, *Vyhodnocení účinku kamerových systémů*, Praha: Institut pro kriminologii a sociální prevenci, vydavatelství KUFR, 2007, 141 s. ISBN 978-80-7338-061-8.
- JELÍNEK, J. a kol.: *Trestní právo hmotné*. 2. vydání. Praha: Leges, 904 s. ISBN 978-80-87212-49-3.
- KUČEROVÁ, Alena a kol. *Zákon o ochraně osobních údajů komentář*, Praha: nakladatelství C.H.Beck, 2012, 536 s. ISBN 978-80-7179-226-0.
- Musil, J., Kratochvíl, V., Šámal, P., a kol. *Kurs trestního práva. Trestní právo procesní*, 3. přepracované a doplněné vydání. Praha C.H.Beck, 2007, 1211 s. ISBN 978-80-7179-72-8.
- ŠÁMAL, P. a kol. *Trestní zákoník II. § 140 až 421. Komentář*. 2. vydání. Praha: C.H.Beck 2012, 2150 s. ISBN 978-80-7400-428-5.

Internetové zdroje:

- Právní předpisy vztahující se k ochraně osobních údajů, stav ke dni 27.3.2013, dostupné na: http://www.oou.cz/index.php?file=personal_data_protection_law
- Stanovisko č. 1/2006. Úřad pro ochranu osobních údajů, dostupné na: http://www.uoou.cz/files/stanovisko_2006_1.pdf
- Výroční zpráva ÚOOÚ za rok 2009, stav ke dni 27.3.2013, dostupné na: http://www.uoou.cz/files/vz_2009.pdf
- Stanovisko č. 4/2004. Úřad pro ochranu osobních údajů, . 27.3.2013, dostupné na: <http://www.uoou.cz/uoou.aspx?menu=50&submenu=52&loc=83>
- Výkladové stanovisko pořadové č. 10/2003, K zákonnosti umístění audio - vizuálních prostředků ve školských zařízeních, kde se vykonává ústavní výchova a ochranná výchova, 17.4.2013, dostupné na:

http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2003/stanovisko%2010-2003.pdf

- Metodika k provozování kamerových systémů, ÚOOÚ, 19.4.2013, dostupné na: http://www.uoou.cz/files/metodika_provozovani_kamerovych_systemu.pdf
- ÚOOÚ, stanovisko k provozování kamerových systémů z hlediska ochrany osobních údajů, č. 1/2006, 21.4.2013, dostupné na: http://www.uoou.cz/files/stanovisko_2006_1.pdf
- HORKÝ, Štěpán. Kamerové systémy, epravo.cz, 23.4.2013], dostupné na: <http://www.epravo.cz/top/clanky/kamerove-systemy-dobry-pomocnik-ale-88307.html>
- Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, 25.4.2013, dostupné na: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:CS:NOT>
- Stanovisko pracovní skupiny WP 29, č. 4/2004 ke zpracování osobních údajů prostředky kamerového sledování, 27.4.2013, dostupné na: <http://www.uoou.cz/uoou.aspx?menu=50&submenu=52&loc=83#pp25>
- Stanovisko Ministerstva vnitra ČR, 30.4.2013, dostupné na: http://www.uoou.cz/files/info_mvcr_kamery.pdf
- Článek IDNES. cz, 3.5.2013], dostupné na: http://zpravy.idnes.cz/plzenska-mestska-kamera-sledovala-byt-ne-krizovatku-pcf-domaci.aspx?c=A070801_144158_domaci_hos
- Mapa kamer, 3.5.2013, dostupné na: <http://www.mapakamer.cz/mapakamer>
- POSPÍŠIL. Filip, prezentace: Vývoj dosavadních snah o novou úpravu kamerových systémů, 3.5.2013, dostupné na: www.slidilove.cz/content/vyvoj-dosavadnich-snah-o-novou-upravu-kamerovych-systemu
- Kamerové systémy v ČR - opravdu dlouhý sumarizační článek z roku 2007, 3.5.2013, dostupné na: <http://www.slidilove.cz/content/kamerov%C3%A9-syst%C3%A9my-v-%C4%8Dr-opravdu-dlouh%C3%BD-sumariza%C4%8Dn%C3%AD-%C4%8Dl%C3%A1nek-z-roku-2007>

- Usnesení Nejvyššího soudu ze dne 24.6.2009, sp.zn.8 Tdo 682/2009, 11.5.2013, dostupné na: <http://pravo4u.cz/judikatura/nejvyssi-soud-cr/8-tdo-682-2009/>
- Výroční zpráva ÚOOÚ za rok 2008, 12.5.2013, dostupné na: http://www.uoou.cz/files/vz_2008.pdf
- Praktické otázky provozování kamerových systémů ve školách a školských zařízeních, ÚOOÚ, 17.5.2013, dostupné na: <http://www.uoou.cz/uoou.aspx?menu=14&loc=383#kamery>
- Stanovisko NS k závažnému narušování soukromí, 17.5.2013, dostupné z na: http://www.nsoud.cz/JudikaturaNS_new/ns_web.nsf/web/Proverejnostamedia~Tiskovezpravy~Stanovisko_NS_k_zavaznemu_narusovani_soukromi~?openDocument&lng=CZ
- Kauza hotelu Savoy, www.centrum.cz, 1.6.2013, dostupne na: http://aktualne.centrum.cz/tema/savoy-hotel_57010/?offset=1
- Bulletin ÚOOÚ 2/2011, 27.5.2013, dostupné na: http://www.uoou.cz/files/zpravodaj/bulletin_2011_02.pdf
- Kamerový systém dokáže odhalit zločin dříve, než se stane, 29.5.2013, dostupné z: <http://www.novinky.cz/internet-a-pc/298262-novy-kamerovy-system-dokaze-odhalit-zlocin-drive-nez-se-stane.htm>

Seznam použitých právních předpisů:

- Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů
- Občanský zákoník, zákon č. 40/1964 Sb. ve znění pozdějších předpisů
- Úmluva o ochraně lidských práv a základních svobod, zákon č. 209/1992 Sb., ve znění pozdějších předpisů
- Listina základních práv a svobod, zákon č. 2/1993 Sb., ve znění pozdějších předpisů
- Zákon č. 202/1990 Sb., o loteriích a jiných podobných hrách, ve znění pozdějších předpisů
- Zákon č. 128/2008 Sb., o obcích (obecní zřízení), ve znění pozdějších předpisů

- Zákon č. 553/1991 Sb., o obecní policii ve znění pozdějších předpisů
- Zákon č. 273/2008 Sb., o Policii ČR, ve znění pozdějších předpisů
- Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů
- Zákon č. 262/2006 Sb., zákoník práce ve znění pozdějších předpisů
- Zákon č. 141/1961 Sb., trestní řád, ve znění pozdějších předpisů
- Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, ve znění pozdějších předpisů
- Mezinárodní pakt o občanských a politických právech (vyhláška Ministerstva zahraničních věcí č. 120/1976 Sb.
- Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat (ETS č.108, Štrasburk, 28 ledna 1981), sděl. Ministerstva č. zahr. věcí č. 115/2001 Sb.
- Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů

Soudní judikatura a rozhodnutí:

- Rozsudek Nejvyššího správního soudu ze dne 12. 02. 2009, čj. 9 As 34/2008–68
- Rozhodnutí Městského soudu v Praze č.j. 11 Ca 298/2008 – 47
- Usnesení Nejvyššího soudu ČR, sp. zn. 8 Tdo 682/2009
- Rozsudek Evropského soudu pro lidská práva, ze dne 16. prosince 1992, Věc Niemietz (Rozsudek ve věci Niemietz versus Německo)
- Rozsudek Nejvyššího soudu ze dne 30.10.2012, sp. zn. 22 Cdo 583/2011
- Rozsudek Městského soudu v Praze ze dne 11.5.2010 , č.j. 11 Ca 433/2008
- Usnesení Nejvyššího soudu ze dne 03. 06. 2009, sp. zn. 3 Tdo 593/2009, uveřejněný pod č. 22/2010 Sbírky soudních rozhodnutí a stanovisek
- Usnesení ÚS k přípustnosti důkazu získaného bezpečnostním kamerovým systémem pro účely trestního řízení ve vztahu k právu na ochranu soukromí, , IV.ÚS 2425/09 ze dne 8. 2. 2010
- Usnesení Nejvyššího soudu ze dne 20.3.2013, č.j. 1 As 113/2012-59
- Usnesení ÚS ze dne 15.4.2004, sp.zn. IV. ÚS 449/03

- Nález ÚS ze dne 3.11.2004, sp. zn. II.ÚS 268/03

Jiné zdroje:

- Navrhovaná novela zákona, trestní zákoník, sněmovní tisk 428/0
- Stanovisko vlády k návrhu zákona, kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění zákona č. 306/2009 Sb.,