UNIVERZITA JANA AMOSE KOMENSKÉHO PRAHA

BAKALÁŘSKÉ KOMBINOVANÉ STUDIUM

2016-2017

BAKALÁŘSKÁ PRÁCE

Břetislav Šmejkal

Ochrana osob a ochrana osobních údajů osob

Praha 2017

Vedoucí bakalářské práce: Ing. Michaela Melicharová

JAN AMOS KOMENSKY UNIVERSITY PRAGUE

BACHELOR COMBINED STUDIES

2016-2017

BACHELOR THESIS

Břetislav Šmejkal

Protecting people and protection of individuals' personal data

Prague 2017

The Bachelor Thesis Work Supervisor: Ing. Michaela Melicharová

Prohlášení

Prohlašuji, že předložená bakalářská práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem při zpracování čerpal, v práci řádně cituji a jsou uvedeny v seznamu použitých zdrojů.

Souhlasím s prezenčním zpřístupněním své práce v univerzitní knihovně.

V Praze dne 20. února 2017 Břetislav Šmejkal

Poděkování

Tímto bych rád poděkoval paní Ing. Michaele MELICHAROVÉ za čas strávený vedením mé práce, za připomínky a poznámky, které mi pomohly práci zpracovat. Zároveň bych rád poděkoval i JUDr. Tomášovi Koníčkovi z odboru bezpečnostní politiky a prevence kriminality MV ČR za konsultace, možnost čerpat z jeho prezentací a poskytnutí aktuálních statistických údajů.

Anotace

Bakalářská práce se zabývá ochranou osobních údajů osob ve spojitosti s ochranou osob, a to hlavně v současném pojetí. Přináší pohled na současné využívání techniky k ochraně osob, z toho plynoucí výhody, ale také potencionální bezpečnostní rizika při možném zneužití osobních údajů. Prostřednictvím jednotlivých kapitol přibližuje důležité aspekty a vztahy mezi bezpečím, soukromím a ochranou osobních údajů.

Klíčová slova

Bezpečnost, bezpečnostní hrozba a riziko, citlivý údaj, kamerový systém, monitorování, ochrana osob, ochrana osobních údajů, osobní údaj, soukromí, zpracování osobních údajů.

Annotation

This thesis deals with the protection of the privacy of individuals in connection with the protection of people, mainly in its current form. It gives an insight into the current use of technology to protect people of its advantages, but also potential security risks of possible misuse of personal data. Through individual chapters it is approaching important aspects of a relationship between safety, private and personal data protection.

Keywords

CCTV, monitoring, safety, personal data processing, personal data privacy, personal protection, protection of personal data, sensitive data.

ÚVOD

Téma této bakalářské práce je problematika ochrany osob a s ní úzce spojená problematika ochrany osobních údajů osob. Toto téma je vybráno záměrně a to hned z několika důvodů. Asi zásadní roli při výběru tohoto tématu hrálo to, že ochrana osob technickými prostředky, a to nejvíce pomocí kamerových systémů, a ochrana osobních údajů jsou každodenním tématem současné společnosti. Dalším aspektem při rozhodování byl fakt, že kamerové systémy jakožto prevenci považujeme za významného pomocníka při ochraně společnosti. V neposlední řadě také proto, že autor se již několik let v oboru bezpečnosti a bezpečnostních technologií pohybuje. I mnohá další témata byla lákavá, ale možnost a potřeba pokusit se alespoň částečně podělit o poznatky a myšlenky tohoto fenoménu dneška byla silnější než cokoliv jiného.

Naše snažení nebude jen o způsobech a možnostech jak chránit osoby, zdraví a majetky občanů, ale i o tom, jak postupovat při ochraně chráněných zájmů společnosti, demokracii a právu na soukromí.

Pokusíme se nastínit oba pohledy toho, že jsme sledováni, víme, že jsme sledováni, a o věcech zdánlivě okrajových, nezajímavých nebo i jen nepřímo souvisejících.

Práci jsme koncipovali do dvou na sebe navazujících částí. První část pojednává o Ochraně osob a Ochraně osobních údajů osob. V části druhé se budeme zabývat svobodou, soukromím a problematikou všude přítomného monitoringu neboli sledování.

Pomocí popisné metody se zaměříme na vývoj, význam a budoucnost ochrany osob pomocí nových technologií. Budeme směřovat na dva největší fenomény v bezpečnostních technologiích, a to na kamerové systémy a konkrétněji na městské dohlížecí kamerové systémy jakožto nástroje v ruce státní správy. Nástroje, který slouží k ochraně života, zdraví a majetku občanů, ale i jako nástroj prevence kriminality a odhalování trestných činů. Pokusíme se nastínit důležité pojmy, vývoj a tvorbu norem pro nové technologie v časových souvislostech. Toto vše vždy v přímé nebo i nepřímé souvislosti s ochranou osobních údajů. Další část práce bude o možném zneužití osobních údajů a možných následcích.

Tato práce je odrazem praxe v oboru, současných problémech společnosti, ale z velké části i studiem oboru Bezpečnostní studia na Univerzitě J. A. Komenského. Pokusíme se o praktický průnik a interaktivitu praktického života a školních teorií, což není vždy samozřejmostí. Na závěr pak zhodnotíme výsledky a poznatky práce, stávající přínos, využití a možný vývoj, kterým by se mohla ochrana osob a ochrana osobních údajů ubírat v následujícím období.

Jako hlavní cíl práce si klademe zodpovědět otázku, jak velkou hrozbou je pro dnešní a budoucí svět být sledován a identifikován, tudíž i určitá ztráta soukromí. Na druhé straně i prevence, předcházení a objasňování trestné činnosti a terorismu, který naší současnou společnost velmi ohrožuje, a možnosti státu s touto hrozbou bojovat.

1 OCHRANA OSOB A MAJETKU

Ochrana osob, života, zdraví a majetku je stará jako lidstvo samo a historie lidstva dává tomuto tvrzení logický základ. Již první pračlověk, který si vzal do ruky na obranu kámen, věděl, že je potřeba se chránit. A to samozřejmě nejen sebe, ale i svou tlupu, svou jeskyni a svůj úlovek nebo sklizenou potravu. Dá se předpokládat, že i málo vyvinutý pračlověk z druhé tlupy, když viděl v ruce protivníka kámen nebo kyj, rozmýšlel, jestli půjde bojovat anebo nepůjde a jestli bude riskovat zranění z boje. V podstatě tento princip funguje dodnes obdobným způsobem, jen s rozdílem technologie a prostředků.

Osoby a majetek chráníme pomocí dvou základních způsobů, a to fyzická ochrana osob a majetku a technická ochrana osob a majetku.

Fyzickou ochranou se rozumí ostraha, strážný, bodyguard neboli tělesný strážce a alternativy v podobě bezpečnostních služeb a detektivních kanceláří. Nelze nezmínit polici a armádu, která od nepaměti tuto funkci plní v různých obměnách.

Technická ochrana osob a majetku se děli na:[1]

- **mechanické a fyzikální zábrany** (zámky, mříže, bezpečnostní folie na sklo, bezpečnostní sklo, ostnatý drát, žiletkový drát, bezpečnostní dveře a zárubně)
- **stavebně-technická opatření** (zpevnění obvodového zdiva, zvýšení oken, hladké stěny, speciálně umístěné okapy a bleskosvody, případně trezorové místnosti)
- **systémy elektronické ochrany** (dříve EZS, dnes PZS-Poplašný Zabezpečovací Systém, CCTV - Kamerový Systém, EKV (ACS) Elektronická Kontrola Vstupu, EPS – Elektrická Požární signalizace, nebo SHZ – Stabilní hasicí zařízení, atd.)
- **chemické prostředky** – zaplynovaní nebo zamlžení prostoru, případně uspaní osoby v prostoru na základě impulsu např. z EZS nebo jiného spouštěče.
- **a jako poslední kombinace uvedených způsobů.**

[1] ŘÍHA, M., SIEGER, L. a PIKOLA, P. *Bezpečnostní systémy: 1.díl* Vyd. 4. Praha: Námořní akademie České republiky, 2011. 182 s. ISBN 978-80-87103-32-6, str. 3.

Většina elektronických systémů ochrany osob vyžaduje určité informace v podobě osobních údajů, která správce systému spravuje. Jak jsem již předeslal v úvodu, tak pro účely této práce se nejvíce hodí kamerové systémy, a to pro jejich aktuálnost, oblíbenost, relativně velkou efektivitu a propojení s informačními technologiemi. Jak jsem se již zmiňoval v předchozí kapitole, v následujících kapitolách budu pracovat a vše demonstrovat na kamerových systémech, a především na Městském Kamerovém Dohlížecím Systému, neboli v odborných a veřejných kruzích již zažitou zkratku MKDS.

2 HISTORIE, VÝVOJ, DŮLEŽITÉ POJMY

2.1 Vývoj technologie ochrany osob

Vývoj technologií a způsobů ochrany života, zdraví a majetku byl, je a bude přímo úměrný vývoji hrozeb, rizik a nebezpečí, které ohrožují chráněné zájmy společnosti. Myslím, že toto tvrzení není potřeba podkládat žádným oficiálním zdrojem, je to jen zákonitý vývoj, tak jako všechna jiná odvětví lidské činnosti.

V rámci práce se nebudeme věnovat fyzické ochraně osob, která má svá specifika. Využívá člověka s jeho potenciálem a lidským faktorem v kombinaci s technickými prostředky. Z velké části dnes fyzická ochrana osob využívá informační technologie jako zdroj rychlých informací o aktuálním stavu nebo aktuální situaci. Tak jako vše lze tyto informace a informační kanály rušit, odposlouchávat, využívat, měnit a jinak zneužívat.

Nejspíš by pro velkou část veřejnosti nebylo zajímavé ani přínosné zde popisovat vývoj zabezpečovacích systémů, informačních systémů a jiných systémů pro technickou ochranu osob, ale dovolte nám zde krátce demonstrovat vývoj kamerových systémů, jakožto zástupce nejvíce a nejrychleji se rozvíjejícího bezpečnostního systému.

Kamerové systémy zaznamenaly po teroristických útocích z 11. září 2001 nebývalý rozvoj a expanzi. Krátce po útocích na výročí dobytí Bastily 14. července 2016 ve francouzském Nice[2] a ihned po útoku kamionem na vánoční trhy v Berlíně[3] bylo rozhodnuto o nutnosti ještě více zintenzivnit bezpečnostní kamerové systémy.

Abych porovnal tuto dobu s dobou od vzniku technologie jakožto takové, dovolím si velmi stručně několik historických milníků.

[2] NOVINKY.CZ, Atentát v Nice, [online]. 2017. [cit. 2017-01-19]. Dostupné z: < https://tema.novinky.cz/atentat-v-nice >

[3] NOVINKY.CZ, V Německu kvůli hrozbě teroru přibude kamer. Téměř všude, [online 2016. Dostupné z: < https://www.novinky.cz/zahranicni/evropa/424337-v-nemecku-kvuli-hrozbe-teroru-pribude-kamer-temer-vsude.html>

1890	první známé použití termínu „TELEVIZE“[4]
1935	první komerční vysílání
1941	první průmyslově vyráběná kamera se superikonoskopem
1969	využití CCD čipu pro přeměnu světla na elektrickou veličinu
1975	komerční využití televizní CCD kamery
70. léta	ÚOOÚ vydal stanovisko č.1/2006 o provozování kamerových systémů z hlediska zákona o ochraně osobních údajů
1994	Zahájení zřizování MKDS na území ČR
1996	uvedení první IP kamery na trh
2006	ÚOOÚ vydal stanovisko č.1/2006 o provozování kamerových systémů z hlediska zákona o ochraně osobních údajů
2012	norma pro IP přenosové protokoly v bezpečnostních aplikacích
2012	ÚOOÚ vydává metodiku pro splnění základních povinností ukládaných zákonem o ochraně osobních údajů
2014	norma pro dohledové video-systémy (VSS) v bezpečnostních aplikacích – doposud zvané CCTV

Z tohoto krátkého výčtu nejdůležitějších milníků je zřejmé, jak rychlý vývoj zaznamenaly bezpečnostní aplikace v oblasti kamerových systémů v poslední době, a to hlavně přechodem na IP technologii.

[4] ČESKÁ TELEVIZE, Technický vývoj televize v datech a souvislostech, [online]. 2016. Dostupné z: < http://www.ceskatelevize.cz/vse-o-ct/historie/televizni-technika/technicky-vyvoj-televize-v-datech-a-souvislostech >

Ještě bychom se krátce vrátili k vývoji kamerových systémů u nás, a to konkrétně do roku 1994 - 95, kdy začíná zřizování MKDS v ČR. Využili jsme pamětníků z té doby, kteří kdysi působili v jedné pardubické společnosti, která dnes již neexistuje. Z jejich vzpomínek jsme se dozvěděli, že ČR v roce 1994 vyslalo skupinu profesionálů na stáž do Velké Británie, aby získali zkušenosti s výstavbou kamerových systémů. Po ukončení stáže a vyhodnocení bylo určeno 5 měst – 5 referenčních projektů, kde se měl instalovat kamerový systém. Jednalo se o města bez infrastruktury a veškeré kamery zde měli být otočné a ovládané bezdrátovým přenosem. Jelikož u nás s těmito technologiemi a v tu dobu nikdo neměl zkušenosti tak se velmi se experimentovalo, a nejlépe z této situace vyšla právě pardubická společnost. Tato společnost využila znalostí zaměstnanců bývalého podniku Tesla Pardubice, kteří vyvíjeli systém na bezdrátové ovládání lesnických strojů pro zpracování dřeva v těžko přístupných lokalitách. Tito vývojáři úspěšně navázali a pokračovali ve vývoji systému pro lesní průmysl, ale aplikovali ho na ovládání otočných kamer. Tyto systémy byly v prvních letech nasazovány s analogovými kamerami v bezdrátových systémech MKDS a projevily velkou stabilitu a spolehlivost. Následně do ČR přicházejí zahraniční technologie Bosch a Pelco, které tento systém předčily a nahradily ho na našem trhu.

Ještě bychom zmínili jeden historický okamžik, a tím je nástup IP technologie. Ve velkém měřítku se IP kamery a IP technologie začala nasazovat zhruba před 11-12 lety. Do tohoto okamžiku analogové kamery neměly konkurenci v kvalitě obrazu a ani v pořizovací ceně. Zlom nastal s uvedením IP kamery s rozlišením 0,3 MPix na trh s bezpečnostní technikou. Rozlišení a dostupnost IP kamer umožnilo postupně nahradit do té doby používané analogové kamery. Dnes se analogové kamery využívají pouze ve speciálních aplikacích případně ve starších a dosluhujících systémech, neboť analogové kamery nemají moderní funkce a technické možnosti IP kamer.

2.2 Důležité pojmy a názvosloví z oboru

Pro následující práci a pro ucelenost kapitoly je nyní nutno zmínit několik pojmů, které budeme používat, a na jejichž základě budeme stavět další hypotézy a zkoumání.

MANAGEMENT SYSTÉMU	správa dat a propojení na další systémy
BEZPEČNOST SYSTÉMU	integrita dat a systému
AUTENTIZACE	ověření identity objektu
AUTORIZACE	povolení přístupu k funkcím, datům atd.
NOTIFIKACE	upozornění na určitou událost, např. pomocí SMS, mail, atd.
VERIFIKACE	ověření, kontrola, zpětná vazba
ŠIFROVÁNÍ DAT	proces, při kterém se nezabezpečená elektronická data převádějí pomocí kryptografie na zabezpečená, data lze následně číst pouze pomocí dešifrovacího klíče
KRYPTOGRAFIE	nauka o metodách utajování smyslu zpráv převodem do podoby, která je čitelná jen se speciální znalostí
PENETRAČNÍ TEST	test ověřující bezpečnost informačních systémů, uložených dat a databází
CENELEC	Comité Européen de Normalisation Electrotechnique - Evropský výbor pro normalizaci v oblasti elektrotechniky, je nezisková technická organizace.
ONVIF	Open Network Video Interface Forum je průmyslové sdružení výrobců v oblasti IP videa a jeho zpracování bez statutu SDO. Standard ONVIF řeší jednotný protokol pro výměnu neobrazových dat, pro přenos videa a

	komprimační formáty MJPEG/MPEG-4/H.264.
PSIA	je sdružení především výrobců z USA, mezi členy patří společnosti Cisco Systems, Pelco, IBM, Texas Instruments, GE Security a další. V Evropě (tedy i v ČR) není tolik rozšířen jako předchozí standard.
CCTV	Closed Circuit Television, uzavřený televizní okruh – kamerový systém
IP CCTV	kamerový systém s využitím IP technologie (internet protokol)
VSS	Video Surveillance System – dohlížecí video systém, laicky řečeno náhrada zkratky CCTV postavená zcela na IP technologii s využitím dalších zabezpečovacích systémů a SW nadstaveb a rozhraní.
VIDEO-ANALÝZA	soubor určitých funkcí, zkoumajících on-line obraz či záznamy z kamer a vyhledávajících specifické události – např. zda pohyb, změna pohybu, rychlosti, odložený předmět- předmět navíc v obraze, nebo opak ztrátu předmětu, kolik objektů vstoupilo do určité oblasti (počítání lidí, vozidel) a mnoho dalších. Na základě vyhodnocení výše uvedených činností upozorní obsluhu (mail, SMS, zobrazení vybrané kamery na monitory, případně dalšími způsoby). Tyto pokročilé funkce snižují nároky na operátora, jeho pozornost a celkově zvyšují účinnost systému.

PTZ	(pan, tilt, zoom) tedy posun, náklon, přiblížení. Jsou to tedy kamery umožňující horizontální a vertikální polohování kamery spolu s úhlem záběru.
SPEED DOME	jiný název pro výkonnější PTZ s využitím vyšších přenosových schopností
NVR	síťový video rekordér – záznamové zařízení používané v rámci datové sítě
DVR	digitální video rekordér – lokální záznamové zařízení
TERMO KAMERA	kamera citlivá na teplotní rozdíly, využití k termovizi
VIDEO PROSTŘEDÍ	zachycení, přenos a zpracování obrazu
PIXEL	nejmenší obrazový prvek, bod obrazu.[5]

Pojmů a hlavně technických je opravdu velmi mnoho, ale pro účely této práce by měly být výše uvedené plně dostačující.

K vývoji bezpečnostních kamerových systémů obecně je nutno konstatovat, že zásadní zásluhu na pokroku tohoto oboru bezpečnosti má již zmíněná IP technologie a bezpečnostní technologie obecně. Bohužel velmi zásadní mírou se k vývoji těchto technologií přispívá také zhoršující se bezpečnostní situace nejen u nás, ale hlavně u našich sousedů a vlastně i na celém světě. Tím jak se zásadně zvětšují ekonomické rozdíly mezi chudými a bohatými lidmi, tak tím se rapidně zhoršuje i bezpečnostní situace. A zatím žádné vládě se sociální politikou ani migrační politikou tyto rozdíly

[5] VOMÁČKA, J., MIKULA, T., VEINER, Z. a RANDA, M. *IP CCTV Guideline -„Průvodce návrhem síťového videa“* Vyd. 1. Praha: Calamarus, 2011. str. 2-3

nedaří snižovat, natož zastavit. Je to smutná realita současnosti a tragické události a teroristické útoky jsou toho důkazem.

Zmiňované problémy, ekonomické a sociální rozdíly jsou problematikou většiny jednotlivých států. Rozdíly jsou patrné i mezi jednotlivými státy a kontinenty. Za této situace se nelze divit, že mnoho rodičů z rizikových oblastí neváhají opustit domovy za vidinou lepšího života pro své potomky. Tento současný problém dnešní doby bohužel technický systém pro ochranu osob nevyřeší.

3 OCHRANA OSOB A MODERNÍ TECHNOLOGIE

3.1 Moderní ochrana osob obecně

V předešlé kapitole jsme si dali za úkol demonstrovat vývoj bezpečnostních systémů na kamerových systémech a účelově jsme nepopisovali historii bezpečnostních systémů jako celku, jelikož jsme to nepovažovali za přínosné pro tuto práci. Naopak v této podkapitole pro atraktivnost tématu bychom chtěli popsat aktuální a moderní způsoby zabezpečení a moderní technologie. Nežli se dostaneme k vybranému vzorku, a to konkrétně kamerovým systémům, popíšeme několik atraktivních a zajímavých technologií.

S určitostí lze konstatovat, že dnešní bezpečnostní technice a technologiím vévodí identifikace, verifikace a autorizace (zjištění, ověření a získání souhlasu) s využitím biometrie[6]. Biometrie je metoda založená na rozpoznávání jedinečných biologických charakteristik jedince. Tyto charakteristiky jsou pro každého člověka jedinečné a neměnné.

Nyní uvedeme několik typických příkladů biologických charakteristik, které se v biometrii využívají. Otisk prstu, oční duhovka, obličej, krevní řečiště, hlas, chůze. Otisky těchto charakteristických znaků se sejmou a uloží na server, do registru nebo do databáze systému, kde ověřují identitu osoby. Pro větší bezpečnost se využívá vícestupňová autentizace, kde zjištěná biologická charakteristika je doplněna o zadávání PIN kódu a dalšího identifikačního média jako například bezkontaktní karty. Toto byl příklad nejvíce využívané moderní techniky, ale samozřejmě existuje mnoho dalších. Ve zkratce uvedu několik dalších příkladů současných trendů ochrany osob. Jedná se o systémy vyhledávání osob a vozidel pomocí GPS a GSM, detekce různých fyzikálních veličin a určitě je potřeba zmínit i termovizuální systémy pro noční vidění, ale také termovizi pro detekci požáru, nebo poruch na elektrickém vedení.

[6] HOSPODÁŘSKÉ NOVINY, Biometrie v Čechách, [online]. 2017. Dostupné z: < http://life.ihned.cz/c1-63229990-biometrie-v-cechach>

Dalším zajímavým fenoménem je ochrana osob v rámci krizového řízení, a to jsou systémy včasného vyrozumívání osob[7]. Jedná se o automatický systém varování, informování a vyrozumění v případě mimořádných událostí. Tento systém automaticky sbírá a vyhodnocuje všechny potřebné informace. Jedná se o měření environmentálních veličin (např. aktuální výšky vodních hladin, nasycenosti půdy, množství srážek, pohybu dešťových mraků), ale také o detekování úniku nebezpečných látek a chemikálií (např. amoniaku, chloru, kyanovodíku). Systém včas vyrozumí všechny odpovědné osoby. Ty následně s využitím systému varují a srozumitelně informují ohrožené obyvatele, a to na celém území nebo jen v zasažené lokalitě. V podstatě se jedná o kombinaci bezpečnostního systému, měření fyzikálních veličin, regulace, EPS, CCTV, IT, veřejného rozhlasu a telefonní ústředny.

A nyní již zmiňované moderní kamerové systémy. Vývoj CCTV je tak rychlý, že se pokusíme popsat jen základní stavební kameny systému, s ohledem na modularitu, automatizaci systému, integraci dalších bezpečnostních systémů a využitelnost dat pro prevenci kriminality.

Dle nového pojetí je kamerový systém postaven na koncepci IP technologie, tedy IP CCTV s následným využitím jako VSS, tedy video dohlížecí systém s integrovanou SW nadstavbou a využitím dalších bezpečnostních systémů.

Dle bezpečnostní analýzy máme dané lokality, které je potřeba sledovat, a mělo by být i dáno, jaký **stupeň identifikace osob** nebo objektů je požadován:

- **Monitorování skupiny** - cíl musí představovat alespoň 5 % výšky obrazu na monitoru (1 pixel na 80mm)
- Pro **detekci** musí cíl představovat minimálně 10 % výšky obrazu na monitoru (1 pixel na 40mm)
- Pro **přehled** je potřeba 25 % výšky obrazu na monitoru (1 pixel na 16mm)
- **Rekognoskace** neboli rozpoznání obrysů je vyžadováno již 50% výšky obrazu na monitoru (1 pixel na 8mm)

[7] COLSYS, VoiceGuard – varovný a informační systém, [online]. 2017. Dostupné z: < http://www.colsys.cz/voiceguard-varovny-a-informacni-system/>

- **Identifikace** cíle - plných 100 % výšky obrazu na monitoru (1 pixel na 4mm)
- Pro **detailní identifikaci, též inspekci** je nutností 400 % výšky obrazu (1 pixel na 1mm)[8]

Na základě těchto informací je potřeba vybrat vhodný typ kamery. Dnes již minimálně od 3 Mpix až do 16 Mpix a více. Také dle této informace a potřeby uživatele jsou navrženy kamery pevné (stacionární), nebo otočné (PTZ, Speed Dome). Pro speciální aplikace se používají termo kamery s funkcí termovize - nočního vidění.

Srdcem i mozkem celého systému je **záznamové zařízení,** které dnes není ničím jiným než výkonným počítačem nebo serverem se speciálním záznamovým softwarem. K tomuto zařízení nezbytně patří klávesnice a joystick pro ovládání kamer a vyhledávání v uložených záznamech. Samozřejmě plní i mnoho jiných servisních funkcí a funkcí spojených s návaznostmi na další systémy. V menších systémech bývá záznamové zařízení jedno, ve větších městech se zařízení skládají. Jedno hlavní (master) a ostatní jsou podřízené (slave). Praxí je vzdálené pracoviště, což znamená možnost ovládat a spravovat systém z dalšího místa, nebo jen možnost náhledu do uložených záznamů. V reálu je to tak, že například na Městské policii je záznam s dohledovou aplikací tzv. tlustý klient a aplikace ve webovém prohlížeči je tzv. tenký klient, služebna Policie ČR. Budoucnost je použití samostatných dekodérů pro přenos obrazu pro tablety nebo smartphony strážníků, pro možnost rychlého zásahu a vyhodnocení situace.

Bez monitorů není možno provozovat žádný kamerový systém, a tak na moderním pracovišti jich bude hned několik. V popředí bývá instalován velký vícenásobný monitor pro zobrazení několika kamer současně, případně map kriminality, nebo řídícího SW, a to dle potřeby a režimu pracoviště. Po straně bude poplachový

[8] VOMÁČKA, J., MIKULA, T., VEINER, Z. a RANDA, M. *IP CCTV Guideline -„Průvodce návrhem síťového videa“* Vyd. 1. Praha: Calamarus, 2011. str. 13

monitor určený pro kamery spojené s poplachovými stavy. Určitě nelze opomenout monitory doplňkové pro mapové podklady a monitory pro vizualizační a nadstavbový systém. Na těchto monitorech se budou zobrazovat údaje z jiných bezpečnostních systémů, jako například měření a regulace budov nebo stavu toku řek. Lze zde dálkově pomocí externích detektorů jiných systémů nebo pomocí analytických funkcí kamer měřit jiné veličiny: teplo, zima, tma, světlo, plameny, kouř.

Pro bezpečnost budovy a operátorského pracoviště bude v nadstavbovém systému integrován systém EPS a PZTS s další návaznosti na ACS. Asi se shodneme, že toto vše obsáhnout je pro člověka nereálné a že potřeba takového systému je nezbytná. SW nadstavbu bude potřeba zásobovat i jinými informacemi, které nebude SW automaticky generovat, a tak bude potřeba tyto informace aktualizovat. Například informace o přesunech mobilních kamerových bodů, ztráty tabletu nebo mobilního telefonu strážníka atp. Tento systém na základě zpětné vazby, poznatků, databází a vhodného využívání inteligentních video-analýz, účinně vyhodnocuje všechna vstupní data a tím přispívá k práci ochránců pořádku a bezpečnostních služeb.

Výše popsaný způsob zvyšuje efektivitu a účinnost kamerových systémů a současně eliminuje často chybující lidský faktor.

3.2 Moderní aplikace a funkce, video-analýza

V současné době již nestačí, aby bezpečnostní a kamerové systémy jen zaznamenávaly, ale také aby včas a předem hlásily a varovaly před rizikem, hrozbou na chráněných společenských zájmech. Jejich současný význam nespočívá jen v eliminaci a minimalizaci škod, ale také ve varování před hrozícím nebezpečí v jakékoliv formě. Tyto hrozby začínají živelnými a přírodními katastrofami v podobě záplav a požárů a končí tím nejhorším, a to například teroristickými útoky.

Pro podporu výše uvedeného tvrzení uvádíme následující případ, ve kterém moderní bezpečnostní technologie a kvalitní policejní práce s maximálním nasazením dokázala zabránit v pokračování série plánovaných bombových atentátů. Jedná se o případ londýnských bombových útoků z roku 2005, tento příklad uvádím záměrně i přes

jeho neaktuálnost, jelikož Velká Británie byla a je ve využívání městských kamerových systémů světovou velmocí.

„Britská policie pracovala s pozoruhodnou efektivitou. Jen málo přes týden po nezdařených londýnských útocích z 21. července zadržela čtveřici hlavních podezřelých. Nyní pravděpodobné pachatele vyslýchá, předpokládá se, že mohou být vodítkem k dalším militantům. Policisté tedy mají všechny čtyři muže, které zachytily po druhých útocích stacionární kamery.“ [9]

Na základě přispění technického pokroku britská policie týden po nezdařených útocích zadržela čtveřici podezřelých, kteří se na snímcích digitálních kamer jen letmo mihli. Tento úspěch byl zásluhou spolupráce vyspělé technologie, a to analytického software, který analyzoval a vyhodnotil v daném čase, na daném místě pohyb všech osob. Na konci této složité operace byly vytipovány čtyři fotografie, které pomohly v pátrání.

Samozřejmě i po tomto příkladu, kdy budou skeptici a odpůrci nových technologií argumentovat, proč by měl systém sám varovat, když je sestrojen, ovládán a kontrolován člověkem? Odpovědí jim budiž obecně známy fakt, že lidskou soustředěnost lze udržet maximálně 20 minut. Tato soustředěnost však s počtem kamer prudce a exponenciálně klesá, a tudíž snižuje schopnost rozpoznávání a okamžitého správného vyhodnocení a úsudku. Tuto přirozenou lidskou nedokonalost lze velmi dobře zmíněným způsobem eliminovat.

To, že se jedná o specifické a speciální funkce analyzující a vyhodnocující, již bylo řečeno. Tyto inteligentní video-analytické funkce probíhají na pozadí celého systému a dokážou na základě výpočtů předvídat a včas varovat.

[9] EGOVERNMENT, Ostře sledovaná města, kamerové systémy, [online]. 2016. [cit. 2016-12-30]. Dostupné z: < http://www.egovernment.cz/kamery/kamery%2006.htm >

Nyní bychom se pokusili několik těchto funkcí podrobněji popsat [10] a vždy se k nim pokusíme dosadit možné protiprávní jednání, které by bylo možné při využití jednotlivé funkce zmírnit nebo eliminovat.

- **PANIC DISORDER**: detekce neočekávaného chování skupiny osob. Detekuje se rychlost a zrychlení v předem definované oblasti zájmu - *terorismus, vandalství, výtržnictví, rabování*
- **LEFT OBJECT**: detekce ponechaného objektu v prostoru - *terorismus*
- **LACK REFILL**: detekce a upozornění na chybějící objekty, předměty - *krádež, zcizení*
- **SMOKE FIRE**: detekce kouře/plamene - *ochrana života, zdraví, majetku, ochrana životního prostředí*
- **GATE FLOW**: počítání objektů, které překročí definovanou hranici - *dopravní přestupky, výtržnictví*
- **AREA COUNTING**: hlídání prostoru a daného počtu osob v čase - *výtržnictví, chuligánství, nepovolené shromažďování*
- **COUNTING**: počítání objektů, které překročí definovanou hranici - *dopravní přestupky*
- **OCCUPANCY RATE**: počítání objektů v prostoru v procentech - *doprava-kolony*
- **PARKING LOT**: detekce a upozornění na obsazení parkovacích ploch - *dopravní přestupky*
- **SLIP FALL**: detekce ležící osoby po dobu delší než definovaný čas - *ochrana života a zdraví*
- **STATIONARY VEHICLE**: detekce stojícího vozidla v dané oblasti déle než je povolný čas - *doprava, krádeže vozidel*
- **ATM:** hlídaní vymezeného prostoru, osob a času před bankomatem - *přepadení, loupež*

[10] IPSECURITY, Videoanaytics [online]. 2016. [cit. 2016-12-30]. Dostupné z: < http://videoanalytics.cz/# >

- **STOLEN OBJECT**: detekce zmizelého objektu - *krádež*
- **AVG SPEED**: měření a detekce rychlosti, upozornění na vysokou/malou rychlost - *doprava*
- **FACE DETECTION**: detekce obličeje ve vymezeném prostoru - *loupež, přepadení*
- **SKIMMER DETECTION**: detekce minimálních změn bankomatu - *krádež*
- **PTZ STAND ALONE**: detekce a automatické sledování cíle - *krádež, loupež, podezřelá osoba*
- **ČTENÍ RZ**: detekce hledaných vozidel -*krádež*

Toto jsou nejspíše nejvíce používané současné video-analytické funkce. Je známa řada dalších, které však nejsou ještě technicky úplně dokonalé, aby měly odpovídající výkonnost a spolehlivost při analytických operacích. V odborné veřejnosti jsou očekávány funkce na detekci zakrytí obličeje a detekci dalších biometrických znaků, které jsou v plánu a které budou určitě dobrým pomocníkem při hledání teroristů a pachatelů trestných činů. Využití video-analýzy v obrazu je v ČR stále na začátku, jelikož na tyto aplikace není připravena většina stávajících systémů. U nových a moderních systémů, kde výpočetní výkony záznamových a vyhodnocovacích zařízení bývají dostatečně dimenzovány, bohužel razantně zvyšují pořizovací cenu, jelikož tyto SW produkty jsou v současné době poměrně finančně náročné.

Je jisté, že nasazení těchto aplikací není jediným a celkovým řešením, ale prostor při pomoci řešení každodenních i specifických okamžiků dnešní doby tu bezesporu je a bude.

3.3 Využití moderních technologických celků

Bezpečnostní systémy mají využití ve všech odvětvích a oborech lidské společnosti, o tom určitě také nikdo nepochybuje. Počínaje bezpečnostním zámkem, požárním čidlem, obyčejným alarmem v bytové jednotce, a konče sofistikovaným bezpečnostním celkem pro ochranu například jaderné elektrárny, který se skládá z mnoha různých systémů a je spravován nadstavbovým systémem.

Z historického vývoje bezpečnostních systémů, který je popsán v kapitole 2.1, již víme, že nasazování kamerových systémů ve městech a obcích se datuje od 70. let minulého století ve Spojeném království. Taktéž jsme se dozvěděli, že první hromadné nasazování v ČR nastalo po roce 1994. Současnost lze charakterizovat jako období celosvětového a hromadného nasazování kamerových systémů, které nastalo po teroristických útocích 11. září 2001.

I přes mnoho odpůrců těchto kamerových, sledovacích nebo v případě měst dohlížecích systémů je jejich význam nezanedbatelný a nezpochybnitelný. Tyto důvody budeme objasňovat v dalším textu v kapitole o prevenci kriminality.

Obecně se kamerové systémy, nejen MKDS, nasazují tam, kde je potřeba a kde mají chránit životy, zdraví a majetek obyvatel a chránit společnost před nežádoucími vlivy protiprávního jednání. Ze současného každodenního života a z logiky věci usuzujeme nebo spíše jen tušíme, kam je vhodné tyto bezpečnostní kamerové systémy nasadit. I přes tyto relativně prosté postřehy nás všech zde tyto nejdůležitější místa zmíníme. Jedná se prioritně o místa s velkým pohybem lidí jako náměstí, křižovatky, nádraží, stanice hromadné dopravy, školy, nemocnice, úřady, okolí velkých společností a okolí nákupních center, památkově chráněné lokality, budovy a v hojném měřítku i železniční přejezdy. Opakem těchto frekventovaných a exponovaných míst, kde se kamerové systémy instalují, bývají například okolí černých skládek, podchody, parky a různá zákoutí vhodná k páchání trestné činnosti od prodeje drog až po trestné násilné činy.

Při plánování umístění kamer se vychází hned z několika skutečností, jako jsou mapa kriminality - výskyt trestných činů v místě a čase. Pokud není k dispozici, tak se postupuje podle požadavku obce, odboru bezpečnostní politiky a prevence kriminality, obecní policie a místního oddělení státní police. Na základě všech těchto informací je důležité nejen správné umístění, ale také zvolení vhodné a odpovídající technologie. Zásadní je určit jestli bude obraz z kamery sloužit jako přehledový, detailní nebo jinak specificky zaměřený. Důležité je a většinou to bývá pravidlem, že vítězí potřeba a také zdravý rozum, tj. potřeba toto místo sledovat, případně delší dojezdová doba příslušné složky policie.

Výstavba a modernizace kamerových systémů je od roku 1996 podporována státem prostřednictvím Programu prevence kriminality. O těchto programech se ještě budeme podrobněji zmiňovat v další kapitole.

3.4 Obsluha systémů a operátor

Obsluhou bezpečnostního systému se obecně rozumí oprávněná a zaškolená osoba, seznámená se zařízením, technickými možnostmi zařízení a v neposlední řadě i s legislativou, ale nemá výjimku ze zákona. Tato osoba zařízení obsluhuje uživatelským způsobem a v případě poruchy informuje servisní organizaci.

Operátor je osoba oprávněná k operacím používání bezpečnostního kamerového systému pro jeho zamýšlený účel a je osobou, která má výjimku ze zákona. Aby se člověk mohl stát operátorem, je potřeba úspěšně absolvovat certifikační kurs, který je zakončen zkouškou a certifikátem.

Obsahem takového kurzu[11] jsou základy prevence kriminality a situační prevence, základy psychologie se zaměřením na krizové situace, na příznaky přípravy a pokusu protiprávního jednání a reakcí na něj a v neposlední řadě etika práce, a konkrétně zásah do soukromí občanů. Součástí kurzu musí být nutně právní minimum a taktika zákroků. Jedná se zejména o právní aspekty ochrany práv a svobod občanů. Nezbytná je i znalost možností instalace a využívání kamerových systémů, využití kamerových záznamů pro policejní a soudní účely. Taktéž je kladen důraz zejména na policejní zákrok na místě činu dle § 28 a § 29 trestního zákona, § 76 odst. 2 trestního řádu. Samozřejmě nesmí chybět dovednost správy a obsluhy kamerového systému. To vše je zakončeno praktickým cvičením a zkouškou.

Na základě tohoto kurzu operátor zná vše potřebné a umí zacházet a ovládat kamerový systém. Dokáže vyhodnotit a předvídat situace běžného života i situace výjimečné, na které je připraven, a je více než nápomocen svým kolegům v terénu, případně ke zpětnému odhalování protiprávních činů.

[11] TRIVIS a.s., Vzdělávací kurzy, [online]. 2017. Dostupné z: <http://www.trivis.cz/kurzy >

Pracoviště operátora je většinou i srdcem celého kamerového systému, ale není to pravidlem. V případě velkých měst je záznamové zařízení uloženo v zabezpečené datové místnosti - serverovně a pracoviště operátorů je dislokované. Na operátorské pracoviště a jeho provozní režim platí zvláštní opatření, jak bezpečnostní tak režimové. Výjimkou je služebna Policie ČR. Také je potřeba brát v patrnost, v jakém režimu kamerový systém funguje. V režimu operátorském 24 hodin, nebo polo-automatizovaném, případně jinak částečně automatizovaném.

Stanovená funkce operátora MKDS je velká výhoda oproti velkým kamerovým systémům zřizovaným v komerční sféře. Velmi často se setkáváme s potřebou kamerového systému, ale velká část zřizovatelů již nechce investovat do obsluhy systému, a to je velká a často zásadní chyba. Funkcí operátora a správce systému se předchází nejen trestné činnosti, ale i chybám systému, ztrátě dat a často také porušení zákonů a zásad ochrany osobních údajů.

Jaké jsou názory na užívání městských kamerových systémů? A co si asi myslí většina lidí dodržujících zákon, kteří dají na svůj vlastní rozum a chtějí žít a cítit se bezpečně? Aniž by se někdo z nás zajímal o aktuální statistiky, mapy kriminalit nebo jiné studie, určitě všichni řekneme stokrát ano kamerovým a městským kamerovým dohlížecím systémům! Vždyť pomáhají asi ne podle požadavků většiny z nás, ale vždyť i nejhloupější kapsář si rozmyslí krást před kamerou a o pomoci v dopravě ani není třeba mluvit.

Zkrátka a dobře MKDS je reálná a nepostradatelná přítomnost dnešní doby. Je to ale určitě i budoucnost, kde pomocí pokroku technologie a video-analytických funkcí bude společnosti pomáhat, chránit občany a demokratické principy nejen naší země, ale všech rozumných lidí. Je to sice jen jeden malý nástroj v boji proti protiprávnímu jednání, ale jsme za něj rádi a myslíme, že nejsme sami.

4 PREVENCE KRIMINALITY, EFEKTIVITA

4.1 Přínosy a využití technologie v ochraně osob

Zřejmě již od nepaměti, kdy se možná ani nemluvilo o prevenci kriminality, byly technické prostředky nápomocny jako ochrana před případným nebezpečím. Tím více v dnešní době, kdy bezpečnostní technologie prožívají neustálý vývoj a zdokonalování, je pro nás všechny samozřejmostí, že součástí prevence kriminality jsou kamery, kamerové systémy a další bezpečnostní technologie, včetně jejich spolupráce, vzájemného propojení a v blízké době i integrace všech systémů do jedné nadstavbové integrační aplikace.

V současné době jsou dozajista nejrozšířenějším technickým nástrojem prevence kriminality bezpečnostní kamerové systémy, které plní současně několik zásadních funkcí. Systémy jednoznačně působí preventivně, ale mají i funkci dohledovou, analytickou a čím dál častěji pomáhají koordinovat práci policie a IZS. Dalším nezvratným přínosem je i větší efektivita zásahu a spolupráce složek IZS. Při nasazení kamerových systémů na frekventovaná a vysoce exponovaná místa vytváříme takzvané bezpečné zóny – bezpečné lokality[12] a pomáháme celkové strategii prevence kriminality. V případě vhodně zvoleného nasazení kamerového systému na vytipované lokality se velmi rychle, téměř okamžitě, snižuje kriminalita, zvláště když vše přesně zapadá do celkového programu prevence kriminality.

Přínos a snížení kriminality pomocí MKDS ve své studii Vyhodnocení účinku kamerových systémů [13] popisují Martin Hill a Angela Sprigss . Výzkumnou a popisnou

[12] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY, Dotační systém prevence kriminality[online]. 2016. Dostupné z:< http://www.mvcr.cz/clanek/pilotni-projekt-bezpecna-lokalita-bezpecne-bydleni-se-rozjizdi-v-brne-a-ve-zline.aspx >

[13] HILL, M. a SPRIGSS, A. *Vyhodnocení účinku kamerových systémů* Vyd. 1. Praha: Institut pro kriminologii a sociální prevenci, 2007. ISBN 978-80-7338-061-8

metodou zodpověděli základní otázky, které jsou pro tuto práci nejen zajímavé, ale i zásadně vypovídající, a to:[14]

- Otázka: Snižují kamerové systémy strach z kriminality?

  Odpověď: Ano snižují, ale lidé si kamer musí všimnout, což u mnoha z nich není.

- Otázka: Odrazují kamerové systémy od trestné činnosti?

  Odpověď: Ano, ale nikoliv zásadně, někteří pachatelé se nechají odradit, někteří se uchýlí k méně závažným trestným činům.

- Otázka: Pomáhají kamerové systémy při dopadení a stíhání pachatelů?

  Odpověď: Ano, ale ne natolik, aby mohly nahradit policisty.

- Otázka: Vedou kamerové systémy k přesunu kriminality?

  Odpověď: Ano, ale jen minimálně a jen určitých TČ jako např.: krádeže vozidel.

Na základě výše uvedených skutečností a poznatků si dovolujeme tvrdit, že vhodně a strategicky instalovaný a využívaný Městský kamerový dohlížecí systém v konceptu prevence kriminality pomáhá všude, vždy a mnoha pozitivními způsoby ve větší či menší míře. Tento poznatek určitě platí i pro kamerové a bezpečnostní systémy pro soukromý sektor, včetně instalace několika málo kamer na rodinném domku, které odstraší většinu potenciálních zlodějů.

[14] HILL, M. a SPRIGSS, A. *Vyhodnocení účinku kamerových systémů* Vyd. 1. Praha: Institut pro kriminologii a sociální prevenci, 2007. ISBN 978-80-7338-061-8, str. 15-17

4.2 Prevence kriminality v ČR

Již několik let jsou naší vládou v rámci Strategie prevence kriminality[15] v ČR na určená období vypisovány dotační tituly. Hlavní dotační titul MV ČR je každoroční Program prevence kriminality. Tyto dotace se poskytují pouze obcím nebo krajům. Jde o dotace investičního, ale také neinvestičního charakteru. Pro naše účely je podstatné, že se v zásadní míře jedná o dotace na MKDS, jelikož výstavba MKDS je považována za jeden ze základních pilířů systému prevence kriminality v České republice. Hlavní úkol, který je uveden ve Strategii prevence kriminality, je omezování možných příležitostí k páchání trestných činů. Předpokládá se, že je plněn především prostředky, které jsou užívány při situační prevenci, tedy také MKDS.

A nyní několik základních čísel pro představu, které byly poskytnuty panem JUDr. Tomášem Koníčkem z odboru bezpečnostní politiky a prevence kriminality MV ČR:

Za období let 1996 – 2014 bylo podpořeno celkem 789 dílčích projektů na MKDS, pro 203 měst a obcí za 562.945.000,- Kč.

V roce 2015 to byly projekty pro 51 obcí v celkové hodnotě 16.060.000,- Kč.

Jen pro zajímavost a celistvost informace uvedu další příklady projektů těchto dotačních titulů z roku 2015:

- Asistent prevence kriminality, bylo vytvořeno 175 pozic v celkové dotaci 22.656.000,- Kč, tento projekt byl podporován i z Evropského sociálního fondu, konkrétně z Operačního programu lidské zdroje a zaměstnanost.
- Domovník - preventista, celkem podpořeno 23 domovníků v 11 obcích v celkové částce 1.288.000,- Kč
- Forenzní identifikační značení jízdních kol a kompenzačních pomůcek, celkem podpořeno 12 projektů v celkové částce 657.000,- Kč
- Výslechové místnosti

[15] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY, Dotační systém prevence kriminality[online]. 2017. [cit. 2017-01-10]. Dostupné z: < http://www.mvcr.cz/clanek/web-o-nas-prevence-prevence-kriminality.aspx>

- Práce s rizikovými dětmi, mladistvými či rodiči, včetně pobytových aktivit a letních či příměstských táborů
- Vybavení nízkoprahových kluboven pro rizikové děti či děti ze sociálně vyloučených nebo rizikových lokalit
- Projekty zaměřené na seniory
- Dluhové poradenství
- Infomační projekty
- Projekty zaměřené na kyberbezpečnost

4.3 Statistické údaje prevence kriminality ČR v číslech

„Více než 40 000 trestných činů je meziroční pokles trestné činnosti na území České republiky. Za rok 2015 bylo oznámeno 247 628 trestných činů, což znamená pokles o 14,2 %. Kromě samotného poklesu kriminality stoupla i objasněnost. Celkem bylo objasněno 126 083 skutků, tedy 50,9 %. Jedná se o téměř dvouprocentní nárůst v objasněnosti a v porovnání s rokem 2013 stoupla objasněnost o téměř 7 %. Pokles trestné činnosti je zaznamenám u všech druhů trestných činů. Dlouhodobě platí, že nejvíce je majetkové trestné činnosti. Za minulý rok bylo 139 092 majetkových trestných činů, meziročně tak majetková trestná činnost klesla bezmála o 20 %. Výrazný pokles nastal také v počtu násilných trestných činů. Meziroční pokles o 1 280 skutků znamená pokles o 7,6 %. „Pokles trestných činů a zároveň zvýšení objasněnosti je vizitkou dobré práce všech policistů“.[16]

Na základě výše uvedené citace tiskové zprávy z portálu informačního servisu Policie ČR o počtu objasněných případů demonstruji aktuální stav trestné činnosti. Tyto informace jsou hlavně zásluhou příslušníků Policie ČR, obecní policie a celkově plněním Strategie prevence kriminality, to asi není třeba zdůrazňovat. A jelikož nelze

[16] POLICIE ČESKÉ REPUBLIKY, Počet objasněných případů stoupá[online]. 2017. [cit. 2017-01-18]. Dostupné z: < http://www.policie.cz/clanek/pocet-objasnenych-pripadu-stoupa.aspx>

reálně porovnat, jakou část na těchto výsledcích mají MKDS, pokusíme se experimentovat s dostupnými čísly.

Velmi jednoduše porovnáme investice do MKDS a snížení registrované kriminality.

Celková škoda za rok 2014	28 696 mil.,- Kč
Celková škoda za rok 2015	26 899 mil.,- Kč
Rozdíl v celkové škodě 2014-2015	1 797 mil.,- Kč
Celková hodnota investic do MKDS v roce 2015	16 mil., - Kč [17]

Vyjde nám, že celkové investice do MKDS je necelé 1 % z meziročního snížení škody TČ. Je nezbytné také brát v úvahu, že systémy nově zbudované, nebo rozšíření stávajících bylo uvedeno do provozu nejdříve v 2Q/2015, spíše později.

Předpokládejme, že další výpočty nejsou nutné, alespoň z tohoto pohledu ne. Ale i když tedy budeme ještě nepatrně používat matematické výrazy a připočítáme pocit bezpečí, které kamery poskytují, snížení počtu vražd a násilí, které nelze měřit penězi, stále nám vychází, že jdeme správnou cestou. Vždyť některé věci jsou neměřitelné a nenahraditelné. Například život člověka, zdraví a psychika člověka bylo, jest a bude jedna z nejcennějších věcí, a jejich ztráta bývá zásadní, nenávratná a nenahraditelná.

[17] POLICIE ČESKÉ REPUBLIKY, Počet objasněných případů stoupá[online]. 2017. [cit. 2017-01-19]. Dostupné z: < http://www.policie.cz/soubor/tk-kriminalistika-v-roce-2015-tisk-ppt.aspx>

4.4 Efektivita bezpečnostních systémů

V dnešní konzumní společnosti se vše přepočítává na peníze, nebo alternativně se suplují obdobnými ekvivalenty jako je efektivita, nákladovost případně jinými pojmy. Ne jinak je tomu i v oblasti bezpečnosti a bezpečnostních systémů.

Z tohoto důvodu jsme do této části práce zařadili právě úvahy o efektivitě. Pokusíme se tedy tuto myšlenku velmi krátce rozvést tak, jak ji vidíme nejen z pohledu člověka, ale vlastně i z pohledu manažera, který se denně setkává s otázkou, jak efektivně využijeme finance vložené do bezpečnostního systému.

Základní obecná představa o efektivitě je nám všem jistě velmi dobře známá. Je to poměr vynaložených nákladů k dosaženému výsledku. Efektivita je také někdy chápána jako porovnávání výsledků dosahovaných v určitých časově nebo jinak oddělených obdobích v závislosti na očekávaném cíli. Ačkoli takovýto výklad neodpovídá obecné definici, srovnávání působení v časových obdobích má velký poznávací účinek, neboť odhaluje trendy působení, a ty jsou důležité pro odhad budoucích výsledků a tím i pro plánování a rozhodování.

Když je řeč o efektivitě, nelze opomenout další oblíbený parametr naší doby, a to **životnost.** Co je to tedy životnost, životaschopnost? Je to pojem, který vyjadřuje aktivní délku činnosti systému.

V technické řeči je životnost dána schopností kladné reakce na měnící se podmínky okolí. Jinak řečeno mít svůj význam v odlišných podmínkách, než při kterých systém vznikal, nebo pro které systém vznikal. V případě systémů pro ochranu osob jde především o nasazování nových technologií, ale také změny bezpečnostních rizik. Životnost spočívá nejen v tom přežít svou dobu provozu, ale i schopnost spolupracovat s novou nebo jinou technologií.

Nechceme a nemůžeme opomenout schopnost **modernizace**. Vždyť tento výraz jde takříkajíc ruku v ruce s výrazem **rozšiřování a nová rizika.** Modernizujeme cokoliv, pak je to činnost vedoucí k dalšímu účelnému využívání po co nejdelší dobu. A pakliže rozšiřujeme bezpečnostní systém, tak také plánujeme, že systém bude aktivní a funkční po dobu co nejdelší. Současné bezpečnostní systémy velmi rychle

stárnou jak po stránce technické, tak po stránce morální, a proto je důležité brát v potaz výše uvedenou myšlenku o efektivitě, životnosti a modernizaci.

Závěrem lze konstatovat, že bezpečnost a ochrana osob byla, je a bude lukrativní odvětví, zvláště v současné mezinárodní situaci a situaci naší společnosti, kdy se sociální rozdíly mezi lidmi začínají prohlubovat.

V této kapitole bylo řečeno, kdy a jak bezpečnostní systém jakožto společensko-technický systém potřebujeme a kdy a kam je vhodné ho umístit. Také jsme se jen opravdu velmi nepatrně dotkli nových technologií a sofistikovaných integrovaných systémů, které zásadně urychlují práci, rozhodování a reakci na TČ, a to nejen pomocí kamerových systémů, ale i jiných bezpečnostních systémů a jiných podpůrných informací a celkovém stavu situace. Závěrem jsme řešili efektivitu, nákladovost, životnost a možnosti modernizace systémů v časových i technických souvislostech. Dovolíme si konstatovat, že vynaložené úsilí a prostředky v naší republice jsou prozatím dostačující a adekvátní situaci v ČR.

5 OCHRANA OSOBNÍCH ÚDAJŮ

V tomto okamžiku se dostáváme k druhé části názvu této práce a to znamená, že se budeme zabývat ochranou osobních údajů. V legislativě ČR je primárně řešena ochrana osobních údajů zákonem č. 101/2000 Sb., o ochraně osobních údajů. Konkrétní principy a způsoby ochrany osobních údajů[18] stanovuje tento zákon v § 13 a to tak, že stanovuje správcům a zpracovatelům údajů přijmout příslušná opatření, aby nemohlo dojít k narušení ochrany osobních údajů. Tato opatření mají preventivní charakter a mají eliminovat úmysl, nahodilost nebo nedbalost při pořizování a zpracovávání osobních údajů. Tato část zákona také řeší bezpečnost nosičů a technologií, které se při zpracování používají. Lze konstatovat, že v nadneseném slova smyslu tento zákon nepřímo nabádá zpracovatele, aby zpracovali bezpečnostní analýzu rizik, na jejímž základě by byla vyhodnocena objektová bezpečnost, personální bezpečnost a obecná technologická bezpečnost. Jinými slovy, aby vyhodnotili, zda-li zpracování provádí prověřená a kvalifikovaná osoba, na dostatečně zabezpečeném místě a s dostatečně vyspělou a zabezpečenou výpočetní technikou.

Mimo zákon č. 101/2000 Sb., o ochraně osobních údajů je ochrana osobních údajů zakotvena Ústavou ČR a LISTINOU ZÁKLADNÍCH PRÁV A SVOBOD, v článku 10 odst.3 *„Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.“* [19]

Co tedy vlastně jsou osobní údaje a čím vším může být osobní údaj? *„Podle § 4 písm. a) OchOsÚ se pro účely tohoto zákona osobním údajem rozumí „jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjektem údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických*

[18] BARTÍK, V. a JANEČKOVÁ, E. *Ochrana osobních údajů v aplikační praxi: vybrané otázky* Vyd. 3. Praha: Linde Praha, 2013.311 s. ISBN 978-80-86131-96-2, str.101-102

[19] POSLANECKÁ SNĚMOVNA PARLAMENTU ČESKÉ REPUBLIKY, Usnesení o vyhlášení LZPS, [online]. 2017. [cit. 2017-01-19]. Dostupné z: < http://www.psp.cz/docs/laws/listina.html>

pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu“.[20]

Na základě výše uvedené citace zákona lze tedy vnímat dva základní pohledy na osobní údaje[21].

První pohled je jednoznačně znalost fyzické osoby, ke které se osobní údaje vztahují. To znamená, že známe jméno, příjmení a další identifikační data, tudíž přesně víme, o koho se jedná. Jedná se o příbuzné, známé kolegy, sousedy apod. V tomto případě je jakákoliv informace, kterou o těchto osobách znám osobní údaj.

Opačný stav a současně druhý pohled je v případě, že vlastníme některé identifikátory, ale nevíme, jakému subjektu je přiřadit. Může jít o IP adresu počítače, registrační značku osobního vozu, nebo tvář osoby na záznamu z kamerového systému. Je nutno zdůraznit, že v obou případech se jedná o relativní možnost identifikace pomocí osobních údajů. Například osobní údaj v podobě Jan Nový z Brna není dostatečně vypovídající o jedné konkrétní osobě, ale Jan Nový z vesnice Horní Lhota, která má 60 obyvatel je již pro konkrétní identifikace vypovídající dostatečně. Taktéž tvář narušitele zachycená na kamerovém systému bude pro majitele objektu pro identifikaci nedostatečná, pakliže se nebude jednat o například o zaměstnance.

Důležitý pojem v ochraně osobních údajů je tzv. citlivý údaj. „*Podle § 4 písm. b) OchOsÚ se pro účely tohoto zákona osobním údajem rozumí „osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů, citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů“.*[22]

[20] VIDRNA, J. a KOUDELKA, Z. *Zaměstnanci v objektivu kamer: právní aspekty monitoringu zaměstnanců* Vyd. 1. Praha: C.H.Beck, 2013. 235 s. ISBN 978-80-7400-453-7, [cit. str.64]

[21] VIDRNA, J. a KOUDELKA, Z. *Zaměstnanci v objektivu kamer: právní aspekty monitoringu zaměstnanců* Vyd. 1. Praha: C.H.Beck, 2013. 235 s. ISBN 978-80-7400-453-7, str. 64-66

[22] VIDRNA, J. a KOUDELKA, Z. *Zaměstnanci v objektivu kamer: právní aspekty monitoringu zaměstnanců* Vyd. 1. Praha: C.H.Beck, 2013. 235 s. ISBN 978-80-7400-453-7, [cit. str.66]

K výše uvedenému výčtu lze dodat, že se s velkou pravděpodobností nejedná o definitivní znění zákona, jelikož je možné, že v brzké době rozšíří o nové citlivé údaje,[23] jako jsou informace o majetkových a finančních poměrech, výši bankovního konta a morálce splácení závazků. Tyto údaje bývají vyžadovány pro bezpečnostní prověrky, případně při žádání a půjčky.

Na základě definice osobních a citlivých údajů je zřejmé, že zdravotnická dokumentace[24] patří do obou kategorií, ale převládají údaje citlivé, a tak je zdravotnická dokumentace upravena legislativně. Jedná se o § 65 z.č. 372/2011 Sb., Zákon o zdravotních službách a podmínkách jejich poskytování[25], kde je uvedeno, jaká osoba může se zdravotnickou dokumentací nakládat a jaká osoba do ní může nahlížet. Jedná se o šest okruhů osob, do kterých patří pacient, zákonný zástupce pacienta, pěstoun, osoba blízká zemřelému pacientovy, správce – tudíž zdravotničtí pracovníci, jež dokumentaci vedou, pověření zdravotničtí pracovníci, kteří nejsou zaměstnanci správce a jako poslední jsou oprávněné osoby se specifickou kontrolní pravomocí a tyto informace potřebují pro výkon své práce.

Pro další práci je nutné zmínit zúčastněné subjekty v rámci ochrany osobních údajů. Jedná se o subjekt údajů, správce a zpracovatele osobních údajů a jako poslední pověřence pro ochranu osobních údajů. Jak nám samotný název napovídá, subjekt údajů je fyzická osoba, ke které se osobní údaje vztahují. Správcem osobních údajů[26] se rozumí každý, kdo provádí zpracování osobních údajů, odpovídá za zpracování, určuje účel a prostředky zpracování. Správce může pověřit zpracováním jiný subjekt, ten se nazývá zpracovatel osobních údajů. Správce i zpracovatel může být právnická i fyzická osoba, která nejen osobní údaje pořizuje a zodpovídá za ně, ale také shromažďuje, ukládá, upravuje, pozměňuje, vyhledává, předává, šíří, uchovává, blokuje a také likviduje. Tento výčet činností obecně nazýváme zpracování osobních údajů a je popsán

[23] VIDRNA, J. a KOUDELKA, Z. *Zaměstnanci v objektivu kamer: právní aspekty monitoringu zaměstnanců* Vyd. 1. Praha: C.H.Beck, 2013. 235 s. ISBN 978-80-7400-453-7, str. 67

[24] BARTÍK, V. a JANEČKOVÁ, E. *Ochrana osobních údajů v aplikační praxi: vybrané otázky* Vyd. 3. Praha: Linde Praha, 2013.311 s. ISBN 978-80-86131-96-2, str.105

[25] ZAKONY PRO LIDI.CZ, Zdravotnická dokumentace a národní zdravotnický informační systém, [online]. 2017. Dostupné z: < https://www.zakonyprolidi.cz/cs/2011-372#cast6 >

[26] VIDRNA, J. a KOUDELKA, Z. *Zaměstnanci v objektivu kamer: právní aspekty monitoringu zaměstnanců* Vyd. 1. Praha: C.H.Beck, 2013. 235 s. ISBN 978-80-7400-453-7, str. 67

v § 4 písm. e) OchOsÚ. Dalším subjektem je pověřenec pro ochranu osobních údajů[27]. Jedná se o nový institut dle nové směrnice EU, kterou podrobněji rozvedeme v kapitole 6.5. Pověřenec pro ochranu osobních údajů bude osoba, která bude plnit roli implementátora a vnitřního auditora dodržování povinností správce nebo zpracovatele osobních údajů. Dále bude působit jako poradce pro správce a zpracovatele a současně bude kontaktní osobou spolupracující s ÚOOÚ. Pověřence budou mít za povinnost jmenovat orgány veřejné moci a organizace, jejichž hlavní činností je zpracování osobních údajů.

Nyní v logickém sledu poslední nejdůležitější pojmy ochrany osobních údajů, a to souhlas se zpracováním osobních údajů a blokace a likvidace osobních údajů. Souhlas se zpracováním osobních údajů je ustanoven v § 5 odst. 4 OchOsÚ *„Subjekt údajů musí být při udělení souhlasu informován o tom, pro jaký účel zpracování a k jakým osobním údajům je souhlas dáván, jakému správci a na jaké období. Souhlas subjektu údajů se zpracováním osobních údajů musí být správce schopen prokázat po celou dobu zpracování“.* [28]

Tento souhlas[29] musí být svobodný a vědomý projev vlastní vůle, nesmí být vynucen. Také není nutné, aby byl souhlas písemný, a je možné jej odvolat. Více se tomuto výrazu budeme věnovat v kapitole 6.5, kde nová směrnice EU tento souhlas upřesňuje.

Blokace a likvidace osobních údajů[30] jsou názvy výstižné s jasným rozdílem, ale pro úplnost je krátce přiblížíme. Blokování údajů je dočasné zastavení zpracování osobních údajů, aniž by byly likvidovány, například z důvodu chyb v databázi a hrozící porušení povinnosti zpracovávat jen přesné osobní údaje. Zatímco likvidace údajů je fyzické zničení, které podléhá nejen zákonu o ochraně osobních údajů, ale také zákonu o archivnictví a spisové službě č. 499/2004 Sb.[31]

---

[27] EPRAVO.CZ, Nařízení EU o ochraně osobních údajů – pověřenec pro ochranu osobních údajů, [online]. 2017. Dostupné z: < http://www.epravo.cz/top/clanky/narizeni-eu-o-ochrane-osobnich-udaju-poverenec-pro-ochranu-osobnich-udaju-103962.html>

[28] ZAKONY PRO LIDI.CZ, Zdravotnická dokumentace a národní zdravotnický informační systém, [online]. 2017. [cit. 2017-01-20]. Dostupné z: < https://www.zakonyprolidi.cz/cs/2000-101#cast1>

[29] VIDRNA, J. a KOUDELKA, Z. *Zaměstnanci v objektivu kamer: právní aspekty monitoringu zaměstnanců* Vyd. 1. Praha: C.H.Beck, 2013. 235 s. ISBN 978-80-7400-453-7, str. 79

[30] VIDRNA, J. a KOUDELKA, Z. *Zaměstnanci v objektivu kamer: právní aspekty monitoringu zaměstnanců* Vyd. 1. Praha: C.H.Beck, 2013. 235 s. ISBN 978-80-7400-453-7, str. 75-77

[31] ZAKONY PRO LIDI.CZ, Zdravotnická dokumentace a národní zdravotnický informační systém, [online]. 2017. Dostupné z: < https://www.zakonyprolidi.cz/cs/2004-499>

Jako poslední část této kapitoly a tématu je skutečnost, že výkonem dodržováním ochrany osobních údajů v ČR je pověřen " Úřad pro ochranu osobních údajů se sídlem v Praze, (dále jen "ÚOOÚ") ". Je to ústřední správní orgán pro oblast ochrany osobních údajů v rozsahu stanoveném zákonem č. 101/2000 Sb., a další kompetence stanovené zvláštním právním předpisem, mezinárodními smlouvami. ÚOOÚ je výkonný orgán pro dozor a kontrolu v oblasti osobních údajů. Jeho činnost plyne z mezinárodních smluv a směrnic EU, které jsou součástí právního řádu. [32]

[32] ŘÍHA, M., SIEGER, L. a PIKOLA, P. *Bezpečnostní systémy: 2.díl* Vyd. 2. Praha: Námořní akademie České republiky, 2011. 182 s. ISBN 978-80-87103-35-7, str. 134.

6 PRÁVNÍ ŘÁD ČR A OCHRANA OSOBNÍCH ÚDAJŮ

6.1 Zaměstnanci a zaměstnavatelé versus ochrana osobních údajů

Skutečnost, že ochrana osobních údajů v ČR je zakotvena ústavou ČR a zákonem o ochraně osobních údajů, jsme řešili v minulé kapitole. Jedná se o práva a povinnosti všech lidí a subjektů. Nyní bychom se letmo a stručně pokusili zaměřit na zaměstnance a zaměstnavatele, jejich vzájemný vztah v souvislosti s ochranou osobních údajů.

Zaměstnavatelé jsou oprávnění[33] dle zákoníku práce po zaměstnanci požadovat efektivní práci a chránit svůj předmět podnikání před nebezpečími jako je škoda způsobená zaměstnancem anebo přímo před trestnou činností. Zaměstnavatelé tedy mohou monitorovat a sledovat využívání pracovní doby zaměstnancem, ale také dodržování zákazu používat výrobní a pracovní prostředky pro potřebu zaměstnance bez souhlasu zaměstnavatele. Tyto oprávnění musí být v souladu s právy zaměstnance.

Práva zaměstnanců[34] v pracovním procesu jsou dána právy na ochranu soukromého a osobního života, na ochranu osobních údajů a samozřejmě jejich lidská práva, a to na ochranu listovního tajemství a tajemství dopravovaných zpráv. Práva zaměstnanců a zaměstnavatelů musí být ve vzájemné rovnováze. Tato rovnováha je dána faktem, že kontrola zaměstnance je povolena v rozsahu nezbytném k dosažení stanoveného účelu a také právem zaměstnance na vysvětlení, odstranění závadového stavu formou opravy, doplnění nebo i likvidací zpracovaných osobních údajů.

Povinností zaměstnavatele [35] jakožto pořizovatele a správce osobních údajů je opravdu mnoho, ale velmi stručně lze shrnout do konstatování, že zaměstnavatel je povinen při pořizování, shromažďování a uchovávání postupovat velmi obezřetně, aby nedošlo k jakémukoliv zneužití osobních údajů. Toto byl opravdu jen krátký popis

[33] VIDRNA, J. a KOUDELKA, Z. *Zaměstnanci v objektivu kamer: právní aspekty monitoringu zaměstnanců* Vyd. 1. Praha: C.H.Beck, 2013. 235 s. ISBN 978-80-7400-453-7, str. 83

[34] VIDRNA, J. a KOUDELKA, Z. *Zaměstnanci v objektivu kamer: právní aspekty monitoringu zaměstnanců* Vyd. 1. Praha: C.H.Beck, 2013. 235 s. ISBN 978-80-7400-453-7, str. 85

[35] VIDRNA, J. a KOUDELKA, Z. *Zaměstnanci v objektivu kamer: právní aspekty monitoringu zaměstnanců* Vyd. 1. Praha: C.H.Beck, 2013. 235 s. ISBN 978-80-7400-453-7, str. 86

vzájemného vztahu zaměstnanců a zaměstnavatelů. Podrobnějšími informacemi a novinkami se budeme podrobněji zabývat v další části práce v podkapitole o nové směrnici EU o ochraně osobních údajů.

6.2 Právní řád ČR a kamerové systémy

Lze konstatovat, že provozování kamerových systémů v České republice k dnešnímu dni není v zásadě legislativně napřímo a doslovně ošetřeno.

Výjimkou je Policie ČR, GIBS a obecní policie, konkrétně se jedná o tyto zákony:

§ 62 z.č. 273/2008 Sb., o Policii ČR, §31 z.č. 341/2011 Sb., o GIBS a § 24b z.č. 553/1991 Sb., o obecní policii.

Dle zákona 101/2000 Sb., O ochraně osobních údajů je vyžadováno registrovat veškeré sledovací kamerové systémy, ale opět s určitými výjimkami.[36] Takto formulované se to může jevit jako velmi prosté, ale samozřejmě všichni ze svých vlastních zkušeností tušíme, jak to v reálném životě s prostými věci často je. V následující podkapitole se nad tímto současným stavem budeme zamýšlet podrobněji a pokusíme se osvětlit pravý stav věci.

6.3 Ochrana osobních údajů v ČR a kamerové systémy obecně

Při nasazení kamerového systému je nutno pečlivě dbát na dodržení tří základních **povinností[37],** které Úřad pro ochranu osobních údajů velmi striktně vyžaduje.

[36] Ústav pro ochranu osobních údajů, Zákon č. 101/2000 Sb. Zákon o ochraně osobních údajů, [online]. 2017. Dostupné z: <http://www. uoou.cz/zakon-c-101-2000-sb-o-ochrane-osobnich-udaju-a-o-zmene-nekterych-zakonu-ve-zneni-ucinnem-od-1-ledna-2015/ds-3109/archiv=0&p1=1261>

[37] Ústav pro ochranu osobních údajů, Registrační formulář, [online]. 2017. Dostupné z:<http://www.uoou.cz/registracni-formular-jak-podat-oznameni-o-zpracovani-osobnich-udaju/ds1519/archiv=0&p1=1511>

1. **Registrace sledovacího systému**

   Při registraci systému jsou uznávány 3 výjimky. První výjimkou je *osobní potřeba,* druhou výjimkou je *On-line přenos bez ukládání záznamů* a poslední *ukládá-li provozování sledovacího systému zvláštní zákon, nebo je-li ho potřeba k uplatnění práv a povinností ze zvláštního zákona.*

2. **Zásadní a nezbytný je souhlas monitorovaných osob.**

   Výjimka je v § 5e zákona číslo 101/2000 Sb., kdy můžeme zpracovávat bez souhlasu monitorovaných osob, a to v případě nezbytném pro ochranu práv a právem chráněných zájmů správce, příjemce nebo dotčené osoby. Zpracování nesmí být v rozporu s právem subjektu na ochranu jeho soukromého a osobního života.

   Pokud tento souhlas není, je nasazení kamer v některých místech omezeno.

   Dle ÚOOÚ je monitoring určitých míst rizikový a komplikovaný. Jsou to místa s vysokým pohybem obyvatel, a to zejména: bytové domy (vchody a výtahy), obce a veřejné prostranství (není-li zřízena v obci obecní policie), dále školy, hotely a restaurace.

3. **Splnění informační povinnosti**

   Splnění informační povinnosti dle § 11 odstavec 1 a 2 se děje pomocí již rozšířené informační tabulky, kde se nachází piktogram kamery s popisem, že prostor je monitorován kamerovým systémem se záznamem, dále informace o správci zpracování a kontaktem na zodpovědnou osobu, které má pravomoc poskytnout o sledovacím systému podrobnější informace.

Nedodržení uvedených povinností penalizuje ÚOOÚ sankcemi již od **25 000,-Kč až do výše 5 000 000,- Kč** pro fyzické osoby a do **výše 10 000 000,- Kč pro právnické osoby** [38].

[38] ŘÍHA, M., SIEGER, L. a PIKOLA, P. *Bezpečnostní systémy: 2.díl* Vyd. 2. Praha: Námořní akademie České republiky, 2011. 182 s. ISBN 978-80-87103-35-7, str. 141

Pro majitele **bytových domů**[39] vydal ÚOOÚ v lednu 2016 dosti zásadní a očekávané stanovisko č. 1/2016 s názvem Umístění kamerových systémů v bytových domech.

V tomto stanovisku ÚOOÚ zohledňuje své dosavadní poznatky a závěry vyplývající z aktuální judikatury Nejvyššího správního soudu. Jde o částečný přelom, kdy k instalaci kamerového systému **není zapotřebí souhlasu všech nájemníků**. Kamerový systém musí sledovat jen prostory, jako jsou sklepy, půdy, vchody, garáže, kolárny, dopisní schránky, výtahy a vnější plášť budovy. Samozřejmě je nutno dbát na pečlivé nastavení kamery, aby nedocházelo ke sledování soukromí obyvatel. Sledování dveří bytů je možné pouze se souhlasem obyvatel dotčených bytů, nebo ve výjimečných a odůvodněných případech. Doba uchování by měla být 7 dní, v případě prostor s malým a příležitostným výskytem pohybu 14 dní. Všechny ostatní povinnosti zůstávají a je nutné je dodržovat.

Po přečtení shora uvedeného textu se relativně prostá věc začíná opět částečně komplikovat a nabízí se myšlenka, že ochrana osobních údajů a bezpečnostní kamerové systémy jsou dva fenomény, které jsou v opozici. A není se ani moc čemu divit, vždyť na straně legislativy se dozvídáme, že instalace a využívání kamerového systému za účelem ochrany majetku, zdraví a života plní svůj prioritní smysl tehdy, pokud správce pořizuje záznam za účelem vyhotovení důkazního materiálu, kterým je možno identifikovat pachatele trestného činu a tyto důkazy by byly použity k jeho potrestání. Pokud shromážděný záznam obsahuje fakta o trestném činu, je přirozené, že jej postižený předá orgánům činným v trestním řízení. K předání osobních údajů získaných kamerovým systémem pro účely trestního řízení existuje zákon § 89 odst. 2 trestního řádu[40], dle něhož za důkaz slouží vše, co může přispět k objasnění věci. Na druhou stranu, a to stranu ochrany osobních údajů, zjišťujeme, že možnost nebo pravděpodobnost zpracování představuje vysoké riziko pro práva a svobody fyzických osob, jako zejména diskriminace, šikany, zneužití identity, poškození pověsti, nebo mnoho dalších neprávních jednání. Z tohoto důvodu je tudíž vhodné nechat posoudit

[39]Ústav pro ochranu osobních údajů, Stanovisko č.1/2016., [online]. 2017. Dostupné z: <http://www.uoou.cz//vismo/rejstrik.asp?id_org=200144&rh=380>

[40] Zákony od centrum.cz, Trestní řád, č. 141/1961 Hlava V, dokazování, [online]. 2017. Dostupné z: <http://zakony.centrum.cz/trestni-rad/cast-1-hlava-5>

dopad na ochranu osobních údajů. Postup posouzení je následující.[41] Správce si vyžádá posudek inspektora ÚOOÚ, který řeší míru porušení ochrany osobních údajů. Patří sem hlavně situace, kdy dochází k sledování a provádění záznamu veřejných prostor. Vlastní posouzení inspektora obsahuje popis plánovaných operací, následně vyhodnocení rizik a v závěru bezpečnostní opatření a mechanismy k zajištění ochrany osobních údajů.

A co s tímto rébusem nyní? Doporučujeme pečlivě se řídit rubem i lícem pomyslné mince, a to Právním řádem, kde bych použil vše dostupné k dopadení pachatele, a samozřejmě velmi pozorně se řídit také legislativou pro ochranou osobních údajů.

Uvidíme v dalším období, jak úspěšná bude v praxi nová směrnice EU a případně jak se bude k legislativě přihlížet na základě nedávných teroristických útoků. Zda se bude více brán zřetel na bezpečnost nebo na možné zneužití záznamů z bezpečnostních kamer a systémů?

6.4 Ochrana osobních údajů a využívání MKDS

MKDS musí monitorovat pouze veřejná prostranství. Obrazový signál není určen pro veřejnost, ale jen pro určité uživatele a pouze pro vymezený účel. Tito uživatelé jsou vyškolení příslušníci Policie ČR, a zaměstnanci obecní policie, kteří mají ve smyslu svých zákonů a zákona č.101/2000 Sb. §5odst. 2 písm. e) tzv. právní titul k některým ustanovením o ochraně osobních údajů.

Nyní bychom se abstraktně opřeli o novelu č.170/2007 Sb.[42]ze dne 7. 6. 2007, jejíž význam je dle mne určující a vypovídající o vzájemné interaktivitě MKDS a UOOU.

[41] Ústav pro ochranu osobních údajů, Zákon č. 170/2007 Sb. Zákon o ochraně osobních údajů, [online]. 2017. Dostupné z: < https://www.uoou.cz/kontrolni-cinnost-inspektoru/ds-1279/archiv=0&p1=1277 >

[42] Ústav pro ochranu osobních údajů, Zákon č. 170/2007 Sb. Zákon o ochraně osobních údajů, [online]. 2017. Dostupné z: <https://www.uoou.cz/zmeny-zakona-o-ochrane-osobnich-udaju/ds-3112/p1=3112>

Provozovatel kamerového systému musí mít jasno ve třech určujících bodech:

- Je náš záměr legitimní?
- Můžeme tohoto záměru dosáhnout jiným způsobem?
- Je třeba určit účel, správce dat, zabránit zneužití dat a jejich ochranu.

Jestliže jsou výše uvedené body zcela a jednoznačně vyřešeny a podepřeny zákonnými prostředky, mělo by být vše v pořádku a nic a nikdo by neměl bránit nasazení kamerového systému. A ačkoliv je mnoho sporů a ještě více odpůrců této technologie, tak pro osoby dodržující a ctící zákony je důležitá skutečnost zjevná po přečtení § 89 odst. 2 trestního řádu, podle něhož za důkaz může sloužit vše, co může přispět k objasnění věci.

Při povinnosti MKDS monitorování pouze veřejného prostranství bude skoro vždy docházet k tomu, že část záběru kamery bude v rozporu s ochranou osobních údajů (okno, balkón, vchod atp.), ale toto se legitimně řeší technickým prostředkem – funkcí kamery, a to maskováním privátních zón. To znamená, že na kameře se pomocí softwarové aplikace zakáže určitá část obrazu a vše je v pořádku.

6.5 Nové nařízení EU o ochraně osobních údajů

V květnu 2016 bylo přijato NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)[43]. Tato nařízení jsou závazná v celém rozsahu a použitelná ve všech členských státech s účinností od května 2018.

Nyní bychom se pokusili stručně nastínit pozitiva a negativa nové směrnice a to za pomoci článku advokátní kanceláře Taylor Wessing Praha[44] . Tato směrnice nám stanovuje práva a povinnosti, která náleží fyzickým osobám, jejichž osobní údaje jsou

[43] EUR-Lex, Nařízení evropského parlamentu a rady (EU) 2016/679, [online]. 2017. Dostupné z: <http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32016R0679>

[44] FEEDIT.CZ, Nové nařízení EU o ochraně osobních údajů. Jak se dotkne České republiky?, [online]. 2017. Dostupné z: <http://www.feedit.cz/wordpress/2016/03/21/nove-narizeni-eu-o-ochrane-osobnich-udaju-jak-se-dotkne-ceske-republiky/>

zpracovávány. Současně logicky stanovuje práva povinnosti subjektů, které údaje zpracovávají nebo za jejich zpracování zodpovídají.

Nově jsou posílena práva fyzických osob, jejichž osobní údaje jsou zpracovávány. Je kladen důraz na to, aby byly zpracovávány skutečně jen údaje nezbytně potřebné. Dále fyzické osoby, jejichž údaje jsou zpracovávány, mají právo být zapomenuty, zejména pokud zpracovávané údaje již nejsou potřebné. Nově má subjekt údajů oproti stávajícím normám právo na přenositelnost svých osobních údajů. V praxi tedy znamená, že pokud se osobní údaje zpracovávají elektronicky, ve strukturovaném a standardně používaném formátu, má subjekt údajů právo na získání kopie zpracovávaných údajů v elektronické podobě.

Naopak směrnice nařizuje subjektům, které záznamy pořizují, aby pořizovali záznamy, které skutečně nezbytně potřebují. Také nařizuje maximální snahu eliminovat rizika spojená se zneužitím, neoprávněným přístupem a také neoprávněným zveřejněním osobních údajů.

Další zásadní změna je povinnost zaměstnavatelů s více než 250 zaměstnanci nebo subjektů, jejichž hlavní činnost spočívá ve zpracování osobních údajů, mít vlastního inspektora ochrany údajů.

Velmi důležitá novinka je také povinnost vést dokumentaci o zpracovávaných údajích. Zde je povinnost tuto dokumentaci na požádání předložit kontrolnímu orgánu. Povinnost provádět posouzení dopadu na ochranu údajů z hlediska práv a svobod subjektů údajů je dalším zásadním prvkem v nové směrnici. A taktéž již zmiňovaný pověřenec pro ochranu osobních údajů.

Kontroverzní bod směrnice je zcela jistě část, ve které se hovoří o odpovědností uloženou správcům údajů, kde souhlas sledovaných subjektů nevytváří právní základ ke zpracování údajů. Jedná se o případy, kdy mezi osobou poskytující své údaje a jejich správcem vzniká významná nerovnováha. V praxi to znamená, že správce údajů vlastně neví, zda se pohybují v mezích legislativy či nikoliv i přes souhlas dotyčné osoby.

Z pohledu administrativy zde vzniká nárůst prováděcích aktů a formulářů, a tím i další zvýšení nákladů a administrativních procesů spojených se zpracováním dat a osobních údajů.

Nařízení klade velký důraz, nebo spíše doporučení, aby jednotlivci i právní subjekty ve veškeré elektronické komunikaci dbali, jak a komu sdělují své osobní údaje, protože dodržování nařízení nelze vymáhat po subjektech mimo území EU a samozřejmě po subjektech, které svou identitu cíleně skrývají.

Směrnice zavádí mnohem tvrdší sankce za jakékoliv porušování pravidel a zákonů o ochraně osobních údajů, než tomu bylo do současnosti. V případě, že zpracovatel údajů poruší pravidla pro ochranu údajů, může mu být udělena pokuta až do výše 20 milionů eur nebo až 4 % z celkového ročního obratu subjektu. Tyto sankce však lze uplatnit jen pro subjekty, které jsou v pravomoci evropských kontrolních orgánů.

Je pravdou, že jako v mnoha jiných případech tak i v tomto nařízení je naše stávající legislativa přísnější než evropská a z velké části je již řadu let uplatňováno to, co EU řeší až nyní. Opravdu ukázkový příklad a pro mne ne zcela pochopitelný je smlouva mezi správcem a zpracovatelem osobních údajů, kde ČR celkem logicky požaduje uzavření v psané formě. Naproti tomu nová směrnice nabízí možnost smlouvy také v elektronické podobě, ale co je zarážející bez požadavku na elektronický podpis.

Na závěr této kapitoly si dovolíme vlastní názor a to ve světle a stínu posledních událostí uprchlické krize a zejména nedávných teroristických útocích ve Francii a v Německu. Doufáme, že touto směrnici je položen nový základ ochraně osobních údajů nejen u nás, ale v celé Evropské unii. Kamerové systémy budou i nadále sloužit k ochraně nás a naší společnosti. Kdybychom se zeptali přímých účastníků atentátů anebo pozůstalých po obětech, kteří neměli to štěstí, že přežili, co by nám řekli? Určitě by chtěli předejít těmto strašným zločinům a odvrátit strach, hrůzu, bolest a smrt svých bližních.

7 SVOBODA A SOUKROMÍ

Jako motto této kapitoly se nám přímo nabízí slova Benjamina Franklina *„kdo se chce vzdát svobody, aby získal bezpečnost, nebude mít ani jedno, ani druhé. A ani si je nezaslouží“*.

Ze samotné historie lidstva je nám známo, že svoboda a soukromí jsou pro člověka natolik důležité, že při obraně své svobody a soukromí často porušujeme svobodu druhých. Svoboda a právo na soukromí patří mezi naše nejcennější práva. Svoboda je v nejširším slova smyslu možnost dělat si co chci, rozhodovat o sobě, mít možnost volby a za svá rozhodnutí nést odpovědnost. Jednoduše řečeno být svým vlastním pánem. Nepředpokládáme, že by bylo nutné podrobně rozebírat všechny dokumenty, ústavy a mezinárodní dohody, kde se o svobodě a soukromí píše. Tím není myšleno, že by to bylo nezajímavé, nebo pro naši práci nepodstatné, ale podrobněji rozebrat LZPS nebo Úmluvu o ochraně lidských práv a základních svobod by rozhodně překročilo stanovený rozsah a téma této práce. Ale dovolte nám využít názoru, že svobodu lze chápat také jako negativní a pozitivní.[45] Politik a filozof Isaiah Berlin (1909-1997) pojem svobody rozdělil na negativní svobodu, která pro něj představovala prostor, ve kterém si člověk může dělat, co uzná za vhodné bez zásahu druhé osoby, a na pozitivní svobodu, kterou definoval, kdo nebo co kontroluje a řídí člověka, jakým člověk má být a co má dělat. Jinými slovy negativní svoboda je ovlivňována vnějšími faktory jednání, respektive možností výběru a pozitivní svoboda vnitřními faktory jednání, neboli jestli má člověk své jednání pod svou vlastní kontrolou. Tato myšlenka nás velmi zaujala v souvislosti se světem internetu a pokusíme se ji více rozvést v následující kapitole o rizikách zneužívání osobních údajů.

Jak napovídá název této kapitoly tak pojem svoboda je jednoznačně velmi úzce spojen s pojmem soukromí a s právem na soukromí.[46] Pojem soukromí nemá

[45] ŠIMÍČEK, V. *Právo na soukromí* Vyd. 1. Brno: Masarykova univerzita, 2011.212 s. ISBN 978-80-210-5449-3, str. 37-39

[46] ŠIMÍČEK, V. *Právo na soukromí* Vyd. 1. Brno: Masarykova univerzita, 2011.212 s. ISBN 978-80-210-5449-3, str. 11-14

jednoznačně vypovídající definici, protože pojem je velmi široký a dynamický, tím je myšleno, že se vyvíjí v průběhu lidských dějin. Jiný význam měl pojem soukromí v pojetí francouzského krále, který vykonával úkony ranní hygieny před šlechtou při státnickém jednání, jiný v době socialismu a zcela jiný je i dnes. Také určitá vyspělost civilizace, tradice, náboženství a etika mají zásadní vliv na význam slov soukromí a svoboda. Stejně tak právní pohled na soukromí v jednotlivých právních kulturách. Jinak na pojem soukromí hledí kontinentální a jinak právo v muslimských zemích.

Pojem soukromí není v naší legislativě přímo definován. Právo na soukromí je samozřejmě definováno a patří mezi nezcizitelná a nezadatelná práva ty jsou ukotvena v naší LZPS v článku 7 odst. 1 *„Nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem.“* [47] A další aspekty spojené se soukromím v článku 10 odst. 2 *„Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.“*[48] A samozřejmě nejen zde, ale i v dalších částech se přímo či nepřímo hovoří o soukromí, jedná se o politická práva a svobody, právo vlastnit majetek. V problematice soukromí také hovoříme o kruhu soukromí[49]. Tyto kruhy představují z pohledu soukromí určité hranice soukromého života:

- kruh veřejných osob, končí na hranicích veřejnosti, jedná se o veřejné osoby a to nejen politiky, ale také o osoby veřejně známé a veřejně vystupující,
- kruh soukromých osob, součástí jsou i vztahy na pracovišti,
- rodinný kruh, rodinné vztahy,
- kruh intimní, to je záležitost tak říkajíc jen mne a nikoho jiného ani rodiny.

Z pohledu vztahu svobody, soukromí a ochrany osobních údajů je pro nás zajímavý zejména kruh osobních osob a rodinný kruh. Je logické, že soukromý život veřejně

[47] POSLANECKÁ SNĚMOVNA PARLAMENTU ČESKÉ REPUBLIKY, Usnesení o vyhlášení LZPS, [online]. 2017. [cit. 2017-01-19]. Dostupné z: < http://www.psp.cz/docs/laws/listina.html>

[48] POSLANECKÁ SNĚMOVNA PARLAMENTU ČESKÉ REPUBLIKY, Usnesení o vyhlášení LZPS, [online]. 2017. [cit. 2017-01-19]. Dostupné z: < http://www.psp.cz/docs/laws/listina.html>

[49] ŠIMÍČEK, V. *Právo na soukromí* Vyd. 1. Brno: Masarykova univerzita, 2011.212 s. ISBN 978-80-210-5449-3, str. 15-17

známé osoby bude diametrálně jiný v mnoha aspektech než život dělníka v továrně. A také kromě exhibionistů nebo jinak psychicky nemocných lidí, nebude mít nikdo z nás potřebu veřejnosti sdělovat nebo odhalovat svou intimitu.

Za předpokladu, že žijeme svobodně a s garantovanou ochranou soukromí, tudíž v demokratickém zřízení, kde tedy mám možnost výběru a své jednání pod kontrolou, tak si mohu také zvolit, jakým způsobem se prezentuji před okolím, jak se chovám v soukromí a jakým způsobem si své soukromí chráním. Tím, že mám možnost volby a mohu si zvolit, jakým způsobem si chci zachovat svobodu, aniž bych přišel o bezpečí. Tímto bychom mohli navázat na odkaz Benjamina Franklina a konstatovat, že o svobodu, bezpečnost, soukromí je třeba neustále pečovat. Zejména ve složitostech dnešní internetové doby je jednoduše potřeba se pojmu soukromí začít znovu učit.

8 KLADY A ZÁPORY MONITORINGU

8.1 Skryté hrozby sledování v kyberprostoru

Současná doba je nazývána nejen dobou globalizace, ale stále více věkem internetu a sociálních sítí. Tyto výdobytky nám přinášejí rychlé informace, usnadnění komunikace, zjednodušení práce, poskytování nových druhů služeb, ale i hrozby v případě neopatrného a nezodpovědného chování v kyberprostoru.

Za naše pohodlí a blahobyt platíme relativně vysokou daň, a to ve větší či menší míře ztrátou soukromí ve formě toho, že jsme sledování. Způsobů je mnoho, můžeme začít pouhou věrnostní kartou do velkoobchodu, z které správce osobních údajů získá nejen základní informace, ale i o to co a za kolik člověk nakupuje. Různé speciální SW aplikace, které monitorují náš pohyb v kyberprostoru zaznamenávající navštívené stránky a mailovou komunikaci, zapnutý mobil monitorující náš pohyb, různé WiFi sítě, které si pamatují vaše údaje, GPS signál našeho automobilu, kamerové systémy a nahrávání telefonních hovorů. Samozřejmě všechny tyto výdobytky moderní doby nám slouží v mnoha ohledech, včetně bezpečnosti a objasňování trestných činů, což je samozřejmě v pořádku. Ano, toto vše nám slouží, je to tedy dobrý sluha, ale zlý pán, a to v případech kdy se s těmito technologiemi nakládá nezodpovědně a v rozporu se zákony. Asi by se zodpovědný člověk divil kolik lidí má svůj PIN ke kreditní kartě nalepen přímo na pouzdru karty a ještě více lidí má k přístupu do svých mailových schránek velmi odolná hesla typu: 123456789. Kupodivu mnoho dalších zařízení jako jsou WiFi routery, web kamery mají stále defaultní login a heslo: admin, admin. Není proto divu, že se v posledních letech rozrostly řady počítačových zločinců, když jim my sami takto nabízíme levnou obživu v podobě zcizení peněz z účtu, vydírání ohledně hackerem zablokovaného účtu nebo počítače, zcizení různých dokumentů nebo intimních fotografií. Do tohoto výčtu hrozeb pro jednotlivce je bohužel nutno připočítat i kybernetické útoky vedené mezi státy, které mohou ohrozit tak křehkou stabilitu mezinárodních vztahů. Mám na mysli například nedávný případ ovlivnění amerických voleb. Tyto hrozby a nebezpečí jsou většinou dílem naši nepozornosti, ledabylosti nebo

lehkovážnosti a záleží jak na jednotlivcích a jejich přístupu ke kybernetické bezpečnosti, tak na opatřeních ze strany organizací a států s důrazem na kontrolu a prevenci dodržování pravidel v kyberprostoru.

Další a neméně závažné nebezpečí kyberprostoru je právem spatřováno v sociálních sítích[50]. Sociální sítě skýtají velký prostor pro škodlivé a nebezpečné jevy. Jedná se zejména o kyberšikanu, kybergrooming, sexting, kyberstalking. Vzhledem k nemožnosti ověřit pravdivost údajů o uživatelích dochází k situacím, kdy uživatel uvede jinou totožnost včetně fotografie a využije důvěřivosti uživatelů, kteří pak svolí k osobní schůzce (tzv. kybergrooming). To, že již několik schůzek skončilo tragicky, je bohužel smutná realita. Pravdivost informací v sociálních sítích není věrohodná ani ověřitelná. Bohužel výzkumy dokazují, že 42,5 % dětí je ochotno svolit ke schůzce s člověkem, kterého znají jen ze sociální sítě. Dalším neblahým jevem je kyberšikana, sloužící jako nástroj pomsty a nactiutrhání, kde pomocí diskusní skupiny nebo falešného profilu oběti je oběť urážena a zesměšňována. Časté k tomuto účelu zneužívají ukradené nebo upravené fotografie uživatele. Bez sociálních sítí si větší část moderní společnosti bohužel neumí představit dnešní ani budoucí svět. Jelikož žijeme v naší uspěchané konzumní společnosti, tak člověk vytváří nové virtuální vztahy a částečně udržuje své staré a stávající společenské vztahy.

Sociální sítě jsou fenomén dnešní doby s návykovým vlivem na populaci. Pomocí informací, které uživatelé vkládají, a to nejen osobních údajů a fotek, ale také informacích o tom kde, kdy a s kým jsou a budou, sami sebe monitorují a tyto informace často veřejně předkládají na pospas široké skupině uživatelů těchto sítí. A tak říkajíc jdou sami naproti mnoha možným problémům, které jsme popisovali, včetně odcizení identity nebo těch nejhorších zločinů proti životu a zdraví. Opravdu ukázkovým příkladem je incident při udílení cen Zlatého Slavíka, kdy zpěvák Radek Banga na protest odešel z ceremoniálu, a následně vyjádřil na sociální síti protest proti

[50]SOCIÁLNÍ SÍTĚ, Nebezpečí sociálních sítí, [online]. 2017. Dostupné z: < http://www.socialnisite.estranky.cz/clanky/nebezpeci-socialnich-siti.html>

ocenění zpěváka skupiny Ortel[51]. Poté se strhla na sociálních sítích diskuze, která bohužel vyústila ve vyhrožování pomstou a smrtí zpěvákovi a jeho rodině.

Nyní použijeme teorii o svobodě Isaiaha Berlina z předcházející kapitoly, a to pohledem negativní a pozitivní svobody. Lze konstatovat, že v kyberprostoru svým jednáním, které máme pod svou vlastní kontrolou, a možností výběru jsem strůjcem své svobody, soukromí a bezpečnosti.

8.2 Rizika zneužití a využití monitoringu

O zneužití a možnostech trestné činnosti v oblasti obecného kyberprostoru jsme hovořili na předchozích stránkách. Nyní bychom se zaměřili na monitoring ve smyslu špionáž, odposlechy, organizovaná zločin a terorismus. Z historie je velmi dobře známo, že mezinárodní a průmyslová špionáž není nic nového. V době války je špionáž součástí válečné strategie, a dnes bohužel i v dobách míru. Asi každý z nás tuší, že naše veškerá komunikace je zaznamenávána a je prováděna diagnostika jejího obsahu. Reprezentativním příkladem hovořící za vše je případ Edwarda Snowdena,[52] který v květnu 2013 vynesl informace z národní bezpečnostní agentury NSA, kde pracoval jako technik. Jednalo se o skutečnost, že USA pomocí utajené operace s názvem PRISM[53] sleduje, sbírá a analyzuje informace a internetovou komunikaci z celého světa. Vše probíhá pomocí specializovaných agentů, kteří mají přístup na servery spolupracujících firem. Mělo se jednat o firmy Google, Apple, Microsoft, Yahoo, Facebook, v podstatě o většinu gigantů v oboru. Toto sledování je postaveno na základě strojové analýzy a následné kontroly specialistů z NSA. Cílem této operace je odhalování terorismu, mezinárodnímu zločinu a hrozeb proti USA. Edward Snowden toto odhalil, protože

[51] IDNES.CZ, Banga za protest proti Ortelovi čelí rasistickým nadávkám i výhružkám smrt, [online]. 2017. Dostupné z: < http://zpravy.idnes.cz/radek-banga-vyhruzky-tomas-ortel-cesky-slavik-gipsy-cz-pgr-/domaci.aspx?c=A161129_110614_domaci_fer>

[52] IDNES.CZ, Je Snowden zrádce, nebo hrdina? Cítím se nevinen, ale obětuji se, říká, [online]. 2017. Dostupné z: <http://technet.idnes.cz/snowden-amnestie-obama-petice-d2w-/sw_internet.aspx?c=A160916_143544_sw_internet_pka>

[53] IDNES.CZ, USA přiznaly šmírování. Tajná NSA sbírá soukromá data z celého světa, [online]. 2017. Dostupné z: <http://technet.idnes.cz/nsa-fbi-sledovani-prism-usa-soukromi-data-f15-/sw_internet.aspx?c=A130607_065544_hw_monitory_pka>

nechtěl žít ve světě bez soukromí. Snowden také odhalil, že proti sledování není v tomto případě obrany. Pro někoho se stal zrádcem, který ohrozil USA, a pro někoho hrdinou bojujícím za svobodu a soukromí. Nebudeme se přiklánět ani k jednomu názoru, jelikož to není jednoduché rozsoudit, ale je docela dobře možné, že pravda bude někde uprostřed, tak jak to často bývá ve složitých otázkách. Otázkou zůstává, proč součástí této špionáže byli i státníci a politici spřátelených zemí, včetně největšího spojence USA, a to Německa?

Je jasné, že obdoba tohoto monitoringu, nebo vlastně špionáže je všude na světě, a to nejen ohledně elektronické komunikace, ale také telefonní komunikace. V demokratických zřízeních se toto děje, nebo mělo dít na vyžádání, na základě např. soudního příkazu. Pravdou zůstává, že pomocí odposlechů, kontroly elektronické pošty, případně další komunikace se daří bojovat s organizovaným zločinem a terorismem, což je zásadní problém naší doby.

ZÁVĚR

Cílem práce bylo zmapovat a přiblížit ochranu osobních údajů nejen obecně, ale také v přímé souvislosti s ochranou osob a majetku. A v této souvislosti se zaměřit na možnosti zneužití osobních údajů v současném světě.

Práci jsme zahájili kapitolou o ochraně osob a majetku, kde jsme uvedli možné způsoby a rozdělení ochrany osob. Na pozadí historického vývoje technologií jsme demonstrovali vazby mezi technikou a bezpečností, a to konkrétně na kamerových systémech. Na časové ose jsme zjistili, že kamerové systémy se vyvíjejí technologicky opravdu velmi rychle, bohužel pro nás i úměrně rychle k současné neustále se zhoršující bezpečnostní situaci ve světě. Pro další část práce bylo nezbytně nutné definovat nové a důležité pojmy z oboru fyzicko-technologické bezpečnosti, abychom měli aktuální přehled o moderních technologiích a trendech v oboru. V této chvíli jsme se z důvodu aktuálnosti tématu a stupňujících se teroristických útocích zaměřili na Městské kamerové systémy. Řešili jsme, kde a za jakých podmínek je vhodné a důležité je nasadit. Neopomněli jsme důležitou funkci operátora MKDS, jeho možnosti, práva, povinnosti a také podmínky, za kterých se člověk může operátorem stát. Zjistili jsme, že je to práce náročná a zodpovědná a pro větší efektivitu je ji potřeba podpořit novou technologií v podobě pokročilé inteligentní video-analýzy. Na jednotlivých funkcích jsme se snažili popsat nejen stávající, ale i další možné využití v situační prevenci kriminality, v předcházení protiprávního jednání, ale také v objasňování trestné činnosti.

Abychom podpořili smysl nových technologií pro ochranu osob, tak jsme v dalším kroku zkoumali interaktivitu bezpečnostních technologií s prevence kriminality a se Strategií prevence kriminality ČR. Nebylo překvapením, že kamerové systémy patří mezi pilíře situační prevence. Avšak na základě studie s názvem Vyhodnocení účinku kamerových systémů z roku 2007 bylo nepatrně překvapením, že tehdejší výsledky této studie nejsou jednoznačné a ani vyloženě optimistické. Na druhou stranu jsem velmi laickým matematickým pokusem na základě číselného poměru finančně vyčíslené škody TČ s částkou investovanou do MKDS došli k závěru více než uspokojivému, a to i přes velkou nepřesnost tohoto výsledku. V rámci tohoto tématu jsme zmínili i další zajímavá čísla a finanční částky, ale i další části Strategie prevence kriminality.

Můžeme-li hodnotit bezpečnostní kamerové systémy a zvláště MKDS, postupem času zastávají nedílnou součást prostředků policie pro prevenci, odhalení a následné vyhodnocení trestného činu. Přispívají k dlouhodobému snižovaní trestné činnosti, a proto mohu bez nadsázky konstatovat, že v ČR se na základě Strategie prevence kriminality daří plnit vytčené cíle a MKDS k tomuto výsledku významnou částí přispívají.

V úplném závěru první části práce o ochraně osob jsme letmo a v duchu dnešní doby řešili efektivitu, nákladovost, životnost a možnosti modernizace bezpečnostních systémů. Zde jsme došli k závěru, že nasazení technologií musí být účelné a efektivní. A aby byl bezpečnostní systém efektivní, měl by být schopný modernizace, rozšiřování, a tím pádem bude jeho životnost vysoká. Ostatně to bychom chtěli po všech technických prostředcích.

Následně jsme se věnovali ochraně osobních údajů, Právnímu řádu ČR, svobodě, soukromí a monitoringu. Zde jsme se opírali jak jinak než o Zákon o ochraně osobních údajů, o novou směrnici EU o ochraně osobních údajů a dalších aspektech Právního řádu ČR. Zvýšená pozornost byla věnována postoji právního řádu ke kamerovým systémům a postoji úřadu pro ochranu osobních údajů ke kamerám obecně, kde jsme zvažovali výhody a nevýhody jejich využití.

V druhé části práce jsme řešili možnosti a rizika spojená se zneužitím osobních údajů a současné kauzy spojené se zneužitím osobních údajů. V souvislosti s osobní svobodou a soukromím jsme poukazovali na nebezpečnost dnešní internetové doby a rizikovost fenoménu sociálních sítí. Bylo nutné upozornit, že ochrana osobních údajů v kybernetickém prostoru je z velké části v rukou jednotlivce a je přímo úměrná jeho zodpovědnému chování nejen ve světě internetu a sociálních sítí, ale v celkovém přístupu k ochraně sebe a své rodiny a svého soukromí.

Kdybychom měli hodnotit a srovnávat tak zřejmě nejvýstižněji citátem anglického filosofa a politika Johna Stuarta Milla *"Svoboda jednoho končí tam, kde začíná svoboda druhého."*. Jen bude více obtížné shodnout se na pomyslné hranici jednotlivých subjektů. Technicky a legislativně zřejmě ve většině případů hranici odvodíme, ale co vyšší princip, který je často v dnešní době přehlušen ne vždy dokonalými zákony? To je otázka, s kterou si budeme muset poradit každý sám. Výsledkem našeho snažení je také fakt, že znalý a schopný člověk je základním zdrojem efektivity bezpečnostních systémů, ale i efektivity a přístupu k ochraně osobních údajů. Technické prostředky na vysoké úrovni mu k tomu dopomáhají,

pakliže s touto technikou zodpovědně a odborně zachází, pak je minimalizováno i zneužití osobních údajů. Je nutné pracovat s lidským faktorem, jakožto nejslabším článkem tohoto řetězu.

Otázkou je, jakým směrem půjde společnost ve vývoji, jak a v jaké míře bude potřebný i vývoj bezpečnostních systémů a jakým způsobem bude prováděna a dodržována ochrana osobních údajů. Bylo by opravdu skvělé a úžasné, kdyby bezpečnostních systémů nebylo zapotřebí, ale na to lidstvo není bohužel připraveno.

Toto byla obecná úvaha o ochraně osobních údajů a ochraně osob. Dle našeho názoru je stále větší povinností ještě více ochraňovat naše společensky chráněné zájmy s maximálním využitím všech prostředků a legitimních předpisů.

SEZNAM POUŽITÝCH ZDROJŮ

Seznam použitých českých zdrojů

- BARTÍK, Václav a JANEČKOVÁ, Eva. *Ochrana osobních údajů v aplikační praxi: vybrané otázky* Vyd. 3. Praha: Linde Praha, 2013.311 s. ISBN 978-80-86131-96-2
- ŘÍHA, Milan, SIEGER, Ladislav a PIKOLA, Pavel. *Bezpečnostní systémy: 1.díl* Vyd. 4. Praha: Námořní akademie České republiky, 2011. 182 s. ISBN 978-80-87103-32-6
- ŘÍHA, Milan, SIEGER, Ladislav a PIKOLA, Pavel. *Bezpečnostní systémy: 2.díl* Vyd. 2. Praha: Námořní akademie České republiky, 2011. 182 s. ISBN 978-80-87103-35-7
- ŠIMÍČEK, Vojtěch. *Právo na soukromí* Vyd. 1. Brno: Masarykova univerzita, 2011.212 s. ISBN 978-80-210-5449-3
- VIDRNA, Jan a KOUDELKA, Zděnek. *Zaměstnanci v objektivu kamer: právní aspekty monitoringu zaměstnanců* Vyd. 1. Praha: C.H.Beck, 2013. 235 s. ISBN 978-80-7400-453-7
- VOMÁČKA, Jaromír, MIKULA, Tomáš, VEINER, Zděnek a RANDA, Martin. *IP CCTV Guideline -„Průvodce návrhem síťového videa“* Vyd. 1. Praha: Calamarus, 2011.

Seznam použitých zahraničních zdrojů

- HILL, Martin a SPRIGSS, Angela. *Vyhodnocení účinku kamerových systémů* Vyd. 1. Praha: Institut pro kriminologii a sociální prevenci, 2007. ISBN 978-80-7338-061-8

Seznam použitých internetových zdrojů

- COLSYS, VoiceGuard – varovný a informační systém, [online]. 2017. Dostupné z: < http://www.colsys.cz/voiceguard-varovny-a-informacni-system/>

- ČESKÁ TELEVIZE, Technický vývoj televize v datech a souvislostech, [online]. 2016. [cit. 2016-12-19]. Dostupné z: < http://www.ceskatelevize.cz/vse-o-ct/historie/televizni-technika/technicky-vyvoj-televize-v-datech-a-souvislostech >
- EGOVERNMENT, Ostře sledovaná města, kamerové systémy, [online]. 2016. Dostupné z: < http://www.egovernment.cz/kamery/kamery%2006.htm >
- EPRAVO.CZ, Nařízení EU o ochraně osobních údajů – pověřenec pro ochranu osobních údajů, [online]. 2017. Dostupné z: < http://www.epravo.cz/top/clanky/narizeni-eu-o-ochrane-osobnich-udaju-poverenec-pro-ochranu-osobnich-udaju-103962.html>
- EUR-Lex, Nařízení evropského parlamentu a rady (EU) 2016/679, [online]. 2017. Dostupné z: <http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32016R0679>
- FEEDIT.CZ, Nové nařízení EU o ochraně osobních údajů. Jak se dotkne České republiky?, [online]. 2017. Dostupné z: <http://www.feedit.cz/wordpress/2016/03/21/nove-narizeni-eu-o-ochrane-osobnich-udaju-jak-se-dotkne-ceske-republiky/>
- HOSPODÁŘSKÉ NOVINY, Biometrie v Čechách, [online]. 2017. Dostupné z: < http://life.ihned.cz/c1-63229990-biometrie-v-cechach>
- IDNES.CZ, Banga za protest proti Ortelovi čelí rasistickým nadávkám i výhružkám smrt, [online]. 2017. Dostupné z: < http://zpravy.idnes.cz/radek-banga-vyhruzky-tomas-ortel-cesky-slavik-gipsy-cz-pgr-domaci.aspx?c=A161129_110614_domaci_fer>
- IDNES.CZ, Je Snowden zrádce, nebo hrdina? Cítím se nevinen, ale obětuji se, říká, [online]. 2017. Dostupné z: <http://technet.idnes.cz/snowden-amnestie-obama-petice-d2w-/sw_ internet.aspx?c=A160916_143544_sw_internet_pka>
- IDNES.CZ, USA přiznaly šmírování. Tajná NSA sbírá soukromá data z celého světa, [online]. 2017. Dostupné z: http://technet.idnes.cz/nsa-fbi-sledovani-prism-usa-soukromi-data-f15-/sw_internet.aspx?c=A130607_065544_hw_monitory_pka
- IPSECURITY,Videoanaytics [online]. 2016.Dostupné z: < http://videoanalytics.cz/# >
- MINISTERSTVO VNITRA ČESKÉ REPUBLIKY, Dotační systém prevence kriminality[online]. 2016. Dostupné z:< http://www.mvcr.cz/clanek/pilotni-projekt-bezpecna-lokalita-bezpecne-bydleni-se-rozjizdi-v-brne-a-ve-zline.aspx >

- MINISTERSTVO VNITRA ČESKÉ REPUBLIKY, Dotační systém prevence kriminality[online]. 2017. Dostupné z: < http://www.mvcr.cz/clanek/web-o-nas-prevence-prevence-kriminality.aspx>
- NOVINKY.CZ, Atentát v Nice, [online]. 2017. Dostupné z: < https://tema.novinky.cz/atentat-v-nice >
- NOVINKY.CZ, V Německu kvůli hrozbě teroru přibude kamer. Téměř všude, [online 2016. Dostupné z: < https://www.novinky.cz/zahranicni/evropa/424337-v-nemecku-kvuli-hrozbe-teroru-pribude-kamer-temer-vsude.html>
- POLICIE ČESKÉ REPUBLIKY, Počet objasněných případů stoupá[online]. 2017. [cit. 2017-01-18]. Dostupné z: < http://www.policie.cz/clanek/pocet-objasnenych-pripadu-stoupa.aspx>
- POSLANECKÁ SNĚMOVNA PARLAMENTU ČESKÉ REPUBLIKY, Usnesení o vyhlášení LZPS, [online]. 2017. [cit. 2017-01-19]. Dostupné z: < http://www.psp.cz/docs/laws/listina.html>
- SOCIÁLNÍ SÍTĚ, Nebezpečí sociálních sítí, [online]. 2017. Dostupné z: < http://www.socialnisite.estranky.cz/clanky/nebezpeci-socialnich-siti.html>
- TRIVIS a.s., Vzdělávací kurzy, [online]. 2017. Dostupné z: <http://www.trivis.cz/kurzy>
- Ústav pro ochranu osobních údajů, Registrační formulář, [online]. 2017. Dostupné z:<http://www.uoou.cz/registracni-formular-jak-podat-oznameni-o-zpracovani-osobnich-udaju/ds1519/archiv=0&p1=1511>
- Ústav pro ochranu osobních údajů, Stanovisko č.1/2016., [online]. 2017. Dostupné z: <http://www. uoou.cz//vismo/rejstrik.asp?id_org=200144&rh=380>
- Ústav pro ochranu osobních údajů, Zákon č. 101/2000 Sb. Zákon o ochraně osobních údajů, [online]. 2017. Dostupné z: <http://www. uoou.cz/zakon-c-101-2000-sb-o-ochrane-osobnich-udaju-a-o-zmene-nekterych-zakonu-ve-zneni-ucinnem-od-1-ledna-2015/ds-3109/archiv=0&p1=1261>
- Ústav pro ochranu osobních údajů, Zákon č. 170/2007 Sb. Zákon o ochraně osobních údajů, [online]. 2017. Dostupné z: < https://www.uoou.cz/kontrolni-cinnost-inspektoru/ds-1279/archiv=0&p1=1277 >
- Ústav pro ochranu osobních údajů, Zákon č. 170/2007 Sb. Zákon o ochraně osobních údajů, [online]. 2017. Dostupné z: <https://www.uoou.cz/zmeny-zakona-o-ochrane-osobnich-udaju/ds-3112/p1=3112>

- Zákony.centrum.cz, Trestní řád, č. 141/1961 Hlava V, dokazování, [online]. 2017. Dostupné z: <http://zakony.centrum.cz/trestni-rad/cast-1-hlava-5>
- ZAKONY PRO LIDI.CZ, Zdravotnická dokumentace a národní zdravotnický informační systém, [online]. 2017. Dostupné z: < https://www.zakonyprolidi.cz/cs/2011-372#cast6 >
- ZAKONY PRO LIDI.CZ, Zdravotnická dokumentace a národní zdravotnický informační systém, [online]. 2017. [cit. 2017-01-20]. Dostupné z: < https://www.zakonyprolidi.cz/cs/2000-101#cast1>
- ZAKONY PRO LIDI.CZ, Zdravotnická dokumentace a národní zdravotnický informační systém, [online]. 2017. Dostupné z: < https://www.zakonyprolidi.cz/cs/2004-499>

SEZNAM ZKRATEK

MKDS	-	Městský kamerový dohlížecí systém
ÚOOÚ	-	Úřad pro ochranu osobních údajů
LZPS	-	Listina základních práv a svobod
EPS	-	Elektrická požární signalizace
CCTV	-	Uzavřený kamerový okruh – kamerový systém
IP	-	Komunikační standart pro přenos dat z anglického Internet Protokol
IP CCTV	-	Kamerový systém využívající IP technologie
VSS	-	Video dohlížecí systém z anglického Video Surveillance System
PZTS	-	Poplašný zabezpečovací a tísňový systém
EKV	-	Elektronická kontrola vstupu
PIN	-	Osobní identifikační číslo z anglického Personal Identification Number
WiFi	-	Bezdrátová komunikace z anglického Wireless Fidelity
TČ	-	Trestný čin
GPS	-	Globální družicový polohový systém z anglického Global Position System

BIBLIOGRAFICKÉ ÚDAJE

Jméno autora: Břetislav Šmejkal
Obor: Bezpečnostní studia
Forma studia: Kombinované studium
Název práce: Ochrana osob a ochrana osobních údajů osob
Rok: 2017
Počet stran textu bez příloh: 50
Celkový počet stran příloh: 0
Počet titulů českých použitých zdrojů: 6
Počet titulů zahraničních použitých zdrojů: 1
Počet internetových zdrojů: 28
Vedoucí práce: Ing. Michaela Melicharová