UNIVERZITA KARLOVA V PRAZE
PRÁVNICKÁ FAKULTA
KATEDRA OBČANSKÉHO PRÁVA

Disertační práce

Kamerové systémy a obrazové záznamy v právní ochraně soukromí

JUDr. Milan Chládek

PRAHA 2012

Rád bych touto cestou poděkoval svému školiteli, Prof. JUDr. Jiřímu Švestkovi, DrSc., za jeho pomoc a vedení při zpracování této práce.

Prohlašuji, že jsem tuto disertační práci zpracoval samostatně, že jsem vyznačil prameny, z nichž jsem pro svou práci čerpal, způsobem ve vědecké práci obvyklým a že práce nebyla využita k získání jiného nebo stejného titulu.

……..

OBSAH

Není-li výslovně v práci uvedeno jinak, jsou právní předpisy v této práci citovány dle legislativního stavu ke dni 1. ledna 2012.

1 ÚVOD

Dnešní doba přináší netušené možnosti. Člověk žijící v české kotlině může z pohodlí svého domova brouzdat virtuálně ulicemi australských měst, posílat obrázky svého domova a přátel svým známým na Filipínách (které třeba ani nikdy v reálu neviděl), může provozovat videohovory a celé videokonference se známými, kteří jsou v jednom okamžiku na různých místech planety atd. Stejně tak může pomocí podrobných leteckých map prozkoumat pozemky nacházející se v jeho sousedství, byť umístěné za vysokými ploty a zdmi anonymních a a tajnůstkářských sousedů. Na druhou stranu stejný člověk může být v průběhu jednoho svého dne terčem zájmu cca stovky pouličních kamer, zájmu fotoaparátu pohyblivého vozidla společnosti Google zrovna mapující terén v české kotlině pro uživatele své aplikace Street View po celém světě, či zájmu speciálního letištního skanneru, který je schopen jej prosvítit a umožnit obsluze přístroje podrobný pohled na jeho tělo.

Člověk, který nežije odloučen od civilizované společnosti, je podroben obrazovému a jinému monitoringu ze strany všemožných státních i soukromých subjektů. Jeho pohyb může být monitorován pomocí nejrůznějších přístrojů na bázi družicového určování polohy (GPS ve firemních i soukromých automobilech), podle signálu mobilního telefonu, pomocí kamer umístěných na silnicích a ulicích, díky zpoplatnění využívání silnic a dálnic lze monitorovat velmi přesně pohyb prakticky všech vozidel; stejně tak, využívá-li člověk výhod železničního, tramvajového či autobusového cestování, ani tam se neubrání evidenci jeho jízd díky systému elektronických čipových zákaznických karet či díky kamerám umístěným přímo v dopravních prostředcích, na zastávkách a nádražích. Pohyb a chování lidí ve městech je nepřetržitě monitorováno stovkami policejních i soukromých kamer, a to nezřídka i v šatnách na plaveckých bazénech, ve fitness klubech, v restauracích, na chodbách škol, úřadů a často i přímo v kancelářích zaměstnanců. Řady různých institucí a soukromých subjektů evidují o každém člověku tak detailní údaje, že se člověk může rázem cítit odhalen až na kost, pokud by se dozvěděl, kam až jeho osobní

data mohou doputovat. Pomocí propojení osobních počítačů ztrácíme pak soukromí i v oblastech, které byly ještě donedávna tabu. Ani v soukromí domácích čtyř stěn nejsme chráněni před sledováním našich aktivit. Není žádným problémem dohledat, a to i zpětně, veškerou aktivitu zadanou a prováděnou pomocí stolního počítače (mnohdy i včetně činností, které jsme prováděli v době momentálního nepřipojení na síti). Lze takto zjistit preference a záliby dané osoby, co má ráda, s kým komunikuje atd. atd. V dnešní době se také může běžně stát, že je člověku doslova ukradena jeho identita. V takovém případě jsou zneužita jména, čísla účtů, různé identifikátory, PIN kódy a jiná data určité osoby, přičemž bývá velmi těžké takové zneužití odhalit, resp. se proti němu účinně stoprocentně bránit. Veřejnosti je známo poměrně hodně případů zneužití obrazových záznamů na Internetu a v dalších médiích. Lidé často nahrávají své fotografie či videa na sociální sítě bez jakéhokoliv rozmyslu a neuvědomují si křehkost internetového systému a snadnost zneužití veškerých dat, která na Internetu o sobě poskytneme.

Čas od času pak zavíří společností aféra o zjevném porušení garantovaného práva na ochranu soukromí, která iluzi soukromí ještě více zničí. Veřejnost se tak dozvídá o nahrávání osob v převlékacích kabinách celonárodního obchodního řetězce, o kamerovém snímání policejních záběrů na soukromé byty, o materiálech důvěrné povahy, které se nedopatřením dostaly ze zabezpečeného systému (úniky dat z banky, ze zdravotnického zařízení apod.), o uniklých přepisech telefonních odposlechů či o nahrávání žáků ve třídách nebo na WC. Byť jsou tyto případy většinou postaveny mimo zákon a jsou nelegální, přesto se čas od času vyskytnou a asi nikdy je nepůjde zcela vymýtit. V lidech tyto excesy nicméně zanechávají hluboce zakořeněné přesvědčení o obecné zneužitelnosti jejich privátních údajů a jejich práva na soukromí.

Ve vyjmenovávání výše uvedených jednotlivých případů zásahů do soukromí pomocí moderních technologií by šlo pokračovat skoro do nekonečna. Již uvedené je ale po pravdě docela znepokojivé, a to ještě nebyly zmíněny metody a postupy bezpečnostních a detektivních agentur, které jsou schopny dle přání klienta zajistit pro něj prakticky veškeré informace dostupné ve všech možných státních i soukromých registrech či

podrobit jakoukoliv osobu odposlechu všeho, co řekne doma i na veřejnosti nebo do mobilu. Už vůbec se pak podrobně nezmiňuji o vojenských či špionážních technologiích, které mohou proniknout de facto kamkoli na zemském povrchu, včetně nitra budov způsobem, který spadá pro běžné smrtelníky spíše do kategorie sci-fi.

Není v silách jednotlivce ani v možnostech této práce poukázat na veškeré aspekty ochrany soukromí v kontextu obrazového sledování a moderních technologií. Téma ochrany soukromí je neskutečně obsáhlé; je však současně i vysoce aktuální a spolu s dalším rozvíjením všech moderních technologií bude nabývat čím dál více na významu. Je potěšitelné, že i Česká republika, a to jak z hlediska právního řádu, informovanosti odborné i laické veřejnosti, tak i z hlediska důležité práce neziskových organizací nezaostává za ostatními demokratickými státy světa a otázce ochrany soukromí přikládá čím dál vyšší pozornost. Domnívám se, že daný jev se stává obecným trendem a ochraně soukromí je obecně celosvětově věnováno stále více pozornosti a právní úprava v této oblasti se stává propracovanější a komplexnější. Přesto jde vývoj této právní úpravy (jak to v právu ostatně většinou bývá) mnohdy až v závěsu za společenským a technickým pokrokem.

V České republice dosud neexistuje mnoho komplexnějších právních publikací, které by předmětnou problematiku obrazových záznamů, kamerového sledování a ochrany soukromí zpracovávaly v celé její šíři. Dosavadní odborné práce se zaměřovaly především na jednotlivé dílčí problémy. Tato disertační práce si samozřejmě v žádném případě neklade za cíl pojmout problematiku v celém měřítku, nicméně se snaží podat i poněkud obecnější pohled na danou věc ve všech jejích souvislostech a pokouší se zpracovat veškeré dílčí problémy v jednom celku. Práce je tedy zaměřena na zhodnocení jednotlivých oblastí právního řádu a společenských vztahů, které jsou dotčeny problematikou obrazového monitoringu v souvislosti se zasahováním do soukromé sféry jednotlivce, a to jak ze strany veřejnoprávních, tak i soukromoprávních subjektů. V práci je místy nabízeno i částečné porovnání a odkazy na právní úpravu ve Slovenské republice, a to zejména s akcentem na institut sledování ze strany

bezpečnostních složek a s tím související problematiku ochrany soukromí (odposlechy, *zákon č. 166/2003 Z.z. o ochrane pred odpočúvaním* atd.).

Dílo je systematicky členěno do osmi základních částí (kapitol). Po **úvodu** zpracovává druhá kapitola **obecný pohled na ochranu soukromí**. Domnívám se, že pro potřeby komplexnějšího zpracování daného tématu je nutné vymezit ochranu soukromí a její instituty v obecnější rovině (byť s důrazem na sledovací a jiné technologie). Druhá kapitola proto pojednává místy až popisně o právním rámci obecné ochrany soukromí v právu České republiky, ale i v právu evropském a mezinárodním. Další kapitola je kapitolou obecnějšího charakteru a zabývá se komplexně a obecně **obrazovými záznamy a snímky**, základním úvodem do problematiky. Čtvrtá kapitola pojednává podrobněji **o kamerových sledovacích systémech** ve všech sférách jejich použití. Pátá kapitola zkoumá **obrazové záznamy v kontextu moderních informačních technologií**, včetně populárních témat sociálních sítí (Facebook, Youtube) a možností rizik narušení soukromí. Šestá kapitola řeší **další oblasti použití obrazových záznamů a snímků**, včetně zajímavé problematiky optického snímkování zemského povrchu (Street View, letecké mapy atd.). Práce pak končí **závěrem** s pokusem o shrnutí problematiky a o nástin možného budoucího vývoje. Zcela na závěr práce je pak uveden **přehled použité literatury**.

1.1 Obrazové sledování v dějinách

Lidé již od nepaměti využívají různých způsobů sledování a průzkumu okolí. V zájmu obrany vlastního území, národa nebo za účelem zajištění lepších technologií a vynálezů byli do okolních teritorií a států vysíláni nejrůznější ***špióni a vyzvědači***, přičemž se často využívaly různé technologie a způsoby, včetně obrazového sledování. Špióni byli často využíváni již starověkými civilizacemi Egypťanů, Řeků a Římanů.[1] V Číně

[1] Také v bibli nacházíme odkazy na vyzvědačství. Například je zde zmínka o vyslání 12 zvědů Mojžíšem, aby jej informovali o síle vojsk v zemi kananejské (Numeri 13). Jozue pak vysílá dva zvědy do země Jericho (Jozue 2:1 a násl.). Zdroj: Bible : Písmo svaté Starého a Nového zákona: český ekumenický překlad. 6. vyd. Praha: Biblická společnost, 1992.

někdy mezi lety 500 až 400 př. n. l. napsal vynikající čínský diplomat a stratég Sun-C knihu ***Umění války***, která obhajuje vyzvědačství jako jeden z hlavních prostředků k vítězství nad nepřítelem. Zhruba od 8. století n.l. v Japonsku působí kasta cvičených válečníků (tzv. ***ninjů***), kteří dovedli vyzvědačské umění k dokonalosti. V Evropě se špionáž a různé špionážní a sledovací techniky používají ve větší míře zhruba od 15. století. Jako budovatel rozsáhlé špionážní sítě proslul například francouzský kardinál Richelieu, který mimo jiné ustanovil v roce 1620 tzv. ***Cabinet Noir***, což bylo seskupení jeho poradců, které mělo analyzovat hlášení a různé údaje ze špionážní sítě.

Určitou formu špionáže, či řekněme přímo institucionalizovanou špionážní službu používal a stále používá prakticky každý stát. V Rusku byla např. založena v roce 1565 Ivanem Hrozným ruská politická policie – ***Opričnina***. Za panování Alexandra II. převzala úlohu zpravodajské služby tzv. ***Ochranka***, která měla kolem roku 1900 na své výplatní listině již 100.000 konfidentů, kteří působili ve všech větších ruských městech i v cizině. Tato organizace byla díky své rozvětvené síti detektivů, agentů, policejních špiclů a důvěrníků schopna shromáždit neskutečné množství zpráv, z nichž většina však zůstala nevyhodnocena. *Ochranka* proslula zavedením **cenzury sdělovacích technologií.**

Již od dávných dob bylo ke špionáži a sledování používáno nejrůznější technické vybavení. V dávných časech se špionáž prováděla pouze s pomocí vlastních očí a lidské paměti, případně v kombinaci s nejrůznějším způsobem zašifrovanými záznamy. Používaly se také neviditelné inkousty, různé druhy maskování a převleků apod. Velmi rozšířené byly různé **komunikační sítě** založené na kouřových, světelných, akustických, vlajkových či jiných signálech, které byly určeny k rychlému dopravování získaných informací. Tyto komunikační sítě byly zárodkem vzniku moderních informačních komunikačních technologií, jejichž rozšíření umožnil vědecký vývoj.

Skutečný **rozmach sledovacích a špionážních technologií** přichází však až s rozvojem vědy a techniky od 19. století, zejména však ve století dvacátém. Spolu s vývojem fotografických a telekomunikačních technologií je umožněno v dosud nebývalém rozsahu využívat těchto technologií i ke

sledovacím účelům. Rozmach špionáže a sledovacích technologií přinesl s počátkem 20. století jak technický pokrok, tak i zejména nutnost vyzvědačství v průběhu válečných konfliktů během první a druhé světové války, jakož i následného období tzv. studené války.

Po vyvinutí fotografické techniky se používá **fotografie a obrazové záznamy** mimo jiné i **ke sledovacím účelům**. Fotografické aparáty bývají montovány již v polovině 19. století na špionážní balony a později na letadla.[2] Ještě před vypuknutím 1. světové války vzniká Královský letecký sbor, jehož 3. eskadra pořizovala (nejprve neoficiálně) snímkování bitevního pole. Posléze existuje u každého britského armádního sboru oddělení zvláštních fotografických analytiků, kteří byli odpovědní za vyvolávání, kopírování a rozbor snímků pořízených leteckým průzkumem. Za druhé světové války je v Británii založeno **Armádní středisko analýzy leteckých fotografií – APIC**. Do konce války vydává APIC na 3810 podrobných zpráv.

Po skončení druhé světové války a začátcích studené války se rozšiřuje využívání všech forem špionáže a dokonalých moderních sledovacích technologií. Vedle leteckého snímkování se začínají rozvíjet i technologie **pokročilého odposlechu spojů**. Výkonná pozemní, ale i letecká či družicová zařízení jsou schopna cíleně zaměřit a monitorovat prakticky veškerou nepřátelskou komunikaci. V roce 1956 je poprvé vysláno do vzdušného prostoru států Varšavské smlouvy později známé letadlo Lockheed U-2, které pořizuje tisíce vysoce ostrých fotografií sovětských vojenských zařízení a výrobních center. Roku 1967 Sověti vypouští svou první špionážní družici Kosmos 168, následovanou řadou dalších družic (nejprve s jaderným pohonem, později nejaderným). Spojené státy využívají k monitorování své družice KH-11 a KH-12.

Spolu s polarizací světa na dva znepřátelené tábory (kapitalistický a komunistický) dochází k posilování úkolů a využití zpravodajských služeb.

---

[2] V roce 1858 je pořízen zřejmě první snímek ze vzduchu, když Felix Tournachon vyfotografoval z koše balonu Paříž. V roce 1862 jsou balony používány k pozorování pozic Konfederace při obléhání Richmondu za americké občanské války. V osmdesátých letech 19. století dosahuje letecká fotografie značného pokroku při pokusném snímkování majorem Elsdalem z Královského ženijního pluku. Roku 1909 jsou pořízeny první snímky z letícího aeroplánu. O tři roky později jsou letecké kamery poprvé užity Francouzy v bojové akci proti vzbouřeným domorodým kmenům v Maroku. Podrobněji viz opět LLOYD, M., tamtéž.

Tyto agentury, jakož i bezpečnostní sbory a policie, dostávají řadu **nových legálních pravomocí ke sledování** nejenom cizích agentů, ale i vlastních občanů, a to jak v souvislosti s bojem proti cizím státům, tak i pro boj s kriminalitou. Je logické, že sledování a monitorování lidí s sebou nese mnohdy **invazivní zásahy do soukromí**. Zejména komunistický blok otázku soukromí příliš neřešil a bezpečnostní orgány i přes své silné pravomoci často jednaly i zcela svévolně bez ohledu na alespoň minimální stupeň právním řádem garantované ochrany soukromí. Asi žádný jiný bezpečnostní orgán v minulosti nesledoval vlastní občany systematičtěji, mnohdy až s paranoickou důkladností, než východoněmecké **Ministerstvo státní bezpečnosti** (obávaná STASI). **STASI** zaměstnávala na 85.000 lidí a k tomu celou řadu dalších donašečů a spolupracovníků. V průběhu její činnosti byly pořízeny neskutečně rozsáhlé a mimořádně podrobné osobní svazky. Prakticky veškeré aktivity skoro všech lidí, s výjimkou těch nejnenápadnějších občanů, byly shromažďovány a archivovány. Obrovská část takto shromážděných informací však nebyla nikdy využita, spoustu materiálů dokonce ani nikdy nikdo nečetl.

I na území tehdejšího Československa existovalo velmi rozsáhlé sledování jednotlivců, zejména v režii policejního aparátu a Státní bezpečnosti.[3] Bezpečnostní orgány v tehdejší paranoické době nasazovaly na občany podezřelé zejména z protistátní činnosti všemožnou techniku a podrobovaly je důkladnému sledování, které zahrnovalo **osobní sledování agenty, tajné pořizování fotografických a video záznamů, prostorový i telefonní odposlech** atd.[4]

Spolu s rozmachem moderních sledovacích technologií se zhruba od počátku 20. století začíná objevovat i otázka s danou problematikou

---

[3] Již v roce 1966 byl kupř. zpracován tzv. „Rozbor využití průmyslové televize pro potřeby StB“ (Archiv Ministerstva vnitra, fond č. A-27, inv. j. 88)

[4] Daniel Povolný odkazuje ve své publikaci Operativní technika v rukou StB na vyšetřovací spis Inspekce Ministerstva vnitra v trestní věci porušování domovní svobody podle § 238 odst. 1 TZ, oznamovatel JUDr. Zdeněk Mlynář. Případ tajných odposlechů Dr. Mlynáře v rámci akce KRAJAN – BŘÍZA je jen jedním z mála „provalených“ případů, kdy tajné odposlechy při „boji s vnitřním nepřítelem“ vyšly na veřejnost. JUDr. Mlynář, jeho návštěvy a rodina byli v letech 1973 – 1974 obrazově sledováni, v jeho bytě probíhaly kontroly a byly v něm instalovány mikrofony, jeho telefon byl dlouhodobě odposloucháván. Celé vyšetřování sledovací kauzy Inspekcí Ministerstva vnitra bylo skončeno se závěrem, že „trestní stíhání se podle § 173 odst. 1 písm. e) tr. řádu přerušuje, protože se nepodařilo zjistit skutečnosti, opravňující konat trestní stíhání proti určité osobě.“ Celá kauza tak vyšuměla do ztracena.

související, a tou je **otázka soukromí každého jednotlivce**, jehož soukromá sféra může být těmito moderními technologiemi podstatně narušena. Již v roce 1890 formuluje americký advokát a později soudce Nejvyššího soudu USA *Louis D. Brandeis* spolu se *Samuelem D. Warrenem* v článku ***The Right to Privacy*** (*Právo na soukromí*) pokrokové myšlenky k otázce garance soukromí v kontextu s rozvojem nových sledovacích technologií a postupů. Ve svém článku zmiňují, že *ačkoliv je právo každého jednotlivce na ochranu své osoby a majetku staré jako právo samo, je nutno čas od času nově definovat povahu a rozsah takové ochrany… Nedávné objevy a obchodní metody vyvolávají potřebu dalšího kroku, který musí být učiněn pro ochranu osoby a pro zajištění těch práv jednotlivce, které soudce Cooley nazývá právem být ponechán o samotě (**the right to be let alone**).* Autoři poukazují ve svém díle na svou dobu velmi pokrokově na možnosti fotografie a jiných metod a technologií, včetně následného zveřejnění informací v novinách, které mohou citelně zasáhnout do soukromí jednotlivce. Článek je považován za **prvotní impuls pro další rozvoj pojmu práva na soukromí** a celé související problematiky – do té doby se otázkou soukromí právní teorie příliš nezabývala.[5]

S rozvíjením a uznáváním širokého katalogu lidských práv, do kterého je postupně zařazováno i právo každého člověka na soukromí, je **sledování pomocí nových technologií** postupně upravováno i právními řády jednotlivých států a mezinárodními dokumenty.[6]

---

[5] Celý článek The Right to Privacy je v anglickém jazyce k dispozici např. online na adrese: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html [cit. 2012-02-18]. Také viz Samuel D. Warren and Louis D. Brandeis: The Right to Privacy. 4 HARVARD LAW REVIEW, VOL. IV, December 15, 1890, No. 5.

[6] K jednomu z asi prvních setkání problematiky moderních sledovacích prostředků na soudní úrovni došlo v roce 1928 ve Spojených státech amerických v případu Olmstead (**Olmstead v. the United States**). Při vyšetřování pašeráka Olmsteada použila vláda odposlech telefonu podezřelého. Olmstead považoval odposlechy za protiústavní, neboť byly v rozporu se Čtvrtým dodatkem Ústavy. Nejvyšší soud sice dovodil, že čtvrtý dodatek Ústavy chránící občany před nezákonnými prohlídkami a sledováním se vztahuje pouze na případy fyzických případů zásahů do soukromí a neshledal umístění odposlechového zařízení na telefonních drátech na ulici poblíž Olmsteadova domu za nelegální, v dané věci však současně vyjádřil již zmiňovaný soudce Louis Brandeis na svou dobu nesmírně pokrokový odchylný disentový názor, kdy poukázal, že v době přijetí předmětného dodatku Ústavy technika vůbec neumožňovala jiné než fyzické zásahy do soukromí, nicméně v dnešní době technologického pokroku je nutno chránit soukromí občanů i před zasahováním do soukromí, které se neděje fyzickým způsobem (tzv. far-reaching means of invading privacy). Ve svém disentu tak soudce Brandeis jasně deklaroval, že každý neospravedlnitelný zásah ze strany

V současné době se více než kdy jindy naplňují na svou dobu vizionářská slova, která formuloval Louis Brandeis na konci 19. století. Dnes, v době, kdy právo prakticky není schopno reflektovat současné, dynamicky se vyvíjející technologie schopné velkých zásahů do soukromí, jsou slova L. Brandeise více než aktuální. V době, kdy není např. v českém právním řádu ani v právním řádu mnoha jiných zemí řádně a pregnantně upravena otázka používání kamerových systémů a jiných monitorovacích technologií, a to zejména ze strany soukromých subjektů, je více než důležité bez ohledu na absenci pozitivní zákonné úpravy hledat právní regulaci těchto nových společenských jevů analogicky v celém právním řádu, zejména v právních normách ústavního charakteru a v normách týkajících se ochrany lidských práv. Následně pomocí kvalitní judikatury lze aplikovat tyto normy na případné mezery v právu, jež mohou způsobovat potenciální nebezpečí pro právo na ochranu soukromí. Na příkladu moderních sledovacích technologií je dobře vidět, jak právo až s odstupem následuje překotný technologický i společenský vývoj, jak nestíhá kontinuálně reagovat na nová schémata a společenské jevy. Lze také pozorovat, jak se v této oblasti objevuje konkrétní právní úprava problematiky zásahů do soukromí nejprve ze strany **státních orgánů**, které jsou většinou snadněji zneužitelné, a jen zvolna je následována podrobnější úpravou zásahů do soukromí i ze strany **soukromých subjektů**. Otázka, zda je pro člověka nebezpečnější veřejnoprávní sféra, či zda se může objektivně cítit více ohrožen ze strany soukromých subjektů, je obtížně zodpověditelná. Významný světový sociolog ***Amitai Etzioni*** poukazuje v této souvislosti na tzv. **paradox soukromí** (The Privacy Paradox). Ze strany ochránců soukromí je totiž často voláno po přijetí legislativy, jež by chránila soukromí kvalitněji a efektivněji, přičemž je však často nedoceňován zajímavý paradox toho, že stát je na jedné straně považován za tzv. Big

státních orgánů, který narušuje soukromí občanů, bez ohledu na použité prostředky, je nutno považovat za porušení Čtvrtého dodatku Ústavy *(every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment).*

Brother, na straně druhé se však obecně spoléhá na jeho aktivitu při ochraně soukromí.[7]

[7] Problematiku mezí (limitů) soukromí ve světle možného zneužití ze strany takových moderních vědních oborů jako je biometrie či progresivní medicínské postupy (včetně databází, registrů DNA atd.) trefně zpracovává přední sociolog Etzioni ve své knize The Limits of Privacy. USA: Basic Books, 1999, v ČR bohužel zatím vydána nebyla.

2 OCHRANA SOUKROMÍ

2.1 Úvod do koncepce lidských práv

Lidská práva bývají nazírána a definována z hlediska více vědních oborů. Můžeme je vymezit jako určité nezadatelné a lidským bytostem přirozené nároky na život a jeho kvalitu.[8] Lidská práva jsou někdy definována i jako soubor nadčasových duchovních hodnot, jejichž základem jsou přirozené archetypy a vzory lidského chování a bytí, které se osvědčily a projevily v dlouhodobé lidské historii.[9] Obecně lze říci, a právní teorie v tom prakticky nalézá shody, že mezi lidská práva patří nejen ta, která jsou v daném časovém období zařazena do katalogu lidských práv vymezených ústavou a dalšími právními normami určitého státu. Naopak, lidská práva stojí dle přirozenoprávní koncepce nad ústavou, pozitivním právem i nad samotným státem a existují bez ohledu na momentálně platné právo. Pouze tyto obecně platné, nadčasové principy a ideje jsou pak kritériem, kterým lze poměřovat platnost lidských práv vymezených právem pozitivním.[10]

Pro vývoj ochrany lidských práv a přirozenoprávních tendencí byl významný **konec 18. století**. V této době totiž byly přijaty první ústavní dokumenty, které lze již označit za moderní přirozenoprávní vymezení **základního katalogu lidských práv**.

---

[8] V moderní době se objevují snahy o přiznání obdobných přirozených práv dokonce i jiným živým bytostem (viz např. uzákonění práv zvířecích primátů v zákoně o ochraně zvířat Animal Welfare Act 1999 na Novém Zélandu či Deklarace práv lidoopů přístupná online na www.greatapeproject.org). Tématu se věnuje článek ŠIMÁČKOVÁ, K.: Myšlenky o rozšíření subjektů přirozených práv v České republice. In: DANČÁK, B. – ŠIMÍČEK, V. (Eds.): Deset let listiny základních práv a svobod v právním řádu České republiky a Slovenské republiky. Masarykova univerzita v Brně a Mezinárodní politologický ústav, 2001.
Pokud jde o nejnovější legislativní vývoj v ČR- návrh nového občanského zákoníku živé zvíře sice již nechápe jako věc, nicméně přirozená práva ve smyslu lidských práv zvířeti nepřiznává (viz ustanovení § 470 nového o.z.).

[9] Viz BLAHOŽ, J. – BALAŠ, V. – KLÍMA, K.: Srovnávací ústavní právo. Praha: ASPI Publishing, 2003, str. 157 a násl.

[10] K problematice základního vymezení lidských práv a svobod srovnej i SUDRE, F.: Mezinárodní a evropské právo lidských práv, Masarykova univerzita v Brně, 1997 nebo PAVLÍČEK, V. a kolektiv: Ústavní právo a státověda. II. Díl Ústavní právo České republiky, Část 2. Praha: LINDE, 2004 či FILIP, J. – SVATOŇ, J. – ZIMEK, J.: Základy státovědy. 3. vydání. Masarykova univerzita v Brně, 2002

Podle právní teorie jsou lidská práva a svobody primárně členěny na **lidská práva**, což jsou práva a svobody náležející naprosto každé lidské bytosti bez ohledu na její státní příslušnost či místo jejího současného pobytu (mají osobní charakter a nevyjadřují bezprostřední spojení s člověka se státem). Druhou velkou skupinou jsou pak **práva občanská**, která vyplývají ze statusu člověka jako občana konkrétního státu (závisí tedy na příslušnosti daného člověka ke státu a jeho právnímu řádu). Podle situace se mohou však jednotlivá práva zařazovat někdy do práv lidských a někdy do práv občanských (kupř. právo na svobodu projevu). Z hlediska terminologie pak není prakticky žádný rozdíl mezi lidským právem a svobodou.[11]

Z hlediska detailnějšího členění se lidská práva a občanské svobody třídí na:

1. ***osobní práva a svobody*** (osobní nedotknutelnost, nedotknutelnost obydlí a dopravovaných zpráv, právo na ochranu soukromé sféry člověka, svoboda pobytu, a nepochybně i primární právo na život, svobodu a rovnost a lidskou důstojnost)
2. ***politická práva a svobody*** (svoboda slova a tisku, svoboda shromažďovací a spolčovací, volební právo apod.)
3. ***sociální, hospodářská a kulturní práva*** (právo na práci a odborové organizování, právo na nemocenské a sociální zabezpečení, právo na vzdělání, právo na ochranu zdraví atd.)[12]

V relativně nedávném vývoji teorie lidských práv můžeme pozorovat snahu o **rozlišování lidských práv podle generací**. Tzv. teorie generací lidských práv rozlišuje lidská práva na základě jejich postupného vývoje v rámci společenských a ústavněprávních změn. Postupně je proto nutno formulovat nová základní lidská práva a občanské svobody, které dříve společnost buď vůbec neakceptovala, nebo existovaly pouze v počáteční formě. Do *první generace lidských práv* jsou tak řazena především ta lidská práva, která formulovala klasická přirozenoprávní doktrína v průběhu 18. a 19. století. Po masivním nástupu sociálních hnutí lze pozorovat vymezení

[11] Srovnej opět BLAHOŽ, J. – BALAŠ, V. – KLÍMA, K. (cit. dříve).
[12] Srovnej tamtéž, str. 171-172.

druhé generace lidských práv, kam řadíme práva hospodářská, sociální a kulturní. Nejnovější *třetí generace lidských práv* pak vznikla v zásadě jako reakce na podmínky a nové skutečnosti, které s sebou přináší moderní technická civilizace. Do této generace pak můžeme zahrnout právo na rozvoj, právo na mír, právo na čisté a zdravé životní prostředí a nedotčenou přírodu. Jako nejnovější politická práva se pak vymezilo právo na informace, právo participovat se na tvorbě politických a státních rozhodnutí, právo na samosprávu, právo na kontrolu státní správy, právo na občanskou neposlušnost a další. Do práv, která můžeme pojmenovat jako práva sociální, hospodářská a kulturní, pak nově patří právo na ochranu zdraví, právo na solidaritu, právo na ochranu dětí a mládeže, právo na užívání kulturních statků a právo na bydlení. Mezi práva třetí generace bývá řazeno i ***právo na soukromí***, resp. ***právo na respektování soukromého života*** (soukromé sféry člověka). Právo na soukromí v moderním slova smyslu se začíná formulovat jako plnohodnotné základní lidské právo po II. světové válce, která byla po neblahých zkušenostech s totalitními režimy velkým impulsem pro rozvoj a nové nahlížení na lidská práva jako na práva přirozená, nezadatelná, nezcizitelná atd., náležející člověku z jeho samotné podstaty coby lidské bytosti. Právo na soukromí bylo dlouhou dobu chápáno jako jakési právo na klid, nedotknutelnost a neporušování citů, jako sféra, v níž je člověk obezděn a má nárok na to, aby nebyl protiprávně znepokojován ve svém příbytku.[13] Je třeba říci, že výše uvedená tzv. třígenerační teorie lidských práv, jež je například často používána v univerzálních světových organizacích (OSN atd.), má i své odpůrce. Ti proti této teorii namítají, že podsouvá myšlenku pokroku, což podněcuje k úvaze, že práv první a druhé generace již bylo dosaženo. Taktéž tato teorie svádí k anachronismu, kdy jako by práva druhé a především pak první generace patřila k jiné, dávné době, k jakési prehistorii lidských práv. V univerzálních organizacích, jako je zejména Organizace spojených národů, totiž převládlo kladení důrazu spíše na nové specifické hrozby a

[13] Viz MATES, P.: K některým otázkách ochrany soukromí v souvislosti se zajišťováním bezpečnosti ve správním právu. In: PAVLÍČEK, V. a kolektiv: Bezpečnost České republiky a potřeba ústavních změn. Sborník příspěvků a statí z mezinárodní konference Praha 18.-19.9.2003. Praha: Univerzita Karlova v Praze – Právnická fakulta, 2004

oblasti zájmu (mír, odzbrojení, životní prostředí) a „starší“ lidská práva prvních dvou generací se tak samovolně dostala poněkud do ústraní, bez ohledu na jejich faktickou realitu v některých členských státech OSN (když stále ještě mnohde nejsou řádně a účinně prosazována základní lidská práva založená zejména na svobodě člověka).

2.2 Pojem soukromí, právo na soukromí

O **definici pojmu soukromí** se pokoušelo již mnoho sociologů i právních teoretiků. Nikdo z nich však nemohl zodpovědně podat vyčerpávající a úplnou definici soukromí, neboť sám pojem je příliš široký a navíc je proměnný jak v čase, tak i v závislosti na podmínkách a okolnostech dané situace a daného člověka. Soukromí bývá často definováno **ve dvojím slova smyslu**. V užším smyslu je jím ochrana subjektivně vytvářené představy o soukromém životě člověka, v širším smyslu může pak soukromí spočívat i v ochraně širšího okolí bezprostředně navazujícího na životní potřeby a zájmy dané osoby spjaté především s rodinou, přáteli apod. Se soukromím člověka úzce souvisí i pojem nedotknutelnosti osoby, který je jako obecný princip namířen proti jakýmkoliv škodným vlivům zvenčí, tedy veřejné moci i soukromým subjektům a má vytvořit právní bariéru proti těmto zásahům.[14]

Otázkou definování pojmu soukromí se v poslední době ve své knize Ochrana soukromí ve správním právu zdařile zabývá P. Mates.[15] V současné době se podle něj ustupuje od klasického pojetí soukromí pouze jako sféry člověka, do níž nikdo nesmí zasahovat bez jeho souhlasu nebo pokud k tomu nemá zákonný důvod, a současně oblasti, o níž není povinen podávat informace a všem se zapovídalo tyto informace získávat a používat bez povolení dotyčné osoby, resp. bez zákonného podkladu (tzv. pojetí „soukromí čtyř stěn“, „*my house – my castle*“). Doktrína i judikatura dospěla k **mnohem širšímu pojetí soukromí**. Bylo například uvedeno, že zaměstnanec v rámci respektování soukromí a lidské důstojnosti má mít

[14] Srov. KLÍMA, K. a kol.: Komentář k Ústavě a Listině. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2005. s 645.

[15] Blíže srovnej MATES, P.: Ochrana soukromí ve správním právu. 2. vydání. Praha: LINDE, 2006, str. 14.

možnost, aby navazoval a udržoval sociální a individuální vztahy na pracovišti.[16] K otázce vymezení soukromého života se již mnohokrát vyjadřoval především **Evropský soud pro lidská práva**, který je bezpochyby velmi významnou institucí, jež zásadně ovlivňuje nazírání na právo na ochranu soukromí. Např. ve známém judikátu týkajícím se sporu advokáta pana Niemietze, v jehož advokátní kanceláři byla provedena podle něj nelegální prohlídka (což soud posléze potvrdil), soud uvedl, že *neshledává nezbytným ani nutným pokoušet se o vyčerpávající definici pojmu "soukromý život". Bylo by však příliš restriktivním omezovat tento pojem na "vnitřní kruh", v jehož rámci může jednotlivec žít svůj vlastní osobní život podle libosti, a zcela z něho vyloučit vnější svět nezahrnutý do tohoto kruhu.* ***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. Tento názor lze podepřít faktem, že - jak správně upozornila Komise -* ***není vždy možné jasně rozlišit, které činnosti jednotlivce tvoří část jeho profesního nebo obchodního života a které nikoli****. Takže zejména v případě osoby provozující svobodné povolání může být její práce v tomto kontextu tak významnou součástí jejího života, že se stává nemožným zjistit, v jakém postavení jedná v určitém okamžiku.* (Soud se v daném rozhodnutí také zabývá pojmem obydlí, kdy uvádí, že mnohdy jsou za obydlí považovány i obchodní místnosti, a to zvlášť u svobodných povolání.)[17] V jiné věci pak Evropský soud pro lidská práva dovozuje: „***soukromý život nesmí být vykládán restriktivně*** *a je třeba pod tento pojem zahrnovat i právo rozvíjet normální vztahy se svými bližními. Soukromí má být pojímáno nikoliv jen jako právo úzce spojené výhradně s osobou jednotlivce, ale jako vše, co přispívá k jeho vývoji, veškeré aspekty jeho duševní a fyzické integrity*."[18]

---

[16] Viz Doporučení č. (89)2 Výboru ministrů členským státům o ochraně osobních údajů používaných pro účely zaměstnání.

[17] Judikát ze dne 16.12.1992 ve věci Niemietz publikován pod č. 27/1996 Sb. r. ES

[18] Rozsudek ve věci Amann proti Švýcarsku z 16.2.2000.

Taktéž český **Ústavní soud** podává ve své judikatuře návod, jak lze nazírat na právo na ochranu soukromého života. Ve svém nálezu sp. zn. II. ÚS 517/99 ze dne 1.3.2000 se Ústavní soud neztotožňuje se zužujícím pojetím práva na ochranu soukromého života, které mimochodem vychází z konstrukce zakotvené v občanském zákoníku, a jehož předmětem je zejména pak **pouze** ochrana proti neoprávněnému získávání informací o skutečnostech ze soukromého života, případně jejich protiprávního šíření. Podle pojetí Ústavního soudu v tomto judikátu, který se zde opírá o dosavadní rozhodnutí Evropské komise a Evropského soudu pro lidská práva týkající se interpretace a aplikace čl. 8 odst. 1 Úmluvy, lze dovodit, že *respektování soukromého života musí zahrnovat do určité míry i* ***právo na vytváření a rozvíjení vztahů s dalšími lidskými bytostmi****. Součástí soukromého života je pak též* ***rodinný život*** *zahrnující i* ***vztahy mezi blízkými příbuznými****, když součástí rodinného života jsou nejen* ***sociální a morální vztahy****, ale také zájmy* ***materiální povahy*** *(např. vyživovací povinnost). Respektování takto pojatého rodinného života zahrnuje* ***závazek státu*** *jednat způsobem umožňujícím normální rozvoj těchto vztahů.*

P. Mates ve své publikaci dále uvádí, že k obdobnému názoru, jako shora v předešlých odstavcích prezentovanému, dochází i konstrukce, podle níž lze pojem soukromí chápat jednak v užším smyslu, jako ochranu **subjektivně vytvářené představy o soukromém životě,** jednak v širším smyslu, jakožto **ochranu rozsáhlejšího okolí, které bezprostředně navazuje na životní zájmy a potřeby osoby**, představované zejména jeho rodinou, příbuznými, přáteli apod. Funkcí právní ochrany soukromí je dle tohoto pojetí vytvoření potřebné bariéry před jakýmikoli škodlivými vlivy zvenčí, tedy jak ze strany veřejné moci, tak ze strany soukromých subjektů. I z tohoto pohledu má právo na soukromí dvě dimenze: předně jde o intimní sféru, kam se má člověk možnost uchýlit a bránit ji vůči těm, jimž sem není povoleno vstupovat, a dále oprávnění zvolit si způsob života, v němž je obsažena i možnost navazování nejrůznějších vztahů s okolním světem, souvisejících s osobností člověka (např. vztahy pracovní, rodinné a sexuální).[19]

[19] Viz MATES, P. (cit. práce, s. 16) a taktéž KLÍMA, K.: Ústavní právo. Praha 1999, s. 213.

Jak je tedy vidět, nelze výklad pojmu soukromí prakticky jednoznačně sjednotit a podat jeho vyčerpávající exaktní definici. Soukromí vždy bude velice individuální a proměnlivý pojem. Lze však uzavřít minimálně v tom smyslu, že **právo na soukromí je jakýsi soubor jednotlivých práv, jež chrání osobnost člověka v jeho celku**. Do těchto jednotlivých práv se řadí právo na nedotknutelnost intimní sféry, právo na osobní identitu (jméno a příjmení), právo na rodinný a sexuální život, právo na nedotknutelnost obydlí, právo na ochranu písemné korespondence a tajemství dopravovaných zpráv vůbec atd. Nelze přitom nezmínit rovněž právo na nejrůznější jiné sociální aktivity, na prvním místě pak aktivity v profesní (pracovní) sféře a vztahy s touto oblastí související. Můžeme také dovodit, že právo na soukromí má nemajetkovou povahu a působí proti všem (*erga omnes*), má univerzální povahu.[20] Právo na soukromí je všeobecně v mnoha státech světa chápáno jako nedílná součást moderního katalogu lidských práv (v některých státech, např. islámských, není však zejména z důvodu náboženských tradic právo na soukromí jednotlivce uznáváno).

Právo na soukromí však není absolutní, v určitých případech je možné jeho **omezení**. Při vymezení přípustnosti a zdůvodnitelnosti zásahů do soukromí se často používá znění čl. 8 odst. 2 Evropské úmluvy o ochraně lidských práv a svobod. Podle něj jsou zásahy do soukromí v zásadě možné pouze **v souladu se zákonem** a současně když je to **v demokratické společnosti nezbytné v zájmu legitimních zájmů** jako národní a veřejná bezpečnost, ochrana zdraví nebo morálky apod. Zákon by měl přitom stanovit i **rozsah zásahu do soukromí** a přesné podmínky jeho provedení. Vždy se také bude uplatňovat zásada přiměřenosti, která umožní jen takové zásahy do soukromí, jejichž pozitiva (veřejné, společenské či jiné zájmy) převáží negativní důsledky narušení soukromé sféry jednotlivce.

Z hlediska subjektu ochrany soukromého života platí, že jím může být **pouze fyzická osoba**. U osoby právnické se s pojmem ochrana soukromí nesetkáváme. Ústavní soud ve svém nálezu sp. zn. III ÚS 35/01 ze dne 3.5.2001 jednoznačně judikoval, že *„soukromí je ona sféra života*

[20] Srovnej opět MATES, P. (cit. práce, s . 20).

člověka, do které nesmí nikdo bez jeho souhlasu nebo bez výslovného dovolení zákona zasahovat ani o ní požadovat či získávat informace a o které subjekt soukromí není povinen nikomu podávat informace, pokud mu to zákon neukládá. Subjektem uvedené ochrany je však fyzická osoba. ***Jen stěží lze hovořit o ochraně soukromí u osob právnických****. U nich by v této souvislosti mohlo jít pouze o ochranu hospodářské soutěže či obchodního tajemství. Tato práva však nepodléhají ochraně dané Úmluvou o ochraně lidských práv a základních svobod."*

Nový občanský zákoník České republiky nicméně patrně poprvé v historii zavádí do legislativy i pojem soukromí právnické osoby – ve svém § 134 uvádí, že **právnické osobě náleží ochrana** proti tomu, kdo bez zákonného důvodu zasahuje do její pověsti nebo soukromí, ledaže se jedná o účely vědecké či umělecké nebo o tiskové, rozhlasové, televizní nebo obdobné zpravodajství; ani takový zásah však nesmí být v rozporu s oprávněnými zájmy právnické osoby.

Například v USA se nyní v rámci práva na soukromí rozlišuje kromě práva na soukromí ve „**fyzickém smyslu**", ochraňujícího zejména tělesnou integritu jednotlivce před nedovolenými prohlídkami či odposlechem, také právo na soukromí v „**informačním smyslu**", ochraňující hlavně korespondenci, záznamy, jakož i právo na soukromí v „**rozhodovacím smyslu**", ochraňující svobodnou volbu jednotlivce v těch záležitostech, které se dotýkají zejména jeho reprodukce, rodiny, zdravotní péče a životního stylu. Již v roce 1967 bylo soudem formulováno stanovisko, že jednotlivec má právo „***na přiměřené očekávání soukromí***" nezávisle na místě, kde se člověk nachází (tedy i mimo prostředí svého domova).[21]

---

[21] V roce 1967 bylo ve Spojených státech amerických vydáno průlomové soudní rozhodnutí v kauze ***Katz versus USA*** (389 US. 347). Nejvyšší soud deklaroval, že státními orgány prováděný odposlech veřejné telefonní budky byl protiústavní, neboť jednotlivec nemůže očekávat při telefonování z budky, byť umístěné na ulici, takový zásah do svého soukromí. Soud formuloval jasné pravidlo, že vždy, kdy jednotlivec **odůvodněně očekává zachování svého soukromí**, státní orgány potřebují k zásahu do soukromí soudní příkaz (*a warrant is required whenever the individual has a reasonable expectation of privacy*). Soud taktéž zejména jasně formuloval, že jednotlivec má právo na ochranu nezávisle na místě, kde se nachází (tj. nikoliv jen ve svém domově), nýbrž má právo na přiměřené očekávání soukromí kdekoliv. Soudní rozhodnutí ve věci Katz je dostupné např. online na http://www.vlex.us/caselaw/U-S-Supreme-Court/Katz-v-United-States-389-U-S-347-1967/2100-19992409%2C01.html [cit. 2012-02-18]. K problematice práva na soukromí v ústavním právu USA dále

Dané **očekávání soukromí** ze strany každého člověka je však dozajista individuální, závislé na dané lidské bytosti (u veřejně známých osob bude míra jejich důvodně očekávaného soukromí nižší) a jednak je také proměnné v čase. Lze jen přitakat, že kupříkladu před nějakými sto padesáti lety existovala potenciálně velmi vysoká míra očekávatelného soukromí každého jednotlivce. Neexistovaly prakticky žádné sledovací a jiné technologie, které by byly, tak jako je tomu v dnešní době, schopny soukromí intenzivně narušit. Míra očekávání soukromí se mění také s ohledem na situaci a prostředí, kde se zrovna daná osoba nachází. Těžko tak dnes lze důvodně očekávat vysokou míru soukromí na rušné ulici v centru velkoměsta, kde je člověk jednak pod dohledem ostatních občanů, ale současně jej monitorují početné kamery, jeho pohyb je detekovatelný podle signálu jeho mobilního telefonu, výběrů z bankomatů atd. Oproti tomu lze doma, v soukromí čtyř stěn, stejně tak i v zaměstnání, v kanceláři, očekávat relativně vyšší míru soukromí, kde člověk většinou neuvažuje, že by jej někdo cizí bez jeho souhlasu podroboval nějakému sledování (byť u některých aktivit lze toto sledování někdy i zde předpokládat).

V následujícím textu se pokusím podat základní přehled právní úpravy ochrany soukromí, a to jak v právu mezinárodním, tak v pojetí práva evropského (EU, Rada Evropy, vybrané ústavní listiny evropských zemí) a samozřejmě českého (včetně zmínky o slovenské právní úpravě).

2.3 Institut ochrany soukromí v mezinárodním právu

Podle ustanovení čl. 10 Ústavy ČR (zákon č. 1/1993 Sb. ze dne 16. prosince 1992, Ústava České republiky) jsou **vyhlášené mezinárodní smlouvy**, k jejichž ratifikaci dal Parlament souhlas a jimiž je Česká republika vázána, součástí právního řádu s tím, že stanoví-li mezinárodní smlouva něco jiného než zákon, použije se mezinárodní smlouva. Tyto mezinárodní smlouvy tedy stojí na pomezí mezi běžnými zákony a ústavními normami. Pokud je český zákon v rozporu se zněním takovéto

---

blížeji viz např. Seltenreich, R.: Právo na soukromí v kontextu ústavního vývoje USA; Právník 1/2000, str. 24 – 26.

mezinárodní smlouvy, je v každém případě nutné aplikovat přímo úpravu dle mezinárodního dokumentu. V mnoha takovýchto mezinárodních smlouvách se hovoří i o právu na ochranu soukromí. Jmenujme alespoň ty nejzásadnější a pro problematiku ochrany soukromí nejdůležitější dokumenty, a to vždy i s citací konkrétního ustanovení, které se zabývá právem na ochranu soukromí:

Mezinárodní pakt o občanských a politických právech (vyhláška ministra zahraničních věcí č. 120/1976 Sb. ze dne 10. května 1976, o Mezinárodním paktu o občanských a politických právech a Mezinárodním paktu o hospodářských, sociálních a kulturních právech), konkrétně:

„**Čl. 17**

1. Nikdo nesmí být vystaven svévolnému zasahování do **soukromého života**, do rodiny, domova nebo korespondence ani útokům na svou čest a pověst.
2. Každý má právo na zákonnou ochranu proti takovým zásahům nebo útokům.“

Úmluva o právech dítěte (sdělení federálního ministerstva zahraničních věcí č. 104/1991 Sb.), která pro tehdejší Českou a Slovenskou Federativní Republiku vstoupila v platnost v souladu se svým článkem 49 odst. 2 dnem 6. února 1991.:

„**Čl.16**

1. Žádné dítě nesmí být vystaveno svévolnému zasahování do svého **soukromého života**, rodiny, domova nebo korespondence ani nezákonným útokům na svou čest a pověst.
2. Dítě má právo na zákonnou ochranu proti takovým zásahům nebo útokům.“

Deklarace o lidských právech jednotlivců, kteří nejsou státními občany země, v níž žijí z 13. prosince 1985:

Čl. 5 odst. 1

Cizinci požívají v souladu s domácím právem s výhradou odpovídajících mezinárodních závazků státu ve kterém jsou přítomni, zejména následující práva:

…..

b) **právo na ochranu proti svévolnému nebo protiprávnímu zasahování do soukromí**, rodiny, domova nebo korespondence

……

Úmluva na ochranu lidských práv a důstojnosti lidské bytosti v souvislosti s aplikací biologie a medicíny: **Úmluva o lidských právech a biomedicíně** (sdělení Ministerstva zahraničních věcí č. 96/2001 Sb.m.s.), která pro Českou republiku vstoupila v platnost podle odstavce 4 téhož článku dne 1. října 2001:

„**Čl. 10 Ochrana soukromí** a právo na informace
1. Každý má právo na **ochranu soukromí** ve vztahu k informacím o svém zdraví.
2. Každý je oprávněn znát veškeré informace shromažďované o jeho zdravotním stavu. Nicméně přání každého nebýt takto informován je nutno respektovat.
3. Pokud je to v zájmu pacienta, může ve výjimečných případech zákon omezit uplatnění práv podle odstavce 2.“

Všeobecná deklarace lidských práv – přijatá Valným shromážděním OSN 10. prosince 1948 ve formě rezoluce č. 217/III. A:

Čl. 12
Nikdo nesmí být vystaven svévolnému **zasahování do soukromého života**, do rodiny, domova nebo korespondence ani útokům na svou čest a pověst. Každý má právo na právní ochranu proti takovým zásahům nebo útokům.

Mezi výše jmenované a pro ČR platné a závazné mezinárodní úmluvy se samozřejmě řadí i řada dokumentů na poli evropské spolupráce, a to jak v rámci EU, tak i v rámci Rady Evropy – k nim však blíže v následující kapitole.

2.4 Institut ochrany soukromí v evropském měřítku

2.4.1 Rada Evropy

Zcela nejzásadnějším dokumentem přijatým na platformě Rady Evropy je v oblasti práva na ochranu soukromí a ostatních lidských práv **Úmluva o ochraně lidských práv a základních svobod** sjednaná v Římě dne 4. listopadu 1950, podepsaná jménem České a Slovenské Federativní Republiky 21. února 1991 (sdělení federálního ministerstva zahraničních věcí č. 209/1992 Sb. ve znění sdělení č. 41/1996 Sb. a sdělení č. 243/1998 Sb.). Pro tehdejší ČSFR vstoupila v platnost v souladu s článkem 66 odst. 3 dnem 18. března 1992. Tato úmluva kromě celého katalogu jiných lidských

práv a základních svobod zmiňuje ve svém článku 8 i právo na respektování rodinného a soukromého života. Pro přehlednost opět citujme:

„**Čl. 8 Právo na respektování rodinného a soukromého života**

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

Společně s ratifikací této Úmluvy uznala tehdejší Česká a Slovenská Federativní Republika na základě vzájemnosti významnou pravomoc **Evropského soudu pro lidská práva** k výkladu a použití Úmluvy. Jakožto vyhlášená a Parlamentem ratifikovaná mezinárodní smlouva, kterou je ČR vázána, je tato Úmluva součástí českého právního řádu a má přednost před vnitrostátními zákony, je bezprostředně závazná. Občané ČR se tedy práv zaručených touto Úmluvou mohou dovolat u příslušné instituce bez ohledu na znění (a případné restrikce a omezení práv z této Úmluvy) zákonů ČR. Je také pravdou, že pod vlivem této Úmluvy a zejména navazující judikatury Evropského soudu pro lidská práva dochází i ke změnám v českém právním řádu a zejména v jeho výkladu, neboť české soudy používají čím dál častěji ve svých rozhodnutích argumentaci dle této Úmluvy a dle Evropského soudu pro lidská práva.

Evropský soud pro lidská práva se po změnách přinesených Protokolem č. 11, který doplnil původní Úmluvu o ochraně lidských práv a základních svobod, stal jedinou permanentně zasedající soudní institucí, která přijímá jak individuální stížnosti, tak i stížnosti mezistátní.[22]

Z hlediska **práva na respektování rodinného a soukromého života** v kontextu moderních technologií vydal Evropský soud pro lidská práva (resp. instituce existující před nabytím platnosti Protokolu č. 11) řadu rozsudků, které se daného tématu týkaly. Ve věci Lüdi versus Švýcarsko například Evropský soud pro lidská práva deklaroval, že použití tajného agenta nenarušilo samo o sobě nebo v kombinaci s telefonním odposlechem

[22] Před nabytím platnosti Protokolu č. 11 existovaly vedle sebe Evropská komise a Soud pro lidská práva. Každá stížnost musela být nejprve projednána před Evropskou komisí.

soukromý život ve významu článku 8. Pan Lüdi (který byl švýcarským překupníkem drog) si tudíž musel být vědom, že se účastní činu, trestného podle článku 19 zákona o drogách, a že v důsledku toho podstupuje riziko setkání s tajným policejním agentem, jehož úkolem bude odhalit jej. Telefonní odposlech byl sice zásahem do soukromého života a korespondence pana Lüdiho, takový zásah však nezakládá porušení Úmluvy, jestliže je v souladu s požadavky odstavce 2 článku 8 Úmluvy. Dotyčná opatření se zakládala na článku 171b a 171c bernského trestního řádu, který, jak shledal Spolkový soud, se používá pouze ve stádiu předběžného vyšetřování, kdy se lze oprávněně domnívat, že zde teprve dojde ke spáchání trestného činu. Mimo jiné to je otázka prevence zločinnosti a Soud nemá pochyby o její nezbytnosti v demokratické společnosti.[23]

2.4.2 Evropská unie

Samozřejmě i v rámci Evropské unie je velmi významnou složkou jejího působení problematika ochrany lidských práv, mezi které je řazeno i právo na soukromí. Soukromím a jeho ochranou se Evropská unie zabývá v řadě svých dokumentů. Vyjmenujme opět zcela demonstrativně alespoň některé.

Předně je takovým dokumentem Lisabonská smlouva, podepsaná 13.12.2007 v portugalském Lisabonu a ratifikovaná 3.11.2009, platná od 1.12.2009. Její součástí je i Listina základních práv Evropské Unie. Listina základních práv Evropské Unie vychází ze znění původní Charty základních práv z Nice. Pokud jde o ochranu soukromí, Listina základních práv Evropské Unie upravuje:

Článek 7
Respektování soukromého a rodinného života
Každý má právo na respektování svého soukromého a rodinného života, obydlí a komunikace.

[23] Podrobněji k judikatuře Evropského soudu pro lidská práva zabývající se ochranou soukromí viz i pojednání k článku 10 Listiny základních práv a svobod v kapitole 2.5.2 této práce. Jako nejvýznamnější rozsudky vztahující se k právu na soukromí zejména v kontextu sledování obecně viz kupř. Niemietz versus Německo, Klass a ostatní versus Německo, Halfordová proti Spojenému Království, Amann proti Švýcarsku, Kopp proti Švýcarsku atd.

Článek 8

Ochrana osobních údajů

1. Každý má právo na ochranu osobních údajů, které se ho týkají.
2. Tyto údaje musí být zpracovány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem. Každý má právo na přístup k údajům, které o něm byly shromážděny, a má právo na jejich opravu.
3. Na dodržování těchto pravidel dohlíží nezávislý orgán.

Jde prakticky o shodné znění, jaké bylo obsaženo v Chartě základních práv z Nice a jejích článcích II-67 a II-68.[24]

Jako další právní normy Evropské unie můžeme zmínit řadu směrnic a nařízení, které se zabývají problematikou ochrany soukromí. Za všechny jmenujme Směrnici Evropského parlamentu a Rady č. 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a s volným pohybem těchto údajů; jakož i nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů, Směrnici Evropského parlamentu a Rady č. 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací - Směrnice o soukromí a elektronických komunikacích, a neposlední řadě kontroverzní Směrnici Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES (tzv. data retention směrnice). Na tomto místě bych rád poukázal na skutečnost, že české právní předpisy, které danou směrnici transponovaly do právního řádu, byly

[24] Česká republika vyjednala na jednání Evropské rady v říjnu 2009 politický příslib ostatních členských států EU připojit ke Smlouvě o EU a ke Smlouvě o fungování EU Protokol o uplatňování Listiny základních práv EU v České republice, v jehož důsledku by měl být dříve sjednaný Protokol Polska a Spojeného království modifikován tak, aby se vztahoval i na ČR (Polsko a Spojené království dojednaly v rámci Protokolu č. 30 výjimku pro své země z uplatňování Listiny základních práv Evropské unie). Listina základních práv EU by se tak v ČR v budoucnu uplatňovala jen s výjimkami, nebyla by de facto soudně vymahatelná. Daná výjimka byla politicky prosazena zejména z iniciativy prezidenta Václava Klause. (viz dokument ze dne 13.04.2011 - Protokol o uplatňování Listiny základních práv Evropské unie v Polsku a ve Spojeném království, dostupný na stránkách Min. zahraničních věcí: http://www.mzv.cz/jnp/cz/zahranicni_vztahy/evropska_unie/pravo_evropske_unie/aktualni_novely_primarniho_prava_eu/lisabonska_smlouva/protokol_o_uplatnovani_listiny.html)[cit. 2012-02-18].

zrušeny nálezem Ústavního soudu Pl. ÚS 24/10 ze dne 22.3.2011.[25] Závazek transponovat evropskou směrnici nadále trvá, v ČR se již se připravuje nová právní úprava (novela zákona o elektronických komunikacích a trestního řádu a nová prováděcí vyhláška, které by umožnila policejním orgánům opět přístup k provozním a lokalizačním údajům). Nicméně i osud samotné evropské data retention směrnice taktéž není zcela jistý; jak vyplývá z hodnotící zprávy Komise Radě a Evropskému parlamentu ze dne 18.4.2011, navrhne Komise revizi stávajícího rámce pro uchovávání údajů.[26] Směrnice je na základě podání Irska z roku 2006 předmětem přezkumu Evropským soudním dvorem. Vnitrostátní transpozice směrnice byly již zrušeny také Nejvyšším správním soudem v Bulharsku a Nejvyšším soudem na Kypru; v současné době jsou předmětem ústavní stížnosti v Maďarsku a Polsku. Jako první v Evropě byly vnitrostátní transpozice zrušeny rumunským ústavním soudem (8.10.2009) a po něm německým Spolkovým ústavním soudem (2.3.2010).[27]

Jak bylo tedy naznačeno výše, Evropská unie Směrnici 95/46/ES aktualizuje a v souvislosti s touto plánovanou aktualizací vydala Evropská komise v listopadu roku 2010 dokument nazvaný **„Komplexní přístup k ochraně osobních údajů v Evropské unii.“**[28] Dokument se nejprve odvolává na směrnici o ochraně osobních údajů z roku 1995, kterou považuje za v tu dobu přelomovou. V současné době však již existuje řada nových problematických aspektů globalizace, pronikání stále dokonalejších

---

25 Ústavní soud zrušil ustanovení § 97 odst. 3 a 4 zákona č. 127/2005 o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a vyhlášku č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání.

26 Viz ZPRÁVA KOMISE RADĚ A EVROPSKÉMU PARLAMENTU - Hodnotící zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES) ze dne 18.4.2011 dostupná na: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:CS:PDF [cit. 2012-02-18].

27 Není také bez zajímavosti, že transpozice směrnice nebyla důsledně provedena několika evropskými státy a v důsledku toho se tyto státy staly předmětem řízení s Komisí evropských společenství a v některých případech na popud Komise judikoval ESD o porušení povinnosti transponovat směrnici do národního právního řádu – Nizozemí, Řecko, Rakousko.

28 Viz SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU, RADĚ, EVROPSKÉMU HOSPODÁŘSKÉMU A SOCIÁLNÍMU VÝBORU A VÝBORU REGIONŮ – Komplexní přístup k ochraně osobních údajů v Evropské unii, ze dne 4.11.2010 č. KOM(2010) 609, dostupné online na: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_cs.pdf [cit. 2012-02-18].

informačních technologií do lidského života a s tím spojených rizik ve vztahu k právu na ochranu soukromí. Způsoby shromažďování osobních dat jsou stále sofistikovanější a objevují se nová geolokační či mobilní zařízení, díky kterým je snadné vysledovat pohyb osob. Dokument si všímá i narůstající tendence státních orgánů využívajících stále více a více osobních údajů o občanech pro prevenci terorismu a trestných činů, nebo pro využití v mnoha aplikacích elektronické veřejné správy. Dokument dává evropským orgánům určité vodítko, jak dále na poli legislativní úpravy ochrany soukromí postupovat, poukazuje na nutnost změny nařízení (ES) č. 45/2001 a dalších dokumentů.

Závěrem bych rád zmínil existenci funkce Evropského inspektora ochrany údajů (European Data Protection Supervisor - EDPS). Jeho úkolem je nadnárodní dohled při zpracování osobních údajů, jakož i garance, že všechny instituce a orgány EU budou respektovat právo svých občanů na soukromí při zpracovávání jejich osobních údajů. EDPS je propojen s národními ochránci osobních údajů prostřednictvím Pracovní skupiny článku 29. Každá instituce nebo orgán EU má pak mít svého vlastního Ochránce osobních údajů (Data Protection Officer – DPO), který by registroval zpracovatelské operace a hlásil rizika a problémy EDPS.

Hlavní bod střetávání názorů a diskusí, jakož i vzájemné nadnárodní kooperace v oblasti ochrany osobních údajů a soukromí na poli Evropské unie představuje již zmíněná tzv. **Pracovní skupina pro ochranu údajů zřízená podle čl. 29** směrnice 95/46/ES („The Article 29 Working Party“), což je de facto poradní orgán pro otázky ochrany údajů a soukromí.

Je složena ze zástupců jednotlivých národních úřadů na ochranu osobních údajů, dále je v ní Evropský inspektor ochrany údajů a zástupci Evropské komise.

2.4.3 Ochrana soukromí v ústavách evropských států

Podívejme se nyní na ústavní dokumenty některých evropských států **z pohledu implementace práva na ochranu soukromí a práv jemu příbuzných**, pro nás zajímavých, tj. práva na nedotknutelnost obydlí, práva na zaručení tajemství dopravovaných zpráv a konečně práva na ochranu osobních údajů. Pro velký rozsah tématu uvádím citace jen těch částí ústav,

které garantují výslovně právo na ochranu soukromí. Ty ústavy, které obsahují garanci pouze práv ochraně soukromí podobných (nedotknutelnost obydlí, korespondence a osobních údajů) uvádím jen ve stručném přehledu.

Na příkladu práva na ochranu soukromí a jemu příbuzných práv můžeme dobře sledovat postupný vývoj a začleňování tohoto institutu do ústavních listin jednotlivých států. Vidíme, že na sklonku vývoje ústavních dokumentů – to se týká tedy historicky nejnovějších ústav zemí bývalého totalitního komunistického bloku – se na rozdíl od starších evropských ústav právo na ochranu a respektování soukromí objevuje již zcela pravidelně. Výtahy z ústav jsou povětšinou ve znění cca k roku 2003, u ústav, kde není znění uvedeno, platí že jsou zpracovány k roku 1997.[29]

Bývalé postsovětské země:

Rusko - Ústava z 25.12.1993

Článek 23
(1) Každý má právo na nedotknutelnost soukromého života, osobní a rodinné tajemství, na ochranu své cti a dobrého jména.
(2) Každý má právo na tajemství listovní, telefonních rozhovorů, poštovních, telegrafních a jiných zpráv. Omezení tohoto práva je přípustné pouze na základě rozhodnutí soudu.
Článek 24
(1) Shromažďování, uchovávání, využívání a šíření informací o soukromém životě osoby bez jejího souhlasu je nepřípustné.
(2) Orgány státní moci a orgány samosprávy, jejich úřední osoby jsou povinny zajistit každému možnost seznámit se s dokumenty a materiály, které se přímo dotýkají jeho práv a svobod, pokud zákon nestanoví jinak.

Litva

Ústava republiky Litva přijatá formou referenda dne 25.10.1992, vyhlášena byla dne 6.11.1992 (znění k roku 2004):

Čl. 22
Soukromý život člověka je nedotknutelný.
Listovní tajemství, tajemství telefonických hovorů, dálnopisných zpráv a dalších osobních sdělení se nesmí porušit.
Informace o soukromém životě osob lze shromažďovat pouze na základě odůvodněného soudního rozhodnutí a zákona.
Zákon a soud chrání osobní a rodinný život každého před svévolným a protiprávním vměšováním a před porušením jeho cti a důstojnosti.

[29] Znění většiny ústav bylo převzato z obou dílů publikace KLOKOČKA, V. – WAGNEROVÁ, E.: Ústavy států Evropské Unie. Praha: LINDE, 2004 a dále z díla PAVLÍČEK, V. a kolektiv: Transformace ústavních systémů zemí střední a východní Evropy. I. a III. část. Praha: Univerzita Karlova v Praze – Právnická fakulta, 1999 (I. část), resp. 2001 (III. část)

Obdobná úprava, včetně výslovné garance práva na soukromý život existuje i v jiných postsovětských státech, např. v ústavě Estonska, Lotyšska, Ukrajiny a Běloruska.

Ostatní evropské státy bývalého komunistického bloku:

Polsko

Ústava Polské republiky schválená dne 2.4.1997 (znění k roku 2003):

Čl. 47
Každý má právo na právní ochranu soukromého a rodinného života, cti a dobré pověsti, jakož i právo rozhodovat o svém osobním životě.

Bulharsko

Ústava schválena dne 12.7.1991

Čl. 32
(1) Osobní život občanů je nedotknutelný. Každý má právo na ochranu před nezákonným zasahováním do svého osobního a rodinného života a proti útoku na svou čest, důstojnost a dobré jméno.
(2) Nikdo nemůže být sledován, fotografován, filmován, zapisován, nebo podroben jiným podobným jednáním bez svého vědomí nebo přes svůj výslovný nesouhlas, vyjma v zákonem stanovených případech.

Lze říci, že v těchto případech jde o moderní ústavy, které často čerpaly z mezinárodních dokumentů, a proto většinou zmiňují výslovné zaručení práva na ochranu soukromí, resp. soukromého života. Tuto garanci tak můžeme dále nalézt v ústavách Maďarska, Rumunska, Slovinska, Chorvatska, Makedonie a jiných států.

Evropské země bývalého západního bloku:

Velká část evropských států, zejména z bloku bývalých „západních" zemí, které své ústavy většinou přijímaly již před desetiletími, nemá právo na ochranu soukromí, resp. soukromé sféry jednotlivce, implementováno přímo do svého ústavního pořádku. Ten tak povětšinou obsahuje jen **garanci příbuzných práv**, jako je nedotknutelnost obydlí, poštovního, telegrafního, telefonického apod. tajemství a garanci ochrany osobních údajů. Jde např. o Dánsko (ústava z roku 1953), Francii (ústava z roku

1958), Itálii (ústava z roku 1947), Rakousko (ústava z roku 1920), Lucembursko či Irsko. Ve Velké Británii, která sice nemá psanou ústavu, pak existuje Zákon o lidských právech z 9.11.1998, kterým se součástí práva Spojeného království přímo stala Evropská úmluva o ochraně lidských práv a základních svobod.

Výjimkami s výslovným zmíněním ochrany soukromého života jsou například Portugalsko, Španělsko, Řecko, Belgie či Nizozemí:

Portugalsko

Ústava z 2.4.1976 (ve znění k roku 2003):

Čl. 26
(1) Každému se přiznává právo na osobní identitu, na rozvoj osobnosti, na občanskou způsobilost, na státní občanství, na osobní čest, na dobré jméno a pověst, na vlastní představy a vlastní vyjádření a na ochranu soukromého a rodinného života jakož i ochranu před jakoukoliv formou diskriminace.
(2) Účinné záruky proti zneužívání nebo proti užití informací o osobách a rodinách, směřující proti lidské důstojnosti budou stanoveny zákonem.
(3) Zákon zaručuje osobní úctu a genetickou identitu osobnosti, zejména v souvislosti s vývojem a použitím technologií při vědeckých pokusech.
(4) Odnětí státního občanství a omezení občanské způsobilosti lze uskutečnit pouze v případech a v míře určené zákonnými předpisy a nelze je opřít o politické důvody.

Portugalská ústava nabízí také velmi konkrétní ústavní **ochranu osobních údajů** v archivech, registrech a podobných systémech. Také zakazuje stanovení jednotného identifikačního čísla pro občany:

Čl. 35
(1) Všichni státní občané mají v mezích zákona právo být seznámeni se všemi trvalými záznamy v archivech nebo výpočetní technikou zřízených registrech, jakož i s účelem těchto údajů a požadovat opravu a aktualizaci těchto údajů.
(2) Zákon stanoví úpravu osobních dat a stanoví podmínky jejich automatizovaného zpracování, uložení do sítě, přenosu a přístupu k nim; současně zaručuje ochranu dat v rámci nezávislého úřadu.
(3) Elektronické zpracování dat nesmí být použito ke zpracování dat o světonázorovém a politickém přesvědčení, o příslušnosti ke stranám nebo odborům, o náboženském vyznání nebo soukromém životě; z toho jsou vyňaty případy výslovného souhlasu oprávněných a výslovného nediskriminujícího zmocnění, jakož i zpracování dat bez personální identifikace.
(4) Přístup třetích osob k osobním archivům a souborům dat a tomu odpovídající propojení jsou zakázány s výjimkou případů stanovených v zákoně.
(5) Je zakázáno stanovit pro státní občany jednotné identifikační číslo.
(6) Každý má přístup k veřejně přístupným databázím; zákon stanoví postup, použitelný pro výměnu dat, přesahujících hranice; stanoví přiměřená ochranná opatření pro údaje týkající se osob a ostatní údaje, jejichž ochrana je oprávněna na základě národních zájmů.
(7) Osobní údaje v normálně ovládaných databázích požívají stejné stanovené ochrany, pokud zákon nestanoví jinak.

Španělsko

Ústava ze 29.12.1978 (ve znění k roku 2003):

Čl. 18

(1) Každý má právo na čest, osobní a rodinné soukromí a právo na vlastní vývoj své osobnosti.

(2) Obydlí je nedotknutelné. Vstup nebo prohlídky nesmí se uskutečnit bez souhlasu majitele nebo bez soudního rozhodnutí, pokud nejde o případ dopadení při činu.

(3) Tajemství dopravovaných zpráv, zejména poštovní, telegrafní a telefonní tajemství se zaručuje, pokud nerozhodne soud jinak.

(4) Zákon omezuje užití informatiky tak, aby byly zajištěny čest, jakož i osobní a rodinné soukromí občanů a plný výkon jejich práv.

Řecko

Ústava ze 9.6.1975 (ve znění k roku 2003):

Čl. 9

(1) Domov každého je chráněným místem. Soukromý a rodinný život jednotlivce je nedotknutelný. Domovní prohlídky smějí být prováděny jen v zákonem stanovených případech a zákonem stanoveným způsobem, avšak vždy jen v přítomnosti reprezentantů soudní moci.

(2) Kdo poruší ustanovení předchozího odstavce, bude potrestán za narušení útočiště domova a za zneužití pravomoci, a je plně odpovědný za náhradu utrpěné škody, jak stanoví zákon.

Belgie

Ústava ze dne 17.2.1994 (znění k roku 2003):

Čl. 22

Každý má právo na ochranu svého soukromého života s výjimkou případu a podmínek, které stanoví zákon. Zákon, dekret nebo pravidlo, stanovené v článku 134 zaručuje ochranu tohoto práva.

Čl. 22 bis

Všechny děti mají právo na zachování své integrity morální, fyzické, psychické a sexuální. Zákon, dekret nebo pravidlo, stanovené v článku 134 zaručuje ochranu tohoto práva.

Nizozemí

Ústava ze 17.2.1983 (ve znění k roku 2003):

Čl. 10

(1) Každý má právo na respektování svého soukromí, není – li povoleno omezení zákonem, nebo na základě zákona.

(2) Ochrana soukromé sféry je v souvislosti s ukládáním a předáváním osobních údajů upravena zákonem.

(3) Právo osoby být informován o údajích o ní shromažďovaných, o jejich využití, jakož i právo na opravu takových údajů stanoví zákon.

Z našeho pohledu zajímavou ústavní úpravu použití technických prostředků při sledování obydlí představuje čl. 13 **německé ústavy** z 23.5.1949:

Čl. 13

(1) Obydlí je nedotknutelné.

(2) Prohlídky smí nařizovat jen soudce, při nebezpečí z prodlení i jiné orgány a jen ve formě tam předepsané je provádět.
(3) Jestliže určité skutečnosti odůvodňují podezření, že někdo spáchal zvláště závažný a zákonem samostatně vymezený trestný čin, lze na základě soudcovského příkazu použít ke sledování činu technické prostředky akustického dozoru nad obydlím, v němž se obviněný patrně zdržuje, pokud by bylo zjištění stavu věci jiným způsobem nepřiměřeně ztížené nebo beznadějné. Toto opatření podléhá časovému omezení. Příkaz vyslovuje sbor, složený ze tří soudců. Při nebezpečí z prodlení příkaz vyslovuje i jednotlivý soudce.
(4) K odvrácení nebezpečí ohrožujícího veřejnou bezpečnost, zvláště pak obecného ohrožení nebo ohrožení života, lze použít technické prostředky akustického dozoru nad obydlím pouze na základě soudcovského příkazu. Při nebezpečí z prodlení může toto opatření nařídit i jiný zákonem určený orgán; rozhodnutí soudce je však třeba neprodleně dodat.
(5) Slouží – li technické prostředky výlučně k ochraně osob, jejichž činnost v bytě je součástí jejich služebního nasazení, může toto opatření nařídit zákonem stanovený orgán. Jakékoliv využití těchto získaných poznatků je přípustné pouze za účelem trestního stíhání nebo k odvrácení nebezpečí, a to pouze, jestliže předtím byla soudcem zjištěna oprávněnost tohoto opatření; při nebezpečí z prodlení je třeba následně bez odkladu dodat soudcovské rozhodnutí.
(6) Spolková vláda podává Spolkovému sněmu každoročně zprávu o použití technických prostředků podle odstavce 3, jakož i o jejich použití v rámci spolkové kompetence podle odstavce 4a, pokud je nutný soudní přezkum podle odstavce 5. Na základě této zprávy provádí parlamentní kontrolu grémium, zvolené Spolkovým sněmem. Rovnocennou parlamentní kontrolu provádějí i země.
(7) Jinak smějí být prováděny zásahy a omezení jen k odvrácení obecného nebezpečí nebo nebezpečí pro život jednotlivých osob; na základě zákona i k předcházení nebezpečí hrozícího veřejné bezpečnosti a pořádku, zvláště k odstranění bytové nouze, k potírání nakažlivých nemocí nebo i k ochraně ohrožených mladistvých osob.

2.5 Institut ochrany soukromí v českém právu

2.5.1 Historický vývoj ochrany soukromí

Zakotvením práva na ochranu soukromí v ústavním zákoně č. 23/1991 Sb. ze dne 9. ledna 1991, kterým se uvozuje **LISTINA ZÁKLADNÍCH PRÁV A SVOBOD** jako ústavní zákon Federálního shromáždění České a Slovenské Federativní Republiky, bylo toto právo začleněno do právního řádu, resp. ústavního pořádku v České republice v takové míře de facto vůbec poprvé. Před přijetím Listiny základních práv a svobod neznal tehdejší československý právní řád ochranu soukromí v moderním slova smyslu. Na svou dobu demokratická meziválečná první republika institut ochrany soukromí v novodobém pojetí nezná. Ústava z roku 1920 (zákon č. 121/1920 Sb.) znala pouze ochranu základní osobní svobody (§ 107) a samozřejmě ochranu svobody domovní (§ 112) a ochranu listovního tajemství (§ 116). Za první republiky se však v zákoně č. 108/1933 Sb. o ochraně cti zřejmě poprvé v historii českého právního řádu

zmiňuje ochrana práv, které s ochranou soukromí v dnešním smyslu úzce souvisejí. Ustanovení § 7 odst. 2 přímo zmiňuje skutečnosti „*života rodinného nebo vůbec soukromého*“. Tento zákon poskytoval základní trestněprávní *ochranu cti* člověka i jiných subjektů, která by se dala považovat za složku obecnější ochrany osobnosti v moderním slova smyslu. Zákon byl roku 1950 zrušen a režim ochrany osobnosti byl přesunut do oblasti občanského práva - zákon č. 141/1950 Sb. občanský zákoník ve svém § 22 zaručoval ochranu jména.

Zřejmě z důvodu tehdejšího politického směrování zaměřeného na budování kolektivistické socialistické společnosti, která rozhodně ochraně soukromí jednotlivců nepřála, však nebyla v této době (zejména 50. léta 20. století) poskytována **prakticky žádná právní ochrana soukromí, cti a důstojnosti**.[30] Doba komunistické totality ostatně ochranu soukromí celou svou ideologií popírala. Navíc jsou známy případy extrémních excesů ze strany veřejné moci při zasahování do soukromé sféry člověka, které nebyly mnohdy nijak omezovány. Ústava z roku 1948 (ústavní zákon č. 150/1948 Sb.) ani ústava z roku 1960 (zákon č. 100/1960 Sb.) s výslovným pojmem ochrana soukromí nepracovaly. Po přijetí zákona č. 40/1964 Sb. - občanský zákoník – se v právním řádu tehdejší ČSSR objevuje komplexnější úprava ochrany osobnosti člověka.[31] V jejím rámci se pak začíná v právní teorii hovořit o **právu na soukromí**: „Na rozvoj osobnosti a na zabezpečení uplatnění občana ve společnosti je však potřebná ochrana i tzv. osobního soukromí, vnitřní, intimní sféry osobnosti. Tuto vnitřní, intimní sféru jako jednu ze složek osobnosti také chrání ustanovení **§ 11 a násl. OZ**.[32] Autoři publikace Občanské právo hmotné z poloviny 80. let minulého století pak o právu na osobní soukromí uvádí: „Toto právo sice občanský zákoník výslovně neuvádí, ale je možné ho odvodit z obecné klauzule § 11 OZ. Spočívá v právu jednotlivce rozhodnout podle vlastního uvážení či, příp. v jakém rozsahu, mají být skutečnosti jeho soukromého života zpřístupněné

---

30 Viz DRGONEC, J.: Právo na súkromie a pravomoc súdných orgánov pri jeho ochrane. Bulletin slovenskej advokacie, 1995, č. 1, s. 26

31 Viz ustanovení § 11 a násl. občanského zákoníku (zákon č. 40/1964 Sb.) v původním znění k 1.4.1964.

32 KRATOCHVÍL, Z.: Nové občanské právo. Praha: Orbis, 1965, s. 63.

jiným.“ [33] **Právo na soukromí totiž nebylo v zákoně č. 40/1964 Sb. nejprve vůbec zmíněno**. Mezi ostatní osobnostní práva jej zařadila spolu s právem na ochranu důstojnosti člověka s účinností od 1.1.1992 až polistopadová velká novela občanského zákoníku – zákon č. 509/1991 Sb.

Asi nejkomplexněji se tématu práva na soukromí (tehdy zvanému právo na osobní soukromí) věnoval Karel Knapp a Jiří Švestka v publikaci Ochrana osobnosti v československém občanském právu, která poprvé vyšla již v roce 1969: „*Právo na osobní soukromí **chrání nedotknutelnost soukromého života**. Jeho úkolem je zajistit **nerušený soukromý prostor,** v němž by se mohla rozvíjet osobnost člověka. Zajištění takové nerušené intimní sféry je nezbytné pro rozvoj každé osobnosti*.“ Autoři dále zmiňují, že: „*kolébkou práva na osobní soukromí se staly Spojené státy americké, kde se nutnost občanskoprávní ochrany osobního soukromí v důsledku stálé intenzifikace technické civilizace a jejích často ničivých zásahů do života jednotlivce jevila nezbytnou již od konce 19. století*.“ [34] Prvním státem, který právo na osobní soukromí uznal v plném rozsahu, se stalo Švýcarsko.[35]

Na počátku 90. let potom píše Viktor Knapp, že soukromím rozumí *„onu sféru života člověka, do které **nikdo nesmí bez jeho souhlasu zasahovat** a do které bez jeho souhlasu nesmí zasahovat ani stát (státní orgán), ledaže by k tomu byl dán výslovný zákonný důvod, a zároveň sféru, o které člověk může utajit informaci před kýmkoliv včetně před státem (státním orgánem).“*[36]

2.5.2 Ochrana soukromí v ústavním pořádku ČR

Z hlediska českého právního řádu je ochrana soukromí upravena především přímo v normách ústavního pořádku země, a to zejména v ***Listině základních práv a svobod***, vyhlášené usnesením předsednictva České národní rady č. 2/1993 Sb. ze dne 16. prosince 1992, o vyhlášení LISTINY

---

[33] FIALA – HRUŠKOVÁ – HURDÍK – KORECKÁ: Občanské právo hmotné. II. díl. Praha: Státní pedagogické nakladatelství, 1984.

[34] KNAPP, K. - ŠVESTKA, J.: Ochrana osobnosti podle československého občanského práva. 2. vydání. Praha: Panorama, nakladatelství a vydavatelství, 1989. Strana 256

[35] Viz článek 28 švýcarského občanského zákoníku (ZGB) **z roku 1907.**

[36] Viz KNAPP, V.: Člověk, občan a právo. Právník 1/1992. str. 7.

ZÁKLADNÍCH PRÁV A SVOBOD jako součásti ústavního pořádku České republiky, ve znění ústavního zákona č. 162/1998 Sb. (dále i jako „LZPS“).

Problematiku zmiňuje Listina základních práv a svobod ve své Hlavě druhé (Lidská práva a základní svobody), oddílu prvním (Základní lidská práva a svobody), konkrétně **čl. 7 odst. 1 a čl. 10.**

„ **Čl. 7**
(1) Nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem.

Čl. 10
(1) Každý má právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno.
(2) Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.
(3) Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.

Tyto dva články zmiňují a pracují výslovně **s pojmem soukromí.** Lze říci, že garantují ochranu soukromého života jednotlivce v jeho **širším, obecnějším** slova smyslu. Už bylo řečeno, že soukromí nelze posuzovat jako izolovanou stránku života člověka, naopak má **mnoho aspektů** a zahrnuje řadu **dílčích složek**. Právě z tohoto důvodu není soukromí a ochrana soukromí zmiňována pouze v těchto dvou článcích, nýbrž i další ustanovení Listiny se věnují tématu ochrany soukromí. Mezi články upravujícími ochranu dalších specifičtějších složek soukromí můžeme zmínit článek 12, který zaručuje ***nedotknutelnost obydlí*** a článek 13, garantující ochranu korespondence a dalších písemností (***ochrana listovního a jemu podobných tajemství***). Okrajově se ochraně dalších složek soukromí věnují taktéž další ustanovení prvního oddílu druhé hlavy LZPS. Jde o článek 6 (ochrana lidského života), článek 8 (ochrana osobní svobody), článek 9 (zákaz nucených prací a služeb), článek 14 (svoboda pohybu a pobytu) a článek 15 (svoboda myšlení, svědomí a náboženského vyznání). Jelikož se zákonodárce zcela v souladu s moderními globalistickými sjednocujícími tendencemi logicky inspiroval v řadě mezinárodních a evropských dokumentů, upravujících ochranu lidských práv, dochází k tomu, že se některé pojmy a garance jednotlivých práv **překrývají.** Jelikož

jde však o ochranu soukromí, které je jedním ze základních lidských práv, lze zde zcela bez okolků uplatnit princip „*superfluum non nocet*“.[37]

Z důvodu důležitosti ustanovení článků 7 a 10 Listiny základních práv a svobod pro další výklad se o těchto ustanoveních zmíním podrobněji.

Institut zaručení nedotknutelnosti osoby a jejího soukromí dle **čl. 7 LZPS** dále specifičtěji rozvíjí právo na život garantované v čl. 6 LZPS. Dává osobě **záruky nedotknutelnosti především v kontextu ochrany její fyzické složky**. Vymezení nedotknutelnosti osoby také úzce souvisí s institutem ochrany **osobní svobody** dané článkem 8 LZPS a navazujícím čl. 9 LZPS. Osobou je zde myšlena podobně jako i u jiných lidských práv toliko osoba fyzická.[38] Z časového hlediska je nedotknutelnost osoby a jejího soukromí garantována v zásadě od narození až po smrt. Plod v těle matky je pak chráněn spíše jako součást matčiny osoby, nikoliv jako samostatná osoba.[39] Ochrana tělesné integrity člověka však vždy nekončí jeho smrtí, právní řád ji garantuje v některých případech i po smrti (viz např. zákaz odnímání orgánů těl u zemřelých, kteří tak písemně zamezili za svého života, jakož i u zemřelých ve výkonu trestu odnětí svobody apod.). Nedotknutelnost osoby a jejího soukromí je zaručena **proti všem rušivým vlivům zvenčí**, a to jak ze strany veřejné moci, tak i ze strany soukromých subjektů. Jak však plyne přímo z textu daného ustanovení Listiny, nedotknutelnost osoby a jejího soukromí může být omezena. Smí se tak však stát pouze v případech stanovených zákonem (viz čl. 7 odst. 1 druhá věta). I z jiných ustanovení Listiny lze ale dovodit, že **omezení tohoto základního práva je přípustné toliko na základě zákona a za podmínek stanovených Listinou základních práv a svobod** (čl. 4 odst. 2 LZPS) a že při používání ustanovení o mezích základních práv a svobod musí být

---

[37] Srovnej MATES, P.: Ochrana soukromí ve správním právu. Praha: LINDE 2004

[38] Viz nález Ústavního soudu sp. zn. III ÚS 35/01 ze dne 3.5.2001, a dále nález sp. zn. IV ÚS 528/98, kdy Ústavní soud uvádí, *že právnická osoba není aktivně legitimována k podání ústavní stížnosti pro porušení čl. 7 a 12 Listiny základních práv a svobod a čl. 8 Úmluvy o ochraně lidských práv a základních svobod , neboť z povahy těmito články zaručených základních práv a svobod plyne, že v rámci domovních prohlídek v zásadě mohou být dotčena pouze základní práva a svobody osob fyzických, nikoliv právnických, byť se mohou dotýkat obchodních aktivit soukromých osob.*

[39] Někteří autoři nicméně považují nascitura za samostatný subjekt ochrany dle čl. 7 LZPS, kdy je sám plod chráněn a je garantována jeho nedotknutelnost. Oproti tomu ale lze poukázat na znění čl. 6 odst. 1 druhá věta LZPS, které stanoví, že život nascitura je hoden ochrany – LZPS mu tedy nezaručuje výslovně právo na život.

šetřeno jejich podstaty a smyslu, přičemž současně taková omezení nesmějí být zneužívána k jiným účelům, než pro které byla stanovena (čl. 4 odst. 4 LZPS). Při určování dovolené míry zásahu do nedotknutelnosti osoby a jejího soukromí je bezesporu nutno se přidržet taktéž znění článku 8 Evropské úmluvy o ochraně lidských práv a základních svobod, který ve svém druhém odstavci blíže zmiňuje přípustné zásahy do soukromého života člověka.[40] Jedním z možných zásahů do záruk daných čl. 7 LZPS je pak případ, kdy byl někdo zbaven života v souvislosti s jednáním, které podle zákona není trestné (viz čl. 6 odst. 4 LZPS). Dovoleným zásahem do osobní integrity jsou pak např. i případy odnímání částí lidského těla v souvislosti s léčebně preventivní péčí, lékařskou vědou, výzkumem a výukovými účely, odběr krve, tkání a orgánů, upravené v § 26 zákona č. 20/1966 Sb. o péči o zdraví lidu, jakož i další výkony a lékařské zákroky dle §§ 27 - 30 tohoto zákona. Z hlediska ochrany veřejného pořádku a umožnění plnění dalších úkolů ze strany bezpečnostních orgánů je pak povoleným zásahem do nedotknutelnosti osoby také např. použití donucovacích prostředků příslušníky Policie ČR, orgány obecní policie, celními orgány a jinými bezpečnostními složkami. Zásah do nedotknutelnosti soukromí osoby je pak možný při úkonech dle trestního řádu, samozřejmě za splnění všech zákonných podmínek (domovní a osobní prohlídka, prohlídka jiných prostor a pozemků, vstup do obydlí, jiných prostor a pozemků, zadržení a otevření zásilek, odposlech a záznam telekomunikačního provozu). Taktéž použití zpravodajské techniky ze strany zpravodajských služeb a použití operativně – pátracích prostředků, které jsou mnohdy taktéž velkým zásahem do nedotknutelnosti osoby a především jejího soukromí, je přípustné v mezích stanovených příslušnými zákony (zákon č. 154/1994 Sb. o Bezpečnostní informační službě, zákon č. 289/2005 Sb. o Vojenském zpravodajství, zákon č. 283/1991 Sb. o Policii České republiky). Tolerovaným zásahem do nedotknutelnosti osoby jsou dále kupříkladu bezpečnostní kontroly prováděné provozovatelem letiště, leteckým dopravcem nebo jimi pověřenými osobami (viz § 85c zákona č. 49/1997 Sb. o civilním letectví).

[40] Viz i názor autorů publikace PAVLÍČEK, V. a kolektiv: Ústavní právo a státověda. II. Díl Ústavní právo České republiky, Část 2. Praha: LINDE, 2004, obsažený v pojednání k danému ustanovení článku 7 LZPS

Článek 10 LZPS je pak úpravou blíže rozvádějící a specifikující **obecnější vymezení nedotknutelnosti osoby a jejího soukromí.** Garantuje ochranu tzv. osobnostních práv (práv na ochranu osobnosti). Čl. 10 LZPS je tedy vůči čl. 7 LZPS v poměru lex specialis.

Článek 10 ve svém odstavci 1 zaručuje každému **právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno**. Ústavně garantovaná ochrana je přitom dále a specielněji rozvedena zejména v občanském zákoníku, v části pojednávající o ochraně osobnosti.[41] Občanský zákoník tak dále zaručuje každé fyzické osobě právo na ochranu její osobnosti, zejména života a zdraví, občanské cti a lidské důstojnosti, jakož i soukromí, jejího jména a projevů osobní povahy. Právo na zachování lidské důstojnosti komplexněji rozvádí zásadu rovnosti všech lidí, zakotvenou v čl. 3 odst. 1 LZPS. Lidskou důstojnost mají všichni lidé stejnou, a to bez rozdílu věku, společenského postavení, hodností a titulů. Oproti tomu osobní čest je označením diferencujícím mezi jednotlivými lidmi zejména v důsledku jejich rozdílného společenského statusu, může tedy dojít k zásahu, který se bude dotýkat osobní cti, ale nedosáhne ještě míry zasažení lidské důstojnosti. Stejně tak dobrou pověstí je míněno dosavadní společenské postavení a pozice konkrétního člověka ve společnosti v závislosti na jeho dosavadním mravním a sociálním jednání. Aby bylo výše uvedené rozlišení zcela pochopitelné, lze uvést, že neexistuje člověk zcela bez osobní cti, naopak dobrou pověst si člověk musí vybudovat, její získání není automatické.[42] Samotný zásah do všech kategorií ochrany dle daného článku lze provést prakticky jakýmkoliv způsobem, tj. slovně, písemně, zvukovým či obrazovým záznamem a jinak. Ochrana jména pak spočívá v zaručení identifikačního jazykového výrazu, které odlišuje jednotlivé lidské bytosti. Používání jména a příjmení a další podmínky pak upravuje podrobněji i zákon č. 301/2000. Sb. o matrikách, jménu a příjmení.

---

[41] Srovnej ustanovení §§ 11 – 13 občanského zákoníku (zákona č. 40/1964 Sb. ve znění pozdějších předpisů).

[42] K podrobnějšímu výkladu a rozlišení jednotlivých kategorií ochrany viz např. publikaci PAVLÍČEK, V. a kolektiv: Ústavní právo a státověda. II. Díl Ústavní právo České republiky, Část 2. Praha: LINDE, 2004

Odstavec 2 článku 10 LZPS pak garantuje každému **právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života**. Dané ustanovení Listiny je pro naši potřebu zřejmě nejzajímavější, neboť jen v jeho mezích lze tolerovat veškeré ingerence ze strany veřejné moci, ale i soukromých subjektů. Tato problematika se tedy dotýká nejen kamerových systémů, ať již instalovaných orgány veřejné správy či soukromými subjekty, nýbrž prakticky veškeré činnosti všech možných subjektů, jež by mohla zasahovat do sféry soukromého či rodinného života. Definice toho, co lze považovat za soukromý a rodinný život je poměrně obtížná. Jen těžko lze totiž definovat něco, co nemá přesné ohraničení, navíc se v čase mění (v závislosti na prostředí, vývoji společnosti, techniky a na mnoha dalších faktorech). Jak již bylo zmíněno, většina odborníků i soudní praxe se shodují v tom, že nelze podat vyčerpávající taxativní definici pojmu soukromí či jeho složek.[43] Tento jev navíc nelze postihnout nikdy v celé jeho šíři. Jedna z definic například uvádí, že do soukromého života (soukromí) člověka náleží zásadně vše, pokud to není veřejné ze své podstaty, nebo se to neděje veřejně, anebo to člověk není povinen podle zákona zpřístupnit nebo vyjevit komukoliv jinému.[44]

Listina stanoví, že do soukromého a rodinného života nelze zasahovat neoprávněně. Tím se rozumí, že **zásahy do soukromého a rodinného života se mohou dít jen na základě zákona a při šetření všech dalších podmínek daných ústavními a zákonnými předpisy** (viz např. výše odkazy na čl. 4 odst. 2 a 4 LZPS). I sám zákonný podklad k zásahům do soukromí musí být v duchu **principu přiměřenosti** odůvodněn pozitivy, která takový nezbytný zásah přinese a vyváží tím své negativní důsledky invaze do soukromé sféry. Hodnoty, jimiž je odůvodňován zásah do soukromí, jsou v moderní společnosti zpravidla bezpečnost, morálka, ochrana zdraví apod.[45] Každý případ zásahu do soukromí je však nezbytně

---

[43] Viz např. rozhodnutí Evropského soudu pro lidská práva v případu Niemietz versus Německo.

[44] PAVLÍČEK, V. a kolektiv: Ústavní právo a státověda - II. Díl (cit. dříve).

[45] Např. článek 8 odst. 2 Úmluvy o ochraně lidských práv a základních svobod uvádí: *Státní orgán nemůže do výkonu tohoto práva* (práva na respektování soukromého a rodinného života, obydlí a korespondence) *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*

nutné posuzovat v jeho individuálních souvislostech. Zde je nutno výslovně zdůraznit, že byť i jakákoliv následná zákonná úprava třeba nezmiňuje princip přiměřenosti, tuto ústavní zásadu zasahovat jen v míře nezbytně nutné a jen je-li to odůvodnitelné zájmy hodnými ochrany v demokratické společnosti, je nezbytné aplikovat při jakémkoliv zásahu do soukromé sféry jednotlivce.

Každý subjekt se může dobrovolně svého soukromí zříci,[46] a to buď fyzicky, že např. umožní přístup do svého obydlí, nebo tak, že své soukromí vyjeví třeba v médiích. V posledních letech přinesl společenský vývoj extrémní využití tohoto institutu dobrovolného svolení k zásahům do soukromí například v tzv. reality show, kdy jsou jednotlivci i celé skupiny lidí podrobováni detailnímu monitorování jejich aktivit či přímo celého jejich života v průběhu určité periody (viz reality show Big Brother, Vyvolení atd.). Do budoucna bude pro právníky jistě zajímavé sledovat vývoj všech témat a přístupů, jež tyto populární show přinášejí. Je přitom jen otázkou času, kdy se reality show přenášené v reálném čase přímo dotkne i některých zatím stále pro široká masmédia nedotknutelných společenských jevů (online přenosy lidských úmrtí, sebevražd, sledování reakcí lidí ve vyhrocených extrémních pro život nebezpečných situacích atd.). Je samozřejmě otázkou jak z hlediska práva na soukromí pohlížet na podobné televizní aktivity zobrazující často detailní osobní projevy natáčených lidí. Podle občanského zákoníku lze bezpochyby dát platně souhlas k pořízení či použití obrazových a zvukových záznamů týkajících se fyzické osoby nebo jejích projevů osobní povahy.[47] Provozovatel realitní show se tedy zřejmě nedopouští neoprávněného pořizování a používání obrazových a zvukových záznamů konkrétních herců, kteří jsou navíc za tuto svou činnost odměňováni. Důležitou a zatím možná spíše teoretickou otázkou zůstává ale problematika souladu těchto reality show s ústavními garancemi práva člověka na soukromí. Toto právo lidské bytosti je nezadatelné, nezcizitelné a fyzická osoba se jej ani za úplatu, ani zcela

---

nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných.

46 Zásada *volenti non fit iniuri*.

47 Srovnej ustanovení § 11 odst. 1 a § 13 zákona č. 40/1964 Sb. (občanský zákoník) v platném znění.

dobrovolně a vědomě, nemůže vzdát. Pokud míra zásahu do soukromí nepřekročí celospolečensky akceptovatelnou a tabuizovanou hranici, budou zřejmě televizní přenosy ve stylu Big Brothera či VyVolených i z hlediska ústavních norem v pořádku. V případě, že zobrazení soukromé sféry sledovaných jedinců tuto hranici překročí, bude třeba se ptát, zda se přitom současně neporušuje ústavní právo na ochranu soukromí fyzické osoby, kterého nemůže být žádný člověk v takovéto extrémní formě nikterak, a to ani se svým souhlasem, zbaven.

Za součást soukromého života lze bezpochyby považovat i **rodinný život**; autoři Listiny chtěli zřejmě uvedením výslovného odlišení soukromého a rodinného života zdůraznit význam rodiny a manželství v duchu jejich tradiční historické ústavní ochrany. Taktéž se zřejmě přidrželi užívání těchto pojmů v mezinárodních dokumentech, zejména v Úmluvě o ochraně lidských práv a svobod (viz text jejího článku 8, který garantuje každému právo na respektování jeho soukromého a *rodinného* života, obydlí a korespondence). Lze ale říci, že pojmy soukromý a rodinný život jsou velmi propojené a budou prakticky vždy posuzovány společně. V rozsudku Evropského soudu pro lidská práva ve věci Marckx versus Belgie se uvádí, že ***pojem rodinný život*** *zahrnuje též vztahy mezi blízkými příbuznými, včetně vztahů mezi vnuky a prarodiči, takže respektování takto pojatého rodinného života zahrnuje závazek státu jednat způsobem umožňujícím normální rozvoj těchto vztahů. I dědické vztahy mezi blízkými příbuznými úzce souvisejí s rodinným životem. Rodinný život zahrnuje nejen sociální, morální či kulturní vztahy např. v oblasti výchovy dětí, ale i zájmy materiální povahy.*

Pojmu soukromí a všem souvisejícím skutečnostem se již mnohokrát věnoval ve své judikatuře Evropský soud pro lidská práva, jak již ostatně bylo v této práci zmíněno dříve.[48]

Konečně čl. 10 ve svém odstavci 3 zakotvuje **ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě**. Jedná se o specielní úpravu ve vztahu k předchozímu odstavci článku 10 LZPS.

[48] K tomu srovnej rozsudky ve věci Niemietz versus Německo, Klass a ostatní versus Německo, Halfordová proti Spojenému Království, Amann proti Švýcarsku, a jiné.

Ačkoliv Listina opět používá poněkud jiné terminologie než jiné právní předpisy či mezinárodní dokumenty, které užívají dnes již zavedený termín **ochrana osobních údajů**, lze *„…údaje o své osobě“* zmiňované v třetím odstavci čl. 10 LZPS považovat za osobní údaje. Podle legální definice obsažené v ustanovení § 4 zákona o ochraně osobních údajů je totiž osobním údajem jakákoliv informace týkající se určeného nebo určitelného subjektu údajů, přičemž za subjekt údajů se považuje fyzická osoba, k níž se osobní údaje vztahují.[49]

Toto ustanovení a vůbec celá problematika údajů o fyzických osobách a jejich ochrana před zneužitím nabývá zejména v poslední době masivního rozvoje informačních technologií nebývalého významu. Lze současně říci, že ochrana osobních údajů (zvaných zejména dříve i soukromé – *private* - údaje) se čím dál více krystalizuje do podoby **samostatného lidského práva, které však stále tvoří součást soukromí**, resp. soukromého života. Zcela prvním impulsem pro počáteční snahy o pochopení problému a pro snahy o jeho právní zakotvení byly nepochybně neblahé zkušenosti s totalitními režimy některých evropských států během 30. let minulého století a zejména během II. světové války. Tyto režimy využívaly identifikační údaje o jednotlivých osobách a celých skupinách osob k jejich persekuci, která vedla až k samotné genocidě (pronásledování Židů, Romů a jiných národnostních etnik). Klíčovým pro rozvoj institutu ochrany osobních údajů však byl zejména globalizující se svět a nástup moderních technologií, které umožňují rychle shromažďovat velké množství dat, prakticky neomezeně je archivovat, předávat je mezi řadou subjektů a dále s nimi pracovat (tj. řadit je do databází a systémů, spojovat a kombinovat je s jinými daty a vytvářet z nich i zcela jiné soubory údajů). Již v roce 1968 byl na půdě Rady Evropy proveden průzkum úrovně ochrany soukromí v souvislosti s moderními technologiemi v legislativě členských států a podle komise expertů pro lidská práva bylo v této souvislosti zjištěno, že dostatečná úroveň ochrany poskytována není. I toto zjištění pak vedle dalších faktorů vedlo k přijetí několika doporučení, jejichž cílem bylo

[49] Pro zajímavost - legální definice v § 3 dřívějšího zákona o ochraně osobních údajů v informačních systémech č. 256/1992 Sb. stanovovala, že osobními údaji jsou informace, které se vztahují k určité osobě.

tuto ochranu zajistit či zlepšit. Daný vývoj pak ústil v přijetí moderní **Úmluvy Rady Evropy č. 108 z roku 1981 o ochraně jednotlivců se zřetelem na automatické zpracování osobních údajů**; a taktéž v přijetí několika na tuto Úmluvu navazujících doporučení Výboru ministrů Rady Evropy, které upravovaly problematiku zpracování osobních údajů v jednotlivých oblastech – platební styk, vědecký výzkum, pojišťovnictví atd.[50] Sama Úmluva o ochraně jednotlivců se zřetelem na automatické zpracování osobních údajů byla pak zdrojem inspirace pro tvůrce českého **zákona o ochraně osobních údajů v informačních systémech** č. 256/1992 Sb. Tento zákon se však především pro absenci efektivních sankcí a neexistenci jakéhokoliv nezávislého kontrolního orgánu v praxi neujal a zůstal tak de facto obsoletní právní normou. Nutnost situaci řešit v souladu s moderními úpravami západních evropských států vyvolal blížící se vstup České republiky do Evropské Unie a povinnost harmonizace českého právního řádu s právem evropských společenství. V návaznosti na důležitou a významnou **Směrnici Evropského parlamentu a Rady č. 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a s volným pohybem těchto údajů** byl pak přijat moderní **zákon č. 101/2000 Sb. o ochraně osobních údajů**.[51]

Nepřípustné je jakékoliv shromažďování, zveřejňování, zneužívání, ale i samotné získávání údajů bez souhlasu dotčené osoby nebo bez zákonného podkladu, a to jak ze strany orgánů veřejné moci, tak i ze strany jakýchkoliv jiných subjektů.

Ustanovení ústavní síly článku 10 odst. 3 LZPS je blíže provedeno a specifikováno samostatným zákonem. Je jím shora již zmíněný **zákon č. 101/2000 Sb. o ochraně osobních údajů**. Zákon upravuje zpracovávání osobních údajů ze strany státních orgánů, orgánů územní samosprávy, jiných orgánů veřejné moci, ale i fyzických a právnických osob. Jsou jím dány právní rámce pro shromažďování, užití a uchovávání osobních údajů. Dozor v dané sféře pak provádí Úřad pro ochranu osobních údajů se sídlem v Praze. Zákon se nevztahuje na zpracování osobních údajů, které provádí

---

[50] Viz SMEJKAL, V. a kol.: Právo informačních a telekomunikačních systémů. 1. vydání. Praha, C. H. Beck 2001, 542 str., ISBN 80-7179-552-6, strana 110-111.

[51] K celé problematice vývoje institutu ochrany osobních údajů viz např. MATES, P.: Ochrana soukromí ve správním právu. Praha: LINDE 2004.

fyzická osoba výlučně pro osobní potřebu. Taktéž se nevztahuje na nahodilé shromažďování osobních údajů, pokud tyto údaje nejsou dále zpracovávány. Některá ustanovení zákona o ochraně osobních údajů se pak nepoužijí při zpracovávání osobních údajů zpravodajskými službami, Policií ČR při odhalování trestné činnosti, Ministerstvem financí v rámci jeho finančně – analytické činnosti, Národním bezpečnostním úřadem při provádění bezpečnostních prověrek, Ministerstvem vnitra při provádění některých jeho činností (vydávání krycích dokladů, činnost inspekce ministra vnitra atd.). Zákon o ochraně osobních údajů se také nevztahuje na zpracování osobních údajů pro statistické a archivářské účely.[52]

Zákon rozlišuje mezi osobním údajem, citlivým údajem a anonymním údajem.

Údaje o osobách uchovává a využívá Bezpečnostní informační služba (§ 16 zákona č. 154/1994 o Bezpečností informační službě), Vojenské zpravodajství (§ 17 a násl. zákona č. 289/2005 Sb. o Vojenském zpravodajství) i Úřad pro zahraniční styky a informace (§ 19 zákona č. 153/1994 Sb. o zpravodajských službách České republiky). Podrobná úprava zpracování osobních údajů Policií ČR je pak v §§ 60-88 zákona č. 273/2008 Sb. o Policii ČR.[53]

Jelikož z titulu své funkce mají následující subjekty přístup k údajům o osobách, je vedle příslušníků zpravodajských služeb a policie zákonem uložena **povinnost mlčenlivosti** zejména soudcům, státním zástupcům, příslušníkům Vězeňské stráže, notářům, advokátům, daňovým poradcům, auditorům, pracovníkům ve zdravotnictví, zaměstnancům orgánů státní správy atd.

Neoprávněné nakládání s osobními údaji (a to i nedbalostní) naplňuje pak skutkovou podstatu trestného činu podle § 180 trestního zákoníku.

Jak bylo řečeno výše, soukromí a jeho specifické složky jsou chráněny také v dalších ustanoveních Listiny základních práv a svobod,

---

[52] K tomu srovnej GERLOCH, A. – HŘEBEJK, J. – ZOUBEK, V.: Ústavní systém České republiky. Praha: PROSPEKTRUM, 2002.

[53] K tématu problematiky zpracování osobních údajů a obrazového sledování ze strany Policie ČR a ze strany zpravodajských služeb viz dále kapitolu 3 této práce.

konkrétně v čl. 12 (nedotknutelnost obydlí) a čl. 13 (ochrana tajemství dopravovaných zpráv).

Čl. 12

(1) Obydlí je nedotknutelné. Není dovoleno do něj vstoupit bez souhlasu toho, kdo v něm bydlí.

(2) Domovní prohlídka je přípustná jen pro účely trestního řízení, a to na písemný odůvodněný příkaz soudce. Způsob provedení domovní prohlídky stanoví zákon.

(3) Jiné zásahy do nedotknutelnosti obydlí mohou být zákonem dovoleny, jen je-li to v demokratické společnosti nezbytné pro ochranu života nebo zdraví osob, pro ochranu práv a svobod druhých anebo pro odvrácení závažného ohrožení veřejné bezpečnosti a pořádku. Pokud je obydlí užíváno také pro podnikání nebo provozování jiné hospodářské činnosti, mohou být takové zásahy zákonem dovoleny též, je-li to nezbytné pro plnění úkolů veřejné správy.

Čl. 13

Nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením.

Článek 12 LZPS zaručuje **nedotknutelnost obydlí a garantuje právo na ochranu obydlí vůbec**. První úprava obdobného institutu ochrany tzv. domovního práva a jeho neporušitelnosti se objevuje již v době habsburské monarchie v zákoně č. 88/1862, který se následně stává součástí zákona č. 142/1867. Ústavní listina Československé republiky z roku 1920 ve svém § 112 nazvaném svoboda domovní pak deklaruje neporušitelnost domovního práva, přičemž podrobnosti (a to zejména základní podmínky přípustnosti domovní prohlídky) upravoval ústavní zákon č. 293/1920 Sb. I další ústavy (ústava z roku 1948 a z roku 1960) znaly institut domovní svobody, resp. nedotknutelnosti obydlí, nicméně vzhledem k charakteru totalitního komunistického režimu nelze mluvit o účinném a v praxi vymahatelném ústavním zakotvení tohoto základního lidského práva.

Článek 12 LZPS rozvíjí a precizuje nedotknutelnost osoby a jejího soukromí dle článku 7 Listiny. Nejedná se však o právo na domov, či právo na určité obydlí ve smyslu, že by stát musel zajišťovat lidem domov. Právo na bydlení (vyplývající z práva na přiměřený životní standard) se sice v mezinárodních dokumentech objevuje, nicméně jeho účinné prosazení do vymahatelných právních předpisů zatím chybí. Ochrana obydlí je spatřována spíše **v garanci státní moci na fyzickou jistotu existujícího obydlí jednotlivců**. Co se týká definice obydlí, v textu ústavních či zákonných předpisů (stejně tak ani v mezinárodních dokumentech) se precizní definice

pojmu obydlí nenachází. Toliko v ustanovení prvního odstavce § 82 trestního řádu je stanoveno, že *domovní prohlídku lze vykonat, je-li důvodné podezření, že* ***v bytě nebo v jiné prostoře sloužící k bydlení nebo v prostorách k nim náležejících (obydlí)*** *je věc nebo osoba důležitá pro trestní řízení.* Obydlím je pak dle judikatury a odborné literatury dům, byt, rekreační chata, chalupa, prostory k nim přináležející, tedy stavby sloužící k trvalému bydlení, dočasnému ubytování nebo individuální rekreaci. Judikatura vykládá pojem obydlí poměrně extenzivně. Např. Evropský soud pro lidská práva uznal ve věci Buckleyová proti Spojenému království, že obytné přívěsy paní Buckleyové postavené na pozemku v jejím vlastnictví (který zakoupila s cílem usadit se na něm), bez toho, že by měla jiné bydliště nebo záměr do budoucna jiné bydliště mít, lze považovat za obydlí a spadají pod ochranu garantovanou článkem 8 Úmluvy o ochraně lidských práv a základních svobod.

Pod pojem obydlí jsou často zahrnovány **i prostory sloužící k podnikání**, neboť nelze mnohdy vést jasnou hranici mezi čistě soukromým a profesním životem.[54]

Do obydlí není dovoleno vstoupit bez souhlasu toho, kdo v něm bydlí. Souhlas může být udělen trvale, pro určité časové období, nebo jen jednorázově. Chráněn je pak oprávněný uživatel obydlí, ať už jeho vlastník, nájemce, oprávněný držitel či jiný subjekt mající právo k užívání daného obydlí. Ochrana obydlí se nevztahuje na osobu, která obydlí užívá neoprávněně. Jednání osoby, která by neoprávněně vnikla do domu nebo do bytu jiného nebo tam neoprávněně setrvala, pak naplňuje skutkovou podstatu trestného činu **porušování domovní svobody** dle § 178 trestního zákoníku.

Do nedotknutelnosti obydlí lze **dovoleně zasáhnout** v případech vymezených v dalších dvou odstavcích článku 12 LZPS. Prvním tolerovaným zásahem do práva chráněného článkem 12 je institut domovní prohlídky, a to jen pro účely trestního řízení a jen na základě písemného odůvodněného příkazu soudce. Způsob provedení domovní prohlídky a další

[54] Rozsudek z 16. 12. 1992 ve věci Niemietz proti Německu. Evropský soud pro lidská práva zde např. uvedl, že konečně i francouzské znění Úmluvy používající slovo „domicile“, které je širší než slovo anglické „*home*“, svědčí závěru, že pojem obydlí může zahrnovat například kancelář osoby, která má svobodné povolání.

bližší úpravu pak stanoví trestní řád. Trestní řád rozlišuje mezi domovní prohlídkou a prohlídkou jiných prostor (tedy prostor nesloužících k bydlení jako jsou sklady, samostatné garáže apod.) a pozemků.

Vedle domovní prohlídky jsou pak druhým dovoleným zásahem do nedotknutelnosti obydlí případy vymezené v odstavci 3 článku 12 LZPS. Těmi jsou pak zásahy dovolené zákonem za splnění podmínky, že jde o zásah v demokratické společnosti nezbytný pro ochranu života nebo zdraví osob, pro ochranu práv a svobod druhých anebo pro odvrácení závažného ohrožení veřejné bezpečnosti a pořádku. Jestliže je obydlí užíváno také pro podnikání nebo provozování jiné hospodářské činnosti, mohou pak být takové zásahy zákonem dovoleny též, je-li to nezbytné pro plnění úkolů veřejné správy. Konkrétním dovoleným zásahem je pak dle ustanovení § 83c trestního řádu umožnění vstupu do obydlí, jiných prostor nebo na pozemek policejnímu orgánu, ovšem jen tehdy, jestliže věc nesnese odkladu a vstup tam je nezbytný pro ochranu života nebo zdraví osob nebo pro ochranu jiných práv a svobod nebo pro odvrácení závažného ohrožení veřejné bezpečnosti a pořádku. Přípustným zásahem je pak i oprávnění policisty dle § 21 zákona o Policii České republiky otevřít byt nebo jiný uzavřený prostor, je-li důvodná obava, že je ohrožen život nebo zdraví osoby anebo hrozí-li větší škoda na majetku (případně, vznikne-li důvodné podezření, že se v bytě nachází mrtvola). Policista může do bytu nebo jiného uzavřeného prostoru následně i vstoupit a provést v souladu se zákonem potřebné služební zákroky, služební úkony nebo jiná opatření k odvrácení bezprostředního nebezpečí. Další zásahy do nedotknutelnosti obydlí umožňuje pak zákon o obecní policii, zákon o péči o zdraví lidu, zákon o Hasičském záchranném sboru České republiky, zákon o státní kontrole, zákon o Nejvyšším kontrolním úřadě, jakož i jiné zákony. U prostor sloužících i k podnikání je pak například umožněn vstup správci daně na základě zákona o správě daní a poplatků nebo inspektorům a pověřeným zaměstnancům dle zákona o ochraně osobních údajů.

Článek 13 Listiny upravuje pak **nedotknutelnost tajemství listovního, jakož i tajemství jiných písemností a záznamů**. Stejně tak jsou chráněny **dopravované zprávy**. Problematika poštovní přepravy je specielně řešena zákonem č. 29/2000 Sb. o poštovních službách. Již při

koncipování Listiny bylo záměrně použito termínu zpráv podávaných *jiným podobným zařízením*. S ohledem na současný překotný technický vývoj nelze totiž s dostatečným předstihem úplně definovat všechny možné způsoby přenosu zpráv. Vedle tradičních technických zařízení jako je telefon a telegraf jsou již dlouho používány i faxy, jakož i elektronická komunikace, zejména přes síť Internet, s mnoha různými způsoby přenosu dat. S novými způsoby komunikace však přichází ruku v ruce i obtížnější možnost kontroly nad dodržováním nedotknutelnosti listovního a obdobného tajemství.

Lze deklarovat, že nikdo (krom adresáta, resp. účastníků komunikace) se nesmí seznamovat s písemnostmi zasílanými poštou či jinými způsoby přepravy a stejně tak ale ani s písemnostmi uschovanými v soukromí. Ochrana je poskytována i všem záznamům, samozřejmě včetně záznamů na elektronických nosičích. Vedle informací zachycených v listinné podobě či zaznamenané na nosiči dat, jsou pak předmětem ústavní ochrany veškeré zprávy, tedy informace přenášené jakoukoliv formou komunikace na dálku (včetně různých signálních forem komunikace – Morseova abeceda, vlajková komunikace atd.). Je lhostejno, zda je písemnost či záznam zasílán poštou jakožto státním podnikem, nebo různými soukromými subjekty, podnikajícími na trhu poskytování poštovních a přepravních služeb.

Zásah do listovního a obdobného tajemství ve smyslu ochrany dle článku 13 LZPS je možný jen v případech a způsobem, který stanoví zákon (jako u ostatních zásahů do základních práv a svobod se i zde uplatní čl. 4 odst. 2 a 4 LZPS). Český právní řád tak umožňuje zásah do listovního a obdobného tajemství příslušnou úpravou obsaženou v trestním řádu v souvislosti s instituty zajištění osob a věcí, zadržení a otevření zásilek a s institutem odposlechu a záznamu telekomunikačního provozu.

Listovnímu a jemu obdobnému tajemství poskytuje ochranu trestní právo hmotné, které vymezuje skutkové podstaty **Porušení tajemství dopravovaných zpráv (**§ 182) a **Porušení tajemství listin a jiných**

dokumentů uchovávaných v soukromí (§ 183) trestního zákoníku (zákona č. 40/2009 Sb.).[55]

Vedle listovního tajemství se můžeme setkat i s pojmy ***poštovní tajemství*** a ***telekomunikační tajemství.***

Poštovní tajemství je širší pojem než listovní tajemství, týká se širšího okruhu chráněných údajů (listovní tajemství chrání jen samu písemnost, poštovní tajemství i další údaje, vzniklé v souvislosti s přepravou zásilky). V právním řádu je zakotveno v zákoně o poštovních službách (zákon č. 29/2000 Sb.). Podle tohoto zákona je povinen provozovatel, osoba podílející se na poskytování poštovních služeb a osoba vykonávající činnost podle § 37 – touto osobou je Český telekomunikační úřad, který vykonává dohlížecí činnost (v zákoně jsou tyto subjekty souhrnně označovány jako "*nositel poštovního tajemství*") - zachovávat mlčenlivost o skutečnostech týkajících se poskytované nebo poskytnuté poštovní služby, které se při své činnosti dozvěděli. Znalosti těchto skutečností smějí využívat pouze pro potřeby poskytování poštovní služby nebo činnosti podle § 37. Povinné subjekty nesmějí ani umožnit, aby se s chráněnými skutečnostmi neoprávněně seznámila jiná osoba.[56] Zákon výslovně neposkytuje ochranu

---

[55] Trestného činu Porušování tajemství dopravovaných zpráv podle § 182 tr. zákoníku se tak dopustí ten, kdo úmyslně poruší tajemství

a) uzavřeného listu nebo jiné písemnosti při poskytování poštovní služby nebo přepravované jinou dopravní službou nebo dopravním zařízením,
b) datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli, který zprávu přijímá, nebo
c) neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková počítačová data.

Přísněji bude potrestán pracovník provozovatele poštovních služeb nebo telekomunikační služby, pokud se dopustí stejného jednání nebo jinému úmyslně umožní spáchat takový čin, nebo pokud pozmění nebo potlačí písemnost obsaženou v poštovní zásilce nebo dopravovanou dopravním zařízením anebo zprávu podanou neveřejným přenosem počítačových dat, telefonicky, telegraficky nebo jiným podobným způsobem.
Trestného činu Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí se dle § 183 dopustí ten, kdo neoprávněně poruší tajemství listiny nebo jiné písemnosti, fotografie, filmu nebo jiného záznamu, počítačových dat anebo jiného dokumentu uchovávaného v soukromí jiného tím, že je zveřejní, zpřístupní třetí osobě nebo je jiným způsobem použije.

[56] Podle ustanovení § 16 odst. 3 zákona o poštovních službách může být informace o poskytované nebo poskytnuté poštovní službě sdělena i odesílateli, adresátovi, právnímu nástupci odesílatele nebo adresáta, zástupci odesílatele nebo adresáta, popřípadě jiným osobám, které s vědomím odesílatele nebo adresáta jednají v jejich

informacím, ze kterých nevyplývá, kdo byl odesílatelem ani kdo byl adresátem. Zásah do poštovního tajemství je pak možný jen v zákoně jasně vymezených případech. Půjde o možnost ***otevření zásilky*** podle ustanovení § 8 citovaného zákona.[57] Zákon také umožňuje ***prodej zásilky*** (pokud ji nelze dodat a současně ji nelze vrátit nebo nemá být podle poštovní smlouvy vrácena, nebo je-li důvodná obava, že se obsah poštovní zásilky do dodání znehodnotí) a ***zničení zásilky*** (jestliže se například obsah poštovní zásilky zcela nebo zčásti znehodnotil, nebo pokud je to nezbytné pro zajištění ochrany zdraví lidí atd.). Ochrana poštovního tajemství je dále významným způsobem prolomena v situaci, kdy má provozovatel poštovních služeb podle zákona o poštovních službách či podle zvláštního právního předpisu povinnost sdělit informace o poskytované nebo poskytnuté poštovní službě osobám a orgánům oprávněným podle zvláštního právního předpisu, nebo jim umožnit, aby tyto informace získaly. Provozovatel poštovních služeb je taktéž v zákonem určených případech povinen vydat těmto osobám a orgánům oprávněným podle zvláštního právního předpisu poštovní zásilku nebo poukázanou peněžní částku, nebo učinit či umožnit jiná opatření.[58]

Konečně ustanovení § 16 odst. 7 zákona o poštovních službách ukládá provozovateli poštovních služeb povinnost vydat na nezbytně nutnou dobu orgánům oprávněným k použití zpravodajské techniky podle zvláštního právního předpisu[59] poštovní zásilku, nebo jim umožnit jiná

---

prospěch. Odstavec 4 pak dále upřesňuje, že zprostit povinný subjekt výše uvedené povinnosti mlčenlivosti může jen odesílatel, adresát, právní nástupce odesílatele nebo adresáta a zástupce odesílatele nebo adresáta.

[57] Otevření zásilky je tak například možné, pokud zásilku nelze dodat a současně ji nelze vrátit nebo nemá být podle poštovní smlouvy vrácena. Dále pokud je důvodné podezření, že zásilka obsahuje věc považovanou podle poštovních podmínek za nebezpečnou, nebo věc, jejíž poštovní podání není podle poštovních podmínek dovoleno. Jako další možné důvody pro otevření zásilky lze pak uvést situaci, kdy zásilka byla poškozena, či existuje důvodná obava, že došlo nebo že by do dodání mohlo dojít ke vzniku škody) atd.

[58] Osoby a orgány podle zvláštních právních předpisů jsou zejména orgány činné v trestním řízení a jejich oprávnění zakotvená v ustanovení § 86 a násl. trestního řádu. Vyhledávání, otevírání, zkoumání nebo vyhodnocování dopravovaných zásilek je pak umožněno Bezpečnostní informační službě na základě zmocnění v ustanovení § 11 a násl. zákona o Bezpečnostní informační službě (stejné oprávnění má i Vojenské zpravodajství dle § 7 a násl. zákona č. 289/2005 Sb. o Vojenském zpravodajství). Celním orgánům je umožněno provádět vnitřní kontrolu poštovních zásilek podle § 48 celního zákona.

[59] Zde se bude jednat o oprávnění Bezpečnostní informační služby dle § 11 a násl. zákona o Bezpečnostní informační službě a o oprávnění Vojenského zpravodajství dle § 7 a násl. zákona o Vojenském zpravodajství.

opatření dotýkající se poštovní zásilky, a to na žádost vedoucího tohoto orgánu nebo jím pověřené osoby a za podmínek stanovených zvláštním právním předpisem. O tomto postupu je pak provozovatel poštovních služeb povinen zachovávat mlčenlivost.

Poštovní tajemství se dle zákona č. 29/2000 Sb. o poštovních službách vztahuje pouze na přepravu poštovních zásilek formou klasického dopisu či jiným obdobným způsobem. Ochrana ve smyslu tohoto zákona není však poskytována elektronickým způsobům komunikace (např. elektronická pošta). Zde již půjde o ochranu **telekomunikačního tajemství** ve smyslu zákona č. 127/2005 o elektronických komunikacích.[60]

Zákon o elektronických komunikacích ve svém § 88 ukládá podnikatelům poskytujícím veřejně dostupnou službu elektronických komunikací povinnost ochrany osobních, provozních a lokalizačních údajů a důvěrnosti komunikací. Vedle garantované důvěrnosti samotné přepravované zprávy je tedy zaručena i ochrana provozních a lokalizačních údajů, které souvisejí se zprávou. Těmito souvisejícími údaji se myslí data nezbytná pro potřeby přenosu zprávy v rámci sítě elektronických komunikací nebo nezbytná pro účtování služby. Lokalizační údaje jsou data zpracovávaná v síti elektronických komunikací, která určují zeměpisnou polohu koncového zařízení uživatele veřejně dostupné služby elektronických komunikací. Pokud provozní údaje, včetně příslušných lokalizačních údajů, již nejsou potřebné pro přenos zprávy, je podnikatel zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací povinen tato data smazat nebo je učinit anonymními. Z této povinnosti byly ještě před vydáním výše zmíněného nálezu Ústavního soudu ze dne 22.3.2011 zákonem vymezeny tři výjimky:

- *odposlech a záznam zpráv ve smyslu § 97 zákona o elektronických komunikacích*

[60] Před účinností zákona č. 127/2005 Sb. upravoval problematiku zákon č. 151/2000 Sb. o telekomunikacích, který přímo používal pojem telekomunikační tajemství. Zákon č. 127/2005 Sb. již pojem telekomunikační tajemství neužívá, upravuje nicméně obdobnou problematiku v části zákona, kde zaručuje ochranu osobních, provozních a lokalizačních údajů a důvěrnost komunikací (část první, hlava pátá, díl první zákona).

- *zpracování provozních údajů, které je nezbytné pro vyúčtování ceny za službu poskytnutou účastníkovi nebo uživateli za přístup. Toto zpracovávání je však možné pouze do konce doby, během níž může být vyúčtování ceny právně napadeno nebo úhrada vymáhána.*[61]
- *zpracování provozních údajů pro účely marketingu služeb elektronických komunikací nebo pro účely poskytování služeb s přidanou hodnotou, a to v rozsahu a v trvání nezbytném pro tyto služby nebo marketing. Toto je nicméně možné jen pokud k tomu dal účastník nebo uživatel, ke kterému se údaje vztahují, svůj souhlas.*

Lokalizační údaje jiné než potřebné k provozu smí podnikatel zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací zpracovávat jen pokud tyto údaje učiní anonymními nebo pokud získá souhlas uživatele nebo účastníka se zpracováním v rozsahu a trvání nezbytném pro poskytování služeb s přidanou hodnotou. V zákoně o elektronických komunikacích existuje tedy pro potřeby této práce velmi významné ustanovení § 97, které upravuje odposlech a záznam zpráv. Toto ustanovení, konkrétně jeho odstavce 3 a 4 byly nicméně zrušeny nálezem Ústavního soudu ze dne 22.3.2011. V současné době se připravuje nová právní úprava, která musí transponovat evropskou úpravu danou směrnicí data retention (Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006). Až do přijetí nové právní úpravy tak provozovatelé veřejné komunikační sítě nebo poskytující veřejně dostupnou službu elektronických komunikací nemusí uchovávat provozní a lokalizační údaje a zejména je nemusí poskytovat orgánům oprávněných k jejich vyžádání podle zvláštního právního předpisu. V zákoně tak zůstal zachován toliko odposlech a záznam zpráv se souhlasem soudu a dále oprávnění vyžadovat informace z databáze všech účastníků veřejně dostupné telefonní služby.

[61] Zákon umožňuje předávání dat souvisejících s poskytováním služby (což jsou zejména údaje o účastnících spojení, pro zajištění propojení a přístupu k síti) mezi jednotlivými podnikateli zajišťujícími veřejnou komunikační síť nebo poskytujícími veřejně dostupnou službu elektronických komunikací, a to za účelem vzájemného vyúčtování a k identifikaci zneužívání sítě a služeb elektronických komunikací.

Spolu s ochranou důvěrnosti komunikace souvisí i možnost zamezení zobrazení účastnického čísla, kterou dává ustanovení § 92 citovaného zákona. Zákon dále zakazuje zneužití cizí adresy elektronické pošty a vymezuje základní podmínky pro vytváření a používání seznamů účastníků služeb elektronických komunikací.

Pro **osoby umístěné ve vazbě, ve výkonu trestu odnětí svobody či v psychiatrických léčebnách** platí z důvodu omezení osobní svobody a naplnění účelu daného zařízení **zvláštní režim** pro jejich korespondenci a jinou komunikaci s okolím.

Obvinění vzetí do vazby mohou přijímat a na svůj náklad odesílat písemná sdělení. Tato korespondence však podléhá kontrole, která zahrnuje i seznámení se s obsahem písemností (§ 13 zákona č. 293/1993 Sb. o výkonu vazby). Kontrolu provádí orgán Vězeňské služby, v některých případech (koluzní vazba, tj. vazba, jejímž důvodem je obava, že obviněný bude mařit objasňování skutečností závažných pro trestní stíhání) pak přímo orgán, který vede trestní řízení. Zákon důsledně zakazuje kontrolu korespondence mezi obviněným a jeho obhájcem, mezi obviněným a státními orgány České republiky nebo diplomatickou misí anebo konzulárním úřadem cizího státu anebo mezi obviněným a mezinárodní organizací, která je podle mezinárodní úmluvy, jíž je Česká republika vázána, příslušná k projednávání podnětů týkajících se ochrany lidských práv. [62]

Obviněnému, který není umístěn v koluzní vazbě, se v odůvodněných případech umožní použití telefonu ke kontaktu s osobou blízkou, v případě závažných důvodů pak i s jinou osobou. Při použití telefonu je nicméně Vězeňská služba oprávněna seznamovat se formou odposlechu s těmito telefonáty a pořizovat jejich záznam. Odposlech a záznam hovorů však obdobně jako u kontroly korespondence opět není možný, komunikuje-li obviněný s osobami uvedenými v předchozím odstavci (obhájce, státní orgány ČR atd.) a dále i s orgánem sociálně-právní ochrany dětí, jde-li o mladistvého.

---

[62] Srovnej i Stanovisko ke sjednocení výkladu zákonů a jiných právních předpisů k otázce přípustnosti kontroly odesílání korespondence obviněným jeho obhájci. Stanovisko vydal Nejvyšší státní zástupce 22.7.2002 pod poř. č. 16/2002.

S určitými odchylkami existuje obdobná úprava zasílání korespondence a užívání telefonu (a jejich kontroly) i pro režim **výkonu trestu odnětí svobody**, který upravuje zákon č. 169/1999 Sb. o výkonu trestu odnětí svobody a jeho prováděcí vyhláška Ministerstva spravedlnosti č. 345/1999 Sb., kterou se vydává řád výkonu trestu odnětí svobody.

Tolik tedy zhruba k základnímu pojednání o nejdůležitějších ustanoveních Listiny základních práv a svobod, jež se týkají problematiky ochrany soukromí.

2.5.3 Ochrana soukromí v zákonech ČR

Problematiku ochrany soukromí a zaručení práva na ochranu soukromí kromě právních norem s ústavní silou upravuje v českém právním řádu i **řada zákonů.**

Nejdůležitějším zákonem, který i nejpodrobněji rozvádí ústavní garance práva na soukromí jednotlivce je bezpochyby **občanský zákoník** (zákon č. 40/1964 Sb. ve znění pozdějších předpisů). Ten ve své hlavě druhé, oddílu prvním (§§ 11-17) upravuje právní institut tzv. **obecné občanskoprávní ochrany osobnosti**. Podle právní teorie je občanskoprávní ochrana osobnosti dle občanského zákoníku speciální úpravou tzv. všeobecného osobnostního práva.[63] Dovolím si zde pro přehlednost a s ohledem na vysokou relevanci vzhledem k tématu práce citovat platnou právní úpravu zakotvující ochranu osobnosti v tomto právním předpise:

„**§ 11**
Fyzická osoba má právo na ochranu své osobnosti, zejména života a zdraví, občanské cti a lidské důstojnosti, jakož i soukromí, svého jména a projevů osobní povahy.

§ 12
(1) Písemnosti osobní povahy, podobizny, obrazové snímky a obrazové a zvukové záznamy týkající se fyzické osoby nebo jejích projevů osobní povahy smějí být pořízeny nebo použity jen s jejím svolením.

(2) Svolení není třeba, použijí-li se písemnosti osobní povahy, podobizny, obrazové snímky nebo obrazové a zvukové záznamy k účelům úředním na základě zákona.

[63] K teoretickým otázkám ochrany osobnosti fyzické osoby srovnej publikaci KNAPP – ŠVESTKA – JEHLIČKA a kol.: Ochrana osobnosti podle občanského práva. 4 vydání. Praha: LINDE, 2004.

(3) Podobizny, obrazové snímky a obrazové a zvukové záznamy se mohou bez svolení fyzické osoby pořídit nebo použít 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.

§ 13

(1) Fyzická osoba má právo se zejména domáhat, aby bylo upuštěno od neoprávněných zásahů do práva na ochranu její osobnosti, aby byly odstraněny následky těchto zásahů a aby jí bylo dáno přiměřené zadostiučinění.

(2) Pokud by se nejevilo postačujícím zadostiučinění podle odstavce 1 zejména proto, že byla ve značné míře snížena důstojnost fyzické osoby nebo její vážnost ve společnosti, má fyzická osoba též právo na náhradu nemajetkové újmy v penězích.

(3) Výši náhrady podle odstavce 2 určí soud s přihlédnutím k závažnosti vzniklé újmy a k okolnostem, za nichž k porušení práva došlo.

§ 14

Zrušen.

§ 15

Po smrti fyzické osoby přísluší uplatňovat právo na ochranu její osobnosti manželu a dětem, a není-li jich, jejím rodičům.

§ 16

Kdo neoprávněným zásahem do práva na ochranu osobnosti způsobí škodu, odpovídá za ni podle ustanovení tohoto zákona o odpovědnosti za škodu.

§ 17

Zrušen.“

Institut ochrany osobnosti jako dílčí složku všeobecného osobnostního práva, jakož i obecnější problematiku ochrany soukromí jednotlivce dále doplňují například následující zákony:

Zákon o ochraně osobních údajů (zákon č. 101/2000 Sb. ve znění pozdějších předpisů)

Zákoník práce (zákon č. 262/2006 Sb.), který se poprvé v historii českého, resp. československého pracovního práva zabývá i otázkou ochrany soukromí zaměstnanců na pracovišti.[64]

Tiskový zákon (zákon č. 46/2000 Sb.) a **zákon o provozování rozhlasového a televizního vysílání** (zákon č. 231/2001 Sb.)

[64] Srovnej ustanovení § 316 platného zákoníku práce a podrobněji i dále v textu této práce.

Zákon o elektronických komunikacích (zákon č. 127/2005 Sb.), který se ve svých §§ 87 - 97 zabývá zabezpečením ochrany osobních, provozních a lokalizačních údajů a důvěrností komunikací.

Trestní a obdobnou ochranu právu na ochranu soukromí a příbuzným souvisejícím právům zakotvuje pak **trestní zákoník** (zákon č. 40/2009 Sb.) a **přestupkový zákon** (zákon č. 200/1990 Sb.).

Problematika související s právem jednotlivce na soukromí je samozřejmě upravena i v řadě dalších právních norem, ať již zákonného nebo podzákonného charakteru. Jejich podrobný výčet však přesahuje možnosti této práce.[65]

2.6 Ochrana soukromí a válka proti teroru

V poslední době jsme celosvětově svědky poměrně masivního prosazování nového druhu legislativy, která spočívá v udílení širších pravomocí bezpečnostním složkám státní moci a s tím souvisejícím postupným omezováním základních lidských práv a svobod. To vše se děje v rámci **boje proti teroru, nadnárodnímu organizovanému zločinu a obdobným druhům nových globálních hrozeb**. Přitom platí, že nejvýznamnějšími impulsy pro zavádění předpisů, které ve větší míře umožňují používání sledovacích technologií a získávání informací z telekomunikací, a které udílí bezpečnostním orgánům i další oprávnění, byly nepochybně teroristické útoky v září 2001 ve Spojených státech a následně teroristické útoky na Madrid a atentáty v londýnském metru dne 7. července 2005. Obecně platí, že se vymezují nové skutkové podstaty trestných činů, policejním a jiným orgánům se rozšiřují pravomoci, zpřísňuje se imigrační a migrační politika, podstatně se zpřísňuje tzv. objektová bezpečnost (letiště, veřejná místa - instalace kamerových systémů), zvažují se dokonalejší identifikační metody, včetně celonárodních

[65] Podrobněji k dalším souvisejícím zákonům viz KNAPP – ŠVESTKA – JEHLIČKA a kol.: Ochrana osobnosti podle občanského práva (cit. dříve), str. 15-36.

databází a registrů (např. v USA a Velké Británii se vážně uvažuje o prolomení dosavadního tabu, kterým by bylo zavedení identifikačních karet všem obyvatelům), posilují se pravomoci orgánů finanční a daňové kontroly, precizuje se tzv. krizové zákonodárství atd. atd.

Koncem září 2001, tedy krátce po útocích na Světové obchodní centrum, se v Paříži koná konference předsedů úřadů pro ochranu osobních údajů, která se ve své závěrečné rezoluci mimo jiné zabývá i tématem ochrany osobních údajů v souvislosti s občanskými svobodami a s bezpečnostními opatřeními, která bude nutné přijmout v souvislosti s útoky 11. září v New Yorku.[66]

Ve Spojených státech je ani ne po padesáti dnech od útoků 11. září 2001 přijat zákon o sjednocení a posílení Ameriky za použití vhodných nástrojů požadovaných k předcházení a čelení terorismu („*Vlastenecký zákon*“).[67] Tento zákon v zájmu nutnosti boje s novými hrozbami teroru a organizovaného zločinu pozměňuje řadu dosud platných zákonů jako je ***Electronic Communications Privacy Act*** z roku 1986, ***Omnibus Crime Control and Safe Streets Act*** z roku 1968 (Title III), 18 USC 2510-2522, ***Digital Telephone Act*** z roku 1994, ***Foreign Surveillance Act*** z roku 1978 (50 USC 1801-1811) a jiné. Zákon mimo jiné nově zavádí příkladně následující:

- rozšíření pravomocí tzv. Pracovních skupin proti elektronické kriminalitě
- širší pravomoci prezidenta v případě, že USA čelí teroristickému útoku
- nové skutkové podstaty (podezření) vztahující se k oblasti terorismu a financování terorismu, podmínky nasazení odposlechu a sdílení zjištěných údajů mezi jednotlivými bezpečnostními službami

---

66 Srovnej NEUWIRT, K.: Ochrana osobních údajů a boj proti terorismu. In. SCHEU, H. (Eds.): Právní aspekty boje proti terorismu. Praha: Univerzita Karlova v Praze – Evropské informační středisko, 2005.

67 V originále: *Act of uniting and strengthening America by providing appropriate tools required to intercept and obstruct terroris*m („***Patriotic Act***“). Návrh zákona byl ve dnech 23.-24. října 2001 projednán Dolní sněmovnou a schválen počtem hlasů 357 pro, 66 proti. Dne 25. října 2001 zákon schválila Horní sněmovna (98 pro, 1 proti) Kongresu USA. Dne 26. října 2001 zákon podepisuje prezident Bush. Bližší pojednání o zákoně viz KRULÍK, O.: Zákon o sjednocení a posílení Ameriky za použití vhodných nástrojů požadovaných k předcházení a čelení terorismu („Vlastenecký zákon), zveřejněný na internetových stránkách Ministerstva vnitra ČR: http://aplikace.mvcr.cz/archiv2008/rs_atlantic/data/files/vlastzak.pdf [cit. 2012-02-18].

- možnosti užití faktů zjištěných z odposlechu a elektronické pošty. V případě, že by jinak došlo k ohrožení z prodlení, lze zjištěné skutečnosti využít okamžitě (pro zatčení nějakých osob, zabavení věcí, atd.)
- uvádí nutnost zlepšení technických možností zpravodajské komunity USA (např. pro odposlech „hlasových schránek" a užití programu Carnivore službou NSA)
- užití údajů z různých databází pro vystopování dopadení pachatele, sdílení dat v registrech, práva vstupovat do nich a dozor Kongresu nad tím, že tyto údaje nebudou zneužity
- pravidla výměny informací se zpravodajskými službami jiných zemí
- nová pravidla běžného platebního styku mezi finančními institucemi a občanem
- sdílení informací o konkrétních osobách mezi Ministerstvem zahraničních věcí a FBI, nový informační systém
- integrovaný systém databáze otisků prstů
- nastoluje nový standard strojově čitelných cestovních dokladů a umístění čteček na hraničních přechodech, stejně jako kroky pro zkvalitňování dokladů proti padělání
- navrhuje možnosti identifikace teroristů podle jejich DNA (vytvoření databanky DNA zločinců – odběru DNA se musí na vyžádání podrobit všechny osoby, odsouzené do federálních vězení, se zvláštním důrazem na pachatele násilných činů)
- vytváří se Systém bezpečného sdílení informací („Secure Information Sharing System") mezi jednotlivými vládními agenturami
- precizuje a rozšiřuje skutkové podstaty trestných činů, nové trestné činy („vnitrostátní terorismus")
- boj proti bioterorismu apod.

V rámci Rady Evropy je 15.7.2002 přijata **Směrnice výboru ministrů Rady Evropy o lidských právech a boji proti terorismu**, která potvrzuje pozitivní závazek státu k ochraně základních práv jednotlivců před teroristickými akty. Směrnice dále stanoví, že všechna opatření proti terorismu musí respektovat lidská práva a zásadu vlády práva (*rule of law*) s tím, že případná omezení lidských práv musí být co nepřesněji vymezena a musí být nezbytná a přiměřená vzhledem ke sledovanému cíli.[68]

Na poli Evropské unie dochází po útocích v září 2001 k přijímání sekundárního unijního práva v rámci tzv. druhého a třetího pilíře EU. Jsou

[68] Blíže k tématu viz ŠTURMA, P.: Odpověď mezinárodního práva na mezinárodní terorismus (vybrané otázky). In: DANČÁK, B. – ŠIMÍČEK, V. (Eds.): Bezpečnost České republiky – Právní aspekty situace po 11. září 2001. Sborník z konference. Brno: Masarykova univerzita v Brně, Mezinárodní politologický ústav, 2002.

jimi dokumenty **Společný postoj Rady EU z 27.12.2001** (2001/931/CFSP) přijatý v rámci společné zahraniční a bezpečnostní politiky, který mimo jiné definuje jednotný pojem teroristického činu, a dále **rámcové rozhodnutí Rady EU z 13.6.2002 o boji proti terorismu** (2002/475/JHA), které přejímá společnou definici teroristického činu a dále stanoví závazky k harmonizaci trestního práva; toto rámcové rozhodnutí bylo dále upraveno v roce 2008.[69] V březnu 2004 se koná bruselský summit Rady EU, který se intenzivně zabýval bojem s terorismem i obecnou kriminalitou. V souvislosti se summitem byl vydán i **Protiteroristický plán Evropské komise** (MEMO/04/66 z 18. března 2004) **a návrh Prohlášení EU k boji proti terorismu zpracovaný pro tento summit** (7468/4/04 REV 4 ze 22. března 2004). V roce 2010 Komise shrnuje dosavadní politiku boje proti terorismu v rámci EU například ve sdělení z 20.7.2010.[70]

V Evropě je za jednoho z hlavních iniciátorů a hybatelů prosazování nových právních předpisů a dokumentů v oblasti sledovacích a informačních technologií považována Velká Británie, jakožto největší spojenec Spojených států ve válce proti teroru. Je to právě Velká Británie, která například na půdě Evropského parlamentu prosazuje v rámci boje proti terorismu svůj plán na celoevropské archivování internetových dat a dat o hovorech uskutečněných mobilními telefony.[71] Byla to také zejména Velká Británie, která se zasadila v době svého předsednictví Evropské unii o přijetí směrnice požadující shromažďování informací o tom, kdo kdy komu emailoval a telefonoval (již několikrát zmiňovaná směrnice data retention), členské země Evropské unie musely směrnici transponovat nejpozději do srpna 2007.

Spolu se snahami o přijetí směrnice o povinném uchovávání veškerých dat o telefonické, mobilní, e-mailové a jiné internetové komunikaci a jiných dokumentů sílilo v Evropě hnutí proti zavádění toho druhu zákonodárství (v souvislosti s bojem proti teroru), které představuje

---

69 Srovnej ŠTURMA, P. – citovaná práce, str. 207.

70 Sdělení Evropské komise dostupné online v českém jazyce na: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/987&format=HTML&aged=1&language=CS&guiLanguage=en [cit. 2012-01-21].

71 V dubnu 2004 navrhla Velká Británie spolu s Francií, Irskem a Švédskem, že by se telekomunikační data měla archivovat nejméně po dobu jednoho roku (společný návrh Rámcového rozhodnutí o uchovávání komunikačních dat).

významný zásah do soukromí.[72] Různé iniciativy brojily a stále brojí proti zavádění sledování a sbírání všemožných informací o osobách a poukazují na jejich zbytečnost. Poukazují přitom na existenci jiných způsobů boje proti terorismu a kriminalitě při používání přesnějších a cílenějších metod. Je nepochybné a lze s těmito aktivisty souhlasit v tom, že pro účely boje s terorismem a jinými hrozbami, včetně kriminality, bude vždy ze získaných informací použito jen zcela nepatrné množství. Vzhledem k ohromnému objemu dat, která budou nyní veřejné i soukromé subjekty uchovávat, se odhaduje použitelnost v řádech desetin procent.[73]

[72] Kupříkladu iniciativa „*Joint Declaration on Data Retention*" poukazovala i na jiné možnosti řešení v rámci boje proti terorismu a především nesouhlasila se snahou obejít parlamenty členských států při omezení základních práv mezinárodními ujednáními bez předchozího souhlasu národních zákonodárných sborů.

[73] Např. Peter Schaar, předseda Pracovní skupiny EU pro ochranu osobních údajů uvádí, že 99,9% občanů „postižených" systémem *data retention* bude zcela nevinných a údaje těchto občanů se dotýkající nebudou mít žádný význam.

3 OBRAZOVÉ ZÁZNAMY A SNÍMKY OBECNĚ

3.1. Úvod do problematiky, historie uchovávání obrazu

Problematika obrazového sledování, uchovávání obrazové informace a její další využití není v lidské historii žádnou čerstvou novinkou. Již od prvního objevu uchovávání obrazových informací se objevovala celá škála možného využití obrazových technologií za nejrůznějšími účely. Lidé si nepochybně spojují pojem obrazové sledování, kamerové systémy a obrazové záznamy až s vývojem posledních několika málo let, kdy jsou technologie umožňující obrazové sledování opravdu masově nasazovány v nejrůznějších oblastech lidské činnosti. Pravda však je, že skutečná historie kamerového sledování či využívání obrazových záznamů se začala psát mnohem dříve.

V roce 1878 probíhají první pokusy s telegrafickým přenosem obrazu, v roce 1884 je vynalezen princip řádkování pomocí tzv. Nipkowova kotouče (rozklad obrazu na jednotlivé body a jeho opětovné složení pomocí rotujícího kotouče s otvory) a v roce 1934 je vynalezena první snímací elektronka Ikonoskopu. V roce 1936 je zavedeno pravidelné televizní vysílání (jedna z prvních velkých událostí byl přenos olympijských her v Mnichově v roce 1936). [74]

Snad první zaznamenané použití kamer pro sledovací účely je z roku 1942, kdy byly kamery užity k vojenským účelům ještě za druhé světové války ve středisku pro vývoj raket V-2 v německém Peenemünde (sledování startů raket).

Již v průběhu 60. let minulého století se začaly objevovat hlasy navrhující instalaci a využití kamer pro policejní účely sledování veřejných prostranství. V roce 1960 londýnská policie použila dočasně umístěné kamery k monitorování veřejných demonstrací na Trafalgarském náměstí (mimo jiné i v souvislosti s návštěvou thajské královské rodiny) a dále pro

[74] Viz článek Jacyszyn, Václav: Od Nipkowa k druhé světové válce, aneb počátky televize. 2007, dostupné online na: http://tele.tym.cz/zajimavosti/pocatky_tv/pocatky_tv.htm [cit. 2012-01-21]
Kamerový systém [online], Wikipedie, dostupné online na: http://cs.wikipedia.org/wiki/Kamerov%C3%BD_syst%C3%A9m [cit. 2012-01-21]

monitorování průběhu oslav tzv. "Guy Fawkes Day". První stálé kamery byly instalovány patrně v roce 1964 na londýnském vlakovém nádraží a v tu stejnou dobu začal provádět testování se čtyřmi kamerami i Liverpool. V roce 1969 mělo být ve Spojeném království instalováno již 69 kamer.[75]

V roce 1969 pak byly instalovány patrně první kamery v USA v objektu New York City Municipal Building poblíže newyorské radnice (City Hall).

Po zavedení magnetofonových kazetových přehrávačů a pásek se objevilo ještě masivnější využívání kamerové technologie, jakož i uchovávání obrazu a jeho využívání jako důkazu. Velká Británie instaluje v roce 1975 kamerový systém za účelem monitorování dopravní situace na velkých dálnicích, instaluje další kamery do největších 4 stanic metra. Kamerové systémy, obrazové nahrávky a další technologické novinky jsou stále častěji využívány nejenom ze strany státních orgánů, ale i nejrůznějších soukromých subjektů a podnikatelů. Zaměstnavatelé začínají využívat obrazové sledování pro kontrolu svých zaměstnanců, soukromí detektivové opatřují podrobné a technicky dokonalé záznamy zejména za účelem dokazování ve složitých rozvodových řízeních, banky a další instituce instalují kamery za účelem posílení bezpečnosti a ochrany majetku. S nástupem počítačových mikročipů se stávají kamerové systémy stále dokonalejší, postupně umožňují sledování a nahrávání i za ztížených světelných podmínek, časem i v noci. Tak jak tomu v oblasti bezpečnosti a související problematiky ochrany soukromí bývá, velké změny se dějí zejména po násilných činech, které hýbou veřejným míněním a umožňují kvalitativní změny ve vnímání reality a pojetí společenských jevů. Tak po útocích na Světové obchodní centrum v roce 1993 instalují ve větším měřítku orgány newyorské policie, FBI a CIA na místě celou řadu kamer za účelem zvýšení bezpečnosti a ochrany proti terorismu. Za stejným účelem jsou instalovány kamery i ve sportovním světě při světovém poháru v socceru[76] v roce 1994 v americkém Giant Stadium. Éra digitalizace pak

---

75 Zdroj informací dostupný na webu žurnálu NOT BORED online na: http://www.notbored.org/england-history.html [cit. 2012-01-21].

76 Viz článek dostupný online na: http://www.video-surveillance-guide.com/history-of-video-surveillance.htm [cit. 2012- 01-21]

přináší ještě masivnější boom využití obrazových metod sledování a uchovávání obrazu.[77]

Zcela zásadní mezník pro rozvoj užití kamerových obrazových metod a vůbec i posun vnímání tohoto jevu ve společnosti nastal v souvislosti s atentáty v USA 11. září 2001. Od této doby nastal boom nejrůznějších stále dokonalejších technologií, a to jak hardwarových, tak i softwarových. Začíná se poprvé používat automatizované obrazové rozpoznávání obličeje (facial recognition system). Jeden z prvních takovýchto systému instaluje americká správa parků (United States Park Service) u sochy Svobody a na Ellisově ostrově v New Yorku.

V prosinci 2003 pak jedna z arizonských škol instalovala systém obrazového sledování s možností rozpoznání obličejů, a to za účelem boje proti sexuálně motivovaným trestným činům a pomoci při vyhledávání ztracených dětí.[78] I v současnosti to byla právě Arizona, která pilotně zavedla systém rozpoznání obličeje na základě fotografie obličeje, oční duhovky a otisku prstů a jeho masivní využití státními orgány, zejména policií. Policisté mají k dispozici zařízení umožňující obrazovou identifikaci konkrétního občana a porovnání jeho údajů s údaji v databázi. Tento systém je nyní rozšiřován mezi policejní orgány po celé USA, když dříve již byl úspěšně užíván na vojenských misích v Iráku a v Afganistánu, kde umožňoval jednodušší identifikace civilistů vstupujících na checkpointech do bezpečných, prověřených zón a jejich odlišení od známých teroristů a nepřátel zavedených v databázi. Užití tohoto systému přímo na půdě amerických ulic nicméně z logických důvodů vyvolává mezi ochránci soukromí obavy a odpor.[79]

---

[77] Jako jeden z hybatelů průniku kamer do nejintimnějšího soukromí občanů je uváděno rozšíření dětských sledovacích zařízení umožňujících přenos obrazu a zvuku a de facto neustálou kontrolu potomků i v době, kdy se jim rodiče nemohou kvůli práci či jiným aktivitám věnovat. Tak došlo k masivnějšímu nasazování kamer a moderních technologií přímo do obydlí soukromých jednotlivců.

[78] Proti spuštění tohoto monitorovacího programu ještě před jeho uvedením protestovala organizace ACLU (The American Civil Liberties Union), která namítala zásah do soukromí, nevhodnost školního prostředí pro zavádění policejních „check-pointů“ a nadbytečnost, neefektivitu, jakož i technickou nedokonalost tohoto prostředku. Dopis organizace ACLU arizonským školským orgánům v původním znění je dostupný online na stránkách organizace ACLU: http://www.aclu.org/technology-and-liberty/letter-arizona-school-officials-school-face-recognition [cit. 2012-01-21].

[79] Viz zprávy z amerického tisku dostupné online na:

Další skok v rozšíření obrazového sledování pak představovalo rozšíření Internetu a informačních technologií. Nyní je celý svět fakticky propojen a není problémem sledovat aktuální záznam z milionu kamer rozmístěných po celém světě odkudkoliv, kde je přístup k Internetu.

Kamerové systémy, obrazové záznamy či obrazové snímky jsou pojmy, se kterými se v dnešní době setkal již každý. Nejinak je tomu v právu a právní vědě. I ta se na danou problematiku zaměřuje, snaží se ji zachytit a prozkoumat ve světle právního myšlení, právního světa a všech relevantních souvislostí. Nejdůležitější souvislost je nepochybně zakotvení institutu obrazového sledování (které zahrnuje jak kamerové sledování kamerovými systémy či jednotlivými kamerami, tak i obrazové sledování fotografickými přístroji a jinými optickými pomůckami, jakož i pořizování jednotlivých obrazových snímků a jejich další využití) a jeho vymezení k institutu ochrany soukromí.

Pokud jde o legislativní výskyt daných termínů, je nepochybné, že termín obrazový záznam se v právním řádu České republiky vyskytuje řádově častěji než termín kamerový systém. Masivnější používání pojmu obrazový záznam či zvukově obrazový záznam bylo započato přijetím občanského zákoníku a trestního zákona počátkem šedesátých let minulého století, jakož i jejich procesních norem (trestní řád, občanský soudní řád). Občanský zákoník z roku 1964 zakotvil první komplexnější ochranu osobnosti a tedy i ochranu práva na vlastní podobu. Před tímto obdobím nebyla ochrana vlastní podoby (podobizny) chráněna v režimu občanského zákoníku, ale v rámci autorského zákona (viz ustanovení § 96 zákona č. 115/1953 Sb.), resp. pak v rámci trestních norem. Lze říci, že přijetím občanského zákoníku, tedy zákona č. 40/1964 Sb. přešlo právo na vlastní podobu a jeho ochrana, jakož i meze a limity ochrany z režimu autorského práva do režimu občanskoprávního kodexu. Jako zajímavost lze říci, že

---

http://www.homelandsecuritynewswire.com/arizona-police-deploy-iris-scanners-and-facial-biometrics-identify-inmates
http://online.wsj.com/article/SB10001424052702303678704576440253307985070.html
http://www.popsci.com/technology/article/2011-07/amid-privacy-fears-police-across-nation-will-roll-out-face-recognizing-iphone-tech-year
http://www.npr.org/2011/08/11/138769662/new-police-scanner-raises-facial-profiling-concerns
[vše cit. 2012-01-21].

jeden z prvních výskytů slova obrazový záznam či podobizna v právním řádu České republiky či jejích právních předchůdců je patrně ustanovení zákona č. 49/1866 českého zemského zákoníku (Honební zákon pro Čechy), který ve svém § 26 c) věta druhá zmiňuje povinnost opatřit honební lístek pevně připojenou podobiznou vlastníka.[80] To je možná v běžně dohledatelné právní úpravě jedna z prvních zmínek používání obrazových záznamů jednotlivých osob za účelem uchovávání dat, registrace a podobně. Ochranou podobizny, resp. problematikou ochrany tzv. *práva na vlastním obraze* se zabýval § 34 zákona č. 218/1926 Sb. o původském právu k dílům literárním, uměleckým a fotografickým (o právu autorském). V této souvislosti nelze nezmínit dostupné rozhodnutí tehdejšího Nejvyššího soudu ČR ze dne 25.6.1941 sp. zn. Rv I 1285/40 ve věci svolení zobrazované osoby, kdy soud deklaroval, že *„Svolení zobrazené (vyfotografované) osoby k tomu, aby byla vykonávána výhradná oprávnění původcova k podobizně, může se státi i činem konkludentním. Nevyloučila-li zobrazená osoba výkon původských práv v určitém směru, může původce vykonávati původská práva k obrazu v plném rozsahu (§ 36 odst. 1 zák.). Zákaz ve smyslu § 34 odst. 3 zák. musí býti odůvodněný, a to i tehdy, bylo-li tu svolení zobrazené osoby podle § 34 odst.1 zák.“*

3.2. Osobnostní práva dle občanského zákoníku se zaměřením na obrazové záznamy

3.2.1. Vymezení pojmů, základní pojetí

Aktuální pojmové vymezení problematiky podává kupříkladu komentář občanského zákoníku nakladatelství C.H.BECK při výkladu vztahujícím se k ustanovení § 12 občanského zákoníku pojednávajícím zejména o zákonné licenci k pořízení nebo použití písemností osobní povahy, podobizen, obrazových snímků a obrazových a zvukových

[80] Viz *§ 26 c)* zákona č. 49/1866 českého zemského zákoníku:
„Lístek honební jest platný jen pro osobu, na jejíž jméno zní a platí s výjimkou odst. 3 § 26 d) stanovenou pro celé území království Českého. Honební lístek musí býti opatřen pevně připojenou podobiznou vlastníka a nesmí býti jiné osobě postoupen.“

záznamů.[81] Stávající, platný občanský zákoník se pokouší o dělení ve svém § 12, kdy rozlišuje: *„Písemnosti osobní povahy**, podobizny**, obrazové snímky** a **obrazové** a zvukové **záznamy** týkající se fyzické osoby nebo jejích projevů osobní povahy….“* Pro zásadnost a důležitost daného zákonného ustanovení, které lze označit ve zkoumané problematice jako klíčové, jej znovu cituji:

§ 12

(1) Písemnosti osobní povahy, podobizny, obrazové snímky a obrazové a zvukové záznamy týkající se fyzické osoby nebo jejích projevů osobní povahy smějí být pořízeny nebo použity jen s jejím svolením.

(2) Svolení není třeba, použijí-li se písemnosti osobní povahy, podobizny, obrazové snímky nebo obrazové a zvukové záznamy k účelům úředním na základě zákona.

(3) Podobizny, obrazové snímky a obrazové a zvukové záznamy se mohou bez svolení fyzické osoby pořídit nebo použít 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.

Pokusím se nyní rozdělit jednotlivé případy předmětu občanskoprávní ochrany dle ustanovení § 12 o.z. Samozřejmě, níže uvedené členění vychází z dikce zákonného ustanovení občanského zákoníku a vztahuje se k ochraně osobnosti, má vztah tedy k člověku nebo lidským projevům osobní povahy (nebereme tedy v potaz např. obrazové záznamy prostředí bez zobrazení lidí či bez vztahu ke konkrétním osobám).

Pomineme-li písemnosti osobní povahy, lze rozlišovat:

Podobizna – hmotné zachycení portrétu (podoby) fyzické osoby. Může jít i o i tzv. karikaturu, tedy zkarikované ztvárnění, z něhož lze objektivně dovodit totožnost určitého člověka, např. podle jeho příznačných osobních tělesných rysů (markantů). Podobizna může být ztvárněna graficky, sochařsky jako busta, socha nebo reliéf a podobně.

Obrazový snímek – hmotné zachycení určitého obrazu, skutečnosti, v našem případě pak zachycení podoby fyzické osoby (jde přitom o širší vymezení než u podobizny, která také zachycuje podobu fyzické osoby, ale pouze jako portrét), která je identifikovatelná. Hmotné zachycení reality je

[81] Viz publikace Švestka, Spáčil, Škárová, Hulmák a kol. Občanský zákoník I. § 1 až 459. Komentář. 2. Vydání. Praha: C.H.BECK, 2009.

pak pouze jednorázové, nesekvenční. Někdy se obrazový snímek používá ve stejném kontextu co fotografie (fotografický snímek). Může jít např. i o rentgenový snímek.

Obrazový záznam – zjednodušeně řečeno video či souborná sekvence jednotlivých obrazových snímků. Lze však hovořit i o jednotlivém obrazovém snímku (např. fotografii) a mít na mysli obrazový záznam, hranice mezi obrazovým snímkem a záznamem tak není ostrá a oba pojmy lze de facto zaměnit. Vždy jde o zachycení podoby, chůze, mluvy, zpěvu nebo jiného projevu osobní povahy člověka, jehož lze tímto způsobem objektivně ztotožnit. Technická povaha záznamu je nerozhodná, může jít např. o film či o fotografii nebo obrazovou nahrávku různého technického druhu. Může se jednat i o záznam parodický s tvůrčí nadsázkou, či záznam zašifrovaný, rozpoznatelný jen strojově. Význam má vždy pouze to, je-li objektivně možno ze záznamu určit totožnost konkrétního člověka.

Obrazově zvukový záznam – obrazový záznam doplněný o zvukový projev, a to buď hlasový projev fyzické osoby, nebo okolní zvukovou kulisu.

Nový občanský zákoník rozlišuje mezi podobiznou, obrazovým záznamem a zvukovým záznamem.[82] Pojem obrazového snímku tak již nová právní úprava opouští, tento pojem pak bude podřazen zcela evidentně pod pojem obrazový záznam. Pro potřeby této práce tedy budu používat, nebude-li specifikováno jinak, pojem obrazový záznam i ve smyslu obrazového snímku.

Z hlediska práva osobnostního je bez významu, zda podobizna či obrazový záznam (snímek) je obsahem uměleckého díla např. jako portrét, které by bylo předmětem autorského práva svého autora (§ 2 odst. 1 autorského zákona). Pokud by tomu tak bylo, jednalo by se o souběh chráněných předmětů, kdy jeden je obsahem druhého, a o souběh

[82] K tématu nového občanského zákoníku srovnej i článek- Jiří Maštalka: Návrh nového občanského zákoníku z pohledu ochrany soukromí a osobních údajů, Právní rozhledy 10/2010

soukromých ochranných práv (osobnostního a autorského) se všemi souběžnými právními důsledky.

Jak již tedy bylo shora zmíněno, podobizny, obrazové snímky a obrazové a zvukové záznamy smějí být zásadně ***pořízeny*** nebo ***použity*** jen se svolením fyzické osoby, které se týkají. Jde o projev principu soukromé – privátní autonomie vůle fyzické osoby. Toto svolení může být úplatné či bezúplatné, lze jej učinit nejenom výslovně, nýbrž i konkludentně. Patrně můžeme dělit toto svolení i na svolení nepodmíněné a svolení podmíněné, podle toho, zda je k němu připojena podmínka. Z povahy věci vyplývá, že jak osoba, která udílí souhlas, tak i příjemce tohoto souhlasu, jsou si vědomy, k jakému účelu, jakým způsobem a v jakém rozsahu má být chráněný statek pořízen nebo použit. Daný souhlas je kdykoliv odvolatelný a doktrína dovozuje, že je tomu tak i tehdy, pokud se dotčená osoba zavázala, že souhlas neodvolá, takový závazek by byl neplatný, vždy je však nutno přihlížet i k jiným právním institutům; výkon osobního práva odvolat svolení (souhlas) proto musí být v souladu s dobrými mravy, právy a oprávněnými zájmy jiných, tedy i nabyvatele svolení. Nabyvatel svolení musí být rovněž chráněn, zejména co do svého legitimního očekávání a vynaložené hospodářské investice. Jinak řečeno, odvolání svolení, které je výkonem práva osobnostního, nesmí být nikomu na újmu.

3.2.2 Zákonné licence

Předmětné ustanovení § 12 občanského zákoníku rozeznává situace, kdy svolení fyzické osoby k pořízení nebo použití písemností osobní povahy, podobizen, obrazových snímků a obrazových a zvukových záznamů, není třeba. Zákon rozeznává tzv. **zákonné licence**, které nahrazují souhlas dotčené osoby. Jde tedy o jakýsi státem dovolený zásah do práva osobnostního, kdy jiný zájem (veřejný) převažuje nad zájmem bezezbytku poskytovat ochranu některým osobnostním právům člověka. Obecně tyto licence rozdělujeme na licenci úřední, tedy případ, kdy se chráněných osobnostních statků použije (zákon výslovně nezmiňuje možnost pořízení!) za účelem úředním na základě zákona a dále na licenci vědeckou, uměleckou či zpravodajskou. Pokud jde o licenci vědeckou, uměleckou a

zpravodajskou, ta se však nevztahuje na písemnosti osobní povahy, ty lze bez svolení dotčené osoby použít jen v rámci úřední licence k úředním účelům na základě zákona.

Výkonem umělecké licence osobnostní jakožto jedné ze zákonných licencí dle ustanovení § 12 občanského zákoníku zůstává nedotčeno souběžné právo autorské svědčící autorovi uměleckého díla, jehož obsahem je ideální statek osobní, jakož i uspořadateli souborného díla, např. sbírky fotografických portrétů.

Legálním předpokladem výjimečně dovoleného zásahu do osobnostního práva podle § 12 odst. 3 je i to, aby se tak stalo **způsobem přiměřeným**, tzn. i funkčně s ohledem na přípustný účel (vědecký, umělecký nebo zpravodajský). Pojem „přiměřenosti“ nutno vyložit jako citlivě vyvážený poměr mezi druhem a povahou ideálního statku, požívajícím legální ochrany a spjatým s osobností, a účelem sledovaným dovoleným zásahem.[83]

Poměrně zajímavá otázka se nabízí, pokud jde o zpravodajskou licenci, tedy pro pořízení a použití podobizen, obrazových snímků a obrazových a zvukových záznamů bez svolení fyzické osoby pro tiskové, filmové, rozhlasové a televizní zpravodajství. V době přijetí občanského zákoníku a předmětné úpravy vůbec neexistovalo tzv. internetové zpravodajství, které je dnes masivně rozšířeno a představuje pro část obyvatelstva i důležitější zdroj informací než televizní či rozhlasové zpravodajství. Jde však o to, zda ve smyslu ustanovení § 12 občanského zákoníku lze rozšířit dovolenou výjimku ze zásahu do osobnostního práva i pokud jde o internetové zpravodajství. Osobně jsem toho názoru, že to možné spíše není, i když by se patrně dalo přisvědčit v některých odůvodněných případech výkladu per analogiam a rozšířili bychom daný výčet zpravodajství o další účelový případ, který v době přijetí občanského zákoníku nebyl znám a který by byl ospravedlnitelný z hlediska upřednostnění obecného dobra zpravodajského i rozumného uspořádání poměru mezi dotčenými právy, svobodami a veřejnými statky. Vždy však bude nutné o to přísněji poměřovat rozšíření zpravodajské licence na tento

[83] Viz Ivo Telec: Svolení, nebo zákonné licence v právu osobnostním, Právní rozhledy 24/2007

případ se zásahem do oprávněných zájmů fyzické osoby. Na druhou stranu je však třeba poukázat na možné zneužití a citlivost tohoto řešení, když internetové zpravodajství má v současné době možná nejširší rozsah působení prostřednictvím Internetu a tak prakticky kdokoliv s přístupem k Internetu má k němu přístup. Pokud bychom dané ustanovení vykládali přísně restriktivně, veškeré internetové zpravodajství by bylo velmi omezeno ve své činnosti a patrně by nemohlo smysluplně fungovat (za předpokladu, že by se dotčené osoby domáhaly svých práv).[84] Naštěstí, do budoucna, zdá se, bude problém vyřešen, neboť nový občanský zákoník ve svém ustanovení § 89 stanoví, že *„podobizna nebo zvukový či obrazový záznam se mohou bez svolení člověka také pořídit nebo použít přiměřeným způsobem též k vědeckému nebo uměleckému účelu a pro tiskové, rozhlasové, televizní nebo **obdobné** zpravodajství."*

Vědecká, umělecká nebo reportážní licence nezahrnuje pořízení a zejména ne následné použití chráněných osobnostních statků ke komerčním účelům (v reklamě apod.). K takovému způsobu užití je vždy nutné opatřit si souhlas dané fyzické osoby. V dané souvislosti se hovoří o tzv. model repase, což je smlouva uzavřená mezi fotografem a fotografovanou osobou, ve které tato fotografovaná osoba vymezuje, jak může fotograf s vytvořenou podobiznou nakládat.

3.2.3 Občanskoprávní prostředky ochrany proti neoprávněným zásahům

V případě zásahu do práva na ochranu osobnosti přiznává platný právní řád řadu občanskoprávních prostředků ochrany. Trestněprávní prostředky ochrany s přihlédnutím k tématu této práce jsou probrány v následující podkapitole.

Základní vymezení prostředků ochrany podává ustanovení § 13, 15 a 16 občanského zákoníku (§ 14, který původně upravoval před

[84] Srovnej Telec, I.: Svolení, nebo zákonné licence v právu osobnostním, Právní rozhledy 24/2007 a opačný názor nezahrnující internetové zpravodajství do zákonných licencí uvedený v komentáři Švestka, Spáčil, Škárová, Hulmák a kol. Občanský zákoník I. § 1 až 459. Komentář. 2. Vydání. Praha: C.H.BECK, 2009

polistopadovou novelizací občanského zákoníku zásah směřující proti osobnosti občana týkající se jeho činnosti ve společenské organizaci, byl zrušen):

§ 13

(1) Fyzická osoba má právo se zejména domáhat, aby bylo upuštěno od neoprávněných zásahů do práva na ochranu její osobnosti, aby byly odstraněny následky těchto zásahů a aby jí bylo dáno přiměřené zadostiučinění.

(2) Pokud by se nejevilo postačujícím zadostiučinění podle odstavce 1 zejména proto, že byla ve značné míře snížena důstojnost fyzické osoby nebo její vážnost ve společnosti, má fyzická osoba též právo na náhradu nemajetkové újmy v penězích.

(3) Výši náhrady podle odstavce 2 určí soud s přihlédnutím k závažnosti vzniklé újmy a k okolnostem, za nichž k porušení práva došlo.

§ 15

Po smrti fyzické osoby přísluší uplatňovat právo na ochranu její osobnosti manželu a dětem, a není-li jich, jejím rodičům.

§ 16

Kdo neoprávněným zásahem do práva na ochranu osobnosti způsobí škodu, odpovídá za ni podle ustanovení tohoto zákona o odpovědnosti za škodu.

Občanskoprávní ochrana osobnosti je poskytována jen tehdy, jedná-li se o takový zásah do osobnostních práv, který je neoprávněný. Neoprávněným zásahem je takový zásah, který je v rozporu s právním řádem, obecně se jím rozumí zásadně každé nepravdivé či pravdu zkreslující tvrzení o fyzické osobě, které zasahuje do její osobnosti. Soudní praxe dotváří a precizuje situace, kdy se jedná o neoprávněný zásah do osobnostních práv fyzické osoby. Je tomu tak například v těchto případech:

- obtěžování pohledem formou nahlížení do cizích oken, za předpokladu, že jde o nahlížení soustavné a závažné a objektivně způsobilé narušovat soukromí fyzické osoby (rozsudek Nejvyššího soudu ČR NS sp. zn. 22 Cdo 2251/2005)
- neopodstatněné zveřejnění fotografií zpodobňujících ohořelé tělesné pozůstatky tragicky zesnulého syna žalobců (rozsudek Nejvyššího soudu ČR sp. zn. 30 Cdo 3361/2007), soudy v tomto případě přiznaly omluvu a každému z žalobců náhradu nemajetkové újmy ve výši 50.000,- Kč

O neoprávněný zásah do osobnosti fyzické osoby nepůjde v těch případech, kdy k němu fyzické osoba sama svolila (za předpokladu, že je způsobilá k tomuto právnímu úkonu a může s dotčenou hodnotou v plné

míře disponovat). Dále půjde o situace, kdy zásah do osobnosti fyzické osoby předpokládá a umožňuje zákon, zpravidla s ohledem na zabezpečení priority veřejného zájmu.

Odpovědnost za porušení osobnostních práv je odpovědností objektivní a proto není třeba zkoumat zavinění.[85] Subjektem odpovědnosti za neoprávněný zásah do práv fyzické osoby bude zpravidla fyzická osoba, která jej způsobila. Pokud však byl neoprávněný zásah způsoben fyzickou osobou, která jednala v rámci svého pověření za účelem plnění činnosti pro jinou fyzickou či právnickou osobu, soudní praxe dovozuje, že občanskoprávní odpovědnost postihuje tuto právnickou či fyzickou osobu jako zaměstnavatele, vydavatele apod. Je-li však například pisatelem článku, resp. autorem relace osoba rozdílná od zaměstnance vydavatelství, televizní stanice apod., může se neoprávněným zásahem postižená fyzická osoba domáhat svých práv jak vůči tomuto pisateli či autorovi relace, tak i po vydavatelství/televizní stanici apod. U zaměstnanců novin, televizních stanic apod., se lze nároků domáhat jen vůči jejich zaměstnavatelům.

Pokud jde o konkrétní prostředky ochrany osobnosti fyzické osoby, jsou následující:

- **upuštění od neoprávněného zásahu do práva na ochranu osobnosti**

  použití tohoto institutu vyžaduje, aby neoprávněný zásah v době vydání soudního rozhodnutí stále trval či hrozilo reálné a bezprostřední nebezpečí jeho opakování v budoucnu. Žalobce musí v tzv. zdržovací (negatorní) žalobě přesně specifikovat, čeho se domáhá, jakého konkrétního jednání se má žalovaný zdržet. Případný výkon rozhodnutí ukládajícího zdržet se závadného jednání se děje formou ukládání pokut dle ustanovení § 351 o.s.ř.

- **odstranění trvajících následků neoprávněného zásahu**

[85] Viz např. nález Ústavního soudu ze dne 20.5.2002, sp. zn. IV. ÚS 315/01:
"Vzniklá nemajetková újma na osobnosti postižené fyzické osoby je pro ni stejně závažná bez ohledu na to, jednal-li původce zásahu zaviněně či nikoliv. Subjektivní prvek zavinění má význam toliko při určování výše náhrady nemajetkové újmy dle § 13 odst. 3 obč. zák. v rámci zohlednění okolností, za nichž k porušení práva došlo."

žalobce se může domáhat, aby byly odstraněny trvající následky zásahu, např. aby došlo ke zničení neoprávněně pořízeného obrazového záznamu. Žalobce musí tak jako v předchozím případě přesně a určitě vymezit to, co má žalovaný vykonat.

- **přiměřené zadostiučinění (morální satisfakce)**

  Morální satisfakce bude spočívat v omluvě, odvolání sporného výroku, či v samotném vydání deklaratorního soudního výroku rozsudku, že došlo k porušení práv na ochranu osobnosti.

- **náhrada nemajetkové újmy v penězích (materiální satisfakce)**

  Přiznání materiální satisfakce, tedy náhrady nemajetkové (imateriální) újmy v penězích má místo tam, kde by předchozí institut morální satisfakce nepostačoval, zejména proto, že byla ve značné míře snížena důstojnost fyzické osoby nebo její vážnost ve společnosti. O výši náhrady rozhoduje v konečném důsledku soud s přihlédnutím k závažnosti vzniklé újmy a k okolnostem, za nichž k porušení práva došlo. Žalobcem v žalobě požadovaná částka je maximum, co soud může přiznat, soud nemůže jít nad návrh a přiznat více – viz zásada iudex non eat ultra petita partium). Lze deklarovat, že české soudy přiznávají v porovnání se zahraniční judikaturou spíše nižší částky náhrady nemajetkové újmy v penězích, pohybují se obvykle v řádu maximálně desítek tisíc korun.[86] Náhrada nemajetkové újmy by neměla plnit pouze funkci satisfakční, ale i preventivně-sankční funkci. V českém prostředí je však druhá funkce spíše symbolická, neboť náhrada v řádu desítek tisíc nebude obvykle hrát pro porušovatele velkou roli, zvlášť pokud porušením osobnostního práva získali řádově větší komerční prospěch.[87]

---

[86] Opatrnější postup českých soudů možná zavinilo i zákonné stanovení paušálních náhrad odškodnění stanovení § 444 odst. 3 občanského zákoníku pro případ usmrcení blízkých osob – zde se odškodění pohybuje v částce 240.000,- Kč, případně 175.000,- Kč a 85.000,- Kč. Soudy jsou pak s ohledem na fakt, že porušení jiných práv, než újma na životě, by měla být odškodněna nižší částkou.

[87] Zde poukazuji na relativní výhodnost porušování osobnostních práv ze strany nejrůznějších bulvárních periodik a vydavatelství. Často je pro ně výhodnější dopustit se porušení osobnostních práv určité fyzické osoby, neboť jsou si vědomy přínosu co do zvýšení prodeje periodika.

Všem výše uvedeným právům domáhat se ochrany odpovídají příslušné žalobní nároky. Výčet prostředků ochrany podaný v § 13 není úplný, teoreticky si lze představit ochranu svépomocí dle ustanovení § 6 a ochranu pokojného stavu poskytnutou orgánem státní správy dle § 5 občanského zákoníku. Lze se dále vedle prostředků uvedených v ustanovení § 13 o.z. domáhat i náhrady škody podle ustanovení § 16 o.z. a vydání bezdůvodného obohacení. Stejně tak si lze představit i uplatnění například nároku na určení (např. určení, že došlo k neoprávněnému zásahu do osobnostního práva).

Ustanovení § 15 občanského zákoníku deklaruje, že *„po smrti fyzické osoby přísluší uplatňovat právo na ochranu její osobnosti manželu nebo partnerovi a dětem, a není-li jich, jejím rodičům.“* Daná úprava chrání ochranu osobnosti fyzické osoby i tehdy, není-li již daná osoba naživu a nemůže se aktivně bránit. Jde o tzv. zvláštní osobnostní právo osob uvedených v předmětném ustanovení. Úvahy o možném rozšíření okruhu osob oprávněných k posmrtné ochraně osobnosti se promítly do znění ustanovení § 82 odst. 2 nového občanského zákoníku, který výslovně rozšiřuje okruh osob na veškeré osoby blízké: *„Po smrti člověka se může ochrany jeho osobnosti domáhat kterákoli z osob jemu blízkých.”*

Soud by při svém rozhodování o výši peněžitého zadostiučinění měl přihlížet i k tomu, zda např. původce neoprávněného zásahu zasáhl do osobnosti fyzické osoby jen z nedbalosti (lehkovážnosti) anebo zda mu lze na neoprávněném zásahu a nastalém závažném nepříznivém následku přičíst úmysl, popř. dokonce zlý úmysl (např. záměrně sledovaný cíl skandalizovat a pomluvit určitou osobu). V případě zlého úmyslu (záměru) na straně původce neoprávněného zásahu by měl soud svůj odsudek nad tímto společensky i právně zvlášť odsouzeníhodným chováním vyjádřit právě citelným určením výše peněžitého zadostiučinění. Obdobně by bylo potřeba postupovat i v případě, že by původce neoprávněného zásahu do osobnostních práv právě tímto zásahem sledoval záměr zvýšit svůj majetkový prospěch (např. původce zásahu do soukromí určité prominentní osoby by kalkuloval se zvýšeným odběrem svého tisku aj.) - k tomu podrobněji viz blíže Knap, K. a kol.: Ochrana osobnosti podle občanského práva. 4. podstatně přepracované a doplněné vydání. Praha: Linde Praha, a.s., 2004. s. 195.

3.2.4 Trestněprávní konsekvence ochrany obrazových záznamů a podobizen

V některých případech je neoprávněný zásah do všeobecného osobnostního práva zároveň zásahem do veřejného zájmu chráněného veřejnoprávní úpravou a tímto se tak občanskoprávní a trestní, resp. správní prostředky ochrany osobnosti doplňují, přičemž jsou na sobě nezávislé. Trestní represe je všeobecně považována až za druhotnou, totiž podpůrně nastupující až po bezvýsledném postihu soukromoprávním, vždy tomu tak však být nemusí. Trestně právní odpovědnost je založena při neoprávněném zásahu do osobnosti fyzické osoby vždy na principu zavinění.

V trestním zákoníku, zákoně č. 40/2009 Sb. jsou v návaznosti na ochranu osobnosti a soukromí zejména trestný čin **pomluvy (§ 184)**, který chrání čest, vážnost a dobrou pověst u spoluobčanů, a trestné činy **porušení tajemství dopravovaných zpráv (§ 182)** a **porušení tajemství listin a jiných dokumentů uchovávaných v soukromí (§ 183)**, čímž je chráněno neoprávněné zasahování do soukromí, jak je to vyjádřeno i v čl. 13 LZPS, podle něhož nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon. Trestným činem **neoprávněného nakládání s osobními údaji (§ 180)** je pak zajištěno provedení čl. 10 odst. 3 LZPS a tedy ochrana osobních údajů před jejich neoprávněným zpřístupňováním, zveřejňováním nebo zneužíváním.

Ochranu uvedeným zájmům poskytují i některá jiná ustanovení trestního zákoníku uvedená v jiných hlavách trestního zákoníku, jako např. v hlavě X. trestního zákoníku mezi trestnými činy narušujícími občanské soužití zařazené nové ustanovení o nebezpečném pronásledování (§ 354), které také směřuje proti zasahování do soukromí osob.

Z hlediska této práce jsou důležitá trestněprávní ustanovení trestního zákoníku vymezující trestné činy **neoprávněné nakládání s osobními údaji (§ 180), porušení tajemství dopravovaných zpráv (§ 182)** a **porušení tajemství listin a jiných dokumentů uchovávaných v soukromí (§ 183**), dále i trestný čin **pomluvy (§ 184)**. Jelikož daná problematika byla již rámcově zmíněna a probrána v kapitole 2 této práce

(podkapitola 2.5.2 Ochrana soukromí v ústavním pořádku ČR), zaměřím se nyní jen na korelaci problematiky s tématem kamerových systémů a zejména obrazových záznamů.[88]

Neoprávněné nakládání s osobními údaji (§ 180)

Objektem trestného činu je právo na ochranu před neoprávněným zveřejňováním osobních údajů a jejich zneužíváním. Předmětné ustanovení obsahuje dvě samostatné skutkové podstaty, jedna chrání každého před neoprávněným zveřejněním, sdělením, zpřístupněním, jiným zpracováním nebo přisvojením si osobních údajů o jiném v souvislosti s výkonem veřejné moci. Druhá skutková podstata sankcionuje neoprávněné zveřejnění, sdělení nebo zpřístupnění třetí osobě osobních údajů získaných v souvislosti s výkonem povolání, zaměstnání nebo funkce pachatele, jestliže tím pachatel porušil státem uloženou nebo uznanou povinnost mlčenlivosti. Trestní právo zde tedy nesankcionuje každé neoprávněné nakládání s osobními údaji, nýbrž pouze kvalifikované – buďto musí jít o neoprávněné nakládání s osobními údaji shromážděnými v souvislosti s výkonem veřejné moci, nebo získané v souvislosti s výkonem povolání, zaměstnání nebo funkce. Předmětem ochrany jsou nepochybně i obrazové záznamy (jednotlivé snímky, fotografie, ale i videa) zachycující jednotlivce nebo projevy osobní povahy.

Porušení tajemství dopravovaných zpráv (§ 182)

Objekt tohoto trestného činu zahrnuje tajemství dopravovaných zpráv, konkrétně tajemství

a) uzavřeného listu nebo jiné písemnosti při poskytování poštovní služby nebo přepravované jinou dopravní službou nebo dopravním zařízením,
b) datové, textové, hlasové, zvukové či **obrazové zprávy** posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli, který zprávu přijímá, nebo

[88] Podrobněji k trestněprávní problematice viz Šámal, P. a kol.: Trestní zákoník I., II. Komentář. 1. Vydání. Praha: C.H.BECK, 2010.

c) neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková počítačová data,

Ustanovení § 182 taktéž sankcionuje prozrazení nebo využití tajemství, o němž se pachatel dozvěděl z písemnosti, telegramu, telefonního hovoru nebo přenosu prostřednictvím sítě elektronických komunikací.

Obrazovou zprávou uvedenou shora pod písmenem b) se pak rozumí prostřednictvím sítě elektronických komunikací přenášený obrazový záznam určitého stavu, děje, procesu nebo jevu zachycený pomocí technického zařízení (zpravidla videokamerou, fotoaparátem, webovou kamerou apod.), a to nejenom ze záznamu, ale i naživo (on line) s využitím nejčastěji Internetu pro uskutečnění spojení např. pomocí programu Skype. V dnešní době je zvlášť poukazováno na ne tak dokonalou bezpečnost přenosu dat pomocí internetových technologií; v porovnání s přenosem dat telefonním přístrojem jde o metodu obvykle méně zabezpečenou a zranitelnější vůči průniku.

Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí (§ 183)

Objektem tohoto trestného činu je listovní tajemství a tajemství jiných písemností, fotografie, filmu nebo jiného záznamu, počítačových dat anebo jiného dokumentu uchovávaného v soukromí. Může tedy jít z našeho tematického pohledu o fotografie osob (trestněprávní ochrany však požívají i fotografie neosobní), obrazové snímky, filmy (zpravidla filmy a nahrávky osobní povahy) a jiné záznamy (např. videozáznam pořízený webkamerou). Porušení tajemství pak může nastat třemi způsoby:

a) zveřejněním
b) zpřístupněním třetí osobě
c) použitím jiným způsobem

Pomluva (§ 184)

Z našeho pohledu je nezajímavější kvalifikovaná skutková podstata tohoto trestného činu, kterým někdo o jiném sdělí nepravdivý údaj,

způsobilý značnou měrou ohrozit jeho vážnost u spoluobčanů, pokud se tak stane tiskem, **filmem**, rozhlasem, **televizí**, **veřejně přístupnou počítačovou sítí** nebo jiným obdobně účinným způsobem.

3.2.5 Nový občanský zákoník

Počátkem roku 2012 podepsal prezident republiky **nový občanský zákoník**, který vstoupí v účinnost 1.1.2014. Občanský zákoník byl publikován ve Sbírce zákonů České republiky jako **zákon č. 89/2012 Sb.** (nový občanský zákoník dále i jen jako „NOZ"). Z hlediska tématu naší práce nás samozřejmě nejvíce zajímá nová úprava a koncepce práva na soukromí a obdobných práv. Již ustanovení § 3 odst. 2 NOZ, kde se hovoří o základních zásadách soukromého práva na čelním místě zmiňuje, že *„každý má právo na ochranu svého života a zdraví, jakož i svobody, cti, důstojnosti a soukromí*."

Nový občanský zákoník prošel dlouholetým vývojem v procesu jeho přijímání. Již v roce 2001 formuloval Telec následující teze:

a) nový kodex musí být založen na přirozenoprávním principu; jedině tak bude učiněno zadost požadavku ústavní konformity předpisu,
b) systematika nového kodexu by měla respektovat význam hodnot a institutů v moderním právním státě, tj. „osobnost-rodina-vlastnictví-smlouva",
c) právní úprava osobnosti, respektive soukromí fyzické osoby by pak měla být obohacena o aktivní věcnou a procesní legitimaci právnické osoby po případ, kdyby byla zasažena osobnostní práva jejího zaměstnance, a rozšířen okruh aktivně legitimovaných k postmortální ochraně o osoby blízké.[89]

Lze deklarovat, že těmto premisám NOZ vyhověl.

Z přijaté právní úpravy, kterou obsahuje nový občanský zákoník, je z našeho pohledu nejzajímavější Oddíl 6 nového občanského zákoníku, konkrétně pak pododdíl 1 nazvaný „Obecná ustanovení" a pododdíl 2

[89] TELEC, I.: Osobnostní práva a rekodifikace českého obecného soukromého práva. Právní praxe 1-2/2001. s. 110-111

nazvaný „Podoba a soukromí“. Pro přehlednost zde texty obou poddodílů cituji:

Pododdíl 1

Obecná ustanovení

§ 81

(1) Chráněna je osobnost člověka včetně všech jeho přirozených práv. Každý je povinen ctít svobodné rozhodnutí člověka žít podle svého.

(2) Ochrany požívají zejména život a důstojnost člověka, jeho zdraví a právo žít v příznivém životním prostředí, jeho vážnost, čest, soukromí a jeho projevy osobní povahy.

§ 82

(1) Člověk, jehož osobnost byla dotčena, má právo domáhat se toho, aby bylo od neoprávněného zásahu upuštěno nebo aby byl odstraněn jeho následek.

(2) Po smrti člověka se může ochrany jeho osobnosti domáhat kterákoli z osob jemu blízkých.

§ 83

(1) Souvisí-li neoprávněný zásah do osobnosti člověka s jeho činností v právnické osobě, může právo na ochranu jeho osobnosti uplatnit i tato právnická osoba; za jeho života však jen jeho jménem a s jeho souhlasem. Není-li člověk schopen projevit vůli pro nepřítomnost nebo pro neschopnost úsudku, není souhlasu třeba.

(2) Po smrti člověka se právnická osoba může domáhat, aby od neoprávněného zásahu bylo upuštěno a aby byly odstraněny jeho následky.

Pododdíl 2

Podoba a soukromí

§ 84

Zachytit jakýmkoli způsobem podobu člověka tak, aby podle zobrazení bylo možné určit jeho totožnost, je možné jen s jeho svolením.

§ 85

(1) Rozšiřovat podobu člověka je možné jen s jeho svolením.

(2) Svolí-li někdo k zobrazení své podoby za okolností, z nichž je zřejmé, že bude šířeno, platí, že svoluje i k jeho rozmnožování a rozšiřování obvyklým způsobem, jak je mohl vzhledem k okolnostem rozumně předpokládat.

§ 86

Nikdo nesmí zasáhnout do soukromí jiného, nemá-li k tomu zákonný důvod. Zejména nelze bez svolení člověka narušit jeho soukromé prostory, sledovat jeho soukromý život nebo pořizovat o tom zvukový nebo obrazový záznam, využívat takové či jiné záznamy pořízené o soukromém životě člověka třetí osobou, nebo takové záznamy o jeho soukromém životě šířit. Ve stejném rozsahu jsou chráněny i soukromé písemnosti osobní povahy.

§ 87

(1) Kdo svolil k použití písemnosti osobní povahy, podobizny nebo zvukového či obrazového záznamu týkajícího se člověka nebo jeho projevů osobní povahy, může svolení odvolat, třebaže je udělil na určitou dobu.

(2) Bylo-li svolení udělené na určitou dobu odvoláno, aniž to odůvodňuje podstatná změna okolností nebo jiný rozumný důvod, nahradí odvolávající škodu z toho vzniklou osobě, které svolení udělil.

§ 88

(1) Svolení není třeba, pokud se podobizna, písemnost osobní povahy nebo zvukový či obrazový záznam použijí na základě zákona k úřednímu účelu.

(2) Svolení není třeba ani v případě, když se podobizna nebo zvukový či obrazový záznam pořídí a použijí k výkonu nebo ochraně jiných práv nebo právem chráněných zájmů jiných osob.

§ 89

Podobizna nebo zvukový či obrazový záznam se mohou bez svolení člověka také pořídit nebo použít přiměřeným způsobem též k vědeckému nebo uměleckému účelu a pro tiskové, rozhlasové, televizní nebo obdobné zpravodajství.

§ 90

Zákonný důvod k zásahu do soukromí jiného nebo k použití jeho podobizny, písemnosti osobní povahy nebo zvukového či obrazového záznamu nesmí být využit způsobem zřejmě nepřiměřeným a nesmí být v rozporu s oprávněnými zájmy člověka.

Jak vidět, hned úvodní ustanovení § 81 NOZ v zásadě odpovídá ustanovení § 11 stávajícího občanského zákoníku. Odstavec 1 daného ustanovení NOZ tak stanoví generální klauzuli všeobecného osobnostního práva, kterou doplňuje demonstrativní výčet chráněných statků v odstavci 2 § 81 NOZ. Nový občanský zákoník pregnantněji stanoví ochranu podoby člověka a dalších záznamů týkajích se člověka nebo jeho projevů osobní povahy.

Ustanovení § 86 NOZ formou generální klauzule ve větě první vyslovuje obecný zákaz zásahů do soukromí člověka bez zákonného důvodu a ten je pak doplněn druhou a třetí větou o demonstrativní výčet zakázaných neoprávněných zásahů do soukromí; těmi jsou ve smyslu tohoto výčtu narušování soukromých prostorů člověka[90], sledování jeho soukromého života včetně pořizování zvukového nebo obrazového záznamu, využívání záznamů pořízených o soukromém životě člověka nebo písemností osobní povahy třetí osobou, popřípadě jejich šíření; obdobně jsou pak chráněny soukromé písemnosti osobní povahy.

Ustanovení § 87 NOZ nově legislativně upravuje podmínky udělení souhlasu k použití písemnosti osobní povahy, podobizny nebo zvukového či obrazového záznamu týkajícího se člověka nebo jeho projevů osobní povahy, když výslovně stanoví, že takovýto souhlas lze odvolat, a to i pokud byl udělen jak na na dobu neurčitou, tak i na dobu určitou – v druhém

[90] Zakazuje se narušit „soukromé prostory“, nikoli pouze „obydlí“ člověka, protože právo na soukromí zasahuje nejen místo, kde člověk bydlí, ale také místo, kde vykonává svou obvyklou profesi.

zmíněném případě je možné souhlas odvolat bez jakékoliv sankce jen pokud to odůvodňuje podstatná změna okolností nebo jiný rozumný důvod, jinak je nutné, aby osoba odvolávající souhlas nahradila škodu z toho vzniklou osobě, které svolení udělila.

Ochrana práva na podobiznu se mění ve dvou detailech. Předně se zakazuje jakékoliv neoprávněné zobrazení člověka, z něhož jej lze identifikovat. Dále se stanoví právní pravidlo, že souhlasem s vlastním vyobrazením člověk uděluje souhlas též k jeho obvyklému a s ohledem na okolnosti případu zároveň i pro něho předvídatelnému rozšíření podobizny. Tato dvě pravidla nebyla v předchozí právní úpravě obsažena.

Jak bylo již zmíněno výše, mění se úprava tzv. zpravodajské licence (ust. § 89 odst. 2 NOZ), která byla rozšířena o pojem „obdobné zpravodajství“, tudíž se dle NOZ vztahuje i na internetové zpravodajství.

Návrh nového občanského zákoníku ve svém § 82 odst. 1 ponechává v repertoáru právních prostředků ochrany osobnosti nároky zdržovací i odstraňovací, když stanoví, že *„člověk, jehož osobnost byla dotčena, má právo domáhat se toho, aby bylo od neoprávněného zásahu upuštěno nebo aby byl odstraněn jeho následek.“* V rámci nároku na poskytnutí zadostiučinění však stanoví jiné priority při poskytnutí satisfakce, když v § 2951 odst. 2 návrhu nového občanského zákoníku (zcela žádoucím způsobem) namísto priority satisfakce morální zakládá spíše prioritu satisfakce relutární (náhrada v penězích). Ten uvádí, že *„Nemajetková újma se odčiní přiměřeným zadostiučiněním. Zadostiučinění musí být poskytnuto v penězích, nezajistí-li jeho jiný způsob skutečné a dostatečně účinné odčinění způsobené újmy.“*

Pokud jde o otázku promlčení osobnostních práv, NOZ stanoví v ustanovení § 612, že v případě práva na život a důstojnost, jméno, zdraví, vážnost, čest, soukromí nebo obdobného osobního práva se promlčují jen práva na odčinění újmy způsobené na těchto právech.

Ustanovení § 83 pak nově upravuje otázku aktivní legitimace k uplatňování práva na ochranu osobnosti, respektive práva na soukromí. Souvisí-li neoprávněný zásah do osobnosti člověka s jeho činností v právnické osobě, může totiž podle nové právní úpravy právo na ochranu jeho osobnosti uplatnit i tato právnická osoba; za jeho života však jen jeho

jménem a s jeho souhlasem. Není-li člověk schopen projevit vůli pro nepřítomnost nebo pro neschopnost úsudku, není souhlasu třeba. Po smrti člověka se právnická osoba může domáhat, aby od neoprávněného zásahu bylo upuštěno a aby byly odstraněny jeho následky.

Po smrti člověka se může podle NOZ ochrany jeho osobnosti domáhat kterákoli z osob jemu blízkých, nikoliv tedy jako tomu bylo dosud, kdy se ochrany osobnosti zemřelého mohl domáhat pouze manžel nebo partner a děti, a nebylo-li jich, pak rodiče zemřelého.

Obecně lze považovat přijetí nového občanského zákoníku a jeho novou právní úpravu ochrany osobnosti a soukromí za krok dopředu, kdy se úprava přibližuje původním tezím platným na území českých zemí, které byly přerušeny nástupem komunistické totality k moci. Lze říci, že NOZ zesiluje a precizuje dosavadní práva spojená s osobností člověka. NOZ završuje úpravu ochrany osobnosti a soukromí na území našich zemí započatou kodexem ABGB a dále zákonem 40/1964 Sb. a jeho polistopadovou novelou.

3.2.6 Exkurz: Fotografie a obrazové záznamy podle autorského zákona

Jak již bylo v této práci shora zmíněno, obrazový záznam může být předmětem nejenom ochrany osobnosti podle občanského zákoníku, nýbrž i předmětem ochrany autorskoprávní. Z pohledu naší práce je i toto téma zajímavé, neboť pokud jde o ochranu soukromí, může být zajímavá duplicita ochrany určitého díla (fotografie), což může mít vliv i na zvýšený stupeň ochrany soukromí a těžší zneužitelnost daného díla. Každá fotografie, která splňuje znaky autorského díla, bude nepochybně chráněna i režimem autorského zákona

Pokud fotografie zachycuje podobu fyzické osoby, je samozřejmě nutné mít souhlas této dotčené osoby s pořízením fotografie. Z hlediska této práce nás zajímají zejména fotografie a obrazové záznamy, které zachycují

fyzické osoby, zejména u těchto snímků lze hovořit i o dopadu na ochranu soukromí fotografované osoby.[91]

Základní vymezení toho, co je to autorské dílo, na které se vztahuje autorskoprávní ochrana podle autorského zákona, nabízí ustanovení § 2 autorského zákona (zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů - autorský zákon). [92] Teorie v zásadě rozlišuje mezi třemi druhy fotografií, přičemž pouze první dva druhy splňují požadavky autorského zákona a požívají autorskoprávní ochrany. Tak lze hovořit o následujících druzích fotografií:

1) **Umělecké dílo fotografické** – fotografie, která je jedinečným, neopakovatelným výsledkem tvůrčí činnosti autora. Jde o umělecké dílo, objektivně způsobilé vnímání coby umění. Klasickým příkladem takového díla je unikátní fotografický portrét modelky v ateliéru, pořízený za užití aranžmá, stylizace, hry barev a stínů a dalších uměleckých postupů.

2) **Původní výtvor – fotografie** – tento druh fotografie není autorským dílem, neboť postrádá znak jedinečnosti (neopakovatelnosti) výtvoru. Splňuje však znak původnosti, jde o vlastní výtvor duševní činnosti a zákon stanoví pro tento druh fotografie zákonnou fikci díla tím, že jej považuje za autorské dílo. Příkladem tohoto druhu fotografie budou snímky pořízené turistou na jeho dovolené, či série

---

91 Byť je samozřejmě možné, že do sféry soukromého života může zasáhnout i fotografie nezobrazující lidskou bytost, ale například její soukromý byt, či jiné předměty a místa soukromé povahy.

92 Dané ustanovení mimo jiné deklaruje, že *„Předmětem práva autorského je dílo literární a jiné dílo umělecké a dílo vědecké, které je jedinečným výsledkem tvůrčí činnosti autora a je vyjádřeno v jakékoli objektivně vnímatelné podobě včetně podoby elektronické, trvale nebo dočasně, bez ohledu na jeho rozsah, účel nebo význam (dále jen "dílo"). Dílem je zejména dílo slovesné vyjádřené řečí nebo písmem, dílo hudební, dílo dramatické a dílo hudebně dramatické, dílo choreografické a dílo pantomimické,* ***dílo fotografické a dílo vyjádřené postupem podobným fotografii, dílo audiovizuální, jako je dílo kinematografické****……*
Za dílo se považuje též počítačový program, je-li původní v tom smyslu, že je autorovým vlastním duševním výtvorem. …… ***Fotografie a dílo vyjádřené postupem podobným fotografii, které jsou původní ve smyslu věty první, jsou chráněny jako dílo fotografické****.“*

reportážních fotografických snímků fotografa dokladující průběh určité události (otevření galerie apod.).

3) **Prostý fotografický záznam** – nejde ani o jedinečný výtvor, ani o původní výtvor. Často se bude jednat o fotografický snímek pořízený automatem (pasová fotografie z automatu), fotografická (xeroxová) kopie apod. Zákon tyto fotografie nechrání podle autorského zákona, nejde vůbec o autorské dílo a v tomto případě se neuplatní ani fikce autorského díla.

Pokud tedy půjde o jeden z prvních dvou případů, fotografie bude chráněna ve smyslu autorského zákona. Ustanovení § 12 odst. 1 autorského zákona stanoví, že jiná osoba než autor může autorské dílo užít bez oprávnění uděleného autorem pouze v případech stanovených tímto zákonem (pokud nepůjde o tzv. volné užití či zákonné licence).

Vedle fotografií (jednotlivých obrazových snímků) rozeznáváme i **obrazové záznamy** ve smyslu filmu. Z hlediska terminologie autorského zákona může jít o tzv. audiovizuální díla. Z našeho pohledu však půjde o autorská díla, resp. díla, na která se vztahuje autorskoprávní ochrana pouze tehdy, pokud půjde o díla tvůrčí, jedinečná. Audiovizuálním dílem není každé zachycení skutečnosti filmovou, televizní či jinou audiovizuální technikou - o dílo audiovizuální požívající autorskoprávní ochranu se pak nebude jednat v případě mechanických reportážních zachycení osobních, rodinných a obdobných událostí, jako např. svateb a už vůbec ne pak o zachycení skutečnosti automatizovaným kamerovým systémem. Může se však jednat o tzv. **zvukově obrazový záznam** a jeho výrobce má pak řadu práv, odvozených od práva autorského (terminologií autorského zákona jsou nazývána jako práva s autorským právem související). Zvukově obrazový záznam je dle definice uvedené v ustanovení § 79 autorského zákona *„záznam audiovizuálního díla nebo záznam jiné řady zaznamenaných, spolu souvisejících obrazů vyvolávajících dojem pohybu, ať již doprovázených zvukem, či nikoli, vnímatelných zrakem, a jsou-li doprovázeny zvukem, vnímatelných i sluchem.“* Výrobce zvukově obrazového záznamu pak má výlučné majetkové právo svůj zvukově obrazový záznam užít a udělit

jinému smlouvou oprávnění k výkonu tohoto práva; jiný může zvukově obrazový záznam užít bez udělení takového oprávnění pouze v případech stanovených tímto zákonem. I v případě práv výrobce zvukově obrazového záznamu se uplatní výjimky z ochrany dle autorského zákona (bezplatné licence, volné užití pro osobní potřebu, kdy účelem není dosažení přímého nebo nepřímého hospodářského nebo obchodního prospěchu atd.).

3.3 Použitelnost obrazového záznamu jako důkazu v řízení

Právní teorií i praxí často diskutovaný případ je použitelnost kamerových, zvukových a obdobných záznamů či snímků (fotografií) **jakožto důkazů** v soudním či jiném řízení. Nutno říci, že již řadu let se mezi odborníky, ale i mezi státními orgány aplikujícími platné právo, vede spor o to, zda lze v rámci řízení (trestního, civilního, správního – přestupkového) použít jako důkazu záznam zvukové či obrazové nahrávky, či obrazový snímek – fotografii. Daný spor není ani po letech zcela vyřešen. V dané věci se často rozlišuje mezi jednotlivými typy řízení, principy ovládající řízení trestní jsou odlišné od principů a pravidel převládajících v řízení civilním. V následujícím textu cituji často odbornou literaturu nebo judikaturu, která se vztahuje nikoliv přímo na obrazové záznamy či snímky, ale i na zvukové záznamy, jsem však toho názoru, že i tyto mohou být pro blízkost tématu a související problematiky přínosné, proto je zde výslovně uvádím.

Lze říci, že existuje již poněkud starší judikatura, která v rámci **občanského soudního řízení** v zásadě neumožňovala provedení důkazu záznamem, který byl pořízen nebo účastníkem opatřen v rozporu s obecně závaznými právními předpisy a jehož pořízením nebo opatřením došlo k porušení práv jiné fyzické nebo právnické osoby.[93] Oproti tomu lze dohledat například stále uznávaný a v komentářích uváděný dokonce ještě

[93] Viz rozhodnutí Nejvyššího soudu ČR ze dne 21.10.1998 sp. zn. 21 Cdo 1009/98 – v tomto případě byl navržen jako důkaz záznam telefonního hovoru, pořízený však bez vědomí druhé strany. Soud vyvodil, že: *Navrhne-li účastník občanského soudního řízení k prokázání svých tvrzení důkaz, který byl pořízen nebo účastníkem opatřen v rozporu s obecně závaznými právními předpisy a jehož pořízením nebo opatřením došlo k porušení práv jiné fyzické nebo právnické osoby, soud takový důkaz jako nepřípustný neprovede. Nepřípustným důkazem je proto i záznam telefonického rozhovoru, který byl takto pořízen bez vědomí hovořících osob.*

starší judikát Krajského soudu v Ostravě ze dne 15.4.1997, sp. zn. 23 C 3/97, který doslova uvádí: *„Jednání spočívající v pořizování záznamů projevů fyzické osoby osobní povahy za tím účelem, aby si jednající opatřil důkazy pro správní, soudní či jiné řízení,* ***porušuje právo na ochranu osobnosti fyzické osoby****. Ustanovení procesních předpisů o tom, že za důkaz mohou v řízení sloužit všechny prostředky, jimiž lze zjistit stav věci (např. § 125 OSŘ , § 34 odst. 1 SpŘ),* ***pouze umožňují provedení takových důkazů v řízení*** *před příslušným státním orgánem (vytvářejí tedy* ***zákonnou úřední licenci*** *k použití projevů fyzické osoby osobní povahy v důkazním řízení), ale nijak* ***nezbavují*** *toho, kdo je pořídil,* ***odpovědnosti za jejich neoprávněné pořízení****.“* Odůvodnění tohoto rozhodnutí budí dojem, že pořízení záznamů osobní povahy je sice porušením práva na ochranu osobnosti, nicméně takovéto záznamy, existují –li již, mohou být v řízení na základě zákonného zmocnění dle § 125 o.s.ř. použity.

Obdobně Vrchní soud v Praze v rozhodnutí ze dne 27.5.2003, sp. zn. 1 Co 62/2003 **připustil provedení důkazu diktafonovým záznamem pořízeným skrytým způsobem** v prostoru určeném pro veřejnost (šlo o audionahrávku diskriminačního odmítnutí romských hostů v restauraci). V odůvodnění soud mimo jiné uvedl, že ustanovení § 125 o.s.ř. nevylučuje provedení důkazu audiozáznamem, záznam se netýkal soukromí dotčených osob a navíc právo k hlasovému projevu není předmětem tohoto řízení.

Poměrně významné rozhodnutí Nejvyššího soudu ze dne 21.12.2004, sp. zn. 30 Co 1224/2004 pak **připustilo využití záznamů telefonních hovorů jako důkazu, předloženého jedním ze žalovaných jakožto účastníkem dané telefonní komunikace** (tento žalovaný byl příjemcem telefonního hovoru). Podle soudu je obecně známou skutečností, že telefonní přístroj bývá vybaven řadou technických funkcí, mimo jiné i nahráváním hovoru. Za této situace soud dovodil, že volající, který iniciuje hovor, je s možností jeho nahrání srozuměn a současně tak de facto konkludentně souhlasí i s možným pořízením zvukového záznamu tohoto telefonátu. Z důvodu existence tohoto souhlasu pak nejde o neoprávněný zásah do práv chráněných § 12 obč. zákoníku a nic nebrání

v občanskoprávním řízení provést důkaz takovýmto záznamem telefonního hovoru.[94]

Stejně tak část komentářové literatury usuzovala i stále usuzuje, že *pro závěr má – li být důkaz určitými prostředky proveden či nikoliv, nemůže být rozhodující, zda například zvukový záznam či obrazový snímek byly pořízeny či nabyty nezákonným způsobem, nýbrž to, zda jde o prostředky, které mohou v jednotlivém konkrétním případě podle jeho okolností sloužit ke zjištění skutečného stavu věci a vést v souladu s funkčností justice k věcně správnému výsledku, který by odpovídal požadavku spravedlivého procesu (§ 125 o.s.ř.).*[95]

Oproti výše uvedeným závěrům však platí pro civilní řízení novější rozhodnutí Ústavního soudu České republiky, který nevnáší do problematiky jasné světlo, nýbrž ji nadále komplikuje. V rozhodnutí I. ÚS 191/05 ze dne 13.09.2006 Ústavní soud nesouhlasí s tím, že „*provedení důkazu v občanském soudním řízení takovým záznamem telefonického hovoru - proti vůli jednoho z volajících - je odůvodněno zákonnou úřední licencí podle § 12 odst. 2 občanského zákoníku. Citované ustanovení totiž stanoví výjimku ze zásady, kdy je třeba svolení fyzické osoby k pořízení anebo k použití písemností osobní povahy, podobizny, obrazového snímku a zvukového záznamu. Svolení není třeba, použijí-li se písemnosti osobní povahy, podobizny, obrazové snímky nebo zvukové záznamy k účelům úředním na základě zákona (tzv. úřední licence). Za projev úřední licence však nelze považovat každé řízení nebo jednání před soudem či jiným orgánem státu, ale jen případy, které výslovně upravuje zákon. Takovým zákonem je trestní řád, který v této souvislosti upravuje odposlech a záznam telekomunikačního provozu v trestním řízení. Občanskoprávní předpisy nic podobného nestanoví*[96]*. Magnetofonový záznam telefonického hovoru*

---

[94] Rozsudek Nejvyššího soudu ČR sp. zn. 30 Co 1224/2004, jenž potvrdil rozsudek Vrchního soudu v Olomouci č.j. 1 Co 6/2003-255, byl publikován např. v Bulletinu advokacie č. 11-12/2005, str. 64-65.

[95] Viz např. JEHLIČKA, O. – ŠVESTKA, J. – ŠKÁROVÁ, M. a kol., str. 129, (cit. dříve) a zde uvedené odkazy na další publikace KNAPP, K. - ŠVESTKA, J.: Ochrana osobnosti podle československého občanského práva. 2. vydání. Praha: Panorama, nakladatelství a vydavatelství, 1989; KNAPP – ŠVESTKA – JEHLIČKA a kol.: Ochrana osobnosti podle občanského práva. 4 vydání. Praha: LINDE, 2004; HANDL, B. – RUBEŠ, J.: Občanský soudní řád. Komentář. Praha: Panorama, 1985.

[96] Zde si dovolím nesouhlasit a poukázat na absentující řádné odůvodnění těchto závěrů ze strany Ústavního soudu. V rámci trestního řízení se naopak používá argumentace

fyzických osob ***je záznam projevů osobní povahy hovořících osob a takový záznam může proto být použit (i jako důkaz v občanském soudním řízení) zásadně jen se svolením fyzické osoby, která byla účastníkem tohoto hovoru.*** *“* [97] Dle mého názoru je však zřejmé, že fyzická osoba obvykle svolení k užití nahrávky, která je v rozporu s jejími zájmy, nedá. To tedy znamená, že se fakticky podstatně ztěžuje možnost užití nahrávek, které budou obsahovat projevy osobní povahy v civilním řízení. Vzhledem k tomu, že obecné soudy v civilním řízení přebírají toto závazné stanovisko Ústavního soudu, lze hovořit o velmi ztížené možnosti uplatňování takovýchto důkazů v civilním řízení. Věřím však, že toto je pouze dočasný odklon a že spíše zvítězí názor, kdy budou civilní soudy poměřovat obě proti sobě stojící práva (právo na soukromí a právo na ochranu majetku, nerušeného výkonu jiných práv apod.) ve všech souvislostech.

V rámci **trestního řízení** pak z minulosti existuje poměrně vyčerpávající výkladové stanovisko Nejvyššího státního zástupce (Vykls 2/2004), ke sjednocení výkladu zákonů a jiných právních předpisů k použitelnosti magnetofonového záznamu rozhovoru jako důkazu v trestním řízení. Podle tohoto stanoviska platí, že **hlasový projev konkrétní osoby neurčený pro veřejnost je osobním projevem požívajícím ochrany soukromí** a jeho pořízení bez souhlasu osoby, o jejíž projev jde, orgány činnými v trestním řízení pro účely důkazního řízení je proto možné jedině na základě zákona a postupem, který je upraven trestním řádem (§ 158d odst. 2 popřípadě odst. 3 trestního řádu). Pokud jde o bez účasti státu pořízený záznam hlasového projevu druhé osoby bez jejího vědomí, posouzení otázky, zda je či není v daném případě použitelný jako důkaz v trestním řízení, bude vždy věcí konkrétního trestního řízení a situace, za níž má být uvedená informace užita (**jeho použitelnost nelze a priori vyloučit,**

---

povolující přípustnost nahrávek jako důkazů i mimo režim výslovné zákonné licence jako jsou odposlechy v trestním řádu – jako důkaz se použije prakticky cokoliv, běžně i nahrávky pořízené soukromými osobami.

97 Na citované rozhodnutí Ústavního soudu dále navazuje a rozvíjí jej i rozhodnutí Nejvyššího soudu České republiky sp.zn. 22 Cdo 4172/2007, ze dne 4.11.2008, kdy v zásadě konstatuje, že *„Pořízení záznamu vlastního telefonického hovoru není nezákonné, důkaz tímto záznamem lze ale v občanském soudním řízení provést jen se svolením fyzické osoby, která byla účastníkem tohoto hovoru.“* Je zajímavé, že Nejvyšší soud ČR dříve nicméně zastával stanovisko opačné a použití záznamu osobní povahy v důkazním řízení za projev úřední licence považoval – viz dříve citované rozhodnutí sp. zn. 30 Co 1224/2004.

může jím být však jen za podmínky, že zásah do soukromí je odůvodnitelný převažujícím zájmem na straně toho, kdo informaci opatřil a následně použil - samotný zájem na náležitém zjištění skutkového stavu věci však zásadně takovým převažujícím zájmem není). Nejvyšší státní zástupkyně dává rozhodujícím orgánům i jakýsi návod, který osobně považuji za poměrně použitelné vodítko a naznačení směru i pro orgány rozhodující v civilním nebo správním (přestupkovém) řízení – *„bude-li orgánům činným v trestním řízení nabídnuta nahrávka, pak bude jen na nich, aby posoudily, do jaké míry je využitelná, a to nejen z hlediska jejího obsahu, ale také – a to především - z pohledu obecných principů, které musí být v rámci trestního řízení dodrženy. Přitom budou přihlížet i k okolnostem, za nichž došlo k zachycení hlasového projevu, a nepochybně též zohlední fakt, pokud by zjevně došlo při takovém postupu k porušení zákona – např. pokud by bylo shledáno, že šlo zjevnou provokaci k protiprávnímu chování, o nahrávku záměrně upravovanou, o použití skrytě nahraného projevu osoby (která se posléze stala obviněným) v její neprospěch, tedy za situace, kterou by bylo možno označit za donucování k doznání nebo za obcházení zákona, nebo že by byly použity takto získané informace od osoby, které jinak zákon přiznává právo nevypovídat a která v průběhu řádného procesu toto právo ohledně takto získaných informací využila, atd.“*[98] Lze říci, že trestní soudy v zásadě obrazové a jiné záznamy projevů soukromé povahy připouštějí jako důkaz v řízení.

Pokud jde o konkrétní trestněprávní judikaturu, mohu zmínit např. usnesení Nejvyššího soudu ČR ze dne 3. 5. 2007, sp. zn. 5 Tdo 459/2007, ve

[98] Budou přihlížet k § 12 odst. 1 obč. zák. z hlediska, zda nejde o nezákonný, resp. přímo protizákonný postup, a v souladu se zásadami trestního řízení budou především posuzovat

- vztah obsahu takto získané informace k předmětu vlastního trestního řízení,
- postavení osoby, o nahrávku jejíhož hlasového projevu jde, v tomto řízení,
- postavení osoby, která nahrávku pořídila,
- okolnosti, za nichž byla nahrávka pořízena (včetně doby, místa a prostředků, které byly použity)
- účel, pro který byla nahrávka pořízena,
- důvody, které vedly jinou osobu k následnému použití nahrávky právě v této podobě (formě) v trestním řízení,
- vztah takto získaných informací k ostatním důkazním prostředkům a důkazům ve věci zjištěným a k tomu, proč je využití právě takto získaných informací v důkazním řízení nezbytné, včetně důvodů, proč nelze tytéž informace získat jiným právně relevantním postupem orgánů činných v trestním řízení.

kterém je konstatováno: *„s ohledem na ustanovení § 89 odst. 2 tr. ř. zásadně nelze vyloučit možnost, aby byl k důkazu použit i zvukový záznam, který byl pořízen soukromou osobou bez souhlasu osob, jejichž hlas je takto zaznamenán (...) Přípustnost takového důkazu je však nezbytné vždy posuzovat též s ohledem na respektování práva na soukromí zakotveného v čl. 8 Úmluvy o ochraně lidských práv a základních svobod a práva na nedotknutelnost osoby a jejího soukromí ve smyslu čl. 7 odst. 1 a čl. 10 odst. 2 Listiny základních práv a svobod".* Obdobně Nejvyšší soud ČR judikoval například v usneseních ze dne 23. 7. 2008, sp. zn. 5 Tdo 769/2008 a ze dne 25. 11. 2009, sp. zn. 3 Tdo 1340/2009.

V řízení správním pak obecně platí, že obrazové a obdobné záznamy jako důkaz v řízení nejsou v zásadě vyloučeny. Nejvyšší správní soud jako nejdůležitější hybatel závazných právních názorů v této oblasti naposledy ve svém rozhodnutí sp. zn. 2 As 45/2010 z 22.12.2011 se vyjadřoval k otázce, zda je záznam ze soukromého kamerového systému, umístěného na nemovitosti, přípustným důkazem ve správním řízení. Po důkladně zpracované argumentaci dospěl k závěru, že tomu tak za určitých okolností je, když odkazuje analogicky na praxi v trestní justici, která akceptuje použití (audio)vizuálních záznamů provedených soukromými osobami pro potřeby dokazování, nevybočí-li pořizovatel záznamu z limitů, které jsou spatřovány zejména v testu proporcionality. Soud tedy přípustnost použití nahrávky pořízené soukromou osobou v přestupkovém řízení nevyloučil.[99]

[99] V rozhodnutí je podrobněji zmíněno, že při posuzování přípustnosti nahrávky je nutno zkoumat, jestli pořízený záznam může vůbec zasáhnout sféru osobnostních práv natáčených lidí. Pokud je tato podmínka splněna, je třeba zároveň posoudit, zda do sféry osobnostních práv člověka bylo zasaženo ze zákona přípustných důvodů či nikoliv. I za situace, kdy byl sporný záznam pořízen v rozporu s předpisy chránícími soukromí, není ale nutně jeho použitelnost pro potřeby dokazování zcela vyloučena. V jednotlivých případech je podle NSS ovšem nutno vždy přísně individuálně uvážit o legitimitě cíle, kterého má být prostřednictvím provedení důkazu dosaženo. Jde tak nejen o posouzení konfliktu jednoho ze základních práv garantovaných ústavou, tedy práva na ochranu soukromí na straně jedné a zájmu společnosti na ochraně před deliktním jednáním, odhalení a potrestání takového jednání na straně druhé, ale především o konfrontaci práva na ochranu soukromí zaznamenané osoby s ústavně zaručenými právy osoby, která záznam pořídila. Například pro potřeby případně uplatňovaného nároku na náhradu škody způsobené protiprávním jednáním. – podrobnější informace dostupnié z vyjádření soudce zpravodaje a mluvčí NSS publikované na serveru Epravo – „Při řešení přestupků lze použít i kamery soukromých subjektů, řekl Nejvyšší správní soud" dostupné na adrese

Nelze taktéž nezmínit ani názor Veřejného ochránce práv – ten ve svém závěrečném stanovisku ve věci podnětu Mgr. E. a L. H., sp. zn. 5432/2009/VOP/IK uvádí následující: *„Domnívám se, že by do sféry soukromoprávní ochrany dle § 12 občanského zákoníku, který je zákonným vyjádřením ústavního práva na ochranu soukromí ve sféře soukromoprávní, mělo spadat především pořizování těch záznamů, jejichž primárním cílem je toto soukromí narušit. Asi není sporu o tom, že pokud někdo např. natočí jinou osobu ať už v intimní nebo běžné každodenní situaci a snímek následně bez jejího svolení rozešle nebo vyvěsí na internet či využije jiným způsobem (a nejedná se přitom o některou ze zákonných licencí zmíněných v ustanovení § 12 odst. 2 a 33 občanského zákoníku), potom jde jednoznačně o jednání, které by bylo namístě řešit podáním civilní žaloby na ochranu osobnosti. Pokud však někdo (např. na základě předchozích negativních zkušeností ať už s pachatelem přestupku, nebo s předchozím správním či trestním řízením, které bylo zastaveno z důvodu, že se nepodařilo obviněnému protiprávní jednání prokázat) pořídí záznam závadného jednání jiné osoby s cílem pořídit důkaz pro případné správní řízení (v jehož rámci jsou nařízená ústní jednání neveřejná, což je z hlediska ochrany soukromí věc nikoliv nepodstatná), dostáváme se tímto zjevně do oblasti práva veřejného. V té hraje dominantní úlohu při ochraně ústavního práva na soukromí zákon o ochraně osobních údajů, na jehož dodržování dohlíží Úřad na ochranu osobních údajů. .... Provozování kamerového systému je Úřadem dlouhodobě považováno za zpracování osobních údajů (pokud je zároveň prováděn záznam pořizovaných záběrů). ..... (Nejen) ve správním řízení je jako důkaz obecně přípustná a akceptovaná svědecká výpověď, která je považována za pravdivou, pokud není prokázán opak. ... Je však všeobecně známo, že taková svědecká výpověď je ryze subjektivním pohledem osoby, která ji podává. Jestliže tedy připouštíme dokazování skrze tyto, jak už bylo řečeno, poněkud subjektivní výpovědi aktérů a svědků incidentu, potom je dle mého soudu namístě se ptát, zdali by neměly být tím spíše připuštěny jako důkazy i zmíněné záznamy, které by mohly popisovanou realitu přiblížit přece jen objektivnějším způsobem.“*

---

http://www.epravo.cz/zpravodajstvi/pri-reseni-prestupku-lze-pouzit-i-kamery-soukromych-subjektu-rekl-nejvyssi-spravni-soud-79621.html [cit.2012-02-13].

Z výše uvedeného je patrné, že stále přesto neexistuje jednoznačný přístup soudů a jiných orgánů k otázce použitelnosti obrazových, zvukových a obdobných záznamů, pořízených bez souhlasu dotčené osoby. Dokonce ani zahraniční teorie a komentářová literatura nemá tuto otázku definitivně vyřešenu. Je to zřejmě logické, neboť i když existuje primární zájem společnosti na garantování práva na soukromí jednotlivců a práva na zákonný proces, v některých případech, a to zejména v občanském soudním řízení, přesto může výjimečně nastat situace, kdy se využití takovýchto záznamů (byť získaných někdy problematickým způsobem) jakožto důkazů jeví za širších souvislostí účelnější. Vždy bude nepochybně záležet na konkrétních okolnostech daného případu a rozhodnutí bude na příslušném soudu, který danou věc rozhoduje. Přesto využiji na tomto místě svého práva jakožto autora této práce uvést svůj názor. S výše uvedeným rozhodnutím Ústavního soudu I. ÚS 191/05 a na něj navazujícím rozhodnutím Nejvyššího soudu sp. zn. 22 Cdo 4172/2007 nesouhlasím. Dle mého soudu lze danou situaci řešit v každém jednotlivém případě podle zdravého rozumu a zásad obecné spravedlnosti. Vždy by měly být zvažovány veškeré okolnosti případu a okolnosti pořízení a následného použití dané nahrávky či fotografie jakožto důkazu sloužícího k prokázání důležitých skutečností pro dané řízení. Záznam bych obecně neodmítal jako nepřípustný, pokud s ním dotčená osoba nesouhlasí (ať již s jeho pořízením, nebo následným použitím). Je logické, že pokud se dotčené osobě záznam tzv. „nehodí“, souhlas neposkytne. V zájmu spravedlivého řešení by tak mělo být možné v odůvodněných případech nahradit souhlas dotčené osoby jinak. Bylo by patrně možné připustit použití záznamu, pokud dotčená osoba o pořízení nahrávky věděla a nijak proti ní neprotestovala a jednala s vědomím, že je o ní a jejím chování pořizován záznam (např. vědomě vstoupila do prostoru monitorovaného kamerou), stejně tak pokud mohla v rámci obvyklého stavu a chodu věcí předpokládat, že bude nahrávána. Obdobně nelze v určitých případech upřednostnit zájem dotčené osoby, která se evidentně dopustila porušení práv a dovolit, aby se dovolávala svých práv daných jí občanským zákoníkem a ustanoveními § 12 a násl.[100]

[100] V této souvislosti lze zmínit příklad za použití logického argumentu ad absurdum: v situaci, kdy se např. v pracovním právu prokazuje platnost či neplatnost výpovědi,

Vždy bude na rozhodujícím orgánu, aby posoudil naproti sobě stojící právo na ochranu soukromí (zájem na nepořízení nahrávky a jejím použití bez souhlasu dotčené osoby) a zájem společnosti a jednotlivců na ochraně majetku, soukromí, bezpečnosti a ochrany zdraví. Podle mého názoru, bude – li narušeno právo na jedné straně (vloupání do soukromého obytného domu), dotčený zloděj se pravděpodobně nemůže úspěšně dovolávat ochrany svého soukromí, tedy toho, že byl na cizím pozemku bez svého svolení „nahrán“ (a dovolávat se a argumentovat „nerušeným“ výkonem své činnosti, bez toho, aby při ní někdo zasahoval do jeho soukromí); zde musí být upřednostněn zájem majitele (obyvatele) domu na ochraně soukromí, majetku, jakož i zájem společnosti na pokojném občanském soužití. Právo dotčené osoby vyslovit souhlas či nesouhlas s pořízením záznamu projevu osobní povahy dle § 12 občanského zákoníku, nebo vyslovit souhlas s použitím takovéhoto záznamu jako důkazu nelze posuzovat samostatně bez ohledu na jiná ustanovení platného práva (právo nebýt rušen ve výkonu svých práv – například právo užívat pokojně svůj byt). Jiná věc by však bylo pořízení nahrávky jednáním, které by bylo za hranicí zákonem vymezených mantinelů, tedy například pořízení nahrávky účelové, zmanipulované, či neúplné, pouze pro výhru v daném sporu bez ohledu na skutečný stav věci (či nahrávky pořízené tajně pomocí speciální technologie například v soukromém bytě protistrany, kdy dotčená osoba nemůže předpokládat, že bude nahrávána; taktéž záznam dotčené osoby pořízený zcela bez ohledu na její soukromý a intimní život – např. intimní záběry z ložnice dotčené osoby atd.). Stejně tak je třeba přísněji posuzovat užití takovýchto nahrávek ze strany orgánů státní moci (trestní řízení); zde je nutno postupovat přísněji pouze v rámci zákonného vymezení, neboť možnost zneužití je tu obvykle vyšší.[101] Je nicméně pravda, že řada mnou uváděných příkladů a názorů

---

když by zaměstnanec odmítl použít jako důkaz dopis (výpověď) s odkazem na listovní tajemství, nelze na tento nesouhlas relevantně pohlížet a důkaz listinou nepřipustit neboť evidentně postačí, že alespoň jeden účastník dané komunikace, daného chování souhlas poskytne.

101 Viz také anglosaská doktrína tzv. ovoce z otráveného stromu (fruits of poisons tree doctrine), kdy rozhodnutí soudu v trestním řízeni se nesmí zakládat na důkazech získaných nezákonným způsobem, jakož i na důkazech,. které byly získány na základě informací, získaných protiprávně – blíže viz *Silverthorne Lumber Co. v. United States, 251 U.S. 385 (1920)*, rozhodnutí dostupné např. online na: http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?court=us&vol=251&invol=385

spadá spíše do oblasti práva trestního či přestupkového, kde je použití audiovizuálních nahrávek rozhodujícími orgány vnímáno benevolentněji. Naproti tomu v civilním řízení jsou soudy přísnější a záznamy projevů osobní povahy bez souhlasu dotčené osoby jako důkaz v řízení nepřipouští. Je však otázkou, proč v rámci trestního řízení platí odlišná pravidla důkazního řízení, když jednak trestní či přestupkové řízení často může souviset s civilními delikty, kterými také může být způsobena značná škoda, stejně tak není dle mého soudu přesvědčivě zdůvodněno teorií ani praxí, proč je v trestním řízení aplikován zcela jiný přístup než v civilním procesu. Budoucnost ukáže, zda daná problematika může být vyřešena výslovnou normativní úpravou. Pokud tomu tak není, podle mého názoru by mělo být postupováno se zdravým rozumem, proto v zásadě v řízení důkaz nahrávkou pořízenou bez souhlasu dotčené osoby neodmítat, zvlášť pokud toto užití projde testem proporcionality, a nepoužít ji pouze v krajních případech jasného překročení zásad proporcionality a přiměřenosti, to vše i v rámci civilního procesu.[102]

Pro větší využívání důkazů, byť pořízených nezákonně v rozporu s ustanovením § 12 občanského zákoníku, se vyjadřuje i např. komentář občanského zákoníku nakladatelství C.H.BECK při výkladu vztahujícím se k ustanovení § 12 občanského zákoníku pojednávajícímu zejména o zákonné licenci k pořízení nebo použití písemností osobní povahy, podobizen, obrazových snímků a obrazových a zvukových záznamů.[103] Daný komentář v zásadě deklaruje, že pro úvahu soudu, zda má být navržený důkaz proveden či nikoliv, nemůže být rozhodující, zda byly podobizny či obrazové snímky pořízeny nebo nabyty zákonným či nezákonným způsobem. V tomto směru rozhodujícím může být jedině to, zda jde o prostředky, které mohou sloužit k objasnění věci (§ 125 o.s.ř.) a

---

[cit. 2012-02-13].

[102] K tématu dále např. práci Protiprávně získané nebo použité důkazy v civilním soudním řízení autora Jana Seidela, dostupný na https://is.muni.cz/www/210560/pfo-nd.pdf [cit. 2012-02-13], kde mimo jiné autor uvádí argumentaci používanou německými soudy, tedy, že „Zda je zásah do základního práva oprávněný, se řídí výsledkem úvahy mezi použitím odporujícími osobnostními právy na jedné straně a pro použití mluvícím právním zájmem na druhé straně.“ – což je de facto užití principu proporcionality.

[103] Viz publikace Švestka, Spáčil, Škárová, Hulmák a kol. Občanský zákoník I. § 1 až 459. Komentář. 2. Vydání. Praha: C.H.BECK, 2009.

tak přispět k naplnění požadavku spravedlivého procesu. Otázka jejich pořízení nebo nabytí je samostatnou věcí občanskoprávní odpovědnosti toho, kdo je nezákonně pořídil či nabyl. Použití podobizen a obrazových snímků v rámci civilního řízení je zákonnou licencí dle § 12 obč. zákoníku kryto pouze potud, pokud má k předmětu řízení skutečně příčinný vztah (nebylo by tak možno považovat za oprávněné použití fotografií předložených jedním účastníkem výhradně za účelem skandalizace druhého účastníka, ačkoliv k předmětu dokazování nemají žádný přímý vztah). Použitím pak nesmí být nikdy zasaženo do všeobecných osobnostních práv ve větší míře, než je nezbytné pro dosažení účelu, pro který byla licence stanovena. V citovaném komentáři autoři zmiňují i J. Telce, který na příkladu domácího násilí dovozuje, že jestliže věrohodně působící oběť domácího násilí pořídila o násilí důkaz skrytou kamerou, který je ve věci jediným důkazem, jímž by se oběť mohla domoci s úspěchem své ochrany, měl by být s ohledem na požadavek spravedlivého procesu takový důkaz připuštěn a vzat v úvahu při hodnocení celého případu.

Ivo Telec je toho názoru, že ačkoli se v případě připuštění nezákonně získaného důkazu (bez svolení dotčené osoby) jedná o neoprávněný zásah do práva osobnostního, je nutno situaci posoudit kontextuálně. Nikoli tedy tak, že by jedna stránka nastalé životní situace byla odtržena od stránek ostatních. Tzn. i v jejím významu z hlediska subjektivního lidského práva na spravedlivý proces, které se zde střetává s právem osobnostním. Srov. čl. 6 Úmluvy o ochraně lidských práv a základních svobod z roku 1950, resp. čl. 36 a násl. Listiny. Právo na spravedlivý proces má každý účastník procesu. Svědčí proto i navrhovateli důkazu, který by nepřipuštěním a neprovedením důkazu mohl být krácen (postižen) na právu a mohl by se stát obětí porušení svého práva na spravedlivý proces. Nepřipuštění důkazu patří mezi skutky, které mohou zavdat porušení práva na spravedlivý proces. Podobné případy, které se týkají jemného vycítění spravedlnosti, je nutno právně řešit s ohledem na jejich konkrétní okolnosti. ***Nástrojem k dosažení řešení může být test poměrnosti cíle a prostředku.***[104]

[104] Viz Ivo Telec: Svolení, nebo zákonné licence v právu osobnostním, Právní rozhledy 24/2007

Osobně se k tomuto výkladu připojuji a jsem toho názoru, že samozřejmě s výjimkou nezákonně získaných důkazů orgány veřejné moci (tedy tam, kde není dána rovnost účastníků), by soudy v rámci civilního řízení neměly obecně důkaz pořízený i bez souhlasu či bez vědomí dotčené osoby odmítat, **vždy by však podle mého názoru měly použití konkrétního důkazu poměřovat testem proporcionality a zkoumat odůvodněnost zásahu do soukromí jednotlivce při pořízení důkazu.** Dovedu si tak představit odmítnutí provedení důkazu například v pracovněprávním sporu, ve kterém zaměstnavatel ve větším rozsahu podrobil zaměstnance skrytému sledování i jeho soukromých aktivit, při kterém sice zjistil zaměstnancovo nelegální chování, nicméně ve větší míře porušil jeho osobnostní práva a zaměstnancem očekávané právo na soukromí – vždy však bude záležet na konkrétní situaci.

Trefně shrnul aktuální postřehy z dané problematiky ve svém článku Použitelnost zvukových a obrazových záznamů jako důkazu z roku 2010 Jan Potměšil, když uvedl následující shrnutí, se kterým souhlasím a ztotožňuji se i s názorem autora na problematiku použitelnosti záznamů v případě kladného vyhodnocení testu proporcionality:

*„V **civilních věcech** soudy důkazy nahrávkou v zásadě odmítají, někdy však platnou úpravu zásahů do osobnostních práv vykládají restriktivně a nahrávku připustí, např. jde-li o záznam služebních nebo pracovních hovorů. V **trestních věcech** soudy nahrávky spíše připouštějí, nebyla-li porušena procesní pravidla ze strany státu, nebo pokud zásah do soukromí byl přiměřený vzhledem k okolnostem věci nebo ve srovnání se zájmem na prokázání, potrestání a prevenci trestných činů. **Ústavní soud v civilních věcech** připuštění nahrávky považuje za zásah do soukromí, v **trestních věcech** je však nevylučuje s ohledem na „nezbytnost danou obecným zájmem na ochraně společnosti před trestnými činy a na tom, aby takové činy byly zjištěny a potrestány“. **Nejvyšší správní soud** bude v oblasti správního řízení pravděpodobně následovat trestní judikaturu, neboť přísně rozlišuje mezi nahrávkami pořízenými státem na jedné straně, a soukromými osobami na straně druhé, kdy použitelnost soukromě pořízených nahrávek nevylučuje. **Veřejný ochránce práv (ombudsman)** považuje nahrávky ve správním, resp. přestupkovém řízení za přípustné, převažuje-li zájem na*

ochraně zájmů chráněných zákonem nad právem pachatele na soukromí. ***Autor*** *považuje nahrávky za přípustné zejména za podmínky kladného výsledku „testu proporcionality" a zohlednění konkrétních okolností věci."*[105]

3.4 Obrazové sledování v trestním řízení a u bezpečnostních složek

Bezpečnostní složky každého státu běžně mívají právně zakotvený režim legálního využívání sofistikovaných metod sledování osob a věcí, jakož i institut odposlechu a záznamu telekomunikačního provozu. Pro potřeby této práce, kdy se zabývám zejména obrazovým záznamem, nás bude zajímat zejména institut sledování osob a věcí.

Sledování osob a věcí jakožto jeden z operativně pátracích prostředků policejního orgánu je nutno odlišit od jiného trestněprávního institutu, kterým je odposlech a záznam telekomunikačního provozu podle ustanovení § 88 a § 88a trestního řádu. Sledování osob a věcí upravuje § 158d trestního řádu. Vedle dalších kriminalistických metod a prostředků (dalekohledy, noktovizory, rentgeny, kamery atd.) je zde uvažováno i o tzv. prostorovém odposlechu, který umožňují technická zařízení, mikrofony, záznamníky atd. umístěná v prostoru. Podle § 158d trestního řádu však nelze provádět odposlech telefonu či telekomunikačního provozu vůbec (toto je pro potřeby trestního řízení upraveno právě v § 88, resp. § 88a tr. řádu).

Dále je nutno zmínit **použití zpravodajské techniky** podle ustanovení § 8 odst. 1 písm. c) zákona č. 154/1994 Sb. o Bezpečnostní informační službě a podle ustanovení § 8 odst. 1 písm. c) zákona č. 289/2005 o Vojenském zpravodajství (v obou případech se zpravodajská technika používá pro nás v nejzajímavějším případě - při pořizování obrazových, zvukových nebo jiných záznamů). Podle příslušných zákonů, které mimochodem používají prakticky shodné vymezení, je jak BIS, tak i Vojenské zpravodajství, oprávněno v oboru své působnosti používat zpravodajské prostředky, kterými je vedle krycích prostředků, krycích

[105] Viz článek Jana Potměšila - Použitelnost zvukových a obrazových záznamů jako důkazu; dostupný na http://www.mvcr.cz/soubor/spravni-pravo-3-10web-potmesil-pdf.aspx [online], [cit.2011-11-18].

dokladů a sledování i zpravodajská technika. Zpravodajskou technikou se pak rozumí technické prostředky a zařízení, zejména elektronické, fototechnické, chemické, fyzikálně-chemické, radiotechnické, optické, mechanické anebo jejich soubory, používané utajovaným způsobem, pokud je při něm zasahováno do základních práv a svobod občanů mimo jiné i při odposlouchávání, popřípadě zaznamenávání telekomunikačního, radiokomunikačního a jiného obdobného provozu, popřípadě zjišťování údajů o tomto provozu.[106]

Další příbuzná problematika je pak vymezena **v celním zákoně a v zákoně o Vězeňské službě a justiční stráži České republiky**. Ustanovení § 37a celního zákona (zákon č. 13/1993 Sb.) stanoví, že celní orgány jsou pro plnění úkolů vyplývajících z mezinárodních smluv oprávněny používat operativně pátrací prostředky stanovené trestním řádem při provádění dohledu nad osobami, o kterých existují závažné důvody domnívat se, že porušují nebo porušily celní předpisy druhé smluvní strany. [107] Operativně pátrací prostředky pak mohou být použity pouze tehdy, jestliže by porušení právních předpisů, jejichž prováděním jsou celní orgány pověřeny, v případě, že by k němu došlo v tuzemsku, bylo posuzováno podle trestního zákona jako úmyslný trestný čin. Zákon č. 555/1992 Sb. o Vězeňské službě a justiční stráži České republiky (§ 16 - § 21) pak dává další zákonné zmocnění pro použití operativně pátracích prostředků. Operativně pátrací prostředky a podpůrné operativně pátrací prostředky podle tohoto zákona používají v objektech Vězeňské služby na žádost ministra nebo s jeho souhlasem orgány k tomu oprávněné podle § 158b trestního řádu. Podpůrné operativně pátrací prostředky pak mohou použít v objektech Vězeňské služby k předcházení a odhalování trestné činnosti přímo pověřené orgány Vězeňské služby. Podpůrnými operativně pátracími prostředky jsou zabezpečovací technika [108] a zvláštní finanční prostředky. Použitím

---

[106] Viz ustanovení § 8 zákona č. 154/1994 Sb. a stejné ustanovení § 8 zákona č. 289/2005 Sb.

[107] Dle zákonné poznámky pod čarou se těmito operativně pátracími prostředky myslí operativně pátrací prostředky podle §§ 158b-f tr. řádu.

[108] Zabezpečovací technikou se rozumí technické prostředky, zařízení a jejich soubory používané za účelem předcházení nebo zamezení ohrožení života a zdraví osob nebo k zabezpečení ochrany majetku a vyhledávání radiotelekomunikační techniky v objektech vazebních věznic a věznic a zabránění nedovolené komunikace osob ve výkonu vazby a ve výkonu trestu odnětí svobody.

zabezpečovací techniky nesmí být zasahováno do ústavně zaručených práv a svobod.

V dalším textu proberu jednotlivé instituty tzv. operativně pátracích prostředků a tzv. podpůrných operativně pátracích prostředků podrobněji. Bezpečnostní orgány mají samozřejmě i řadu jiných oprávnění, například využívat data a osobní údaje z nejrůznějších registrů, zmiňovat je a popisovat by však bylo s ohledem na vymezení tématu této práce nadbytečné.

3.4.1 Operativně pátrací prostředky

3.4.1.1 Sledování osob a věcí dle § 158d trestního řádu

Operativně pátrací prostředky je policejní orgán oprávněn používat v rámci trestního řízení o úmyslném trestném činu. Institut je v právním řádu České republiky upraven v zákoně č. 141/1961 Sb. o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.[109] Podle ustanovení § 158b trestního řádu se pak rozlišují následující druhy operativně pátracích prostředků:

a) předstíraný převod,
b) sledování osob a věcí,
c) použití agenta.

Oprávnění k použití operativně pátracích prostředků má pouze policejní orgán, pokud k tomu byl pověřen příslušným ministrem, v případě, že jde o útvar Policie České republiky pak policejním prezidentem, jde-li o útvar Bezpečnostní informační služby, jejím ředitelem, a jde-li o útvar Úřadu pro zahraniční styky a informace, pak má oprávnění k použití

[109] Institut operativně pátracích prostředků upravovaly nejprve §§ 33-37 zákona o Policii České republiky. Novela trestního řádu provedená zákonem č. 265/2001 Sb. vypustila úpravu operativně pátracích prostředků ze zákona o Policii ČR a nově jej zařadila do hlavy deváté (Postup před zahájením trestního stíhání), konkrétně do §§ 158b – 158f trestního řádu.

operativně pátracích prostředků policejní orgán, pokud byl k tomu pověřen ředitelem Úřadu pro zahraniční styky a informace.

Je třeba se zmínit o tom, že zákon striktně určuje, že používání operativně pátracích prostředků nesmí sledovat jiný zájem než **získání skutečností důležitých pro trestní řízení**. Operativně pátrací prostředky je přitom možné použít jen tehdy, nelze-li sledovaného účelu dosáhnout jinak nebo bylo-li by jinak jeho dosažení podstatně ztížené. Práva a svobody osob lze omezit jen v míře nezbytně nutné. Uplatňují se zde tedy zásady subsidiarity, přiměřenosti a zdrženlivosti.

Operativně pátrací prostředky neslouží samy o sobě jako důkazní prostředek v trestním řízení ve smyslu ustanovení § 89 a násl. trestního řádu.

Stejně tak ani operativně pátrací prostředky nejsou vyšetřovacími úkony podle § 165 odst. tr. řádu a nepřipadá tak v úvahu účast obhájce při jejich použití, a to ani v případě, že jsou nasazeny až po zahájení trestního stíhání ve smyslu § 158f tr. řádu. Při použití operativně pátracích prostředků mohou nicméně být pořízeny (a děje se tak zpravidla) **zvukové, obrazové či jiné záznamy**. Pokud byly tyto záznamy pořízeny způsobem, který odpovídá daným ustanovením trestního řádu, tyto již lze jako důkaz v trestním řízení použít. Jakmile se s těmito záznamy nakládá jako s důkazem, jsou součástí spisu a obviněný a jeho obhájce se s nimi mohou samozřejmě seznamovat.

Co se týká stadia trestního řízení, v jehož rámci jsou operativně pátrací prostředky využívány, je možné se s nimi setkat jak v přípravném řízení (a to ve fázi před zahájením trestního stíhání i po něm), tak i v řízení před soudem. Po podání obžaloby v řízení před soudem o použití operativně pátracích prostředků rozhoduje předseda senátu (výjimečně i samosoudce) soudu prvního stupně i bez návrhu státního zástupce.[110]

Pro naše účely je nejzajímavější institut **sledování osob a věcí**, který v trestním řádu blíže upravuje § 158d. Tím se podle trestního řádu rozumí *získávání poznatků o osobách a věcech prováděné utajovaným způsobem technickými nebo jinými prostředky.*

[110] Srovnej § 158f trestního řádu.

Technickými prostředky se zde rozumí podle komentáře k trestnímu řádu *všechny prostředky, které umožňují sledování osob a věcí na dálku (tedy od klasického dalekohledu přes přístroje využívající infračerveného, rentgenového i jiného záření až po přístroje umožňující vidění v noci, tzv. noktovizory atd.), prostorové odposlechy i přístroje ke zjišťování obsahu písemností, zásilek i jiných záznamů, zpravidla bez porušení jejich uzavření apod.* Jinými prostředky se pak rozumí *zejména klasické sledování, kdy pověřený policejní orgán sleduje fyzicky – vlastním pozorováním – pohyb a komunikaci osoby nebo pohyb věci a nakládání s ní konkrétními osobami.* [111] Nelze smysluplně podat vyčerpávající výčet všech v úvahu připadajících prostředků a metod použitelných při sledování osob a věcí. Technický vývoj jde velmi rychle kupředu, a proto se neustále objevují dokonalejší a výkonnější sledovací prostředky a systémy. Policejní orgány jsou vedle osobních sledovacích pomůcek vybaveny samozřejmě i propracovanými systémy umožňujícími technicky velmi pokročilé sledování například i skrz pevné objekty. Některé vrtulníky české policie jsou vybaveny např. infračervenými kamerami tzv. systému FLIR (Forward Looking Infra-Red), jsou využívány rentgenové detektory, různé zvukové monitorovací prostředky atd.[112]

---

[111] Viz komentář k trestnímu řádu ŠÁMAL, K. - KRÁL, V. - BAXA, J. a kol.: Trestní řád. Komentář. I. a II. Díl. 5. vydání. Praha: C. H. Beck, 2005

[112] K otázce invaze do soukromí pomocí technických prostředků jako jsou např. policejní infrakamery se zajímavě již v minulosti vyjadřoval např. Nejvyšší soud USA ve svém rozhodnutí Kyllo vs. US z 11.6.2001 (Kyllo v. United States, 533 U.S. 27 (2001), No. 99-8508). V daném případě byla při vyšetřování pana Kylla, podezřelého z pěstování marihuany, použita detektivem bez řádného soudního příkazu (warrant) infrakamera, namířená na dům pana Kylla, která odhalila zdroje velkého tepla používané pro pěstování této drogy. Nejvyšší soud USA oproti názoru nižších soudů dovodil, že sledování soukromého domu pomocí infra snímků (Thermovision imaging) bylo protiústavní, neboť je nutno jej uvažovat ve světle čtvrtého dodatku Ústavy, který zaručuje lidem právo na ochranu svobody osobní, domovní, písemností a majetku, které může být narušeno jen na základě předem vydaného řádného soudního příkazu (search warrant). Rozhodnutí je velmi významné, neboť rozvíjí Čtvrtý dodatek americké Ústavy i v novodobé éře moderních sledovacích technologií, které mohou výrazně zasahovat do soukromí občanů, kdy stanoví základní mantinely používání těchto technologií a prostředků orgány státní moci. K problematice se vyjadřoval i kanadský Nejvyšší soud ve svém rozhodnutí z roku 2004 ve věci R. v. Tessling (2004 SCC 67), kdy **naopak** usoudil, že člověk nemůže důvodně očekávat dostatečné soukromí při vyzařování tělesného a jiného tepla ven z domu a rozhodl, že přelety vrtulníku vybaveného infrazařízením nad domem a sledování pomocí kamery FLIR neporušují ústavní právo na ochranu před neodůvodněnými prohlídkami a zatčením (right to be free from unreasonable search and seizure). Při argumentaci o zásahu do soukromí musí totiž být brána v úvahu povaha a charakter samotných infra snímků a zejména míra informací o soukromí a intimní sféře jednotlivce, které z nich lze při

Sledování osob a věcí je možné rozdělit do tří základních typů[113]:

a) *obecné sledování osob a věcí*
b) *sledování osob a věcí, při kterém jsou pořizovány zvukové, obrazové nebo jiné záznamy*
c) *sledování osob a věcí, které zasahuje do nedotknutelnosti obydlí, do listovního tajemství nebo při kterém je zjišťován obsah jiných písemností a záznamů uchovávaných v soukromí za použití technických prostředků.*

Ad a)

Při obecném sledování osob a věcí **nejsou pořizovány zvukové, obrazové nebo jiné záznamy** a ani při něm **nejde o zásah do ústavně garantovaných práv občanů**. Zákon tedy nestanoví pro jeho použití tak přísné podmínky jako u ostatních dvou typů. Pověřený policejní orgán nepotřebuje k jeho použití žádné povolení. Tento druh sledování je opravdu určen především pro operativní a základní pátrací činnost, kdy budou především zjišťovány údaje a skutečnosti významné pro další postup a směr pátrání policejních orgánů. Nebudou pořizovány žádné záznamy ve smyslu důkazních prostředků (v úvahu by připadal maximálně výslech osoby (policisty), která prováděla sledovací činnost a mohla by se jako přímý

---

jejich kvalitě získat (obdobný názor jako konečné rozhodnutí kanadského soudu měl však ve svém disentu i americký soudce John Paul Stevens ve shora zmiňované kauze Kyllo v. US).
K zásahům do soukromí ze strany orgánů veřejné moci v USA viz blíže kupříkladu COOLBRIDGE, T.: Kyllo v. United States: Technology Versus Individual Privacy - Fourth Amendment case. In: FBI Law Enforcement Bulletin. Washington: Federal Bureau of Investigation, October 2001, ISSN-0014-5688

[113] Toto rozdělení používá komentář k trestnímu řádu autorů ŠÁMAL, K. - KRÁL, V. - BAXA, J. a kol. (citováno dříve), naopak publikace CÍSAŘOVÁ, D. a kol.: Trestní právo procesní. 2. vydání. Praha: LINDE, 2002 rozlišuje druhy sledování osob a věcí podle toho, zda je při nich pořizován záznam o průběhu úkonu (to by byly dva první typy sledování) nebo zda je nutno o úkonu sledování osob a věci sepsat protokol (případ ad c)). Autoři této publikace dokonce polemizují s otázkou, zda prosté vizuální sledování bez pořizování obrazového záznamu bude možné považovat za sledování spadající do režimu § 158 odst. 2 tr. řádu. Podle učebnice JELÍNEK, J. a kol.: Trestní právo procesní. 4. aktualizované vydání. Praha: EUROLEX BOHEMIA, 2005 je pak sledování osob a věcí ve smyslu § 158d tr. řádu dělitelné na sledování, při kterém je pořizován obrazový, zvukový a jiný záznam a na sledování, kterým má být zasahováno do některých základních lidských práv a svobod.

svědek vyjádřit do protokolu k určitým skutečnostem). Policejní orgán o proběhlém sledování učiní pouze úřední záznam.

Ad b)

Při použití druhého typu sledování osob a věcí **jsou pořizovány zvukové, obrazové nebo jiné záznamy**. Pro tento způsob sledování vyžaduje § 158d odstavec 2 tr. řádu písemné povolení státního zástupce. Pokud má být zvukový, obrazový nebo jiný záznam pořízený při sledování použit jako důkaz, je třeba k němu připojit protokol s veškerými náležitostmi dle § 55 a 55a tr. řádu. Zákon umožňuje použití záznamu pořízeného při sledování a připojeného protokolu jako důkazu i v jiné trestní věci, než je ta, v níž bylo sledování s pořízením zvukového, obrazového či jiného záznamu provedeno. Může se tak stát nicméně pouze tehdy, je-li i v této jiné věci vedeno řízení o úmyslném trestném činu, nebo pokud s tím souhlasí osoba, do jejíž práv a svobod bylo sledováním zasahováno.

V návaznosti na znění odstavce 5 citovaného paragrafu pak lze vyvodit, že nesnese-li věc odkladu a současně se nejedná o třetí typ sledování (viz shora ad c/), lze sledování zahájit i bez povolení. V takovém případě je však policejní orgán povinen o povolení bezodkladně dodatečně požádat, a pokud je do 48 hodin neobdrží, je povinen sledování ukončit, případný záznam zničit a informace, které se v této souvislosti dozvěděl, nijak nepoužít. O věc, která nesnese odkladu, se bude jednat, pokud hrozí, že by v mezidobí opatřování povolení byl již účel sledování zmařen nebo by již sledování nebylo fakticky uskutečnitelné.

Ad c)

Z hlediska ústavně zaručených práv a svobod týkajících se zejména soukromí jednotlivce je pak nejvýznamnější třetí typ sledování osob a věcí, při kterém dochází k odůvodněným zásahům do práva na nedotknutelnost obydlí a práva na listovní tajemství a tajemství jiných písemností a záznamů uchovávaných v soukromí.

Ustanovení § 158d odst. 4 tr. řádu stanoví bližší náležitosti procesu udílení povolení státním zástupcem či soudcem. To lze vydat jen na základě písemné žádosti. Žádost musí být přitom odůvodněna podezřením na

konkrétní trestnou činnost a, jsou-li známy, též údaji o osobách či věcech, které mají být sledovány. V povolení pak musí být stanovena doba, po kterou bude sledování prováděno s tím, že tato doba nesmí být delší než šest měsíců. Tuto dobu může však ten, kdo sledování povolil, na základě nové žádosti písemně prodloužit, a to vždy na dobu nejvýše šesti měsíců.

Podle trestního řádu existuje možnost pro použití sledování osob či věcí bez řádného povolení státního zástupce či soudce u těch typů sledování, kdy je toto povolení jinak vyžadováno. Sledování lze tak totiž provést bez patřičných povolení, pokud s tím výslovně souhlasí ten, do jehož práv a svobod má být sledováním zasahováno. Pokud je však takový souhlas dodatečně odvolán, sledování se neprodleně zastaví.[114]

Při sledování osob a věcí může pověřený policejní orgán potřebovat aktivní pomoc či spolupráci od jiných subjektů. Pro tento případ ustanovení § 158d odst. 9 tr. řádu zakotvuje povinnost provozovatelů telekomunikační činnosti, jejich zaměstnanců a jiných osob, které se na provozování telekomunikační činnosti podílejí, jakož i pošty nebo osoby provádějící dopravu zásilek, bezúplatně poskytovat policejnímu orgánu provádějícímu sledování podle jeho pokynů nezbytnou **součinnost**. Tyto subjekty se přitom nemohou dovolávat povinnosti mlčenlivosti stanovené zvláštními zákony.[115] Dané ustanovení opět nemá suplovat a nahrazovat jiné procesní instituty trestního práva, nýbrž slouží jako jakási příprava a získání potřebných údajů pro následné nařízení zadržení, záměny či sledování zásilky nebo pro nařízení odposlechu atd.

---

[114] Ustanovení § 158d odst. 6 doslova stanoví, že sledování lze provést bez splnění podmínek podle odstavce 2 a 3, přičemž však odstavec 3 krom nutnosti povolení soudce zakazuje výslovně i provádění jiných úkonů než takových, které směřují k umístění technických prostředků. Je tedy nicméně přinejmenším sporné, zda by i v případě souhlasu dotčené osoby se sledováním mohly být současně provedeny i jiné úkony - např. úkony domovní prohlídky. Domnívám se, že spíše nikoliv, neboť sám institut domovní prohlídky dle § 82 a násl. tr. řádu nepřipouští možnost dobrovolného souhlasu s ní, vždy je nutný příkaz soudce.

[115] Podobné ustanovení existuje v zákoně o Policii ČR. Dle jeho § 47a odst. 3 je policie oprávněna při sledování osob a věcí žádat v rozsahu potřebném pro plnění konkrétního úkolu policie od právnických a fyzických osob, které zajišťují telekomunikační činnost, předávání dat souvisejících s poskytováním telekomunikační služby způsobem umožňujícím dálkový a nepřetržitý přístup. Právnické a fyzické osoby, které zajišťují telekomunikační činnost, jsou povinny žádosti policie bez zbytečného odkladu vyhovět ve vyžádané formě a v rozsahu stanoveném zvláštním zákonem. Zde se však nejedná o sledování osob a věcí v rámci trestního řízení, nýbrž o sledování většinou ještě před zahájením úkonů trestního řízení či o sledování osob a věcí při plnění jiných úkonů Policie ČR.

V případě, že při sledování nebyly zjištěny žádné skutečnosti důležité pro trestní řízení, je nutno záznamy předepsaným způsobem zničit.

3.4.1.2 Operativně pátrací prostředky dle celního zákona

Ustanovení § 37a celního zákona (zákon č. 13/1993 Sb. ve znění pozdějších předpisů) stanoví, že celní orgány jsou pro plnění úkolů vyplývajících z mezinárodních smluv oprávněny používat **operativně pátrací prostředky stanovené trestním řádem**[116] při provádění dohledu nad osobami, o kterých existují závažné důvody domnívat se, že porušují nebo porušily celní předpisy druhé smluvní strany. Operativně pátrací prostředky pak mohou být použity pouze tehdy, jestliže by porušení právních předpisů, jejichž prováděním jsou celní orgány pověřeny, v případě, že by k němu došlo v tuzemsku, bylo posuzováno podle trestního zákona jako úmyslný trestný čin. Dále platí, že používáním operativně pátracích prostředků nesmí být sledován jiný účel, než který je uveden v příslušné mezinárodní smlouvě. Zákon také požaduje maximálně šetřit práva a svobody dotčených osob, když umožňuje jejich omezení jen v míře nezbytně nutné (§ 37c odst. 2 zákona č. 13/1993 Sb.). Zákon dále ukládá celním orgánům, aniž by to však konkrétněji specifikoval, povinnost zabezpečit ochranu operativně pátracích prostředků, jakož i informací získaných při provádění dohledu podle § 37a před vyzrazením a zneužitím.

Co se týká dalších způsobů ochrany používání sledovacích institutů před zneužitím, ustanovení § 37d celního zákona zakotvuje kontrolu použití odposlechu a záznamu telekomunikačního provozu a použití sledování osob a věcí. Tu provádí Poslanecká sněmovna, která k tomuto účelu zřizuje kontrolní orgán (složený z pěti poslanců výboru určeného Poslaneckou sněmovnou).

[116] Dle zákonné poznámky pod čarou se těmito operativně pátracími prostředky myslí operativně pátrací prostředky podle §§ 158b tr. řádu.

3.4.1.3 Operativně pátrací prostředky dle zákona č. 555/1992 Sb.

Zákon č. 555/1992 Sb. o Vězeňské službě a justiční stráži České republiky ve znění pozdějších předpisů (konkrétně jeho § 16 - § 21) dává další zákonné zmocnění pro použití **operativně pátracích prostředků i podpůrných operativně pátracích prostředků**. Operativně pátrací prostředky a podpůrné operativně pátrací prostředky podle tohoto zákona používají v objektech Vězeňské služby orgány k tomu oprávněné podle § 158b trestního řádu, a to na žádost ministra nebo s jeho souhlasem. Podpůrné operativně pátrací prostředky mohou v objektech Vězeňské služby k předcházení a odhalování trestné činnosti pak použít přímo pověřené orgány Vězeňské služby. Podpůrnými operativně pátracími prostředky jsou zabezpečovací technika (technické prostředky, zařízení a jejich soubory používané za účelem předcházení nebo zamezení ohrožení života a zdraví osob nebo k zabezpečení ochrany majetku a vyhledávání radiotelekomunikační techniky v objektech vazebních věznic a věznic a zabránění nedovolené komunikace osob ve výkonu vazby a ve výkonu trestu odnětí svobody) a zvláštní finanční prostředky. Použitím zabezpečovací techniky nesmí být zasahováno do ústavně zaručených práv a svobod.

Obdobně jako celní zákon, i zákon č. 555/1992 Sb. stanoví alespoň ty nejzákladnější meze používání operativně pátracích prostředků a podpůrných operativně pátracích prostředků. Ty mohou být použity jen v souladu s účelem výkonu vazby a výkonu trestu odnětí svobody a nesmí omezovat nad míru nezbytně nutnou práva jiných osob, zejména osob ve výkonu vazby a ve výkonu trestu odnětí svobody. Zákon výslovně zakazuje jejich použití při styku mezi osobou ve výkonu vazby nebo ve výkonu trestu odnětí svobody a jejím obhájcem.

Na tomto místě je vhodné zmínit i zákon č. 129/2008 Sb. o výkonu zabezpečovací detence. Institut zabezpečovací detence je koncipován jako určitá analogie ústavního ochranného léčení s tím, že je určen pro zvláštní kategorii pachatelů (typicky zvlášť závažných úmyslných trestných činů, trpících duševní poruchou a bez potřebného náhledu na svůj zdravotní stav a spáchanou trestnou činnost), kteří dokazují, že nemají zájem podrobit se léčbě své psychické poruchy, ačkoliv bez tohoto kroku jejich další pobyt na svobodě je nebezpečný. Tento zákon č. 129/2008 Sb. mimo jiné například

ve svém ustanovení § 35 odst. 4 v rámci možnosti umístění chovanců po nezbytně nutnou dobu do izolační místnosti s vybavením omezujícím možnost sebepoškození chovance stanoví, že *„po dobu pobytu v izolační místnosti je chovanec trvale sledován zaměstnanci Vězeňské služby, a to i s využitím kamerového systému.“*

3.4.2 Podpůrné operativně pátrací prostředky

Podpůrné operativně pátrací prostředky jsou vedle operativně pátracích prostředků spíše vedlejšími, pomocnými opatřeními konanými v rámci operativně pátrací činnosti. Lze říci, že tyto prostředky jsou používány zejména ve stadiu předcházení trestné činnosti.[117] Rozlišujeme podpůrné operativně pátrací prostředky používané jednak policisty dle zákona o Policii České republiky a jednak celníky dle celního zákona.[118]

3.4.3 Sledovací prostředky zpravodajských služeb

Dalším subjektem, který je ze zákona oprávněn využívat různých sledovacích metod a utajených způsobů činnosti, která může zasáhnout do soukromí lidí, jsou **zpravodajské služby**. Po sametové revoluci v roce 1989 a převzetí moci demokratickými politickými subjekty se tehdejší reprezentace rozhodla neudílet zpravodajským službám příliš velké pravomoci, a to především s ohledem na negativní zkušenosti z minula. V dobách vlády komunistického režimu byly zpravodajské služby zcela v područí vládnoucích stranických garnitur a jejich demokratické řízení či kontrola byly velmi omezeny.

V současné době existují v České republice tři agentury, pověřené zpravodajskými úkoly. Jsou jimi Bezpečnostní informační služba, Vojenské zpravodajství a Úřad pro zahraniční styky a informace.[119] Z právního

---

[117] Viz ŠÁMAL, K. - KRÁL, V. - BAXA, J. a kol.: Trestní řád. Komentář. I. a II. Díl. 5. vydání. Praha: C. H. Beck, 2005, strana 1160.

[118] Vedle toho existují i již zmiňované podpůrné operativně pátrací prostředky ve smyslu zákona č. 555/1992 Sb., o Vězeňské službě a justiční stráži České republiky.

[119] Vedle těchto tří českých zpravodajských služeb existují v České republice ve sféře odhalování závažných bezpečnostních hrozeb dále speciální útvary Policie ČR a Celní správy - jejich úkoly se do jisté míry s úkoly zpravodajských služeb prolínají. Zčásti

hlediska je činnost zpravodajců zajištěna trojicí zákonů. Zákon č. 153/1994 Sb. o zpravodajských službách České republiky, ve znění pozdějších předpisů, plní úlohu jakési zastřešovací právní normy pro všechny tři zpravodajské služby. Současně tento zákon vymezuje i základní právní rámec pro fungování **Úřadu pro zahraniční styky a informace** (dále i jako „ÚZSI"). Zákon č. 154/1994 Sb. o Bezpečnostní informační službě, ve znění pozdějších předpisů (dále v textu i jako „zákon o BIS") pak podrobněji stanoví pravomoci a další podmínky pro chod **Bezpečnostní informační služby** (dále v textu i jako „BIS"). Činnost **Vojenského zpravodajství** je pak dána v rámci zákona č. 289/2005 Sb. o Vojenském zpravodajství, ve znění pozdějších předpisů.

3.4.3.1 Zákon o zpravodajských službách České republiky, ÚZSI

Sám výše zmíněný „zastřešovací" zákon č. 153/1994 Sb. o zpravodajských službách České republiky ve znění pozdějších předpisů obsahuje jak zakotvení pravomocí stejných pro všechny tři zpravodajské služby, tak i zvláštní ustanovení platná pro Úřad pro zahraniční styky a informace.

V tzv. zvláštních ustanoveních daného zákona o Úřadu pro zahraniční styky a informace (§ 17-19) je pak tomuto úřadu umožněno pro ochranu činností, které ÚZSI koná na území České republiky, a jestliže je to nezbytné pro plnění úkolů v jeho působnosti, používat **sledování osob a věcí**, krycí doklady, **nástrahovou a zabezpečovací techniku** a využívat osob jednajících v jeho prospěch, které musí být starší 18 let. V těchto zvláštních ustanoveních jsou vymezeny i podmínky uchovávání údajů o fyzických a právnických osobách, přičemž ÚZSI skutečnost o vedení

---

zpravodajské povahy (na poli tzv. praní peněz) je i finanční analytický odbor Ministerstva financí ČR. Konečně je nutno se zmínit i o Národním bezpečnostním úřadu (NBÚ), který je však spíše specifickým správním úřadem, než zpravodajskou službou. NBÚ je ale významným příjemcem zpráv zpravodajských služeb, týkajících se zadaných bezpečnostních prověrek fyzických i právnických osob, proto je jistě nutné v rámci této práce se o něm alespoň takto zmínit. Blíže viz ZEMAN, P: Zpravodajské služby ČR, jejich právní postavení a vývoj. In: Bulletin Analýzy & studie. Praha: Centrum strategických studií, 2002-2006. ISSN 1214-8393. [online]. Dostupné na: http://www.strat.cz/bulletin/page.php?id=217 [cit. 2011-11-18].

evidence o fyzických a právnických osobách ani její obsah těmto osobám ze zákona **nesděluje**.[120]

3.4.3.2 Bezpečnostní informační služba

Zákon č. 154/1994 Sb. ve znění pozdějších předpisů dává Bezpečnostní informační službě poměrně široké možnosti použití zpravodajské techniky při nejrůznějších způsobech sledování a zjišťování informací. Zákon jim dává souhrnné označení ***specifické prostředky získávání informací***. Jsou jimi jednak **zpravodajské prostředky** a jednak **využívání služeb osob jednajících ve prospěch Bezpečnostní informační služby**.

Zpravodajské prostředky se dále dělí na zpravodajskou techniku, krycí prostředky a krycí doklady, a sledování. Krycí prostředky a krycí doklady (§ 13) slouží jako jedna z metod nejrůznějšího utajení, ať již pro příslušníka BIS nebo zájmů či objektů BIS. Sledování je upraveno poměrně prozaicky a stručně jednou větou § 14. Největší pozornost věnuje zákon o BIS zpravodajské technice. Tou se rozumějí nejrůznější technické prostředky a zařízení pokud je při něm zasahováno do základních práv a svobod občanů při

a) vyhledávání, otevírání, zkoumání nebo vyhodnocování dopravovaných zásilek,

b) odposlouchávání, popřípadě zaznamenávání telekomunikačního, radiokomunikačního a jiného obdobného provozu, popřípadě zjišťování údajů o tomto provozu,

c) pořizování obrazových, zvukových nebo jiných záznamů,

d) vyhledávání použití technických prostředků, které by mohly znemožnit nebo znesnadnit plnění úkolů v rámci Bezpečnostní informační služby,

e) identifikaci osob nebo předmětů, popřípadě zjišťování jejich pohybu za použití zabezpečovací a nástrahové techniky.

[120] Jako určitý problém se může jevit absence podrobnější úpravy kontroly a dohledu nad činností ÚZSI. S výjimkou poměrně vágního ustanovení § 12 zákona č. 153/1994 Sb. o zpravodajských službách České republiky není kontrola tohoto zpravodajského úřadu totiž nikde zakotvena.

Zákon dává také negativní vymezení toho, co se nepovažuje za použití zpravodajské techniky. Podle zákona jím není

a) *zachycování, poslech, monitorování a vyhodnocování informací, které jsou šířeny způsobem, jenž k nim umožňuje přístup předem neurčeného okruhu osob,*
b) *pořizování obrazových nebo zvukových záznamů,*
c) *používání zabezpečovací a nástrahové techniky,*
d) *monitorování telekomunikačního, radiokomunikačního nebo jiného obdobného provozu bez odposlechu jeho obsahu, popřípadě zjišťování údajů o tomto provozu,*

ovšem pouze za předpokladu, že shora uvedenými činnostmi není zasahováno do základních práv a svobod občanů.

V zákoně o BIS jsou samozřejmě vymezeny i **základní podmínky používání zpravodajské techniky**, zejména s ohledem na zabránění jejího možného zneužití. Tak může BIS použít zpravodajskou techniku jen po předchozím písemném povolení předsedy senátu vrchního soudu příslušného podle sídla Bezpečnostní informační služby (dále v textu již jen jako „soudce“)[121] a za předpokladu, že by odhalování nebo dokumentování činností, pro něž má být použita, bylo jiným způsobem neúčinné nebo podstatně ztížené nebo v daném případě nemožné. Použití zpravodajské techniky pak v žádném případě nesmí překročit rozsah tohoto povolení a nesmí zasahovat do práv a svobod občanů nad nezbytně nutnou míru.[122]

---

[121] Zde se nabízí otázka, zda by z hlediska ústavní zásady „nikdo nesmí být odňat svému soudci“ neměl být jako soud příslušný k rozhodování o povolení použití zpravodajské techniky stanoven spíše obecný soud osoby, jež bude dotčena použitím zpravodajské techniky, byť daná právní úprava je zřejmě v souladu se zněním článku 28 odst. 1 Listiny základních práv a svobod (*Nikdo nesmí být odňat svému zákonnému soudci. Příslušnost soudu i soudce stanoví zákon*.). Ke stejné otázce např. ve slovenské obdobné právní úpravě srovnej DRGONEC, J.: Ústavoprávné aspekty použitia sledovacích technológií mocenskými zložkami štátu. In: DANČÁK, B. – ŠIMÍČEK, V. (Eds.): Bezpečnost České republiky – Právní aspekty situace po 11. září 2001. Sborník z konference. Brno: Masarykova univerzita v Brně, Mezinárodní politologický ústav, 2002, s. 118-119. J. Drgonec ve svém článku taktéž dedukuje jako vhodnější stanovení příslušnosti soudu spíše hledisko bydliště dotčené osoby namísto sídla bezpečnostního orgánu, který bude zpravodajskou techniku používat.

[122] Zákon o BIS stanoví ve svém § 10 odst. 1 nutné náležitosti písemné žádosti, na jejímž základě soudce vydá povolení k použití zpravodajské techniky. Ta má obsahovat základní informace o druhu uvažované zpravodajské techniky, době trvání jejího použití a další údaje identifikující osobu či předmět, kde má být použita zpravodajská technika. V případě, že zpravodajská technika má být použita vůči ústavnímu činiteli nebo má být jejím použitím zasahováno do práva nedotknutelnosti obydlí, musí být tato informace součástí žádosti. V žádosti je nutno uvést důvody pro použití

3.4.3.3 Vojenské zpravodajství

Můžeme říci, že oprávnění ke sledování a získávání informací má Vojenské zpravodajství prakticky totožná jako Bezpečnostní informační služba. Obdobně jako zákon o BIS i zákon č. 289/2005 Sb. o Vojenském zpravodajství zná tzv. ***specifické prostředky získávání informací.*** Jsou jimi obdobně jako u BIS jednak **zpravodajské prostředky** a jednak **využívání služeb osob jednajících ve prospěch Vojenského zpravodajství**. I další dělení a způsoby použití zpravodajských prostředků, kterými jsou vedle použití zpravodajské techniky krycí doklady, krycí prostředky a sledování osob a věcí, je obdobné. Zákon o Vojenském zpravodajství nabízí navíc definici toho, co se rozumí sledováním osob a věcí – je jím získávání poznatků o osobách a věcech prováděné utajovaným způsobem technickými nebo jinými prostředky (viz § 15 odst. 1 zákona č. 289/2005 Sb.).

3.5 Exkurz: Ochrana soukromí a obrazové sledování na Slovensku

Slovensko mělo po dlouhou dobu společnou historii s Českou republikou, i právní řád byl v moderním období až do roku 1993, kdy došlo k rozdělení republik, shodný. Po rozpadu společného státu převzala Slovenská republika dosavadní právní stav a teprve od 1.1.1993 se začíná právní řád Slovenské republiky od ČR odlišovat. Základní principy a pojmy jsou však mimo jiné i s ohledem na společné členství v Evropské Unii stejné.

Ústava Slovenské republiky byla schválena Slovenskou národní radou 1. září 1992 jako zákon č. 460/1992 Sb. (Ústava Slovenskej

---

zpravodajské techniky, a to včetně zdůvodnění, že by odhalování nebo dokumentování činností, pro něž má být použita, bylo jiným způsobem neúčinné nebo podstatně ztížené nebo v daném případě nemožné (§ 9 odst. 1). Pokud již byla vůči dané osobě podávána dříve žádost o použití zpravodajské techniky, uvede se i tato skutečnost. Zákon také stanoví náležitosti rozhodnutí o povolení použití zpravodajské techniky a vůbec podmínky celého schvalovacího procesu. Soudce je oprávněn požadovat od Bezpečnostní informační služby informace k posouzení, zda důvody pro používání zpravodajské techniky trvají; pokud soudce zjistí, že důvody používání zpravodajské techniky pominuly, povolení k jejímu použití odejme. O ukončení používání zpravodajské techniky je BIS povinna bezodkladně písemně soudce informovat.

republiky). Na několika místech se výslovně zmiňuje o zaručení práva na ochranu soukromí:

Čl. 16
(1) Nedotknuteľnosť osoby a jej súkromia je zaručená. Obmedzená môže byť len v prípadoch ustanovených zákonom.
(2) Nikoho nemožno mučiť ani podrobiť krutému, neľudskému či ponižujúcemu zaobchádzaniu alebo trestu.

Čl. 21
(1) Obydlie je nedotknuteľné. Nie je dovolené doň vstúpiť bez súhlasu toho, kto v ňom býva.
(2) Domová prehliadka je prípustná len v súvislosti s trestným konaním, a to na písomný a odôvodnený príkaz sudcu. Spôsob vykonania domovej prehliadky ustanoví zákon.
(3) Iné zásahy do nedotknuteľnosti obydlia možno zákonom dovoliť iba vtedy, keď je to v demokratickej spoločnosti nevyhnutné na ochranu života, zdravia alebo majetku osôb, na ochranu práv a slobôd iných alebo na odvrátenie závažného ohrozenia verejného poriadku. Ak sa obydlie používa aj na podnikanie alebo vykonávanie inej hospodárskej činnosti, takéto zásahy môžu byť zákonom dovolené aj vtedy, keď je to nevyhnutné na plnenie úloh verejnej správy.

Čl. 22
(1) Listové tajomstvo, tajomstvo dopravovaných správ a iných písomností a ochrana osobných údajov sa zaručujú.
(2) Nikto nesmie porušiť listové tajomstvo ani tajomstvo iných písomností a záznamov, či už uchovávaných v súkromí, alebo zasielaných poštou, alebo iným spôsobom; výnimkou sú prípady, ktoré ustanoví zákon. Rovnako sa zaručuje tajomstvo správ podávaných telefónom, telegrafom alebo iným podobným zariadením.

Na rozdíl od České republiky, kde stále chybí zákon, který by komplexněji vymezoval a zastřešoval problematiku použití moderních sledovacích technologií ze strany orgánů státní moci, na Slovensku existuje zákon o ochraně soukromí před neoprávněným použitím informačně-technických prostředků a o změně a doplnění některých zákonů (**zákon o ochraně před odposlechem**), v originálním znění - *zákon č. 166/2003 Z. z. z 24. apríla 2003 o ochrane súkromia pred neoprávneným použitím informačno - technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním)*. V České republice je obdobná právní úprava roztříštěná do množství dílčích, resortních zákonů a chybí právní norma, která by problematiku komplexně zakotvovala. Použití sledovací techniky je tak speciálně upraveno v zákoně o Policii ČR, v zákoně o BIS, v zákoně o Vojenském zpravodajství a dalších zákonech. Slovenský zákon o ochraně před odposlouchávánim se oproti tomu snaží jednak **veškeré jednotlivé dílčí úpravy sjednotit**, přičemž však specielnější použití zvláštních předpisů ponechává v platnosti. Slovenský zákon o

ochraně před odposloucháváním stanoví **podmínky použití informačně-technických prostředků** bez předchozího souhlasu toho, komu je zasahováno do soukromí **orgánem státu**, který informačně-technický prostředek používá. V rámci trestního řízení se však při použití informačně-technických prostředků stále uplatní speciální právní úprava, vymezená ve slovenském trestním řádu (zákon č. 141/1961 Sb. o trestním řízení soudním ve znění pozdějších předpisů). **Informačně-technickými prostředky** se pak podle § 2 zákona rozumí zejména elektrotechnické, radiotechnické, fototechnické, optické, mechanické, chemické a jiné technické prostředky a zařízení nebo jejich soubory (sestavy) používané utajeným způsobem při:

a) *vyhledávání, otvírání, zkoumání a vyhodnocování poštovních zásilek a jiných dopravovaných zásilek*
b) *odposlechu a záznamu v rámci telekomunikačních činností*
c) ***pořizování a využívání obrazových, zvukových nebo jiných záznamů.***

Zákon o ochraně před odposlechem stanoví, že informačně-technické prostředky může používat Policejní sbor, Slovenská informační služba, Vojenské zpravodajství, Železniční policie, Sbor vězeňské a justiční stráže a Celní správa. V zákoně je výslovně stanoveno, že orgány územní samosprávy, soukromé bezpečnostní služby ani jiné fyzické či právnické osoby nesmí použít informačně-technický prostředek. Mohou tak učinit tedy **pouze výše uvedené orgány státu**. Samotné použití informačně-technických prostředků pro všechny výše uvedené orgány státu s výjimkou Slovenské informační služby pak technicky zabezpečuje Policejní sbor. Zákon obsahuje poměrně zajímavé ustanovení, které stanoví, že příslušník nebo zaměstnanec orgánu státu, který plní úkoly související s technickým zabezpečením použití informačně-technických prostředků, se musí podrobit ve lhůtě určené vedoucím daného státního orgánu psychofyziologickému ověření pravdomluvnosti.[123]

Ustanovení § 5 zákona pak povoluje použití informačně-technických prostředků jen tehdy, pokud je to **v demokratické společnosti nezbytné** na zajištění bezpečnosti státu, obranu státu, předcházení a objasňování trestné

[123] Viz ustanovení § 2 odst. 5 tohoto zákona.

činnosti nebo na ochranu práv a svobod jiných. Zákon dále stanoví, že použitím informačně-technického prostředku se může základní právo nebo svoboda omezit jen v nezbytném rozsahu a ne déle, než je nutné k dosažení zákonem stanoveného účelu. Údaje získané informačně-technickými prostředky lze pak použít výlučně k dosažení zákonného účelu při plnění úloh státu (pokud splňují podmínky uvedené v předchozí větě).

Z důvodu omezení svévole státního orgánu, který používá informačně-technický prostředek je v zákoně deklarováno, že informačně-technický prostředek lze použít jen na základě **předchozího písemného souhlasu zákonného soudce**, a to jen po nezbytnou dobu nepřesahující šesti měsíců (soudce může na základě nové žádosti tuto dobu i opakovaně prodloužit vždy maximálně o šest měsíců). Zákon taktéž umožňuje při splnění přísných podmínek použití informačně-technického prostředku Policejním sborem i bez předchozího souhlasu soudce.

Soudce, který dal souhlas k použití informačně-technického prostředku, jakož i orgán státu, který informačně-technický prostředek využívá, musí soustavně zkoumat **trvání důvodů** k použití těchto prostředků. Pokud tyto důvody pominuly, použití musí bezodkladně skončit.

Zákon o ochraně před odposlechem stanoví přísná pravidla pro **použití zvukového, obrazového nebo zvukově-obrazového záznamu**, který byl pořízen použitím informačně-technického prostředku, a to včetně možnosti jejich použití jako důkazu. Použití informačně-technického prostředku, pořízení či zkopírování záznamu, které by se uskutečnilo v rozporu se zákonem o ochraně před odposlechem, zakládá odpovědnost státu dle zvláštního předpisu a stejně tak i osoby, která zákon porušila tím, že nezákonnou činnost nařídila, schválila nebo se jí dopustila jiným způsobem.

Zákon dále obsahuje základní podmínky **provádění kontroly nad použitím informačně-technických prostředků**, za kterou je odpovědná Národní rada Slovenské republiky a její výbor pověřený kontrolou použití informačně-technických prostředků. Národní rada Slovenské republiky projedná v plénu zprávu pověřeného výboru, jejíž součástí musí být zjištěné případy nezákonného použití informačně-technických prostředků včetně uvedení informace o zodpovědnosti osob. Přitom však nesmí být odhalena

totožnost osob, proti kterým se použily informačně-technické prostředky, ani jinak porušit jejich právo na soukromí. Zprávu, kterou projednalo plénum, mohou uveřejnit hromadné sdělovací prostředky. I přes existující právní úpravu a instituty kontroly a ochrany před zneužitím, události roku 2011 ukázaly, že právní úprava i tak není dostatečná a že kontrola byla neúčinná.[124]

Na Slovensku existuje také preciznější zákonná právní úprava **monitorování prostor pomocí audio či video techniky**. Ustanovení § 10 odst. 7 *zákona č. 428/2002 Z. z. o ochrane osobných údajov* ve znění pozdějších předpisů totiž výslovně umožňuje monitorovat místo veřejně přístupné pomocí videozáznamu nebo audiozáznamu, děje-li se tak za účelem veřejného pořádku a bezpečnosti, odhalování kriminality anebo v případě narušení bezpečnosti státu. Může se tak dít pouze za předpokladu, že prostor je zřetelně označen jako monitorovaný (označení se nevyžaduje, stanoví-li tak zvláštní zákon). Pokud zvláštní zákon nestanoví jinak, lze pořízený záznam využít toliko pro trestní řízení či pro řízení o přestupcích. V ČR takováto výslovná úprava a stanovení alespoň základních podmínek a důvodů, kdy lze nainstalovat kamerové či audio zařízení, chybí.

[124] Slovenskem otřásl na přelomu let 2011 a 2012 velký skandál odposlechů novinářů na popud vojenské kontrarozvědky (Vojenského obranného zpravodajství). Ten ukázal, že i stávající úprava se musí změnit a zřejmě vylepšit stávající kontrolní mechanismy. Zdroj: článek Skandál s odposlechy stál slovenského ministra obrany funkci, dostupný online na: http://www.rozhlas.cz/zpravy/evropa/_zprava/skandal-s-odposlechy-stal-slovenskeho-ministra-obrany-funkci--979545 [cit. 2012-02-18].

4 KAMEROVÉ SYSTÉMY DETAILNĚJI

4.1 Rozmach kamerových sledovacích systémů

V roce 1787 navrhl anglický filozof Jeremy Bentham originální model budovy, zvaný Panoptikon (název vznikl složením slov Pan – „vše, všichni“ a Opticon – „pozorovat“). Budova měla být určena jako věznice, ale i výrobní prostory, nemocnice a další místa, kde je potřeba mít více lidí pod dohledem. Z centrální místnosti (inspection house) měli být dozorci schopni pozorovat veškeré vězně (pracovníky apod.), aniž by dozorci byli sami viděni. Myšlenky Pantoptikonu ve vztahu ke společnosti a myšlení lidí dále rozvinul historik a filozof Michel Foucault, který se tímto tématem zabýval ve své knize Dohlížet a trestat. Foucault viděl v myšlence Panoptikonu metodu hierarchizace, integraci do systému, disciplínu. Vězni jsou viděni, ale sami nevidí. Systém Panoptikonu zavádí do vědomí trestanců neustálý pocit strach a nejistotu, což by vedlo k tomu, že by se hlídali nakonec i sami. Permanentní pocit toho, že jsou sledováni, by zajišťoval automatické fungování moci. Bentham a Foucault deklarovali, že moc musí být viditelná, ale neověřitelná. Žít s vědomím, že nikdy nevíme, zdali jsme zrovna sledováni nebo ne, má obrovský vliv na lidskou psychiku.[125] Moderní kamerové systémy vychází vlastně z těchto principů nastíněných Benthamem a Foucaultem. Lidé jsou neustále pod dohledem kamerových systémů, pod dohledem určité autority, aniž by věděli, zda jsou v danou chvíli opravdu někým sledování a kým konkrétně, případně za jakým účelem. Ve Velké Británii jsou dokonce k vybraným kamerám instalovány i zvukové reproduktory, umožňující bezpečnostním pracovníkům udílet pokyny a varování na místo snímané kamerou. Zde je již evidentní podobnost s Orwellowým Big Brotherem.

Používání kamerových sledovacích systémů dosáhlo v posledních letech nebývalého rozmachu. V rámci Evropy nicméně existují poměrně razantní rozdíly v zavádění kamer na veřejná prostranství - některé země sledují své občany doslova na každém kroku (Velká Británie), jinde se s používáním kamer začíná teprve nyní a mnohem pomaleji (Dánsko, Rakousko). Česká republika patří k zemím, kde se kamery objevily poměrně

[125] Zdroj: Bentham, Jeremy *The Panopticon Writings.* Ed. Miran Bozovic (London: Verso, 1995), dostupné online na: http://cartome.org/panopticon2.htm [cit. 2012-02-18].

brzy a v současné době je používání kamerových systému již velmi rozšířené. Nad kamerami, které nás potkávají prakticky na každém kroku, se již nikdo nepozastavuje. Kamery jsou využívány v hojné míře jak veřejnoprávními subjekty (bezpečnost na ulicích, monitorování a kontrola dopravy, zajištění větší bezpečnosti ve vybraných objektech atd.), tak i mezi soukromými subjekty. V poslední době se také objevují nové možnosti dalšího využití kamerových systémů, jako je propojení kamer s globálním satelitním pozičním systémem (GPS), automatické rozpoznávání státních poznávacích značek vozidel (*systém ZTC/MAZ-VIS* - Vehicle Identification Systém - technika dokáže ve spojení s patřičným softwarovým vybavením porovnávat projíždějící vozidla s databázemi odcizených či jinak pro policii zajímavých aut), technologie rozpoznávání konkrétního člověka podle jeho obličeje (*facial recognition system*) či podle jeho chůze, používání webových kamer, které umožňují přenášet obraz v aktuálním čase prostřednictvím sítě Internet prakticky kamkoliv na světě, propojení kamerových systémů s dalšími zabezpečovacími prvky jako jsou pohybové detektory, zvukové hlásiče, které posílají signál na pult centrální ochrany a mnoho dalších. Použití kamer je pak široce uplatňováno i ve zdravotnictví při provádění složitých operací, ve stavebnictví a jiných oborech lidské činnosti při monitoringu nepřístupných prostorů (potrubí, kanalizace, jeskyně). Škála možného využití kamer je prakticky nepřeberná.

Evropský primát v používání kamerových a obdobných sledovacích zařízení drží asi Velká Británie, kde dosáhly sledovací technologie obrovského rozmachu. V poslední době se zde začínají používat specielní kamerové systémy s technologií rozpoznávání konkrétního člověka dle jeho obličeje či dle způsobu jeho chůze. Zatím tyto systémy samy o sobě nezaručují velkou úspěšnost, nicméně se intenzivně pracuje na jejich dalším vývoji. Od roku 2006 je právě ve Velké Británii zprovozněn celonárodní systém, umožňující rozpoznávání pohybu jednotlivých vozidel na všech hlavních dálnicích a silnicích. Za tímto účelem jsou v zemi rozmístěny již stávající kamerové systémy, které byly dále mohutně rozšířeny a jsou nyní schopny zaznamenat desítky milionů poznávacích značek denně a sledovat tak pohyb vozidel po zemi. Systém využívá samozřejmě i satelitní globální systém. Celostátní monitorovací středisko pro pohyb automobilů je schopno

uchovávat údaje o datu, čase a místě pohybu každého vozidla, jehož poznávací značku zaznamenají jednotlivá snímací zařízení a tyto záznamy uchovávat po řadu měsíců až let. Je pravdou, že zkušební provoz omezené části systému v letech 2003 – 2004 prokázal zlepšení při identifikaci zločinců a míře úspěšnosti boje bezpečnostních složek s kriminalitou.

Další ze zemí, kde jsou kamerové systémy a moderní metody rozpoznání dalších přídavných atributů hojně užívány, je Čína. V rámci projektu Golden Shield Čína již několik let masivně zavádí statisíce až miliony nových kamer a systémů ke sledování svých občanů.

Čínská jižní megapole Chongqing například oznámila plány rozšířit do roku 2014 městský kamerový systém až na neuvěřitelných více jak 500.000 kamer. Plán tzv. Mírumilovného Chongqingu zahrnuje pokrytí půlmilionu křižovatek, ulic a parků v území větším jak 400 čtverečních mil, o 25% větším než je plocha New Yorku. S provedením zakázky je spojena americká společnost Cisco, která je v USA za tyto aktivity kritizována.[126] Čína patří mezi největší uživatele kamerových systémů a dalších sledovacích technologií. Vzhledem k autoritářské formě vlády v této zemi je nepochybně odůvodnitelná obava, zda toto dalekosáhlé využívání moderních technologií státem a jinými subjekty splňuje i požadavky na ochranu soukromí čínských občanů.

4.2 Kamerové systémy v ČR

V České republice je výslovně právně zakotveno a upraveno používání kamerových sledovacích zařízení toliko pro činnost policejních a bezpečnostních orgánů státu, a dále okrajově pro některé zvláštní provozy či zařízení (atomové elektrárny, kasina atd.). Pro používání kamerových systému ze strany jiných než nestátních subjektů však nejsou dána zcela jasná zákonná pravidla. Od účinnosti zákona o ochraně osobních údajů se na danou problematiku vztahuje alespoň tento zákon, který upravuje nakládání s osobními údaji, a to ve všech těch případech, kdy dochází k uchovávání

[126] Článek Wall Street Journalu „Cisco Poised to Help China Keep an Eye on its Citizens“ dostupný online v anglickém jazyce na: http://online.wsj.com/article/SB10001424052702304778304576377141077267316.html [cit. 2012-01-21].

záznamů umožňujících přímo či nepřímo identifikovat fyzické osoby. Úřad pro ochranu osobních údajů ve svém **stanovisku** k dané problematice deklaroval, že fyzická osoba je identifikovatelná, pokud ze snímku, na němž je zachycena, jsou patrné její charakteristické rozpoznávací znaky (zejména obličej) a na základě propojení rozpoznávacích znaků s dalšími disponibilními údaji je možná **plná identifikace osoby**.[127] Osobní údaj pak, podle názoru Úřadu, ve svém souhrnu tvoří ty identifikátory, které umožňují příslušnou osobu spojit s určitým, na snímku zachyceným jednáním. Lze říci, že pokud technické zařízení umožní **zaznamenání rozpoznatelné lidské tváře**, prakticky vždy půjde o zpracování osobních údajů dle zákona o ochraně osobních údajů. Podle předmětného stanoviska pak kamerový systém, který takto zpracovává osobní údaje, lze provozovat:

- v rámci plnění úkolů uložených zákonem (Policií ČR, obecní policií atd.), nebo
- na základě řádného souhlasu subjektu údajů (tento souhlas však je realizovatelný jen ve velmi omezených případech, kdy lze jednoznačně vymezit okruh potenciálně dotčených osob), nebo
- i bez souhlasu subjektu údajů na základě zmocnění v ustanovení § 5 odst. 2 písm. e) zákona č. 101/2000 Sb.

Třetí uvedený případ je dle citovaného zmocňovacího ustanovení zákona o ochraně osobních údajů možný, pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce osobních údajů, příjemce nebo jiné dotčené osoby. Současně však také platí, že takové zpracování osobních údajů nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života. Úřad pro tuto možnost ve svém stanovisku pak vymezil podmínky, za nichž je provozování kamerového systému dle ust. § 5 odst. 2 písm. e) zákona č. 101/2000 Sb. možné:

- *kamerové sledování nesmí nadměrně zasahovat do soukromí*

[127] Viz Zásady provozování kamerového systému z hlediska zákona o ochraně osobních údajů – stanovisko č. 1/2006 Úřadu pro ochranu osobních údajů, publikované např. na internetových stránkách tohoto úřadu (www.uoou.cz)

- *je nutné předem specifikovat účel monitorování a pořizování záznamů*
- *je nutno stanovit lhůtu pro uchovávání záznamů (tato doba by neměla přesáhnout časový limit přípustný pro naplnění účelu provozování kamerového systému - ideálně 24/48 hodin, neměla by přesáhnout dobu několika dnů)*
- *nutno zajistit řádnou ochranu zařízení a záznamů před neoprávněným nebo nahodilým přístupem, zničením, poškozením nebo jiným neoprávněným zpracováním*
- *subjekt údajů musí být o užití kamerového systému vhodně informován (nápisem v monitorované místnosti, při vstupu apod.)*
- *je třeba garantovat subjektu údajů i další práva, zejména právo na přístup ke zpracovávaným datům a právo na námitku proti jejich zpracovávání*
- *zpracování osobních údajů je nutno registrovat u Úřadu pro ochranu osobních údajů*

Stanovisko Úřadu pro ochranu osobních údajů sice není právně závazné, nicméně působí silou své přesvědčivosti jakožto názor vydaný nezávislým orgánem, který je pověřen dozorem a kontrolou v dané problematice; navíc je zřejmé, že Úřad ve své zákonem vymezené rozhodovací praxi (kontrolní činnost) bude postupovat podle tohoto svého stanoviska. [128]

---

[128] Česká republika není jedinou zemí, kde chybí podrobnější zákonná právní úprava používání kamerových systémů. Např. v Itálii tamější Úřad pro ochranu osobních údajů (Garante per la protezione dei dati personali) také pro absenci podrobnější zákonné úpravy vydal obdobná pravidla pro kamerové sledování. Ve svých pokynech uvádí jako nejdůležitější zásady zásadu přiměřenosti, tj. instalovat kamery jen není-li jiná alternativa (zvukový alarm apod.), zásadu informovat dotčené osoby o instalaci kamer a jejich účelu. Je také stanovena max. přípustná doba uchovávání záznamů, která by neměla překročit 24 hodin (nejde – li o výjimečnou situaci vyžadující delší dobu archivace; u bank je lhůta pak omezena na 1 týden). Striktně zakázáno je v Itálii kamerové sledování vlastních zaměstnanců. Také je zakázáno sledování větších veřejných prostranství ve městech, stejně jako využívání kamer při boji s drobnými přestupky (vstup na trávník, porušování zákazu kouření atd.). Obdobně jako v ČR je možné užívání kamer soukromými subjekty jako ochranu před vandalismem, krádežemi, násilím či požáru, subjekt však musí zaručit, že kamera snímá výlučně jeho majetek a ne třeba i část veřejného prostranství.
Zdroj: www.statewatch.org/news/2004/may/19italy-surveillance.htm [cit. 2012-02-18].
Obdobně např. ve Švýcarsku je sledování pomocí kamer upraveno také pouze obecně v rovině zákona o ochraně dat z roku 1992 (Bundesgesetz vom 19. Juni 1992 über den

Pokud dochází k prostému sledování prostoru pomocí kamerových či jiných bezpečnostních systémů bez archivace údajů, zákon o ochraně osobních údajů použít nelze (příklad – člen bezpečnostní agentury může bez problému použít kameru, která je vlastně jakýmsi „prodloužením jeho oka“, umožní mu pozorovat najednou více míst; jakmile však bude obraz z kamery jakkoliv uložen na záznamové médium, je zde již mnohem vyšší potenciální společenská nebezpečnost a na věc se bude vztahovat zákonná úprava dle zákona č. 101/2000 Sb.).

Jak vyplynulo z výše uvedeného, kamerové systémy tak rozeznáváme dvojího druhu, jednak kamerové systémy se záznamem (archivace záznamu) a pak kamerové systémy provozované bezzáznamově. Obecně lze deklarovat, že druhý typ kamerového sledování je z hlediska právního posuzování a dopadů na režim ochrany soukromí jednotlivce a ochrany osobnosti benevolentnější. I toto kamerové sledování, byť nebude záznam ukládán, není možné instalovat a provozovat zcela svévolně. Taktéž na kamerové systémy bez záznamu se alespoň v některých případech vztahuje právní úprava a minimálně podmínky dané příslušnými ustanoveními občanského zákoníku (ochrana osobnosti). I když totiž nepůjde o pořizování záznamů či snímků, které by byly následně uchovávány na hmotných nosičích, nelze tedy aplikovat výše v této práci zmíněnou právní úpravu dle ustanovení § 12 o.z., dalo by se takovéto monitorování podřadit pod obecnější § 11 o.z., který chrání osobnost jednotlivce jako celek. Soustavné sledování a monitorování konkrétní osoby, navíc na uzavřeném prostoru, by již zásahem do osobnostních práv nepochybně bylo. Bude tomu tak zejména tehdy, kdy je konkrétní osoba podrobena soustavnému dohledu, a to zvlášť tehdy, pokud o něm neví a nemůže jej rozumně očekávat. Stejně tak například zákoník práce umožňuje

---

Datenschutz (DSG; SR 235.1)). Je však zajímavé, že podle názoru švýcarského úřadu pro ochranu dat (Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)) je lhostejno, zda jsou záznamy z kamerového sledování ukládány či nikoliv, monitorování pomocí kamer spadá v každém případě do režimu tohoto zákona (v ČR spadá pod režim zákona o ochraně osobních údajů dle stávajícího výkladu zřejmě jen monitorování s pořizováním záznamů). Tento úřad také na svých internetových stránkách zveřejnil v lednu 2006 podrobný návod pro provádění videokontroly soukromými osobami (stylem i obsahem obdobný Zásadám provozování kamerových systémů českého ÚOOÚ) – blíže k tomu viz [cit. 2012-02-18]: http://www.edoeb.admin.ch/dokumentation/00445/00507/00603/index.html?lang=de

kamerové sledování pouze v případech stanovených § 316 zákoníku práce, tj. v zásadě buďto za účelem kontroly případného zneužívání pracovních prostředků zaměstnavatele nebo za účelem sledování zaměstnanců z jiného závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele.

V následujícím výkladu bych se pokusil provést i jakési základní dělení kamerových systémů, a to sice dělení na kamerové systémy výslovně povolené zákonem, dále na kamerové systémy na pracovišti, kamerové systémy v dětských domovech a školských zařízeních a konečně na kamerové systémy v jiných sférách použití.

4.3 Kamerové systémy povolené zákonem

Jako jedno z prvních setkání českého právního řádu s problematikou kamerových sledovacích systémů lze zřejmě chápat zákonné vymezení podmínek **zajištění bezpečnosti jaderných zařízení**. Ustanovení § 4 odst. 7 a následující odstavce zákona č. 18/1997 Sb. ve znění k datu přijetí tohoto zákona určuje základní podmínky kategorizace jednotlivých druhů jaderných zařízení a stanoví podmínky zajištění jejich ochrany. Prováděcí vyhláška č. 144/1997 Sb. Státního úřadu pro jadernou bezpečnost ze dne 19. června 1997 o fyzické ochraně jaderných materiálů a jaderných zařízení a o jejich zařazování do jednotlivých kategorií pak dále zabezpečení jednotlivých kategorií jaderných zařízení upřesňuje. Tato vyhláška ještě operuje s dnes již poněkud zastaralým pojmem *televizní technika*.[129]

Další oblastí používání kamerových sledovacích systémů, které se dostalo zákonného podkladu, je oblast provozování hazardních her v kasinech. Novelizací zákona č. 202/1990 Sb. o loteriích a jiných podobných hrách, provedenou **zákonem č. 149/1998 Sb.** bylo do loterijního zákona zavedeno nové znění **§ 37**, které stanoví: *„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*

[129] Srov. kupříkladu ustanovení § 6 odst. 2 písm. a) či § 6 odst. 3 vyhl. č. 144/1997 Sb. Ustanovení § 12 odst. 1 však již zmiňuje přímo pojem kamerový systém. Zajímavé je také, že vyhláška ve svém § 8 odst. 2 rozeznává již i biometrickou identifikaci (např. geometrie ruky, otisk prstů).

(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." Tímto právním předpisem se stala vyhláška Ministerstva financí č. 285/1998 Sb. **o podmínkách monitorování a uchovávání záznamů v kasinu**. Tato prováděcí vyhláška pak již výslovně používá pojem kamerový systém. Máme-li se alespoň v základních rysech zmínit o používání kamerových systémů v kasinech v kontextu jejich přípustnosti s ohledem na ochranu soukromí hráčů, můžeme dovodit, že monitorování hracích prostor v kasinu je z hlediska ochrany soukromí jednotlivce v pořádku, nepřekračuje-li monitoring prostor vymezení a účel stanovený v zákoně č. 202/1990 Sb. a jeho prováděcí vyhlášce. Jiná otázka však nastává v případě provozování automatických výherních hracích přístrojů např. na tzv. elektronickou ruletu, které se v současnosti běžně vyskytují často **nejen v kasinech**, ale i v hernách nebo dokonce v restauračních zařízeních, barech. I tato herní zařízení na elektronickou ruletu bývají pravidelně vybavena kvalitním monitorovacím zařízením, které snímá hráče u herního stolu, aniž k tomu má provozovatel zařízení zákonný podklad, tak jako je tomu při monitoringu hry v kasinu. Souhlas hráče s monitorováním hry a jeho osoby mimo kasino je tedy nutno dovozovat z akceptace herního řádu, resp. herních podmínek, které se svým rozhodnutím zahrát si na příslušném herním zařízení hráč podvolil akceptovat. Jinak obecně platí, že účel monitorování je v tomto případě položen spíše ve prospěch provozovatele herního zařízení, neboť monitorování mu má zaručit, že hráči se při hře nedopouštějí podvodů či nepovolených manipulací se zařízením. Monitorování i zde má samozřejmě sloužit při řešení eventuelně vzniklých sporných otázek, na kterou sázku hráč vsadil apod. (tak jak je tomu v kasinu při hře rulety na klasickém stole s lidskou obsluhou). Monitorovací zařízení pak také slouží ke kontrole obsluhujícího personálu a správnosti vyplácených výher (zařízení elektronické rulety běžně zaznamenává a uchovává přehled o průběhu každé hry, včetně výše sázek a výher

konkrétního hráče; majitel herního zařízení může být dokonce o průběhu každé hry informován pomocí SMS, či online připojení, a to v reálném čase). Provozovatel herního zařízení je oprávněn monitorovat průběh hry, stanoví-li tak v hracím řádu a především pokud jsou hráči o monitoringu řádně informování (upozorněním v hracích prostorách, odkazem v herním řádu, který hráči svou hrou akceptují). V žádném případě však provozovatel zařízení není oprávněn (tak jako je tomu ostatně i u záznamů z monitorování hry v kasinech) využít záznamů z průběhu hry o jednotlivých hráčích k jinému než výše stanovenému účelu vyloučení podvodů při hře, kontroly personálu, přehledu o proběhlých hrách a sázkách apod.

Kamerové systémy zmiňuje i Výklad č. MI02/2003 Ministerstva informatiky k § 4 odst. 4 vyhlášky č. 366/2001 Sb. nazvaný Bezpečnost informačního systému pro certifikační služby (ISCS) z hlediska požadavků objektové bezpečnosti. Ten doporučuje pro efektivní střežení hranice zabezpečené oblasti využívat perimetrické bezpečnostní systémy, k nimž se řadí perimetrické detekční systémy, bezpečnostní osvětlení, ***kamerové systémy***. Perimetrické detekční systémy mohou být přitom instalovány skrytě (obvykle z estetických důvodů) nebo zjevně jako odrazující prvek.[130]

S kamerovými systémy jako s technickými prostředky bezpečnostní ochrany pracuje vyhláška Ministerstva průmyslu a obchodu ze dne 4. června 2004 č. 373/2004 Sb., kterou se stanoví podrobnosti o rozsahu bezpečnostních opatření **fyzické ochrany objektu nebo zařízení** zařazených do skupiny A nebo do skupiny B.[131] Vyhláška byla zrušena zákonem č. 59/2006 Sb. o prevenci závažných havárií, jehož prováděcí vyhláška č. 250/2006 Sb. opět zmiňuje kamerové systémy jako technické prostředky bezpečnostních opatření fyzické ochrany objektů nebo zařízení.[132]

Ve vyhlášce Ministerstva financí ze dne 28. června 2004 č. 416/2004 Sb., kterou se provádí zákon č. 320/2001 Sb. **o finanční kontrole ve veřejné správě** a o změně některých zákonů, je pojem kamerových systémů užíván jako technický prostředek využívaný v operačních postupech k

130 Srov. bod 4.7 Vnitřní ochrana objektu daného Výkladu č. MI02/2003.
131 Viz § 4 odst. 1 písm. b) této vyhl. č. 373/2004 Sb.
132 Srov. § 5 písm. b) této vyhlášky.

dosažení vyšší účinnosti průběžné kontroly, zejména k odstranění nebo zmírnění provozních, finančních, právních a jiných rizik a k zajištění ochrany osob a majetku.[133]

V oblasti justice je již několik let v platnosti instrukce Ministerstva spravedlnosti č. 90/2004-SM **o justiční stráži**, jejíž ustanovení § 4 odst. 1 písm. d) popisuje napojení ostatních prvků zabezpečovacích prostředků (např. sledovacího kamerového systému, systému kontroly vstupů, videotelefonu, základnové radiostanice, detektorů elektrického zabezpečovacího systému, požární signalizace) do služebny justiční stráže. Taktéž Instrukce Ministerstva spravedlnosti ze dne 8. září 2004 č. 762/2004-OGI/OV, o eskortních místnostech v budovách soudů zmiňuje požadavek umístění kamerových systémů v místnostech eskorty a jiných objektech, resp. i jejich propojení se služebnou justiční stráže.[134] Obdobně viz aktualizovaná instrukce Ministerstva spravedlnosti, publikovaná pod č. 395/2009-OBKŘ.

Z výše uvedeného demonstrativního přehledu je patrné, že pojem kamerových systémů našel v právním řádu své místo a právní řád tento pojem a pojmy jemu blízké zná a používá. Domnívám se, že jde o příklad postupného pronikání nové technologie i do právního systému a jeho čím dál častější (v porovnání např. s devadesátými léty 20. století) a obvyklejší užívání v právních předpisech různé právní síly. Časem bude komplexněji a precizněji řešena jistě i otázka kolize užití kamerových systémů s právem jednotlivce na ochranu soukromí.

---

[133] Viz ustanovení § 20 této vyhlášky:
K dosažení vyšší účinnosti průběžné kontroly, zejména k odstranění nebo zmírnění provozních, finančních, právních a jiných rizik a k zajištění ochrany osob a majetku, se využijí v operačních postupech technické prostředky, zařízení a programová vybavení, například mechanismy ke znehodnocení obsahu bezpečnostních schránek, indikátory pravosti peněz, čidla, bezpečnostní rámy a **kamerové systémy**.

[134] Co se týká instalování kamerových systémů v prostorách věznic, právní předpisy ČR tuto otázku nijak neupravují. Např. na Slovensku je ale v platnosti *vyhláška č. 664/2005 Z.z. kterou se vydává poriadok výkonu trestu odňatia svobody* a ta ve svém § 92 odst. 2 umožňuje u tzv. oddílu (místnosti) s bezpečnostním režimem jeho zabezpečení kamerovým systémem. Stejně tak *zákon č. 475/2005 Z.z. o výkone trestu odňatia slobody a o zmene a doplnení niektorých zákonov*, dává možnost vybavit některé speciální cely kamerovým systémem, přičemž však s touto skutečností musí být odsouzený seznámen ve vnitřním řádu.

Příkladem první komplexnější úpravy užití kamerových systémů je zakotvení oprávnění státní a obecní policie k užívání kamerových dohlížecích systémů v zákoně o Policii ČR, resp. v zákoně o obecní policii.

4.4 Kamerové systémy provozované Policií ČR a obecní policií

Policie České republiky je zmocněna k používání kamerových dohlížecích systémů se záznamovou technologií zákonem č. 273/2008 Sb. o Policii České republiky, konkrétně ustanovením paragrafu 62:

§ 62
Pořizování záznamů

(1) Policie může, je-li to nezbytné pro plnění jejích 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.

(2) Jsou-li k pořizování záznamů podle odstavce 1 zřízeny stálé automatické technické systémy, policie informace o zřízení takových systémů vhodným způsobem uveřejní.

Ustanovení § 63 pak umožňuje, nelze-li zjistit totožnost předvedené osoby na základě sdělených údajů ani v dostupných evidencích, aby policista získal informace potřebné ke ztotožnění osoby mimo jiné pořizováním obrazových, zvukových a jiných záznamů – přitom platí, že nelze-li daný úkon (např. pořízení obr. záznamů) pro odpor osoby provést, je policista oprávněn tento odpor překonat; způsob překonání odporu musí pak být přiměřený intenzitě odporu. Ustanovení § 65 zákona o Policii České republiky pak upravuje tzv. *získávání osobních údajů pro účely budoucí identifikace*. Policie může při plnění svých úkolů pro účely budoucí identifikace u vybraných osob (obvinění, osoby ve výkonu trestu odnětí svobody, osoby, jimž bylo uloženo ochranné léčení nebo zabezpečovací detence atd.) pořizovat obrazové, zvukové a obdobné záznamy.[135]

Obdobnou právní úpravu pořizování obrazových a jiných záznamů jako je uvedeno v ustanovení § 62 nyní platného zákona o Policii České republiky obsahovalo od roku 2001 již i ustanovení § 42f dříve platného

[135] Do konce roku 2011 obsahoval zákon o Policii České republiky oprávnění a povinnosti Inspekce MV, kde v ustanovení § 107 upravoval tzv. zkoušku spolehlivosti policisty, když tento § 107 stanovil, že *„Průběh zkoušky spolehlivosti inspektor dokumentuje **obrazovým a zvukovým záznamem** a sepíše o něm úřední záznam.“*
Nyní obdobné ustanovení platí v rámci zákona č. 341/2011 Sb. o Generální inspekci bezpečnostních sborů: *„Průběh zkoušky spolehlivosti se dokumentuje **obrazovým a zvukovým záznamem**. O zkoušce spolehlivosti inspekce pořídí úřední záznam.“*

zákona č. 283/1991 Sb. o Policii České republiky, přičemž předmětné ustanovení § 42f bylo do zákona o policii č. 283/1991 Sb. zařazeno zákonem č. 60/2001 Sb. ze dne 11. ledna 2001.[136]

Oprávnění k provozování monitorovacích záznamových systémů vyplývá samozřejmě i pro obecní policii, a to ze zákona České národní rady ze dne 6. prosince 1991, č. 553/1991 Sb. **o obecní policii,** z jeho ustanovení § 24b, které bylo do zákona o obecní policii implementováno zákonem č. 311/2002 Sb. ze dne 13. června 2002:

§ 24b

(1) 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.

(2) Jsou-li k pořizování záznamů podle odstavce 1 zřízeny stálé automatické technické systémy, je obecní policie povinna informace o zřízení takových systémů vhodným způsobem uveřejnit.

Citované ustanovení tak dává obecní policii možnost záznamově monitorovat veřejně přístupná místa (tedy ne místa soukromá), je-li to třeba pro plnění jejích úkolů. Taktéž mohou orgány obecní policie zaznamenávat průběh zákroku nebo úkonu (již nyní se tak děje např. v praxi obecní policie v Kladně, Přerově, zatím pomocí diktafonů). Zákon vyžaduje, aby v případě, že za účelem pořizování záznamů z míst veřejně přístupných budou zřízeny stálé automatické technické systémy, obecní policie vhodným způsobem uveřejnila informace o zřízení takových systémů – jakým způsobem se tak má přesně stát, však zákon již nestanoví; v praxi se tak děje povětšinou informativní kampaní v místních sdělovacích médiích obce. Je taktéž vhodné, ne-li dokonce nutné, podmínky provozování automatizovaného záznamového zařízení vymezit alespoň v interní normě zřizovatele.

V minulosti se objevila otázka, zda mohou kamerové systémy provozovat obce samy, tj. obce, kde není například zřízena obecní policie, a to za účelem ochrany proti vandalismu, boje s kriminalitou, ochrany

[136] Viz text ustanovení § 42f dnes již neplatného zákona č. 283/1991 Sb.:
(1) Policie je oprávněna, je-li to potřebné pro plnění úkolů policie, pořizovat zvukové, obrazové nebo jiné záznamy z míst veřejně přístupných, popřípadě též zvukové, obrazové nebo jiné záznamy o průběhu služebního úkonu nebo služebního zákroku.
(2) Jsou-li k pořizování záznamů podle odstavce 1 zřízeny stálé automatické technické systémy, je policie povinna informace o zřízení takových systémů vhodným způsobem uveřejnit.

bezpečnosti. Jednoznačnou odpověď podalo stanovisko ÚOOÚ č. 2/2008 (zveřejněné ve Věstníku ÚOOÚ č. 49/2008) „K možnosti obcí provozovat kamerový systém se záznamem na veřejných prostranstvích“. Úřad pro ochranu osobních údajů se v souvislosti s registrační povinností správců osobních údajů zabýval problematikou zpracování osobních údajů prostřednictvím záznamu z kamerového systému provozovaného na veřejných prostranstvích (jako jsou například náměstí, ulice) ze strany obce, která nemá vlastní obecní policii, a to za účelem předcházení a odhalování pouliční kriminality, vandalismu a za účelem zajišťování bezpečnosti občanů a návštěvníků obce. Při posuzování takového oznámení o zpracování osobních údajů dospěl v řízení vedeném podle § 17 zákona č. 101/2000 Sb. k závěru, že by se jednalo o zpracování osobních údajů, které je v rozporu se zákonem. S ohledem na fakt, že jde o monitorování veřejně přístupných míst, a to zpravidla ve velkém rozsahu, hrozí tak poměrně zásadní zásah do soukromí občanů. Úřad ve svém stanovisku dovodil, že z tohoto důvodu nelze na situaci aplikovat ani zmocnění dané ustanovením § 5 odst. 2 písm. e) zákona č. 101/2000 Sb.[137] Obec, která by chtěla nainstalovat kamerový systém ve větším rozsahu na veřejných prostranstvích, by tak porušila platné právní předpisy České republiky, protože kamerový systém je v obcích na veřejných prostranstvích možné provozovat jedině prostřednictvím obecní policie nebo Policie České republiky.

Podrobnější vymezení podmínek používání kamerových systémů bývá také běžně upravováno **v obecních vyhláškách**. Např. obecně závazná vyhláška Města Rožnov pod Radhoštěm č. 1/2004, o městské policii stanoví:

[137] Dané ustanovení umožňuje zpracovávat osobní údaje bez souhlasu subjektu údajů pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby; takové zpracování osobních údajů však nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života. ÚOOÚ však dovodil, že o tento případ u obcí nejde. Při jejím hodnocení je třeba vycházet z komplexního posouzení problematiky monitorování veřejných prostranství za účelem zajištění veřejného pořádku a předcházení a odhalování trestné činnosti. Dle názoru Úřadu je zřejmé, že i zákonodárce vnímal „sledování“ občanů na veřejnosti, a to jak státem, tak i jinými subjekty, jako zásah do jejich soukromí, a proto se rozhodl k výslovnému zákonnému zmocnění (např. § 42f odst. 1 zákona č. 283/1991 Sb. a § 24b odst. 1 zákona č. 553/1991 Sb.) pro pořizování obrazových záznamů z veřejně přístupných míst. A contrario, pokud by bylo pořizování obrazových záznamů z veřejně přístupných míst možné provádět na základě obecného předpisu upravujícího ochranu osobních údajů, tedy dle zákona č. 101/2000 Sb., nebyla by tato zvláštní zmocnění vůbec třeba.

Čl.5
Úkoly městské policie

1. Strážníci zabezpečují místní záležitosti veřejného pořádku a plní další úkoly podle zvláštního právního předpisu.

2. **Městská policie zajišťuje obsluhu monitorovacího kamerového systému**, kterým je monitorováno území města. **Monitorované území města je označeno viditelně tabulkami a textem**: "Prostor je nepřetržitě sledován Městskou policií prostřednictvím monitorovacího kamerového systému".

Obecně závazná vyhláška Města Chomutova č. 9/2003, kterou se nově upravuje zřízení městské policie, pak obsahuje následující ustanovení:

Čl.3
Prevence kriminality

Při zabezpečování místních záležitostí veřejného pořádku a prevenci kriminality ve městě využívá městská policie **městského kamerového systému a technických prostředků** oddělení situační prevence kriminality s řídícím centrem umístěným v sídle Městské policie Chomutov.

Konečně i příkladně vyhláška zastupitelstva Města Brna č. 1/1992, kterou se ve městě Brně zřizuje Městská policie podle zákona ČNR č. 553/1991 Sb. říká:

Čl.2

(1)

Při zabezpečování místních záležitostí veřejného pořádku a plnění dalších úkolů podle zákona o obecní policii 1) nebo jiného zákona 2 , 3) Městská policie Brno zejména:

- dohlíží na dodržování obecně závazných právních předpisů o ochraně veřejného pořádku, včetně dodržování vyhlášek statutárního města Brna,
- přispívá k ochraně a bezpečnosti osob a majetku,
- přispívá k ochraně majetku s využitím pultu centrální ochrany,
- **podílí se na provozu městského kamerového systému,**

…

Čl.7

Při plnění úkolů Městské policie Brno, za podmínek a v rozsahu stanoveném v zákoně, je strážník oprávněn:

- …….
- **pořizovat zvukové, obrazové nebo jiné záznamy**
- …….

Ani pokud jde o kamerové sledování, vykonávané obecní nebo státní policií, není možné sledovat soukromé prostory, snímky zveřejňovat nebo je například uvádět na webových stránkách města či obce.[138] Zde je však autor nucen zmínit, že toto se zhusta nedodržuje; řada měst, včetně hlavního města Prahy nabízí na svých stránkách přenosy z některých vybraných

[138] Blíže viz BORGULA, A: Zveřejňování záznamů z městských kamerových systémů, dostupné online na: http://aplikace.mvcr.cz/archiv2008/ministerstvo/opk/servis/leden07.pdf [cit. 2012-01-23]

kamer zařazených do městských kamerových systémů. Je samozřejmě diskutabilní, nakolik je daným zveřejněním porušeno právo konkrétních osob, zda vůbec půjde o zveřejnění osobních údajů ve smyslu zákona č. 101/2000 Sb. Je třeba taktéž zmínit, že často jde jen o komprimované, upravené záběry, neumožňující zaostření obrazu, poskytující jen orientační přehled z dané lokality. Podle mého názoru jde tedy o zveřejnění údajů, které neporušují, alespoň v případě hl. m. Prahy na stránkách http://kamery.praha.eu/Situace.jsp#, zákon o ochraně osobních údajů. Pokud by však byla z dostupných snímků rozpoznatelná konkrétní fyzická osoba, o porušení zákona by se nepochybně jednalo.

Jak je vidět z citací zákonných předpisů, mohou státní policie a městská (obecní) policie využívat pro plnění svých úkolů kamerové systémy. Pokud se tak děje na úrovni města či obce, pro označení těchto monitorovacích systémů se vžil název **městské kamerové dohlížecí systémy (MKDS)**. Tyto jsou pak budovány v úzké spolupráci s orgány dané obce, jakož i jinými subjekty působícími na poli prevence kriminality. Městské kamerové dohlížecí systémy jsou v praxi zřizovány především za účelem prevence kriminality [139], ale jsou využitelné i při mnoha mimořádných událostech, např. i ze strany záchranné služby, hasičů atd. Riziková místa s vyšší mírou kriminality jsou vytypovávána na základě podrobných analýz Policie ČR. Podle zkušeností s používáním městských kamerových systémů se snížily v monitorovaných oblastech případy krádeží aut, vloupání do objektů, přepadení a projevů vandalismu a kriminalita a další negativní jevy se z těchto oblastí vytěsňují jinam. Skutečnost částečného přesunutí kriminality do nemonitorovaných oblastí lze pak nicméně omezit lepší koordinací policejních složek v návaznosti na

[139] Podle Mgr. Gjuričové, ředitelky odboru prevence kriminality Ministerstva vnitra ČR bylo během minulých osmi let ze státního rozpočtu podpořeno 3 188 dílčích projektů programu prevence kriminality částkou více než 550 mil. Kč. V současné době program prevence kriminality realizuje 95 měst České republiky s počtem obyvatel nad 10 tisíc, dalších 43 menších měst program připravuje. V oblasti situační prevence, jejíž úkolem je ztížit dostupnost cílů trestné činnosti, bylo podpořeno 499 projektů částkou 317 316 800,- Kč. Značná část těchto finančních prostředků byla vynaložena na zřizování MKDS - bylo podpořeno 257 projektů MKDS v celkové výši 262 769 000,- Kč. Blíže viz Sborník příspěvků ze semináře "Městské kamerové dohlížecí systémy - účinný prvek prevence kriminality", konaném dne 22.9.2004 v Sokolově, časopis Policista 1/2005, Praha: odbor prevence kriminality Ministerstva vnitra ČR.

poznatky z kamerového systému, jakož i umístěním kamer na příhodných místech a tak, aby nebylo jednoznačně patrné, jakou oblast zabírají.[140]

Kamerový systém tvořený obvykle sítí stacionárních kamerových stanovišť (bodů) může být flexibilně doplňován tzv. mobilními kamerami, které jsou osazovány většinou do předem připravených pozic dle aktuální potřeby. Dále existují tzv. mobilní kamerové soustavy, které využívá a vyhodnocuje prakticky jen Policie ČR, a to na takových místech, kde se bezpečnostní situace velmi rychle mění (sportovní události, masové kulturní akce atd.).

V poslední době se uvažuje **propojit** městský kamerový dohlížecí systém zřizovaný Policií ČR nebo obecní policií také se sledovacím zařízením jiných subjektů, a to včetně soukromých. Takovéto přidružení zařízení jiných subjektů slibuje zejména rozšíření monitorované plochy a tím i akceschopnosti a efektivity při řešení problémů. Jelikož ale sledovací zařízení jiných subjektů nejsou zaměřena primárně k využití pro úkoly Policie ČR či obecní policie, lze o takové integraci hovořit spíše jako o subsidiární, a to zejména pro případy konkrétních výjimečných, předem nadefinovaných událostí. V praxi se také někdy objevuje propojení městského kamerového dohlížecího systému s místním rozhlasem.[141] Policie tak může např. varovat výtržníky či organizovat pomoc při nějaké mimořádné události (oheň, povodeň), kdy má k dispozici aktuální kamerové záběry z postižených míst.

Jak vyplývá z textu zákonného zmocnění pro státní či obecní policii, kamerové systémy provozované těmito subjekty mohou monitorovat pouze **místa veřejně přístupná**. Pro bližší vymezení pojmu místo veřejně přístupné lze použít judikaturu a odborné komentáře pro výklad ustanovení

---

[140] K praktickým otázkám používání městských dohlížecích kamerových systémů (MKDS) se opakovaně vyjadřuje odbor prevence kriminality Ministerstva vnitra České republiky, a to jak na internetu na webu www.mvcr.cz, tak i ve svém časopise Policista. Tento odbor vydal i zásady provozování městského kamerového dohlížecího systému, které jsou použitelné jako návod pro všechny zřizovatele těchto monitorovacích systémů. Nejnovější dokument k otázce kamerových dohlížecích systémů - Aktualizované stanovisko k provozování kamerových systémů obecní policií – právní stav ke dni 10. října 2011 je přístupný online zde: www.mvcr.cz/soubor/kamery-na-web-pdf.aspx [cit. 2012-01-23]
Další informace jsou dostupné zde: http://www.mvcr.cz/clanek/kamerove-systemy.aspx?q=Y2hudW09Mg%3d%3d

[141] Reproduktory místního rozhlasu mají propojeny s kamerovým systémem např. ve Slaném.

§ 202 odst. 1 dříve platného zákona č. 140/1961 Sb. tr. zákona (trestný čin výtržnictví), které tento pojem taktéž používá.[142] Je otázka, zda lze na podrobnější definování pojmu *místo veřejně přístupné* použité v předpisech upravujících použití kamerových systémů, použít legální definici pojmu v ustanovení § 34 zákona č. 128/2000 Sb. o obcích, které říká, že *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.*

Je velmi žádoucí a v praxi se tak prakticky vždy děje, aby byly podmínky a činnost městského kamerového dohlížecího systému podrobněji vymezeny **v interním předpise (směrnici) jeho zřizovatele**. Většinou bývají přijata poměrně rozsáhlá vnitřní opatření (někdy celé komplexy směrnic a řádů), která upravují zejména pracovní náplň obsluhy městského kamerového dohlížecího systému, možnosti ovládání a nastavování kamer, postupy při pozorování scény, vyhodnocování a předávání poznatků, zaškolení obsluhy, postupy a vztahy při součinnosti s dalšími subjekty (zejména pak se složkami integrovaného záchranného systému), stanovení oprávněných osob, které mohou do monitorovacího střediska vstupovat a se systémem nakládat atd. Otázku ochrany údajů získaných při monitoringu pak upravuje institut povinnosti mlčenlivosti dle § 52 zákona o Policii České republiky, resp. dle § 26 zákona o obecní policii.

Městské kamerové dohlížecí systémy jsou většinou provozovány jako **automatizované**. Tím se rozumí zejména možnost přednastavení záběrů kamer v čase, automatické průběžné ukládání záznamů a další činnosti, ke kterým není potřeba lidské obsluhy. Automatizace činnosti

---

[142] Soudní praxe v souvislosti s výkladem ustanovení § 202 tr. zákona považuje za místo veřejnosti přístupné každé z míst, kam má přístup široký okruh lidí individuálně neurčených a kde se také zpravidla více lidí zdržuje. Nejvyšší soud ČR pak v této souvislosti ve svém rozhodnutí ze dne 5.3.2003, sp. zn. 6 Tdo 220/2003 judikoval, že se nemůže jednat o prostor, který je jakkoliv uzavřen některé části obyvatel nebo který by měla možnost navštěvovat pouze malá vymezená část obyvatel, neboť tehdy již není splněna podmínka možnosti přístupu individuálně neurčených lidí. Proto, podle tohoto výkladového názoru, není možné za místo veřejnosti přístupné považovat uzavíratelnou část společných prostor např. panelového domu nebo obydlí podobného typu, které je určeno k bydlení více uživatelů či vlastníků takového domu.
Podle názoru Nejvyššího soudu v jeho rozhodnutí sp. zn. 3 Tdo 969/2002 je pak nutno považovat za místo veřejnosti přístupné podle dikce ustanovení § 202 odst. 1 tr. zák. čekárnu zdravotnického zařízení, přičemž pro posouzení tohoto znaku není důležité, zda jde o zdravotnické zařízení státní nebo soukromé, ani to, jakému režimu podléhají návštěvy v něm.

MKDS pak do značné míry eliminuje lidský faktor v činnosti celého systému. Pracovník obsluhy je nicméně přítomen a má pak více času zaměřit se na konkrétní nestandardní situace.

Při posuzování problematiky z hlediska ochrany soukromého života jednotlivce je pak nutno zaměřit se na to, zda při monitorování veřejně přístupného místa je či může být narušeno **soukromí fyzické osoby**. Je pravda, že osoba vyskytující se na veřejně přístupném místě, navíc řádně informovaná o existenci kamerového systému, nemůže očekávat takovou míru soukromí jako na uzavřeném, neveřejném místě.[143] Pokud jsou veřejné prostory monitorovány necíleně, tj. pokud jsou sledovány všechny osoby vstupující a pohybující se v daném prostoru, je vše v pořádku. Jakmile by se však monitorování zaměřilo na dlouhodobější sledování určitých osob, navíc

---

[143] Evropský soud pro lidská práva se ve věci Peck vs. Spojené království Velké Británie a Severního Irska vyjadřoval k otázce snímání občanů na veřejném prostranství pomocí kamerových dohlížecích systémů:
Stěžovatel, trpící depresemi, se pokusil o sebevraždu v noci na liduprázdné ulici, aniž by tušil, že je filmován kamerou městského kamerového dohlížecího systému. Operátor systému viděl stěžovatele s nožem v ruce, nikoli však jeho pokus i sebevraždu. Zalarmoval policii, která poskytla stěžovateli lékařskou pomoc a pak ho propustila. Městská rada, která instalovala kamerový systém, vydala tiskovou informaci, jejíž součástí byly dvě fotografie stěžovatele pořízené kamerou. Zpráva byla nadepsána "Odvrácené riziko - partnerství mezi MKDS a policií řeší potenciálně nebezpečnou situaci." Fotografie pak byly uveřejněny dvěma regionálními deníky a celostátní televizí (BBC) v relaci nazvané "porážka zločinu". Tvář stěžovatele byla částečně zamaskována, ale tak nedostatečně, že velké množství jeho příbuzných a známých ho poznalo. Nezávislá televizní komise konstatovala, že maskování bylo nedostatečné. Stížnosti podané u tiskové stížnostní komise a u soudu však byly zamítnuty s odůvodněním, že městská rada postupovala dle zákona.
Stěžovatel nenamítal, že monitorování jeho jednání kamerou a vytvoření trvalého záznamu zasáhly do jeho práva na respektování soukromého života. Namítal, že takovým zásahem bylo zveřejnění nahrávky způsobem, který nemohl předvídat.
Soud zjistil porušení čl. 8 Evropské úmluvy o lidských právech a základních svobodách (právo na respektování rodinného a soukromého života, tedy že každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence). Stěžovatel byl sice na veřejné ulici, ale nebyl tam za účelem účasti na veřejné události ani nebyl veřejnou osobou. Bylo pozdě v noci, byl hluboce rozrušen a ve stavu úzkosti. Ačkoli se procházel na veřejnosti s nožem v ruce, nebyl obviněn z porušení zákona. Zveřejnění události, které stěžovatel nemohl předvídat, široce překročilo její veřejný charakter na ulici. Jde o vážný zásah do jeho práva na respektování soukromého života, který nebyl přiměřený ve smyslu čl. 8 odst. 2 Evropské úmluvy (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). Městská rada měla využít jiných možností, jak propagovat účinnost zvoleného systému při odhalování a prevenci trestné činnosti. Když už zvolila případ stěžovatele, měla si od něj vyžádat souhlas se zveřejněním, nebo sama zamaskovat tvář stěžovatele anebo jinak se postarat o vyloučení možnosti jeho identifikace. Zdroj: časopis Policista 1/2005.

dokonce s archivováním těchto vybraných dat, mohlo by se pak již jednat o zásah do soukromí těchto jednotlivců. Je rozhodně žádoucí, aby technologie kamerového systému umožňovala v případě záběru do neveřejných prostor např. rozostření obrazu, případně úplné zablokování těchto neoprávněně pořizovaných záběrů (současné technologie toto již bez problémů umožňují).

Vedle ustanovení § 62 zákona o Policii České republiky se na problematiku kamerových systému zřizovaných Policií ČR vztahují i další ustanovení zákona o Policii ČR. Jsou to zejména ustanovení uvedená v hlavě X. nazvané *Práce s informacemi.*

Ustanovení § 24a zákona o obecní policii zakotvuje zpracovávání osobních údajů, které obecní policie potřebuje k plnění úkolů podle tohoto nebo zvláštního zákona.

Lze tedy uzavřít, že provozování bezpečnostních kamerových systémů obecní či státní policií není z důvodu existence zákonného zmocnění neoprávněným zásahem do soukromého či rodinného života ani zásahem do soukromí jednotlivce a jako takové není v rozporu s čl. 8 Úmluvy o ochraně lidských práv a základních svobod, ani s čl. 7 odst. 1 a čl. 10 odst. 2 Listiny základních práv a svobod. Vždy je však nutno **poměřovat** oprávnění policie k užívání kamerových systémů s ohledem na ústavně zaručené právo na soukromí. Je však otázka, zda by neměla být právní úprava používání kamerových systémů a jiných technických zařízení pro monitorování míst či situací pregnantnější a detailnější. Často se hovoří o uzákonění režimu a podmínek nakládání se záznamy, stanovení jasné doby uchovávání záznamů, určení toho, co má být archivováno a co ne atd. V praxi jsou sice skoro vždy tyto otázky řešeny určitým interním aktem zřizovatele automatizovaného technického systému, v zájmu zvýšení garancí práva na soukromí jednotlivců by však bylo vhodnější zakotvit danou problematiku v právní normě o síle zákona či alespoň podzákonného prováděcího předpisu.

Patrně nejpropracovanější a nejrozsáhlejší městský kamerový systém existuje v ČR v hlavním městě Praze.

4.4.1 Městský kamerový systém hl. m. Prahy

V Praze je městský kamerový systém budován již od roku 1997. Koordinaci a financování výstavby Městského kamerového systému převzalo Hlavní město Praha. Postupná další výstavba a rozvoj Městského kamerového systému (dále i jen jako „MKS“) probíhá v souladu s "Koncepcí rozvoje Městského kamerového systému Hl. m. Prahy" schválenou usnesením číslo 22/13 z 5. 10. 2000 Zastupitelstva Hlavního města Prahy.[144] MKS v současné době představuje poměrně složitý mechanismus systémů, koncipovaný však jako otevřený metropolitní systém s víceuživatelským přístupem.[145]

Celkem je ke dni 23.1.2012 na území hlavního města Prahy umístěno 639 kamerových stanovišť a 61 monitorovacích pracovišť MKS. Tento počet se samozřejmě neustále zvyšuje, aktuální stav by měl být dostupný vždy na stránkách hl. m. Prahy.[146]

---

144 Hned na úvod se samozřejmě nabízí otázka, kdo přesně je zřizovatelem, či provozovatelem MKS? Podle zákona o obecní policii, či zákona o Policii ČR, které byly citovány výše, by kamerový systém měla provozovat přímo obecní policie či Policie ČR. Zdá se však, že MKS je provozován přímo hl. m. Prahou, konkrétně se jako zodpovědný, výkonný subjekt zaštiťující veškeré aktivity spojené s MKS zmiňuje odbor krizového řízení Magistrátu hl. m. Prahy. Lze dohledat, že konečným příjemcem dotací na projekt MKS je právě tento odbor. Na stránkách magistrátu se pak přímo uvádí:

Projekt JPD2 - Městský kamerový systém hlavního města Prahy:

Na přípravě a realizaci projektu se vedle Magistrátu hlavního města Prahy podílejí i tito partneři:

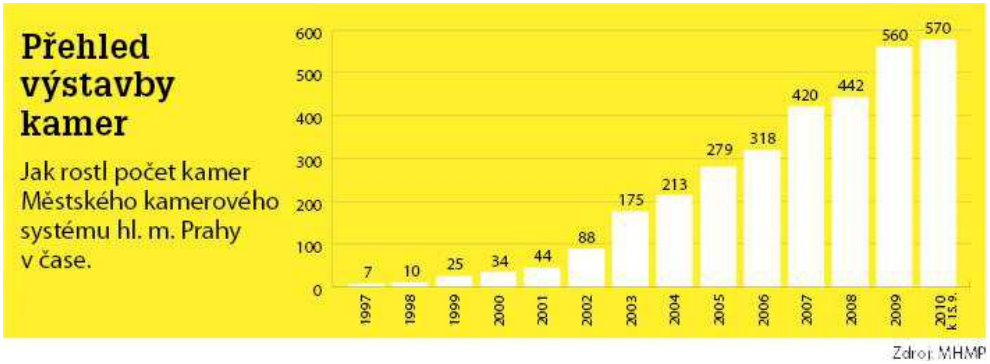
- Policie České republiky – správa hl. m. Prahy
- Městská Policie hlavního města Prahy
- Zdravotnická záchranná služba hl. m. Prahy - územní středisko záchranné služby
- atd.

http://www.praha.eu/jnp/cz/home/magistrat/odbory_mhmp/dopravy/projekty_jpd2/projekt_jpd2_mestsky_kamerovy_system.html.

Za vlastníka systému MKS pak v jedné odpovědi na dotaz žadatele o informaci označilo Krajské ředitelství policie hl. m. Prahy, Integrované operační středisko právě Magistrát hl. n. Prahy. Viz http://www.policie.cz/clanek/sprava-hl-m-prahy-vyzadane-informace-odpoved-krajske-reditelstvi-policie-hl-m-prahy-integrovane-operacni-stredisko.aspx

145 Finanční prostředky vynaložené na výstavbu MKS k 1.1.2010 činí celkem částku ve výši 866.270.000,- Kč, naprostá většina prostředků byla alokována z rozpočtu hl.m.Prahy, zhruba 1/10 pak z rozpočtu jednotlivých městských částí a necelá 1/10 pak z dotací EU a dotací státního rozpočtu.

146 Viz podrobné informace na webových stránkách Magistrátu hl.m.Prahy, odboru krizového řízení dostupných na http://www.praha.eu/jnp/cz/home/magistrat/odbory_mhmp/krizoveho_rizeni/krizove_rizeni/mestsky_kamerovy_system.html



Zdroj: MHMP

Do Městského kamerového systému hl.m. Prahy jsou zahrnuty také kamery Technické správy komunikací Praha a Dopravního podniku hl.m. Prahy.

Kamerový systém Technické správy komunikací (TSK) – TVD zajišťuje monitorování dopravy na křižovatkách a ostatních komunikacích pomocí kamer pro potřeby řízení dopravy. Počet provozovaných kamer v systému Technické správy komunikací (TSK) hlavního města Prahy je aktuálně přes 260 a jsou používané na křižovatkách a v tunelech.

Počet provozovaných kamer v systému Dopravního podniku (DP) hlavního města Prahy je více než 950. Kamerový systém Dopravního podniku je na území hlavního města instalován převážně k následujícím účelům:

- monitorování situace zejména v DP Metro převážně pevnými přehledovými kamerami,
- monitorování situace na povrchu u DP Metro, zejména u navazujících nástupišť povrchové dopravy převážně přehledovými, otočnými a pevnými kamerami,
- kamery sledující provoz na autobusových a tramvajových terminálech a zastávkách a sledujících situaci pro potřeby policie.

Standardní typy kamer zapojovaných do MKS jsou tzv. přehledové kamery, dále pevné analogové a IP kamery a konečně HDTV kamery s infračervenými reflektory umožňují detekci SPZ/RZ s využitím pro měření rychlosti a kontroly jízdy na červenou.

K MKS existuje přístup přes tzv. monitorovací pracoviště, jedná se prakticky o všechna pracoviště Záchranného bezpečnostního systému hlavního města Prahy, konkrétně jde o tyto subjekty:

- operační středisko Policie ČR - Krajské ředitelství policie hl. m. Prahy
- operační střediska Obvodních ředitelství Policie ČR - Praha I až Praha IV
- operační středisko Policie ČR - Národní protidrogové centrály
- Centrální operační středisko Městské policie hl. m. Prahy
- operační střediska Obvodních ředitelství Městské policie Praha 1 až Praha 15
- operační středisko Krizového štábu hl. m. Prahy
- operační středisko Dopravní řídící ústředny hl. m. Prahy
- centrální dispečink Dopravního podniku hl. m. Prahy
- Krajské operační a informační středisko Hasičského záchranného sboru hl. m. Prahy
- operační středisko Zdravotnické záchranné služby hl. m. Prahy - zdravotnické operační středisko ZZS
- dispečink Technické správy komunikací hl. m. Prahy

Pokud jde o dobu uchovávání záznamů a jejich kvalitu, záznamy z MKS jsou uchovávány až po dobu 30 dnů v počtu min. 5 snímků za vteřinu pro každou kameru. Datové úložiště má k dispozici celkovou kapacitu 10 TB pro každých 16 kamer. Operativní datová úložiště jsou na operačních střediscích OS PČR Praha I až IV a OS PČR Praha I. [147]

[147] Některé údaje byly kromě webových stránek Magistrátu hl. m. Prahy převzaty i ze studie „Bezpečné město Praha 13“ zpracované společností AB via s.r.o. a dostupné na webu internetového deníku Česká pozice online na http://www.ceskapozice.cz/sites/default/files/bezpecna_praha13_-_studie_v11_2011.pdf [cit. 2012-01-23].
V této souvislosti je třeba zmínit, že projekt MČ Praha 13 „Bezpečné město Praha 13“ je nicméně kritizován za jeho přílišnou nákladnost. V září 2011 byla dokončena první fáze projektu „Bezpečná Praha 13“ - spočívala v osazení 31 objektů mateřských a základních škol celkem 352 stacionárními kamerami s nahrávacím zařízením. Aktuální studie od ABvia navrhuje instalaci celkem 155 nových kamer. Z toho 96 stacionárních do šesti lokalit: po šestnácti kamerách by měly získat objekty Hasičské zbrojnice Červeňanského, kulturní dům Mlejn, MŠ Bronzová, Středisko sociálních služeb Lukáš, Poliklinika Lípa a připravovaná parkovací rampa v ulici Klausova. Dále

Z hlediska iformovanosti sledovaných osob, MKS prozatím nabízí možnost zjistit, kde obecně jsou kamery instalovány na webových stránkách Magistrátu hl. m. Prahy, uvažuje se i o označení monitorovaných míst samolepkami s piktogramy na chodníku.

4.4.2 Další kamerový monitoring ze strany Policie ČR a obecní policie

V této kapitole bych ještě k danému tématu chtěl zmínit několik oblastí, které vyvolaly v minulosti spory. Šlo zejména o měření rychlosti a současné pořizování obrazových záznamů vozidel a řidičů. Úřad na ochranu osobních údajů v dané věci při jedné ze svých kontrol v roce 2009 deklaroval, že *„tento způsob měření rychlosti však současně zpracovává i osobní údaje osob, které se nedopustily přestupku, a proto je toto nepřetržité sledování všech projíždějících vozidel silným zásahem do soukromí jednotlivce a jeho umístění musí být podloženo skutečnou nebezpečností daného úseku vyvolávající potřebu stálého dozoru. Úřad není kompetentní k posuzování oprávněnosti volby daných míst.“* Kontrola v daném případě také uložila zcela odstranit obrazovou informaci o spolujezdci.

V této souvislosti nemohu nezmínit zajímavý judikát rakouského ústavního soudu z 15.6.2007, který rozhodoval o stížnosti fyzické osoby, jíž byl správním orgánem vyměřen trest za to, že na dálnici A22 v tunelu Kaisermühlen překročila maximální povolenou rychlost. Ústavní soud pak v rozhodnutí uvedl několik zajímavých právních postřehů k této tematice, jež se nepochybně mohou za určitých podmínek vztahovat i na české právní prostředí:

- **část dat získaných úsekovými kontrolami jsou osobní údaje** ve smyslu rakouského zákona a nakládání s nimi podléhá zákonu o ochraně osobních údajů

---

se počítá s 59 otočnými kamerami s možností přibližování. Součástí navrhované fáze „Bezpečné Prahy 13“ a 130milionové investice má být rovněž vybudování centrálního dohledového centra, které by mělo být kompatibilní s městským kamerovým systémem pražského magistrátu.

- státní správa a policie jsou oprávněny **zaznamenávat osobní údaje jen po dobu, která je nezbytně nutná pro naplnění účelu, pro který byla získána** a pak jsou povinny zajistit jejich smazání
- **provozovatel systému úsekových kontrol nemá k dispozici pověření**, které by jej opravňovalo k provádění měření a nesplňuje tak požadavek rakouského práva, že předání výkonu dohledu nad silničním provozem od policie na jiný subjekt je možné pouze na základě pověření ministrem vnitra
- definice "v určitých úsecích" **nedovoluje instalaci úsekových kontrol na celém území spolkové země**; základem pro instalaci úsekových kontrol je podložené zjištění, že na hlídaném úseku je obzvláště nutné sledovat dodržování nejvyšší dovolené rychlosti, aby se předešlo vzniku mimořádně nebezpečných situací
- z rakouského zákona na ochranu informací plyne, že **sběr osobních údajů**, v tomto případě o řidičích, **musí být prováděn předvídatelnou formou a to jak ohledně času, tak ohledně místa.**[148]

V České republice se soudy přípustností důkazů získaných kamerovým systémem při měření rychlosti již také zabývaly. Jistý P.P. se údajně dopustil přestupku překročení maximální dovolené rychlosti v březnu 2008 a zaplatil pokutu. Později v roce 2010 zjistil, že získaný důkaz, totiž záznam o měření rychlosti vyhotovený údajně městskou policií, je pravděpodobně výsledkem činnosti soukromého subjektu Czech Radar, a žádal o obnovu řízení, čemuž bylo po projednání věci ve správním soudnictví vyhověno. Soud ve své argumentaci uvedl, že pokud bylo měření výsledkem činnosti soukromé osoby, nelze výsledek takového měření užít jako důkaz v řízení o přestupku podle zákona o přestupcích s přihlédnutím k

[148] Rozhodnutí rakouského ústavního soudu k této otázce v německém jazyce je dostupné na webových stránkách rakouského Ústavního soudu (Verfassungsgerichtshof) na: http://www.vfgh.gv.at/cms/vfgh-site/attachments/8/9/4/CH0006/CMS1183626340872/section_control_g147-06.pdf [cit. 2012-02-13]. Další informace k případu v českém jazyce viz http://www.osbid.org/index.php?t=article&n=clanek-usekove-mereni-rychlosti-v-rakousku--53 [cit. 2012-02-13] a zde http://vseorakousku.cz/titulni_strana/novinky/rakousky_ustavni_soud_usekove_mereni_rychlosti_je_nezakonne/ [cit. 2012-02-13].

ust. § 79 odst. 8 zákona č. 361/2000 Sb. Pokud by takové měření bylo jako důkaz užito, pak by se jednalo o důkaz opatřený v rozporu se zákonem, a tudíž nepoužitelný v daném řízení.

Vedle úsekového měření rychlosti jsou kamerové systémy Policií ČR a případně i obecní policií dále využívány v dopravě například při monitorování možného průjezdu křižovatky na červenou. V ČR byly již v roce 2007 zavedeny na dálnicích a dalších významných silnicích tzv. mýtné brány. Ty obsahují mimo jiné i kamerové systémy. Do budoucna se počítá s jejich využitím pro měření rychlosti. Již nyní jsou ale data z kamer přístupná policejním orgánům, veřejně policejní orgány přiznaly využití určitých záznamů z kamer mýtných bran v mediálně známé kauze dopadení uprchlého Tomáše Pitra.[149] Například v Německu však Ústavní soud využití záznamů z kamer instalovaných v četných mýtných branách z důvodu kolize s právem na ochranu soukromí zakázal.[150]

4.5 Obrazový monitoring na pracovišti

4.5.1 Ochrana soukromí zaměstnance versus oprávněné zájmy zaměstnavatele

Zapojení do pracovního procesu přináší na jedné straně pro každého člověka nové obzory, nové sociální role a přístupy, na straně druhé je také nepochybně potenciálním zásahem do soukromí, neboť člověk je vystaven pracovním záležitostem mnohdy i ve svém soukromí (telefonáty, emaily a jiné kontakty po skončení pracovní doby atd.). Na druhu pracovní činnosti pak také záleží zájem zaměstnavatele na výsledcích práce a ruku v ruce s tím jde i kontrola práce zaměstnance a snaha o monitorování hospodaření se svěřenými prostředky.

---

149 Viz zpravodajský článek na portále Idnes dostupný online na: http://technet.idnes.cz/jak-velky-bratr-zatkl-pitra-pomohly-mytne-brany-i-skype-pjk-/tec_technika.aspx?c=A100813_101728_tec_technika_vse [cit. 2012-02-13].

150 Německý ústavní soud například ve svém rozhodnuté 1 BvR 2074/05; 1 BvR 1254/07 ze dne 11.3.2008 prohlásil nařízení spolkového státu Schleswig-holstein upravující používání automatických systémů rozpoznávající registrační značky nákladních vozidel za neplatné – rozhodnutí dostupné v německém jazyce na: http://www.bundesverfassungsgericht.de/entscheidungen/rs20080311_1bvr207405.html [cit. 2012-02-13].

V poslední době se zejména s rozvojem informačních technologií stal z výše uvedeného problém, který by mohl ve velké míře zasáhnout soukromou sféru jednotlivce. Pro zaměstnavatele dnes není technický problém podrobně sledovat práci zaměstnance na svěřené počítačové technice, má také přístup k údajům o provedených telefonních hovorech (nedochází-li dokonce přímo k samotnému odposlechu a nahrávání hovorů zaměstnavatelem).

Soudy, zejména pak Evropský soud pro lidská práva, judikovaly, že soukromí jednotlivce nekončí v pracovním procesu, nýbrž zaměstnanec naopak oprávněně očekává, že bude **přiměřeně zachováno jeho právo na ochranu jeho soukromí**, jehož součástí je i právo na ochranu jeho osobních údajů, také v pracovněprávních vztazích a že tato práva bude zaměstnavatel respektovat.[151]

Například i otázka zavedení moderního čipového sledování docházky může v některých případech znamenat narušení soukromé sféry zaměstnance.[152]

Jelikož však má i zaměstnavatel často oprávněný a legitimní zájem na sledování práce zaměstnance za účelem jeho kontroly a dodržení bezpečnostních pravidel, stejně tak i za účelem ochrany zaměstnavatele před vznikem jakékoliv škody, která by mohla nastat v souvislosti s prací

---

[151] Viz například rozhodnutí ESLP, ve věci Niemietz proti Německu, č. stížnosti 13710/88. Ve věci Niemietz versus Německo Evropský osud pro lidská práva deklaroval, že by bylo nepřiměřené omezovat pojem soukromého života na "vnitřní kruh", ve kterém může jednotlivec žít svůj vlastní osobní život, jaký si vybral, a vyloučit z něj svět, který nezapadá do této oblasti, přičemž respekt k soukromému životu musí rovněž zahrnovat jistý stupeň práva ustavovat a rozvíjet sociální vztahy s ostatními lidskými bytostmi.
Dále k dané problematice existují rozhodnutí Evropského soudu pro lidská práva ve věci Halford v. The United Kingdom ze dne 25. 6. 1997 stížnost c. 20605/92 nebo též Klass and Others v. Germany ze dne 6. září 1978, stížnost c. 5029/71.

[152] V dubnu 2005 bylo vydáno zajímavé rozhodnutí francouzského Nejvyššího soudu, kterým bylo zakázáno zavedení kontroly pracovní doby zaměstnanců pomocí biometrického systému. Jistá francouzská firma chtěla kontrolovat docházku svých zaměstnanců pomocí systému využívajícího otisky prstů. Předem řádně informovala své zaměstnance a věc konzultovala s francouzským Úřadem na ochranu dat i s podnikovou radou. Nejvyšší soud však usoudil, že byť byly dojednané podmínky provozování monitorovacího systému dodrženy, došlo k porušení principu přiměřenosti. Nasazení takovéto technologie není v případě běžné kontroly docházky zaměstnanců odůvodnitelné, zejména s ohledem na francouzský zákoník práce, který zmiňuje zásadu proporcionality mezi kontrolou zaměstnance a sledovaným účelem, a dále i s ohledem na evropské směrnice o ochraně osobních údajů. Podrobnosti případu viz Informační bulletin Úřadu pro ochranu osobních údajů č. 2/2005, s. 13-14 nebo internetové stránky francouzského Úřadu pro ochranu dat www.cnil.fr.

zaměstnance, je z tohoto důvodu nutno nalézt **přiměřenou rovnováhu** mezi těmito zaměstnavatelovými požadavky na sledování zaměstnance a právem zaměstnance na respektování jeho soukromí. Při hledání konsensu mezi těmito dvěma požadavky by se měl uplatnit zejména **princip přiměřenosti.**

V českém právním řádu dlouho neexistoval žádný právní předpis, který by nějakým způsobem relevantně upravoval podmínky eventuelního monitorování zaměstnance různými technickými prostředky, např. formou kamerových systémů, odposlechem a sledováním elektronické komunikace či kontrolou využívání internetových prohlížečů zaměstnanci. Daný stav byl odrazem především toho, že v oblasti pracovního práva neexistoval modernější komplexní předpis – od roku 1965 platil, byť s poměrně velkými dílčími změnami, zákon č. 65/1965 Sb. (zákoník práce).

Tento právní předpis však prakticky nijak nereflektoval bouřlivý rozvoj informačních technologií a problémy s tím související. Praxe si tak musela při výkladu možností sledování práce a činnosti zaměstnance většinou vypomáhat právními normami z jiných odvětví práva pomocí výkladového pravidla „analogia iuris“. Především se na situaci aplikovala Listina základních práv a svobod v jejích částech chránících soukromou sféru jednotlivce, dále ustanovení občanského zákoníku - § 11 a násl. o ochraně osobnosti a taktéž se podpůrně používaly mezinárodní předpisy závazné pro Českou republiku (zejména Evropská úmluva o ochraně lidských práv a základních svobod a související judikatura Evropského soudu pro lidská práva). Na straně druhé oprávnění zaměstnavatele kontrolovat a sledovat své zaměstnance pomocí moderních sledovacích technologií se dovozovala z obecnějších ustanovení tehdy platného zákoníku práce, zejména ustanovení, jež dávala zaměstnavateli právo, aby prováděl kontrolu věcí, které zaměstnanci vnášejí nebo odnášejí od zaměstnavatele (§ 170 odst. 3 dříve platného zákoníku práce – zákona č. 65/1965 Sb.), a to včetně prohlídek zaměstnanců; jiné ustanovení stanovilo, že zaměstnavatel je povinen soustavně kontrolovat, zda zaměstnanci plní své pracovní úkoly tak, aby nedocházelo ke škodám (§ 170 odst. 2); ustanovení § 74 pak dávalo pravomoci vedoucím zaměstnancům ke kontrole jednotlivých zaměstnanců. Zákon č. 65/1965 Sb. zákoník práce ve znění

pozdějších předpisů byl však po dlouhé diskusi nahrazen s účinností k 1.1.2007 **novým zákoníkem práce**.

4.5.2 Právní úprava sledování na pracovišti dle zákona č. 262/2006 Sb.

Pro jasnější vymezení situace v otázce sledování zaměstnanců pomocí technických sledovacích prostředků tedy bylo zásadní až přijetí nového zákoníku práce – zákona č. 262/2006 Sb. ze dne 21.4.2006 (dále v textu i jen jako „zákoník práce“). Tato základní pracovněprávní norma poprvé v historii České republiky **komplexněji upravuje institut ochrany soukromí zaměstnance**, kdy deklaruje a zaručuje zaměstnanci soukromí, ale současně dává zaměstnavateli možnost zásahů do soukromí v případě závažných důvodů spočívajících na straně zaměstnavatele. Problematika je v novém zákoníku práce upravena v **§ 316** zařazeném do části třinácté (Společná ustanovení) hlavy VIII., nazvané Ochrana majetkových zájmů zaměstnavatele a ochrana osobních práv zaměstnance. Z názvu a taktéž ze znění prvního odstavce § 316 je patrné, že zákonodárce řeší problematiku ochrany soukromí zaměstnance zejména z pohledu souvisejícího **s ochranou majetkových práv zaměstnavatele.**

Podle prvního odstavce daného paragrafu 316 platí, že zaměstnanci nesmějí bez souhlasu zaměstnavatele užívat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele včetně výpočetní techniky ani jeho telekomunikační zařízení. To, zda je tento zákaz dodržován, je pak zaměstnavatel oprávněn **přiměřeným způsobem kontrolovat.** Může se tak dít například tzv. rámcovým sledováním komunikace. Zaměstnavatel tedy v zásadě smí sledovat datum, čas a dobu trvání komunikace a může zjišťovat, s kým zaměstnanec komunikoval. Nikdy však nesmí sledovat obsah komunikace. Běžná byla dosavadní praxe řady zaměstnavatelů, kteří pomocí různých technických zařízení či v součinnosti s poskytovateli služeb elektronických komunikací zjišťovali například, na která telefonní čísla zaměstnanec volal. V případě, že zaměstnanec využíval telefonu či jiného zařízení na pracovišti k soukromým účelům, na základě zjištěných údajů pak

po zaměstnanci požadoval náhradu škody (např. úhradu nákladů soukromých telefonátů).[153]

Druhý odstavec již však zakotvuje z obecnější roviny na druhé straně **zákaz pro 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.** Průlom do této zásady je pak možný jen na základě závažného důvodu spočívajícího **ve zvláštní povaze činnosti zaměstnavatele**. Tímto závažným důvodem pak budou podle J. Matejky zřejmě takové činnosti zaměstnavatele, u kterých je nutno dbát zvýšených nároků na chování zaměstnanců (např. vzhledem k ochraně utajovaných skutečností, povinnosti mlčenlivosti, ochraně obchodního tajemství, know how apod.).[154] Já se osobně domnívám, že byť to dané ustanovení přímo nezmiňuje, na situaci se bude moci bezpochyby aplikovat i zásada přiměřenosti. V jejím rámci tak bude vždy nutné poměřovat odůvodnitelnost zvolené formy sledování zaměstnance, jakož i otázku, zda nelze požadovaného cílu dosáhnout i jinak. Oproti prvnímu odstavci § 316 vidíme tedy možnost mnohem širšího a detailnějšího monitorování zaměstnanců, jejich aktivit, včetně obsahu jejich komunikace s třetími subjekty.

Odstavec třetí posuzovaného ustanovení dále upřesňuje, že i v případě, že je u 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.**

Čtvrtý odstavec § 316 nového zákoníku práce pak **zakazuje zaměstnavateli vyžadovat od zaměstnance informace, které bezprostředně nesouvisejí s výkonem práce a s pracovněprávním**

---

[153] Vždy však bude záležet na důkazní situaci, neboť pouze na základě samotného čísla volaného účastníka nelze pokaždé automaticky dovodit, že šlo o soukromý telefonát. Viz JOUZA, J.: Zákoník práce s komentářem. 2. vydání. Praha: BOVA POLYGON, 2007, str. 657.

[154] Viz článek J. Matejky: Ochrana soukromí na pracovišti dle zákona č. 262/2006 Sb., In: IT Právo – server o internetovém a počítačovém právu. [online]. Praha: Společnost pro právo informačních technologií (SPIT) [cit. 2012-02-18]. Dostupný z www: http://www.itpravo.cz, ISSN: 1801 4089

vztahem. Ustanovení dává příkladmý (tedy ne taxativní) výčet dvou skupin informací. Do první skupiny patří informace o sexuální orientaci, původu, členství v odborové organizaci, informace o členství v politických stranách nebo hnutích, nebo o příslušnosti k církvi nebo náboženské společnosti – tyto informace nesmí zaměstnavatel vyžadovat od zaměstnance nikdy. Pak existuje druhá skupina informací, které může zaměstnavatel po zaměstnanci požadovat, jestliže je pro to dán věcný důvod spočívající v povaze práce, která má být vykonávána, a je-li tento požadavek přiměřený, nebo v případech, kdy to stanoví tento zákon nebo zvláštní právní předpis. Do této druhé skupiny demonstrativně vyjmenovaných informací jsou zařazeny informace o těhotenství, o rodinných a majetkových poměrech, a informace o trestněprávní bezúhonnosti.

4.5.3 Provozování kamerových systémů na pracovišti

Přípustnost sledování zaměstnanců pomocí kamerových systémů byla zvlášť v posledních letech předmětem široké diskuse. Na toto téma byla vydána řada dílčích pojednání a názorů. Důvodem široké diskuse nad tématem byla zejména skutečnost absence jasného zákonného vymezení přípustnosti zavedení kamerového sledování zaměstnanců. Jak již bylo zmíněno, původní zákoník práce upravoval otázku sledování zaměstnanců jen velmi okrajově, zejména s akcentem na oprávnění zaměstnavatele kontrolovat práci svých zaměstnanců. Oproti tomu bylo stavěno právo zaměstnance na zachování svého soukromí i na pracovišti.[155]

Zejména pak po vydání Zásad provozování kamerového systému z hlediska zákona o ochraně osobních údajů, které publikoval Úřad pro ochranu osobních údajů, se názory na dané téma většinou ustálily na vyslovení přípustnosti instalování kamerových systémů v případě, že to vyžaduje oprávněný zájem zaměstnavatele a budou současně splněny podmínky dané zákonem o ochraně osobních údajů (v případě, že kamerový

[155] K tématu viz např. Hansel, M.: Problém kamerových systémů instalovaných zaměstnavatelem, Právo a podnikání č. 9/2003, s. 6; Matejka, J.: K oprávnění zaměstnavatele kontrolovat práci zaměstnance pomocí moderních technologií, Právo a zaměstnání č. 5/2003, s. 7, Jouza, L.: Ochrana soukromí na pracovišti, Právní rádce č. 5/2003, s. 29.; Štefko, M.: Může zaměstnavatel sledovat své zaměstnance?, Národní pojištění č. 12/2004, s. 5 atd.

systém bude pořizovat záznamy), přičemž však každý případ musí být posuzován z hlediska práva zaměstnance na své soukromí.

Podle platné právní úpravy v zákoníku práce, která byla citována výše v této práci, je třeba rozlišovat v zasahování do soukromé sféry zaměstnance případ, kdy zaměstnavatel přiměřeným způsobem **kontroluje zákaz užívání** výrobních a pracovních prostředků zaměstnavatele včetně výpočetní techniky a jeho telekomunikační zařízení pro svou osobní potřebu bez souhlasu zaměstnavatele. Druhým zásahem do soukromí zaměstnance je pak případ **přímého sledování zaměstnance**, a to otevřeným či skrytým sledováním, odposlechem a záznamem jeho telefonických hovorů, kontrolou elektronické pošty nebo kontrolou listovních zásilek adresovaných zaměstnanci. U obou dvou případů jde o zcela různé účely, pro něž se sledování provádí. Zatímco v prvním případě jde o zabránění zneužívání majetku zaměstnavatele, v druhém případě je účelem sledování zvláštní povaha činnosti zaměstnavatele, vyžadující kontrolu zaměstnanců.

Tímto závažným důvodem spočívajícím ve zvláštní povaze činnosti zaměstnavatele bude zejména případ takových činností zaměstnavatele, u kterých je nutno dbát zvýšených nároků na **chování zaměstnanců** (např. vzhledem k ochraně utajovaných skutečností, povinnosti mlčenlivosti, ochraně obchodního tajemství, know how, apod.). Jednou z možností sledování zaměstnanců je instalace kamerového systému. Otázkou i nadále nicméně zůstává, **zda může zaměstnavatel na pracovišti například instalovat kamerový systém v situaci, kdy nebude dán závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele**, tak jako to požaduje § 316 odst. 2 zákoníku práce v platném znění. Může jít příkladmě o monitorování prostor prodejny či školského zařízení. V těchto případech zřejmě nepůjde o zvláštní činnost zaměstnavatele, která by odůvodňovala nutnost sledování zaměstnanců. Kamerový systém bude vyžadován nikoliv primárně za účelem sledování chování zaměstnanců, nýbrž z jiných oprávněných důvodů, jako je například zajištění bezpečnosti v daných prostorách, ochrana před krádežemi či vandalismem, ochrana před šikanou atd. Prostory pracoviště, a tím pádem chtě nechtě i zaměstnanci přítomní na pracovišti, budou tak monitorováni jako celek. I v tomto případě bude instalování sledovacích technologií zřejmě odůvodnitelné, nelze-li jeho

účelu dosáhnout jinak, vždy však bude záležet na konkrétních okolnostech. Na situaci se bude v případě pořizování záznamů bezpochyby vztahovat režim zákona o ochraně osobních údajů č. 101/2000 Sb. a rozhodně bude více než vhodné i nadále aplikovat i Zásady provozování kamerových systémů vydané Úřadem pro ochranu osobních údajů. Podle mého názoru tedy platí, že i v případě, kdy nebude splněna podmínka závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele pro narušení soukromí zaměstnance, bude možné, tak jako tomu bylo doposud, používat kamerové systémy na pracovišti i z důvodu jiných oprávněných zájmů zaměstnavatele. O to více než před přijetím nové právní úpravy v zákoníku práce však bude nutno poměřovat přípustnost instalace kamer z hlediska ústavně garantovaného práva na soukromí zaměstnanců. Stěží lze připustit argument, že kamery monitorují prostory nikoliv za účelem sledování zaměstnanců, nýbrž z důvodu ochrany majetku a zajištění bezpečnosti a že zaměstnance nikdo nesleduje. Pokud budou zaměstnanci podrobeni soustavnému dozoru kamer, kdy budou navíc pořizovány záznamy z monitorování, půjde bez ohledu na skutečný účel využívání kamer v každém případě o zásah do soukromí zaměstnanců a ten je v tomto případě odůvodnitelný jen za splnění řady podmínek.

V následujícím textu se pokusím vymezit základní podmínky instalování kamerového systému na pracovišti, a to zejména s ohledem na ochranu osobních údajů. Budu se zabývat spíše obecnějšími otázkami provozu kamerového systému, zejména v souvislosti s ochranou soukromí a s ochranou osobnosti zaměstnance ve smyslu § 11 a násl. občanského zákoníku. V zásadě je i na pracovišti možné provozovat kamerový systém tzv. **bezzáznamově**, kdy bude docházet k průběžnému sledování záběrů kamer k tomu určeným pracovníkem, nebo **s pořizováním obrazových či i zvukových záznamů**, kdy budou záběry kamer archivovány na datová média.

4.5.3.1 Provozování kamerových systémů bez pořizování obrazových záznamů

V tomto případě se zákon na ochranu osobních údajů neuplatní – nejde totiž o pořizování a shromažďování záznamů (a tedy ani o zpracování osobních údajů). Poněkud sporné však může být, zda se bude jednat o zásah do osobnostních práv zaměstnance ve smyslu § 11 a násl. obč. zákoníku. I když totiž nepůjde o pořizování záznamů či snímků, které by byly následně uchovávány na hmotných nosičích, dalo by se takovéto monitorování podřadit pod obecnější § 11 o.z., který chrání osobnost jednotlivce jako celek. Soustavné sledování a monitorování konkrétní osoby, navíc v uzavřeném prostoru, by již takovým zásahem do osobnostních práv nepochybně bylo. Dokonce, i když nebudou z kamerového systému pořizovány záznamy, jeho instalace je po nabytí účinnosti nového zákoníku práce přípustná pouze v případech stanovených § 316 zákoníku práce, tj. buď za účelem kontroly případného zneužívání pracovních prostředků zaměstnavatele, nebo za účelem sledování zaměstnanců z jiného závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele.

Sledování bude však také možné, jak bylo naznačeno výše, i v případech ochrany jiných oprávněných zájmů zaměstnavatele (ochrana pracoviště před vandalismem, krádežemi apod., tj. nikoliv závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele). Tento poslední případ byl před přijetím nové právní úpravy dané zákonem č. 262/2006 Sb. ostatně pro ospravedlnitelnost instalace kamerové kontroly důvodem jediným. I nadále však jej lze dle mého názoru aplikovat. Co se však mění, je nepochybně **zákaz skrytého monitorování zaměstnanců** bez jejich vědomí z jiného důvodu než je zákonný podklad v § 316 odst. 2 zákoníku práce. Pokud tedy bude kamerový systém instalován například z důvodu ochrany prostor před vandalismem či krádežemi, zaměstnanci budou muset být o sledování určitě informováni.

Vždy bude nutné poměřovat míru potenciálního zásahu do soukromí zaměstnanců a eventuelně dalších osob, vyskytujících se na pracovišti, a to zejména s ohledem na charakter a využívání monitorovaných prostor:

vnější prostory, parkoviště, vstupy, schodiště, chodby – riziko omezení soukromí minimální, souhlas zaměstnanců nebude třeba, přesto s ohledem na slušnost a korektnost je vhodné alespoň **upozornění** na instalovaný kamerový systém

kanceláře – z důvodu potenciální možnosti zásahu do soukromí je vhodný **souhlas zaměstnanců**, alespoň konkludentní (zaměstnavatel vyhlásí, kde a proč budou instalovány kamery a vymezí lhůtu, ve které mohou zaměstnanci vyjádřit svůj nesouhlas; po uplynutí lhůty lze mít za to, že ti co se nevyjádřili, ač mohli a měli, souhlasí). Příhodnější je nicméně výslovný písemný souhlas. V žádném případě nelze takto sledovat zaměstnance skrytě, bez jejich vědomí. V takovém případě by jasně šlo o případ narušení jejich soukromí, neboť zaměstnanci by oprávněně očekávali, že do jejich soukromí není žádným tajným sledováním, o němž by nevěděli, zasahováno.

sociální zařízení, ubytovny atd. – monitorování je zcela **vyloučeno**, zásah do soukromí zaměstnanců není prakticky žádným způsobem odůvodnitelný

Pro případ návštěv jiných osob než zaměstnanců na pracovišti **je vhodné** umístit ve vstupních prostorách upozornění na kamerový systém (tabulka, piktogram) – návštěva má možnost zvolit, zda s monitorováním souhlasí (a do objektu pak vstoupí), či nikoliv (pak nevstoupí). Vhodnost umisťování těchto informačních tabulek či jiných způsobů informování subjektů dotčených monitorováním je nutno vždy zvažovat v závislosti na konkrétní situaci. Situace bude odlišná v případě malé firmy s relativně úzkou a pravidelnou klientelou, která přichází do monitorovaných prostor, a naopak v případě mamutích obchodních center, kde vesměs každý očekává nižší míru svého soukromí s ohledem na obecné povědomí o existenci vysokého počtu kamer v těchto prostorách.

4.5.3.2 Provozování kamerových systémů s pořizováním obrazových záznamů

Podmínky provozu kamerových systémů s pořizováním záznamů jsou v porovnání s předchozím způsobem provozování kamerového systému nepochybně přísnější, a to především s ohledem na nutnou aplikaci režimu § 12 a násl. občanského zákoníku (*...podobizny, obrazové snímky a obrazové a zvukové záznamy týkající se fyzické osoby nebo jejích projevů osobní povahy smějí být pořízeny nebo použity jen s jejím svolením*). Bez výjimky se zde také uplatní režim zákona na ochranu osobních údajů, neboť již půjde o zpracování osobních údajů. Tak jako tomu bylo v předchozím případě kamerového systému bez pořizování záznamů, i zde bude monitoring možný zejména na základě zmocnění v § 316 zákoníku práce. V takovém případě bude nutné vyhovět podmínkám daných tímto ustanovením (viz především povinnost zaměstnavatele informovat zaměstnance o rozsahu kontroly a o způsobech jejího provádění dle § 316 odst. 3). Je ovšem otázkou, zda v případě, že budou na pracovišti zavedeny kontrolní mechanismy podle § 316 odst. 2 zákoníku práce, bude z hlediska občanskoprávní ochrany osobnosti **nutné svolení monitorovaných osob** k pořizování, resp. využívání *písemností osobní povahy, podobizen, obrazových snímků nebo obrazových a zvukových záznamů* (§ 12 občanského zákoníku)? Zřejmě až následná judikatura ve sporných případech tuto situaci vyřeší.

Monitorování zaměstnanců se současným pořizováním obrazových či i zvukových záznamů bude však i nadále pravděpodobně možné i pro případ ochrany i jiných oprávněných zájmů zaměstnavatele (jako již několikrát zmiňovaná ochrana před vandalismem, krádežemi apod.). Protože v právním řádu není výslovné zmocnění pro pořizování kamerových záznamů za jiným účelem než dle § 316 zákoníku práce, je toto oprávnění třeba dovozovat z obecnější právní úpravy. Jelikož se nebude jednat ani o použití následných záznamů pro úřední účely dle § 12 občanského zákoníku, bude proto v návaznosti na § 12 obč. zákoníku jednoznačně **nutný souhlas zaměstnanců**, kteří budou podrobeni dohledu, byť někdy i nezamýšlenému (např. v případě dohledu spíše nad prostorami než nad činností zaměstnanců). Nejlépe je požadovat výslovný a písemný souhlas, jehož obsahem by mělo být:

- *vymezení kde a jak budou záznamy pořizovány a používány*
- *k jakému účelu se tak bude dít*
- *prohlášení zaměstnance, že s tímto pořízením a použitím záznamů souhlasí*
- *podmínky zabezpečení záznamů před neoprávněným použitím*
- *lhůta pro uchovávání záznamů atd.*

Zaměstnanec se nemůže platně vzdát svých ústavou zaručených práv, a to ani výslovně a zcela dobrovolně.[156]

V případě, že zaměstnavatel neobdrží souhlas s pořizováním záznamů z kamerového systému a potenciálně tak neoprávněně zasáhne do osobnostního práva zaměstnance, má zaměstnanec dle § 13 obč. zák. právo domáhat se, aby

- *bylo upuštěno od neoprávněných zásahů do práva na ochranu jeho osobnosti*
- *byly odstraněny následky těchto zásahů*
- *bylo mu dáno přiměřené zadostiučinění (omluva, peněžní satisfakce)*

Otázkou pak samozřejmě je, zda se pro toto někdy radikální řešení, jež může vést k citelnému zhoršení a eskalaci vztahů se zaměstnavatelem, zaměstnanec vždy svobodně rozhodne, nebo bude s ohledem na jistotu pracovního poměru monitorování bez jeho souhlasu raději mlčky tolerovat.

Z hlediska zákona na ochranu osobních údajů se použití kamerového systému se záznamy považuje za zpracování osobních údajů, pokud účelem záznamů je jejich využití k identifikaci fyzických osob v souvislosti s určitým jednáním. Tak tomu však bude **prakticky vždy**, neboť fyzickou osobu lze ze záznamu snadno identifikovat zejména dle

[156] Nepřípustnost vzdání se ústavního práva soukromí stanoví ve svém článku např. J. Aujezdský. Viz: AUJEZDSKÝ, J.: Skutečně může zaměstnavatel číst Vaší poštu? In: IT Právo – server o internetovém a počítačovém právu. [online]. Praha: Společnost pro právo informačních technologií (SPIT), 2004, ISSN: 1801 4089 Dostupný z www: http://www.itpravo.cz/index.shtml?x=160355 [cit. 2012-02-18].

obličeje, navíc se bude jednat o úzce vymezenou skupinu konkrétních lidí. Samotné zpracování osobních údajů ve smyslu zákona na ochranu osobních údajů je možné i bez souhlasu dotčené osoby, *pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby; takové zpracování osobních údajů však nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života (*§ 5 odst. 2 písm. e) zákona č. 101/2000 Sb.) V každém případě je však provozovatel kamerového systému (správce osobních údajů) povinen z hlediska zákona č. 101/2000 Sb. respektovat **následující podmínky**:

- *kamerové sledování nesmí nadměrně zasahovat do soukromí*
- *je nutné předem specifikovat účel monitorování a pořizování záznamů*
- *je nutno stanovit lhůtu pro uchovávání záznamů (ideálně 24/48 hodin, několik dnů)*
- *je nutno zajistit řádnou ochranu zařízení a záznamů před neoprávněným nebo nahodilým přístupem, zničením, poškozením nebo jiným neoprávněným zpracováním*
- *subjekt údajů musí být o užití kamerového systému vhodně informován (nápisem v monitorované místnosti, při vstupu apod.)*
- *zpracování osobních údajů je nutno registrovat u Úřadu pro ochranu osobních údajů*

Instalace kamer je pak samozřejmě zcela vyloučena v prostorách, které slouží čistě soukromým účelům (sociální zařízení, pokoje ubytoven apod.).

4.5.4 Řešení problematiky monitoringu na pracovišti

Tak jako v jiných společenských vztazích i na pracovišti bude vždy platit **zásada přiměřenosti a subsidiarity**. Vždy půjde o to najít v případné problémové oblasti nejlepší možné řešení. Domnívám se, že ve sporných otázkách bude mít přednost spíše ústavně garantovaná zásada práva na ochranu soukromí zaměstnance, tato ale bude muset být vždy současně

poměřována s oprávněnými zájmy zaměstnavatele a v některých případech bude muset ustoupit. Východiskem tedy nesmí být ani naprostá nedotknutelnost veškerého jednání zaměstnancem, jeho korespondence, dokumentů, zpráv a jiných věcí z titulu ochrany zaměstnancova soukromí, ale stejně tak ani podrobení zaměstnance totální kontrole veškerého jeho jednání, kontrole veškerého obsahu jeho korespondence, telefonátů a jiných komunikačních prostředků. Pokud bude existovat jiná možnost s potenciálně nižší mírou narušení soukromí zaměstnance, bude nutné dát přednost právě jí, a to i pokud bude znamenat o něco vyšší finanční náklady.

Domnívám se, že vždy bude nicméně nutné tato ustanovení s poměrně vágním obsahem (*…závažný důvod…*, *…zvláštní povaha činnosti* ….. atd.) vykládat **přísně zužujícím výkladem** a vždy bude nutné se ptát na potřebnost takového monitorování z hlediska garance ústavně zaručeného práva zaměstnance na soukromí (tj. z hlediska principu přiměřenosti, principu proporcionality a dalších obecných právních zásad). Jsem toho názoru, že soudy aplikující nové znění zákoníku práce by měly skutečně nepoužívat extenzivní výklad v neprospěch zaměstnance, neboť je třeba naopak spíše zvrátit obecný společenský trend, kdy celá řada zaměstnavatelů (podle některých průzkumů až 40% českých firem) v současnosti podrobuje své zaměstnance nějaké formě otevřeného či skrytého sledování, včetně přímého odposlechu. Často se tak přitom dělo a děje s tichým (či vynuceným) souhlasem zaměstnanců, kteří v zájmu udržení místa nijak neprotestují. Je logické, že zvlášť nadnárodní a větší firmy mají obavy před vyzrazením důležitých dat a jejich předáním konkurenci – to však samo o sobě nesmí ospravedlňovat nepřípustné monitorování a kontrolu jejich zaměstnanců.

V případě, že zaměstnanec je toho názoru, že kamerový systém je u zaměstnavatele instalován neoprávněně a že došlo nebo dochází k neoprávněnému zásahu do soukromí zaměstnance, může se zaměstnanec obrátit na zaměstnavatele se stížností na výkon práv a povinností vyplývajících z pracovněprávních vztahů. Takovou stížnost je zaměstnavatel se zaměstnancem povinen projednat dle § 14 odst. 3 zákoníku práce. Pokud však zaměstnavatel nevyhoví požadavkům zaměstnance vyjádřeným v takové stížnosti, musí mít zaměstnanec možnost obrátit se též na orgán,

který disponuje potřebnou rozhodovací autoritou. Tímto orgánem je dle současné právní úpravy Inspekce práce nebo Úřad na ochranu osobních údajů. U Inspekce práce, která provádí kontrolu dle ustanovení § 5 zákona č. 251/2005 Sb. však lze narazit na problém, že Inspekce práce není nadána pravomocí za případné porušení práva zaměstnance vyplývající z ustanovení § 316 uložit zaměstnavateli jakoukoliv sankci – zákon o inspekci práce nezná skutkovou podstatu, za kterou by mohl orgán inspekce práce uložit zaměstnavateli sankci.[157] V případě iniciování stížnosti u Úřadu na ochranu osobních údajů mohou nastat dvě situace. Buď se zaměstnanec obrátí nejprve na zaměstnavatele jako na správce (zpracovatele) osobních údajů a pokud ten závadný stav neodstraní, zaměstnanec pak podá žádost o zajištění nápravy k ÚOOÚ. Ten by měl zahájit návrhové řízení, věc projednat a rozhodnout o návrhu. Nejde tedy o prostý podnět k ÚOOÚ, ale o kvalifikované návrhové řízení.[158] Tento stav však již byl změněn rozhodnutím Nejvyššího správního soudu ze dne 16.3.2010, sp. zn. 1 As 93/2009, ve kterém NSS dovodil, že de facto všechna řízení vedená před ÚOOÚ mohou být zahájena jen z moci úřední a podání stěžovatele tak je nutno považovat toliko za podnět k provedení kontroly a zahájení řízení o uložení nápravných opatření dle § 40 zákona o ochraně osobních údajů.[159]

4.6 Kamerové systémy v dětských domovech a ve školských zařízeních

Ve výchovných ústavech v České republice došlo na přelomu století k několika tragickým událostem, kdy byli napadeni vychovatelé těchto ústavů. Pod dojmem těchto událostí byly následně v některých ústavech a školských zařízeních ve větší míře nainstalovány a používány kamery. Dělo se tak asi v osmnácti dětských domovech a výchovných ústavech, ve dvou z nich byly dokonce prováděny odposlechy. Zařízení byla přitom namontována tak, aby byl sledován nejen vchod a venkovní prostory budov,

[157] Viz i názor autorů publikace BARTÍK, V. JANEČKOVÁ, E: Kamerové systémy v praxi. Praha: LINDE, 2011.

[158] Srovnej rozhodnutí Nejvyššího správního soudu ze dne 30.8.2007, sp. zn. 4 Ans 6/2006.

[159] Dále viz BARTÍK, V. JANEČKOVÁ, E: Kamerové systémy v praxi. Praha: LINDE, 2011.

ale i klubovny, jídelny, oddělené místnosti, zdravotní izolace, třídy, chodby a v jednom případě dokonce i ložnice. To samozřejmě vyvolalo bouřlivou mediální diskusi, do které se zapojil i úřad Veřejného ochránce práv, který namítal porušení práv dětí na soukromí, zaručených ústavními předpisy i mezinárodními úmluvami.

Ministerstvo školství, mládeže a tělovýchovy jako ústřední státní orgán, do jehož působnosti spadají ústavy a školská zařízení, si nechalo zpracovat u Ústavu státu a práva Akademie věd ČR stanovisko, které v zásadě konstatovalo, že používání kamerových systémů v ústavech není porušením zásady nedotknutelnosti obydlí, protože *"veřejná zařízení jako školy, výchovné ústavy, nemocnice, věznice, kasárna nejsou obydlím osob."* Ústav státu a práva také dovodil, že bez zasahování do základních lidských práv a svobod občanů může obrazové a zvukové záznamy pořizovat každý, aniž by pro to potřeboval oporu ve zvláštním zákoně. 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 o sobě nenarušuje ani jeho obydlí, ani soukromí, ani dobré jméno atd., a zejména neporušuje míru jeho svobody pohybu nebo jiného počínání. [160] Toto stanovisko však bylo poměrně rozporuplné, a proto vyvolalo v odborné veřejnosti další reakce, včetně právního rozboru věci podaného Právnickou fakultou Masarykovy univerzity v Brně a následně i stanoviskem Nejvyššího státního zástupce ze dne 25.7.2003.[161] Ve stanovisku Právnické fakulty MU v Brně se uvádí, že výchovné ústavy jako veřejná zařízení

[160] Stanovisko Ústavu státu a práva Akademie věd ČR ze dne 21.1.2003, č. j. 221/02, podepsané ředitelem ústavu JUDr. Jaroslavem Zachariášem, CSc. (toto stanovisko bylo poskytnuto MŠMT na základě žádosti Ligy lidských práv dle zákona č. 106/1999 Sb.).

[161] Viz Šimíček, V.: Odborné stanovisko k otázce ústavně právní přípustnosti instalace odposlechů a kamerových systémů ve výchovných ústavech a podobných zařízeních; PF MU, Brno, 2003, str. 3, a dále viz Výkladové stanovisko Nejvyššího státního zástupce ze dne 25.7.2003, Vykls 10/2003: K zákonnosti umístění audio - vizuálních prostředků ve školských zařízeních vykonávajících ústavní výchovu a ochrannou výchovu.

mohou činit pouze to, co zákon dovoluje, a tím instalace a využití sledovacích kamerových systémů není, neboť zde není zákonné zmocnění. Toto stanovisko také požaduje extenzivní výklad pojmu obydlí při aplikaci na tyto ústavy a prostory, které obývají děti, neboť jde o prostory, které jednotlivci slouží k bydlení a nejsou proto veřejně přístupné (z tohoto důvodu se na tyto prostory bude vztahovat ochrana obydlí dle čl. 12 LZPS). Ve stanovisku brněnské právnické fakulty je také zmíněn názor, že použití kamerového systému v ústavech 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.

Při přípravě výkladového stanoviska Nejvyššího státního zástupce se i na jednotlivých odborech Nejvyššího státního zastupitelství objevily poměrně protichůdné názory na řešení problematiky. Se stanoviskem Právnické fakulty MU v Brně se v podstatě ztotožnil netrestní odbor Nejvyššího státního zastupitelství. Analytický a legislativní odbor Nejvyššího státního zastupitelství argumentoval zejména tím, že zákonnost použití kamerových systémů lze dovodit i z jiných ustanovení zákona o ústavní výchově ukládajících pracovníkům zařízení řadu práv a povinností ve vztahu k osobám ubytovaným, které mnohdy již soukromí narušují. Platný zákon však nestanoví přesné způsoby provádění všech dohledových činností, například nekonkretizuje v odstavci 3 § 22 zákona č. 109/2002 Sb. v tehdy platném znění povinnost sledovat stav dítěte umístěného do tzv. oddělené místnosti pověřeným pracovníkem v minimálně 30 minutových intervalech a nestanoví přesný způsob, jak má být sledování prováděno. Pokud by bylo toto sledování prostoru oddělené místnosti ve stanovených termínech prováděno pomocí audio - vizuálních prostředků, nemohlo by pak být kvalifikováno jako porušení zákona či výše uvedených základních práv. Konečné **stanovisko Nejvyššího státního zástupce pak konstatovalo, že:**

I. umístění audio - vizuálních prostředků v objektech školských zařízení určených k vykonávání ústavní výchovy, ochranné výchovy či poskytování preventivně výchovné péče, kde je na základě

*příslušného zákonného opatření umístěno dítě a dočasně nebo trvale tak zbaveno svého rodinného prostředí, **je bez zvláštní zákonné úpravy v rozporu** s právy zakotvenými v čl. 8 odst. 1 Úmluvy o lidských právech , čl. 16 ve spojení s čl. 20 odst. 1 Úmluvy o právech dítěte a s čl. 7 odst. 1 , čl. 10 odst. 2 a čl. 12 odst. 1 Listiny základních práv a svobod.*

*II. umístění těchto prostředků v prostorách zařízení, ve kterých je umožněn nekontrolovatelný pohyb osob, které nejsou zaměstnanci zařízení, **není porušením práv dítěte** garantovaných normami uvedenými v bodu I.*[162]

Celá kauza pak byla prozatím skončena přijetím zákonné novely č. 383/2005 Sb., měnící zákon č. 109/2002 Sb. ze dne 5.2.2002 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 o ústavní výchově tak v současné době upravuje pro zařízení, ve kterých jsou umístěny děti s uloženou ochrannou výchovou, problematiku **použití speciálních technických prostředků k zabránění útěku dětí**. Vedle toho je pak dále možné na základě rozhodnutí ředitele zařízení v těchto zařízeních za účelem zajištění bezpečnosti dětí, zaměstnaných osob a svěřeného majetku využívat **audiovizuální systémy** (viz § 15 citovaného zákona). Zákon o ústavní výchově povoluje využití audiovizuálních systémů pro následující účely:

- *pro kontrolu okolí budovy či více budov na jednom ohraničeném pozemku,*

[162] K celé problematice viz např. článek R. Jelínkové: V soukromí kamer a odposlechů. Právní kritika „velkochovů dětí“ v Čechách a na Moravě. In: dvouměsíčník ViaIuris číslo 4/2003, vydavatel: Ekologický právní servis a Liga lidských práv, Bratislavská 31, 602 00 Brno. Autorka v článku dokonce uvádí, že vzhledem k tomu, že účelu, jež může být užíváním kamer a odposlechů v zařízeních ústavní výchovy sledován, lze dosáhnout i jinak, bylo by tedy sledování dětí v ústavech s vysokou pravděpodobností protiústavní i v případě zákonného podkladu. Svou argumentaci opírá zejména o fakt, že po proběhlé mediální kritice a po výzvě veřejného ochránce práv většina ředitelů dotčených ústavů kamery a odposlechy odstranila s tím, že jim v péči o svěřence stejně nijak zvlášť nepomáhají.

- *pro kontrolu vnitřních prostor zařízení, kam nemají děti přístup,*
- *pro kontrolu chodeb, místností určených pro zaměstnance zařízení a oddělené místnosti.*

Předtím, než dojde k samotné realizaci celého projektu, kterým se do ústavu zavede audiovizuální technika, je však nutné, aby příslušné ministerstvo **schválilo plány** pro využívání audiovizuální techniky včetně rozmístění sledovacích bodů v zařízeních a dále plány rozmístění speciálních stavebně technických prostředků v zařízeních a jejich jednotlivé druhy. Zákon vyžaduje, aby o umístění a způsobu využívání audiovizuální techniky byly ředitelem zařízení předem informovány všechny děti umístěné v zařízení a všichni zaměstnanci zařízení.

V poměrně nedávné době pak českou společnost pobouřil a rozdělil další obdobný případ, kdy ředitel jednoho pražského gymnázia rozhodl o **instalaci kamer**, které by snímaly žáky nejen na chodbách, ale dokonce i **v samotných třídách**. Mělo se tak dít za účelem ochrany před šikanou a jinými negativními jevy, které se ve školních zařízeních v posledních letech objevují čím dál častěji. Rozhodnutí ředitele tohoto gymnázia vyvolalo intenzivní protesty samotných žáků, kteří nesouhlasili s takovým zásahem do jejich soukromí při sledování ve třídách. Do věci se vložil i Úřad pro ochranu osobních údajů, který správně poukázal na fakt, že gymnázium si nepožádalo o registraci jakožto správce osobních údajů, které by používáním kamerového systému získávalo. I pod dalšími tlaky (veřejný ochránce práv, školní inspekce) se rozhodl ředitel gymnázia instalovat kamery toliko na chodby. Je nicméně evidentní, že obdobných případů bude v blízké budoucnosti pouze přibývat a bude záležet na celkovém postoji společnosti, včetně jejího zákonodárného sboru, jaké bude postupně zaujímat k věci stanovisko a zda bude tolerovat rozšiřování povolených zásahů do soukromí jednotlivce.[163]

[163] V dané věci bylo následně vydáno i vyjádření odboru legislativního a právního Ministerstva školství, mládeže a tělovýchovy ČR ze dne 6.12.2006, které uvedlo následující: „Při hledání odpovědi na otázku, zda kamery ve školách připustit, a pokud ano, tak kde konkrétně, je nutné vždy posoudit povahu toho kterého prostoru. Listina základních práv a svobod a mezinárodní úmluvy o lidských právech sledují jeden základní cíl - ochranu práv a svobod člověka. V tomto případě jde zejména o právo na nedotknutelnost osoby a jejího soukromí. Proto je nutné vymezit, které prostory ve

Vzhledem k citlivosti problematiky a zájmu veřejnosti se danému tématu věnoval podrobně i Úřad pro ochranu osobních údajů. Ten postupně vydal několik dokumentů, které se tématem zabývaly. Uveďme na tomto místě alespoň Vyjádření a doporučení ÚOOÚ k možnosti instalovat kamerový systém v prostorách školy ze dne 12.3.2007 (vydané v návaznosti na publikované vyjádření odboru legislativního a právního Ministerstva školství, mládeže a tělovýchovy ČR ze dne 6.12. 2006) Toto vyjádření a doporučení v zásadě deklarovalo následující:

1. Skutečnost, že neexistuje zvláštní právní úprava podmínek pro provozování kamerových systémů neznamená, že škola při splnění svých zákonných povinností správce osobních údajů nemůže rozhodnutí o instalaci kamerového systému se záznamem učinit.
2. Pokud se škola k tomuto kroku rozhodne, ocitá se toto zpracování v režimu zákona a musí proto splnit zde uváděné zákonné podmínky:
   - Učinit oznámení o zpracování podle § 16 zákona
   - Zpracovávat osobní údaje pouze se souhlasem subjektu údajů podle § 5 odst. 2, pokud škola neprokáže kvalifikovaný důvod, který by ji opravňoval ke zpracování osobních údajů bez souhlasu.
   - Provozovat systém tak, aby bylo soukromí osob s ohledem na jejich právo podle § 10 zákona narušováno minimálně (posuzováno je např. i umístění kamer, úhel záběru, zobrazovací schopnost apod.).

školách jsou pojmově vhodné a určené k realizaci těchto práv. Zajisté není sporu o tom, že místnosti sloužící jako příslušenství (záchody, umývárny apod.) jsou prostory takové povahy, že se v nich očekává poskytnutí velké míry soukromí, a jelikož slouží žákům k uspokojování základních lidských potřeb, jako je zejména osobní hygiena, je nepochybné, že si zaslouží nejvyšší možnou ochranu. Sledování kamerami by v tomto případě představovalo nadměrný a neoprávněný zásah do soukromí žáků. Jinou povahu však mají společné, obslužné nebo žákům (studentům) běžně nepřístupné prostory, jako jsou chodby, šatny, ředitelna, sborovna apod., kde ani žádné soukromí není možné a kde mají přístup nejen žáci (studenti), ale i učitelé, návštěvy, příp. další osoby, nebo kam naopak není volný přístup povolen. Zde již dochází ke střetu zájmu mezi právem na ochranu soukromí a povinností zařízení zajistit bezpečnost žáků (studentů) i zaměstnanců školy. Jelikož prostory svou povahou soukromé nejsou, je možné v nich připustit prostorové sledování kamerami. Totéž ještě více platí u okolí školy, jako je prostor před vstupními dveřmi, zahrada, oplocení atd.

Závěr: Za současného právního stavu je podle našeho názoru možné umístit kamerový systém:
• ve společných a obslužných prostorách školy (vyjma tříd), kam mají přístup nejen žáci, ale i učitelé, návštěvy, popř. další osoby,
• v prostorách školy, kam nemají žáci volný přístup (např. ředitelna, sborovna, kabinet učitele),
• vně školy a u jejího vchodu.“

- Informovat monitorované osoby o instalaci a provozu systému podle § 11 zákona.
- Přijmout bezpečnostní opatření pro provozování systému a ochranu zpracovávaných informací podle § 13 zákona a stanovit přiměřenou dobu pro uchovávání záznamů podle § 5 odst. 1 písm. e).
- Respektovat podmínky zvláštních právních předpisů upravujících možnosti sledování osob (zejména § 316 odst. 2 zákoníku práce).

Čistě z právního hlediska je zřejmě nediskutabilní, že instalování kamer přímo do tříd by bylo za současného právního stavu nezákonným zásahem do ústavně garantovaného práva na soukromí. Byť se v dané věci jednalo o soukromou školu, tedy neveřejnoprávní subjekt, ani tato nemůže zasahovat do zaručeného soukromí jednotlivce bez zákonného zmocnění a stanovení podmínek zásahu. I když existují právní předpisy umožňující instalaci kamerových systémů a provádění obrazových záznamů, v daném případě by šlo o natolik invazivní zásah do soukromí dětí a učitele ve třídě, že by jej nešlo odůvodnit v zájmu jiných společensky významných důvodů. Žáci a učitel by totiž ve třídě byli podrobeni **soustavnému adresnému monitorování**, které je velmi odlišné od vcelku nahodilého a na konkrétní osoby nezaměřeného sledování běžného na ulicích, bankách, obchodech apod.

Na shora provedeném poměrně podrobném nástinu problematiky umisťování kamerových a jiných sledovacích zařízení ve školských a výchovných zařízeních jsem chtěl ukázat, že pokud se uvažuje o použití moderních technologií, které zasahují do soukromí jednotlivce na poměrně uzavřeném prostoru, přičemž pro to není výslovná opora v zákoně, téměř vždy to vyvolá bouřivou reakci veřejnosti, laické i odborné. K dané problematice se pak vyjadřuje kdekdo, od naprostých laiků, kteří však cítí (často oprávněně) ohrožení jejich práva na soukromí, až po fundované odborné kapacity na problematiku ochrany lidských práv. Doslova společenskou a mediální krizi pak většinou vyřeší až jasné stanovení pravidel, upravujících alespoň základní vymezení použití sledovacích technologií v dané oblasti. Názorně zde můžeme pozorovat jev typický pro společenské a technologické změny, které právo nedokáže v reálném čase sledovat. Po vymezení aktuálního společenského problému a snahách o jeho

řešení přichází až ex post právní úprava, která většinou zdárně ukončuje přechodné období, kdy jsou na danou problematiku většinou subsidiárně aplikovány nejrůznější obdobné právní normy, včetně mezinárodních, jakož i různé judikáty, taktéž i zahraniční. Nedomnívám se však, že by šlo o jev vždy nezbytně negativní. Naopak jde o věc pro právo zcela běžnou a dokonce někdy i přínosnou. Právo tak totiž může, již obohaceno o určité společenské zkušenosti, správněji a efektivněji reflektovat dosavadní „bezprávní“ vakuum a přijmout kvalitnější a přesnější právní normu, šitou na míru.

Na těchto příkladech je také vidět velmi významná role **nezávislých subjektů**, s kvalifikovaným odborným obsazením, které byť nejsou třeba ani vybaveny rozhodovací pravomocí a nemohou ukládat sankce, mohou dosáhnout podstatných společenských změn, které se následně promítají do právního pořádku. Po přechodnou dobu mohou dokonce tyto nezávislé organizace (jako je Úřad pro ochranu osobních údajů, úřad Veřejného ochránce práv) svým výkladem práva jako celku, resp. podáváním stanovisek, dokonce zaplnit právní vakuum a nalézt smysluplné řešení (srovnej například problematiku používání kamerových systémů a její zpracování pro praxi Úřadem pro ochranu osobních údajů v jeho Zásadách provozování kamerových systémů, cit. dříve). I když většinou tato stanoviska nebo odborné výklady nejsou právně závazné, dokážou silou své přesvědčivosti a vahou odborníků nebo osobností, kteří za nimi stojí, přesvědčit a ukázat správný směr.

4.7 Kamerové systémy ve zdravotnictví

Snahy o masivnější nasazování kamerových systémů se postupně začaly objevovat i u některých zdravotnických zařízení. Jako nejdůležitější důvody byly uváděny ochrana bezpečnosti, ochrana práv osob, ochrana majetku, dokladování průběhu nejrůznějších situací, jež mohou v daném zařízení nastat, prevence před nežádoucím jednáním apod.

Veřejný ochránce práv používání kamerových systémů se zřetelem na respekt k lidské důstojnosti a soukromí (tedy nikoli s ohledem na ochranu osobních údajů) několikrát komentoval v dílčích zprávách adresovaných

navštíveným zařízením a v některých zveřejněných souhrnných zprávách. Ve zprávě z následných návštěv psychiatrických léčeben odmítl používání kamer na toaletách psychiatrických léčeben a poukázal na absenci zákonné licence pro používání kamerových systémů ve zdravotnických zařízeních vůbec. [164] Konkrétní doporučení také formuloval v bodě 106 Zprávy z návštěv domovů pro osoby se zdravotním postižením.[165]

V zásadě lze říci, že ve zdravotnických zařízeních se pohybují **tři kategorie osob**, které mohou být předmětem obrazového monitoringu. Jednak jde o zaměstnance (lékaři, sestry, pomocný personál atd.), dále se v objektu pohybují samozřejmě pacienti a konečně pak další návštěvy (rodinní příslušníci, ale např. i osoby vstupující do zdravotnického zařízenínelegálně – zloději apod.). Na obrazové sledování se tak bude aplikovat přípustnost instalace kamerové systému obdobně jako na pracovišti (nasazení obrazového monitoringu se záznamem odůvodní jen zvláštní povaha činnosti zaměstnavatele) a dále bude nutné přísněji posuzovat hledisko nakládání s osobními údaji pacientů – zde se může jednat o nakládání s citlivými údaji týkajícími se zdravotního stavu pacientů. Má-li být kamerový systém ve zdravotnickém zařízení instalován, bude se rozlišovat mezi **prostory vstupními a vnějšími** a mezi **prostory vnitřními** (čekárny, ambulance atd.). Půjde-li o vnější prostory a vstupy do budov a na jednotlivá oddělení, hledisko posuzování poměru mezi zásahem do soukromí a důvody pro instalaci kamer, bude zřejmě vyváženo ve prospěch důvodů pro instalaci kamer. Pokud jde o vnitřní prostory, zde bude nutné

---

[164] K tématu viz Zpráva o návštěvě zařízení – Psychiatrické léčebny v Dobřanech ze dne 12.6.2008, kde Veřejný ochránce práv zmiňuje užití kamerového systému na mnoha místech léčebny, včetně toalet, společenských místností, izolačních místností, příjmové ložnici atd. Pacient je de faxto podroben celodennímu nepřetržitému sledování. Zpráva hovoří o mnoha případedch, ve kterých je kamerový systém užíván nadbytečně, pacienti nejsou informováni o sledování, neexistuje vnitřní řád nebo pravidla pro používání kamerového systému atd.

[165] Dále viz Zpráva z domovů pro osoby se zdravotním postižením ze dne 14.10.2009, dostupná online na internetových stránkách Veřejného ochránce práv http://www.ochrance.cz/?id=101624 [cit. 2012-02-18].
Veřejný ochránce práv ve své zprávě uvádí následující:
„Doporučuje se poměřit míru zásahu do soukromí v případě interiérových kamer, které umožňují rozpoznat zabírané osoby, a míru jejich potřebnosti. Lze si například představit zapínání kamery na noc, kdy v části areálu není přítomen personál. Tedy stanovení pravidel používání kamer, případně instalace spínačů. Za všech okolností musí být v místech zabíraných kamerami upozornění, klienti musí být vzhledem ke své schopnosti rozumět o kamerách informováni.“

velmi přísně posuzovat, proč je zde nutné kamerový systém provozovat (záležet také bude, zda monitorování probíhá například jen v noci nebo v době, kdy se na chodbách vnitřních prostor nepohybují zaměstnanci a je nutné sledovat prostor například z důvodu kontroly a zamezení vstupu neoprávněných osob). Kamery by se měly instalovat pokud možno se souhlasem pacientů a po konzultaci s Úřadem pro ochranu osobních údajů. Kamery by neměly být umístěny takovýn způsobem, aby šlo pacienta na snímku snadno identifikovat a snímek by vypovídal o jeho stavu, úrazu nebo nemoci. V každém případě je umisťování kamer v prostorách zdravotnických zařízení citlivým tématem a provozovatelé nemocnic a obdobných zařízení by měly veškeré důvody pro instalaci kamerového systému či pro volbu jiného alternativního řešení vždy pečlivě zvažovat.

4.8 Kamerové systémy v bytových domech

Kamerové systémy bývají často umísťovány i v obytných domech. Motivací majitelů domů k zavedení kamerového dohledu společných a dalších prostor v domě je samozřejmě ochrana majetku, zejména ochrana před vandalismem, krádežemi atd. Kamerové systémy jsou nejčastěji v domech umístěny u vchodových vstupních dveří, u výtahů, sklepních prostor, garáží a vnitřních dvorů. Oproti zájmu na ochraně majetku stojí pak zájem obyvatel domu, případně dalších osob (návštěv apod.) na ochraně jejich soukromí. Judikatura, včetně Úřadu na ochranu osobních údajů, otázku, zda jde při provozování kamerového systému o zpracování osobních údajů, již vyřešila. Bude-li v obytném domě provozován kamerový systém se záznamem, jde o zpracování osobních údajů, neboť budou pořizovány záznamy se snímky osob, které jsou nepochybně ze snímků a záznamů určitelné. Obyvatelé domu mohou samozřejmě namítat narušení svého soukromí, neboť mohou být pod přímým dohledem a jistě nelze připustit, že správce (provozovatel) kamerového systému, či jiná osoba, která bude mít k záznamům přístup, bude moci bez omezení a určitých mantinelů a pravidel evidovat pohyb obyvatel domu, s kým se stýkají, pozorovat jejich zvyky a chování.

Úřad na ochranu osobních údajů se k řešení otázky, zda je možné v domě intalovat kamerový systém, postavil poměrně přísně. Jak vyplývá z jeho stanoviska č. 1/2008, měl by správce kamerového systému v bytovém domě, kterému není uloženo zpracování osobních údajů zákonem nebo který nedisponuje souhlasem všech obyvatel domu, prokázat, že zpracování osobních údajů je:

- prokazatelně vhodný způsob (prostředek) k vyřešení daného problému
- prokazatelně nutný způsob (prostředek) pro jeho řešení, tj. zasahuje do soukromí prokazatelně méně než alternativní objektivně srovnatelné legální možnosti,
- proporcionální vůči např. svému přínosu pro bezpečnost, a že
- bude pravidlně revidován, aby bylo zajištěno trvalé naplnění výše uvedených aspektů

Úřad taktéž provedl pokus o základní rozdělení prostor v domě na **prostory, kde obyvatelé domu obvykle nežijí svůj soukromý život a monitorování těchto prostor tak do soukromí nezasahuje** (půdy, sklepy, garáže, vchody na působu, kočárkáren atd.) a na **prostory, které jsou již se soukromým životem obyvatel domu spjaty** (vchodové dvdeře do domu, přístupové chodby k bytům atd.).

V jedné z věcí, řešených ve správním řízení Úřadem na ochranu osobních údajů, existuje i rozsudek Městského soudu v Praze ze dne 28.2.2007, č.j. 7 Ca 204/2005-49, který podpořil ÚOOÚ, když potvrdil jeho rozhodnutí o uložení pokuty ve výši 180.000,- Kč ve správním řízení o porušení povinnosti správce osobních údajů. V dané kauze soud posuzoval přípustnost monitorování prostor v domě při současném zavedeném systému čipového kódování. Soud dovodil, že *„ochrana majetku či útoky na členy družstva nemůže zdůvodnit natolik razantní omezení práva na soukromí, kdy společné prostory v domě jsou bez souhlasu všech uživatelů bytů nepřetržitě monitorovány kamerovým systémem, záznamy z takového monitorování jsou ukládány a osoby na těchto záznamech jsou identifikovatelné. Takovým postupem jsou systematicky shromažďovány bez souhlasu osob informace o jejich pohybu ve spolčných prostorách domu, které jsou ukládány na*

paměťové médium a umožňují kontrolu pohybu těchto osob ve společných prostorách.“

Lze tedy uzavřít, že soudy i ÚOOÚ posuzují přípustnost a podmínky instalace kamerového systému v obytném domě **přísně**. Praxe však ukazuje, že se kamery do domů instalují poměrně často, mnoho případů se však k projednání ze strany ÚOOÚ, správního či obecného soudu ani nedostane (kde není žalobce, není ani soudce). Chtěl bych zmínit, že považuji instalaci kamerového systému v obytném domě, a to i bez souhlasu všech dotčených osob, za možnou, nicméně pouze za splnění určitých podmínek. Je jasné, že se málokdy podačí sehnat souhlas všech obyvatel domu (často se v domě nezdržují, mění se majitelé bytů atd.), i pokud souhlas chybí, lze však maerový systém instalovat. Bude však třeba posuzovat **testem přiměřenosti** vhodnost a nutnost jeho zavedení, bude nutné zajistit správní uchovávání údajů a zabezpečit záznamy před jejich zneužitím. Lze jen doporučit, aby si provozovatel kamerového systému podal u ÚOOÚ oznámení o zamýšleném zpracování osobních údajů podle § 16 zákona o ochraně osobních údajů a případné nedostatky, na které ÚOOÚ upozorní, pak odstranil. Osobně jsem názoru, že pokud správce domu udělá vše rozumné pro získání souhlasu dotčených osob s instalací kamerového systému (např. hlasováním a vyjádřením souhlasu kvalifikované kupř. ¾ nebo čtyřpětinové většiny všech majitelů bytových jednotek na schůzi společenství bytových jednotek) a většinový souhlas i získá, a dále učiní vše pro zajištění nezneužití uchovávaného záznamu a současně jsou splněny i další zákonné důvody přípustnosti provozování kamerové systému, nebyl bych tak zásadně přísný jako ÚOOÚ a soud při posuzování přípustnosti instalace kamer v domě. Svůj názor odůvodňuji zejména určitou uzavřeností společenství navenek a sdílením společných prostor.

4.9 Další použití kamerových systémů

Kamery a kamerové systémy jsou v dnešní době používány nejrůznějšími veřejnoprávními i soukromými subjekty, a to v míře někdy až zarážející. Jsou instalovány v prostorách správních úřadů za účelem odhalování korupce a z bezpečnostních důvodů, v prostorách plaveckých

bazénů, obchodních domů, bank, směnáren, čerpacích pump a v mnoha jiných lokacích.[166] Možností využití kamerových systémů je opravdu celá řada, přičemž stále platí spíše tendence k stále většímu využití kamerových systémů.[167]

I když instalace a používání kamerových systémů v těchto případech nebývá prakticky nijak konkrétně upraveno v právních předpisech, lze je považovat za **legální a možné**. Vždy je však nutno přinejmenším dbát ústavně zaručených práv jednotlivce na ochranu soukromí, na ochranu osobnostních práv (§ 11 a násl. občanského zákoníku) a je nutné se v případě, že budou pořizovány záznamy, vypořádat i s režimem zákona na ochranu osobních údajů. Podle tohoto zákona a zejména podle výkladu používaného Úřadem pro ochranu osobních údajů je nutné v případě pořizování záznamů ze snímacího kamerového zařízení pohlížet na problematiku jako **na zpracování osobních údajů** ve smyslu § 4 odst. e) zákona č. 101/2000 Sb. a provozovatel kamerového systému tak musí splnit řadu podmínek vyžadovaných tímto zákonem pro správce provádějící zpracování osobních údajů, a to včetně registrace u Úřadu pro ochranu osobních údajů.

Další celospolečensky často diskutovanou otázkou je pořizování nejrůznějších **tajných obrazových či zvukových nahrávek**. Pomocí takovýchto záznamů, pořizovaných **ve skrytu a bez vědomí** nahrávané

---

166 Instalace bezpečnostních kamerových systémů v bankách není v ČR speciálně právně ošetřena, oproti tomu např. v sousedním Slovensku je od roku 2005 v platnosti novela zákona č. 483/2001 Z.z. o bankách, která ukládá povinnost zabezpečit bankovní prostory, ve kterých se uskutečňuje styk s klienty a současně manipulace s peněžní hotovostí kamerovým monitorovacím bezpečnostním systémem s 24-hodinovým záznamem v kvalitě, která umožňuje rozlišení osoby (viz § 38a odst. 2 slovenského zákona o bankách).

167 Např. vedení švýcarské železniční společnosti CFF se rozhodlo na vybraných tratích instalovat sledovací kamery přímo do vagónů svých vlakových souprav. Po dohodě se švýcarským spolkovým úřadem pro ochranu dat byla vydána i závazná pravidla pro zavedení kamerových systémů a jejich používání ve vlakových soupravách. Samozřejmostí má být informování cestujících o sledování pomocí viditelných štítků umístěných ve voze. Velmi přísně bylo stanoveno nakládání se záznamy. Videozáznamy nebudou vůbec průběžně sledovány, budou se ukládat, a nedojde – li k mimořádné události, budou po uplynutí 24 hodin mazány. V případě mimořádné události je k prohlížení záznamů oprávněna železniční policie ve spolupráci s kantonálními policejními složkami. Blíže viz článek Švýcarské zkušenosti: videokamery proti vandalismu, zveřejněný v Informačním bulletinu Úřadu pro ochranu osobních údajů, č. 2/2004, s. 9-10. Pro zajímavost - citovaný článek zmiňuje studii, ze které vyplývá, že zavedení kamer na železnici posiluje v pasažérech pocit bezpečí a může snížit vandalismus až o 80%.

osoby, jsou následně fyzické osoby usvědčovány kupříkladu z korupce, z politické lži, takovéto nahrávky mohou být taktéž účinným prostředkem a pojistkou při důležitých obchodních jednáních. Serioznější novináři a jiní publicisté formulují zásady pořizování tajných nahrávek alespoň do svých profesních kodexů, které odůvodňují pořizování těchto utajených nahrávek veřejným zájmem.[168] Stejně tak ale mohou být tajně pořizované obrazové nebo zvukové záznamy používány ze zcela zištných a účelových důvodů, jako jsou snahy některých bulvárních novinářů po chvilkové slávě a finanční odměně, nebo dokonce hůře jako prostředek ke šmírování a monitorování ze strany bezpečnostních agentur v zájmu jejich klientů či přímo ze strany kriminálních živlů. Z hlediska platného práva se lze proti **neoprávněnému** pořizování podobizen, písemností (např. deníky, dopisy) a jiných záznamů osobní povahy či týkajících se fyzické osoby nebo jejích projevů osobní povahy bránit v současné době prakticky jen v intencích občanského zákoníku a jím zakotveného institutu ochrany osobnosti. Podle § 11 a násl. občanského zákoníku platí, že **pořizování nebo použití takovýchto záznamů je možné jen se svolením dotčené osoby**. Svolení zákon nevyžaduje pouze v případě tzv. **úřední, vědecké, umělecké nebo reportážní licence**. Ustanovení § 11 odst. 3 obč. zákoníku výslovně dovoluje použití podobizen, obrazových snímků a obrazových a zvukových záznamů pro vědecké a umělecké účely a pro tiskové, filmové, rozhlasové a televizní zpravodajství, pokud se tak bude dít přiměřeným způsobem. Ani takovéto použití však nesmí být v rozporu s oprávněnými zájmy fyzické osoby.[169]

Ještě před přijetím současného trestního zákoníku, zákona č. 40/2009 Sb. existovaly snahy o zařazení speciálního trestného činu ***„Porušení důvěrnosti ústního projevu a jiného projevu osobní povahy“***.[170] Tento

---

[168] Například Kodex českého rozhlasu upravuje pořizování tajných nahrávek ve svých bodech 21.13 – 21.16 (*Skrytý mikrofon*).

[169] Podrobněji a úplněji k tématu ochrany osobnosti např. viz JEHLIČKA, O. – ŠVESTKA, J. – ŠKÁROVÁ, M. a kol.: Občanský zákoník. Komentář. 10. vydání. Praha: C. H. BECK, 2006. str. 96-158 nebo KNAPP – ŠVESTKA – JEHLIČKA a kol.: Ochrana osobnosti podle občanského práva. 4 vydání. Praha: LINDE, 2004.

[170] Zmiňovaný návrh trestního zákoníku definoval trestný čin porušení důvěrnosti ústního projevu a jiného projevu osobní povahy takto: *„Kdo v úmyslu získat pro sebe nebo pro jiného majetkový nebo jiný prospěch, způsobit jinému škodu nebo jinou vážnou újmu, anebo ohrozit jeho společenskou vážnost, poruší důvěrnost **neveřejně** pronesených slov nebo jiného projevu osobní povahy tím, že ho **neoprávněně** zachytí*

trestný čin měl účinněji v trestněprávní rovině postihovat neoprávněné odposlechy a jiné neoprávněné dokumentování projevů osobní povahy v souvislosti například s konkurenčním obchodním bojem či za účelem jiných zištných zájmů (kupř. neoprávněné pořízení nahrávky bulvárním novinářem čistě za účelem finanční odměny a zvýšení obratu periodika). Dne 21.3.2006 nicméně Poslanecká sněmovna svým hlasováním o Senátem vráceném vládním návrhu trestního zákoníku definitivně odmítla jeho přijetí. V novém trestném zákoníku, zákoně č. 40/2009 Sb. se tento trestný čin již neobjevil. Do budoucna by přesto bylo více než vhodné nějakým způsobem tento trestný čin či jemu obdobný do trestního zákona zařadit, aby se zlepšila ochrana práva jednotlivce na jeho soukromí, a to zejména v kontextu moderních záznamových a obdobných technologií.

---

*záznamovým zařízením a takto zhotovený záznam **zveřejní** nebo ho **jiným obdobným způsobem použije**, bude potrestán odnětím svobody až na jeden rok, propadnutím věci nebo jiné majetkové hodnoty nebo zákazem činnosti."*

5 OBRAZOVÉ ZÁZNAMY A INFORMAČNÍ TECHNOLOGIE

5.1 Soukromí a nové technologie

Současný svět přináší neskutečné technologické možnosti usnadnění kvality života a jeho rozšíření směrem do dříve netušených sfér. Dnes není problém surfovat po internetu a prohlížet přitom reálné fotografie měst na druhé straně planety, tak jak je zachytily kamery nejrůznějších organizací typu StreetView, či fanoušků technologií a fotografů. Můžeme být v kontaktu s nepřeberným množstvím lidí z celého světa, můžeme své soukromí odhalit lidem z Číny, Argentiny, či obyvatelům polynéského souostroví, pokud mají připojení na Internet.

V poslední době dochází k opravdovému masivnímu rozšiřování moderních technologických pomůcek a jejich aplikací mezi drtivou většinu populace, což samo o sobě není problémem z právního hlediska, nicméně ve spojení s jistým potenciálním rizikem zneužití technologií a ztráty soukromí se tímto tématem musíme zabývat. Prakticky každý občan západního světa, dnes však již i občané zemí bývalého třetího světa, může využívat zázraků moderní techniky a vědy. Existují malé přístroje, dříve nemyslitelné, pomocí kterých se lze online připojit k celosvětovému fenoménu Internet, sdílet fotografie, videa, nejrůznější informace a sebe sama ve virtuálním světě. To s sebou nese, vedle nesporných kladů, samozřejmě i řadu rizik.

Spolu s rozmachem moderních informačních technologií, kam je zařazována i „Síť sítí“ – Internet, si společnost musí uvědomit, že rozmach těchto moderních technologií a jejich pronikaní do všech oblastí lidského života s sebou přináší i určitou ztrátu soukromí a další nové hrozby a možnosti zásahů do soukromé sféry každého člověka. Ten tyto technologie, chce-li být zařazen do současné společnosti, musí využívat. Internet má oproti jiným technologiím svá specifika. Aktivity na něm probíhající mohou být velmi anonymní, neosobní, na druhou stranu technologie umožňuje získání až podivuhodně podrobných detailů ze soukromého života lidí, které jsou na něm přístupné. Internet svou otevřeností a de facto i demokratičností jistě významně přispívá k otevřenější společnosti a ke globalizaci celého světa. I Internet je samozřejmě předmětem právní regulace, v některých

státech dokonce i silné cenzury a omezování, nicméně vynutitelnost práva je na Internetu slabší než v jiných oblastech. Na Internetu se dá poměrně jednoduše získat až alarmující množství osobních dat, včetně obrazových záznamů. Každému člověku se může stát, že se objeví na Internetu například delikátní video znázorňující jeho osobu v choulostivých situacích, či jiný video nebo audio záznam vysoce narušující jeho soukromí. Obrana proti takovéto publikaci pak může být někdy velkým problémem. Často se sice objevují soudní rozhodnutí, která zakazují určitou formu jednání na Internetu, nebo požadují stáhnutí citlivého obsahu z určitých internetových stránek, jenže ani tato soudní či jiná ochrana není nikdy stoprocentní.[171]

Jeden z poměrně známých a veřejnosti prezentovaných případů byla kauza americké rodiny Smithových, kteří umístili svou rodinnou fotografii (fotografii rodičů a jejich dvou malých dětí) na sociální síť a také na svůj internetový blog. Tuto fotografii ve zvětšené velikosti však jistý Mario Bertuccio, majitel pražského obchodu Grazie použil (aniž by jakkoliv

---

[171] Z poslední doby je známo třeba rozhodnutí brazilského soudu, které přikázalo celosvětově působícímu internetovému serveru YouTube, aby znemožnil stahování videa zachycujícího soukromí brazilské modelky Daniely Cicarelli a jejího přítele, a to alespoň internetovým uživatelům v Brazílii (s ohledem na teritoriální působnost a pravomoc brazilského soudu). Jde o opakované rozhodnutí v té samé věci, neboť uživatelé serveru YouTube našli cestu, jak předchozí soudní rozhodnutí obejít (předmětné video bylo sdíleno pod jinými jmény atd.).
Server YouTube, ve vlastnictví společnosti Google Inc. se sídlem v americké Kalifornii, je častým terčem soudních rozhodnutí, neboť umožňuje prakticky nekontrolovatelné sdílení videonahrávek všeho druhu, od nahrávky popravy Saddáma Hussaina až po mnohdy i tajně pořízená videa zachycující soukromí amerických středoškoláček v jejich bytech (pomocí webkamer a jiných způsobů). I přes dobrou snahu by nebylo v technických ani personálních možnostech provozovatele serveru v reálném čase v takovém rozsahu kontrolovat obsah všech zveřejňovaných videí. Prostředky ochrany osobnosti, či ochrany soukromí jednotlivce jsou tak v případě těchto serverů omezenější a mohou se zaměřovat spíše na následnou náhradu škody či finanční vyrovnání. Společnost Google Inc. nicméně již v minulosti deklarovala, že vyjde vstříc požadavkům vládních či soudních orgánů na poskytnutí informací o uživatelích jeho serverů a jiných dat, které jsou opodstatněné (např. na základě soudního příkazu), v souladu se zákony USA (kde se nachází sídlo Google Inc.) a pokud požadavek pochází ze země, kde je předmětná informace uložena. Tak byla třeba po delším soudním procesu nakonec poskytnuta brazilským orgánům data o brazilských uživatelích komunitního serveru Orkut.com napojeného na Google, a to v rámci boje a prevenci proti dětské pornografii a šíření nesnášenlivých a rasistických materiálů.
Internetové zdroje:
http://www.lupa.cz/clanky/deset-kroku-ktere-google-pouziva-k-ochrane-soukromi-uzivatelu/
http://technet.idnes.cz/brazilsky-soud-nakazal-youtube-aby-zablokoval-video-pcj-/tec_denik.asp?c=A070105_133229_tec_denik_dno [obojí cit. 2012-01-27].

informoval rodinu Smithových či by si vyžádal jejich souhlas) ve výlohách svých obchodů jako komerční reklamu na svou zásilkovou službu.

Stejně tak je známo z poslední doby několik případů zneužití fotografií či videí v dětské pornografii, kdy sdílení fotografií a videí mezi tisíci uživateli nebylo nikdy v historii snazší, právě díky expanzi informačních systémů jako jsou počítače vybavené připojením k Internetu, chytré (smart) telefony a další osobní komunikační prostředky. Často se citlivé fotografie či videa posílají nejdřív jen mezi partnery nebo nejlepším kamarádům a kamarádkám např. jako důkaz lásky nebo přátelství, někdy jsou takové fotky i formou flirtování. Když se pak ale vztah nebo kamarádství rozpadne, intimní fotky mohou skončit jako pomsta v mobilech dalších známých nebo se veřejně vystaví na Internet. Pak je již riziko narušení intimní sféry vysoce reálné.

5.2 Počítačová kriminalita obecně

Nežádoucí aktivity na Internetu, jež postihují soukromí jeho uživatelů, spadají mnohdy do oblasti tzv. **počítačové kriminality.** S touto oblastí kriminality je však poměrně obtížné bojovat. Internet s sebou přináší problémy někdy neurčitelné soudní jurisdikce a příslušnosti, důkazní problémy, neidentifikovatelné a nevystopovatelné subjekty zločinu atd. Lépe odhalitelné a postižitelné jsou většinou nelegální aktivity provozované v největším rozsahu, kdy se dá jednodušeji vypátrat postižitelný viník. Počítačová kriminalita zaměřená cíleně na menší skupiny jednotlivců či firem je pak o to hůře odhalitelná a pro soukromí lidí o to nebezpečnější. Ten, kdo by si chtěl na Internetu zachovat alespoň určitou míru soukromí, by rozhodně neměl spoléhat na pomoc zvenčí a na to, že státní orgány budou garantovat nějakou míru bezpečnosti v Internetu. Jediná cesta je správné chování v souladu s obecnými bezpečnostními zásadami pro užívání internetových služeb a zejména instalace kvalitních softwarových utilit a jiných ochranných prostředků.

Sám pojem **počítačová kriminalita** je poměrně obtížně definovatelný. Někdy se za počítačovou kriminalitu označují trestné činy zaměřené proti počítačům a trestné činy páchané pomocí počítače. Odbor

bezpečnostní politiky MVČR zpracoval dokument „Analýza současného stavu a trendů vývoje trestné činnosti na úseku informačních technologií a internetu včetně návrhu řešení“. V tomto dokumentu je počítačová kriminalita definována jako *„páchání trestné činnosti, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení včetně dat, nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět této trestné činnosti, ovšem s výjimkou majetkové trestné činnosti, nebo jako nástroj trestné činnosti“*. Není zde tedy pracováno jen se samotným pojmem počítačová kriminalita, ale vzhledem k prolínání výpočetní techniky s komunikačními technologiemi je operováno s termínem **informační kriminalita**. Uvedený pojem začíná nahrazovat původní pojem počítačová kriminalita. V zahraničí se pak stále častěji používá označení **cybercrime**, tedy **kybernetická kriminalita**. Označení kybernetická kriminalita je tak pojmově širší než dosavadní počítačová kriminalita a lépe odpovídá současnému pojetí a faktickému stavu, kdy mnohá trestná činnost je páchána v prostředí kyberprostoru (tím je myšlena oblast počítačových systémů a sítí, v níž jsou ukládána data a v níž probíhá on-line komunikace), zejména v prostředí Internetu.[172]

5.2.1 Trestné činy související s počítačovou kriminalitou v trestním zákoníku

Počítačovou a kybernetickou kriminalitu se snaží postihovat trestněprávní předpisy každého státu. Český trestní zákoník, zákon č. 40/2009 Sb. vychází pojmově, pokud jde o počítačovou kriminalitu, z **Úmluvy o počítačové kriminalitě**, schválené Výborem ministrů Rady Evropy 8.11.2001 Česká republika tuto Úmluvu podepsala v roce 2005, avšak dosud neratifikovala (i řada jiných členů Rady Evropy ji zatím

[172] K tématu počítačové kriminality dále viz např.:
SMEJKAL, V.: Počítačová a internetová kriminalita v České republice. Právní rozhledy, 1999, č. 12
SMEJKAL, V.: Kriminalita v prostředí informačních systémů a rekodifikace trestního zákoníku. Trestněprávní revue, II., 2003.
GŘIVNA, T., POLČÁK, R. a kol.: Kyberkriminalita a právo. Praha, Auditorium, 2008
MATĚJKA, M.: Počítačová kriminalita. Praha: Vydavatelství a nakladatelství Computer Press, 2002, s. 21

neratifikovala) Ani tato úmluva neobsahuje jednotnou definici počítačové kriminality jako takové, ale souhrn aktivit, které by smluvní strany měly v rámci svého práva postihovat jako trestný čin.

Úmluva o počítačové kriminalitě dělí počítačovou kriminalitu do čtyř oblastí:

1. **Trestné činy proti důvěřivosti, integritě a dostupnosti počítačových dat a systémů**
   - neoprávněný přístup
   - neoprávněné odposlouchávání
   - narušování dat
   - narušování systémů
   - zneužívání zařízení
2. **Trestné činy se vztahem k počítači**
   - počítačové padělání
   - počítačový podvod
3. **Trestné činy se vztahem k obsahu počítače**
   - dětská pornografie
4. **Trestné činy související s porušováním autorského práva a souvisejících práv**

Český trestní zákoník upracuje ve své hlavě V. (trestné činy proti majetku) i několik skutkových podstat trestných činů, jež mají přímou souvislost s počítačovou kriminalitou. Jde o následující trestné činy (pro přehlednost uvádím pouze základní skutkové podstaty, trestní zákoník upravuje u každého ze jmenovaných trestných činů i kvalifikované skutkové podstaty):

§ 230 Neoprávněný přístup k počítačovému systému a nosiči informací

(1) Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.
(2) Kdo získá přístup k počítačovému systému nebo k nosiči informací a
a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,
b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,
c) padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo
d) neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat,
bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

Celá norma § 230 trestního zákoníku je konstruována na ochranu informací uložených v počítačovém systému. První odstavec ustanovení tohoto trestného činu upravuje postih překonání bezpečnostního opatření a současně neoprávněného získání přístupu k počítačovému systému. Nevyžaduje se další manipulace s počítačem či s daty, jinými slovy stačí tzv. nabourat se do systému. Postih tedy bude čekat pachatele útoků, kdy pachatel, ať již ručně nebo pomocí robota, zkouší hesla tak dlouho, až se strefí. Obtížněji by však byl již postižitelný pachatel, který by pomocí tzv. sociálního inženýrství vylákal přístupové údaje z jiné osoby podvodným jednáním. Druhý odstavec trestného činu dle § 230 pak postihuje následné jednání hackera či jiné osoby, která již přístup do systému získala a dopustí se následujícího:

- neoprávněně užije uložená data,
- neoprávněně vymaže uložená data nebo je jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu, případně je učiní neupotřebitelnými,
- padělá nebo pozmění uložená data tak, aby byla považována za pravá
- neoprávněně vloží data do systému

§ 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

(1) Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2 vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává
a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo
b) počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části,
bude potrestán odnětím svobody až na jeden rok, propadnutím věci nebo jiné majetkové hodnoty nebo zákazem činnosti.

K naplnění skutkové podstaty tohoto trestného činu není zapotřebí získat přístup k informačnímu systému a eventuálně manipulovat s daty uloženými v tomto systému (tak jak je uvedeno v trestném činu dle § 230). V případě trestného činu dle § 231 postačí, pokud si někdo opatří nebo přechovává zařízení včetně počítačového programu, nebo počítačové heslo, přístupový kód nebo podobný prostředek, jímž lze získat přístup k počítačovému systému, to vše v úmyslu spáchat trestný čin neoprávněného

přístupu k počítačovému systému. Jde o fázi jakési přípravy obstarání si zmíněného zločinného nástroje, která ovšem, zřejmě s ohledem na nebezpečnost, spočívající zejména v obtížné odhalitelnosti, je postihována jako samostatný trestný čin (obdobně je v trestním zákoníku postihováno kupříkladu držení padělatelského náčiní nebo neoprávněné držení platebního prostředku).

§ 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

(1) Kdo z hrubé nedbalosti porušením povinnosti vyplývající ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté
a) data uložená v počítačovém systému nebo na nosiči informací zničí, poškodí, pozmění nebo učiní neupotřebitelnými, nebo
b) učiní zásah do technického nebo programového vybavení počítače nebo jiného technického zařízení pro zpracování dat,
a tím způsobí na cizím majetku značnou škodu, bude potrestán odnětím svobody až na šest měsíců, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

Tento trestný čin upravuje trestné jednání osob, které nakládají s důležitými údaji a způsobí ztrátu nebo změnu počítačových dat či zásah do software počítače či jiného zařízení pro správu dat. Ke spáchání tohoto trestného činu postačí hrubá nedbalost vyplývající ze zaměstnání či funkce. Je však nutné, aby vznikla minimálně značná škoda, tj. škoda v minimální výši 500 tisíc Kč.[173]

Další trestné činy, které upravuje trestní zákoník, jež mají souvislost s počítačovou kriminalitou, jsou trestný čin dle ustanovení § 270 - Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi a trestné činy související s pornografií a dětskou pornografií upravené v ustanoveních § 191 až 193 trestního zákoníku.

5.2.2 Dětská pornografie

Pokud jde o pornografii a zejména pak dětskou pornografii, tak trestné činy související s dětskou pornografií jsou také kybernetické trestné činy, tedy delikty, při jejichž páchání jsou použity prostředky informačních a komunikačních technologií. Informační technologie více než kdykoliv dříve v minulosti umožňují masivní a poměrně jednoduché šíření

[173] Dále viz: SOKOL, T., SMEJKAL, V.: Postih počítačové kriminality podle nového trestního zákona. Právní rádce 7/2009, s. 43.

obrazových materiálů zpodobňujících dětskou pornografii. Naštěstí mnoho států přijalo řadu opatření v boji proti dětské pornografii a lze deklarovat, že i přes masivní šíření dětské pornografie v prostředí Internetu a dalších informačních technologií je dosahováno v boji proti dětské pornografii alespoň částečných úspěchů. Přesto je dětská pornografie i z hlediska této práce jedním z nejvážnějších zásahů do práva na ochranu soukromí, zde konkrétně práva na ochranu soukromí dotčených dětí. V souvislosti s dětskou pornografií se v právní rovině řeší i otázka kolize práva na svobodu projevu. Při řešení této otázky se někdy používá tzv. **test pornografické povahy díla**, který by měl být aplikován obecným soudem, a který spočívá na posouzení, zda celkový dojem díla způsobuje morální pohoršení osobě s běžným cítěním. Nejvyšší soud ČR ve shodě s doktrínou stojí na stanovisku, že za pornografii nebudou považovány „předměty svou povahou určené k vědeckým, uměleckým, osvětovým cílům“. Pokud jde o umělecká díla, nelze je za pornografii považovat ani kdyby dané dílo „zobrazovalo nejintimnější chvíle lidí, příp. i vyvolalo sexuální vzrušení či vzbuzovalo pocit studu nebo ošklivosti“.[174] Hranice mezi uměleckým a neuměleckým projevem však je hranicí velmi vágní a subjektivní.[175]

Sexuálním zneužíváním dětí se zabývá i již shora zmíněná **Evropská úmluva o počítačové kriminalitě**. Ta ukládá členským státům úmluvy přijmout opatření a postihovat následující jednání:

- výroba dětské pornografie za účelem jejího rozšiřování prostřednictvím počítačových systémů,
- nabízení nebo zpřístupnění dětské pornografie prostřednictvím počítačových systémů,

---

[174] Dále viz např. BARTOŇ, M.: Virtuální pornografie, limity svobody umělecké tvorby a svobody projevu a trestní zákon. Právní rozhledy 17/2008, s. 617.

[175] Nejvyšší soud řešil ve svém rozhodnutí ze dne 28.12.2004 sp. zn. 7 Tdo 1077/2004 případ majitele modelingové agentury, který za honorář pořizoval fotografické materiály zobrazující děti, které byly nabízeny prostřednictvím sítě Internet. Soud v daném případě dovodil následující právní názor:
Za pornografické dílo zobrazující dítě (tj. osobu mladší osmnácti let) ve smyslu ustanovení § 205 odst. 1 písm. a) TrZ je třeba pokládat např. snímky obnažených dětí v polohách vyzývavě předvádějících pohlavní orgány za účelem sexuálního uspokojení, snímky dětí zachycující polohy skutečného či předstíraného sexuálního styku s nimi apod. Nejde-li o takové snímky, pak závěr o pornografickém charakteru díla nelze bez dalšího dovozovat jen z toho, že jsou za účelem uspokojení osob trpících sexuální deviací (tj. osob, pro které jsou sexuálně atraktivní nedospělé osoby) zpřístupňovány takovými prostředky, které tyto osoby vyhledávají (např. počítačovou sítí Internet).

- rozšiřování nebo přenos dětské pornografie prostřednictvím počítačových systémů,
- získání dětské pornografie prostřednictvím počítačových systémů pro sebe či pro druhé,
- držení dětské pornografie v počítačovém systému nebo v počítačovém prostředku pro ukládání dat.[176]

Signatáři úmluvy o počítačové kriminalitě jsou kromě evropských států i Kanada, Japonsko, Jihoafrická republika a USA. V USA je dětská pornografie dlouhou dobu penalizována. Při zavedení trestnosti přechovávání závadných materiálů pro privátní účely to vnímala široká veřejnost v USA spíše jako zásah do soukromí, čili základního lidského práva. Otázka ochrany ústavních práv je ve Spojených státech amerických podstatná, zásah do soukromí nebo svobody slova a tisku byl několikrát posuzován Nejvyšším soudem Spojených států amerických (viz například debatu nad ústavní ochranou dětské pornografie v rozhodnutí *New York v. Ferber* z roku 1982 – v tomto rozhodnutí Nejvyšší soud USA deklaroval, že právo na svobodu projevu dle 1. dodatku ústavy neomezuje stát v zakazování prodeje materiálů zobrazujících děti zapojené do sexuální aktivity).[177]

I v českém prostředí je dětská pornografie jevem rozšířeným, jak ukazuje několik případů z poslední doby, které cituji v poznámce pod čarou.[178] V roce 2010 policisté evidovali případů spojených s dětskou

---

176 Podrobněji viz BAYEROVÁ, M.: Evropská úmluva o počítačové kriminalitě a sexuální zneužívání dětí. Trestněprávní revue 5/2003, s. 156.

177 Detailněji k trestání dětské pornografie v USA viz studie POREMSKÁ, M.: Pornografie v USA. Trestněprávní revue 8/2008, s. 233.

178 Níže jsou uvedeny příkladmo některé kauzy, které byly v minulosti řešeny v ČR v souvislosti s dětskou pornografií, tak jak o nich informovala česká média [vše cit. 2012-02-13]:
Europol rozbil patrně největší pedofilní síť na internetu. V rámci jedné z nejrozsáhlejších operací svého druhu se podařilo rozbít rozsáhlou mezinárodní síť dětské pornografie na internetu. Při zátahu bylo zatčeno přes 180 podezřelých, sdělil Evropský policejní úřad. Osoby podezřelé z pedofilie byly členy online fóra na boylover.net, které podporovalo sexuální vztahy mezi dospělými a mladými chlapci. Webové stránky umožňující přístup k pedofilním fotografiím a filmům operovaly ze serveru se sídlem v Nizozemsku. Zdroj: http://zpravy.idnes.cz/europol-rozbil-patrne-nejvetsi-pedofilni-sit-na-internetu-po1-/zahranicni.aspx?c=A110316_161013_zahranicni_abr
Ředitel základních škol dostal za držení dětského porna podmínku. Obvodní soud pro Prahu 2 uložil bývalému řediteli dvou pražských základních škol Miroslavu Galbavému dvouletý podmíněný trest za šíření a přechovávání dětské pornografie a ohrožování mravnosti. Policisté zajistili v budovách škol a v jeho bydlišti videokazety,

pornografií 130, v roce 2011 to bylo již 193, což je téměř o polovinu více.[179] Dětskou pornografii a zneužití fotografií a videí na Internetu umožňují často uživatelé Internetu svou neopatrnou aktivitou, i samy děti. Nezletilí své

DVD a další materiály s pornem, na kterém byly nezletilé dívky. Zdroj: http://zpravy.idnes.cz/reditel-zakladnich-skol-dostal-za-drzeni-detskeho-porna-podminku-pyl-/krimi.aspx?c=A100323_113542_krimi_cen

Policie obvinila třicet lidí z velkého zátahu proti držitelům dětského porna. V materiálech, které kriminalisté zadrželi (bylo zadrženo celkem 160 počítačů), převažují fotografie a videa s dospívajícími dívkami, ale někdy snímky ukazovaly sex dospělých s dětmi, kterým může být teprve jeden rok, nebo sex dětí se zvířaty. I v tomto případu figuroval mezi dětmi oblíbený učitel. Zdroj: http://zpravy.idnes.cz/policie-obvinila-tricet-lidi-z-velkeho-zatahu-proti-drzitelum-detskeho-porna-189-/krimi.aspx?c=A100318_072759_krimi_cen

Cizinec, který psal školačkám, jde před soud. Obětí je podle žaloby 118. Českolipský okresní soud řeší počátkem roku 2012 případ muže, v jehož počítači policisté nalezli dětskou pornografii a ohromné množství korespondence s nezletilými dívkami, které dotyčný kontaktoval na sociální síti Facebook a přes komunikační programy ICQ a Skype. Objekty svého zájmu si vybíral podle fotek nebo dalších informací, které o sobě školačky poskytly. Zdroj: http://zpravy.idnes.cz/cizinec-ktery-psal-skolackam-jde-pred-soud-obeti-je-podle-zaloby-118-1cc-/krimi.aspx?c=A120202_102307_usti-zpravy_oks

V Chorvatsku odpykal trest za dětské porno. Česká policie ho zatkla znovu. Břeclavská policie zadržela jednapadesátiletého muže, který podle ní vyráběl dětské porno. Podezřelý byl přitom před týdnem propuštěn z vězení v Chorvatsku, kde byl přes rok kvůli focení nahých dětí na pláži (Chorvati u muže našli skoro 2 600 fotografií nahých dětí). Česká policie zjistila, že pořizoval a sbíral nahrávky obnažených dětí hrajících si na plážích už od roku 2004. Nebyla to jen chorvatská letoviska, ale i rekreační zařízení v Česku. Zdroj: http://zpravy.idnes.cz/v-chorvatsku-odpykal-trest-za-detske-porno-ceska-policie-ho-zatkla-znovu-1q7-/krimi.aspx?c=A101013_163924_krimi_jba

Policie si přišla pro muže, který sdílel desetitisíce klipů s dětským pornem. Policie v roce 2009 obvinila šestadvacetiletého muže z Olomoucka z přechovávání a šíření dětské pornografie. V počítači měl téměř šedesát tisíc filmů a videoklipů, na některých byly teprve čtyřleté děti. Přístup k souborům umožnil i dalším uživatelům internetu. Zdroj: http://zpravy.idnes.cz/policie-si-prisla-pro-muze-ktery-sdilel-desetitisice-klipu-s-detskym-pornem-1vn-/krimi.aspx?c=A090327_122245_krimi_pei

Rakouská pedofilní centrála měla 63 českých klientů. V roce 2007 provedl zátah rakouský spolkový kriminální úřad proti pedofilskému serveru. Při něm bylo zajištěno 8 terabajtů dat na několika počítačích a záznamových médiích. Mezi dvěma a půl tisíci klienty ze 77 států se našlo i 63 Čechů, kteří využívali služeb tohoto serveru. Zdroj: http://www.novinky.cz/krimi/108773-rakouska-pedofilni-centrala-mela-63-ceskych-klientu.html

Policisté zadrželi sedm Čechů a tři Poláky šířící dětskou pornografii. Policisté v roce 2011 zadrželi skupinu pachatelů, která organizovala fotografování pod záminkou propagace nudismu a za tímto účelem si prý zaplatila inzeráty i v českém tisku. Fotografování se účastnily celé rodiny, ale ve skutečnosti šlo jedině o to získat snímky nebo videonahrávky dětí. Některým "modelům" bylo jen šest nebo osm let. Pornografické snímky a filmy pak členové skupiny rozšiřovali prostřednictvím internetu. Zdroj: http://zpravy.idnes.cz/policiste-zadrzeli-sedm-cechu-a-tri-polaky-sirici-detskou-pornografii-1zg-/krimi.aspx?c=A111205_173125_krimi_brd

[179] Dětské pornografie v Česku výrazně přibylo, víc je i případů znásilnění. Zdroj: http://zpravy.idnes.cz/detske-pornografie-v-cesku-vyrazne-pribylo-vic-je-i-pripadu-znasilneni-133-/krimi.aspx?c=A120119_114531_krimi_zep

fotky například sami posílají pedofilům za kredit do mobilu nebo v případě, pokud je daný pedofil určitým způsobem zmanipuluje.[180]

Často pomůže, pokud daný stát přijme účinná opatření pro internetové prostředí, kdy podstatně **ztíží nebo znemožní přístup na závadné stránky**. V červnu 2009 byl například v Německu přijat zákon o ztížení přístupu k obsahům s dětskou pornografií (Gesetz zur Bekämpfung der Kinderpornografie in Kommunikationsnetzen ze dne 19.6.2009, tisk 604/2009 BGBl). Pokud budou některé webové stránky obsahovat dětskou pornografii, pak mohou být německými úřady přímo zrušeny. Pokud toto možné nebude, pak budou uživatelé upozorněni, že vstupují na stránku s nelegálním obsahem a že další prohlížení je trestnou činností.[181] Podpůrci zákona argumentují situací v Norsku, kdy se denně díky automatickému přesměrování na stránku s výstrahou zabrání přístupu na stránky s dětskou pornografií až 15 000 uživatelům. V Dánsku je to dokonce 50 000 případů.[182]

Možnost odpojení uživatele internetu od stránky s pornografickým obsahem je řešena i v České republice.

Těžko si někdo z nás umí představit svůj život bez každodenního prohlížení webových stránek, posílání emailových zpráv či sdílení soukromých informací na Facebooku, ale právě tyto obyčejné rutinní činnosti jsou zárodkem pro možnost šíření dětské pornografie. Zejména poslední jmenovaná aktivita je v poslední době velmi oblíbená, ale mnozí náctiletí si neuvědomují, že nezabezpečením svého profilu stovkám neznámých uživatelů a zveřejňováním mnohdy velmi intimních fotografií často ulehčují práci pachatelům dětské pornografie.

5.2.3 Nové druhy informační kriminality

Pokud by někdo psal práci zaměřenou na ochranu soukromí ve vztahu ke sledovacím technologiím například před patnáci lety, jeho práce

---

[180] Děti na internetu riskují, své fotky posílají pedofilům za kredit do mobilu. Zdroj: http://zpravy.idnes.cz/deti-na-internetu-riskuji-sve-fotky-posilaji-pedofilum-za-kredit-do-mobilu-1ul-/domaci.aspx?c=A091122_195910_domaci_vel

[181] GŘIVNA, Tomáš; HERCZEG, Jiří. Právo na přístup k Internetu, blokace stránek a digitální gilotina. *Trestněprávní revue*. 2010, roč. 9, č. 05, s. 144. ISSN 1213-5313.

[182] Tamtéž. s. 144.

by v dnešní době byla patrně hodně zastaralá. Během několika málo let se vynořilo tolik nových pojmů, nových způsobů jednání a činností, jaké si před 15-20 lety lidé vůbec neuměli představit. Ruku v ruce s moderními technologiemi samozřejmě jde i možnost jejich zneužití pro činnosti, které jsou sice lidskému rodu přirozené (v každé populaci se objevuje jisté procento deviantního chování), nicméně jde o činnosti nežádoucí a někdy nebezpečné.

Aktivitu na Internetu lze také poměrně jednoduše monitorovat a odposlouchávat. Emailová korespondence prochází přes řadu různých uzlů a směrovačů, kde lze nasadit její přímý odposlech, stejně tak i komunikace přes různé chatovací programy, IP telefonie atd., o odesílání nejrůznějších citlivých informací na bankovní servery ani nemluvě.

Již několik let používají na Internetu hackeři a jiní škůdci ke své činnosti tzv. *boty* či celé *botnety* (*bot network*). To jsou relativně samostatné utility, schopné infikovat cizí počítač, rezidovat v něm a pomocí dálkové správy plnit příkazy svého autora. Boty mají většinou podobu trojských koní, nicméně trendem poslední doby je vytvářet hybridní programy, schopné plnit několik funkcí současně. Botnet je pak celá síť takto infikovaných počítačů navzájem propojená. Boty a botnety se liší od typických virů a jiného malware především svou autonomií a schopností plnit příkazy dle pokynů dálkové správy. V tom je nutno spatřovat velkou hrozbu. Boty a botnety jsou nejčastěji používány pro šíření spamu, dále pro DoS útoky (útoky, které mají znepřístupnit a zahltit určitou službu, počítač, server či celou síť), pro sniffing (odposlech dat a vůbec všech aktivit na napadeném počítači) atd. Boty jsou dokonce schopny vyřazovat z činnosti a pozměňovat antivirové programy a firewally na napadených počítačích tím, že mění jeho celé systémové soubory. Podle expertů je až sedm procent celosvětového počtu počítačů nějakým způsobem zapojeno do infikované bot sítě. Před soud se přitom dostanou jen ta nejzávažnější celosvětová narušení, menší cílené útoky například na jednotlivce nejsou prakticky nijak vystopovatelné.[183] Tyto infikované automatizované sítě lze napadnout i

[183] Asi prvním soudním procesem s tvůrcem botnet systému, resp. celé armády tzv. zombie počítačů je případ kalifornského občana Jeansona Jamese Anchety. Podle zprávy internetového serveru SecurityFocus z 23.1.2006 se u kalifornského soudu doznal

zničit, resp. převzít.[184] Snadné šíření těchto automatických programových utilit a vytváření sítí umožňují zejména uživatelé, kteří se nikterak nebrání proti útokům a hrozbám Internetu. Nastává odklon od tvorby škodlivého softwaru, který by pouze mazal data či jinak poškozoval hostitelský počítač a spíše se vytváří rezidentní software, který zůstává skryt v napadeném počítači a vykonává zde různou nežádoucí činnost (sledovací aktivity, rozesílání reklamních spamů atd.), především za účelem krádeže dat, případně za účelem reklamy.

Oproti tomu však existují i speciální programy (tzv. remailery) a postupy, jež umožňují odesílat emaily a jiná data anonymně, nevystopovatelně, přičemž lze i zamezit jejich odposlechu pomocí speciálního šifrování a směrování. Stejně tak lze maskovat celou svou identitu při pohybu na Internetu pomocí anonymizerů IP adresy i jinak. Lze říci, že riziko pohybu a přítomnosti dané osoby na Internetu lze využitím bezpečnostních postupů a nástrojů snížit na rozumnou míru. Člověk, který by chtěl užívat Internet alespoň v relativním soukromí, by rozhodně měl instalovat různé *firewally, antivirové* a *antispyware* programy a měl by dodržovat obecně platné zásady bezpečného chování na síti.

Pokusím se nyní provést základní rozdělení rizik a způsobů chování, které je spojeno s moderními technologiemi a je způsobilé podstatně zasáhnout do soukromí jednotlivců. Níže uvedené způsoby chování se obvykle řadí mezi tzv. počítačovou kriminalitu a vykazují společné charakteristické rysy, zejména jde obvykle o jednání, které alespoň

Ancheta ke zločinům, které mu byly kladeny za vinu. Měl vytvořit síť 400.000 infikovaných počítačů, které nabízel k pronájmu k různým nelegálním aktivitám jako je šíření spamu, reklamy apod., za což měl získat až 60.000 dolarů.
V říjnu 2005 byli v Holandsku zatčeni tři muži, kteří kontrolovali ohromnou síť obsahující přes 1.500.000 napadených počítačů na celém světě a využívali ji ke krádeži citlivých údajů.
V květnu 2006 se doznal jiný kalifornský občan - Christopher Maxwell, že spolu s dalšími dvěma komplici vytvořil botovou síť, pomocí níž vyřadil až na krizový záložní systém celou Northwest nemocnici v Seattlu. Tato síť měla také napadnout jiné instituce a způsobit škody ve statisících dolarů a naopak více než 100.000 dolarů měl Maxwell vydělat na příjmech z nevyžádaných reklam.
Zdroj v anglickém jazyce: The SecurityFocus Website, SecurityFocus Symantec Corporation, http://www.securityfocus.com/news/11370 [online], [cit. 2012-02-18].

[184] Tak se hovoří o vzájemných útocích těchto sítí botnetů mezi jednotlivými zločineckými internetovými komunitami a dokonce i o globální kybernetické válce botnetů, v níž by mohl během několika málo minut během masivních nárazových útoků vzniknout jediný botnet s miliony infikovaných osobních i firemních počítačů. To už se však dostáváme poněkud mimo naše téma.

potenciálně může poškozovat soukromí ostatních či zneužívat jejich osobní data.

Spyware

Lidé pracující na osobním počítači mohou být samozřejmě vedle obecně známého nebezpečí počítačových virů postiženi i relativně novými hrozbami, například tzv. **spywarem**. To je označení pro skupinu programů a utilit, které jsou zaměřeny na **sledování aktivit na počítači** (spy = špehovat). Když je pak počítač připojen na Internet, tyto utility odesílají získaná data ke svým šiřitelům či na zcela náhodné adresy.

Spyware je podskupinou tzv. malware, tedy programů, které běží na osobním počítači povětšinou zcela bez vědomí jeho uživatele a jež mohou různým způsobem škodit – zpomalováním počítače, poškozováním dat či odesíláním různých informací z počítače do Internetu. Velká část těchto utilit má také ryze reklamní či obchodní účel. Tyto programy, zejména pak z kategorie spyware, mají přístup ke všem souborům uloženým v počítači a průběžně monitorují veškeré procesy a činnosti v systému. Zneužití například v situaci, kdy člověk používá internetové bankovnictví bez zabezpečení vyššího řádu, či má na svém počítači uložena důvěrná data, je pak zcela evidentní. Různé *keyloggery* jsou schopny sledovat veškeré stisky klávesnice či dokonce snímat části obrazovky (tzv. *screen-scraping*). Ze záznamu takovéhoto *keyloggeru* se následně dají vyčíst všechna přístupová hesla, která člověk během práce zadal, čísla kreditních karet, ale i obsah komunikace zadané přes takto monitorovaný počítač, internetové adresy atd. Šikovný hacker dále dokáže pomocí dálkového přístupu z počítače na druhé straně planety získat z cílového počítače veškerá data a dokonce jej i ovládat.[185]

[185] Viry a různé utility se nevyhýbají dokonce ani mobilním telefonům a kapesním počítačům. S ohledem na jejich softwarovou i hardwarovou variabilitu, danou množstvím různých výrobců, je však globálnější napadení zatím nepravděpodobné.

Spam

Další oblastí, jež podstatně zasahuje do soukromé sféry uživatelů Internetu, je **spam**.[186] Spam jsou nevyžádaná sdělení nejrůznějšího druhu (zejména reklamní či nabídek na různou pochybnou spolupráci), šířená pomocí elektronické pošty, nejrůznějších internetových diskusních fór, komunikačních prostředků, ale např. i pomocí mobilních telefonů. V České republice dlouho neexistovala právní úprava problematiky spamu. Přinesla ji až s účinností od 1.6.2002 novela zákona o regulaci reklamy, zákon č. 138/2002 Sb., která **zakázala šíření nevyžádané reklamy**, pokud vede k výdajům adresáta nebo pokud adresáta obtěžuje.

Od září 2004 je pak v platnosti tzv. **„antispamový" zákon** č. 480/2004 Sb. o některých službách informační společnosti, který transponoval do českého právního řádu směrnice Evropské unie upravující tuto problematiku. Jednalo se zejména o směrnici Evropského Parlamentu a Rady 2002/58 ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací – tzv. **směrnice o soukromí v elektronických komunikacích**. Tato směrnice upravuje danou otázku ve svém čl. 13 nazvaném Nevyžádaná obchodní sdělení. Podle jeho prvého odstavce platí, že *„Automatické volací systémy bez zásahu člověka (automatické volací přístroje), faximilní přístroje (faxy) nebo* ***elektronickou poštu*** *je možno použít pro účely přímého marketingu pouze v případě účastníků, kteří k tomu dali předchozí souhlas."* Členským státům EU bylo uloženo danou směrnici transponovat do svých národních právních řádů. V ČR se tak stalo již zmíněným **zákonem č. 480/2004 Sb. o některých službách informační společnosti.**

Úprava boje proti spamu je obsažena i v zákoně č. 127/2005 Sb. o elektronických komunikacích, ve znění pozdějších předpisů, kdy je v jeho § 93 stanoveno, že *použít adresu elektronické pošty pro odeslání zprávy nebo zpráv třetím osobám bez souhlasu držitele této adresy elektronické pošty je*

[186] K problematice spamu a příbuzných témat viz sdělení Komise Evropských společenství č. KOM (2006) 688 ze dne 15.11.2006 nazvaném Boj proti spamu a špionážnímu („spyware") a škodlivému software („malicious software"). Dokument je dostupný např. z www: http://europa.eu/legislation_summaries/information_society/internet/l24189a_en.htm [cit. 2011-11-05].

zakázáno. Ustanovení § 95 a § 96 pak upravuje problém ve vztahu k vytvářeným seznamům účastníků elektronických komunikací.

Krádeže identit

Čím dál obvyklejšími se stávají různé druhy **krádeží identit.** Vedle zneužití osobních údajů fyzicky existující osoby (použití čísel PIN kódů cizích kreditních karet, různých přihlašovacích hesel do databází apod.) běžně dochází k ovládání celých cizích počítačů (tzv. *botnety, zombie počítače*) a jejich prostřednictvím jsou pak mimo jiné např. tajně rozesílány spamy, viry a jiná data. Podle mnoha odborných názorů se nelegální krádeže dat, hackerství a obdobné nežádoucí aktivity stávají stále častěji předmětem zájmu profesionálních kriminálních skupin. Od dříve spíše nadšených amatérů, kteří rozesílali viry spíše pro svou zábavu a z potřeby zviditelnit a proslavit se ve své komunitě, jsou v současné době schopní hackeři najímáni jako vysoce cenění profesionálové. Počítačová kriminalita a kyber - terorismus se tak stávají čím dál větší celospolečenskou hrozbou. Krádeže identit i v méně nebezpečném rozsahu mohou však představovat **velké narušení soukromí běžných uživatelů Internetu**. Vedle poměrně neškodného vydávání se za určitou osobu na různých komunikačních diskusních fórech jde pak zejména o zneužití různých kódů a bezpečnostních hesel, jakož i identifikačních znaků uživatelova počítače. Tímto způsobem pak mohou různí Internetoví podvodníci využívat uživatelův počítač k páchání nežádoucích aktivit a jejich činnost je tak ještě nesnadněji odhalitelná a vystopovatelná. Ve světě jsou ostatně známy poměrně četné případy, kdy do bytu nic netušícího občana přišla policie a on musel vysvětlovat, že za rozšiřováním dětské pornografie či nacistických propagačních materiálů rozhodně nestojí.[187]

[187] V ČR se zmedializoval případ krádeže identity známého překladatele Viktora Janiše. IP adresa počítače pana Janiše byla totiž stejná, jakou používali podvodníci v případu nelegálních inzerátů v inzertních novinách Annonce. Dne 30.1.2003 byla u něj provedena domovní prohlídka, byl mu zabaven počítač i počítač přítelkyně a spolubydlícího. Kauza ukazuje na problémy tzv. sdílených veřejných IP adres (kdy jednu IP adresu sdílí několik uživatelů v rámci jedné sítě) apod., a dokazuje, že soukromí zcela nevinných lidí může být i díky běžnému používání Internetu velmi citelně narušeno, byť se později vše řádně vysvětlí. Zdroj: NACHTMANN, P.: Ukradli vám IP adresu? Policie vám sebere počítač!. In: Idnes.cz, Praha: MAFRA, a.s., 1998-2007. Dostupné z www: http://technet.idnes.cz/ukradli-vam-ip-adresu-

Phishing

Velkým problémem může být zneužití důvěřivosti mnoha lidí, kdy se spousta podvodníků prezentuje na Internetu jako někdo jiný. Za tímto účelem mohou vytvořit opravdu věrohodně vypadající internetové fake stránky, na první pohled nerozeznatelné např. od domovských stránek velké bankovní instituce. Vylákání různých vysoce zneužitelných dat a hesel je pak o to snazší. Po zaslání podvrženého emailu s žádostí o ověření určitých dat či za účelem jiné aktivity je uživatel přesměrován na podvrženou stránku, kam důvěřivě v domnění, že jde o stránky banky, zadá své osobní údaje včetně čísla kreditní karty a PINU…. Jde o takzvaný ***phishing*** (někdy překládáno jako „*rhybaření*"). Zde se tedy nabízí paralela s anglickým slovem fishing – rybaření, kdy rybář nahazuje háčky v naději, že uloví nějakou rybku (oběť). Phishing nepochybně spadá do oblasti krádeží identit. V této souvislosti se hovoří i o tzv. **sociálním inženýrství** – to je termín pro metodu, jež vede legitimní počítačové uživatele k poskytnutí užitečných informací, které pomáhají útočníkovi získat neautorizovaný přístup do jejich počítačového systému.

Spy-phishing

je situace, kdy v počítači nasazený trojský kůň zachytává určitá data (přístupová hesla) z nějaké předem určené internetové stránky a dále je rozesílá třetí straně. Rozšiřují se také útoky za účelem vylákání důležitých kódů a čísel na IP telefonii - tzv. ***vishing,*** což je obdoba phishingu u VoIP telefonie, kdy jsou automaticky telefonicky rozesílány informace o smyšlených hrozbách v internetovém bankovnictví s nutností zavolat na určená čísla jakoby asociovaná s bankovní institucí, na kterých je pak nutno zadat důležitá data jako číslo kreditní karty, PIN a jiná, která pak již lze snadno zneužít - nebo na mobilní telefony, tam se pak hovoří o tzv. ***SMiShing****u*.

policie-vam-sebere-pocitac-fte-/sw_internet.asp?c=A030220_5202715_sw_internet [cit. 2012-02-18].

Pharming

Vedle phishingu existuje jeho sofistikovanější varianta, tzv. ***pharming***, kdy hacker pozmění záznamy v systému doménových jmen (DNS – Domain Name Systém) tak, že po zadání doménového jména na uživatelově počítači (např. *www.xxxxbanka.cz*) dojde na přesměrování nikoliv na pravé stránky, nýbrž na hackerem vytvořené fake stránky – jsou přitom přiřazovány jiné IP adresy. Nic netušící uživatel na těchto stránkách, jež mohou vypadat naprosto stejně jako stránky pravé, zadá s důvěrou své přihlašovací údaje, hesla, čísla kreditních karet a hacker může slavit úspěch. Tento druh pharmingu nicméně vyžaduje špatně zabezpečený hostitelský server, který by šlo přesměrovat. Pokročilé metody pharmingu ale umožňují dokonce přímý zásah do souborů v uživatelově počítači (např. zásah v souboru *hosts* v operačním systémy Windows), kdy dojde k úpravě, jež bude následně automaticky přesměrovávat vybraná uživatelem zadaná doménová jména na internetové stránky hackera. Na uživatelově počítači lze většinou počítat s mnohem nižší mírou zabezpečení než je tomu např. u serverů velkých bankovních institucí. Pharming je pro svou sofistikovanost mnohem náročnější na odhalení, než je phishing. Ten je určen spíše pro zanedbatelné množství lidí, kteří se takříkajíc chytnou (v obrovských objemech lákavých spamů toto číslo však může být pro hackery již zajímavé). Boj s phishingem a pharmingem je o to těžší, že modifikované internetové stránky nebývají většinou v provozu více než 48 hodin.[188]

Sniffing

Sniffing (v překladu „čenichání, čmuchání“) slouží k monitoringu a odchytávání elektronické komunikace v rámci počítačové sítě, především

[188] Společnost Microsoft v obraně před phishingem bojuje pomocí akce Microsoft Global Phishing Enforcement Initiative (GPEI), kdy podala např. jen v USA 117 soudních žalob, jenž následně vedly k uzavření asi 4 700 phishingových stránek. Stejná akce probíhá od března 2006 i v Evropě, na Blízkém východě a v Africe. Blíže [online] viz VŠETEČKA, R.: Sto phishingových gangů zamíří před soud. In: Idnes.cz, Praha: MAFRA, a.s., 1998-2007. Dostupné z www: http://technet.idnes.cz/sto-phishingovych-gangu-zamiri-pred-soud-f1i-/software.asp?c=A060321_101732_bezpecnost_vse [cit. 2012-02-18].
V rámci boje proti phishingu, pharmingu a obdobným hrozbám souvisejícím s krádežemi identit byla založena i globální organizace The Anti-Phishing Working Group (APWG) – blíženi k jejím aktivitám viz její internetové stránky v anglickém jazyce http://www.antiphishing.org.

Internetu, cizím subjektem, který není odesílatelem ani adresátem této komunikace.

Sexting

Slovo sexting je složeninou vzniklou ze slov „sex“ a „textování“ = elektronické rozesílání textových zpráv, fotografií či videa se sexuálním obsahem).

Kybergrooming

Tímto pojmem se obvykle označuje jednání osoby, která se na Internetu snaží vyvolat falešnou důvěru, zmanipulovat vyhlédnutou oběť a přimět ji k osobní schůzce, kde může dojít ke zneužití.

Kyberstalking

Je vlastně stalking v prostředí internetu, mobilních telefonů a dalších informačních technologií, kdy je obět ze strany stěžovatele bombardována nejrůznějšími obtěžujícími zprávami, SMS, emaily, zasíláním fotografií a videí apod.

Kyberšikana

Je de facto šikana v prostředí informačních technologií (Cyberbullying). Povětšinou se jedná o úmyslné publikování nadávek, zesměšňujících informací, zveřejňování choulostivých nebo pozměněných fotografií a videí, zasílání výhružek a jiných zpráv a další činnosti, které mají především poškodit, popřípadě zesměšnit oběť před okolím.

Happy slapping

Je v poslední době poměrně populární mezi mladými lidmi. Tento pojem znamená de facto „spokojené fackování“. Účelem happy slappingu je nečekaně fyzicky napadnout buď mladistvého, nebo dospělého člověka, přičemž komplic agresora celý čin nahrává na mobilní telefon nebo kameru. Získané video poté umístí na Internet (např. na populární server YouTube).

Video je určeno k tomu, aby pobavilo, obětí se může stát prakticky kdokoliv.[189]

Problematika těchto modelových směrů chování a užívání nových termínů je vysoce aktuální, právem a právní vědou nepříliš zatím uchopená. Mnoho z těchto způsobů komunikace a jednání je ve většině demokratických států kriminalizováno, často však jen pomocí aplikace skutkových podstat trestných činů obecnějších. V době, kdy se současné platné trestní normy přijímaly, prakticky žádné z výše uvedených způsobů jednání nebyly rozšířené a známé. Pokud jde o Happy slapping, tak kupříkladu ve Velké Británii byl takový zločin poprvé potrestán až v roce 2008, kdy byla do vězení na dva roky poslána dívka, která na svůj mobilní telefon natočila muže, jenž byl jejími komplici ubit k smrti. Tento muž zemřel v nemocnici na následky natržené sliznice. Komplicové ve věku 19ti a 17ti let byli odsouzeni k 7 a 6 letům odnětí svobody. Státní návladní, který měl tento případ na starosti, prohlásil: „To je poprvé, co byl nějaký takový čin odsouzen k trestu odnětí svobody.“[190]

5.2.4 Pravomoci státních orgánů a meze soukromí na Internetu

Především **v návaznosti na udílení větších pravomocí bezpečnostním orgánům** dochází v poslední době v porovnání s minulostí k nevídaným zásahům do soukromí. V prosinci 2006 například proběhla v Klášterci nad Ohří velká policejní akce, kdy byly na základě řádných soudních příkazů provedeny domovní prohlídky ve 14 domácnostech, přičemž byly v těchto soukromých bytech zabaveny domácí počítače. Podnětem pro celou akci bylo trestní oznámení majitele videopůjčovny,

---

189 Blíže k tématu bezpečí na Internetu a v prostředí informačních technologií viz mimo jiné i internetové portály a jejich materiály:
Metodický portál www.rvp.cz, viz např. odkaz: http://clanky.rvp.cz/clanek/s/Z/9673/STRUCNY-UVOD-DO-PROBLEMATIKY-BEZPECNEHO-INTERNETU.html/ [cit. 2011-11-05]
projekt E-Bezpečí dostupný na portále e-bezpeci.cz, viz např. odkaz: http://cms.e-bezpeci.cz/content/blogcategory/0/20/lang,czech/ [cit. 2011-11-05].
projekt Národního centra bezpečnějšího internetu na doméně saferinternet.cz, viz např.:
http://www.saferinternet.cz/pro-rodice/sexting-kybergrooming [cit. 2011-11-05].

190 Blíže viz http://cms.e-bezpeci.cz/content/view/71/39/lang,czech/

který díky sdílení dat na vysokorychlostní internetové komunální síti citelně přicházel o zisk (svou roli zde sehrála i lobby protipirátských organizací jako je Business Software Alliance (BSA) či Česká protipirátská unie (ČPU), které samy podávají řady trestních oznámení a bojují proti nelegálnímu šíření autorských děl na Internetu).[191]

Ačkoliv není jisté, zda se podaří v soudním řízení prokázat vinu a úmysl konkrétních fyzických osob, které měly nelegálně nabízet data, celá akce nicméně ukazuje, že rozšiřování pravomocí bezpečnostním orgánům logicky vede i k mnohem citelnějším zásahům do soukromí. Z našeho pohledu není až tak zajímavé, zda a v jaké míře dochází k činnosti, která je v rozporu s autorským a trestním zákonem, nýbrž to, jaké má stát prostředky pro boj proti tomuto fenoménu a jak moc může při boji s touto kriminalitou legálně zasáhnout do soukromí fyzických osob. Před změnou zákonů, které stanovily povinnost poskytovatelům internetového připojení poskytovat údaje o veškerém provozu na jednotlivých internetových připojeních, se policejní aktivity omezovaly na potírání těch nejzávažnějších trestných činů v oblasti ochrany autorských práv. Policie ČR, resp. orgány činné v trestním řízení sice mohly vyžadovat po providerech již zmíněné logy, nicméně neexistovala povinnost tyto logy vytvářet a archivovat. Postihovány tak dosud byly pouze výdělečné aktivity různých prodejců a šiřitelů nelegálních autorských děl, kteří tak činili za úplatu. Příkazy k domovní prohlídce soukromého bytu byly vydávány jen zcela výjimečně, prakticky jen u velkých dealerů, kteří touto činností profitovali na vlastní účet.

Jak je však v současné době vidět, je poměrně jednoduché na základě několikaměsíčního monitorování internetového provozu získat soudní příkaz k domovní prohlídce prakticky jakékoliv právnické i fyzické osoby. Není samozřejmě jisté, že podezřelým fyzickým osobám, u nichž byly zabaveny domácí počítače a další materiál, nakonec bude udělen trest, či zda vůbec budou konkrétní osoby obviněny. Celá akce však zcela jistě vyvolá v dané komunitě, která ve větších objemech, byť stále jen pro svou potřebu, stahuje

[191] Viz např. článek Jana Wágnera: V ČR probíhá rozsáhlý zátah proti uživatelům P2P sítí, zveřejněný na internetovém serveru Lupa.cz (www.lupa.cz), server o českém Internetu. ISSN 1213-0702. Dostupný z www: http://www.lupa.cz/clanky/v-cr-probiha-rozsahly-zatah-proti-uzivatelum-p2p-siti/ [cit. 2012-02-18].

autorská díla (a z principu P2P sítí současně i sdílí), strach a obavy. Řada jednotlivců tak může raději této činnosti dobrovolně zanechat.

Zde je vidět nesporný silně preventivní význam dané policejní akce. Není určitě sporu o tom, že nelegální sdílení autorských děl na Internetu je nežádoucím celospolečenským problémem, otázkou však je, zda boj proti tomuto jevu pomocí podrobného monitorování internetových aktivit občanů a následných domovních prohlídek v soukromých bytech je přiměřenou cestou, zda neexistuje alternativa, která by méně zasahovala do práva fyzických osob na nedotknutelnost soukromí.[192]

Myslím, že rozhodně přijatelnější by bylo tyto nové pravomoci a technické monitorovací prostředky v rukou státních orgánů používat opravdu jen pro boj se **závažnou kriminalitou a terorismem**. Ostatně zejména tímto účelem bylo zavádění nové bezpečnostní legislativy, jejíž vlna po teroristických útocích proběhla po celém světě, a jež často citelně zasahuje do soukromí jednotlivců, odůvodňováno.

Monitorovat běžný provoz českých domácností a využívat nově svěřených policejních pravomocí za účelem eventuelního trestněprávního postihu v řádu finančních pokut či několikaměsíčního trestu odnětí svobody (navíc ve většině případů u dosud jinak netrestaných osob) je přinejmenším zarážející.

To, že jde v každém případě stejně o trestnou činnost (jejíž odhalování u běžných občanů je přitom pro policejní složky logicky

---

[192] Dle mého osobního názoru jde ale o natolik závažný zásah do soukromí, kterým mohou být postihnuti i zcela nevinní lidé (data od providerů, na jejichž základě došlo k domovním prohlídkám, nemusí mít s ohledem užívání jedné přípojky pomocí různých routerů dostatečnou vypovídací hodnotu, časté je i zneužívání cizích IP adres a krádeže identit na P2P sítích, v rámci jedné rodiny může být dokonce problém s jistotou určit konkrétního viníka – to vše se však většinou zjistí až ve fázi trestního řízení po provedené domovní prohlídce), že je na místě se ptát po odůvodnitelnosti využívání těchto trestněprávních institutů při potírání takového druhu kriminality, která je v ČR navíc bohužel stále běžná a rozšířená, a to někdy dokonce i na pracovištích státních orgánů. Daným opatřením může být z čistě logického pohledu postižena vždy jen naprosto minimální část „obětních beránků“, což z hlediska rovnosti před zákonem není jistě žádoucí jev, když drtivá většina jiných lidí zůstane nepotrestána (a to čistě z důvodu nedostatečné kapacity policejních složek). Pro boj s tímto druhem kriminality by bylo jistě vhodnější zvolit jiné metody než invazivní domovní prohlídky a monitorování internetových aktivit občanů. Nejde ostatně o problém pouze v České republice, nýbrž na celém světě, kdy dochází s ohledem na globalizaci a moderní sdělovací technologii k celosvětovému propadu tržeb klasického způsobu prodeje autorských děl a nastává doba jiného způsobu legálního šíření těchto autorských děl.

relativně nejjednodušší), která by měla být celospolečensky vymýcena, by nemělo být argumentem odůvodňujícím zavádění výše popsaných postupů. Jsem toho názoru, že využívání těchto sledovacích postupů a technologií ze strany policejních orgánů či zpravodajských služeb je odůvodnitelné opravdu jen u nejzávažnější kriminální činnosti a v rámci boje proti terorismu. V boji s méně závažnou kriminalitou není z důvodu ústavního zaručení práva na ochranu soukromí takovýto invazivní zásah do soukromí jednotlivců přípustný.

5.3 Zveřejňování fotografií v médiích

Do obsahu této práce jsem zařadil i kapitolu Zveřejňování fotografií v médiích, neboť toto téma je poměrně aktuální, vysoce sledované a závažné. Jsou to právě nejrůznější média, která mají moc zasáhnout ve vyšší míře do soukromí občanů, a to jak jednotlivců, tak i vysoce exponovaných osob jakými jsou politici, herci, zpěváci, sportovci apod. Je nepochybné, že všichni jednotlivci požívají ochrany svého soukromí, lze však současně deklarovat, že u osob tzv. veřejného zájmu existuje oprávněný zájem na jejich kontrole, právu na vyšší přísun informací o jejich životě, jakož i právo na svobodu projevu. Právo na soukromí si tak může **konkurovat** s jinými právy, a v souvislosti s veřejně činnými osobami je to nejčastěji **právo na informace** a s ním úzce spjatou **svobodou projevu.**

Ve věci existuje rozhodnutí Ústavního soudu sp. zn. I. ÚS 453/01, kde se Ústavní soud pokusil vypořádat s otázkou, za jakých podmínek lze publikovat informace difamační povahy, které bývají nejčastějším důvodem sporů o ochranu soukromí. Svou argumentaci Ústavní soud dále rozvedl v nálezu sp. zn. IV. ÚS 23/05, v němž se vyslovil k tomu, kdy lze postihnout základní právo na čest, přičemž tyto závěry lze vztáhnout i na další osobnostní práva. Dovodil, že toto právo se uplatňuje jednak ve sféře soukromé, jednak sociální, kterou tvoří oblast společenská, občanská a profesionální. Zatímco v prvé sféře platí úplné informační sebeurčení, v dalších již nikoli, protože se zde mohou vyskytovat fakta, která jsou předmětem oprávněného veřejného zájmu. Její tzv. vnější okraj tvoří veřejná sféra, v níž podle mínění Ústavního soudu nejsou žádná omezení pro šíření

pravdivých informací a jež se zcela kryje s profesionální sférou veřejně činných osob. Jak tedy patrno, byla tím na první pohled zcela otevřena možnost publikovat o těchto osobách cokoli z jejich veřejného života za podmínky, že je to pravdivé. Tato možnost se týká i dovolené kritiky (uvedený judikát byl ostatně vydán v souvislosti se svobodou projevu a bylo jím přiznáno právo televizní redaktorky na kritické hodnocení veřejného činitele).[193]

V České repblice je zveřejňování citlivých fotografií známých osobností široce diskutovaným tématem, které obvykle rozvíří veřejné mínění, vždy když se objeví fotografie ze soukromí známých osob.[194]

Je ovšem otázka, zda lze oddělit veřejný život určité osoby od jejího života soukromého. U veřejně činných osob to mnohdy totiž prakticky možné není, resp. daná hranice je sporná a někdy hůře nalezitelná.[195]

---

193 Srovnej k tématu dále i MATES, P.: ÚS k ochraně soukromí veřejně činných osob. Právní zpravodaj 12/2007.

194 Například v roce 2009 byla medializována kauza tzv. **fotografií tehdejšího premiéra Topolánka ve vile italského premiéra Berlusconiho**. Berlusconi s rodinou Topolánka byl zachycen na řadě fotografií, které následně byly publikovány v italském tisku. Berlusconi se bránil proti zveřejnění a italské úřady, posuzující v daném případě porušení práva na soukromí mu daly za pravdu a nařídily zákaz dalšího zveřejňování fotografií. Tato kauza souvisela s dalšími **fotografiemi a videem z Toskánska**, kde byl zachycen Topolánek s dalšími politiky, lobbisty a podnikateli. Tato kauza je pak propojena přes osobu, která měla dané fotografie a video natočit (Petra Bakeše, bývalého specialistu na sledování v Úřadu pro zahraniční styky a informace (ÚZSI)) s kauzou Savoy. **Kauza Savoy** představovala únik videonahrávky pořízené hotelovými kamerami v pražském hotelu Savoy se záznamem schůzky lobbisty Miroslava Šloufa a prezidentova kancléře Jiřího Weigla, na níž se sešli krátce před volbou prezidenta republiky v roce 2008. Byť v kauze Savoy padly odsuzující trestní rozsudky a soud deklaroval porušení práv nahrávaných osob, rozsudky byly postaveny zejména na porušení služebních povinností osoby, která nahrávky získala. V dané věci se vyjadřoval i ÚOOÚ, který prohlásil, že hotel Savoy porušil zákon na ochranu osobních údajů a že kamery v hotelu byly instalovány a provozovány nelegálně (hotel neinformoval své návštěvníky o jejich natáčení kamerovým systémem, samotné nahrávání a uchovávání záznamu pak hotel nenahlásil ÚOOÚ, neregistroval svůj kamerový systém, a konečně nebyl vůbec dán důvod pro oprávněné provozování kamerového systému - šlo o nadměrné a zřejmě i nadbytečné snímání prostoru kamerami.
Zdroje:
Berlusconi nechal zabavit fotografie z večírků s nahým Topolánkem. Dostupné online na:
http://www.mediafax.cz/zahranici/2878466-Berlusconi-nechal-zabavit-fotografie-z-vecirku-s-nahym-Topolankem [cit. 2012-01-26]
ÚOOÚ: Kamery v hotelu Savoy porušovaly zákon. Dostupné online na:
http://www.epravo.cz/top/clanky/uoou-kamery-v-hotelu-savoy-porusovaly-zakon-54328.html?mail [cit. 2012-01-26]

195 Někdy je naopak stanovení jasné hranice poměrně jednoduché. Příklad neetického, ale i nepochybně protiprávního jednání představovalo zveřejnění fotografií Petry Buzkové na titulní straně v deníku Super v roce 2001, jak se nahá sluní na pláži s odhaleným

Za jeden z prvních případů neoprávněného zveřejnění fotografie konkrétní fyzické osoby, zasahující podstatně do jejího soukromí, se označuje osud fotografie Otto von Bismarcka na jeho smrtelné posteli. Bismarckův zaměstnanec, lesník Louis Spörcke, se nechal podplatit od dvou fotografů z Hamburku, aby jim pomohl se zajištěním fotografie slavného státníka. Tito fotografové, Max Priester a Willy Wicke, bývají označováni za první paparazzi v dějinách. Po skonu Bismarcka za pomoci lesníka Spörckeho fotografové vnikli do Bismarckova domu a pořídili čtyři fotografie zesnulého na jeho posteli. Tito fotografové se pak snažili snímky zpeněžit, nicméně rodina zemřelého Bismarcka zamezila jejich snahy soudním procesem. Bylo požadováno zničení fotografie a veškerých kopií. V řízení soud posuzoval nejen vniknutí na cizí pozemek, ale i skutečnost, jestli může mít fotograf autorské právo na snímek jiného člověka. Soudce rozhodl ve prospěch mrtvého kancléře s tím, že fotografové nejednali v zájmu Německa, ale jen pro svůj vlastní prospěch a že nemohou profitovat z nezákonného vniknutí do Bismarckova domu (viz rozsudek ze dne 28.12.1899, Bismarck). [196] V návaznosti na tento rozsudek byl v Německu přijat zákon upravující autorská práva k portrétům a fotografiím (autorský zákon - KunstUrhG - KUG, ze dne 9.1.1907 (RGBl. 1907, p. 7)). Podle ustanovení § 22 tohoto zákona, které je stále v platnosti, obraz nebo podobizna osoby nesmí být běžně zveřejněna bez souhlasu dané osoby. Po smrti fyzické osoby musí předmětný souhlas ke zveřejnění dát členové rodiny dotčené osoby; toto právo mají po dobu 10 let od smrti dotčené osoby. Ustanovení § 23 odst. 1 KUG deklaruje, že souhlasu není třeba, pokud se jedná o fotografie z oblasti soudobých dějin. Tato výjimka nicméně neplatí, jestliže by zveřejnění bylo v rozporu s oprávněnými zájmy této osoby. [3] K soudobým dějinám patří zejména fotografie osob, které patří mezi tzv. absolutní osobnosti současných dějin *(„Absolute Person der*

---

poprsím. Zcela jistě zde nešlo o veřejný zájem na uveřejnění těchto fotografií, který by nějak souvisel s výkonem její politické funkce, ale o pouhou touhu po senzaci.

[196] Další informace viz článek prof. Thomase Lundmarka Princess Caroline in Bismark's Shadow: Photographs of Public Figures in German Law, dostupný na http://jurist.law.pitt.edu/world/gercor2.htm [online] [cit. 2012-01-26]

Zeitgeschichte").[197] Pro zařazení do okruhu takových osob je rozhodující význam, který jim veřejnost na základě jejich postavení a známosti ve společnosti přikládá. Patří sem zejména monarchové, představitelé států, jako prezidenti, premiéři a další význační politici.

P. Hajn dělí osoby, jež se dostanou do hledáčku mediální pozornosti, do dvou základních kategorií, a to na **"osobnosti veřejného zájmu"** a na tzv. **"ostatní fyzické osoby"**, přičemž osobnosti veřejného zájmu ještě dále kategorizuje na:

- *nositele veřejné autority (politici, církevní hodnostáři, vědci a vysokoškolští profesoři aj.),*
- *fyzické osoby populární v jiných oblastech veřejného života (sportovci, umělci apod.),*
- *fyzické osoby, které se staly předmětem veřejného zájmu na základě náhodných skutečností (vysoký věk, autonehoda atd.),*
- *fyzické osoby, které se staly předmětem veřejného zájmu na základě činů negativního charakteru (pachatelé zločinu apod.).*[198]

Osobnosti veřejného zájmu bývají taktéž děleny do dvou základních kategorií, a to na tzv. **osoby absolutního veřejného zájmu**, kam spadají osoby, dobrovolně vstupující do veřejného života (jedná se hlavně o politiky) a veřejnost má oprávněný zájem být informována šíř o jejich soukromí (s výjimkou úzké privátní sféry - soukromí v užším smyslu), a na tzv. **osoby relativního veřejného zájmu,** což jsou osoby, které jsou známé jen díky určité skutečnosti. Veřejnost má právo být o těchto osobách informována jen ve vztahu k těmto skutečnostem, na jejichž základě se staly známými.

---

[197] K německému rozlišování absolutních a relativních osobností soudobých dějin srov. rozhodnutí *Gertz v. Robert Welch* , kde Nejvyšší soud USA definoval dva druhy veřejných osobností:
- veřejná osobnost v obecném smyslu – osoba, která je tak známá, že se stane veřejnou osobností pro všechny účely a ve všech souvislostech,
- veřejná osobnost v omezeném smyslu – osoba, která se dobrovolně angažuje v konkrétní veřejné záležitosti, a stane se tak z ní veřejná osobnost pouze v této věci.

Blíže k tématu viz článek Herczeg, J.: Případ Caroline von Hannover – zveřejnění fotografií ze soukromí prominentů, [Právní rozhledy 23/2004.

[198] Hajn, P. Reklama a nositelé veřejné autority II. Právo a podnikání, květen 2000, č. 6, s. 3.

Z relativně nedávné doby existuje známý případ nejstarší dcery monackého knížete, Caroline von Hannover, která si koupila na trhu v Paříži láhev olivového oleje. Někdo ji přitom pozoroval a vyfotil. Sporná fotografie následně vyšla v německém časopisu Bunte a princezna se domáhala zákazu zveřejňování této fotografie a dalších podobných snímků, které ji ukazují v běžných situacích, jako je nakupování, návštěva restaurace či jízda na koni. Německé soudy nejprve s ohledem na výše uvedenou výjimku z povinnosti udělení souhlasu se zveřejněním u absolutních osobností soudobých dějin žalobu princezny zamítly, ta se však domáhala ochrany u Evropského soudu pro lidská práva ve Štrasburku. Ten judikoval, že je nutno rozlišovat mezi zpravodajstvím vyvolávajícím politickou nebo veřejnou diskusi a takovým, které slouží pouze k uspokojení zvědavosti, vůči němuž mají i tzv. absolutní osobnosti současných dějin právo na ochranu soukromí, bez ohledu na to, že určitá informace se týká události odehrávající se na veřejnosti.[199]

Konfliktem mezi dvěma ústavně zaručenými právy, konkrétně právem na ochranu osobnosti, a to zejména ve formě práva na nedotknutelnost soukromí, a na druhé straně právem na informace a svobodu tisku, se zabýval německý Spolkový soudní dvůr v souvislosti s uveřejněním snímků prázdninového sídla (spolu s příslušným popisem cesty k tomuto sídlu) známé německé televizní novinářky a moderátorky. Byť moderátorce odvolací soud nakonec v plném rozsahu nevyhověl, přesto lze z rozhodnutí dovodit zajímavé podněty ke zpracovávané problematice. V této kauze Spolkový soudní dvůr mimo jiné konstatoval, že soukromí prominentů nekončí u domovních dveří vlastního domu a je nutné ho chránit

[199] Viz Rozsudek Evropského soudu ze dne 24. 6. 2004, stížnost č. 59320/00, ve věci Caroline von Hannover v. Německo. Soud mimo jiné uvedl následující: *„Všeobecným právem na ochranu osobnosti chráněná soukromá sféra není omezena na vlastní domov. Jednotlivec musí mít zásadně možnost se zdržovat také na jiných, zřetelně odloučených místech, kde bude chráněn před pozorností tisku.Všeobecné právo na ochranu osobnosti není zaručeno v zájmu komercializace vlastní osoby. Ochrana soukromí ustupuje do pozadí, jestliže někdo sám zveřejňuje určité události, které jsou obvykle pokládány za privátní, třeba tím, že uzavírá exkluzivní smlouvy o zpravodajství ze svého soukromí. Rozsah ochrany osobnostních práv rodičů a dětí je posílen čl. 6 Ústavy, pokud jde o zveřejnění snímků, které zobrazují specifickou náklonnost rodičů k dětem. Záruky svobody projevu dle čl. 5 Ústavy zahrnují také zábavné publikace a příspěvky, stejně jako doprovodné fotografie. To platí zásadně také pro zveřejnění snímků, které zobrazují veřejně činné osoby v běžném životě nebo v soukromí.“*

i v blízkém okolí jejich obydlí (nemovitosti), pokud takto získané pohledy do soukromí nejsou třetím osobám jinak přístupny a nejsou na vůli dotčených. Nikdo proto nemusí strpět, aby jeho soukromí bylo proslíděno při překonávání existujících překážek za pomoci takových nástrojů, jakými jsou např. žebřík, teleobjektiv, letadlo apod.[200]

Daná problematika je řešena na celém světě, zmiňme ještě alespoň okrajově Spojené státy americké.[201]

Jak již bylo zmíněno výše v této práci, prostředky ochrany osobnosti proti nezákonnému zásahu do soukromí bývají často nedostatečné. Zisk vydavatelů bulvárních periodik prakticky vždy převyšuje výši přisouzeného přiměřeného zadostiučinění, které se pohybuje obvykle v řádu desetitisíců korun.

Závěrem této podkapitoly bych rád zmínil kauzu fotografií dětí určených k adopci. V roce 2011 se v ČR objevila kauza zveřejňování fotografií a citlivých informací dětí, pro které byli hledáni adoptivní rodiče nebo pěstouni. Tyto fotografie a informace zveřejňoval na svém webu Fond ohrožených dětí (FOD). Na předsedkyni fondu a další pracovníky fondu dokonce podal Úřad na ochranu osobních údajů trestní oznámení, když předtím zjistil závažné nedostatky v nakládání s osobními údaji dětí. Fond se naopak bránil tím, že děti nebo jejich zákonní zástupci dali souhlas se zveřejněním své fotky, protože chtějí najít rodinu.[202]

---

200 Předmětný rozsudek Spolkového soudního dvora ze dne 9.12.2003 (VI ZR 373/02 - KG) je ve zkrácené verzi dostupný v Právních rozhledech - SRN: BGH (Spolkový soudní dvůr), VIZR 373/022, [PR 16/2004 str. 621]

201 V USA existují poměrně jasně formulované zákony, doložené řadou precedenčních případů. V nich se střetává ochrana soukromí a právo na informace. Existuje dokonce seznam veřejných prostor, kde se fotografovat dovoluje a kde fotografování vyžaduje speciální povolení nebo kde to možné není. Dům, byt, hotel, auto, tam všude je třeba žádat souhlas. Dále se hlídá, aby fotografie nebyla užita bez svolení fotografovaného k podpoře prodeje výrobku. V Americe může fotograf snímat z veřejného prostoru, ulice, chodníku i dění na zahradách, v okně i domě, ale nesmí narušit vlastnictví a bez povolení na zahradu vstoupit. Rovněž tak nesmí užívat příliš extrémní teleobjektiv a hledat extrémní úhly záběru, jako je např. lezení po stromech atd. Fotograf je limitován běžným pohledem chodce z ulice. Viz Štecha, P. Inventura dokumentaristických projektů – víra v pravdivost fotografie. Článek ze dne 19.9. 2002. Dostupné na http://www.paladix.cz/clanky/inventura-dokumentaristickych-projektu-vira-vnbsppravdivost-fotografie.html [cit. 2012-01-26].

202 Je pravda, že veřejné umisťování fotografií dětí funguje od 60. let 20. století, kdy jistý Antonín Mores z Olomouce dal do časopisu Vlasty inzerát, že děti hledají rodiče. Fotografie nevidomého chlapce, romské holčičky a chlapce, který měl jen jedno oko, vzbudily velký zájem. Mores dostal během krátké doby 150 žádostí o tyto děti, z toho ve 40 případech se jednalo o nevidomého chlapce. Viz zpravodajský článek na webu

Byť byly uznávány argumenty pro zveřejnění fotografií zejména s poukazem na dobrý úmysl najít touto cestou dětem náhradní rodinu, ve věci vydal veřejný ochránce práv stanovisko, kde mimo jiné deklaroval, že náhradní rodinná péče v České republice není založena na přímém zprostředkování z nabídky dětí komukoli. Ani orgánům sociálně-právní ochrany dětí, zařízením pro ústavní výchovu, ani nevládním organizacím nedává žádný zákon oprávnění zveřejňovat osobní údaje o dětech vhodných pro náhradní rodinnou péči na Internetu. Tyto informace, včetně citlivých údajů o zdravotním stavu či etnickém původu, mohou být poskytovány pouze státem prověřeným zájemcům o náhradní rodinnou péči, nikoli široké veřejnosti.[203]

Již před stanoviskem ombudsmana bylo vydáno ve věci stanovisko Ministerstva práce a sociálních věcí, které podrobně popsalo daný případ a označilo za nepřípustné zveřejňování osobních údajů a fotografií dětí, kterým má být zprostředkována náhradní rodinná péče, na internetu či v tisku.[204] Ministerstvo se zabývalo i otázkou souhlasu dětí a jejich zákonných zástupců se zveřejněním údajů a fotografií na internetu a dovodilo, že „Zveřejnění údajů a fotografií na internetu či v jiných médiích lze podle platné právní úpravy podložit pouze výslovným souhlasem osoby, o jejíž záznam nebo snímek se jedná nebo jejího zákonného zástupce (§ 9 písm. a/ zákona č. 101/2000 Sb.). V této souvislosti si je však třeba klást otázku, kdo je v případě nezletilého dítěte oprávněn souhlas dát, aby takový právní úkon byl jednak platný, a jednak nebyl v rozporu se zájmem dítěte, jakožto objektivní a směrodatnou právní kategorií.” Ministerstrvo dovodilo, že zákonný zástupce takovou osobou často není (neplní své povinnosti, proto je hledána náhradní péče), stejně tak souhlas samotného dítětě bude nutné

Eurozprávy dostupný online na http://domaci.eurozpravy.cz/kauzy/15124-vesecka-vratila-policii-pripad-fondu-ohrozenych-deti/ [cit. 2012-01-26].

[203] Viz stanovisko Veřejného ochránce práv Veřejné inzerování dětí pro náhradní rodinnou péči je nepřípustné. Dostupné online na http://www.ochrance.cz/tiskove-zpravy/tiskove-zpravy-2012/verejne-inzerovani-deti-pro-nahradni-rodinnou-peci-je-nepripustne/ [cit. 2012-01-26]

[204] Stanovisko MPSV ve věci oprávnění subjektů provádějících zprostředkování náhradní rodinné péče a osob pověřených k výkonu sociálně-právní ochrany dětízveřejňovat osobní údaje dětí. Dostupné online na: http://www.mpsv.cz/files/clanky/10285/Stanovisko_MPSV-osobni_udaje_deti.pdf [cit. 2012-01-26]

posuzovat s ohledem na jeho volní a rozumovou vyspělost odpovídající jeho věku.

5.4 Sociální sítě

Sociální sítě jsou jedním z nejmódnějších, nejaktuálnějších a nejdiskutovanějších pojmů na celosvětové síti Internet. Snad každý člověk, který používá Internet, se s nimi již setkal a má s nimi přímou zkušenost. Pokud jde o tuto práci, za sociální síť považuji službu na Internetu, která registrovaným členům umožňuje vytvářet si osobní (ale dnes již často i firemní) veřejný či částečně veřejný profil, komunikovat spolu, sdílet informace, fotografie, videa, provozovat chat a další aktivity. Vzájemná komunikace mezi jednotlivými uživateli sociálních sítí pak probíhá buď soukromě mezi dvěma uživateli, nebo hromadně mezi uživatelem a skupinou s ním propojených dalších uživatelů. Jako asi první internetová sociální síť je označována komunita Sixdegrees, vzniklá již v roce 1997, posléze ale víceméně zanikla. V roce 2003 vzniká portál MySpace, v roce 2004 pak Facebook.

Někdy se rozlišuje mezi sociálními sítěmi, které většinou vyžadují registraci svých uživatelů (fungují na principu jasně definovaného členství), a mezi sociálními médii, kam sociální sítě také spadají, ale které jsou širším pojmem; zahrnují de facto veškeré internetové aplikace, které mají za cíl interakci uživatelů, jejich spolupráci a sdílení obsahu. Ve své práci zmiňuji v této kapitole sociálních sítí např. server Youtube a různé mediální servery určené pro sdílení videa a fotografií, někdy by patrně nebyly označeny jako sociální síť, ale spíše sociální médium, pro potřeby této práce v tom však praktický rozdíl nevidím.

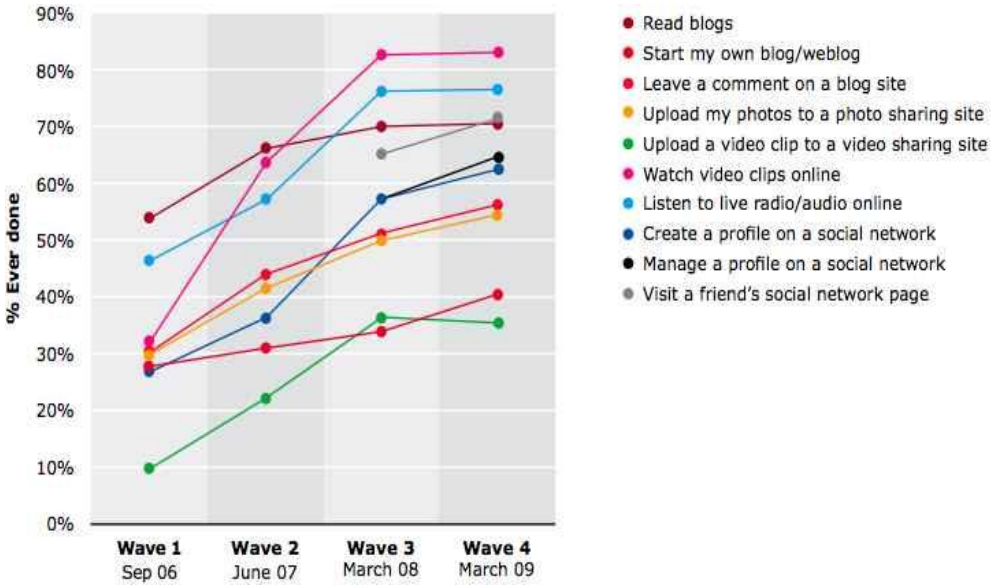
Uživatelé sociální sítě používají zejména ke sdílení fotografií, videa, zpráv nejrůznějšího charakteru, souborů a k nejrůznější další interakci a komunikaci.

Fenoménem sociálních sítí a sociálních médií se již několik let zabývá mediální výzkumná agentura Universal McCann, která každoročně od roku 2006 zveřejňuje studie zaměřené právě na výzkum sociálních sítí a médií. Podle jejího výzkumu z roku 2009 pokud jde o aktivity uživatelů

internetových sociálních sítí a médií vítězí sledování videoklipů (82,9 %), čtení blogů (72,8 %). Studie dále uvádí, že 76% uživatelů sociálních sítí uploaduje (nahrává) fotky, 33% pak uploaduje videa; jako zajímavost je pak zmíněno, že 98% aktivních internetových uživatelů na Filipínách již vidělo online video, například v USA, Koreji, nebo ve Španělsku sleduje či sledovalo online video 8 z deseti uživatelů. Tato data jsou přitom starší dvou let, dnes tedy budou údaje ještě vyšší.[205]

Tabulka seřazení jednotlivých aktivit podle četnosti (2006 – 2009)

(Zdroj: agentura Universal McCann)



Vedle nesporných výhod a možností, které sociální sítě a média na Internetu přinášejí, existuje však i **řada rizik**. Za jedno z nejdůležitějších témat, která jdou ruku v ruce s užíváním sociálních sítí, je označováno téma ztráty soukromí, či ohrožení soukromí uživatele internetové sociální aplikace. Uživatel sociální sítě tím, že vystavuje své fotografie, videa a další záznamy a informace, odhaluje často ve velké míře své soukromí a svůj svět. To s sebou logicky nese riziko zneužití.

Evropská agentura ENISA (European Network and Information Security Agency) se zaměřila na výzkum spojený s užíváním speciálních sítí

[205] Jednotlivé studie dostupné na Internetu na stránkách agentury Universal McCann www.umww.com, v češtině jsou pak k dispozici výtahy ze studií například zde: http://www.tyinternety.cz/socialni-site/wave-4-socialni-media-v-cislech-od-universal-mccann-85 http://www.lupa.cz/clanky/aktivni-uzivatele-v-cesku-sleduji-online-video/ [cit. 2012-02-15].

jejich uživateli a koncem roku 2010 vydala poměrně zajímavou studii „Online as soon as it happens“. Ve studii se pokusila mimo jiné i o výhled do roku 2014, kde se snaží předvídat pozitivní i negativní aspekty fungování sociálních sítí a jejich dopady na život lidí. Organizace ENISA sice nepopírá příznivé efekty sociálních sítí v oblasti on-line spolupráce, ale obává se úniku citlivých osobních dat, které jsou v těchto sítích jen pod velmi omezenou kontrolou uživatelů a podle ní by státy EU měly začít uvažovat o reálných sankcích za přečiny v této oblasti. ENISA také doporučuje Evropské komisi revizi existující směrnice o ochraně dat. Report dále upozorňuje na příliš bezstarostné chování uživatelů sociálních sítí, kteří zde bez jakýchkoliv obav zveřejňují řadu citlivých údajů. To je výraznou hrozbou nejen pro soukromí, ale i pro ohrožení pověsti člověka (například při objevení „nevhodné fotografie“ zaměstnavatelem) a dokonce může dojít podle reportu k psychickému poškození v důsledku pocitu, že uživatel je neustále sledován.

Ve zprávě jsou zmíněny i konkrétní případy narušení soukromí. Zpráva zmiňuje kupříkladu případ zneužití video nahrávky zachycující útok násilníka na cestující v nočním autobuse v Paříži. Jistý policista toto video nasdílel na svém profilu na Facebooku a video se začalo neskutečně rychle šířit po celém světě. Oběť napadení si stěžovala podanou žalobou u soudu namítajíce porušení tajemství probíhajícího vyšetřování. Policista sice video ihned smazal, nicméně na další osud nahrávky, kolující mnoha kanály po Internetu již neměl vliv. Jiný případ se pak stal v říjnu 2009, kdy řecká organizace přijímající žádosti o odstranění nelegálního obsahu na Internetu obdržela report jisté mladé ženy, která prokázala, že její expřítel vytvořil na internetu její falešný profil s jejími fotografiemi, kde byla dotčená žena znázorněna nahá. Profil byl následně odstraněn.[206]

Díky možnosti označovat lidi na fotografiích, kterou nabízí většina sociálních sítí, je velmi snadné vyhledat na internetu něčí fotografii. Mladým lidem hrozí na internetu i další rizika, jako je navazování známostí

[206] Krátké shrnutí studie v českém jazyce je dostupné online na webu ICT manažer na http://www.ictmanazer.cz/2011/11/socialni-site-zivna-puda-pro-spionaze-i-paranoiu/, celá studie je pak v anglickém znění dostupná na webu organizace ENISA. Studie Online as soon as it happens. Dostupné online na: http://www.enisa.europa.eu/act/ar/deliverables/2010/onlineasithappens [cit. 2012-02-05]

za účelem sexuálního zneužití (grooming) a kyberšikana. Děti a mladiství potřebují vhodné nástroje, jimiž by mohli zabezpečit a odpovědným způsobem spravovat svou identitu na internetu.

Podle celoevropského průzkumu vypracovaného pro Evropskou komisi má 77 % mladých lidí ve věku 13–16 let a 38 % dětí ve věku 9–12 let profil na stránkách sociální sítě. Čtvrtina dětí, které navštěvují stránky sociálních sítí, jako je Facebook, Hyves, Tuenti, Nasza-Klasa, SchuelerVZ, Hi5, Iwiw nebo Myvip, uvádí, že jejich profil je „veřejný“, což znamená, že ho všichni vidí, a mnoho dětí tam má svou adresu a/nebo telefonní číslo.[207] Jiná studie, výzkum společnosti Microsoft, uvádí, že 79 procent dospívajících v Evropě aktivně používá sociální sítě.[208]

Evropská komise vyvíjí aktivity i ve vztahu k sociálním sítím. Podle dokumentu zpracovaného jejím orgánem pro ochranu osobních dat a jejich bezpečnost (Article 29 Data Protection Working Party) – Opinion 5/2009 „on online social networking“ existuje řada rizik při provozování a užívání sociálních sítí. K datům uživatelů sociálních sítí mívají například přístup nejen jejich provozovatelé, ale i zástupci třetích stran (provozovatelé spřátelených serverů, reklamní servery apod.). Pracovní skupina dovozuje, že na režim provozování sociálních sítí (a to i když je provozovatel mimo EU) se vztahuje evropské nařízení o ochraně dat (nařízení 95/46/EC). Deklaruje řadu povinností, které se vztahují zejména na provozovatele sociálních sítí. Provozovatelé by měli uživatele jasně informovat o své identitě, o proceduře nakládání s osobními údaji, o použití dat třetími stranami, o případném sdílení dat v kategoriích třetími stranami a o použití citlivých dat. Provozovatelé by měli varovat uživatele předem ohledně případných bezpečnostních rizik, měli by uživatelům sdělit, že mohou porušit zákon vložením informace o někom jiném - provozovatel by měl informovat uživatele, že pokud nahraje fotku nebo informaci týkající se

[207] Viz tisková zpráva Evropské komise - Digitální agenda: Podle průzkumu používají sociální sítě čím dál mladší děti a mnohé si nejsou vědomy rizik v oblasti ochrany soukromí. Zpráva je dostupná na webu Evropské komise online na: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/479&format=HTML&aged=1&language=CS&guiLanguage=en [cit. 2012-02-15].

[208] Viz Tisková zpráva společnosti Microsoft ze dne 9.2.2010: Polovina dětí reaguje na internetu na zprávy od cizích lidí – ze zvědavosti. Dostupné online na: http://www.microsoft.com/cze/presspass/msg/20100209_news1.mspx [cit. 2012-02-15].

někoho jiného, měl by k tomu mít souhlas této osoby. Uživatelé by měli mít přístup k jednoduchému systému, ve kterém mohou vznést stížnost k otázce ochrany dat k provozovateli sociální sítě.[209]

Obecné **povědomí lidí o možnostech zneužití moderních technologií** a hrozbě, kterou užívání moderních technologií představuje, je stále v některých případech poměrně nízké. Proto nepřekvapí zprávy z médií například o nedávném pokusu kanadských vědců z University of British Columbia, Vancouver, Kanada, kdy tito vědci založili tzv. Síť sociálních botů (Socialbot Network /SbN/), pomocí které infiltrovali prostředí populární sociální sítě Facebook a za pomocí touto sítí vytvořených profilů bylo přidáno jako přátelé celkem 3.055 osob z původně rozeslaných 8.570 žádostí o přátelství.[210] Zajímavý je i údaj o celkovém přenosu dat tohoto experimentu (směrem dovnitř systému bot sítě přinesl celkem 250 GB dat, ven pouze 3 GB dat). Tento experiment myslím názorně ukazuje zranitelnost současného stavu stále teprve začínajících sociálních sítí, které pořád ještě nemají propracovány zavedené systémy ochrany soukromí a technických záruk ochrany. Stejně tak i uživatelé těchto sítí nemají vypěstovány základní návyky chování, které by rapidně omezily možnosti průniku neoprávněných osob nebo systémů do soukromí těchto uživatelů. Ochranné systémy sítě Facebook byly schopny zadržet cca 20 procent „útoků“ automatizované sítě kanadských výzkumníků, zbytek útoků mohli však sami odmítnout a „zneškodnit“ sami uživatelé, to se však v poměrně vysokém, až alarmujícím procentním čísle případů, nestalo. Výzkumníci v průběhu osmitýdenního experimentu získali obrovské množství osobních dat uživatelů sítě Facebook, údaje o jméně, profilu (včetně fotografií), pracovišti, emailové adresy atd. atd. Lze deklarovat, že pokud určité procento uživatelů povolí přístup těmto narušitelům uživatelského prostředí

---

209 Celé znění dokumentu Opinion 5/2009 „on online social networking“ je v anglickém jazyce dostupné na http://www.scribd.com/doc/16736099/ARTICLE-29-DATA-PROTECTION-WORKING-PARTY-Opinion-52009-on-online-social-networking [cit. 2011-11-05].

210 Zdroj viz internetově přístupný archiv publikací University of British Columbia - Publications of the Laboratory for Education and Research in Secure Systems Engineering (LERSSE) – The Socialbot Network: When Bots Socialize for Fame and Money. Dostupné online na: http://lersse-dl.ece.ubc.ca/record/264/files/ACSAC_2011.pdf?version=1 [cit. 2011-11-05].

do systému, zvyšuje se pravděpodobnost dalšího proniknutí a snazší další masivnější infiltrace nelegálního „vetřelce“ do systému právě díky dřívějším autorizacím reálných uživatelů.

Obecně je problém, že při jakékoliv přítomnosti konkrétního uživatele v síti Internet po něm zůstává tzv. digitální stopa. Řada informací, fotografií a dalších údajů je tak někde v systémech serverů dlouho archivována, není zcela jasné, zda si ji někdo třeba neokopíroval a neuchovává (byť v rozporu se zákonem a pravidly nakládání s osobními údaji) po neurčitou dobu a může ji za řadu let použít proti uživateli. V této souvislosti se někdy, zvlášť pak v poslední době, hovoří o tzv. **právu být zapomenut (right to be forgotten)**, právu na vymazání informací například po zrušení užívání některé internetové služby jako je např. Facebook, Youtube apod. Právě Facebook byl kritizován za uchovávání dat a například fotografi i po zrušení uživatelského účtu.

5.4.1 Facebook

"Lidé si skutečně zvykli nejenom sdílet více informací a různými způsoby, ale být v tomto směru i více otevření a to i vůči více lidem. Tato sociální norma je něco, co se vyvinulo časem." Mark Zuckeberg, zakladatel sítě Facebook, 8.1.2010

Asi snad žádná jiná celosvětová sociální síť nevyvolává od svého vzniku tolik kontroverních otázek a problematických aspektů jejího používání. Lze také říci, že je to Facebook, který udává směr vývoje v dané oblasti, je to právě Facebook, který patří k organizacím, na které se nejvíce zaměřují státní orgány zabývající se mimo jiné ochranou soukromí. Není divu, tato technologie umožňuje lidem chovat se způsobem dosud nevyzkoušeným, neznámým a se kterými nemají zatím mnoho zkušeností a jsou tedy zranitelnější.

Facebook je rozsáhlý společenský webový systém sloužící hlavně k tvorbě sociálních sítí, komunikaci mezi uživateli, sdílení multimediálních dat (např. fotografií a videí), udržování vztahů a zábavě. Se svou bezmála již miliardou (sic!) aktivních uživatelů je tak jednou z největších společenských sítí na světě. Je přeložen do šedesáti osmi jazyků. Uvádí se, že denně je na

tuto sociální síť nahráno 250 milionů fotek. Facebook byl založen Markem Zuckerbergem, bývalým studentem Harvardovy univerzity. Není patrně v možnostech této práce popisovat schopnosti systému a podávat jeho zevrubný popis. Spíše se zaměřím na jeho rizika ve vztahu k ochraně soukromí, která jsou často laickou i odbornou veřejností probírána.

The New York Times v roce 2010 spočítaly, že nastavení soukromí na Facebooku obnáší více než 170 předvoleb v 50 kategoriích. Prohlášení o ochraně soukromí (Privacy statements) se rozrostlo z 1004 slov v roce 2005 na 5830 slov v roce 2010, přičemž svým rozsahem v listopadu 2009 překonalo Ústavu Spojených států a je několikanásobkem délky textů jiných podobných služeb. Pravdou je, že původně bylo soukromí na Facebooku nastaven tak, že profily a informace byly primárně soukromé a jejich zveřejnění vyžadovalo aktivní zásah uživatele, nyní je situace přesně opačná, uživatel se musí aktivně bránit formou volby zveřejnění údajů sám, řada lidí se může překliknout, či složitým volbám a menu nemusí rozumět.[211]

V roce 2008 podala organizace Canadian Internet Policy and Public Interest Clinic (CIPPIC) 35-stránkovou stížnost kanadské komisařce na ochranu osobních údajů. Zástupkyně komisařky na ochranu osobních údajů po proběhlém řízení dospěla k závěru, že Facebook porušuje kanadský zákon na ochranu soukromí (PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT). Největší pochybení tehdy komisařka spatřovala v uchovávání veškerých údajů ze zrušeného profilu na Facebooku, zpráva však uváděla řadu dalších problematických aspektů fungování systému – přístup jiných aplikací k údajům uživatelů Facebooku, nakládání s daty zemřelých uživatelů, nakládání s údaji neuživatelů Facebooku apod.[212]

---

[211] Zajímavý podnět nabízí srovnání jednotlivých verzí Prohlášení o ochraně soukromí Facebooku, jak jej podává Kurt Opsahl ve svém článku Facebook's Eroding Privacy Policy: A Timeline dostupném online na https://www.eff.org/deeplinks/2010/04/facebook-timeline [cit. 2011-11-05].

[212] Závěry šetření kanadského komisaře na ochranu soukromí v jeho zprávě REPORT OF FINDINGS INTO THE COMPLAINT FILED BY THE CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC (CIPPIC) against FACEBOOK INC. ze dne 16.7.2009 jsou dostupné online na http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.pdf [cit. 2011-11-05]

Facebooku je často vyčítána přílišná **jednostrannost podmínek užívání a podmínek ochrany soukromí**. Uživatelé dávají Facebooku nevýhradní, přenosnou, převoditelnou, celosvětovou bezúplatnou (royalty-free) licenci na použití veškerého obsahu podléhajícího právům duševního vlastnictví, který uživatelé zveřejní na Facebooku nebo v návaznosti na něj. Spekuluje se, že Facebook v současné době obsahuje cca 10 miliard soukromých fotografií, ke každé fotografii tak má Facebook tuto pro něj velice výhodně koncipovanou bezúplatnou licenci. Je jasné, že určitá forma licence je pro Facebook nutná, aby nevznikaly případné problémy s nahráním a uchováváním fotografií a jiného autorsky chráněného obsahu na server Facebooku, nicméně není patrně důvodu, aby daná licence byla takto rozsáhlá. Fotografie uživatelů Facebooku byly jednu dobu využívány Facebookem k propagačním účelům, aniž se to konkrétní uživatel dozvěděl. Nyní lze tuto možnost jako řadu dalších v nastavení soukromí odmítnout, ale opět je nutno podotknout, že tento postup není zcela jednoduchý a lze pochybovat, že všichni uživatelé budou podrobně dbát na nastavení svých účtů.

Kritizovalo se například i **využívání fotografie uživatele do různých reklamních kampaní** na Facebooku. Když se někomu například facebooková stránka inzerenta líbí, mohou pak virtuální přátelé této osoby vidět fotku daného uživatele u této kampaně, případně jen informaci, že se mu daná firma/produkt líbí.

V prosinci 2011 americká Federální obchodní komise donutila Facebook ke změně pravidel a souhlasu s pravidelnými audity. Podmínky, které federální obchodní komise Facebooku stanovila a formulovana do návrhu dohody s Facebookem, ještě nejsou definitivní, budou nyní dále veřejně připomínkovány. Jde o následující požadavky:

- během 180 dní od vydání finálního znění dohody, a dále pak každé dva roky, bude muset Facebook projít externím auditem ochrany soukromých údajů. Tato povinnost skončí v roce 2032.
- sliby uživatelům nesmí být jakýmkoliv způsobem zavádějící.
- jakékoliv zásahy, které by změnily platné nastavení soukromí uživatelů, musí mít jejich předchozí informovaný souhlas.

- do třiceti dnů od smazání profilu uživatele nesmí být nikomu dostupný žádný obsah z tohoto profilu.
- Facebook bude muset zřídit speciální program určený k vyhodnocování rizik nových produktů a úprav stávajících produktů pro ochranu soukromí.[213]

Jedna z posledních novinek, kterou provozovatelé sítě Facebook zavádí do svého systému, je tzv. **automatické rozpoznávání obličejů** a **automatizované přiřazování konkrétních lidí k těmto fotografiím.** Tato technologie je od počátku kritizována. Když totiž některý z uživatelů Facebooku bude mít fotku, na které je jiná osoba, automaticky mu systém navrhne tuto jinou osobu na snímku označit. Řada uživatelů logicky protestuje, že Facebook automaticky k fotkám, ke kterým sami nemají přístup, navrhuje přidání jejich jmen. Tzv. taggování (označování lidí na fotografiích jménem) je obecně od počátku kritizováno, nyní může být jméno přidáno k fotografii i automaticky (pokud uživatel tuto možnost nevypne v nastavení soukromí svého účtu).

5.4.2 Další zahraniční sociální sítě

Vedle Facebooku, který je označován za krále sociálních sítí, existuje i řada dalších portálů, které mají za cíl globálně sdružovat své uživatele a umožňovat tak například filipínskému teenagerovi sdílet fotografie s potomkem původních amerických indiánů žijícím v civilizované rezervaci na území USA. V následujícím textu provedu alespoň letmé shrnutí nejdůležitějších sociálních sítí existujících v zahraničí a v následující kapitole pak ryze českých.

Myspace (dříve MySpace) – jedna z nejstarších sociálních sítí, založená již v roce 2003, ještě před sítí Facebook. Sdružuje internetové profily lidí, má funkce ukládání a sdílení multimédií. Je to stále jedna z nejpoužívanější

[213] Viz článek Facebook čeká 20 let auditů kvůli špatné ochraně soukromí uživatelů. Dostupný online na http://tech.ihned.cz/c1-54053250-facebook-ceka-20-let-auditu-kvuli-spatne-ochrane-soukromi-uzivatelu [cit. 2012-02-15].

sociálních sítí na světě, zejména v USA. Kvůli ochraně dětí je server přístupný pouze lidem starším 14 let. Jako každá sociální síť, i Myspace v průběhu let své existence čelila problémům s ochranou soukromí a s úniky dat. Například v lednu 2008 bylo více než 567.000 soukromých fotografií uživatelů této sítě neoprávněně staženo a umístěno na Internet.[214]

Twitter – sociální síť, jež vznikla v roce 2006, zaměřuje se zejména na tzv. mikrology, sdílení krátkých zpráv, pocitů a dalších interakcí, zpravidla nepřesahujících jednu dvě věty. V souvislosti se sítí Twitter existuje nedávný rozsudek z americké Virginie, kde tamější soud ve svém šedesátistránkovém rozsudku ze dne 10.11.2011 výslovně umožnil americkým federálním vyšetřovatelům nahlédnout do soukromých dat uživatelů sítě Twitter v rámci vyšetřování tzv. whistleblowerských stránek WikiLeaks a současně nepovolil odtajnění důvodu vyšetřování a dalších informací. Rozhodnutí vzbudilo u uživatelů a ochránců soukromí nevoli zejména z důvodu, že státní orgány budou využívat a mít přístup k datům na Internetu tajně, bez poskytnutí dalších informací jednotlivým uživatelům a z toho důvodu, že vyšetřovací orgány zde postupovaly nestandardně, bez soudního příkazu na základě jiného právního titulu – dle zákona z roku 1994 (Stored Communication Act).[215]

Badoo – to je další sociální síť, která ovšem nemá nejlepší pověst díky kontroverzní a agresivní politice získávání nových členů. Obvykle lidem chodí email, ve kterém je daný člověk zván do sítě Badoo, k pozvánce jsou připojeny někdy i fotografie přátel (pocházející například z Facebooku, jde patrně o krádež dat). Provozovatel sítě pak využívá kontakty uživatelů k reklamní činnosti.

---

[214] Více informací v anglicky psaném článku Pillaged MySpace Photos Show Up in Massive BitTorrent Download, dostupném online na http://www.wired.com/politics/security/news/2008/01/myspace_torrent [cit. 2012-02-15].

[215] Celé rozhodnutí je dostupné v anglickém jazyce online na https://www.eff.org/sites/default/files/filenode/MemorandumOpinion1353.pdf [cit. 2012-02-15].

Youtube – je portál, založený v roce 2005, který umožňuje nahrávání, prohlížení a sdílení videozáznamů. Jako jiné obdobné portály, Youtube ze svého samotného charakteru přináší zásadní rizika týkající se práva na ochranu soukromí. Často bude záležet na konkrétních uživatelích, co ze svého soukromí na tomto serveru odhalí, mnohdy se však může stát i to, že jiné osoby umístí na Youtube videa odhalující soukromí jiné osoby bez jejího svolení. Youtube má poměrně propracovaný systém odstraňování závadného obsahu, včetně obsahu zasahujícího do práv na ochranu soukromí. Přesto nelze zamezit situacím, kdy soukromí bude, a to často i zásadně, narušeno. K několika soudním případům viz poznámku v úvodu této kapitoly 5.[216]

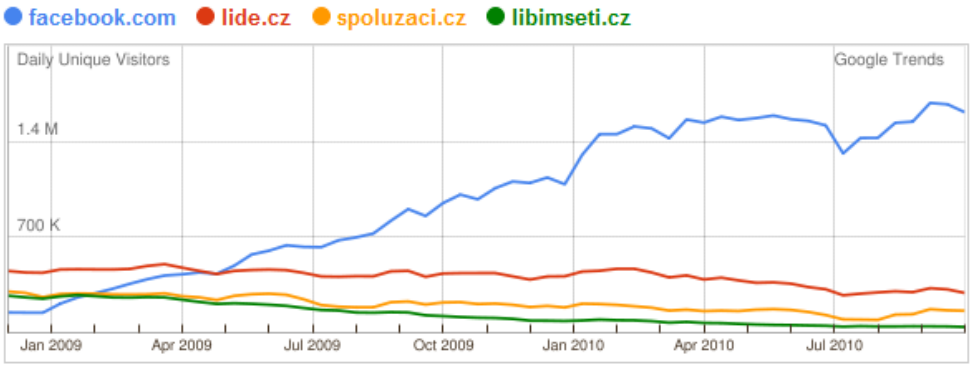
Google Picasa, Flickr – zmíněné názvy představují webové portály umožňující sdílení fotografií jejich uživateli. Služby jsou poměrně rozšířené, existuje i česká obdoba jako je např. web Rajče.net spojené s portálem Idnes.cz. Často bývá řešena otázka autorských práv, resp. rozsahu licenčního oprávnění, které obvykle provozovatelé serveru po svých uživatelích vyžadují. Akceptací podmínek serveru a služby (což nelze odmítnout, pokud chcete daný server používat), autor (uživatel služby) předmětné fotografie udílí licenční oprávnění provozovateli serveru k užití,

[216] Z hlediska provozování tzv. videowebů jako je např. YouTube a další je zajímavá problematika nového zákona o audiovizuálních mediálních službách na vyžádání – zákon č. 132/2010 Sb. Tento zákon zapracovává již existující evropské dokumenty, zejména směrnici Rady 89/552/EHS, o koordinaci některých právních a správních předpisů členských států upravujících provozování televizního vysílání (tzv. směrnice "Televize bez hranic"). Tímto zákonem se nově regulují služby obdobné televiznímu vysílání, které jsou uživateli poskytnuty v jím zvoleném čase. Zákon je zaměřen na internetové webové vysílání. Provozovatelé webů, na kterých se objevují videa, která jsou strukturovaná podle témat a současně majitelé chtějí na jejich provozu vydělávat, se musí evidovat u Rady pro rozhlasové a televizní vysílání (RRTV). Ta dané vysílání reguluje, kontroluje a případně sankcionuje. Zákon upravuje používání obchodních sdělení (reklama), zavádí podporu evropské tvorby, zakazuje používání podprahových informací, zakazuje nabádání k nenávisti z důvodu pohlaví, rasy, barvy pleti, jazyka, víry a náboženství, politického nebo jiného smýšlení, národního nebo sociálního původu, příslušnosti k národnostní nebo etnické menšině, majetku, rodu nebo jiného postavení. Pornografický obsah má být dostupný pouze tak, aby se k němu nesměli běžně dostat děti a mladiství. Zákon se nicméně vztahuje pouze na provozovatele se sídlem v ČR, resp. v EU, například na server YouTube či jiné mimoevropské servery se daná regulace nevztahuje.

zpravidla pro jeho propagaci a pro samotné užití fotografie v rámci dané sdílecí služby.[217]

5.4.3 České sociální sítě

Vedle Facebooku, který je v Česku nejvíce užívanou sociální sítí, existují na českém Internetu i ryze české sociálně-mediální projekty. Zastoupení nejvýznamnějších sociálních sítí v ČR dokládá následující graf:



Návštěvnost jednotlivých sociálních sítí Facebook.com, Lide.cz, Spoluzaci.cz a Libimseti.cz (Zdroj: Google Trends for WebSites)

Lidé.cz – jedna z nejstarších ryze českých sociálních sítí, provozovaná portálem Seznam.cz. Server umožňuje svým členům vytvářet profily, sdílet fotografie a dané fotografie i tzv. hodnotit. Síť umožňuje i seznamování lidí, funguje jako internetová seznamka. Jde o nejnavštěvovanější server mezi českými sociálními sítěmi.

Spolužáci.cz – komunitní server, sdružující současné a bývalé spolužáky ze škol v rámci celé ČR. Uživatelům umožňuje kontakt a výměnu informací mezi spolužáky jednotlivých tříd, a to od základních škol až po vysoké školy. Uživatel může vstoupit do „své“ třídy po zadání hesla (obvykle jméno třídního učitele), zanechávat spolužákům vzkazy, sdílet fotografie a

[217] Podrobněji k tématu viz článek „Fotoalba na Internetu vás mohou připravit o vaše práva“ dostupný online na http://www.lupa.cz/clanky/fotoalba-na-internetu-vas-mohou-pripravit-o-prava/ [cit. 2012-02-15].

další dokumenty apod. Server je přes shodného provozovatele Seznam.cz propojen i se serverem Lide.cz, se kterým sdílí registrační proces.

Libimseti.cz, Stesti.cz, Ukazse.cz a další seznamky – mezi sociální sítě jsou často zařazovány i seznamky. Jde o servery zaměřené na seznamování lidí, kdy jednotliví uživatelé často vkládají své profily doplněné o celé fotogalerie, případně i videa a další textové doprovodné informace. Riziko zneužití je nasnadě. Uživatelé často vkládají své osobní údaje, své i intimní fotografie a mohou se stát oběťmi potenciálních pachatelů, kteří mají na danou síť obvykle neomezený přístup a záleží jen na chování a opatrnosti jednotlivých uživatelů, kolik ze svého soukromí odtajní – citlivé fotografie lze zpřístupnit uživatelům, kteří znají heslo. V roce 2008 se však stal například případ, kdy hackeři nabourali systém serveru Libimseti.cz, prolomili uživatelská hesla k uzamčeným fotogaleriím a odcizili tisíce osobních fotografií, zejména mladých dívek, které pak nabízeli na různých undergroundových internetových fórech.[218]

Takových případů krádeže dat se stává pravděpodobně každý rok několik, jen se o nich nikdo ani nemusí dozvědět. Není ostatně v silách provozovatelů těchto webů, aby útokům hackerů zamezily, ani nejlépe střežené weby nejsou prakticky schopny odolat cílenému útoku hackerů nebo jejich skupin. Riziko krádeže a zneužití dat, které uživatel na sociální sítě nahraje, je proto vždy reálné a je proto především odpovědností každého uživatele, jakou část své soukromé sféry umístí na sdílený prostor na síti.

5.5 Problém geolokace obrazových záznamů

Závěrem této části mé práce chci poukázat na jedno z dalších z hlediska soukromí rizikovějších témat, a to problém geolokace, v našem pohledu nás zajímá zejména **geolokace obrazových záznamů**. Technologie geolokace umožňuje například přidávat do tzv. metadat jednotlivých obrazových snímků (záznamů) i geolokalizační údaje, tj. údaj (tzv. geotag) o

[218] Zdroj: Hacker stáhl tisíce intimních fotek ze seznamky Líbímseti.cz, článek na serveru Živě.cz, dostupný online na: http://www.zive.cz/bleskovky/hacker-stahl-tisice-intimnich-fotek-ze-seznamky-libimseticz/sc-4-a-144169/default.aspx [cit. 2012-02-15].

tom, na jakém místě byla fotografie pořízena – fotografický aparát nebo mobil musí být touto funkcí samozřejmě vybaven. Moderní komunikační přístroje jako smartmobily iPhone a další umožňují pak nejrůznější další aplikace postavené na tomto principu a umožňující například sdílení fotografií pouze omezenému okruhu uživatelů, kteří se nachází v dosahu přístroje.[219]

Fotografie či videa s geolokačními údaji lze pak **dále sdílet** na sociální síti, webových fotoalbech atd. Z nedávné doby je evidován poměrně zajímavý případ vystavení fotografií příslušníků americké armády v Afgánistánu, které na webový server Picasa nahrál jeden z vojáků. Fotografie byla opatřena geotagem a údaji o přesné poloze. Riziko je pak zřejmé.[220] Uživatelé také mohou vkládat konkrétní fotografie i do celých již existujících systémů, jako je Google StretView a podobné, které obsahují databáze fotografií vztahujících se k danému místu na zemi.

---

[219] Existuje aplikace Color, která kupříkladu umožňuje v restauraci pořízení fotografie, kterou uživatel nasdílí všem dalším uživatelům této aplikace v dosahu např. 30 metrů, jim se zpráva o nových fotografiích zobrazuje jako tzv. feed. Další informace viz http://www.tyinternety.cz/startupy/color-nova-fotograficka-geolokacni-sit-meni-pravidla-hry-3246 [cit. 2012-02-15].

[220] Viz článek na serveru IDNES.CZ: Nový nepřítel Pentagonu. Chytré mobily vojáků v bojových operacích. Dostupný online na: http://zpravy.idnes.cz/novy-nepritel-pentagonu-chytre-mobily-vojaku-v-bojovych-operacich-1fz-/zpr_nato.aspx?c=A110118_174514_zpr_nato_inc [cit. 2012-02-15].

6 DALŠÍ OBLASTI POUŽITÍ OBRAZOVÝCH SNÍMKŮ A ZÁZNAMŮ

6.1 Obrazové snímkování zemského povrchu

6.1.1 Google Street View

Odbornou ale i laickou veřejnost oslovil v nedávné době intenzivně řešený případ americké společnosti Google Inc. se sídlem v Kalifornii, která v roce 2007 zahájila nejprve na území USA službu Google Street View. Street View je v zásadě vysoce technicky propracovaný systém, umožňující uživatelům Internetu a této služby společnosti Google Inc. využívat podrobné interaktivní mapy s vysoce detailními panoramatickými 360 stupňovými záběry z reálných ulic. Google dané mapy připravil pomocí speciálního vozidla, vybaveného kamerami, které projelo veškerá místa, následně přístupná v dané službě a pořídilo podrobné záběry z těchto míst.

Na úvod je nutno přiznat, že daná technologie je opravdu revoluční. Nikdy v historii neměli lidé možnost na Internetu brouzdat ulicemi měst, reálně od nich vzdálených tisíce kilometrů a mít alespoň částečný zážitek, jako by daná místa opravdu navštěvovali. Praktické využití aplikce je taktéž nasnadě, usnadňuje situaci řidičům, návštěvníkům dané lokality, kteří si mohou místo předem prohlédnout atd.[221] Na druhou stranu, jak tomu obvykle v takovýchto případech bývá, novinka rozvířila i názory ve vztahu k právu na ochranu soukromí. Spolu s technickou realizací aplikace byly pořízeny samozřejmě nejenom fotografie samotných ulic, ale i konkrétních fyzických osob, které se v době pořizování snímků na veřejném prostranství

[221] Jako jeden z přínosů zavedení služby Street View se uvádí mimo jiné i zachování pohledu na naši dobu jako součást kulturního dědictví a umožnění budoucím generacím pohlédnout plasticky do běžného života v ulicích. Tato hypotéza byla potvrzena již v roce 2009 při zničení větší části středoitalského historického města Aquila. Podrobná fotografická dokumentace (pořízená v srpnu 2008) je však díky službě Google Street View zachována a lidé se tak mohou i nadále dívat na původní historické budovy, i v případě, že již nebudou obnoveny.
Zdroj: internetový článek Google Street View zachoval města před zemětřesením. Dostupné online na http://navigovat.mobilmania.cz/Bleskovky/AR.asp?ARI=114226 [cit. 2012-02-15].
Skoro každý člověk by pak určitě měl zájem virtuálně se projít ulicemi třeba svého rodného města v době jeho narození, před 30, 50 nebo 70 lety.

nacházely, někdy bylo možné vidět do soukromých prostor (dvorů, přes okna do bytů), byly rozpoznatelné poznávací značky aut atd. Společnost Google proto vyvinula nástroj, který umožňuje rozmazání tváří osob i poznávacích značek aut. Uživatelé, kteří se na fotografiích i přesto identifikují, mají možnost nahlásit inkriminované snímky přímo na Google a společnost zaručí jejich vymazání.[222] Google byl také kritizován za tzv. **Wardriving**, což je výraz pro vyhledávání bezdrátových Wi-Fi sítí osobou v jedoucím vozidle pomocí přenosného počítače nebo PDA – při snímkování ulic totiž Google zjišťoval i další údaje, například dostupnost bezdrátových sítí apod., s využitím například pro další tzv. geolokační služby. Spekuluje se i o tzv. **piggybackingu**, tedy připojování se k sítím a používání jejich služeb bez svolení. Google měl takto získat zhruba 600 GB dat z WiFi sítí v třiceti zemích.[223]

V České republice nepovolil společnosti Google Inc. český Úřad pro ochranu osobních údajů zpracování osobních údajů v rámci služby Street View. Své rozhodnutí ze dne 2.9.2010 odůvodnil zejména tím, že společnost Google Inc. jakožto správce osobních údajů sídlící mimo EU neustanovila na území České republiky svého zástupce (zpracovatele osobních údajů) a dále tím, že služba využívá technické postupy, které nepřiměřeně zasahují do soukromí občanů (např. nastavení kamery pořizující snímky nad rozsah běžného pohledu z ulice). Úřadu zejména vadilo to, že kamery společnosti Googlu při snímkování zabíraly prostor z výšky 2,7 metru nad úrovní terénu a tedy i prostor za ploty a okny domácností. Takovýto pohled jde nad rámec běžného pohledu kolemjdoucího a vymyká se i obecně akceptovatelnému pojetí a vnímání soukromí občany, kteří třeba i své ploty a další zábrany volí

---

[222] Google Street Views po celém světě eviduje tzv. hluchá místa, tj. místa, jejichž fotodokumentace z nejrůznějších důvodů není v aplikaci přístupná, většinou z důvodu ochrany veřejného zájmu, bezpečnosti, vojenské ochrany, či ochrany soukromí. Taky bylo např. vyřazeno předměstí St. Paul města North Oaks, Missisippi z důvodu soukromých cest se zákazem vstupu, a Google tak neměl legální možnost pořídit dané snímky. Stejně tak dům rodiny Boringů z města Franklin Park byl vymazán, neboť manželé Boringovi tvrdili, že Street View znehodnotilo jejich nemovitý majetek, způsobilo jim psychickou újmu a došlo k narušení zákazu vstupu na jejich soukromou cestu, kam neměla společnost Google přístup. Tyto případy jsou však spíše ojedinělé a kuriózní. Zdroj: Blurred Out: 51 Things You Aren't Allowed to See on Google Maps, dostupné v anglickém jazyce online na: http://www.itsecurity.com/features/51-things-not-on-google-maps-071508/ [cit. 2012-02-15].

[223] Zdroj: Google wardriving? A co má vlastně být? Dostupné online na: http://www.lupa.cz/clanky/google-wardriving-a-co-ma-vlastne-byt/ [cit. 2012-02-15].

(včetně jejich výšky) právě z důvodu zamezení běžným pohledům z ulice.[224] V roce 2011 nicméně ÚOOÚ přehodnotil svá rozhodnutí a po odstranění některých problematických aspektů společností Google snímkování de facto povolil, když zapsal dne 23.5.2011 do registru zpracování osobních údajů Úřadu pro ochranu osobních údajů společnost Google Ireland Ltd. se sídlem v Irsku jakožto správce, který je odpovědný za provozování služby Google Street View na území ČR.[225]

Můj názor na danou problematiku zavádění aplikace služby Google Street View je spíše pozitivní. Je nesporné, že společnost Google Inc. řadu věcí podcenila a dopustila se porušení zásad ochrany soukromí a v některých případech i nelegálního až trestného jednání (neoprávněný sběr osobních údajů, hesel z WiFi komunikace atd.). Každá takováto vysoce moderní a složitá aplikace však s sebou přináší vedle nových možností a výhod i rizika a problémy při zavádění. Na dané situaci je potěšující, že se po celém světě proti službě Street View zdvihnul odpor občanů, institucí a dalších subjektů. Řada problémů se tak mohla odstranit. Přesto však se

---

[224] Rozhodnutí ÚOOÚ ze dne 2.9.2009 a následné potvrzující druhoinstanční rozhodnutí předsedy Úřadu pro ochranu osobních údajů ze dne 15.11.2010 jsou dostupná na webu ÚOOÚ online na: http://uoou.cz/files/noindex/REG-1197-10-21.pdf a http://uoou.cz/files/noindex/REG-1197-10-27.pdf [cit. 2012-02-15].

[225] Rozhodnutí o povolení registrace zpracování osobních údajů předcházela jednání ÚOOÚ se společností Google, kdy se Google rozhodl přistoupit na četné výtky ke své aplikaci a přistoupil na následující podmínky:

- **snížení výšky stožáru**, na kterém je kamera umístěna, na 2,3 - 2,4 m oproti původním 2,7 m.
- jmenování **odpovědného správce na území EU - společnost Google Ireland Ltd.** Tato společnost bude plně odpovídat za to, že sběr osobních údajů na území ČR a zpracování v datových centrech se provádí v souladu s českými právními předpisy o ochraně osobních údajů. Tuto společnost lze kdykoliv kontaktovat např. v případě stížnosti, dotazu či žádosti o rozmazání určitého snímku. Oznámení bude neprodleně posouzeno během 48 hodin. Čeští občané mají možnost komunikovat se společností v českém jazyce.
- zaměstnance Googlu zavazují **vnitřní předpisy a zásady etického jednání** k bezpečnému nakládání s osobními údaji a jejich ochraně.
- speciálně jsou **proškoleni a informováni řidiči** vykonávající práci pro účely služby Street View. Jsou instruováni, že mají plánovat svou jízdu tak, aby se vyhnuli určitým místům (například školám) v určitých časově vytížených obdobích, eventuálně, jízdu zde v nevhodném čase mají přerušit a vrátit se ve vhodnější době.
- **před prováděním záznamů** pro Street View **budou informovány místní orgány** (jako například obecní úřady) či informační stánky pro turisty, aby si byli vědomi toho, že v místě jejich působení dochází k pořizování snímků. **Veřejnost bude o pořizování snímků informována** prostřednictvím médií, reklamní kampaně a webové stránky Street View, která bude dostupná v českém jazyce.

zaváděním služby Stret View zůstává řada otazníků a oblastí potenciálního zneužití v souvislosti s fungováním služby. Stále není příliš jasné, co se bude dít s původními zdrojovými obrazy veřejných prostranství, které zachytila vozidla Google (před anonymizací a dalšími úpravami). Ty budou patrně i nadále někde ve společnosti Google archivovány (po určitou dobu, původně to byl rok, nyní patrně 6 měsíců) a přístupny tak např. úřadům, v USA někdy i bez soudního rozhodnutí, jak to stanoví Patriot Act. Vždy nelze vyloučit ani selhání lidského faktoru a techniky. Street View přináší hodně kontroverzí nepochybně i proto, že jde na rozdíl od individuálního sběru dat jednotlivci o masivní projekt, zahrnující neskutečné množství dat. Přesto se jednotlivé prvky projektu příliš neliší od sběru dat individuálními fotografy, kteří následně své fotografie nebo videa vystaví na internetu. Problém je však v oné velikosti projektu, šíři jeho záběru a možnosti neskutečně detailního zpracování veřejných prostranství.

6.1.2 Satelitní a letecké mapy

Předchůdce výše uvedeného projektu Street View byly systémy satelitního mapování zemského povrchu. Tyto projekty byly již delší dobu dostupné armádě a dalším institucím národních států. Teprve s rozvojem informačních technologií a Internetu začaly pronikat i mezi běžnou veřejnost. Satelitní snímkování zemského povrchu je stále dokonalejší a soukromé společnosti je využívají k zpřístupnění prakticky celého zemského povrchu uživatelům svých internetových aplikací z tepla jejich domova. Existují tak známé služby jako **Google Earth**, **Google Maps**, v ČR pak aplikace **Mapy.cz**, které eviduje podrobné satelitní mapy a mapy vytvořené na podkladě leteckého snímkování (Mapy.cz umožňují prohlížení ulic a zemského povrchu i formou technicky zdařilé aplikace „Ptačí pohled“, umožňující podrobný pohled na jednotlivá místa v ČR). Aplikace Google Earth (systém byl vytvořen společností Keyhole, Inc., ve spolupráci s americkou CIA, původně se nazýval Earth Viewer) obsahuje satelitní snímky celého světa ve vysokém rozlišení, stovky trojrozměrných měst a archivy historických snímků.

Na rozdíl od Google Street View, který přináší pohled z veřejného prostranství z výšky cca 2,5 metru (tedy poměrně standardní pohled z ulice, z veřejně přístupného místa), jsou podrobné satelitní a letecké mapy z hlediska práva na ochranu soukromí někdy ještě více kontroverzní. Nepřináší sice tak kvalitní záběry (v současnosti je však kvalita již velmi zdařilá a pravděpodobně bude časem ještě vyšší), na druhou stranu není s jejich pomocí problém zjistit uspořádání sousedovy zahrady, byť má vysoký plot neumožňující pohled do ní a další často delikátní informace.

Společnost Google provozuje taktéž poměrně novou službu Google Places, která obsahuje adresář míst s uvedením adres a dalších základních údajů a také fotografie a videa, hodnocení a recenze nebo přehled souvisejících míst. Google Places je pak propojeno na další služby Google, takže místa v něm uvedená uživatelé najdou také ve webové vyhledávání, na mobilu, jakož i na Google Maps a Google Earth. Obdobných služeb jako Google Places existuje více, podrobnější popis však přesahuje možnosti této práce.

6.1.3 Další družicové optické sledování

Spolu s rozvojem vesmírných technologií lidstvo vždy pomýšlelo na možnosti i optického pozorování povrchu Země. Nejprve za vojenskými, ryze špionážními účely, v poslední době po skončení studené války pak i ve větší míře pro účely mírové. Spolu s rozvojem těchto technologií, vypouštěním celé řady satelitů, vyvstává logicky i otázka, zda tyto moderní technologie nemohou zasáhnout do soukromí obyvatel planety. Jsem toho názoru, že v dané fázi ne, neboť jsou obvykle užívány pro optické pozorování spíše podpůrně, technologie a rozvíjení možností je teprve v plenkách, nicméně s ohledem na zaměření této práce musím tyto technologie zmínit. Potenciálně samozřejmě mohou tyto technologie při nesprávném stanovení limitů jejich využívání podstatně zasáhnout a ovlivnit soukromí jednotlivců.

V rámci Evropské unie se již nějakou dobu úspěšně používá systém **MARS** (Monitoring Agriculture with Remote Sensing), což je **kontrola zemědělských aktivit prostřednictvím satelitních družic**. Projekt tohoto

dálkového průzkumu země běží od konce osmdesátých let 20. století. Pomocí infračervených a jiných detektorů dokáží satelitní družice rozpoznat druh rostlin pěstovaných na zemědělských plochách. Tím je po vyhodnocení snímků kontrolováno, zda daní zemědělci nezneužívají poměrně štědrý systém evropských zemědělských dotací v rámci Společné zemědělské politiky EU tím, že papírově pěstují více dotovanou rostlinu a ve skutečnosti mají vysetou např. obyčejnou pšenici. V roce 2003 tak bylo nasnímáno cca 15 tisíc kilometrů čtverečných polí v Evropě, v roce 2004 již 50 tisíc, v roce 2005 pak cca 150 tisíc, přičemž zobrazovaná plocha bude neustále stoupat. Od roku 2000 je tento projekt dokonce rozšířen i za hranice EU zejména za účelem kontroly využívání dotací a pomoci ze strany EU rozvojovým zemím. Projekt má také velké využití i v jiných oblastech než v kontrole dotační politiky, např. v oblasti zemědělského výzkumu, sbírání dat pro statistické účely v zemědělství, ve zjišťování prognóz úrody, při pořizování tzv. ortosnímků, parcelových map atd. Od 1.6.2004 je **projekt sloučen s projektem kontroly rybářských aktivit na moři.**[226]

Dále Evropa využívá program **GMES** (Global Monitoring for Environment and Security - Globální monitoring životního prostředí a bezpečnost).[227] GMES je **globální monitorovací síť**, která poskytuje údaje pomáhající při řešení otázek, jako je změna klimatu nebo bezpečnost obyvatelstva (systém pomohl například v roce 2010 při pomoci Haiti postiženému zeměstřesením, při hašení lesních požárů ve středomořských státech nebo při ničivých povodních ve střední Evropě atd.). Celý systém zahrnuje vedle vesmírných satelitů i další vzdušné a další pozorovací prostředky jako pozorovací balóny, letecký průzkum, námořní průzkum, síť seizmických přístrojů atd. V rámci systému GMES provádí Evropská Unie celou řadu dalších dílčích nejrůznějších monitorovacích projektů - HELM (Harmonised European Land Monitoring), nebo například projekt GEO-PICTURES. Tento projekt kombinuje satelitní pozorování a komunikaci, navigaci a přímé pozorování planety Země se zaměřením na pomoc při

[226] Vzniká tzv. AGRIFISH unit, sloučení dosavadní satelitní technologie pro kontrolu zemědělství a projektu satelitní kontroly rybářství. Sledování na moři je usnadněno tím, že každá rybářská loď je vybavena GPS zařízením.

[227] Podrobnější informace v anglickém jazyce viz webové stránky Evropské Komise: http://ec.europa.eu/enterprise/policies/space/gmes/key_documents/index_en.htm [cit. 2012-02-15]

nouzových událostech (povodně, masivní požáry, zemětřesení). Umožňuje uživatelům poskytnout detailní snímky povrchu, videosekvence nebo naopak mapy a snímky povrchu ve větším měřítku pro větší přehlednost konkrétní situace.[228]

V září roku 2008 představila Evropská unie program s názvem Kopernikus. Jde de facto o přejmenování dosavadních aktivit v rámci systému GMES. Tento projekt se stane jedním ze základních pilířů vesmírné politiky EU, jehož „cílem je především monitorovat pomocí evropských družic stav životního prostředí na zemi, v oceánech i v atmosféře a zlepšit bezpečnost lidstva v podmínkách, kdy mimo jiné kvůli klimatickým změnám roste riziko přírodních dalších katastrof.“ [229] Služby projektu Kopernikus by měly zahrnovat například informace o stavu půdy a úrody, moří a oceánů, atmosféry, systém může pomoci například i při humanitárních krizích, přírodních katastrofách a v neposlední řadě i jako ostraha bezpečnosti. Uvádí se, že získané informace budou použitelné v boji s organizovaným zločinem, terorismem i při sledování pohybu imigrantů.

Projekt umožní zacílit tzv. geo-informační služby pro bezpečnostní aplikace cílené na vyhledávání osob, pro humanitární účely, na ochranu hranic a na námořní průzkum, pro pomoc celním orgánům, proti teroristickým aktivitám atd., to vše nejen v rámci EU, ale i za jejími hranicemi.[230]

Výše uvedené aktivity evropských institucí přináší bez jakýchkoliv sporů nesmírný užitek nejen pro kontrolory dotační politiky, ale i pro agronomy, specialisty zabývající se výživou a hledáním nových zdrojů potravy, pro oceánografy a řadu dalších vědců z nejrůznějších oborů. Na

---

228 Viz informační leták projektu GEOPICTURES, dostupný online na http://ec.europa.eu/enterprise/policies/space/files/geopictures_en.pdf [cit. 2012-02-15]

229 IDNES.CZ: Přichází Kopernikus: vesmírný systém, který bude hlídat kontinent. Dostupné online na: http://zpravy.idnes.cz/prichazi-kopernikus-vesmirny-system-ktery-bude-hlidat-kontinent-p9y-/zahranicni.aspx?c=A080922_112350_zahranicni_jba [cit. 2012-02-15] Dále viz článek "Projekt Kopernikus není Velký bratr," říká OndřejMirovský, dostupný online na http://www.ceskatelevize.cz/ct24/exkluzivne-na-ct24/osobnosti-na-ct24/30202-projekt-kopernikus-neni-velky-bratr-rika-ondrej-mirovsky/ [cit. 2012-02-15]

230 Další podrobné informace v anglickém jazyce k aktivitám Kopernikus viz webové stránky Evropské Komise – Kopernikus: observing our planet for a safer Word – dostupné online na: http://ec.europa.eu/enterprise/magazine/articles/competitiveness-energy-environment/article_7096_en.htm [cit. 2012-02-15]

druhé straně se sledováním zemského povrchu čím dál víc **zmenšuje zdání soukromí jednotlivců.** [231] Každý zemědělec a jeho pole, i každá rybářská loď jsou tak pod prakticky nepřetržitým dohledem z vesmíru. [232] Do budoucna pak budou stále větší plochy území pod dohledem z vesmíru, uvažuje se i o monitorování měst, obyvatel apod.

6.1.4 Bezpilotní letecké sledování povrchu země

Bezpilotní letecké prostředky se používají pro armádní účely již řadu desetiletí. V poslední době nicméně dochází k využití bezpilotních letadel a dalších prostředků **i pro civilní použití** nebo pro použití ze strany jiných než armádních bezpečnostních sborů, zejména ze strany policejních orgánů. Masivnější rozvoj nasazení bezpilotních prostředků za účelem monitoringu nastal za války v Perském zálivu. V USA je využívají policisté pro sledování míst anebo dopravy. [233] To však vyvolává také obavy o soukromí, ale také o bezpečnost letového provozu.

V červnu 2011 nasadila americká policie bezpilotní letoun typu Predator (známý z vojenského nasazení v Afgánistánu) při sledování a zadržení hledaných zločinců v Severní Dakotě. Predatory také hlídkují u hranic s Mexikem kvůli pašerákům drog.

---

231 K právním ale i etickým problémům vznikajícím při dálkovém průzkumu Země viz zajímavý článek v anglickém jazyce SLONECKER – SHAW – LILLESAND: Emerging Legal and Ethical Issues in Advanced Remote Sensing Technology. In: Photogrammetric Enginneering Remote Sensing. Ročník 64, č.6 (1998), s.589-595 nebo online na http://ibis.geog.ubc.ca/courses/geob373/lectures/Handouts/PERS_Remote_Sensing_Ethics.pdf [cit.2012-01-29].

232 Již v roce 1994 využil dat ze satelitního družicového systému MARS pro prokázání viny zemědělce při podvodu s evropskými dotacemi poprvé i obecný soud – stalo se tak v německém Regensburku.

233 Bezpilotní letadla jsou také mnohonásobně levnější. Texasští policisté oceňují letovou hodinu dálkově řízeného vrtulníku na 30 dolarů ((asi 570 korun), zatímco pilotovaný stroj na stejnou dobu vyjde na 500 dolarů (asi 9500 korun). Letouny mohou být vedle normální kamery vybaveny také infračervenou kamerou a poslouží nejen k bezpečnostnímu monitorování, ale třeba i k hledání ztracených turistů. Podle policistů bezpilotní letadla jsou vhodná také například pro sledování větších davů, pro průzkum terénů před policejními zásahy a pro rychlejší reakce na závažné nehody na dálnicích. Naopak se nehodí třeba pro sledování podezřelých snažících se uniknout v rychle jedoucím autě. Zdroj: Bezpilotní letouny už v Americe špehují i nad městy, zpravodajský článek dostupný na serveru E15 http://magazin.e15.cz/veda-a-technika/bezpilotni-letouny-uz-v-americe-spehuji-i-nad-mesty-725778 [cit.2012-01-29].

Bezpilotní letecké stroje se užívají již i v Evropě. Ve Velké Británii jsou využívány od roku 2011 pro kontrolování silničního provozu a další policejní aktivity. Ekologičtí aktivisté pak nasadili bezpilotní letadlo při monitorování pohybu a aktivit velrybářských lodí u Antarktidy.[234]

V rámci EU se uvažuje o nasazení bezpilotních strojů v projektu **INDECT**, což je systém pro automatickou detekci abnormálního chování lidí na veřejných prostranstvích a na internetu. V rámci sledování abnormálního chování jsou sledována a vyhodnocována data z různých druhů senzorů. V případě městských prostor se počítá s využitím kamerových systémů v kombinaci se zvukovým záznamem z mikrofonů. Pro sledování pohyblivých objektů se uvažuje mimo jiné právě i o nasazení bezpilotních strojů.[235]

6.2 Speciální letištní skenery

Na některých vybraných letištích ve Spojených státech byly nainstalovány **speciální skenery osob** – ***backscattery***. Vypadají jako kovové bezpečnostní rámy a jejich speciální paprsky pronikají skrze oblečení a umožňují vidět osobu, která rámem projde, jako by byla zcela nahá. Obrázky, které vidí obsluha skeneru, jsou zcela reálné a je na nich možné vidět i takové detaily, jako jsou mateřská znaménka, jizvy, tetování apod. Tyto bezpečnostní rámy budou tedy na jednu stranu schopné odhalit potenciálního teroristu, na stranu druhou ovšem umožní zobrazení našich nejintimnějších míst. Americká bezpečnostní služba uvádí, že „snímky nebude možné uchovávat, tisknout nebo kamkoli odesílat a že přístroj je

---

[234] Podrobněji viz článek ze dne 27.1.2011: Policejní bezpilotní letoun přečte značku auta z 200metrové výšky, dostupný online na: http://www.ceskatelevize.cz/ct24/svet/161922-policejni-bezpilotni-letoun-precte-znacku-auta-z-200metrove-vysky/ [cit.2012-01-29].
PRYSZCZ, M.: Možnosti využití bezpilotních prostředků pro civilní účely. Brno: VUT, 2007.
Sadecký, Z.: Zamyšlení nad uplatněním UAV v bezpečnostní praxi. Dostupné online na http://www.uav.estranky.cz/clanky/autorovy-prispevky/zamysleni-nad-uplatnenim-uav-v-bezpecnostni-praxi.html [cit.2012-01-29].
článek ze dne 25.12.2011: Aktivisté sledují japonské velrybáře za pomoci bezpilotních letounů, dostupné online na http://www.ceskatelevize.cz/ct24/svet/158171-aktiviste-sleduji-japonske-velrybare-za-pomoci-bezpilotnich-letounu/?mobileRedirect=off [cit.2012-01-29]

[235] Více informací o projektu INDECT viz webové stránky projektu dostupné online na http://www.indect-project.eu/

smaže okamžitě poté, co cestující opustí kontrolní stanoviště. Nikdo jiný kromě pracovníka u monitoru umístěného na vzdáleném místě je údajně nebude moci vidět. Přístroje budou navíc používány pouze k druhotné kontrole, tedy poté, kdy cestující vzbudí podezření při klasické kontrole."

Každý si také údajně bude moci vybrat, zda se podrobí raději osobnímu „prošacování", nebo projde skenerem. Přesto mnohé lidi tato technologie velmi zneklidňuje, i z toho důvodu, že ji budou obsluhovat zase jen lidé. A je snadné si představit situaci, kdy rámem projde například nějaká známá osobnost a zanedlouho se snímky jejího nahého těla objeví v bulvárních médiích. Můžeme tedy konstatovat, že stejně jako výše uvedené technologie, i tato opět naráží na ono dilema: bezpečnost, nebo soukromí.[236]

V listopadu 2011 Evropská komise schválila **pravidla používání letištních skenerů zobrazujících lidské tělo**. Obrázky z prohlídky se podle komise nebudou moci nicméně ukládat a obsluha navíc bude muset být v jiné místnosti než lidé procházející skenery. Pasažéři taktéž tuto proceduru mohou odmítnout a podstoupit jiný druh prohlídky.[237]

Do budoucna se dokonce pak uvažuje o masivním nasazení ještě více vyspělejšího skanneru na bázi tomografu (obdoba CT snímkování známého z lékařství). Pomocí této technologie pak mohou bezpečnostní pracovníci odhalit nejenom zbraně a nejrůznější věci pod oděvem, nýbrž oproti běžným rentgenovým skannerům mnohem dokonaleji i předměty ukryté uvnitř lidského těla (nejčastěji půjde o ampule s drogami apod.). Tyto CT skannery jsou již využívány např. na švýcarských letištích a vlakových nádražích a v USA.[238]

---

[236] Viz dále Letištní rentgen v USA svléká cestující do naha. Dostupné online na: http://digiweb.ihned.cz/c1-19966800-letistni-rentgen-v-usa-svleka-cestujici-donaha [cit.2012-01-29].

[237] Viz tisková zpráva komise - Ochrana letectví: Komise přijímá nová pravidla o používání bezpečnostních skenerů na evropských letištích, dostupná online na http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/1343 [cit.2012-01-29]

[238] Zajímavý článek upozorňující na zavádění rentgenových skannerů na letištích v kontextu ochrany soukromí a střetu se 4. dodatkem americké ústavy nabízí práce autora Andrewa Welcha Full-Body Scanners: Full Protection from Terrorist Attacks or Full-On Violation of the Constitution?; práce je dostupná online na http://law.du.edu/documents/transportation-law-journal/past-issues/v37-03/Welch-Body-Scanners.pdf [cit.2012-01-29].

6.3 Pasy s biometrickými údaji

S tématem této práce jistě souvisí i velice aktuální celoevropské, možná dokonce celosvětové téma, kterým je zavádění **cestovních dokladů vybavenými nosiči biometrických údajů**. Z pohledu této práce je nejzajímavější samozřejmě zobrazení obličeje formou fotografie a dále snímek oční duhovky, kterými mají být mimo jiné do budoucna všechny pasy vybaveny. Pro všechny členské státy Evropské unie vyplynula povinnost vydávat cestovní doklady se strojově čitelnými údaji a s nosičem dat s biometrickými údaji (označované i termínem *elektronické pasy* či *e-pasy*) na základě *Nařízení Rady (ES) č. 2252/2004 ze dne 13.12.2004 o normách pro bezpečnostní a biometrické prvky v cestovních pasech a cestovních dokladech vydávaných členskými státy*. Toto nařízení Rady je pro všechny členské státy závazné a přímo aplikovatelné, nicméně pro stanovení bližších podmínek a zvládnutí celého přechodu na nový typ cestovních dokladů byl v České republice přijat zákon ze dne 14.3.2006 č. 136/2006 Sb., kterým se mění některé zákony na úseku cestovních dokladů. Ten vstoupil v účinnost dnem 1. září 2006.[239]

Samotné nařízení Rady č. 2252/2004 požadovalo zavedení prvního z biometrických údajů na cestovních dokladech, jímž je **zobrazení obličeje** formou uložené digitální fotografie, a to ve lhůtě nejpozději do 18 měsíců od schválení technických specifikací pro cestovní pasy a cestovní doklady, Komisí ES, tj. do 28. 8. 2006. Do 28.6.2009 pak byla zavedena v celé Evropské Unii druhá generace pasů, které obsahují i další biometrický údaj – dva **otisky prstů** držitele pasu. Zatím jen ve fázi úvah je třetí generace cestovních dokladů, které budou navíc obsahovat i **snímek oční duhovky**. Česká republika spolu s mnoha ostatními členskými státy zavedla nové pasy první generace až ke konci dané lhůty, například v Německu ale fungují pasy s digitální fotografií již od podzimu 2005. Spojené státy americké,

[239] Občanské sdružení Iuridicum remedium ještě před účinností zákona č. 136/2006 Sb. upozorňovalo na skutečnost, že v procesu zavádění pasů s RFID čipy na území členských států Evropské unie sehrál podstatnou roli tlak USA a k jeho schválení došlo podle tohoto sdružení v zásadě nestandardním způsobem. Opatření totiž neprošlo běžnou diskusí v národních parlamentech ani v evropském parlamentu a nebylo přihlédnuto ani k námitkám ochránců osobních dat, kteří varovali před riziky spojenými s novou technologií.

iniciátor celého zavádění nových pasů, vydávají pasy s biometrickými údaji od října 2006.

Nařízení podává ve své úvodní části výčet důvodů, pro které se Rada Evropské Unie rozhodla přijmout danou úpravu. Mimo jiné má být harmonizace bezpečnostních prvků a začlenění biometrických identifikátorů důležitým krokem směrem k používání nových prvků s ohledem na budoucí vývoj na evropské úrovni, který by měl učinit cestovní doklady bezpečnějšími a zavést spolehlivější spojení mezi držitelem a cestovním pasem a cestovním dokladem jako důležitý příspěvek k zajištění jeho ochrany před podvodným použitím. Dané nařízení je nepochybně jednou z mnoha právních norem, které byly přijaty zejména v reakci na současný celosvětový boj proti terorismu.

Je nesporným faktem, že Evropská Unie byla před přijetím nové úpravy i pod vlivem Spojených států amerických, které požadovaly z bezpečnostních důvodů co nejrychlejší zavedení moderních cestovních dokladů s biometrickými údaji. Impulsem pro zavádění nových moderních pasů s biometrickými údaji se stal zřejmě fakt, že při teroristických útocích na Spojené státy v září 2001 použili teroristé falešné pasy. V návaznosti na to sdělily americké úřady cca 27 státům, jejichž občané dosud cestovali do USA bez víz, že od 26.10.2006 musí jejich státní příslušníci mít biometrické pasy, anebo budou muset požádat o americké vízum.

Samotné uchovávání biometrických údajů je po technické stránce řešeno **nosičem dat s biometrickými údaji** ve formě plastové (polykarbonátové) stránky, ve které je uložen bezkontaktní čip s anténou a s uloženými daty (jde o tzv. ***RFID čip***). Tato datová stránka obsahující údaje o držiteli cestovního pasu se strojově čitelnými údaji a s nosičem dat s biometrickými údaji; obsahuje také pouhým okem viditelná personalizovaná data a strojově čitelnou zónu. Obdobná technologie je používána u čipových platebních karet, jakož i u nových řidičských průkazů. Speciální technologií tisku (tzv. *laserové gravírování*) pak bude viditelně černobíle zobrazen obličej držitele cestovního dokladu. Každý pas se strojově čitelnými údaji a

s nosičem dat s biometrickými údaji bude celosvětově označován na titulní stránce logem, označujícím přítomnost čipového modulu.[240]

Požadovaný údaj o zobrazení obličeje je pořizován k tomu určenou speciální technologií přímo příslušným úřadem (kterým je obecní úřad obce s rozšířenou působností, příslušný podle místa trvalého pobytu občana, v hlavním městě Praze je jím úřad městské části určený Statutem hlavního města Prahy, a ve městech Brno, Ostrava, Plzeň magistrát těchto měst; dále jsou jimi i zastupitelské úřady České republiky s výjimkou konzulárních úřadů vedených honorárním konzulárním úředníkem). Žadatel o vydání cestovního dokladu se taktéž podepíše s využitím speciální technologie pro účely elektronického zpracování žádosti o vydání cestovního dokladu.[241]

Technickou specifikaci pro nové pasy určila v roce 2003 Mezinárodní organizace pro letectví (International Civil Aviation Organization).

V souvislosti se zaváděním nových cestovních dokladů s moderními čipovými technologiemi se však objevují i hlasy upozorňující na snadnou **zneužitelnost těchto dokladů.** [242] Počátkem srpna 2006 proběhla v americkém Las Vegas konference odborníků na bezpečnostní systémy, kde německý počítačový odborník Lukas Grünwald poukázal na relativní snadnost zkopírování zašifrovaných biometrických údajů držitele dokladu, čehož by mohly zneužít kriminální živly i teroristé. Již v březnu 2006 pak nizozemští odborníci upozornili, že RFID čipy jsou ohroženy i viry, které by se přes čtečky mohly dostat do některého centrálního systému a v nejhorším případě jej vyřadit dočasně z provozu. Často je upozorňováno i na fakt, že citlivé biometrické údaje (nyní tedy digitální scan obličeje i otisky prstů) a další údaje o držiteli pasu mohou zkopírovat třeba orgány nedemokratických

---

[240] Podrobněji k procesu zavádění nových cestovních dokladů s biometrickou technologií viz odpovědi na časté otázky zpracované odborem informatizace veřejné správy Ministerstva vnitra ČR – Cestovní doklady s biometrickými prvky (CDBP). Dostupné online na: http://aplikace.mvcr.cz/archiv2008/rady/faq/biometrika.html [cit.2012-01-29] a dále dokument Biometrika. MVČR. Dostupné online na: http://www.mvcr.cz/clanek/biometrika.aspx [cit.2012-01-29].

[241] Postup při vydávání cestovních dokladů podrobněji stanoví ustanovení §§ 17-28 zákona č. 329/1999 Sb. o cestovních dokladech, ve znění pozdějších předpisů.

[242] V ČR je největším odpůrcem zavádění čipových technologií zřejmě občanské sdružení Iuridicum remedium – viz internetové stránky tohoto sdružení www.iure.org a www.bigbrotherawards.cz.

států, do nichž držitelé pasů cestují a mohou tak být neoprávněně vytvářeny celé databáze těchto údajů, se kterými pak může být nekontrolovaně nakládáno.[243]

I samotné české státní orgány nezpochybňují relativně snadnou **možnost detekce čipu** obsaženého v nových pasech. Výkonným zařízením lze totiž čip v pase detekovat až na vzdálenost několika metrů. Ochrana samotných dat uložených na čipu je pak zajišťována především tzv. technologií *Basic Access Control*, která znemožňuje načtení čipu u zavřeného pasu (k tomu jsou nutná data obsažená na stránkách pasu). Navíc jsou biometrické údaje zašifrovány a chráněny elektronickým klíčem. Při vydávání pasu jsou sice biometrické údaje o držiteli pasu po dobu maximálně 60 dnů uchovávány v databázi v souvislosti s výrobou a případnou reklamací pasu, pak jsou však mazány a zůstávají uloženy toliko na čipu v cestovním dokladu. Do informačního systému evidence cestovních dokladů jsou zaváděny pouze údaje o e-pasu a jeho držiteli bez biometrických údajů.

Závěrem je třeba se zmínit o tom, že používání biometrických údajů v cestovních dokladech není novinkou, i stávající pasy obsahují fotografii a podpis jejich držitele. Co je však nové, je možnost **automatické verifikace osoby pomocí biometrických technologií.** Kontrola cestujících osob, včetně vyhledávání a porovnávání s různými databázemi (Interpol, trestní rejstříky atd.) již nebude oproti minulosti probíhat manuálně, nýbrž bude zautomatizována a tím velmi zefektivněna. Možnost tzv. biometrické verifikace je bezesporu významným bezpečnostním faktorem elektro-

[243] Viz např. Biometrické pasy s čipem mohou být "klonovány". Dostupné online na http://hn.ihned.cz/c1-19036740-biometricke-pasy-s-cipem-mohou-byt-klonovany [cit.2012-01-29]
V zájmu co největší objektivity jsem však povinen uvést, že pan Lukas Grünwald použil pro zkopírování německý pas, přičemž německé pasy ale nejsou vybavovány nepovinným vyšším stupněm zabezpečení proti kopírování, tzv. aktivní autentizací (e-pasy např. v ČR však ano). Pas bez vyššího stupně zabezpečení je sice technicky možné neoprávněně zkopírovat, nicméně nikdy nelze měnit v pase uložené údaje (lze tedy de facto zhotovit prostý duplikát pasu, ten ale těžko zneužije podvodník bez možnosti změny biometrických údajů); pas vybavený aktivní autentizací navíc obsahuje tzv. soukromý asymetrický klíč, který nelze zkopírovat a nelze tak vytvořit úplnou kopii pasu (právě aktivní autentizaci používá i ČR). Stejně tak samotné získávání údajů o cestujících osobách ze strany nedemokratických států není nic nového, pokud se tak děje, tak i se starými pasy. Přístup k zašifrovaným biometrickým údajům však budou mít jen ty státy, resp. subjekty, které budou vybaveny elektronickým certifikátem. Otázky kolem případné zneužitelnosti této moderní technologie však přesto zůstávají.

nických pasů vybavených biometrickými daty. Je totiž pravda, že stávající digitální fotografie a z ní čitelné biometrické údaje mají stále velkou **chybovost** (až 10%, při špatných světelných podmínkách dokonce až 50%) a nemohou tak být samy o sobě spolehlivým autentizačním údajem.

Po kompletním zavedení biometrických údajů s otisky prstů nebo dokonce se schématem oční duhovky však bude identifikace prakticky stoprocentně bezchybová (chybovost v řádech desetin procenta). Již nyní však e-pasy poskytují výrazně dokonalejší ochranu před zneužitím.[244]

6.4 Policejní databáze a evidence obsahující obrazové záznamy

Pouze okrajově a zcela závěrem této práce bych chtěl zmínit existenci nejrůznějších databází užívaných bezpečnostními složkami, které obsahují obrazové záznamy osob, a jež jsou určeny zejména k identifikaci osob.

Rozkazem policejního prezidenta č. 10/2004 byl zaveden nejprve zkušební provoz databázového informačního systému **FODAGEN** (FOtografie, DAktyloskopie, GENetika). Systém je využíván jednotlivými pracovišti Služby kriminální policie a vyšetřování za účelem sběru a ukládání informací o osobách a obsahuje základní popis, fotografie, daktyloskopické údaje a vzorky genetického materiálu Tento systém zprostředkovává zjednodušený vstup do jednotlivých stávajících informačních systémů C-AFIS, CODIS, INFO-DNA a evidenci třídílných kriminalistických fotografií.[245]

Policie ČR dále využívá systém **ViCLAS**, jehož smyslem je zjišťování a evidování významných vlastností a vzájemných souvislostí mezi sledovanými trestnými činy a osobami zejména při objasňování nejzávažnějších případů násilné a mravnostní trestné činnosti typu vražd, znásilnění, únosů. Systém je bohužel zastaralý, je vystaven na technologii z roku 1994, byl k nám importován z Kanady. Identifikaci určité osoby lze zjednodušit pomocí tzv. portrétní identifikace díky počítačovým systémům

---

[244] K problematice elektronických pasů viz ŘÍHA, Z.: Elektronické pasy. In: Zpravodaj ÚVT MU. ISSN 1212-0901, 2006, roč. XVII, č. 1, s. 7-12.

[245] Blíže např. HLAVÁČEK, J. a kol.: FODAGEN aneb Proč potřebujeme zkvalitnit evidenci pachatelů. Kriminalistický sborník, 2002, č. 4, s. 27-37

Poridos anebo **Facette**. Další databází je např. systém **FISH** (forenzní automatický systém pro rukopisy), který uchovává digitalizované vzorky písma jednotlivých osob, databáze pachových stop, hlasových záznamů, nejrůznějších obrazových a video záznamů atd..[246] Informace o vyšetřovaných případech se dostanou, mimo jiné, i do dalších centrálních policejních databází, jako jsou informační systémy *NTC, ZOP, AVIZO, SOV, ZEP, DOTAZY* apod.

Z hlediska využití kamerových systémů je pro nás zajímavý systém **AKV - automatická kontrola vozidel**. Účelem provozování tohoto systému je vedení údajů získaných v místě nasazení automatickým kamerovým systémem o průjezdu motorových vozidel a jejich následné zpracování porovnáním s údaji jiných informačních systémů s cílem zvýšit úspěšnost pátrání po motorových vozidlech, zefektivnit odhalování a vyšetřování trestných činů, zejména souvisejících s motorovými vozidly a samozřejmě i zefektivnit boj proti terorizmu.

Policejní orgány dále provozují celostátní informační systém **TELEFOTO - Aktuální obrazové informace.** Tento systém obsahuje aktuální obrazové informace a sdělení určených pro policejní pracovníky při plnění úkolů, zejména při pátrání po pachatelích zvlášť závažných trestných činů, po hledaných a pohřešovaných osobách, po identitě (totožnosti) osob, které nemohou nebo nechtějí prokázat svoji totožnost, po identifikaci nálezů mrtvol nebo částí lidských těl neznámé totožnosti, po odcizených nebo ztracených věcech atd.

Jako další informační systémy Policie ČR jmenujme systém *C-PATROS* (pátrání po osobách), *C-PATRMV* (pátrání po vozidlech) či systém *C-ENO* (evidence nežádoucích osob).

Policejní orgány samozřejmě využívají celou řadu dalších nástrojů, databází a informačních nástrojů. Chtěl jsem v této kapitole jen nastínit přehled těch pro tuto práci nejzajímavějších systémů, které určitým způsobem zpracovávají nebo pracují s obrazovými informacemi. Osobně

---

[246] K dalším biometrickým systémům a nejrůznějším evidencím viz kupříkladu VANČO, E.: Biometrie, biometrika - geneze, vývoj a současné pojetí. Časopis Kriminalista č. 1/2005 nebo STRAUS, J.: Příspěvek k identifikaci objektů a systémů v kriminalistice. Časopis Kriminalista č. 2/2005

nevidím v těchto databázích a informačních systémech z pohledu ochrany soukromí problém, policejní orgány jsou ostatně vázány nejrůznějšími povinnostmi uvedenými mimo jiné v zákoně o Policii České republiky (viz Hlava X. - Práce s informacemi - zákona č. 273/2008 Sb.).

7 ZÁVĚR

Téma obrazového monitoringu s akcentem na ochranu soukromí jednotlivce je tématem nesmírně zajímavým, aktuálním a veřejností široce diskutovaným. Je to téma, které zasahuje do sféry života snad každého jednotlivce. Každý z nás se ve svém běžném denním životě setkává s kamerovými systémy zhusta instalovanými v ulicích měst, v šatnách plaveckých stadionů, v metru a všude možně jinde. Hodně z nás má přímou zkušenost s nahráváním fotografií na internetový virtuální prostor, sdílený miliony lidí celého světa. Část z nás má také přímou zkušenost, kdy jeho obrazové záznamy či jeho identita byla ohrožena. Ve své práci jsem chtěl poukázat na čím dál větší rozvoj obrazových sledovacích technologií a jejich rozšíření do všech možných sfér lidského života. Beru tento nástup sledovacích prostředků jako nutný, jako něco, co může nesmírně zlepšit a zefektivnit práci mnoha lidí a úřadů. Poznatky získané při oficiálním (úředním) provozu lze pak mnohdy využít i např. ve vědecké sféře, kde nesmírně zrychlí vědecký pokrok (kupř. satelitní sledování země, počasí, přírodních jevů, zákonitostí atd.). Je samozřejmé, že všechny tyto technologie mají potenciál v obrovské míře narušit a zneužít soukromí lidí.

Troufám si tvrdit, že v horizontu let či několika málo desetiletí budou moderní informační technologie, včetně obrazového a jiného sledování ještě na řádově vyšším stupni vývoje, než jsou nyní. Bude-li to nutné či žádoucí, nebude žádným technickým problémem monitorovat prakticky všechno do neskutečných detailů a podrobností. Stejně tak budou technologická zařízení pro archivaci dat na takovém stupni vývoje, že umožní bez větších problémů archivovat a obsáhnout prakticky celý lidský život od narození až po smrt ve všech jeho souvislostech a aspektech, od nejpodrobnějších údajů o samotné osobě, po její sociální zázemí, její názory, zvyky, potřeby, její aktivity, včetně velmi podrobných zvukových i obrazových záznamů.

Už teď není problém se zaměřit na prakticky jakoukoliv osobu na celém světě (možná s výjimkou zcela odlehlých oblastí bez civilizačního pokroku) a zjistit o ní prakticky cokoliv. Lze bez problému monitorovat její

veškerý pohyb, vést evidenci jejích veškerých aktivit, a to i v natolik soukromých oblastech, kde to ještě před pár desetiletími bylo zcela nepředstavitelné. Není problém danou osobu pozorovat, i když je ve zdánlivém bezpečí domova a uzavřených čtyř stěn. Dosavadní omezení, která zabraňují naprosté devastaci a anulování zdání soukromého života, spočívají v současném systému záruk právní ochrany, jakož i ještě stále v technologických omezeních, kdy prostě nelze nepřetržitě sledovat a monitorovat každého člověka. V blízké budoucnosti již však dozajista nebude žádným problémem archivovat kontinuálně obsah nejen veškeré elektronické komunikace, ale i všech jejích dalších aktivit. Ruku v ruce s tím budou vyvinuta či zdokonalena zařízení schopná analyzovat a zaměřovat se na možné problémy a rizika v souvislosti s bojem proti terorismu a kriminalitě, ale i s dalšími sférami státní správy. Stejně tak dostane tyto možnosti ve větší či menší míře i soukromý sektor a netušený rozmach informačních technologií si bude vyžadovat stále preciznější a dokonalejší právní úpravu, která se bude neustále měnit a vyvíjet.

Bude jen na společnosti a jejím uvědomění, nakolik dovolí v zájmu a nezbytnosti vědeckého a společenského vývoje tolerovat zásahy do soukromí jednotlivců. Každý člověk má sociální a dokonce i biologickou potřebu soukromí a málokdo snese naprosté odhalení svého soukromého života. Bude jen a jen na lidech samotných, jakým směrem se budou společenské změny v této problematice dít.

Není sporu o to, zda osobní údaje a další data a skutečnosti týkající se konkrétní osoby lze zneužít, jde spíše o to, zda tyto citlivé údaje vůbec jde uhlídat. Ne nadarmo se v tomto kontextu v poslední době ve sféře informačních technologií začíná prosazovat pojem právo být zapomenut *(right to be forgotten*), dnes není problém zjistit o dané konkrétní osobě až zarážející množství údajů, problémem se však stává i možnost vystopování daných informací i po delším čase a v různých místech virtuálního světa, problémem se stává nemožnost zastavit šíření určité závadné infroamce o dané osobě. Domnívám se, že stoprocentní záruky nemůže poskytnout sebelepší právní řád či sebedokonalejší ochranná technologie. Vždy budou existovat cesty, jak se neoprávněně dostat k citlivým údajům a tyto následně použít pro vlastní potřebu či je dále šířit. Jedno z hlavních hledisek, které má

vliv na možnost zneužití osobních údajů, je však vždy hledisko opatrnosti každého jednotlivce. Je na každém člověku, nakolik umožní ostatním nahlédnout do svého soukromí, nakolik opatrně se bude chovat, aby zamezil možnému zneužití svých údajů; to platí, zejména pokud jde o využívání moderních informačních technologií jako je síť Internet a mobilní komunikační zařízení.

Společnost by měla stanovit co nejlepší systém účinných záruk a pojistek před neoprávněným získáváním jakýchkoliv privátních informací a ty případy, kdy se tomuto neoprávněnému shromažďování údajů nepodaří zabránit, pak kriminalizovat či je postihnout jinými právními sankcemi. Lze tedy oddělit případy narušení soukromí (mnohdy samozřejmě i nechtěné) od případů, kdy po takovémto narušení soukromí dojde i ke zneužití získaných dat.

Jinými slovy, pokud již selháním lidského faktoru, nedokonalostí zabezpečení či jakkoliv jinak dojde k neoprávněnému úniku dat, je třeba, aby zde byly takové právní prostředky (zejména trestněprávní instituty a právní prostředky ochrany osobnosti), které by zamezily použití a dalšímu využívání či šíření ze strany subjektů, které takovéto informace již neoprávněně získaly.

Ve společnosti spolu s technickým pokrokem sílí i hlasy jednotlivců a skupin, které bojují někdy až fanaticky proti zásahům do soukromé sféry člověka. Je pravdou, že ještě před několika málo desetiletími byly např. úvahy o očipování lidí, o sledování každého kroku a projevu člověka pouze v mysli autorů scifi románů. Nyní jsou tyto představy realitou, která může v myslích mnoha lidí vyvolat pochopitelné obavy o veškerou ztrátu soukromí. Pronikání moderních technologií, včetně sledovacích, do běžného života lidí však nelze zabránit, snad jen s výjimkou totální negace jakéhokoliv vývoje a zakonzervování současného stavu.

Je v celku jedno, na základě jakých důvodů dochází v poslední době k masivnímu nárůstu využívání sledovacích technologií ve všech aspektech lidského života. Je lhostejno, zda hrozba terorismu a nutnost boje s kriminalitou je či není tím hlavním důvodem pro tuto invazi do soukromí obyvatelstva. Podstatné je, že se tak děje a že technický pokrok, který je tím zásadním impulsem pro tento stav, nelze zastavit, stejně jako požadavky

mnoha oblastí lidských aktivit, které mohou na rozšíření sledovacích technologií v zájmu celé společnosti profitovat.

Mám-li vyjádřit svůj osobní názor na téma postupujícího pronikání obrazových sledovacích technologií a rozšiřování pravomocí bezpečnostních služeb a orgánů z důvodu boje proti teroru a kriminalitě, domnívám se, že daný vývoj je logický a v této fázi vývoje lidské společnosti patrně nevyhnutelný. V případě, že k omezování soukromí jednotlivců bude vždy docházet pouze z důvodu zajištění bezpečnosti a jiného významného veřejného zájmu, je čím dál vyšší využívání moderních technologií schopných invaze do soukromí v pořádku. V žádném případě jich však nesmí být zneužito nad nezbytně nutnou míru a vždy musí existovat účinný a efektivní systém jejich kontroly. Společnost si musí sama určovat svou toleranci k omezení práv na soukromí jednotlivců – v nedávné historii lze nalézt příklady, kdy se státy v okamžitém strachu z nenadálého teroristického útoku či krize rozhodly překotně měnit zavedená pravidla ochrany soukromí ve směru k jejich omezení a rozšíření pravomocí bezpečnostních orgánů (viz legislativní vývoj v USA po útocích v září 2001 a přijetí např. poměrně kontroverzního zákona Patriotic Act).

Jsem přesvědčen, že cesta do budoucna není v zabraňování rozšiřování pravomocí bezpečnostních a špionážních služeb, a stejně tak ani i ve zřejmě marných snahách o omezování všemožných jiných zásahů do soukromí lidí pomocí moderních technologií. Technický pokrok a zejména vůle lidí využít jej pro své komerční a jiné účely si cestu do soukromí lidí vždy najdou. Spíše bude vhodnější nebránit využití moderních technologií pro prospěšné účely a v odůvodnitelné míře (boj se zločinem, zvyšování bezpečnosti, vědecké a jiné využití atd.) a naopak se snažit **zajistit co nejlepší záruky proti zneužití poznatků takto získaných o soukromí jednotlivých lidí**. Zabránit tedy tomu, aby informace a osobní údaje o jednotlivcích získané z veřejně prospěšného důvodu nebyly neoprávněně použity i jinak. Právě tudy by mělo jít i právo a všechny jeho nástroje a instituty umožňující účinnou regulaci problematiky zásahů do soukromí.

Nesmírně významnou roli hrají bezesporu i státní instituce pověřené kontrolou dodržování státem garantovaného práva na soukromí, jakož i mnohé nevládní organizace a sdružení, které mohou zejména svými

praktickými podněty poukázat na možná rizika zneužití technologií a nástrojů vedoucích k neoprávněným zásahům do soukromí lidí. Je jen a jen žádoucí, aby vedle sebe existovaly dostatečné silné vládní instituce zaměřené na ochranu soukromí a stejně tak i řada zcela nezávislých nevládních organizací, které mohou mnohdy flexibilněji a cíleněji reagovat na aktuální problémy a hrozby.

Zneužití moderních sledovacích technologií pro proniknutí do soukromí jednotlivců může představovat obrovský problém v nedemokratických totalitních státech s rozvinutým bezpečnostně policejním aparátem; obdobným, jakým byly bezpečnostní složky a jejich oprávnění a použitelné prostředky v komunistických státech (a obdobným jako např. v dnešní době již ne tak utopistické Orwellově knize „1984“). V těchto státech totiž neexistují demokratické záruky (jako nezávislá justice a jiné instituce na kontrolu zásahů do soukromí) proti zneužití moci a veškerých jejích nástrojů, včetně sledovacích technologií, často však tyto státy (snad s výjimkou Číny) současně ani nedisponují potřebnou vyspělou technologií, jež by umožňovala sledování lidí a způsobovala narušení soukromí.

Pokud jde konkrétně o kamerové systémy, asi těžko kdokoliv zabrání jejich dalšímu využívání a rozšiřování. Faktem je, že se zatím jednoznačně nepotvrzují hypotézy o celkovém snížení kriminality v důsledku instalace kamer, spíše dochází k přesunu kriminality a jiným jevům. Část lidské populace bude vždy proti rozšiřování kamerových systémů a jakémukoliv pronikání sledovacích systémů do běžného života, rozhodný bude však názor většinové společnosti. Podle mého názoru se většinový názor ustaluje na toleranci nárůstu užití kamerových systémů, lidem kamery v ulicích a veřejných prostranstvích nevadí, zvykají si na ně a mnohdy možná díky jejich existenci i přizpůsobují své jednání (počítají se sníženou mírou soukromí a s tím, že mohou, ale nemusí, být zrovna sledováni – i zde se projevuje v této práci již zmíněná paralela s myšlenkou Panopticonu Jeremy Benthana). Lidé taktéž často a rádi využívají i další možnosti a systémy, které mají potenciál narušit jejich soukromí – viz nadšení lidí z možností aplikace Google StreetView a dalších aplikací, masivní rozšíření sdílení

fotografií na webu a na sociálních sítích či oblíbenost pořizování a sdílení videí na portálu Youtube a dalších.

Právní řád jen postupně kamerové systémy a obdobné technologické novinky přijímá a stanoví jasné mantinely jejich využívání. Zejména v počátečním období byl hybatelem a jakýmsi vodítkem pro užívání kamer v ČR Úřad na ochranu osobních údajů. Stále žijeme v době, kdy právní řád nestanoví jasná pravidla použití kamerových systémů, praxe tak mnohdy využívá stanovisek a fundovaných názorů ÚOOÚ.

Zpracovávané téma ochrany soukromí a obrazového monitoringu svým rozsahem, ale i stále aktuálnějším významem přesahuje možnosti této disertační práce. Ta si kladla za cíl spíše základní seznámení s problematikou, setřídění a vymezení hlavních témat. Téma si však jistě zaslouží větší pozornost, včetně publikace možná i rozsáhlejších děl, než je toto.

Svou práci jsem se rozhodl uzavřít citátem z knihy George Orwella „*1984*“. I když se ve světle současného technologického pokroku a společenské situace ukázaly vizionářské představy Orwellovy antiutopické společnosti v mnohém až neskutečně pravdivé, doufejme, že se jeho vize nenaplní ani dnes ani v budoucnu a že demokratické státy světa nepřipustí zneužití moderních technologií k sledovacím účelům, jež by zasáhly do soukromí jednotlivců nad nezbytnou míru:

„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, ze zvyku, který se stal pudovým - v předpokladu, že každý zvuk, který vydá, je zaslechnut, a každý pohyb, pokud není tma, zaznamenán.“[247]

[247] ORWELL, G.: 1984. Praha: Naše Vojsko, 1991

8 SEZNAM LITERATURY A DALŠÍCH PRAMENŮ

Knižní monografie

- ADAMUS, V. (Eds.): Mezinárodní dokumenty o lidských právech – anglicky a česky. Praha: LINDE, 2000
- BÁRÁNY, E.: Moc a právo, Bratislava 1997, s. 183
- BARTÍK, V. JANEČKOVÁ, E: Kamerové systémy v praxi. Praha: LINDE, 2011.
- BARTOŇ, M.: Svoboda projevu a její meze v právu ČR. Praha: LINDE, 2002
- BERGER, V.: Judikatura Evropského soudu pro lidská práva. Praha: IFEC s.r.o.
- BEZOUŠKA, P - HULMÁK, M. - KAVKA, J. - PÍTRA, V.: Praktikum Občanské právo hmotné. Plzeň, Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2005
- BLACK, H.: Blackův právnický slovník, I. a II. díl. 6. vydání, Praha: VICTORIA PUBLISHING, 1993
- BLAHOŽ, J. – BALAŠ, V. – KLÍMA, K.: Srovnávací ústavní právo. Praha: ASPI Publishing, 2003
- BLAHOŽ, J. – KLÍMA. K. – SKÁLA, J. a kolektiv: Ústavní právo Evropské Unie. 1. vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2003
- BLAHOŽ, J.: Sjednocující se Evropa a lidská a občanská práva. Praha: ASPI, 2005
- BRABEC, F. a kolektiv: Bezpečnost pro firmu, úřad, občana. Praha: Nakladatelství Public History, 2001
- BRZYBOHATÝ, M.: Terorismus I., Praha: Police History, 1999
- BUŘIČ F., ČECH B.: Technické prostředky bezpečnostních služeb; Praha, Policejní akademie ČR, 1994
- CÍSAŘOVÁ, D. a kol.: Trestní právo procesní. 2. vydání. Praha: LINDE, 2002

- ČAPEK, JAN: Právnický slovník evropské ochrany lidských práv. Praha: ORAC 1998
- ČEPELKA, Č. – ŠTURMA, P.: Mezinárodní právo veřejné. 1. vydání. Praha: EUROLEX BOHEMIA s.r.o., 2003
- DANČÁK, B. – ŠIMÍČEK, V. (Eds.): Bezpečnost České republiky – Právní aspekty situace po 11. září 2001. Sborník z konference. Brno: Masarykova univerzita v Brně, Mezinárodní politologický ústav, 2002
- DANČÁK, B. – ŠIMÍČEK, V. (Eds.): Deset let listiny základních práv a svobod v právním řádu České republiky a Slovenské republiky. Masarykova univerzita v Brně a Mezinárodní politologický ústav, 2001
- DAVID, V. – MALACKA, M.: Fenomén mezinárodního terorismu. Praha: LINDE, 2005
- DAVID, V. – SLADKÝ, P. – ZBOŘIL, F.: Mezinárodní právo veřejné. 2. vydání. Praha: LINDE, 2005
- DOLEŽÍLEK, J. (Eds.): Přehled judikatury ve věcech ochrany osobnosti. Praha: ASPI Publishing s.r.o., 2002
- DUNNIGAN, J. F.: Bojiště zítřka – Tváří v tvář globální hrozbě kybernetického terorismu. Praha: Baronet, a.s., 2004
- ELIÁŠ, K. – ZUKLÍNOVÁ, M.: Principy a východiska pro nový kodex soukromého práva. Praha: LINDE, 2001
- ENCYKLOPEDIE: SVĚTOVÝ TERORISMUS, Od starověku až po útok na USA, Praha: Svojtka & Co. 2001
- FIALA – HRUŠKOVÁ – HURDÍK – KORECKÁ: Občanské právo hmotné. II. Praha: Státní pedagogické nakladatelství, 1984
- FIALA, J. a kol.: Občanské právo hmotné. 3.vydání, Brno: Masarykova univerzita v Brně, 2002
- FIALA, J. a kolektiv: Občanské právo hmotné. 3. vydání. Brno: MU v Brně, nakladatelství Doplněk, 2002
- FILIP, J. – SVATOŇ, J. – ZIMEK, J.: Základy státovědy. 3. vydání. Masarykova univerzita v Brně, 2002
- FILIP, J.: Vybrané kapitoly ke studiu ústavního práva. Brno: Masarykova univerzita v Brně, 1999

- FLÉGL, V.: Člověk a lidská práva (Sbírka úmluv a deklarací). Praha: SPEKTRUM, 1990
- FLÉGL, V.: Listina základních práv a svobod v aplikační praxi ČR. Praha: C. H. BECK, 1997
- FLÉGL, V.: Ústavní a mezinárodní ochrana lidských práv. Praha: C. H. BECK, 1997
- FLÉGL, V.: Významné mezinárodní dokumenty k ochraně lidských práv. Praha: C. H. BECK, 1998
- GERLOCH, A. – HŘEBEJK, J. – ZOUBEK, V.: Ústavní systém České republiky. Praha: PROSPEKTRUM, 2002
- GIFFORD, C.: Svět špionáže. Havlíčkův Brod: Fragment, 2006
- GRÓNSKÝ, J.: Komentované dokumenty k ústavním dějinám Československa, I. – 1914-1945, Praha: UK Karolinum, 2005
- GŘIVNA, T., POLČÁK, R. a kol.: Kyberkriminalita a právo. Praha, Auditorium, 2008
- HERZÁN, MARTIN: Totalitní světovláda. Bratislava: Eko-konzult, 2002
- HOLUB, M. – FIALA, J. – BIČOVSKÝ, J.: Občanský zákoník. Poznámkové vydání s judikaturou a literaturou. 11. vydání, Praha: LINDE 2005
- HOLUB, M. a kolektiv autorů: Občanský zákoník – komentář. 2. vydání, Praha: LINDE, 2003
- HUBÁLKOVÁ, E.: Evropská úmluva o lidských právech a Česká republika – Judikatura a řízení před Evropským soudem pro lidská práva. Praha: LINDE, 2003
- HUNDÁK, Š.: Použití operativně pátracích prostředků k získání důkazů pro trestní řízení. Praha: Policejní akademie České republiky, 2004
- CHMELÍK I. a kolektiv: Zločin bez hranic – vyšetřování terorismu a organizovaného zločinu; Praha: LINDE, 2004
- JEHLIČKA, O. – ŠVESTKA, J. – ŠKÁROVÁ, M. a kol.: Občanský zákoník. Komentář.10. vydání. Praha: C. H. BECK, 2006

- JECHOUTEK, J. – HLAVÁČEK, J. (Eds.): Ochrana dat a právní úprava v ČR – sborník referátů a sdělení ze semináře konaného dne 20.4.1993 v Praze. Praha: LERINGO, 1993
- JELÍNEK, J. a kol.: Trestní právo procesní. 4. aktualizované vydání. Praha: EUROLEX BOHEMIA, 2005
- JOUZA, J.: Zákoník práce s komentářem. 2. vydání. Praha: BOVA POLYGON, 2007
- KLÍMA, K. a kol.: Komentář k Ústavě a Listině. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2005
- KLÍMA, K. a kol.: Praktikum českého ústavního práva. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2004
- KLÍMA, K.: Ústavní právo. 2. vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2004
- KLOKOČKA, V. – WAGNEROVÁ, E.: Ústavy států Evropské Unie, Díl první. Praha: LINDE, 2004
- KLOKOČKA, V.: Ústavy států Evropské Unie. Díl druhý. Praha: LINDE, 2005
- KNAPP, K. - ŠVESTKA, J.: Ochrana osobnosti podle československého občanského práva. 2. vydání. Praha: Panorama, nakladatelství a vydavatelství, 1989
- KNAPP – ŠVESTKA – JEHLIČKA a kol.: Ochrana osobnosti podle občanského práva. 4 vydání. Praha: LINDE, 2004.
- KNAPPOVÁ - ŠVESTKA - DVOŘÁK (Eds.): Občanské právo hmotné, svazek I., 4. vydání, Praha: ASPI Publishing s.r.o., 2005
- KONÍČEK T. - KŘEČEK S. - KOCÁBEK P.: Městské kamerové dohlížecí systémy, Praha: Odbor prevence kriminality Ministerstva vnitra ČR, 2002
- KRATOCHVÍL, Z.: Nové občanské právo. Praha: Orbis, 1965, s. 63
- KRIEGER, W. (Eds.): Tajné služby ve světových dějinách (Špionáže a utajené akce od antiky po současnost). Olomouc: FONTÁNA, 2006
- KUČEROVÁ, A. - BARTÍK, V. - PECA, J. - NEUWIRT, K. - NEJEDLÝ, J.: Zákon o ochraně osobních údajů. Komentář. 1. vydání. Praha: C. H. BECK, 2003

- KUNC, J. (Eds.): Demokracie a ústavnost, Praha: Vydavatelství Univerzity Karlovy, 1996
- LLOYD, M.: Guinessova kniha špionáže. Praha: Olympia, 1996
- MAREŠ, M.: Terorismus v ČR. Brno: Centrum strategických studií, 2005
- MATĚJKA, M.: Počítačová kriminalita. Praha: Vydavatelství a nakladatelství Computer Press, 2002, s. 21
- MATES – ČECHMÁNEK – HROMÁDKA – KRAMÁŘ – RAJMAN: Policejní právo – právní předpisy s komentářem. 3. vydání. Praha: LINDE, 2006
- MATES P. - NEUWIRTH K.: Právní úprava ochrany osobních údajů v ČR – poznámkové vydání se zapracovanou důvodovou zprávou. Praha: IFEC 2000
- MATES, P. - MATOUŠOVÁ, M.: Evidence, informace, systémy – právní úprava. Praha: CODEX Bohemia, s.r.o., 1997
- MATES, P.: Ochrana osobních údajů. Praha: Univerzita Karlova v Praze – Nakladatelství Karolinum, 2002
- MATES, P.: Ochrana soukromí ve správním právu. 2. vydání. Praha: LINDE 2006
- MATOUŠOVÁ, M. – HEJLÍK, L.: Osobní údaje a jejich ochrana. Praha: ASPI Publishing s.r.o., 2003
- MATOUŠOVÁ, M. a kolektiv: Ochrana osobních údajů v otázkách a odpovědích. Praha, ASPI Publishing s.r.o., 2004
- MIKULE, V. – SLÁDEČEK, V.: Ústavní soudnictví a lidská práva (Předpisy, dokumenty, komentáře a poznámky). Praha: CODEX, 1994
- MUSIL, J. – KRATOCHVÍL, V – ŠÁMAL, P. a kol.: Kurs trestního práva. Trestní právo procesní. 2. přepracované vydání. Praha, C. H. BECK, 2003
- MUSIL, S. (Eds.): Počítačová kriminalita. Nástin problematiky. Kompendium názorů specialistů. Praha, Institut pro kriminologii a sociální prevenci, 2000
- NĚMEC, M.: Mafie a zločinecké gangy, Praha: Eurounion 2003

- ONDŘEJ, J. - POTOČNÝ, M.: Obecné mezinárodní právo v dokumentech. Vydání druhé. Praha: C. H. BECK, 2004
- ONDŘEJ, J.: Mezinárodní právo veřejné, soukromé, obchodní. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2004
- ORWELL, G.: 1984. Praha: Naše Vojsko, 1991
- PAVLÍČEK, V. – HŘEBEJK, J.: Ústava a ústavní řád České republiky. Komentář. 1. díl - Ústavní systém, 2. vydání. Praha: LINDE, 1998
- PAVLÍČEK, V. a kolektiv: Bezpečnost České republiky a potřeba ústavních změn. Sborník příspěvků a statí z mezinárodní konference Praha 18.-19.9.2003. Praha: Univerzita Karlova v Praze – Právnická fakulta, 2004
- PAVLÍČEK, V. a kolektiv: Právo a bezpečnost státu (Sborník statí). Praha: Univerzita Karlova v Praze – Právnická fakulta, 2002
- PAVLÍČEK, V. a kolektiv: Transformace ústavních systémů zemí střední a východní Evropy. Sborník statí a texty ústav. I. část. Praha: Univerzita Karlova v Praze – Právnická fakulta, 1999
- PAVLÍČEK, V. a kolektiv: Transformace ústavních systémů zemí střední a východní Evropy. Sborník příspěvků a statí z konference. II. část. Praha: Univerzita Karlova v Praze – Právnická fakulta, 2000
- PAVLÍČEK, V. a kolektiv: Ústava a ústavní řád České republiky. Komentář. 2. díl - Práva a svobody, 2. vydání. Praha: LINDE, 2002
- PAVLÍČEK, V. a kolektiv: Ústavní právo a státověda. II. Díl Ústavní právo České republiky, Část 2. Praha: LINDE, 2004
- PAVLÍČEK, V.; JIRÁSKOVÁ, V. a kolektiv: Transformace ústavních systémů zemí střední a východní Evropy. Texty ústav zemí střední a východní Evropy a stati. III. část. Praha: Univerzita Karlova v Praze – Právnická fakulta, 2001
- PLECITÝ, V. – HLAVSA, P. - KOCOUREK, J.: Civilní kodexy (Občanský zákon, Občanský soudní řád). Praha: EUROUNION, s.r.o., 2000
- PLECITÝ, V. – KOCOUREK, J.: Občanský zákoník. 3. vydání. Praha: EUROUNION Praha, s.r.o., 2004

- PLECITÝ, V. - VRABEC, J. – SALAČ, J.: Základy občanského práva. 2. vydání. Plzeň, Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2005
- PLECITÝ, V. – VRABEC, J.: Základy občanského práva. 2. vydání, Praha: PROSPEKTUM, 1999
- Pocta Jiřímu Švestkovi k 75. narozeninám. Praha: ASPI, a.s., 2005
- Pocta Martě Knappové k 80. narozeninám. Praha: ASPI, a.s., 2005
- POTOČNÝ, M. – ONDŘEJ, J.: Mezinárodní právo veřejné – Zvláštní část. 3. doplněné a rozšířené vydání. Praha: C. H. BECK, 2002
- POVOLNÝ, D.: Operativní technika v rukou StB, 1. vydání, Praha: Úřad dokumentace a vyšetřování zločinů komunismu PČR, 2001
- POŽÁR, J.: Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN: 80-86898-38-5
- PRYSZCZ, M. Možnosti využití bezpilotních prostředků pro civilní účely. Brno: VUT, 2007.
- REISCHL, G.: Sběratelé elektronických dat pod lupou. Praha: Euromedia Group, 2001
- ROUČEK, J. – SEDLÁČEK, F.: Komentář k čs. obecnému zákoníku občanskému. Praha 1933
- SCHEINOST (Eds.): Legislativa a policie v boji proti organizovanému zločinu – sborník studií. Praha: Institut pro kriminologii a sociální prevenci, 1997
- SCHEU, H. (Eds.): Právní aspekty boje proti terorismu. Praha: Univerzita Karlova v Praze – Evropské informační středisko, 2005
- SLOUPENSKÝ, A. – ŽEHRA, F.: Bankovní bezpečnost. Praha: Bankovní institut, a.s., 1997
- SMEJKAL, V. a kol.: Právo informačních a telekomunikačních systémů. 1. vydání. Praha, C. H. Beck 2001, 542 str., ISBN 80-7179-552-6
- SMEJKAL, V.: Internet a §§§ (Internet a paragrafy). 2. aktualizované, přepracované a doplněné vydání, GRADA, Praha 2001, 289 str., ISBN 80-247-0058-1
- SUDRE, F.: Mezinárodní a evropské právo lidských práv, Masarykova univerzita v Brně, 1997

- ŠÁMAL, P. a kol.: Trestní zákoník I., II. Komentář. 1. Vydání. Praha: C.H.BECK, 2010.
- ŠÁMAL, K. - KRÁL, V. - BAXA, J. a kol.: Trestní řád. Komentář. I. a II. Díl. 5. vydání. Praha: C. H. Beck, 2005
- ŠÁMAL, P. – NOVOTNÝ, F. - RŮŽIČKA a kol.: Přípravné řízení trestní. Praha: C. H. BECK, 2003
- ŠIMÍČEK, V.: Odborné stanovisko k otázce ústavně právní přípustnosti instalace odposlechů a kamerových systémů ve výchovných ústavech a podobných zařízeních. Brno: Právnická fakulta Masarykovy Univerzity, 2003
- ŠTURMA, P.: Mezinárodní a evropské instrumenty proti terorismu a organizovanému zločinu. Praha: C. H. BECK, 2003
- ŠTURMA, P.: Mezinárodní a evropské kontrolní mechanismy v oblasti lidských práv. Praha: C. H. BECK, 2003
- ŠVESTKA, SPÁČIL, ŠKÁROVÁ, HULMÁK a kol.: Občanský zákoník I. § 1 až 459. Komentář. 2. Vydání. Praha: C.H.BECK, 2009
- TICHÝ, L. - ARNOLD, R. - SVOBODA, P. - ZEMÁNEK, J. - KRÁL, R.: Evropské právo. 3. vydání. Praha: C. H. BECK, 2006
- TUREČEK, J.: Technické prostředky bezpečnostních služeb – detektory pro bezpečnostní prohlídku osob, zavazadel a zásilek; Praha: Policejní akademie ČR, 1999
- ZEMANOVÁ, Š. a kolektiv: Lidská dimenze mezinárodní politiky. Praha: Vysoká škola ekonomická a Nakladatelství Oeconomica, 2004
- ZOUBEK, V.: Postmoderní problémy lidských práv a globální bezpečnosti. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2004

Dílčí články v časopisech a souborných dílech:

- ADÁMEK, L.: Má ochrana osobních údajů v policii šanci? Kriminalistický sborník 4/2004

- BARTOŇ, M.: Virtuální pornografie, limity svobody umělecké tvorby a svobody projevu a trestní zákon. Právní rozhledy 17/2008, s. 617
- BAYEROVÁ, M.: Evropská úmluva o počítačové kriminalitě a sexuální zneužívání dětí. Trestněprávní revue 5/2003, s. 156
- ČELIKOVSKÝ, J.: Schengenské acquis a Česká republika. In: časopis INTEGRACE, číslo 8/2001. Praha: Institut pro evropskou politiku EUROPEUM, 2001
- FRYŠTÁK, M.: Mezinárodní policejní spolupráce. Časopis Policista 4/2003
- FUČÍK, P. - ŠÍPEK, J.: Schengenský informační systém – technický pohled. In: časopis INTEGRACE, číslo 8/2001. Praha: Institut pro evropskou politiku EUROPEUM, 2001
- GŘIVNA, Tomáš; HERCZEG, Jiří. Právo na přístup k Internetu, blokace stránek a digitální gilotina. Trestněprávní revue. 2010, roč. 9, č. 05, s. 144. ISSN 1213-5313
- HAJN, P.: Reklama a nositelé veřejné autority II. Právo a podnikání, květen 2000, č. 6, s. 3
- HANSEL, M.: Problém kamerových systémů instalovaných zaměstnavatelem, Právo a podnikání č. 9/2003
- HERCZEG, J.: Případ Caroline von Hannover – zveřejnění fotografií ze soukromí prominentů. Právní rozhledy 23/2004
- HLAVÁČEK, J. a kol.: FODAGEN aneb Proč potřebujeme zkvalitnit evidenci pachatelů. Kriminalistický sborník, 2002
- HRDINA – HOŠTIČKA - MATES: Ochrana osobních údajů v obchodním rejstříku. Právní rádce 8/2003.
- JOUZA, L.: Ochrana soukromí na pracovišti. Právní rádce 5/2003
- KNAPP, V.: Člověk, občan a právo. Právník č. 1/1992
- KOKTAN, P.: Bezpečnost bank a peněžních ústavů, Praha: Kriminalistický sborník č. 9, 1992
- LAUBY, M.: Forenzní genetická analýza DNA a její význam při dokazování. Bulletin advokacie č. 4/2002
- MAŠTALKA, J.: Ochrana osobních údajů, Právní rádce 7/1999, str. 23 – 24

- MAŠTALKA, J. - MĚSÍČEK, J.: Právní úprava zpracování osobních údajů v působnosti Policie české republiky. Kriminalistický sborník 4/2004
- MAŠTALKA, J.: Návrh nového občanského zákoníku z pohledu ochrany soukromí a osobních údajů, Právní rozhledy 10/2010
- MATEJKA, J.: K oprávnění zaměstnavatele kontrolovat práci zaměstnance pomocí moderních technologií, Právo a zaměstnání č. 5/2003, s. 7
- MATES, P.: ÚS k ochraně soukromí veřejně činných osob. Právní zpravodaj 12/2007
- MUSIL, J.: Ochrana osobních dat a kriminalistický informační systém, Praha: Československá kriminalistika č. 1, 24, 1991
- MUSIL, J.: Porušuje ukázání fotografií nezúčastněných osob při rekognici právo na ochranu osobnosti?. Trestní právo č. 7-8/2000, s. 31-35
- ONDRUŠ, R.: Kamerové systémy v praxi obecní policie, Správní právo 5-6/2004
- POREMSKÁ, M.: Pornografie v USA. Trestněprávní revue 8/2008, s. 233
- PUŽMANOVÁ, R.: Biometrické systémy v praxi. In: časopis IT Systems, číslo 3/2004. Praha: CCB, s.r.o., 2004
- REPÍK, B.: Odposlech telefonu. Právní fórum 4/2004, Příloha, s. 61
- RŮŽIČKA, M.: Operativně pátrací prostředky. Právní rádce 11/2001
- ŘÍHA, Z.: Elektronické pasy. In: Zpravodaj ÚVT MU. ISSN 1212-0901, 2006, roč. XVII, č. 1, s. 7-12.
- SELTENREICH, R.: Právo na soukromí v kontextu ústavního vývoje USA, Právník 1/2000, str. 23 – 26
- SKÁLA, J.: Právní ochrana osobních údajů v informačních systémech, Právník 1/1994, str. 22 a následující
- SMEJKAL, V.: Počítačová a internetová kriminalita v České republice. Právní rozhledy, 1999, č. 12
- SMEJKAL, V.: Kriminalita v prostředí informačních systémů a rekodifikace trestního zákoníku. Trestněprávní revue, II., 2003.

- SOKOL, T., SMEJKAL, V.: Postih počítačové kriminality podle nového trestního zákona. Právní rádce 7/2009, s. 43.
- SOUČEK, J. – ŠKRABALOVÁ, P.: Odposlech a záznam telekomunikačního provozu z pohledu de lege lata i de lege merenda. Trestní právo 4/2002.
- STRAUS, J.: Příspěvek k identifikaci objektů a systémů v kriminalistice. Časopis Kriminalista č. 2/2005
- SVATOŠOVÁ, H.: Databanky v bankách opět v ústavních mezích. Právní fórum 5/2004
- ŠEVČÍK, V.: Některé ústavní aspekty odposlechu a záznamu telekomunikačního provozu, Bulletin advokacie č. 6-7/1996. Praha: ČAK, 1996
- ŠIMÁČKOVÁ, K.: Myšlenky o rozšíření subjektů přirozených práv v České republice. In: DANČÁK, B. – ŠIMÍČEK, V. (Eds.): Deset let listiny základních práv a svobod v právním řádu České republiky a Slovenské republiky. Masarykova univerzita v Brně a Mezinárodní politologický ústav, 2001
- ŠIMKOVÁ, R: Legislativní problémy národní databáze DNA. Kriminalista 3/2003
- ŠLOSARČÍK, I.: Schengen: návod k použití. In: časopis INTEGRACE, číslo 8/2001. Praha: Institut pro evropskou politiku EUROPEUM, 2001
- ŠTEFKO, M.: K problému sledování vlastních zaměstnanců, Právo a zaměstnání č. 1/2005, str. 7 až 11
- ŠTEFKO, M.: Může zaměstnavatel sledovat své zaměstnance?, Národní pojištění č. 12/2004, s. 5
- TELEC, I.: Svolení, nebo zákonné licence v právu osobnostním, Právní rozhledy 24/2007
- TELEC, I.: Osobnostní práva a rekodifikace českého obecného soukromého práva. Právní praxe 1-2/2001. s. 110-111
- VANČO, E.: Biometrie, biometrika - geneze, vývoj a současné pojetí. Časopis Kriminalista č. 1/2005

- VANTUCH, P.: K možnosti využití odposlechů a záznamů telekomunikačního provozu jako důkazu ve věci. Bulletin advokacie č. 11-12/2005
- VANTUCH, P.: Kdy lze užít odposlech telekomunikačního provozu jako důkaz proti obviněnému. Bulletin advokacie č. 11-12/2006. Str. 48-56
- VANTUCH, P.: Národní databáze DNA a odběr biologického materiálu obviněným. Trestněprávní revue č. 1/2004
- VANTUCH, P.: Nové možnosti odběru DNA. Právní rádce – měsíčník Hospodářských novin, č. 6/2006.

Cizojazyčná díla:

- BELLIA – BERMAN – POST: Cyberlaw – Problems of policy and jurisprudence in the Information age. USA: WEST GROUP, 2003
- BRANDEIS, L. – WARREN, S.: The Right to Privacy. In: 4 HARVARD LAW REVIEW 193-220 (1890-91), VOL. IV, December 15, 1890, No. 5. USA, Cambridge, MA. ISSN: 0017-811X
- COOLBRIDGE, T.: Kyllo v. United States: Technology Versus Individual Privacy - Fourth Amendment case. In: FBI Law Enforcement Bulletin – October 2001. Washington: Federal Bureau of Investigation, 2001. ISSN-0014-5688
- DRGONEC, J.: Právo na súkromie a pravomoc súdných orgánov pro jeho ochrane. Bulletin slovenskej advokacie, 1995, č. 1, s. 26
- DRGONEC, J.: Právo na súkromie podľa Ústavy Slovenskej republiky. Časopis pro právní vědu a praxi č. 2/2000, s. 203-212
- DRGONEC, J.: Ústavoprávné aspekty použitia sledovacích technológií mocenskými zložkami štátu. In: DANČÁK, B. – ŠIMÍČEK, V. (Eds.): Bezpečnost České republiky – Právní aspekty situace po 11. září 2001. Sborník z konference. Brno: Masarykova univerzita v Brně, Mezinárodní politologický ústav, 2002
- ETZIONI, A.: The Limits of Privacy. USA: Basic Books, 1999

- HOFFER, S.: World Cybespace Law. USA: JURIS PUBLISHING, INC., 1999. ISBN: 1-57823-072-1
- CHASE, H.W. – DUCAT, C.R.: Edward S. Corwin's The Constitution and What it means today. 14th edition. Princeton University Press, 1978
- LETOWSKA, E.: Liberal concept of human rights in Central and Eastern Europe. Warsaw, 1998
- STREET, F. L.: Law of the Internet. Charlottesville, VA: LEXIS LAW PUBLISHING, 1998. ISBN: 0-327-00856-3
- SVÁK, J.: Zásady a tendencie v ochrane práva na súkromie. Justičná revue č. 11/2000, s. 1199

Webové zdroje, včetně cizojazyčných:

- AUJEZDSKÝ, J.: Skutečně může zaměstnavatel číst Vaší poštu? In: IT Právo – server o internetovém a počítačovém právu. [online]. Praha: Společnost pro právo informačních technologií (SPIT), 2004, ISSN: 1801 4089 Dostupný z www: http://www.itpravo.cz/index.shtml?x=160355 [cit. 2012-02-18].
- BENTHAM, J.: The Panopticon Writings. Ed. Miran Bozovic (London: Verso, 1995). Dostupné i online na: http://cartome.org/panopticon2.htm [cit. 2012-02-18].
- BITTO, O.: Pohodlí si ceníme více než soukromí. In: server Živě.cz – o počítačích a Internetu. [online]. Praha: Computer Press, a. s., 2006, ISSN 1214-1887. Dostupný z www: http://www.zive.cz/h/Uzivatel/AR.asp?ARI=129321&CAI=2114 [cit. 2012-02-18].
- BORGULA, A: Zveřejňování záznamů z městských kamerových systémů. Dostupné online na: http://aplikace.mvcr.cz/archiv2008/ministerstvo/opk/servis/leden07.pdf [cit. 2012-01-23]
- HRUBEŠOVÁ, H.: USA - Cenzura na Internetu. . In: IT Právo – server o internetovém a počítačovém právu. [online]. Praha: Společnost pro

právo informačních technologií (SPIT), 2006, ISSN: 1801 4089. Dostupný z www: http://www.itpravo.cz/index.shtml?x=1940902 [cit. 2012-02-18].

- IURIDICUM REMEDIUM: Doporučení Výboru pro občanská a politická práva ohledně provozu kamerových systémů. [online] Praha: Iuridicum remedium, o.s. Dostupné z www: http://www.iure.org/539454 [cit. 2012-02-18].
- IURIDICUM REMEDIUM: Big brother awards: Nové technologie. [online] Praha: Iuridicum remedium, o.s. Dostupné z www: http://www.bigbrotherawards.cz/nove_technologie.html [cit. 2012-02-18].
- JACYSZYN, V.: Od Nipkowa k druhé světové válce, aneb počátky televize. Dostupné online na: http://tele.tym.cz/zajimavosti/pocatky_tv/pocatky_tv.htm [cit. 2012-01-21]
- JAPPEL, C.: Pouliční kamery sledují každý náš krok. Jak fungují? Magazín Idnes [online]. Praha**:** MAFRA, a.s., 2005 [cit. 2012-02-18]. Dostupný z www: http://technet.idnes.cz/tec_technika.asp?r=tec_checktech&c=A051129_192229_tec_checktech_cti [cit. 2012-01-21]
- KRULÍK, O.: Zákon o sjednocení a posílení Ameriky za použití vhodných nástrojů požadovaných k předcházení a čelení terorismu („Vlastenecký zákon), zveřejněný na internetových stránkách Ministerstva vnitra ČR [cit. 2012-02-18]: http://aplikace.mvcr.cz/archiv2008/rs_atlantic/data/files/vlastzak.pdf
- LUNDMARK, T.: Princess Caroline in Bismark's Shadow: Photographs of Public Figures in German Law. Dostupné online na http://jurist.law.pitt.edu/world/gercor2.htm [cit. 2012-01-26]
- MAREK, M: Monitorování elektronické pošty a ochrany soukromí zaměstnanců v souvislosti se Stanoviskem Úřadu pro ochranu osobních údajů k této otázce. In: IT Právo – server o internetovém a počítačovém právu. [online]. Praha: Společnost pro právo informačních technologií

(SPIT), 2003, ISSN: 1801 4089. Dostupný z www: http://www.itpravo.cz/index.shtml?x=132240 [cit. 2012-02-18].

- MATEJKA, J.: Ochrana soukromí na pracovišti dle zákona č. 262/2006 Sb., In: IT Právo – server o internetovém a počítačovém právu. [online]. Praha: Společnost pro právo informačních technologií (SPIT), 2006, ISSN: 1801 4089. Dostupný z www: http://www.itpravo.cz/index.shtml?x=1919872 [cit. 2012-02-18].
- MATEJKA, J.: Odposlech a záznam telekomunikačního provozu, I. a II. díl. In: IT Právo – server o internetovém a počítačovém právu. [online]. Praha: Společnost pro právo informačních technologií (SPIT), 2003, ISSN: 1801 4089. Dostupný z www: http://www.itpravo.cz/index.shtml?x=129172 [cit. 2012-02-18].
- MOKRÝ, L.: Evropský právní rámec ochrany osobních údajů a soukromí v e-mailové komunikaci. In: Právo IT [online]. Praha: European Association For Commercial And Corporate Law, 2006. Dostupný z www: http://www.pravoit.cz/view.php?nazevclanku=evropsky-pravni-ramec-ochrany-osobnich-udaju-a-soukromi-v-e-mailove-komunikaci&cisloclanku=2006050001 [cit. 2012-02-18].
- POTMĚŠIL, J.: Použitelnost zvukových a obrazových záznamů jako důkazu. Dostupné online na http://www.mvcr.cz/soubor/spravni-pravo-3-10web-potmesil-pdf.aspx [cit.2011-11-18].
- SADECKÝ, Z.: Zamyšlení nad uplatněním UAV v bezpečnostní praxi. Dostupné online na http://www.uav.estranky.cz/clanky/autorovy-prispevky/zamysleni-nad-uplatnenim-uav-v-bezpecnostni-praxi.html [cit.2012-01-29].
- SEIDEL, J.: Protiprávně získané nebo použité důkazy v civilním soudním řízení. Dostupné online na https://is.muni.cz/www/210560/pfo-nd.pdf [cit. 2012-02-13].
- SLONECKER – SHAW – LILLESAND: Emerging Legal and Ethical Issues in Advanced Remote Sensing Technology. In: Photogrammetric Enginneering Remote Sensing. Ročník 64, č.6 (1998), s.589-595 nebo online na:

http://ibis.geog.ubc.ca/courses/geob373/lectures/Handouts/PERS_Remote_Sensing_Ethics.pdf [cit.2012-01-29].

- SOKOL, T.: Identifikace osob pomocí analýzy DNA. In: Právní rádce Ihned.cz [online]. Praha: Economia, 2002, ISSN 1213-7693. Dostupný z www: http://pravniradce.ihned.cz/3-11549730-identifikace+osob-F00000_d-b9 [cit. 2012-02-18].
- SOKOL, T.: Odposlech. In: Měsíčník Právní rádce internetového serveru Ihned.cz (www.ihned.cz) [online]. 26.1.2005. Praha: Economia, 2005, ISSN 1213-7693 [cit. 2012-02-18]. Dostupný z www: http://pravniradce.ihned.cz/3-15548090-odposlech-F00000_d-70
- ŠTECHA, P.: Inventura dokumentaristických projektů – víra v pravdivost fotografie. Dostupné na: http://www.paladix.cz/clanky/inventura-dokumentaristickych-projektu-vira-vnbsppravdivost-fotografie.html [cit. 2012-01-26]
- ŠTĚDROŇ, B.: Kontrola práce zaměstnanců pomocí telekomunikační techniky z pohledu švýcarského práva. In: IT Právo – server o internetovém a počítačovém právu. [online]. Praha: Společnost pro právo informačních technologií (SPIT), 2005, ISSN: 1801 4089. Dostupný z www: http://www.itpravo.cz/index.shtml?x=261542 [cit. 2012-01-26]
- ŠTĚDROŇ, B.: Německo: Využívání internetu pro soukromé potřeby v práci může vést k okamžitému ukončení pracovního poměru. In: IT Právo – server o internetovém a počítačovém právu. [online]. Praha: Společnost pro právo informačních technologií (SPIT), 2005, ISSN: 1801 4089. Dostupný z www: http://www.itpravo.cz/index.shtml?x=315830 [cit. 2012-02-18].
- Úřad pro ochranu osobních údajů: Zásady provozování kamerového systému z hlediska zákona o ochraně osobních údajů – stanovisko č. 1/2006 Úřadu pro ochranu osobních údajů. [online] Praha: ÚOOÚ, 2006 [cit. 2012-02-18]. Dostupné z www: http://www.uoou.cz/stanovisko_2006_1.pdf (www.uoou.cz)

- Úřad pro ochranu osobních údajů: Jaké jsou povinnosti správců provádějících zpracování osobních údajů pomocí kamerových systémů? Sekce Poradna: Často kladené otázky. [online] Praha: ÚOOÚ, 2006 [cit. 2012-02-18]. Dostupné z www: http://www.uoou.cz/index.php?l=cz&m=bottom&mid=01:15&u1=&u2=&t=#a4
- Úřad pro ochranu osobních údajů: Monitorování elektronické pošty a ochrana soukromí a osobních údajů zaměstnanců. Úřad pro ochranu osobních údajů k problémům z praxe - č. 1/2003. [online] Praha: ÚOOÚ, 2003. Dostupné z www: http://www.uoou.cz/index.php?l=cz&m=top&mid=02:02:15&u1=&u2=&t= [cit. 2012-02-18].
- Úřad pro ochranu osobních údajů: Vyjádrení a doporucení ÚOOÚ k možnosti instalovat kamerový systém v prostorách školy. Dostupné z www: http://www.uoou.cz/files/vyjadreni_a_doporuceni_uoou.pdf [cit. 2012-02-18].
- VRŠEK, P.: Moderní databázové systémy a ochrana osobních údajů. In: IT Právo – server o internetovém a počítačovém právu. [online]. Praha: Společnost pro právo informačních technologií (SPIT), 2002, ISSN: 1801 4089 [cit. 2012-02-18]. Dostupný z www: http://www.itpravo.cz/index.shtml?x=63674
- Wikipedie: Otevřená encyklopedie: Soukromí [online]. c2005 [cit. 2012-02-18]. Dostupný z WWW: http://cs.wikipedia.org/w/index.php?title=Soukrom%C3%AD&oldid=232952
- ZAJÍČEK, L.: Odposlechy teroristy neodhalí. In**:** Lupa.cz (www.lupa.cz), server o českém Internetu [online]. Praha: Internet Info, s.r.o., 2001, ISSN 1213-0702 [cit. 2012-02-18]. Dostupný z www: http://www.lupa.cz/clanky/odposlechy-teroristy-neodhali/
- ZEMAN, P: Zpravodajské služby ČR, jejich právní postavení a vývoj. In: Bulletin Analýzy & studie. Praha: Centrum strategických studií,

2002-2006. ISSN 1214-8393. [online]. Dostupné na: http://www.strat.cz/bulletin/page.php?id=217 [cit. 2012-02-18].

Další webové zdroje

- Projekt JPD2 - Městský kamerový systém hlavního města Prahy. Dostupné online na: http://www.praha.eu/jnp/cz/home/magistrat/odbory_mhmp/dopravy/projekty_jpd2/projekt_jpd2_mestsky_kamerovy_system.html [cit. 2012-01-23]
- Městský kamerový systém. Dostupné online na: http://www.praha.eu/jnp/cz/home/magistrat/odbory_mhmp/krizoveho_rizeni/krizove_rizeni/mestsky_kamerovy_system.html [cit. 2012-01-23]
- Studie „Bezpečné město Praha 13“. AB via s.r.o. Dostupné na webu internetového deníku Česká pozice online na http://www.ceskapozice.cz/sites/default/files/bezpecna_praha13_-_studie_v11_2011.pdf [cit. 2012-01-23].
- Úsekové měření rychlosti v Rakousku. Dostupné online na: http://www.osbid.org/index.php?t=article&n=clanek-usekove-mereni-rychlosti-v-rakousku--53 [cit. 2012-02-13]
- Rakouský ústavní soud: úsekové měření rychlosti je nezákonné. Dostupné online na: http://vseorakousku.cz/titulni_strana/novinky/rakousky_ustavni_soud_usekove_mereni_rychlosti_je_nezakonne/ [cit. 2012-02-13].
- IDNES.CZ: Jak Velký bratr zatkl Pitra, pomohly mýtné brány i Skype. Dostupné online na: http://technet.idnes.cz/jak-velky-bratr-zatkl-pitra-pomohly-mytne-brany-i-skype-pjk-/tec_technika.aspx?c=A100813_101728_tec_technika_vse [cit. 2012-02-13].
- IDNES.CZ: Europol rozbil patrně největší pedofilní síť na internetu. Dostupné online na:

http://zpravy.idnes.cz/europol-rozbil-patrne-nejvetsi-pedofilni-sit-na-internetu-po1-/zahranicni.aspx?c=A110316_161013_zahranicni_abR [cit. 2012-02-13]

- IDNES.CZ: Ředitel základních škol dostal za držení dětského porna podmínku. Dostupné online na: http://zpravy.idnes.cz/reditel-zakladnich-skol-dostal-za-drzeni-detskeho-porna-podminku-pyl-/krimi.aspx?c=A100323_113542_krimi_cen [cit. 2012-02-13]
- IDNES.CZ: Policisté zadrželi sedm Čechů a tři Poláky šířící dětskou pornografii. Dostupné online na: http://zpravy.idnes.cz/policiste-zadrzeli-sedm-cechu-a-tri-polaky-sirici-detskou-pornografii-1zg-/krimi.aspx?c=A111205_173125_krimi_brd [cit. 2012-02-13]
- IDNES.CZ: Děti na internetu riskují, své fotky posílají pedofilům za kredit do mobilu. Dostupné online na: http://zpravy.idnes.cz/deti-na-internetu-riskuji-sve-fotky-posilaji-pedofilum-za-kredit-do-mobilu-1ul-/domaci.aspx?c=A091122_195910_domaci_vel [cit. 2012-02-13]
- Sdělení Komise Evropských společenství č. KOM (2006) 688 ze dne 15.11.2006 nazvaném Boj proti spamu a špionážnímu („spyware“) a škodlivému software („malicious software“). Dokument je dostupný např. z www: http://europa.eu/legislation_summaries/information_society/internet/l24189a_en.htm [cit. 2011-11-05]
- Vesecká vrátila policii případ Fondu ohrožených dětí. Dostupné online na: http://domaci.eurozpravy.cz/kauzy/15124-vesecka-vratila-policii-pripad-fondu-ohrozenych-deti/ [cit. 2012-01-26]
- stanovisko Veřejného ochránce práv „Veřejné inzerování dětí pro náhradní rodinnou péči je nepřípustné“ dostupné online na http://www.ochrance.cz/tiskove-zpravy/tiskove-zpravy-2012/verejne-inzerovani-deti-pro-nahradni-rodinnou-peci-je-nepripustne/ [cit. 2012-01-26]
- Stanovisko Ministerstva práce a sociálních věcí ve věci oprávnění subjektů provádějících zprostředkování náhradní rodinné péče a osob

pověřených k výkonu sociálně-právní ochrany dětízveřejňovat osobní údaje dětí. Dostupné online na: http://www.mpsv.cz/files/clanky/10285/Stanovisko_MPSV-osobni_udaje_deti.pdf [cit. 2012-01-26]

- 84 % aktivních uživatelů v Česku si prohlíží online video. Dostupné online na: http://www.lupa.cz/clanky/aktivni-uzivatele-v-cesku-sleduji-online-video/ [cit. 2012-02-15].
- Studie Online as soon as it happens. Dostupné online na: http://www.enisa.europa.eu/act/ar/deliverables/2010/onlineasithappens [cit. 2012-02-15].
- Digitální agenda: Podle průzkumu používají sociální sítě čím dál mladší děti a mnohé si nejsou vědomy rizik v oblasti ochrany soukromí. Dostupné online na: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/479&format=HTML&aged=1&language=CS&guiLanguage=en [cit. 2012-02-15].
- Tisková zpráva společnosti Microsoft ze dne 9.2.2010: Polovina dětí reaguje na internetu na zprávy od cizích lidí – ze zvědavosti. Dostupné online na: http://www.microsoft.com/cze/presspass/msg/20100209_news1.mspx [cit. 2012-02-15].
- Opinion 5/2009 „on online social networking“. Dostupné online na: http://www.scribd.com/doc/16736099/ARTICLE-29-DATA-PROTECTION-WORKING-PARTY-Opinion-52009-on-online-social-networking [cit. 2011-11-05].
- The Socialbot Network: When Bots Socialize for Fame and Money. Dostupné online na: http://lersse-dl.ece.ubc.ca/record/264/files/ACSAC_2011.pdf?version=1 [cit. 2011-11-05].
- Facebook's Eroding Privacy Policy: A Timeline. Dostupné online na https://www.eff.org/deeplinks/2010/04/facebook-timeline [cit. 2011-11-05].

- REPORT OF FINDINGS INTO THE COMPLAINT FILED BY THE CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC (CIPPIC) against FACEBOOK INC. Dostupné online na http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.pdf [cit. 2011-11-05].
- IDNES.CZ: Facebook čeká 20 let auditů kvůli špatné ochraně soukromí uživatelů. Dostupné online na http://tech.ihned.cz/c1-54053250-facebook-ceka-20-let-auditu-kvuli-spatne-ochrane-soukromi-uzivatelu [cit. 2012-02-15].
- Pillaged MySpace Photos Show Up in Massive BitTorrent Download. Dostupné online na http://www.wired.com/politics/security/news/2008/01/myspace_torrent [cit. 2012-02-15].
- Fotoalba na Internetu vás mohou připravit o vaše práva. Dostupné online na http://www.lupa.cz/clanky/fotoalba-na-internetu-vas-mohou-pripravit-o-prava/ [cit. 2012-02-15].
- Hacker stáhl tisíce intimních fotek ze seznamky Líbímseti.cz. Článek na serveru Živě.cz, dostupný online na: http://www.zive.cz/bleskovky/hacker-stahl-tisice-intimnich-fotek-ze-seznamky-libimseticz/sc-4-a-144169/default.aspx [cit. 2012-02-15].
- IDNES.CZ: Nový nepřítel Pentagonu. Chytré mobily vojáků v bojových operacích. Dostupné online na http://zpravy.idnes.cz/novy-nepritel-pentagonu-chytre-mobily-vojaku-v-bojovych-operacich-1fz-/zpr_nato.aspx?c=A110118_174514_zpr_nato_inc [cit. 2012-02-15].
- Google Street View zachoval města před zemětřesením. Dostupné online na http://navigovat.mobilmania.cz/Bleskovky/AR.asp?ARI=114226 [cit. 2012-02-15].
- Blurred Out: 51 Things You Aren't Allowed to See on Google Maps, dostupné v anglickém jazyce online na:

http://www.itsecurity.com/features/51-things-not-on-google-maps-071508/ [cit. 2012-02-15].

- Google wardriving? A co má vlastně být? Dostupné online na: http://www.lupa.cz/clanky/google-wardriving-a-co-ma-vlastne-byt/ [cit. 2012-02-15].
- IDNES.CZ: Přichází Kopernikus: vesmírný systém, který bude hlídat kontinent. Dostupné online na: http://zpravy.idnes.cz/prichazi-kopernikus-vesmirny-system-ktery-bude-hlidat-kontinent-p9y-/zahranicni.aspx?c=A080922_112350_zahranicni_jba [cit. 2012-02-15].
- Projekt Kopernikus není Velký bratr, říká OndřejMirovský. Dostupný online na http://www.ceskatelevize.cz/ct24/exkluzivne-na-ct24/osobnosti-na-ct24/30202-projekt-kopernikus-neni-velky-bratr-rika-ondrej-mirovsky/
- Kopernikus: observing our planet for a safer Word – dostupné online na: http://ec.europa.eu/enterprise/magazine/articles/competitiveness-energy-environment/article_7096_en.htm [cit. 2012-02-15]
- Bezpilotní letouny už v Americe špehují i nad městy. Dostupné na serveru E15 online: http://magazin.e15.cz/veda-a-technika/bezpilotni-letouny-uz-v-americe-spehuji-i-nad-mesty-725778 [cit.2012-01-29].
- Policejní bezpilotní letoun přečte značku auta z 200metrové výšky. Dostupné online na http://www.ceskatelevize.cz/ct24/svet/161922-policejni-bezpilotni-letoun-precte-znacku-auta-z-200metrove-vysky/
- Aktivisté sledují japonské velrybáře za pomoci bezpilotních letounů. Dostupné online na http://www.ceskatelevize.cz/ct24/svet/158171-aktiviste-sleduji-japonske-velrybare-za-pomoci-bezpilotnich-letounu/?mobileRedirect=off [cit.2012-01-29].
- Letištní rentgen v USA svléká cestující do naha. Dostupné online na: http://digiweb.ihned.cz/c1-19966800-letistni-rentgen-v-usa-svleka-cestujici-donaha [cit.2012-01-29].

- Ochrana letectví: Komise přijímá nová pravidla o používání bezpečnostních skenerů na evropských letištích. Dostupné online na: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/1343 [cit.2012-01-29].
- WELCH, A.: Full-Body Scanners: Full Protection from Terrorist Attacks or Full-On Violation of the Constitution? Dostupné online na: http://law.du.edu/documents/transportation-law-journal/past-issues/v37-03/Welch- Body-Scanners.pdf [cit.2012-01-29]
- Cestovní doklady s biometrickými prvky (CDBP). Dostupné online na: http://aplikace.mvcr.cz/archiv2008/rady/faq/biometrika.html [cit.2012-01-29]
- Biometrika. MVČR. Dostupné online na: http://www.mvcr.cz/clanek/biometrika.aspx [cit.2012-01-29].
- Biometrické pasy s čipem mohou být "klonovány". Dostupné online na http://hn.ihned.cz/c1-19036740-biometricke-pasy-s-cipem-mohou-byt-klonovany [cit.2012-01-29]
- Aktualizované stanovisko k provozování kamerových systémů obecní policií – právní stav ke dni 10. října 2011. Dostupné online: www.mvcr.cz/soubor/kamery-na-web-pdf.aspx [cit. 2012-01-23]
- Při řešení přestupků lze použít i kamery soukromých subjektů, řekl Nejvyšší správní soud. Dostupné na adrese: http://www.epravo.cz/zpravodajstvi/pri-reseni-prestupku-lze-pouzit-i-kamery-soukromych-subjektu-rekl-nejvyssi-spravni-soud-79621.html [cit.2012-02-13].
- Dopis organizace ACLU arizonským školským orgánům. Dostupný zde: http://www.aclu.org/technology-and-liberty/letter-arizona-school-officials-school-face-recognition [cit. 2012-01-21].
- Wall Street Journal: Cisco Poised to Help China Keep an Eye on its Citizens. Dostupný online v anglickém jazyce na: http://online.wsj.com/article/SB10001424052702304778304576377141077267316.html [cit. 2012-01-21].
- Arizona police deploy iris scanners and facial biometrics to identify inmates. Dostupné zde:

http://www.homelandsecuritynewswire.com/arizona-police-deploy-iris-scanners-and-facial-biometrics-identify-inmates [cit. 2012-01-21].

- Device Raises Fear of Facial Profiling. Dostupné zde: http://online.wsj.com/article/SB10001424052702303678704576440253307985070.html [cit. 2012-01-21].
- Amid Privacy Fears, Police Across the Nation Will Roll Out Face-Recognizing iPhone Tech This Year. Dostupné zde: http://www.popsci.com/technology/article/2011-07/amid-privacy-fears-police-across-nation-will-roll-out-face-recognizing-iphone-tech-year [cit. 2012-01-21].
- New Police Scanner Raises 'Facial Profiling' Concerns. Dostupné zde: http://www.npr.org/2011/08/11/138769662/new-police-scanner-raises-facial-profiling-concerns [cit. 2012-01-21].
- Kamerový systém. Wikipedie. Dostupné online na: http://cs.wikipedia.org/wiki/Kamerov%C3%BD_syst%C3%A9m [cit. 2012-01-21].
- Sdělení Evropské komise: Politika EU pro boj proti terorismu: Komise podává přehled hlavních úspěchů a dalších úkolů. Dostupné online na: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/987&format=HTML&aged=1&language=CS&guiLanguage=en [cit. 2012-01-21].
- Protokol o uplatňování Listiny základních práv Evropské unie v Polsku a ve Spojeném království, dostupný na stránkách Min. zahraničních věcí: http://www.mzv.cz/jnp/cz/zahranicni_vztahy/evropska_unie/pravo_evropske_unie/aktualni_novely_primarniho_prava_eu/lisabonska_smlouva/protokol_o_uplatnovani_listiny.html [cit. 2012-02-18].
- ZPRÁVA KOMISE RADĚ A EVROPSKÉMU PARLAMENTU - Hodnotící zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES) ze dne 18.4.2011 dostupná na: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:CS:PDF [cit. 2012-02-18].

- SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU, RADĚ, EVROPSKÉMU HOSPODÁŘSKÉMU A SOCIÁLNÍMU VÝBORU A VÝBORU REGIONŮ – Komplexní přístup k ochraně osobních údajů v Evropské unii, ze dne 4.11.2010 č. KOM(2010) 609. Dostupné online na: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_cs.pdf [cit. 2012-02-18].

ABSTRAKT DISERTAČNÍ PRÁCE

JUDr. Milan Chládek

Kamerové systémy a obrazové záznamy v právní ochraně soukromí

Tato disertační práce s názvem Kamerové systémy a obrazové záznamy v právní ochraně soukromí si klade za cíl základní rozbor a seznámení s danou, vysoce aktuální a v poslední době často diskutovanou problematikou. Oblast obrazového sledování je velmi zajímavým a z právního pohledu zatím ne příliš řešeným tématem. Právní věda a praxe řeší často případy dopadající do této problematiky tzv. za pochodu, často s aplikací norem obecnějšího charakteru a rozhodující (právo aplikující) orgány často právo dotváří, neboť zákonodárce s ohledem na vysokou aktuálnost a novost tématu ještě nebyl schopen postihnout veškeré možné situace. Práce se snaží pojmout téma poměrně široce, od obecného úvodu a tematického přehledu práva na soukromí nabízí nejprve konkrétní práci s obecnější tematikou práva na soukromí v kontextu obrazových záznamů, dále se zabývá detailněji kamerovými systémy a v poslední třetině práce se nabízí pohled na vysoce moderní technologie využití obrazového sledování a jiných metod využívajících obrazového záznamy a snímky v prostředí informačních technologií a dalších oblastí využití. Disertační práce je vedle nezbytného úvodu (kapitola 1), závěru (kapitola 7) a seznamu literatury (kapitola 8) členěna do pěti základních kapitol.

Kapitola 2 pojednává o obecném tématu ochrany soukromí spíše bez specifického a konkrétního akcentu na obrazové záznamy a kamerové systémy – v této kapitole je podán základní přehled institutu soukromí, práva na soukromí a jeho ochrany, a to v mezinárodním, evropském i národním měřítku.

Kapitola 3 již zpracovává téma obrazových záznamů a snímků, a to spíše z obecnějšího pohledu. Od historie uchovávání obrazu přechází k osobnostním právům podle v současné době platného a účinného

občanského zákoníku (zákon č. 40/1964 Sb.) a po popisu právní úpravy v již přijatém novém občanském zákoníku se dotýká okrajově i tematiky autorskoprávní ochrany obrazových záznamů. V druhé polovině této kapitoly je pak zmíněno využití obrazového sledování při práci bezpečnostních složek – Policie ČR, celních orgánů a zpravodajských služeb; v rámci exkurzu na konci kapitoly je krátce popsána situace vztahující se k ochraně soukromí a obrazovému sledování na Slovensku. Kapitola 3 také zpracovává možnosti použití obrazových záznamů (videí a fotografií) v rámci dokazování, a to jak v trestním, civilním, ale i správním řízení. V poslední době bylo toto téma samozřejmě jako téma vysoce aktuální mnohokrát řešeno, prozatím ne se zcela jasným a definitivním závěrem.

Pokud jde o kapitolu 4, ta se snaží rozebrat tematiku kamerových systémů co nejpodrobnějším způsobem. Tato kapitola podává přehled všech základních známých oblastí využití kamerových systémů, nejprve zmiňuje využití kamerových systémů povolených zákonem a dále kamerových systémů využívaných ze strany veřejné moci – státní a obecní policií, posléze je probíráno téma obrazového sledování na pracovišti. Konečně jsou popsány i další možnosti využití – v dětských domovech, ve zdravotnictví atd. Tato kapitola je jednou ze stěžejních kapitol práce, kamery a kamerové systémy jsou v dnešní době používány nejrůznějšími veřejnoprávními i soukromými subjekty, a to v míře někdy až zarážející – práce se tak nutně na dané téma zaměřuje a zmiňuje i možná rizika a potenciální hrozby masivního užívání kamerových systémů.

Kapitola 5, nazvaná Obrazové záznamy a informační technologie, popisuje širokou škálu možností využívání obrazových záznamů v prostředí informačních technologií, zejména v prostředí Internetu a v rámci sociálních sítí. Informační technologie přináší vedle svých nesporných pozitiv i rizika zneužití, která se disertační práce snaží pojmenovat. Běžní uživatelé informačních technologií zpravidla nevěnují příliš pozornosti ochraně svého soukromí a právě obrazové záznamy bývají často terčem zásahů a právo na soukromí jednotlivců je v tomto potenciálně velmi rizikovém prostředí moderních technologií, jako je Internet, moderní telefony a tablety, často ohroženo či porušeno. Existuje i řada nových způsobů nelegálního chování

spojených s problematikou informačních technologií, které dříve nebyly známy, jako je kyberstalking, happy slapping, kyberšikana atd. Problematika těchto modelových směrů chování a užívání nových termínů je vysoce aktuální, právem a právní vědou zatím nepříliš uchopená.

Kapitola 6 je zaměřena na obrazové sledování a snímkování zemského povrchu, zmiňuje kupříkladu diskutabilní zavedení a využití systému Google StreetView, satelitní mapy, bezpilotní sledování povrchu zejména ze strany policejního orgánů, letištní skannery a další témata.

Každé téma se snaží disertační práce alespoň základně pojmenovat a specifikovat, uvést, pokud je to možné relevantní judikaturu nebo odborné a zpravodajské články k danému tématu a podat tak téma v širším pojetí. Poslední dvě kapitoly (kapitola 5 a kapitola 6) jsou tematicky zaměřeny na nejnovější oblasti využití obrazového sledování a použití obrazových záznamů, to vše v kontextu rozvoje moderních technologií. Ještě před několika málo desetiletími nebyla řada modelových situací a možností využití obrazového sledování a využívání obrazových informací vůbec technicky známa, natož aby byla podchycena i z právního hlediska. Právo samozřejmě nestačí pružně a aktuálně reagovat bez prodlevy na tyto rychlé změny způsobené technickým pokrokem, právní úprava a vůbec zakotvení nových technologických možností a jejich konsekvencí tak přichází až se zpožděním. Disertační práce se snaží poukázat na všechny souvislosti, i na rizika s využíváním nových technologií spojená.

Disertační práce svým rozsahem zpracovávané tematiky spadá vedle základní oblasti občanského práva i do oblasti práva ústavního, trestního, práva pracovního a práva správního. Práce se snaží nabídnout alespoň rámcový přehled celé problematiky, úmyslně není řešena oblast pouze práva občanského.

DISSERTATION ABSTRACT

JUDr. Milan Chládek

Camera systems and video records in legal protection of privacy

The main goal of this dissertation named Camera systems and video records in legal protection of privacy is the basic analysis and familiarization with the highest actual and in the recent time wide-discussed problems. The field of the video surveillance is highly interesting and for the time being by the law science not solved topic. The legal science and practice solve problem belongs to this problematic area often as you go along, often by the aplication of the more generic rules and therefore the deciding authorities often make the law complete by theirselves because the legislator was not able to cover all the possible situations – just because of high actuality and novelty of this topic. This work tries to cover the topis by the relative wide way, from the generic introduction and tematic survey of the right to privacy offers first the concrete work with generic topic of right to privacy in relation to the video records, further focusing on camera systems and the last third of the work focuses on highly modern technologies of using video surveillance and on other methods using video records and snapshots in the area of informatic technologies and further areas of the use. The dissertation is divided among the Introduction (Chapter 1), Conclusion (Chapter 7) and list of the bibliography (Chapter 8) into five basic chapters.

The Chapter 2 discusses the general topic of the protection of the privacy rather without specific and concrete accent on video records and camera systems – there is the basic survey of the legal institute of the privacy, right to the privacy and its protection in this chapter, namely in international, European and national scale.

Chapter 3 deals with the topic of the video records and snapshots, from the general point of view – from the history of keeping of the image turns to the personal rights according to the valid Civil Code (Act Nr. 40/1964 Coll.) and after description of the legal conception ivolved in the

new civil code deals also in peripheral way with the copyright protection of the video records. In the second half of this charter there is the description of the using the video surveillance during the work of the security bodies – by the Police, by customs authorities and intelligence bodies; there is the short description of the situation regarding the protection of the privacy and of the video surveillance within the Slovak republik at the end of the chapter. The Chapter 3 describe also the possibilities of use of the video records (videos and photograps) within the use of proofs of evidence – within the penal, civil and within the administrative proceedings as well. This theme has been often discussed, although not with the clear and definitive conclusion so far.

As for the Chapter 4 – this charter tries to describe the topic of the camera systems by the very detailed way. This chapter offers the survey of the all basic and known fields of use of camera systems, first the use of the camera systems permitted by the law is described, then the camera systems used by the public authorities, later the topic of the video surveillance on the workplace is discussed. Finally, the further possibilities of the use of camera systems are described – use in children‘s homes, in healthcare etc. This chapter is one of the main chapters of the dissertation, cameras and camera systems are used in recent time by the various public and private subjects, in very startling and extended way – it is the reason why the dissertation focus on this topic and also the risk and potential threats of massive use of camera systems is mentioned.

Chapter 5, named Video records and information technologies, describes the wide scale of the possibilites of the camera records‘ use within the field of informatic technologies, namely on Internet and within the social media networks. The information technologies bring among the positive effect also the risk of the misuse, to which this dissertation tries to point out. The common users of the information technologies usually does not pay big attention to the protection of their privacy and namely the video records are often subject of the threats and attacks and the right to privacy of the individuals is often threatened in this potentially dangerous environment of the modern technologies as Internet or modern smart cell phones and tablets are. There is also the high number of new models of illegal behaviour

related to the problematics of the informatic technologies, which were not known in the past, such as cyberstalking, happy slapping, cyber bullying etc. These model ways of the behaviour and using of the new terms is highly actual, by the law and legal science not touched so far.

Chapter 6 focuses on the video surveillance and monitoring of the earth surface, this chapter mentions for instance the problematic introduction and the use of the Google StreetView system, the satelite maps, unmanned aerial surveillance of the surface (namely by the police authorities), airport scanners and other topics.

The dissertation tries to name and specify every single theme and problem, at least via basic way, the dissertation tries to point out on the relevant judicature or expert opinions and news articles on the relevant topic and refers to the topic in general and broad approach. Last two chapters (chapter 5 and chapter 6) are tematically focused on the newest fields of the use of the video surveillance and use of the video records, namely in relation to the development of the modern technologies. Numbers of model stuations and possibilities of the video surveillance has not been known at all, let alone describe by the legal science and by the law. The law can not of course flexibly react without delay on the quick changes caused by the technical development; so that the legal enactement comes logically with some delay. The dissertation tries to point out to all the consequences, also on the risks connected with the use of the modern technologies.

The dissertation belongs by the extent of the themes among the basic field of the civil law also to the field of the constitutional law, penal law, labour law and administrative law. The work tries to offer at least the basic survey of the issues, the dissertation is focused intentionally not only on the field of the civil law.

Kamerové systémy a obrazové záznamy v právní ochraně soukromí

Camera systems and video records in legal protection of privacy

Klíčová slova disertační práce:

Kamerové systémy, ochrana soukromí, obrazové záznamy

Keywords of the dissertation:

Camera systems, protection of the privacy, video records