ZÁPADOČESKÁ UNIVERZITA V PLZNI

Fakulta právnická

Katedra ústavního a evropského práva

Diplomová práce

Právo na bezpečnost a povinnost státu hájit své občany v ČR a ve světě
Kamerové systémy

Simona Holubová

Plzeň, 2012

ZÁPADOČESKÁ UNIVERZITA V PLZNI

Fakulta právnická

Katedra ústavního a evropského práva

Diplomová práce

Právo na bezpečnost a povinnost státu hájit své občany v ČR a ve světě
Kamerové systémy

Simona Holubová

Obor: Právo

Studijní obor: Právo a právní věda

Vedoucí práce: JUDr. Tomáš Pezl

Plzeň, 2012

Prohlašuji, že jsem předkládanou diplomovou práci zpracovala samostatně a že jsem uvedla veškeré prameny, z nichž jsem pro svou práci čerpala způsobem pro vědeckou práci obvyklým.

V Plzni dne 30. března 2012 Simona Holubová

Na tomto místě bych ráda poděkovala JUDr. Tomášovi Pezlovi za vedení mé diplomové práce, vstřícný přístup a odborné rady a připomínky, které mi při psaní této diplomové práce poskytl.

Obsah

1. Úvod

Od osmdesátých let dvacátého století se začaly používat průmyslové kamery ke sledování veřejně přístupných míst. Zpočátku byly těmito prostředky střeženy věznice, letiště, banky, ambasády, tedy místa, která do té doby byla pod nepřetržitým dohledem zaměstnanců dotyčného zařízení. Od devadesátých let dvacátého století se kamerové systémy postupně začaly užívat na monitorování veřejného prostranství a postupně se rozšířily i do škol, zdravotních zařízení, soukromých budov. Dalo by se mluvit o invazi kamerového sledování současné společnosti.

Technické zázemí zjednodušuje procesy lidské činnosti a zároveň účinně nahrazuje člověka jako pracující subjekt. Je tomu tak z důvodu, že je všeobecně uznáván fakt, že technické přístroje jsou ve své činnosti účinnější, rychlejší a spolehlivější. Člověk jako pracující subjekt může leccos přehlédnout či opomenout, kdežto technika je koncipována tak, že k omylům tohoto typu jejím prostřednictvím nedochází. V současné době dochází k dynamickému vývoji všech technologií a nastává tak problém v adaptaci okolní společnosti na daný vývoj.

Technologické zázemí se vyvíjí takovou rychlostí, že pokud chce zákonodárce nastavovat pro užívání techniky určité hranice, je potřeba rychle reagovat na nově vzniklé situace. Může se pak ale stát, že nově vydaný zákon, který řešil poměry v době, kdy se právní úprava začala připravovat, je při svém vyhlášení již zastaralý. Stejně tak u kamerových systémů došlo k vývoji od kamer tak velkých, že se daly jen stěží zakrýt, k webkamerám, jejichž užívání lze díky jejich malé velikosti častokrát jen těžko odhalit.

Kamerové systémy se staly velkým problémem současné doby. Proto bych předpokládala, že jejich užívání bude dostatečně právně upraveno. Na stranu druhou je nutno přijmout fakt, že kamerové systémy jsou používány teprve krátce na to, aby se mohla očekávat existence propracované legislativy. Zákonodárci tedy nenahrává skutečnost, že technický vývoj jde rychle dopředu, proto ještě nestihl problematiku dostatečně upravit.

Cílem této práce je, zjistit jaká existuje právní úprava kamerových systémů v České republice, jaké jsou postupy při řešení případných sporů mezi provozovateli a fyzickými

osobami, které jsou kamerami sledovány, jakým způsobem je řešeno nezákonné používání kamerového systému.

Svého cíle bych se chtěla dobrat pomocí komparace s britskou právní úpravou, a to srovnáním případů, které se staly na území České republiky, s případy, které se udály a byly řešeny ve Spojeném Království.

Domnívám se, že Velká Británie by se dala v současné době považovat za velmoc v užívání kamerových systémů; začala užívat kamerové systémy již od sedmdesátých let dvacátého století, proto by se dala označit za průkopníka masového nasazení kamerového monitoringu. Od devadesátých let dvacátého století začalo Spojené království seznam míst pro instalaci kamer postupně rozšiřovat, až se v současné době můžeme s kamerovým sledováním ve Velké Británii setkat téměř všude. Předpokládám tedy, že právní úprava a proces řešení sporných situací, je zde příkladně upravena.

Pro potřeby této práce jsem zvolila analýzu jednotlivých případů, které bych chtěla rozebrat podle relevantních zákonů a judikatury. Chtěla bych porovnat, jak se od sebe v takovém případě liší česká a britská právní úprava.

Dále bych se pomocí judikatury chtěla dobrat odpovědi na otázku, jakou cestou se mohou subjekty osobních údajů dovolat svých práv, a tato zjištění opět porovnat se situací ve Velké Británii.

Práci jsem rozdělila do sedmi kapitol, přičemž v první kapitole rozeberu samotný pojem „kamerové systémy“ a jeho vliv na právo na ochranu soukromí. Také rozeberu základní zákonné povinnosti pro provozování kamerových systémů v České republice. Dále porovnám rozdíl mezi kamerovým systémem pořizující záznam a kamerovým systémem bez záznamu. V dalších kapitolách (kapitole 3. až 8.) rozeberu kamerové systémy podle místa jejich instalace, respektive podle prostorů, které jsou daným kamerovým místem sledovány a je pořizován záznam. Právní zjištění pak aplikuji na případy a zanalyzuji jejich řešení, to vše v komparaci s Velkou Británií.

2. Kamerové systémy

2.1. Pojem „kamerové systémy“

Kamerový systém, v angličtině Closed Circuit Television (CCTV), neboli také uzavřený televizní okruh je definován jako *„automaticky provozovaný stálý technický systém umožňující pořizovat a uchovávat zvukové, obrazové nebo jiné záznamy ze sledovaných míst“, a to např. formou pasivního monitorování prostoru nebo pořizování cílených záběrů (zachycování pohybu) anebo reportážním způsobem“*[1]

Ve smyslu alternativního pojmenování „uzavřený televizní okruh“ lze kamerový systém definovat jako užití videokamer tak, aby přenášely signál na určité místo, na omezený počet monitorů či okruh monitorů. Pro lepší pochopení je příhodné porovnání s televizním vysíláním, kde dochází k přenosu signálu z místa na místo nebo na více míst nebo prostřednictvím bezdrátového připojení, avšak signál televizního vysílání, na rozdíl od kamerového systému, není veřejně sdílený. [2]

Kamerové systémy slouží ke sledování prostorů, monitorování jak venkovních prostranství, tak vnitřních částí budov a později pak k případnému zobrazování zachycených záběrů, jejich archivaci a zpracování získaných osobních údajů, pokud se však nejedná o sledování bez záznamu, kdy ke zpracování osobních údajů nedochází. Provozovatel se může vzdáleně do systému připojit, sledovat obrazy online, prohlížet záznamy a zároveň kamerové zařízení vzdáleně ovládat. [3]

2.2. Účel kamerových systémů

Již odnepaměti bylo lidskou přirozeností chránit některé životní hodnoty, které byly v průběhu doby společností ohodnoceny jako velmi významné. Tím je míněno konkrétně právo na život, právo vlastnit majetek, nedotknutelnost obydlí, práva hospodářská, sociální a kulturní, tedy práva obsažená v Listině základních práv a

[1] Úřad pro ochranu osobních údajů; Komentář k Zásadám provozování kamerového systému z hlediska zákona o ochraně osobních údajů; 26. února 2012; dostupné na http://www.uoou.cz/uoou.aspx?menu=14&loc=328#kamery

[2] VERMAN ROMESH. *Distance Education In Technological Age*. Pvt. Ltd.: Anmol Publications, 2005. ISBN 8126122102, str. 166

[3] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 10

svobod. Tato práva jsou pro jednotlivé subjekty natolik významná, že projevují vlastní zájem k jejich ochraně. V důsledku technického pokroku se jednotlivým subjektům naskytla možnost chránit tato svá práva pomocí dohledové techniky, tedy také prostřednictvím kamerových systémů.

Užívání kamerových systémů slouží k řadě účelů, které lze rozdělit na:

1. ochranu jednotlivců
2. ochranu majetku
3. veřejný zájem
4. odhalování, prevence a stíhání trestné činnosti
5. získávání důkazů
6. jiné legitimní zájmy[4]

Účelem kamerových systémů je obvykle předcházení a odhalování trestné činnosti, stejně tak jako vandalismu, a to ve vnitřních prostorách i v bezprostřední blízkosti veřejně přístupných objektů (sportovní objekty, podzemní prostory metra, supermarkety a další obchody, benzínové čerpací stanice, zdravotnická a školská zařízení, okolí státních hranic, ale např. také vnitřní prostory vozů taxi), tak i v soukromých bytech a jejich sousedstvích, a to z bezpečnostních důvodů a zároveň s cílem zajistit důkazy v případě spáchání trestné činnosti v okolí monitorovaného objektu.[5]

Je tedy zřejmé, že užívání kamerových systémů je účelné. Provozovatelé však musí dodržovat přísná pravidla, a to z důvodu snadné zneužitelnosti kamer. Získávání informací o dění na sledovaných místech, respektive identifikování a filmování pohybu osob, je značným zásahem do soukromí, jež je choulostivou sférou života subjektů osobních údajů. Proto by provozovatelé měli mít na paměti, že kamerové systémy jsou instalovány především ku prospěchu společnosti.[6]

4 Úřad pro ochranu osobních údajů; Stanovisko č. 4/2004 ke zpracování osobních údajů prostředky kamerového sledování; 27.února 2012; dostupné na http://www.uoou.cz/uoou.aspx?menu=50&submenu=52&loc=83#pp3

[5] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 10

[6] Tamtéž, str. 11- 12

2.3. Pojem soukromí

Pro další účely této práce je příhodné definovat pojem soukromí.

„Pojem soukromí je interpretačně složitý a je možné jej chápat ve dvojím slova smyslu. V užším jako ochranu subjektivně vytvářené představy o soukromém životě člověka, v širším slova smyslu může spočívat i v ochraně širšího okolí bezprostředně navazujícího na životní potřeby a zájmy dané osoby a především spjaté s rodinou, přáteli apod.“[7]

„Je to ona sféra života člověka, do které bez výslovného dovolení zákona ani toho, koho se to týká, nikdo (ani stát) nesmí zasahovat a kterou člověk může před kýmkoliv (i před státem), s výjimkou případů výslovně v zákoně uvedených, utajit, současně je to ale také určitý prostor, do kterého za výše uvedených podmínek nikdo bez dovolení oprávněného nesmí vstupovat ani nahlížet ani pořizovat obrazové snímky, odposlouchávat tam apod.“[8]

Soukromí je tedy ta sféra života, která je erga omnes chráněna proti veškerým cizím zásahům a kterou člověk může před kýmkoli utajovat. Ani stát ani jakýkoli jiný subjekt není oprávněn do soukromí člověka zasahovat s výjimkou případů výslovně uvedených v zákonech a jiných právních předpisech. Každý člověk má tedy právo na své soukromí. Je to určitý prostor, který má každá fyzická osoba, a má právo jej bránit, a zároveň s tím koresponduje povinnost ostatních subjektů zdržet se zásahu do takového prostoru. Právo na soukromí bývá obvykle chráněno spolu s právem na ochranu rodiny, nedotknutelnost osobnosti a s právem na ochranu osobních údajů. Právo na soukromí je právem universálním, a to v tom smyslu, že jeho porušením bývají narušena i další práva. Zásah do soukromí je možný pouze na základě souhlasu fyzické osoby, jejímž právem je rozhodovat dle vlastního uvážení, jakým způsobem, v jakém rozsahu a zda vůbec mohou být zpřístupněny informace o jejím soukromí. Využití informací a skutečností ze soukromého života člověka lze na základě jeho svolení, pro které však není předepsána žádná forma. Je tedy možno jej udělit jak výslovně, tak konkludentně. Subjekt musí být plně způsobilý k právním úkonům a souhlas musí být učiněn svobodně, jasně a srozumitelně. Výjimkou z výše uvedeného je *„veřejný zájem*“. Hranice užívání

[7] KLÍMA, Karel. Ústavní právo. 3. rozšířené vydání. Plzeň: Aleš Čeněk, s.r.o., 2006. ISBN 80-7380-000-4, str. 284

[8] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 12

zjištěných skutečností ze soukromého života subjektů, a to v souladu s oprávněným veřejným zájmem, jsou dány právními předpisy a soudní judikaturou, hovoříme tedy o zásahu do soukromí na základě *legální licence*. [9]

Z toho je tedy zjevné, že právo na soukromí není absolutní. Zásah do soukromí se děje v souladu se zákonnou úpravou. Omezení soukromí může být jednorázové jako reakce na mimořádnou událost i jako relativně trvalé. K oprávněnému zásahu do soukromí je třeba kumulativního splnění zákonných podmínek a již zmíněného požadavku demokratické společnosti, aby zásah naplňoval legitimní cíle ochrany společenských hodnot a zároveň byl nezbytný. Dále je nutno podotknout, že soukromí je zákonem chráněno před *neoprávněným zásahem*, nikoli před takovým zásahem, ke kterému existuje zákonná licence. Zároveň jakékoli oprávněné omezení je přípustné pouze jako výjimka z výkonu základních práv a svobod.[10]

Ke skutečnostem soukromí patří intimní sféra života fyzické osoby jako je lidské tělo, zdravotní stav, obydlí, korespondence, zápisníky, deníky, majetkové poměry a další skutečnosti, které si člověk nepřeje zveřejňovat a vnímá je jako intimní či choulostivé.

K zásahům do práva na soukromí dochází například:

- prostřednictvím dotazníkových akcí
- při uzavírání pracovního poměru
- při jednání s pacientem v nemocnicích
- v rámci smluvního vztahu se zprostředkovateli telefonních služeb
- **provozování kamerových systémů**[11]

2.4. Kamerové systémy bez záznamu

Nejzákladnějším dělením kamerových systémů je v rozdělení na kamerové systémy se záznamem a systémy bez záznamu. Kamerové systémy bez záznamu jsou monitoringem, kde dochází k přenosu obrazu online. Je velmi obtížné posoudit otázku legality těchto systémů. Existuje názor, že pouhé zrakové a sluchové pozorování, které

[9] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 12
[10] Tamtéž.
[11] Policejní akademie České republiky; Právo na soukromí; 28. února 2012; dostupné na http://www.polac.cz/g2/view.php?katedry/kspd/pril9.ppt

není zaznamenáváno a není ani právně upraveno, není věcí intenzivní kontroly. Navíc na místech s určitou koncentrací osob je určitý monitoring považován za samozřejmý, i když s intenzitou odpovídající povaze věci.[12]

Je-li provozován kamerový systém bez záznamu, nedochází následně ke zpracování osobních údajů, neboť nejsou ani žádné osobní údaje ukládány. Kamerové systémy bez záznamového zařízení tak nepodléhají zákonu o ochraně osobních údajů, a proto provozovatel ani není povinen instalaci kamerového systému registrovat u Úřadu pro ochranu osobních údajů (dále jen Úřad), jenž je zákonným regulátorem pro nakládání s osobními údaji. Tento typ kamerového systému se tak stává možným řešením v případech, kdy se instalace kamerového systému se záznamem jeví jako nezákonná, porušující některé z ústavních práv subjektů.

Domnívám se však, že i kamerový monitoring bez pořízení záznamu je zásahem do soukromí. Kamery totiž snímají počínání jednotlivých fyzických osob, přestože se nedá snímaný obraz následně použít. To by samo o sobě nevadilo, pokud by u monitoru, do kterého je přenášen signál z kamer, neseděla osoba, která je pověřena dohledem monitorovaných prostorů. Svým pozorováním se stává svědkem dějů a situací, nahlíží do soukromého počínání jednotlivých subjektů a tím narušuje jejich soukromí. Je však nutno podotknout, že podle dikce zákona o ochraně osobních údajů tomu tak není.

2.5. Kamerové systémy se záznamem

Kamerový systém se záznamem je elektronická sestava, která pořizuje záznam. V takovém případě se pak jedná o zpracování osobních údajů, a to vždy, jsou-li tímto zařízením uchovávány informace pro účely pozdější identifikace fyzické osoby v souvislosti s určitou zaznamenanou situací.

„…kamerový systém pro účely tohoto textu budeme chápat jako „automaticky provozovaný stálý technický systém umožňující pořizovat a uchovávat zvukové, obrazové nebo jiné záznamy ze sledovaných míst“, a to např. formou pasivního monitorování prostoru nebo pořizování cílených záběrů (zachycování pohybu) anebo

[12] Nejvyšší státní zástupce, Výkladové stanovisko NSZ (Vykls)[Vykls 10/2003 K zákonnosti umístění audio-vizuálních prostředků ve školských zařízení vykonávajících ústavní výchovu a ochranou výchovu] ASPI [databáze] ASPI stav k 15.3.2012 [cit. 2012-03-15]

reportážním způsobem. Používané kamerové systémy určitě umožňují řadu způsobů uchovávání záznamů od zastaralejší formy v podobě videokazet až po moderní formy digitalizace a zálohování dat zpracovávaných počítačovými technologiemi.“[13]

Z uvedeného vyplývá a je zřejmé, že samotné sledování prostřednictvím kamer není zpracováním osobních údajů. Aby tomu tak bylo, musí se provádět záznam a současně splnit zákonné předpoklady. Kritéria činností nazývaná „ zpracování osobních údajů“ jsou dána v zákoně č. 101/2000 Sb., o ochraně osobních údajů o změně některých zákonů, ve znění pozdějších předpisů (dále jen zákon o ochraně osobních údajů), §4 písm. e). [14] Pokud se sledování nedá podřadit pod toto ustanovení, pak se nejedná o zpracování osobních údajů. [15]

Nicméně skutečnost, že nejsou naplněny stanovené podmínky, neznamená libovůli provozovatele k instalaci kamer; zároveň je nutné respektovat ustanovení občanského zákoníku upravující ochranu osobnosti, tedy § 11 a následující.[16]

„Údaje uchovávané v záznamovém zařízení, ať obrazové či zvukové, jsou osobními údaji za předpokladu, že na základě těchto záznamů lze přímo či nepřímo identifikovat konkrétní fyzickou osobu (tedy: informace z obrazových či zvukových nahrávek umožňují, byť nepřímo, identifikaci osoby). Fyzická osoba je identifikovatelná, pokud ze snímku, na němž je zachycena, jsou patrné její charakteristické rozpoznávací znaky (zejména obličej) a na základě propojení rozpoznávacích znaků s dalšími disponibilními údaji je možná plná identifikace osoby. Osobní údaj pak ve svém souhrnu tvoří ty identifikátory, které umožňují příslušnou osobu spojit s určitým, na snímku zachyceným, jednáním.“[17]

---

[13] Úřad pro ochranu osobních údajů, Komentář k Zásadám provozování kamerového systému z hlediska zákona o ochraně osobních údajů, 10. března 2012, dostupné na http://www.uoou.cz/uoou.aspx?menu=14&loc=328#kamery

[14] „e) zpracováním osobních údajů jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace,“ zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, §4 písm. e)

[15] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 19

[16] Tamtéž.

[17] Úřad pro ochranu osobních údajů, Stanovisko č. 1/2006, 10.březen 2012, dostupné na http://www.uoou.cz/files/stanovisko_2006_1.pdf

Stanovisko Úřadu doplňuje judikatura Nejvyššího správního soudu, který ve svém rozhodnutí upřesňuje význam pojmu zpracování osobních údajů takto:

„Plná identita fyzické osoby v současných podmínkách technologicky vyspělé společnosti, tj. za vysokého stupně rozvoje elektronických a jiných médií, která jsou většině populace snadno dostupná, ve své podstatě neznamená nic jiného, než možnost tuto osobu určitým způsobem kontaktovat, aniž by bylo nutno znát místo jejího aktuálního pobytu.“[18]

Nebude-li kontakt možný, pak získaná informace nedosahuje kvality osobního údaje, tedy není možno fyzickou osobu bez dalších doplňujících údajů identifikovat. [19]

Nicméně je jasné, že každý znak postavy, odlišující fyzickou osobu od ostatních, zakládá minimálně potenciální osobní údaj. Není vyloučeno, že správce osobních údajů někdy v budoucnu získanou informaci k identifikaci použije, a proto by s každým, byť prozatím jen potenciálním údajem, mělo být nakládáno jako s osobním údajem. [20]

2.5.1. Povinnosti správce osobních údajů

Provozovatelé kamerových systémů podléhají řadě povinností, které jsou uvedeny v právních předpisech. Je-li monitoring kamerovým systémem zároveň zpracováním osobních údajů, pak se správce[21] musí řídit zákonem č. 101/2000 Sb., o ochraně osobních údajů.

[18] Nejvyšší správní soud (NSS), sp. zn. 9 As 34/2008 – 68 - Rozsudek [Ochrana osobních údajů: zpracovatel osobních údajů] ASPI [databáze] ASPI stav k 15.3.2012 [cit. 2012-03-15]

[19] Tamtéž.

[20] Úřad pro ochranu osobních údajů, Komentář k Zásadám provozování kamerového systému z hlediska zákona o ochraně osobních údajů, 11.března 2012, dostupné na http://www.uoou.cz/uoou.aspx?menu=14&loc=328#kamery

[21] „ správcem každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak,“ z. č. 101/2000 Sb. o ochraně osobních údajů, § 4 písm. j)

2.5.2. Stanovení účelu zpracování osobních údajů

V souladu s § 5 odst. 1 písm. a) zákona o ochraně osobních údajů[22] má správce povinnost, a to ještě před zahájením procesu zpracování údajů, určit účel, pro který budou osobní údaje zpracovávány. Účel musí být správcem stanoven jasně a jednoznačně tak, aby vylučoval použití nashromážděných informací k jiným účelům. K tomuto úkonu musí dojít vždy. Správce by měl, respektive musí, účel zpracování osobních údajů vždy předem znát. [23]

Je-li tedy kamerový systém provozován například ve škole z důvodu ochrany před poškozováním školního zařízení, pak je účelem ochrana majetku. Kamerové systémy na veřejných prostranstvích, a to především městské kamerové dohlížecí systémy, jsou zřizovány za účelem zabezpečování veřejného pořádku.

Účel může být stanoven správcem nebo může být určen právními normami; musí korespondovat s důležitými zájmy správce, a to zájmy právem chráněnými. Pořízený záznam lze použít pouze ke zjištění vzniklé události, která poškozuje důležitý zájem správce. Užití pořízeného záznamu pro jiný než stanovený účel je možné pouze a jen z důvodu právem chráněného veřejného zájmu, jímž je ochrana osob a majetku a prevence kriminality.[24]

2.5.3. Stanovení prostředků a způsobu zpracování osobních údajů

Stejně tak jako u stanovení účelu zpracování osobních údajů by měl správce jednoznačně určit, kterými prostředky a jakým způsobem[25] budou osobní údaje zpracovávány. Jak vybrané prostředky, tak způsob by měly být zvoleny přiměřeně požadovanému účelu. Volbu prostředků stejně jako způsob zpracování může za správce stanovovat některý z právních předpisů, častěji je však výběr ponechán na vůli

[22] Správce je povinen: a) stanovit účel, k němuž mají být osobní údaje zpracovány, § 5 odst. 1 písm. a) zákona č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů

[23] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str.22 - 28

[24] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str.22 - 28

[25] „Základním rozlišením prostředků a způsobů zpracování osobních údajů je skutečnost, zda ke zpracování dochází manuálním nebo automatizovaně. Možná je i kombinace obou těchto metod zpracování osobních údajů.“ BARTÍK, Václav, Janečková, Eva. Zákon o ochraně osobních údajů s komentářem. 1. vyd. Olomouc: ANAG, 2010. ISBN 978-80-7263-613-6, str. 72

samotného správce s jediným omezením, a to právě požadavkem, aby způsob a prostředky odpovídaly účelu. [26]

Kamerové systémy by měly být, respektive mohou být používány pouze podpůrně, čímž je míněno až tehdy, jeví-li se ostatní opatření jako nedostatečná. Zdá-li se instalace pancéřových dveří, lepšího pouličního osvětlení nebo poplachového zařízení jako nepostačující k ochraně daného zájmu, pak je skutečnost užívání kamerového systému skutečně odůvodněná. [27] V mnoha případech se také jako příhodnější nabízí dozor daného místa prostřednictvím místních zaměstnanců, kteří svou přítomností a sledováním místa mohou také dohlížet na ochranu majetku nebo bezpečnosti přítomných osob. Vhodnějším se toto řešení jeví především ve školách nebo nemocnicích, kde by kamerové systémy nad míru narušovali soukromí přítomných osob.

Je třeba tedy aplikovat zásadu přiměřenosti, a to v tom smyslu, že provozovatel by měl používání kamerového monitoringu odůvodňovat účelem určité vážnosti, nikoliv drobností jako např. instalace kamer pro kontrolu, zda se studenti při vstupu do školy přezouvají. V tomto případě postačí osobní dohled některého ze zaměstnanců zařízení.

Příčinou nepřehledné situace v problematice kamerových systémů je absence limitujícího pravidla, které by stanovovalo konkrétní hranice, kdy ještě mohou být monitorovací zařízení používána a kdy je jejich instalace nepřiměřená. Je však zřejmé, že stanovit jasné hranice je složité, respektive nemožné. Proto je nezbytné posuzovat případ od případu. Je především nutno zvážit, zda umístění kamerového systému jako dalšího ochranného prostředku je opravdu účelné, tedy skutečně efektivní, nebo zda to je například pouhé efektní přesunutí vandalů a delikventů k páchání trestné činnosti do jiné, méně střežené lokality. V této souvislosti se nabízí i otázka, zda by při celoplošném monitorování veřejného prostoru trestná činnost sama zcela nevymizela. Takovéto úvahy však spíše vzbuzují oprávněné obavy z tendence k nadměrným

[26] BARTÍK, Václav, Janečková, Eva. Zákon o ochraně osobních údajů s komentářem. 1. vyd. Olomouc: ANAG, 2010. ISBN 978-80-7263-613-6, str. 72

[27] Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance, 12.března 2012, dostupné na http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp89_en.pdf

zásahům do soukromí fyzických osob. Proto je nadměrná instalace kamerových systémů přijímána spíše negativně a jako problém současné společnosti.[28]

2.5.4. Povinnost zpracovávat pouze přesné osobní údaje

V § 5 odst. 1 písm. c) zákona o ochraně osobních údajů[29] je dána povinnost správce zpracovávat pouze přesné osobní údaje.

„...zpracováním nepřesných osobních údajů podle § 5 odst. 1 písm. c) ZOOÚ není pouze zpracování nesprávných údajů, ale i zpracování formálně správných údajů v souvislosti s nesprávnou informací.“[30]

Směrnice 95/46/ES ukládá povinnost spravovat pouze přesné údaje v míře nezbytné a pak informace aktualizovat. Problematickou se stává ta část ustanovení, kde jak zákonodárce, tak směrnice mluví o aktualizaci. Je otázkou, zda přesné znamená aktuální. Udržovat záznam z kamerového systému aktuální je totiž ve své podstatě nemožné. Na záznamy z monitorovacího zařízení lze ale nahlížet tak, že byly aktuální k jinému, minulému časovému období. Pro účely zákona však musí být přijata veškerá opatření, aby nepřesné a neúplné údaje s ohledem na účely, pro které byly shromažďovány, byly vymazány nebo opraveny.[31] Je však těžké si představit možnou opravu údaje, pořízeného kamerovým systémem. V takovém případě, pokud je pořízený údaj nepřesný či neúplný, přichází v úvahu jen jeho likvidace.

---

[28] Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance, 12.března 2012, OBLIGATIONS AND APPROPRIATE PRECAUTIONS APPLYING TO THE DATA CONTROLLE, dostupné na http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp89_en.pdf

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

[30] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 25

[31] BARTÍK, Václav, Janečková, Eva. Zákon o ochraně osobních údajů s komentářem. 1. vyd. Olomouc: ANAG, 2010. ISBN 978-80-7263-613-6, str. 72

2.5.5. Povinnost zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny

Povinnost zpracovávat osobní údaje pouze k účelu, k němuž byly shromážděny je dána § 5 odst. 1 písm. f) zákona o ochraně osobních údajů.[32] Zákon označuje za nepřípustné, aby informace, shromážděné pro předem daný účel, byly následně použity k jinému účelu, který ani nebude subjektu osobních údajů či Úřadu při registraci oznámen.

Toto ustanovení brání libovůli správců, kteří mají často za to, že pokud získají nějaké informace o určitých subjektech, mohou pak s nimi nakládat dle svého uvážení a potřeby. Nemůže se tedy stát, aby informace získané pro poskytování zdravotní péče byly užity pro komerční potřeby správce nebo je správce předával dál jiným subjektům pro další zpracování.[33]

2.5.6. Povinnost shromažďovat osobní údaje pouze otevřeně

§ 5 odst. 1 písm. g) zákona o ochraně osobních údajů[34] ukládá správci povinnost shromažďovat osobní údaje pouze otevřeně. Tím zákonodárce výslovně zakazuje shromažďovat údaje pod záminkou jiného účelu.

„Správce proto musí vždy, pokud hodlá využívat shromážděné osobní údaje nikoliv pro jediný účel, ale pro několik účelů, postupovat vždy v souladu se všemi svými povinnostmi, které mu z příslušných ustanovení ZOOÚ vyplývají a požádat například subjekt údajů o poskytnutí souhlasu ke zpracovávání osobních údajů pro všechny tyto účely.“[35]

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

[33] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 25

[34] „g) shromažďovat osobní údaje pouze otevřeně; je vyloučeno shromažďovat údaje pod záminkou jiného účelu nebo jiné činnosti,“ z. č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, § 5 odst. 1 písm. g)

[35] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 26

2.5.7. Povinnost nesdružovat osobní údaje, které byly získány k rozdílným účelům

Uložením povinnosti respektive zákazu sdružování osobních údajů, získaných k rozdílným účelům, vytvořil zákonodárce v § 5 odst. 1 písm. h) zákona o ochraně osobních údajů [36] překážku, aby správce nemohl sdružovat osobní údaje, které jsou sice předmětem jeho zpracování pro předem zvolené účely, ale samy údaje jsou předmětem rozdílných zpracování pro odlišné účely. Docházelo by pak ke spojení získaných údajů, jehož následkem by bylo zkvalitnění získaných informací a tím větší ohrožení zásahem do soukromého života jednotlivých fyzických osob. [37]

2.5.8. Povinnost uchovávat osobní údaje pouze ke stanovenému účelu a v rozsahu nezbytném pro naplnění daného účelu

Povinnost je uložena v § 5 odst. 1 písm. d) zákona o ochraně osobních údajů [38] a hovoří o uchovávání osobních údajů jako o jednom ze základních oprávnění správce při zpracování osobních údajů. Správce osobních údajů by ještě před zahájením zpracování měl znát i rozsah osobních údajů, které hodlá zpracovávat. Toto ustanovení se váže na povinnost správce předem určit účel zpravování osobních údajů a povinnost, že správce smí shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu. V § 5 odst. 1 písm. d) zákona o ochraně osobních údajů se tedy předpokládá, že správce již splnil předchozí povinnosti. [39]

V tomto ustanovení jde o vztah mezi účelem a informací, která má být prostředkem pro dosažení účelu. Správce musí vymezit minimální rozsah konkrétních osobních údajů, které budou k naplnění účelu skutečně potřebné. Rozhoduje se tedy o každém osobním údaji, zda je pro daný účel nezbytný či nikoliv. Nepotřebné osobní údaje by měl správce bez odkladu zlikvidovat.[40]

---

[36] h) nesdružovat osobní údaje, které byly získány k rozdílným účelům, z. č. 101/2000 Sb. o ochraně osobních údajů o změně některých zákonů, ve znění pozdějších předpisů, § 5 odst. 1 písm. h)

[37] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 26

[38] d) shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanového účelu, z. č. 101/2000 Sb. o ochraně osobních údajů o změně některých zákonů, ve znění pozdějších předpisů, § 5 odst. 1 písm. d)

[39] BARTÍK, Václav, Janečková, Eva. Zákon o ochraně osobních údajů s komentářem. 1. vyd. Olomouc: ANAG, 2010. ISBN 978-80-7263-613-6, str. 75

[40] Tamtéž.

2.5.9. Povinnost uchovávat osobní údaje pouze nezbytně nutnou dobu pro naplnění účelu zpracování

Každý ze správců osobních údajů, jestliže už vynaložil určité úsilí na získání informací o okolních subjektech, má samozřejmě velký zájem uchovat si získaná data co nejdéle. Doba uchovávání osobních údajů je však zákonem omezena a je jednou z dalších povinností správce toto omezení respektovat. [41]

Spornou otázkou, kterou zákonodárce řeší v § 5 odst. 1 písm. e) zákona o ochraně osobních údajů[42], je možná doba uchování získaných osobních údajů. Prvním předpokladem pro posuzování možné délky uchování osobních údajů je úzká souvislost mezi stanoveným účelem a samotnou dobou pro uchování. Neměla by být příliš krátká ani neúměrně dlouhá, nýbrž taková, aby odpovídala určenému účelu. Doba se tedy posuzuje s ohledem na okolnosti, pro které se zpracování koná. Jinak řečeno, lhůta pro uchování osobních údajů by měla být přiměřená, odpovídat konkrétním aspektům daného případu. Otázku přiměřenosti je nutno posuzovat u každého případu zvlášť.[43]

Dobu pro uchovávání údajů musí každý správce uvést při registraci u Úřadu. Úřad následně posoudí, zda zpracovatelem uvedená doba je přiměřená vzhledem k určenému účelu. Doba uchovávání by neměla přesáhnout 24 hodin, pokud jde o trvale střežený objekt. Je přípustná i doba delší, neměla by ale ani tak přesáhnout lhůtu několika dnů. Například při pořizování záznamu přes víkend dovoluje již z logiky věci uchovávání záznamů po dobu alespoň tří dnů. Doba 14 dnů pro uchovávání je podle Úřadu zjevně nepřiměřená, jelikož získané záznamy jsou průběžně zpracovány, a proto jakákoli zaznamenaná incidenční situace bude odhalena neprodleně po zpracování. Výjimkou jsou záznamy pořízené policejním orgánem, jež se řídí zvláštními právními předpisy.[44] Lhůta se nevztahuje na pořízenou kopii, kdy je záznamu použito jako důkazního prostředku. Po uplynutí stanovené doby by mělo dojít ke zničení záznamu, což

[41] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 27

[42] e) uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování. Po uplynutí této doby mohou být osobní údaje uchovávány pouze pro účely státní statistické služby, pro účely vědecké a pro účely archivnictví. Při použití pro tyto účely je třeba dbát práva na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů a osobní údaje anonymizovat, jakmile je to možné, z. č. 101/2000 Sb. o ochraně osobních údajů o změně některých zákonů, ve znění pozdějších předpisů, § 5 odst. 1 písm. e)

[43] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 27

[44] z. č. 553/1991 Sb. o obecní policii, ve znění pozdějších předpisů; z. č. 273/2008 Sb. o Policii České republiky ve znění pozdějších předpisů

znamená, že pominutím nebo nenaplněním účelu zpracování dojde k likvidaci záznamu.[45]

2.5.10. Souhlas subjektu údajů

Jelikož zpracováním osobních údajů dochází k zásahu do soukromí nositele osobních údajů, zákonná úprava ochrany osobních údajů stanovuje pro jejich správce pravidlo , a tím je získání souhlasu subjektu osobních údajů. *„Proto směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a s volným pohybem těchto údajů (dále jen „směrnice 95/46/ES“), i zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon o ochraně osobních údajů“) stanoví obecné pravidlo, že zpracování osobních údajů se může zásadně dít pouze se souhlasem jejich nositele, právní terminologií subjektu údajů (s výhradou některých výjimek, v českém právním řádu upravených v § 5 odst. 2 citovaného zákona).“*[46]

Samotná směrnice upravuje výraz souhlas takto:

„Pro účely této směrnice se rozumí ´souhlasem dotčené osoby´ jakýkoli svobodný, výslovný a vědomý projev vůle, kterým dotčená osoba přijímá, aby osobní údaje, které se jí týkají, byly předmětem zpracování.“[47]

Poskytnutí souhlasu je právním úkonem a je tedy třeba vzít v úvahu úpravu podle zákona č. 40/1964 Sb., občanského zákoníku, ve znění pozdějších předpisů. Podle této úpravy je právním úkonem projev vůle právního subjektu, směřující ke vzniku, změně nebo zániku právních vztahů, respektive práv a povinností, které právní předpisy s takovým projevem vůle spojují. Právní úkon je pak platný, je-li učiněn svobodně, vážně, určitě a srozumitelně.

Dle úpravy zákona o ochraně osobních údajů, § 4 písm. n) je:

[45] Úřad pro ochranu osobních údajů, Stanovisko č. 1/2006, 15.března 2012, dostupné na www.uoou.cz/files/stanovisko_2006_1.pdf
[46] Úřad pro ochranu osobních údajů, Stanovisko č. 2/2008, 13.březen 2012, dostupné na http://www.uoou.cz/files/stanovisko_2008_2.pdf
[47] Úřad pro ochranu osobních údajů, Stanovisko č. 2/2008, Směrnice 95/46/ES v čl. 2 písm. h), 13.březen 2012, dostupné na http://www.uoou.cz/files/stanovisko_2008_2.pdf

„souhlasem subjektu údajů svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů“[48]

Pojem „vědomý“ byl do zákona včleněn novelou zákona o ochraně osobních údajů č. 439/2004 Sb. z důvodu konformního výkladu se směrnicí 95/46/ES. Je tedy další náležitostí, a to vedle těch, jež jsou stanoveny občanským zákoníkem, kterou souhlas musí obsahovat. Úřad pro ochranu osobních údajů deklaruje, že:

„Subjekt údajů si při poskytování souhlasu má být vědom, resp. dle okolností je zjevné, že si mohl a měl být vědom, důsledku svého konání, poskytnutí souhlasu se zpracováním svých osobních údajů. Toto zpracování je očekávaným a předpokládaným důsledkem souhlasu a subjekt údajů s ním vědomě a cíleně souhlasí.“[49]

Důsledkem splnění všech náležitostí, jak podle občanského zákoníku, tak podle zákona o ochraně osobních údajů a unijního práva, je platnost souhlasu a následné legální zpracování osobních údajů.[50]

Pokud jde o kamerové systémy, lze princip udělení souhlasu použít jen tehdy, je-li možno vymezit okruh osob, který bude kamerovým systémem snímán. Tím se stává povinnost správce velmi sporná. Pro posouzení, zda je dána povinnost získat souhlas subjektu údajů či nikoliv, se zjišťuje pomocí výjimek z § 5 odst. 2 zákona o ochraně osobních údajů[51] nebo ze zákonného zmocnění. Teprve tehdy, chybí-li zákonné

---

[48] Z. č. 101/2000 Sb. o ochraně osobních údajů o změně některých zákonů, ve znění pozdějších předpisů, § 4 písm. n)

[49] Úřad pro ochranu osobních údajů, Stanovisko č. 2/2008, 13.březen 2012, dostupné na http://www.uoou.cz/files/stanovisko_2008_2.pdf

[50] Tamtéž.

[51] Správce může zpracovávat osobní údaje pouze se souhlasem subjektu údajů. Bez tohoto souhlasu je může zpracovávat,

a) jestliže provádí zpracování nezbytné pro dodržení právní povinnosti správce,
b) jestliže je zpracování nezbytné pro plnění smlouvy , jejíž smluvní stranou je subjekt údajů , nebo pro jednání o uzavření nebo změně smlouvy uskutečněné na návrh subjektu údajů,
c) pokud je to nezbytně třeba k ochraně životně důležitých zájmů subjektu údajů. V tomto případě je třeba bez zbytečného odkladu získat jeho souhlas. Pokud souhlas není dán, musí správce ukončit zpracování a údaje zlikvidovat,
d) jedná-li se o oprávněně zveřejněné osobní údaje v souladu se zvláštním právním předpisem. Tím však není dotčeno právo na ochranu soukromého a osobního života subjektu údajů,
e) pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby; takové zpracování osobních údajů však nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života,
f) pokud poskytuje osobní údaje o veřejně činné osobě, funkcionáři či zaměstnanci veřejné správy, které

zmocnění a všechny výjimky jsou vyloučeny, lze v činnosti správce shledat porušení zákonné úpravy, respektive §5 odst. 2 zákona o ochraně osobních údajů. [52]

V zásadě jedinou možnou výjimkou, kterou naše právní úprava nabízí, je zmíněný § 5 odst. 2 písm. e) zákona o ochraně osobních údajů. Ten hovoří o možnosti zpracovávat osobní údaje i bez daného souhlasu subjektu údajů, ale pouze v případě nezbytném pro ochranu práv a právem chráněných zájmů, a to konkrétně správce, příjemce nebo jiné dotčené osoby. [53]

Příjemcem se rozumí každý subjekt, kterému jsou osobní údaje zpřístupněny, vyjma samotného správce.[54]

Dotčenou osobu lze negativně vymezit jako fyzickou osobu, která není ani správcem ani příjemcem. Dotčená osoba je taková osoba, jíž by se zpracování osobních údajů v obsahu tohoto ustanovení, tedy v rámci zpracování osobních údajů bez podání souhlasu subjektu údajů, mohlo dotknout, např. tím, že by získané informace mohly být využity k ochraně jejích práv či právem chráněných zájmů, tedy těch, na které se výjimka vztahuje. [55]

Subjekt údajů dává své svolení na základě informace o provozu kamerového systému na určitém místě, v určitém prostoru, objektu. Otázkou je i forma podání souhlasu, respektive zda je přípustné konkludentní podání souhlasu. Tato forma by měla být teoreticky přípustná, ale pouze v případě, že by byla subjektu údajů dána možnost souhlas odepřít, tedy na základě včasného informování ještě před vstupem do monitorované oblasti.

---

vypovídají o jeho veřejné anebo úřední činnosti, o jeho funkčním nebo pracovním zařazení, nebo,
g) jedná-li se o zpracování výlučně pro účely archivnictví podle zvláštního zákona.

z. č. 101/2000 Sb. o ochraně osobních údajů o změně některých zákonů, ve znění pozdějších předpisů, § 5 odst. 2

[52] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 29
[53] BARTÍK, Václav, Janečková, Eva. Zákon o ochraně osobních údajů s komentářem. 1. vyd. Olomouc: ANAG, 2010. ISBN 978-80-7263-613-6, str. 94-96
[54] § 4 písm. o) z. č. 101/2000 Sb. o ochraně osobních údajů o změně některých zákonů, ve znění pozdějších předpisů
[55] BARTÍK, Václav, Janečková, Eva. Zákon o ochraně osobních údajů s komentářem. 1. vyd. Olomouc: ANAG, 2010. ISBN 978-80-7263-613-6,str. 94-96

2.5.11. Informační povinnost správce

Subjekt osobních údajů může řádně udělit souhlas jen ke zpracování těch údajů, o kterých je řádně poučen, a proto dle dikce § 5 odst. 4 zákona o ochraně osobních údajů má správce osobních údajů dále uloženou povinnost informovat subjekty údajů:

- jaký je zamýšlený účel zpracovávání údajů
- jaká kategorie osobních údajů bude zpracovávána a v jakém rozsahu
- kdo bude údaje zpracovávat, tedy identifikace správce
- na jakou dobu je souhlas se zpracováváním údajů udělen

Z povahy věci je zřejmé, že k řádnému udělení souhlasu, a to na základě podaného poučení, musí být uvedené informace subjektu sděleny ještě před udělením tohoto souhlasu.[56]

§ 11 odst. 1 a 2 zákona o ochraně osobních údajů dále doplňují informační povinnost správce o:

- rozsah, v jakém budou osobní údaje zpracovávány
- způsob zpracovávání
- okruh osob, jimž mohou být osobní údaje zpřístupněny

Informační povinnosti je správce zproštěn v případě, kdy jsou subjektu údajů dané informace o bodech uvedených v zákoně již známy. [57]

Správce plní svou informační povinnost obvykle prostřednictvím textu uvedeného v příslušné smlouvě, na příslušném formuláři nebo v rámci ustanovení všeobecných obchodních podmínek. Je nutno podotknout, že informace musí být subjektu údajů sděleny ve srozumitelné a přehledné formě; konkrétní podobu, v jaké by měly být informace poskytnuty, však zákon jednoznačně nestanoví. [58]

V případě kamerových systémů se záznamem je obvyklým způsobem plnění informační povinnosti umístění tabulek v prostorách, nejčastěji budovách, opatřených

[56] Úřad pro ochranu osobních údajů, Stanovisko č. 2/2008, 13.březen 2012, dostupné na http://www.uoou.cz/files/stanovisko_2008_2.pdf
[57] BARTÍK, Václav, Janečková, Eva. Zákon o ochraně osobních údajů s komentářem. 1. vyd. Olomouc: ANAG, 2010. ISBN 978-80-7263-613-6,str. 151
[58] Tamtéž.

monitorovacím zařízením. Je však diskutabilní, zda splnění informační povinnosti až po vstupu do sledovaných prostor je řádným splněním povinnosti správce. V takovém případě se pravděpodobně jedná právě o možnost konkludentního udělení souhlasu, kdy však subjekt údajů nemá možnost předem svůj souhlas ke zpracovávání údajů neudělit. Tuto situaci by mohlo řešit umístění informační tabule již u vchodu do budovy, většinou je ovšem některá z kamer nainstalována tak, aby monitorovala již vchod. Sledování vchodu budovy není však bráno jako velké narušení práva na soukromí, neboť zde subjekt údajů velkou míru soukromí očekávat nemůže. Pak se stává diskutabilním případ Campbell v. MGM [2004] (viz. podkapitola 5.2.)

Správce osobních údajů také musí poučit subjekt údajů o tom, zda je poskytnutí informací dobrovolné nebo jestli jde o povinnost poskytnout údaje správci na základě zvláštního zákona. Ze zákona však vyplývá, že tuto povinnost má správce pouze v případě, že získává a shromažďuje údaje přímo od subjektů údajů.[59]

Jestliže zvláštní zákon ukládá subjektu údajů povinnost poskytnout správci určité informace, pak musí být správcem poučen o následcích případného nesplnění této povinnosti. V poučení musí být také zahrnuta případná možnost odmítnutí poskytnout osobní údaje, a to například pokud by tak způsobil nebezpečí trestního stíhání sobě nebo osobě blízké. [60]

Pokud správce poruší svou informační povinnost a potřebná poučení subjektu údajů neposkytne, nastupuje podle zákona sankční povinnost, a to konkrétně podle § 44 odst. 2 písm. f)[61] a § 45 odst. 1 písm. f)[62] zákona o ochraně osobních údajů. Zákon však nechává na samotném správci, jak se vyrovná s nutností prokázat splnění své informační povinnosti. Sám o sobě totiž žádnou konkrétní formu prokazatelnosti neurčuje, a proto lze doporučit, aby správce v daném případě postupoval obdobně jako

[59] BARTÍK, Václav, Janečková, Eva. Zákon o ochraně osobních údajů s komentářem. 1. vyd. Olomouc: ANAG, 2010. ISBN 978-80-7263-613-6, str. 152

[60] Tamtéž.

[61] Fyzická osoba se jako správce nebo zpracovatel dopustí přestupku tím, že při zpracování osobních údajů
f) neposkytne subjektu údajů informace v rozsahu nebo zákonem stanoveným způsobem (§ 11), z. č. 101/2000 Sb. o ochraně osobních údajů o změně některých zákonů, ve znění pozdějších předpisů, § 44 odst. 2 f)

[62] Právnická osoba nebo fyzická osoba podnikající podle zvláštních předpisů se jako správce nebo zpracovatel dopustí správního deliktu tím, že při zpracování osobních údajů
f) neposkytne subjektu údajů informace v rozsahu nebo zákonem stanoveným způsobem (§ 11), . č. 101/2000 Sb. o ochraně osobních údajů o změně některých zákonů, ve znění pozdějších předpisů, § 45 odst. 1 f)

u udílení souhlasu subjektem údajů, tedy tak, aby si nechal poskytnutí informací subjektem údajů prokazatelným způsobem potvrdit.[63]

Povinnosti uvedené v § 11 odst. 1 a 2 zákona o ochraně osobních údajů musí správce osobních údajů splnit vždy, nevztahuje-li se na něj některá z výjimek uvedené v odst. 3.[64]

Převedeme-li výše uvedená pravidla a povinnosti správce na kamerové systémy, uvědomíme si, že jednotlivé body informační povinnosti jsou velmi těžce proveditelné. V praxi se informační povinnost ohledně monitoringu kamerovým systémem řeší pomocí tabulí, na kterých je uvedeno například: „Prostor je sledován kamerovým systémem se záznamem!“

Z toho lze vyvodit, že bude docházet ke zpracování osobních údajů. Další potřebné informace subjektu údajů však poskytnuty nejsou. Jelikož zde není uvedena identifikace správce, dokonce ani kde by bylo možné další informace získat, možnost subjektu údajů aktivně se podílet na zpracování osobních údajů podle § 12 a § 21 zákona o ochraně osobních údajů je tak značně snížena, viz níže.[65]

Smyslem informační povinnosti správce je volba možnosti subjektu údajů aktivně se podílet, respektive svobodně se rozhodnout, zda chce poskytnout své osobní údaje či nikoli. Může se také domáhat nápravy, nejsou-li jeho údaje zpracovány v souladu s právními předpisy. V § 12 a § 21 zákona o ochraně osobních údajů je uvedena možnost subjektu údajů žádat správce o poskytnutí informací ohledně zpracování svých

[63] BARTÍK, Václav, Janečková, Eva. Zákon o ochraně osobních údajů s komentářem. 1. vyd. Olomouc: ANAG, 2010. ISBN 978-80-7263-613-6, str. 151 - 152

[64] Informace a poučení podle odstavce 1 není povinen správce poskytovat v případech, kdy osobní údaje nezískal od subjektu údajů, pokud

a) zpracovává osobní údaje výlučně pro účely výkonu státní statistické služby, vědecké nebo archivní účely a poskytnutí takových informací by vyžadovalo neúměrné úsilí nebo nepřiměřeně vysoké náklady; nebo pokud ukládání na nosiče informací nebo zpřístupnění je výslovně stanoveno zvláštním zákonem. V těchto případech je správce povinen přijmout potřebná opatření proti neoprávněnému zasahování do soukromého a osobního života subjektu údajů,
b) zpracování osobních údajů mu ukládá zvláštní zákon nebo je takových údajů třeba k uplatnění práv a povinností vyplývajících ze zvláštních zákonů,
c) zpracovává výlučně oprávněně zveřejněné osobní údaje, nebo
d) zpracovává osobní údaje získané se souhlasem subjektu údajů, z. č. 101/2000 Sb. o ochraně osobních údajů o změně některých zákonů, ve znění pozdějších předpisů, § 11 odst. 3

[65] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 31 - 32

údajů a s tím korespondující povinnost správce takové informace poskytnout. V tomto smyslu může dále žádat o poskytnutí informací ohledně:

„účelu, o osobních údajích, které jsou předmětem zpracování, včetně informací o jejich zdroji, povaze případného automatizovaného zpracování a o příjemcích osobních údajů, tedy o těch, komu byly osobní údaje subjektu údajů zpřístupněny. Ustanovení § 21 potom zakotvuje právo subjektu údajů požadovat po správci vysvětlení zpracování svých osobních údajů v případě, kdy subjekt zjistil nebo se domnívá, že toto zpracování neprobíhá řádným způsobem, a právo požadovat po správci nápravu tohoto stavu.“[66]

V případě zpracování osobních údajů prostřednictvím kamerových systémů jsou však práva uvedená v § 21 zákona o ochraně osobních údajů z podstaty věci omezena, a to především z důvodu krátké doby, dané pro uchování takto získaných údajů. Oprava těchto údajů je zpravidla nemožná, neboť v takové situaci je nutné záznam zlikvidovat.[67]

2.5.12. Povinnost správce chránit osobní údaje

Podle § 13 zákona o ochraně osobních údajů náleží správci jako další povinnost zajistit bezpečnost zpracování osobních údajů, a to jak před jednáním úmyslným, tak nedbalostním, stejně jako proti působení přírodních a jiných událostí, která by mohla mít vliv na zneužití osobních údajů. [68]

Správce je tedy povinen přijmout taková opatření, která zabrání neoprávněnému nebo nahodilému přístupu k získaným údajům, jejich změně, zániku či zničení, stejně jako neoprávněnému přenosu nebo zpracování. Volba opatření náleží čistě a jen na správci, který své rozhodování odvozuje od jím zvoleného způsobu zpracování osobních údajů a samozřejmě na svých vlastních finančních a personálních možnostech. [69]

[66] Úřad pro ochranu osobních údajů, Stanovisko č. 2/2008, 13.březen 2012, dostupné na http://www.uoou.cz/files/stanovisko_2008_2.pdf
[67] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 32
[68] BARTÍK, Václav, Janečková, Eva. Zákon o ochraně osobních údajů s komentářem. 1. vyd. Olomouc: ANAG, 2010. ISBN 978-80-7263-613-6, str. 158
[69] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 33

Ve smyslu výše zmíněných požadavků na správce osobních údajů stanovila Pracovní skupina pro ochranu osobních údajů WP 29[70] několik požadavků na zajištění bezpečnosti při zpracovávání osobních údajů, a to konkrétně na kamerové systémy.

a) Získaný záznam by mělo mít možnost shlédnout jen omezený počet subjektů, respektive fyzických osob. Jsou jimi:
    - konkrétně určené osoby, tedy osoby, které pracují s určitým kamerovým systémem
    - subjekty údajů, které požádají o přístup k údajům
    - pověření pracovníci policejního nebo soudního orgánu, kteří získávají přístup k daným údajům na základě příkazu, vydaného za účelem odhalení trestné činnosti
    - samozřejmě také osoby, které na kamerových systémech provádí technickou údržbu
b) Správce by měl provést taková opatření, aby se zabránilo nedovolenému úniku dat, zamezilo přístupu třetím osobám, neoprávněné manipulaci s daty, změnám či zničení údajů. Podle publikace Evy Janečkové a Václava Bartíka, nazvané Kamerové systémy v praxi, by mohlo být v řadě případů vhodným řešením použití dvou přístupových klíčů, přičemž jeden z nich by měl ve svém držení správce a druhý z nich policie. Tím by se zabránilo neoprávněnému přístupu k údajům a zároveň by nebylo narušeno oprávnění příslušných subjektů osobních údajů na žádost shlédnout získaný záznam.
c) Významný bodem je také kvalita pořízených záznamů, která se odvíjí od faktu, že záznamy jsou pořizovány stejným záznamovým zařízením.
d) Pro danou ochranu pořízených osobních údajů je důležité vyškolit osoby, které budou se získanými záznamy nakládat. Je tedy třeba, aby provozovatelé a správci kamerových systémů prošli školením, byli obeznámeni s příslušnými

[70] WP 29 byl ustanoven článkem 29. Směrnie 95/46/EC. Jde o nezávislý evropský poradní orgán na ochranu dat a soukromí. Jeho úkoly jsou popsány ve článku 30 směrnice 95/46/EC a článku 15 směrnice 2002/58/C; Iuridicum Remedium, Pracovní skupina podle článku 29 směrnice (dále jen WP 29), 15. Března 2012, dostupné na www.iure.org/15/pracovní-skupina-podle-clanku-29-smernice-dale-jen-wp29

opatřeními, odpovídajícími riziky a mechanismy směrovanými ke správné identifikaci monitorovaných osob. [71]

2.5.13. Oznamovací povinnost správce

Správce je ještě před zahájením zpracovávání získaných dat povinen oznámit plánované zpracovávání osobních údajů Úřadu. Podle § 16 zákona o ochraně osobních údajů je správce povinen splnit oznamovací povinnost vždy, pokud se na něj nevztahuje některá z výjimek obsažených v § 18 zákona o ochraně osobních údajů.

Podle tohoto ustanovení se oznamovací povinnost nevztahuje na zpracování osobních údajů, které jsou součástí datových souborů veřejně přístupných na základě zvláštního zákona, ...nebo jde-li o zpracování, které sleduje politické, filosofické, náboženské nebo odborové cíle, prováděné v rámci oprávněné činnosti sdružení, a které se týká pouze členů sdružení, nebo osob, se kterými je sdružení v opakujícím se v kontaktu souvisejícím s oprávněnou činností sdružení, a osobní údaje nejsou zpřístupňovány bez souhlasu subjektu údajů.“[72]

Jelikož se kamerové systémy používají na zpracování osobních údajů, je tedy nutné pohlížet na ně ve smyslu § 16 zákona o ochraně osobních údajů. V některých případech jsou kamerové systémy určeny jako nutný prostředek pro naplnění práv a povinností vyplývající ze zvláštních předpisů. V takovém případě se na zpracování osobních údajů kamerovým systémem vztahuje výjimka uvedená v § 18 odst. 1 písm. b) zákona o ochraně osobních údajů [73]. [74]

Z § 4 zákona o ochraně osobních údajů, který definuje postavení správce[75] a zpracovatele,[76] vyplývá, že oznamovací povinnost náleží správci. Právě jemu přísluší

[71] Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance, 14.března 2012, G) Additional Requirements, dostupné na http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp89_en.pdf

[72] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 34

[73] Oznamovací povinnost podle § 16 se nevztahuje na zpracování osobních údajů,
b) které správci ukládá zvláštní zákon nebo je takových osobních údajů třeba k uplatnění práv a povinností vyplývajících ze zvláštního zákona, z. č. 101/2000 Sb. o ochraně osobních údajů o změně některých zákonů, ve znění pozdějších předpisů, § 18 odst. 1 písm. b)

[74] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 34-36

[75] j) správcem každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit

určení účelu, prostředků zpracování a případné pověření zpracovatele, který je příslušnou činností pověřen či zmocněn právě správcem, a to na základě smlouvy o zpracování osobních údajů podle § 6 zákona o ochraně osobních údajů. [77]

Oznamovací povinnost je nutná v případě prvotního oznámení Úřadu stejně tak při změně již registrovaného zpracování. [78] Nesplnění této povinnosti je důvodem ke zrušení zpracovávání osobních údajů prostřednictvím kamerového systému, a to rozhodnutím Úřadu, respektive autoritativním soudním rozhodnutím, jež je vynutitelné.

2.6. Rozdělení kamerových systémů podle umístění

Kamerové systémy lze rozdělit do několika skupin podle místa umístění kamer a především podle prostoru, který snímají. V současné době se můžeme s kamerovými systémy setkat téměř všude, a proto je třeba dbát výše stanovených pravidel, aby pojem „soukromí“ na úkor potřeb současné společnosti zcela nevymizel.

Studie politického sociologa Barringtona Morra, uvádí, že soukromí má všelidský charakter, jeho kořeny jsou v sociální sféře a je tedy sociálně vytvořené; v současné době plné technologií a sociální organizace vesměs postrádá svůj význam.[79]

Je tedy zjevné, že lze do soukromí osob zasáhnout prostřednictvím kamer, a to prakticky na jakémkoli místě, kde se bude fyzická osoba nacházet či pohybovat. Je však nutné, jak již bylo výše uvedeno, kontrolovat intenzitu a míru zásahu, jež by měla odpovídat danému cíli. [80]

S kamerovými systémy se tedy člověk může setkat:

- na veřejném prostranství
- na místě veřejně přístupném

---

zpracovatele, pokud zvláštní zákon nestanoví jinak, z. č. 101/2000 Sb. o ochraně osobních údajů o změně některých zákonů, ve znění pozdějších předpisů, § 4 písm. j)

[76] K) zpracovatelem každý subjekt, který na základě zvláštního zákona nebo pověření správce zpracováv osobní údaje podle tohoto zákona, z. č. 101/2000 Sb. o ochraně osobních údajů o změně některých zákonů, ve znění pozdějších předpisů, § 4 písm. k)

[77] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 34-36

[78] Tamtéž.

[79] NOVÁK, Daniel. *Problémy ochrany soukromí a osobních údajů v právu EU*. Brno, 2010/2011. Disertační práce. Právnická fakulta Masarykovy univerzity, str. 5

[80] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 46

- na pracovišti
- ve zdravotnickém zařízení
- v soukromých objektech pro potřeby soukromých účelů

3. Kamerové systémy na veřejném prostranství

„Veřejným prostranstvím jsou všechna náměstí, ulice, tržiště, chodníky, veřejná zeleň, parky a další prostory přístupné každému bez omezení, tedy sloužící obecnému užívání, a to bez ohledu na vlastnictví k tomuto prostoru.“[81]

Používané kamerové systémy na veřejném prostranství jsou městské dohlížecí kamerové systémy, dále jen MDKS, provozované obcemi, respektive obecní policií.[82] Užívání kamerových systémů městkou policií vyplývá z jejich základních úkolů, a to ochrany veřejného pořádku a bezpečnosti.[83]

Pro řešení jakéhokoliv problému ohledně kamerových systémů je třeba odpovědět si na pár základních otázek, ohledně jejich provozování a následného zpracování osobních údajů. Tedy:

- kdo provozuje MDKS – obecní policie
- za jakým účelem – zabezpečování veřejného pořádku
- informační povinnost vůči veřejnosti – prostřednictvím obecního úřadu
- kdo je odpovědným správcem – obec, jelikož právě ta zřizuje obecní policii

[81] §34 zákona č. 128/2000 Sb. o obcích (obecní zřízení), ve znění pozdějších předpisů

[82] Obecní policie je oprávněna, je-li to potřebné pro plenění jejích úkolů podle tohoto nebo jiného zákona, pořizovat zvukové, obrazové nebo jiné záznamy z míst veřejně přístupných, popřípadě též zvukové, obrazové nebo jiné záznamy o průběhu zákroku nebo úkonu, § 24 b odst. 1 z. č. 533/1991 Sb. o obecní policii, ve znění pozdějších předpisů

[83] Obecní policie při zabezpečování místních záležitostí veřejného pořádku a plnění dalších úkolů podle tohoto nebo zvláštního zákona

a) přispívá k ochraně a bezpečnosti osob a majetku,
b) dohlíží na dodržování pravidel občanského soužití,
c) dohlíží na dodržování obecně závazných vyhlášek a nařízení obce,
d) se podílí v rozsahu stanoveném tímto nebo zvláštním zákonem na dohledu na bezpečnost a plynulost provozu na pozemních komunikacích,
e) se podílí na dodržování právních předpisů o ochraně veřejného pořádku a v rozsahu svých povinností a oprávnění stanovených tímto nebo zvláštním zákonem činí opatření k jeho obnovení,
f) se podílí na prevenci kriminality v obci,
g) provádí dohled nad dodržováním čistoty na veřejných prostranstvích[5)] v obci,
h) odhaluje přestupky a jiné správní delikty, jejichž projednávání je v působnosti obce,
i) poskytuje za účelem zpracování statistických údajů Ministerstvu vnitra (dále jen „ministerstvo“) na požádání údaje o obecní policii, § 2 z. č. 533/1991 Sb. o obecní policii, ve znění pozdějších předpisů

Zjednodušeně řečeno, odpovědí na jednotlivé otázky je samotné zmocnění obce, jíž je obecní policie zřízena a na jehož základě zabezpečuje místní záležitosti - veřejný pořádek a bezpečnost.[84]

Kamerové systémy umístěné tak, aby monitorovaly veřejná prostranství, představují ze všech možných případů sledování prostor nejmenší zásah do soukromí. Zásah do soukromé sféry života člověka tak bude minimální, je-li respektován fakt, že bude monitorováno pouze veřejné prostranství a důsledně respektována povinnost nezahrnovat do záběru kamer soukromé prostory. V opačném případě dochází k překročení pravomocí a porušení právních předpisů, proti kterému se v rámci práva na ochranu soukromí může domáhat jakýkoliv subjekt ochrany, má-li důvodnou obavu domnívat se, že jeho soukromí bylo neoprávněně narušeno.

3.1. Případová studie v českém právním řádu

Jako ukázka negativního účinku při použití kamer na veřejném prostranství je příkladná kauza, která se odehrála v srpnu roku 2007 v Plzni[85], kde kamera, která měla původně sledovat dopravní situaci Na Belánce, rušné dopravní křižovatce, byla namířena přímo do oken jednoho ze zdejších bytů. Záběry získané touto kamerou byly přenášeny na webové stránky plzeňského magistrátu, byly tedy volně přístupné. Pochybení bylo přiřčeno městské policii, která byla Magistrátem města Plzeň pověřena obsluhou a správou kamer. Špatné, respektive nezákonné nasměrování předmětné kamery bylo způsobeno ruční manipulací jednoho ze strážníků městské policie. Majitel bytu se obrátil se stížností na Úřad pro ochranu osobních údajů, který jasně konstatoval porušení práva na soukromí.[86]

Základním pramenem pro právní zakotvení kamerových systémů v českém právním řádu, a to především s ohledem na ochranu osobních údajů, je ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod (dále jen Listina), kde čl. 7 odst. 1 uvádí:

---

[84] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 130

[85] Plzeňská městská kamera sledovala byt, ne křižovatku. *IDNES.cz* [online]. 2007[cit. 2012-03-16]. Dostupné z: http://zpravy.idnes.cz/plzenska-mestska-kamera-sledovala-byt-ne-krizovatku-pcf-/domaci.aspx?c=A070801_144158_domaci_hos

[86] Plzeňská městská kamera sledovala byt, ne křižovatku. *IDNES.cz* [online]. 2007[cit. 2012-03-16]. Dostupné z: http://zpravy.idnes.cz/plzenska-mestska-kamera-sledovala-byt-ne-krizovatku-pcf-/domaci.aspx?c=A070801_144158_domaci_hos

„ Nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem.“[87]

„Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.“[88]

S ohledem na dikci Listiny čl. 7 odst. 1 vyplývá přípustnost zásahu do soukromí, a to v případech stanovených zákonem. Je tedy třeba zkoumat, zda v daném případě některá ze zákonných výjimek existuje. MKDS smí monitorovat pouze veřejná prostranství, která jsou definována v § 34 zákona č. 128/2000 Sb., o obcích (obecní zřízení), ve znění pozdějších předpisů, dále jen zákon o obcích, jak je již výše uvedeno. Z tohoto ustanovení jasně vyplývá, že pokud kamera byla nasměrována do okna soukromého bytu, došlo k jasnému pochybení policejního orgánu.

Pokud MKDS je zřízen za účelem ochrany majetku obce, ochrany veřejného pořádku a kontroly uložených povinností, za které obec podle §10 zákona o obcích může v rámci samostatné působnosti ukládat sankce, pak v daném případě shromažďované informace daný účel rozhodně nenaplňovaly.[89]

Vezmeme-li v úvahu § 11 odst. 1 zákona o ochraně osobních údajů, který hovoří o povinnosti správce informovat subjekt o shromažďování údajů, především o jeho účelu a rozsahu, nemůžeme dojít k závěru, že daný občan byl přiměřeným způsobem o sledování svého bytu informován, a to ani za předpokladu, že se o sledování kamerovým systémem mohl dozvědět na webových stránkách plzeňského magistrátu, což by se dalo považovat za způsob uveřejnění použití provozování kamerového systému, nikoliv však za „vhodný způsob“, který jako podmínku sledování uvádí ve svém stanovisku ministerstvo vnitra.[90]

Problém celého případu je především v nasměrování kamery do oken soukromého bytu, což není monitorováním veřejného prostranství, ale bytové jednotky, a to bez splnění oznamovací či informační povinnosti správce, takže se jedná o porušení ústavně

[87] zákon č. 2/1993 Sb., Listina základních práv a svobod, čl. 7 odst. 1

[88] zákon č. 2/1993 Sb., Listina základních práv a svobod, čl. 10 odst. 3

[89] Aktualizované stanovisko k provozování kamerových systémů obecní policií –právní stav ke dni 10. října 2011, 18.března 2012, dostupné na http://www.google.com/cse?cx=015489265366623571386%3Aizzrwg3bmqm&q=kamerov%C3%A9+syst%C3%A9my&ok.x=0&ok.y=0&ok=ok#gsc.tab=0&gsc.q=kamerov%C3%A9%20syst%C3%A9my&gsc.page=1

[90] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str.153

zakotveného práva na soukromí. Zvážíme-li nastalou situaci z možného pohledu, že kamera byla nasměrována do oken bytu za účelem získání důkazů pro trestní řízení, a zahrneme-li do úvahy rozhodnutí Nejvyššího soudu:

„S ohledem na ustanovení § 89 odst. 2 tr. ř. lze za důkaz použitelný v trestním řízení pokládat též obsah obrazového záznamu z kamerového systému, který poškozený nainstaloval za účelem zjištění identity osoby poškozující jeho majetek (např. jeho obydlí, jeho automobil).“[91]

„Při využití takto získaných osobních údajů v souladu se zákonem (tj. jejich předáním orgánům činným v trestním řízení) pak i podle názoru Nejvyššího soudu nelze takové jednání považovat za zásah do soukromí zaznamenaných osob (k tomu srov. zejména str. 4/4 pravomocného přezkumného rozhodnutí předsedy Úřadu pro ochranu osobních údajů /dále jen „Úřad“/ ze dne 19.12.2008, zn. VER-2041/08-28).“[92]

„Přípustnost takového důkazu je však nezbytné vždy posuzovat i s přihlédnutím k právu na soukromí zakotvenému v čl. 8 Úmluvy o ochraně lidských práv a základních svobod a na nedotknutelnost osoby a jejího soukromí ve smyslu čl. 7 a čl. 10 odst. 2 Listiny základních práv a svobod. Přitom je třeba porovnat na jedné straně zájem na provedení trestního řízení, odhalení pachatele trestného činu a jeho potrestání, na straně druhé zájem na ochraně soukromí (srov. přiměřeně též č. 7/2008 Sb. rozh. tr.).“[93]

mohli bychom považovat takovýto postup za přípustný. V daném případě však o účel nalezení důkazů pro trestní řízení nešlo. Jedná se tedy o neoprávněný zásah do ústavně zaručeného práva na soukromí.

V případě porušení zákonem stanovených povinností správce a následným neoprávněným pořizováním záznamu kamerovým systémem může poškozený žádat

[91] Rozhodnutí předsedy Úřadu pro ochranu osobních údajů ze dne 19.12.2008, zn. VER-2041/08-28, 18.března 2012, dostupné na http://www.profipravo.cz/index.php?page=article&id_category=196&id_article=254228&csum=2b09ed87

[92] Nejvyšší soud (NS) ČR, 3 Tdo 593/2009 – Usnesení (Rt)[Důkaz] ASPI [databáze]. ASPI stav k 15.3.2012 [cit. 2012-03-18]

[93] Tamtéž.

provozovatele kamerového systému o nápravu, anebo přímo podat stížnost k Úřadu, a to i bez toho, že by požádal provozovatele o nápravu.[94]

Ve zmíněném plzeňském případu dospěl Úřad v červnu 2008 k závěru, že došlo k porušení zákona na ochranu osobních údajů, a uložil plzeňské radnici přijmout kroky k nápravě. Záznamy z kamer již neměly být přístupné na internetu a přístup úředníků magistrátu k záznamům měl být zamezen. Strážník, který byl zodpovědný za špatnou manipulaci s kamerou, byl finančně sankcionován.[95]

Úřad pro ochranu osobních údajů je správním orgánem, jenž zahajuje správní řízení z moci úřední. Stížnost podaná subjektem, který se důvodně domnívá, že byla porušena jeho práva, či jiným právním subjektem, který informuje úřad o porušení povinností daných zákonem na ochranu osobních údajů, je pouze podnětem pro zahájení správního řízení. Nejde o stížnost jako takovou, kdy by se stěžovatel mohl žalobou bránit proti nečinnosti správního úřadu. Považuje-li Úřad svá zjištění za dostatečná, vydá příkaz k odstranění nedostatků, proti kterému je přípustný odpor. Další spor mezi Úřadem a správcem osobních údajů se řeší správní žalobou. Náhrada škody dotčeným subjektům se pak vymáhá prostřednictvím občanskoprávní žaloby. Náhradu škody pak dotčené subjekty mohou vymáhat prostřednictvím občanskoprávní žaloby.

3.2. Komparace se situací ve Velké Británii

Pro porovnání s britskou judikaturou je příhodný případ Wood and Commissioner of Plolice for the Metropolis, Case No: C1/2008/1466 z dubna roku 2005[96], kdy se Andrew Wood, člen kampaně proti obchodu se zbraněmi, zúčastnil výroční valné hromady Reed Elsevier, informační společnosti pohybující se ve vědeckém, lékařském, právnickém a obchodním sektoru. Poté, co Adrew Wood opustil valné shromáždění, stal se objektem sledování místní policie, která opatřila několik snímků a snažila se dopátrat jeho

[94] Užij si svá práva.cz, Veřejné kamerové systémy, 18.března 2012, dostupné na http://www.uzijsisoukromi.cz/verejne-kamerove-systemy/
[95] Užij si svá práva.cz, Veřejné kamerové systémy, 18.března 2012, dostupné na http://www.uzijsisoukromi.cz/verejne-kamerove-systemy/
[96] England and Wales Court of Appeal (Civil Division) Decisions, Wood and Commissioner of Plolice for the Metropolis, Case No: C1/2008/1466, 18.březen 2012, dostupné na http://andrewwood.members.gn.apc.org/judicialreview/andrewwood_judgment_appeal_court_final.pdf

identity. Wood podal žalobu k soudu, kde napadl průběh policejního dozoru a pravomoc policejního orgánu vměšovat se do obchodních a politických záležitostí svých občanů.[97]

Soud rozhodl a v odůvodnění uvedl, že došlo k porušení čl. 8[98] Evropské úmluvy o lidských právech (dále jen EÚLP), tedy k porušení práva na respektování soukromého a rodinného života, a na základě znění tohoto článku, že bylo porušeno i relevantní ustanovení zákona o lidských právech (Human Rights Act 1998), jež je vnitrostátním předpisem britského práva. [99] Dále byl porušen britský zákon o ochraně osobních údajů – The Data Protection Act z roku 1998 (dále jen DPA).[100]

Britský odvolací soudu konstatoval, že k porušení práva je potřeba určitého stupně závažnosti útoku na Úmluvou zaručené právo, a jako kontrastní případ zmínil, že dle jeho názoru pouhé povrchní vyhledání osoby nestačí, podobně jako tomu bylo v případu R v. Gillan v Commissioner of Police for the Metropolis [2006] 2 AC 307, paragraph 28, kde narušení práva na soukromí jen stěží dosahovalo potřebné úrovně útoku pro aplikaci Úmluvy. Druhou podmínkou stanovil určité legitimní očekávání, tedy zda s ohledem na okolnosti dotyčná osoba důvodně očekávala určitý stupeň soukromí. V případě Andrew Wooda soud vydal rozhodnutí, ve kterém uvedl, že policie porušila zákon, když bezdůvodně sledovala občana, jež při svém pohybu, ač na veřejném

[97] England and Wales Court of Appeal (Civil Division) Decisions, Wood and Commissioner of Plolice for the Metropolis, Case No: C1/2008/1466, 18.březen 2012, dostupné na http://andrewwood.members.gn.apc.org/judicialreview/andrewwood_judgment_appeal_court_final.pdf

[98] Článek 8 (ECHR)- Právo na respektování soukromého a rodinného života
1. Každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence.
2. Státní orgán nemůže do výkonu tohoto práva zasahovat kromě případů, kdy je to v souladu se zákonem a nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, ochrany pořádku a předcházení zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných, Úmluva o ochraně lidských práv a základních svobod, Článek 8 - Právo na respektování soukromého a rodinného život, 17.března 2012, dostupné na http://www.ustrcr.cz/data/pdf/projekty/usmrceni-hranice/umluva.pdf

[99] Tamtéž.

[100] The Data Protection Act 1998 (DPA)
Zákon upravuje shromažďování, uchovávání a následné použití osobních údajů. Vztahuje se na fyzické a digitální formy informací včetně snímků zachycených kamerovými systémy. Podle zákona musí být všechny veřejné bezpečnostní kamery registrovány u informační komise (The Information Commissioner), která pro provozovatele kamerových systémů stanovuje určité podmínky. Provozovatel musí předem určit účel užití kamerového systému, ke kterému a pouze k němu by měli být užity získané informace. Provozovatel by dále měl uvést umístěný kamer, které by měli být instalovány tak, aby nedocházelo k zachycování invazivních či neopodstatněných obrazů. Následně mají jednotlivé subjekty právo na kopii veškerých údajů.
A Study of CCTV at Harvard, Legislation, 17.března 2012, dostupné na http://www.eecs.harvard.edu/cs199r/fp/JanaRachel.pdf

prostranství, očekával určitou míru soukromí. Rozsudek podložil rozhodnutím Rozsudku Evropského soudu pro lidská práva ve věci Marper v. Spojené království. [101]

Při komparaci s britským právním řádem je vhodné uvést fakt, že Spojené království se řídí jinou právní kulturou než Česká republika. Zatímco český právní řád je založen na základu kontinentálního práva, jež je založeno na psaném právu, kdy soudce právo nalézá, ale nevytváří, angloamerický systém, na němž je založena britská právní úprava, nemá vesměs psané právo, soudci mají v rukou právotvornou moc a vystupují jako tvůrci zákona. Součástí rozhodnutí je tzv. ratio decidendi, jež je precedenční částí rozhodnutí a je závazné do budoucna pro obdobné případy.

V rámci případu Wood v. Commissioner of Police for the Metropolis se v závěrečné řeči Lord Collins z Mapesbury zabýval problematikou přiměřenosti užívání snímků k policejním účelům. Zmínil důležitost užití dostupných moderních technologií, míněno kamerové systémy, orgány činnými v trestním řízení k získání důkazů o trestné činností. Konstatoval, že takto získaný důkaz má neocenitelnou hodnotu přesvědčivosti a objektivnosti. Umožňuje nevinné rychle z případu vyloučit a vinné rychleji usvědčit. Uzavřený televizní okruh označil za „jev, jenž má blahodárné účinky“.[102]

Na rozdíl od českého správního sytému, kde Úřad pro ochranu osobních údajů funguje jako správní dozor, který z moci úřední zahajuje správní řízení a případně je v postavení jako strana sporu při podání správní žaloby, Information Commissioner´s Office (dále jen ICO), jenž je britskou obdobou českého Úřadu, funguje jako dozor, jenž informuje o porušení zákona a následně iniciuje zahájení soudního řízení, v němž ale není stranou sporu, respektive rozhodnutí ICO jsou pod soudním dohledem. [103]

[101] England and Wales Court of Appeal (Civil Division) Decisions, Wood and Commissioner of Plolice for the Metropolis, Case No: C1/2008/1466, 18.březen 2012, dostupné na http://andrewwood.members.gn.apc.org/judicialreview/andrewwood_judgment_appeal_court_final.pdf

[102] England and Wales Court of Appeal (Civil Division) Decisions, Wood and Commissioner of Plolice for the Metropolis, Case No: C1/2008/1466, 18.březen 2012, dostupné na http://andrewwood.members.gn.apc.org/judicialreview/andrewwood_judgment_appeal_court_final.pdf

[103] ICO, About the ICO, 24.března 2012, dostupné na http://www.ico.gov.uk/about_us.aspx

4. Kamerové systémy na místech veřejně přístupných

„Místem veřejnosti přístupným je takové místo, kam má přístup široký okruh lidí individuálně neurčených a kde se také zpravidla více lidí zdržuje, takže hrubá neslušnost nebo výtržnost by mohla být postřehnuta více lidmi. Takové místo nemusí být přístupné bez omezení komukoli a kdykoli. Postačí, že je přístupné jen některým osobám za určitých okolností a určitou dobu…“[104]

Místo veřejně přístupné ve výše uvedeném smyslu je širokým pojmem, zahrnujícím taková místa, která jsou veřejností vyhledávána pro sportovní, kulturní nebo jiné společenské potřeby. Jsou jimi supermarkety a jiné obchody, banky, divadla a kina, plovárny, restaurace a mnohé další. Na místě veřejně přístupném fyzická osoba oprávněně očekává přiměřenou míru soukromí, a to alespoň takovou, která odpovídá danému místu.[105] Sledování by se mělo vyhnout místům jako jsou toalety, převlékárny a vymezené diskrétní zóny. V těchto prostorách je totiž nepopíratelně zvýšená hladina projevů osobní povahy, kterou nikdo nesmí sledovat, a to ani za předpokladu, že by na konkrétním místě bylo upozornění o instalaci kamerového zařízení.[106]

4.1. Případová studie v českém právním řádu

Pokud jsou tato místa monitorována kamerovým systémem, je to v prvé řadě z důvodu ochrany majetku, osob a bezpečnosti. Tento účel ochrany vlastnických práv, práv na ochranu života a zdraví zaměstnanců, hotelových hostů a ochranu dobrého jména uvedl jako účel ve své registraci provozovatel hotelového kamerového systému, který se stal předmětem soudního sporu[107] mezi vlastníkem hotelu a Úřadem pro ochranu osobních údajů. Žalobce – vlastník Hotelu[108], se domáhal zrušení rozhodnutí[109] Úřadu na ochranu osobních údajů, kterým nebylo povoleno zpracování osobních údajů prostřednictvím kamerového systému. Jako důvod zamítnutí bylo nesplnění podmínek stanovených

[104] Nejvyšší soud (NS) ČR, 8 Tdo 682/2009 – Usnesení [K trestnému činu výtržnictví – místo veřejnosti přístupné (§202)] ASPI [databáze] ASPI stav k 15.3.2012 [2012-03-18]
[105] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 118
[106] Tamtéž, str. 50
[107] Rozsudek Městského soudu v Praze, sp. zn. 11 Ca 433/2008-89, 19.března 2012, dostupné na http://www.uoou.cz/files/judik_rozsudek_ms_-_hotel.pdf
[108] Jméno hotelu bylo v získaném Rozsudku začerněno, proto je v této práci hotel s velkým H, jako zdůraznění, že se jedná o konkrétní zařízení
[109] Rozhodnutí Úřadu pro ochranu osobních údajů, zn. REG – 1218/08 ze dne 9.července 2008

zákonem, konkrétně porušení § 5 odst. 1 písm. e), § 5 odst. 2 a § 10 zákona o ochraně osobních údajů. [110]

Žalobce jako účel zřízení kamerového systému uvedl ochranu osob a majetku, zdraví a bezpečnost subjektů pohybujících se v prostorách hotelu. Konkrétně šlo o provozování kamerového systému v budově Hotelu a zároveň v jeho okolí - sledování vchodu, haly, recepce, vstupů do výtahu, restaurace a lobby-baru, provozních a technických prostor Hotelu a vnějších veřejných přilehlých prostor, tedy chodníku, vozovky a zastávky MHD před Hotelem. [111]

Dle Úřadu byl počet kamer nad míru zbytečný. Nehledě na to, že není žádné oprávnění monitorovat kamerami i zastávku MHD, která s Hotelem samotným nemá nic společného. Na zastávce, stejně jako na zmíněném chodníku a vozovce, se pohybují osoby, které nejsou hotelovými hosty ani náhodnými návštěvníky, takže ani v nejmenším nemohlo dojít k udělení souhlasu se zpracováním jejich osobních údajů a řádnému splnění informační povinnosti.

Vlastník Hotelu však namítl, že samotné pořizování záznamu kamerovým systémem, kde jsou zachyceny postavy a obličeje, nijak neumožňuje identifikovat daný subjekt. Na základě vizuálního záznamu není správce schopen přímo či nepřímo identifikovat zachycenou osobu, tedy se podle žalobce nejedená o osobní údaje ve smyslu zákona o ochraně osobních údajů. Úřad namítl, že § 4 písm. a) zákona o ochraně osobních údajů osobním údajem rozumí:

„… jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu“[112]

Záznam lidské tváře umožňuje jasně určit lidskou identitu, a to na základě fyziologických znaků. Je zřejmé, že žalovaný měl na mysli, že bez dodatečných informací o monitorované osobě není možné určit její identitu, a proto není třeba jejího

[110] Rozsudek Městského soudu v Praze, sp. zn. 11 Ca 433/2008-89, 19.března 2012, dostupné na http://www.uoou.cz/files/judik_rozsudek_ms_-_hotel.pdf
[111] Tamtéž.
[112] §4 písm. a) z. č. 101/2000 Sb. o ochraně osobních údajů o změně některých zákonů, ve znění pozdějších předpisů

souhlasu. Naopak osoby, které dodatečné informace poskytnou při zápisu na hotelové recepci, pak podávají, byť konkludentně, souhlas se zpracováním svých osobních údajů a není tedy žádné právní překážky k jejich monitorování. Úřad namítl, že i kdyby k identifikaci zaznamenané osoby bylo potřeba dalších údajů, je samotný záznam též osobním údajem a spadá pod aplikaci daného zákona s ohledem na fakt, že základním identifikačním znakem každé fyzické osoby je její vzhled. K udělování konkludentního souhlasu se vyjádřil tak, že o konkludentní souhlas by se jednalo pouze v případě, že by subjekt údajů při vstupu do Hotelu měl možnost využít své právo a souhlas se zpracováním osobních údajů by mohl neudělit.

Vlastník Hotelu dále tvrdil, že v jeho případě není ani souhlasu subjektu údajů zapotřebí, neboť jsou dány tři zákonné výjimky, a to dle § 5 odst. 2 písm. a), b), c)[113] zákona o ochraně osobních údajů. Je však nutné zmínit opět účel, pro který vlastník hotelu kamerový systém zřídil. Tedy na ochranu vlastnických práv (nejen svých, ale i hotelových hostů a příležitostných návštěvníků hotelu), práv na ochranu života a zdraví zaměstnanců (o této problematice více v další kapitole), stejně tak jako na ochranu dobrého jména hotelu. Vlastník Hotelu prohlásil, že jde o nabídku služeb nejvyšší úrovně a kamerový systém představuje minimální zásah do soukromí.[114]

Toto je však velmi diskutabilní. Je samozřejmé, že kamerové systémy jsou účinným prostředkem k ochraně vlastnických práv. Sám žalobce odkázal na §433 občanského zákoníku[115], který zavádí odpovědnost za vnesené věci do budovy Hotelu. Odpovědnost

---

[113] **(2)** Správce může zpracovávat osobní údaje pouze se souhlasem subjektu údajů. Bez tohoto souhlasu je může zpracovávat,

a) jestliže provádí zpracování nezbytné pro dodržení právní povinnosti správce,[12)]
b) jestliže je zpracování nezbytné pro plnění smlouvy , jejíž smluvní stranou je subjekt údajů , nebo pro jednání o uzavření nebo změně smlouvy uskutečněné na návrh subjektu údajů,
c) pokud je to nezbytně třeba k ochraně životně důležitých zájmů subjektu údajů. V tomto případě je třeba bez zbytečného odkladu získat jeho souhlas. Pokud souhlas není dán, musí správce ukončit zpracování a údaje zlikvidovat, z. č. 101/2000 Sb. o ochraně osobních údajů o změně některých zákonů, ve znění pozdějších předpisů

[114] Rozsudek Městského soudu v Praze, sp. zn. 11 Ca 433/2008-89, 19.března 2012, dostupné na http://www.uoou.cz/files/judik_rozsudek_ms_-_hotel.pdf

[115] (1) Provozovatel poskytující ubytovací služby odpovídá za škodu na věcech, které byly ubytovanými fyzickými osobami nebo pro ně vneseny, ledaže by ke škodě došlo i jinak. Vnesené jsou věci, které byly přineseny do prostor, které byly vyhrazeny k ubytování nebo k uložení věcí, anebo které byly za tím účelem odevzdány provozovateli nebo některému z pracovníků provozovatele.

je objektivní a k porušení zákonné povinnosti se nevyžaduje zavinění, čímž sám zákon motivuje provozovatele ubytovacích služeb k předcházení takových incidentů. [116] Úřad však namítl, že v souladu s uvedeným ustanovením občanského zákoníku by byl vlastník Hotelu oprávněn sledovat jen ta místa, kam by věci byly uloženy, vneseny, respektive místa k tomu určená. Dle jeho slov to popírá nutnost monitorovat hosty, návštěvníky a zaměstnance.[117] Avšak stojí za úvahu, zda a jak by utrpěla prestiž Hotelu, kdyby návštěvníkům baru nebo restaurace byly odebírány kabelky a příruční zavazadla. Na stranu druhou hoteloví hosté si věci ukládají především ve svých pokojích a monitorování pokojů je příliš velký zásah do soukromí oproti sledování hotelové haly nebo restauračního zařízení, kde je narušení soukromí očekávatelné i přiměřené. Majitel Hotelu namítl, že v této situaci zákon výslovného souhlasu subjektů údajů nevyžaduje a to na základě § 5 odst. 2 písm. e) zákona o ochraně osobních údajů[118], podle kterého provozovatel „*…shledává kamerový systém naprosto nezbytný pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby. Hosté o systému vědí a provoz kamerového systému nevnímají vůbec jako zásah do svých práv, ale naopak jako opatření pro jejich ochranu.“*[119]

Úřad oponoval tím, že správce sice hovoří o ochraně práv správce, ale vlastník Hotelu však již jmenovitě neuvádí, o která jeho práva jako správce se jedná. I když, jak už bylo řečeno, provozovatel zmiňuje majetkové a právem chráněné zájmy třetích osob, zákon sám takovéto zájmy nezná. Dále Úřad nepřijal tvrzení, že osoby, pohybující se v Hotelu,

---

(2) Je-li s provozováním nějaké činnosti zpravidla spojeno odkládání věcí, odpovídá ten, kdo ji provozuje, občanovi za škodu na věcech odložených na místě k tomu určeném nebo na místě, kam se obvykle odkládají, ledaže by ke škodě došlo i jinak.
§ 433 z. č. 40/1964 občanský zákoník, ve znění pozdějších předpisů

[116] FIALA, Josef. Komentář k §433 zák. č. 40/1964 Sb. [Odpovědnost za vnesené a odložené věci] ASPI [databáze]. ASPI stav k 15.3.2012 [cit. 2012-03-19]

[117] Rozsudek Městského soudu v Praze, sp. zn. 11 Ca 433/2008-89, 19.března 2012, dostupné na http://www.uoou.cz/files/judik_rozsudek_ms_-_hotel.pdf

[118] **(2)** Správce může zpracovávat osobní údaje pouze se souhlasem subjektu údajů. Bez tohoto souhlasu je může zpracovávat,
e) pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby; takové zpracování osobních údajů však nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života, § 5 odst. 2 písm. e) z. č. 101/2000 Sb. o ochraně osobních údajů o změně některých zákonů, ve znění pozdějších předpisů

[119] Rozsudek Městského soudu v Praze, sp. zn. 11 Ca 433/2008-89, 19.března 2012, dostupné na http://www.uoou.cz/files/judik_rozsudek_ms_-_hotel.pdf

akceptují provoz kamerového systému, neboť bez dostatečného splnění informační povinnosti o něm ani neví.[120]

Úřad ve svém rozhodnutí dále napadal dobu zpracování osobních údajů, která mu v rozmezí 8-12 dní přišla nepřiměřená. Sám navrhl dobu od 3 do 4 dnů s následným vymazáním a s možností uchování deliktních incidentů po dobu delší, odděleně od ostatních záznamů. Vlastník Hotelu označil za nemožné selektovat záběry deliktních incidentů a zároveň se ohradil, že Úřad své doporučení doby pro uchování záznamu nijak nepodložil ani neodůvodnil. „Přiměřenost" doby tedy není nijak přiřaditelná. Úřad však později uvedl, že pokud je kamerový systém zaveden z důvodu ochrany majetku, jsou krádeže zavazadel či jiných věcí hostů zjišťovány obvykle do 48 hodin, což je logické už z důvodu, že se okradený subjekt neprodleně ozve a krádež oznámí.[121]

Úřad sám zdůraznil ve svém rozhodnutí, že neshledává nezákonným kamerový systém obecně, ale posouzením konkrétních okolností instalace kamerového systému dovodil závěr, že nejsou splněny zákonem dané podmínky jeho provozování. Sledování prostoru hotelu za stanoveným účelem shledal jako legální a legitimní prostředek, avšak považuje za nutné posoudit zásahu do osobních práv sledovaných osob ve smyslu daného zákona, především zda je míra tohoto zásahu je adekvátní sledovanému účelu. Tomu totiž odporuje skutečnost, že sledované subjekty byly zaznamenávány při svých schůzkách, rozhovorech a dalších činnostech, které podávají komplexní informace o sledované osobě, jsou tedy již nad rámec účelu a kamerový systém staví do nezákonné roviny. Sám soud zhodnotil, že jde bezpochyby o shromažďování osobních údajů, neboť subjekty zachycené na záznamu mohou být později identifikovány.

Soud dále zkoumal problematiku konfliktu ochrany dvou práv uvedených v Listině základních práv a svobod, která jednak deklaruje nedotknutelnosti osoby a jejího soukromí, právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním osobních údajů, a jednak právo vlastnit majetek včetně práva na jeho ochranu. Také zmínil již judikovaný názor[122], že při střetu dvou zájmů je třeba přiznat větší váhu zájmu na ochranu soukromí jako jednomu ze základních lidských

[120] Rozsudek Městského soudu v Praze, sp. zn. 11 Ca 433/2008-89, 19.března 2012, dostupné na http://www.uoou.cz/files/judik_rozsudek_ms_-_hotel.pdf
[121] Rozsudek Městského soudu v Praze, sp. zn. 11 Ca 433/2008-89, 19.března 2012, dostupné na http://www.uoou.cz/files/judik_rozsudek_ms_-_hotel.pdf
[122] Rozsudek Městského soudu v Praze, sp. zn. 7 Ca 204/2005ze dne 28:2:2007; Rozsudek Městského soudu v Praze, sp. zn. 11 Ca 298/2008-47 ze dne 30.11.2009

práv. S přihlédnutím k nálezu Ústavního soudu[123] soud rozhodl, že právu na ochranu majetku bylo v tomto případě dáno bezdůvodně přednost.

Soud dále zamítl námitku na aplikaci výjimek obsažených v § 5 odst. 2 zákona na ochranu osobních údajů a podanou žalobu proti rozhodnutí Úřadu zamítl.

4.2. Komparace se situací ve Velké Británii

Z dění ve Spojeném království stojí za zmínku projekt nazvaný „Internet Eyes“, v překladu Internetové oči.[124] V říjnu 2009 Tony Morgan založil firmu Internet Eyes Limited, jejíž podnikání bylo založeno na internetové aplikaci, kde by se promítaly záběry zachycené přístroji kamerových systémů umístěných v obchodech, nádražích, bankách a samozřejmě na ulicích. Tyto záběry měly sledovat najmutí brigádníci nebo pracovníci. Nakonec byl systém nastaven tak, že na určených stánkách se může zaregistrovat jakýkoliv občan a promítané záběry sledovat; jeho motivací je finanční odměna za sledování kamerových záběrů. Společnost oceňuje nejen čas strávený na stránkách pozorováním záběrů, ale honoráře zvyšuje při odhalování zločinnosti, což je primárním cílem tohoto projektu.. [125]

Zajímavé je, že při spuštění tohoto systému 4. října 2010 se neozývaly žádné protesty od místních občanů, žádné námitky ani negativní postoje. Příčinou bylo téměř neviditelné informování místních médií. Přitom bylo možné nalézt několik důvodů, proč takový systém zpochybnit. ICO nejprve plánovaný projekt „privatizace kamerového sledování“[126] odmítala a jeho spuštění proto muselo být odloženo.

---

[123] Č.j. IV. ÚS 154/97: „Při střetu práva na informace a jejich šíření s právem na ochranu osobnosti a soukromého života, tedy základních práv stojících na stejné úrovni, je především věcí obecných soudů, aby s přihlédnutím k okolnostem každého případu zvážily, zda jednomu právu nebyla bezdůvodně dána přednost před právem druhým.“
Ústavní soud (ÚS), IV. ÚS 154/97 – Nález (ÚS) [Lidská důstojnost, osobní čest, dobrá pověst] ASPI [databáze] ASPI stav k 15.3.2012 [cit. 2012-03-21]

[124] Kamerové sledování prostřednictvím internetových stránek The Internet Eyes je projekt soukromé společnosti za použití soukromých kamer za účasti občanů. Jedná se o privatizaci dozoru státu. BBC New, Public to monitor CCTV from home, 21.března 2012, dostupné na http://news.bbc.co.uk/2/hi/uk_news/england/london/8293784.stm

[125] Lupacz, Sledování odstartovalo. Je to bezpečnostní průšvih, 21.března 2012, dostupné na http://www.lupa.cz/clanky/sledovani-londynanu-zacalo-bezpecnostni-prusvih/

126 Kamerové sledování prostřednictvím internetových stránek The Internet Eyes je projekt soukromé společnosti za použití soukromých kamer za účasti občanů. Jedná se o privatizaci dozoru státu. BBC New, Public to monitor CCTV from home, 21.března 2012, dostupné na http://news.bbc.co.uk/2/hi/uk_news/england/london/8293784.stm

Následně byl však projekt spuštěn, a to se souhlasem ICO, které potvrdilo splnění všech podmínek správce.[127]

Při zpracovávání osobních údajů se musí dodržovat určitá pravidla, a to především s ohledem na právo na ochranu soukromí, dle čl. 8 EÚLP. Dle britského regulátora pro ochranu osobních údajů ICO a právní úpravy, především DPA 1998, musí správce před zprovozněním kamerového systému určit účel, pro který budou osobní údaje zpracovávány, stejně jako tomu je v české právní úpravě. Otázkou je, zda za stanoveným účelem, a to potlačováním vandalismu, prevence a odhalování trestné činnosti a terorismu, lze v takovéto míře narušovat soukromí. Jak již bylo uvedeno, na veřejných prostranstvích a veřejně přístupných místech může člověk očekávat jen určitou míru soukromí a obeznámen s touto skutečností měl by podle ní jednat. Vneseme-li však toto pravidlo do případu Peck v. The United Kingdom[128], zjistíme, že právo na ochranu osobních údajů dle čl. 8 EÚLP je nepopiratelné, a to ať už subjekt údajů se svým soukromím nakládá jakkoli, respektive ať už se na veřejnosti chová jakkoli, pokud to není v rozporu se zákonem.

Pan Peck, trpící depresemi, se pokusil spáchat sebevraždu tím, že si chtěl podřezat zápěstí. Naneštěstí si pro svůj plán vybral veřejně místo, které bylo monitorováno kamerovým systémem. Pan Peck, aniž by si toho byl vědom, byl natočen kamerou, jak drží kuchyňský nůž v ruce.[129] Posoudíme-li případ pana Pecka z hlediska stanoveného účelu, nesplňuje ani jeden z bodů. Kamerový systém v chování pana Pecka nezaznamenal ani vandalismus, zločinnou činnost či šíření terorismu. Přesto do jeho chování zasáhla policie a podle zákona na ochranu duševního zdraví (the Mental Health Act 1983) osobu zadržela.

Tím však případ *Peck v. The United Kingdom* nekončí. O několik měsíců později vydala Rada[130] několik fotografií pořízených z uvedeného kamerového záznamu, a to jako podklad k článku o preventivních přínosech kamerových systémů. Fotografie byly

[127] Kamerové sledování prostřednictvím internetových stránek The Internet Eyes je projekt soukromé společnosti za použití soukromých kamer za účasti občanů. Jedná se o privatizaci dozoru státu. BBC New, Public to monitor CCTV from home, 21.března 2012, dostupné na http://news.bbc.co.uk/2/hi/uk_news/england/london/8293784.stm

[128] European Court of Human Rights, CASE OF PECK v. THE UNITED KINGDOM, Application no. 44647/98, 21.března 2012, dostupné na http://www.worldlii.org/eu/cases/ECHR/2003/44.html

[129] Tamtéž.

[130] Brentwood Borough Council

zveřejněny i v regionální televizi, kde už byla tvář pana Pecka na žádost Rady zakryta. Soud v tomto případě konstatoval vážný zásah do soukromí subjektu. Především porušení čl.8 EÚLP, který připisuje každému právo na soukromí a rodinný život. Užití záznamu nebylo v souladu s určeným účelem, pro který je kamerový systém provozován, a osobní údaje nebyly shromažďovány v souladu s tímto účelem. Vezmeme-li v úvahu, že dle zákona na ochranu duševního zdraví by byla určitá právní možnost na základě záběru subjekt údajů zadržet, pak ale není dáno žádné zákonné oprávnění užít tyto záběry pro, řekněme, popularizaci účinnosti užívání kamerových systémů v regionální televizi. Ač byla tvář pana Pecka zakryta, byly zřetelné i další fyziologické znaky, podle kterých mohla být jeho osoba rozpoznána, a tím bylo vážně narušeno jeho soukromí. Tak uvedl Evropský soud pro lidská práva.[131]

Vrátíme se zpět k projektu The Internet Eyes a porovnáme ho s případem Peck v. The United Kingdom. Zjistíme, že i když je účel kamerového systému dostatečně určitý, není možné zabránit, aby kamery nesledovaly i další činnosti, pro daný účel irelevantní a tedy narušující soukromí.

Diskutabilní otázkou je informační povinnost správce. To, že jsou občané informováni o monitorovacím projektu a o skutečnosti, že mohou být sledování téměř na každém kroku, ještě neznamená, že jsou si v dané situaci, na daném místě vědomi, že je právě sleduje některá z kamer. Nehledě na způsob zpracování, kdy je může pozorovat kdokoli, nikoli jen určený správce nebo jím pověřený zaměstnanec. Samozřejmě se nabízí otázka, zda je vůbec takové užívání kamerového systému přiměřené, zda by k danému účelu nestačilo nasazení dostatečného počtu strážníků a privátního dozoru v obchodech a jiných veřejně přístupných místech a zda je tedy v souladu s podmínkami provozování kamerových systémů, jež stanovuje ICO.[132]

Projekt The Internet Eyes byl nakonec ICO schválen. V konkrétních případech je však subjekt osobních údajů nadále oprávněn podat žalobu k soudnímu přezkoumání daného případu, zda pořízení záznamu bylo ještě v souladu se zákonem o ochraně osobních

[131] NOUWT, Sjaak. Reasonable Expectations of Privacy?: Eleven country reports on camera surveillance and workplace privacy (Information Technology and Law Series). The Hague: T.M.C. Asser Press, 2005. ISBN 9789067041980, str. 109-110

[132] NOUWT, Sjaak. Reasonable Expectations of Privacy?: Eleven country reports on camera surveillance and workplace privacy (Information Technology and Law Series). The Hague: T.M.C. Asser Press, 2005. ISBN 9789067041980, str. 106

údajů DPA, zda kamerový systém splňuje registrační podmínky dané ICO či nebyl-li porušen čl. 8 EÚLP.

5. Kamerové systémy na pracovišti

Pracoviště[133] je již specifické místo, které smí být sledováno průmyslovými kamerami. Elementární důvody užívání kamer na pracovišti se nachází v § 316 zákona č. 262/2006 Sb., zákoníku práce, ve znění pozdějších předpisů (dále jen zákoník práce).[134]

Dodržování zákazů je zaměstnavatel oprávněn kontrolovat pomocí kamerového systému a přiměřeným způsobem tak monitorovat své zaměstnance. Pro účely této diplomové práce je důležitý odstavec 3 § 316 zákoníku práce[135], podle kterého však zaměstnavatel nesmí bez závažného důvodu podrobovat zaměstnance otevřenému či skrytému sledování, odposlechu a záznamu telefonních hovorů, kontrole elektronické pošty a listovních zásilek. Pokud existuje závažný důvod, který spočívá ve zvláštní povinnosti[136] zaměstnance, pak je zaměstnavatel povinen o rozsahu monitoringu pracovní činnosti zaměstnance informovat.[137]

Základní body stanovené zákoníkem práce pro používání monitoringu na pracovišti musí být splněny, ať už se jedná o kamerový systém se záznamem nebo bez záznamu, tedy online. Zda jsou zásady stanovené v zákoníku práce respektive v § 316 odst. 2 zákoníku práce dodržovány, kontroluje Státní úřad inspekce práce.

Státní úřad inspekce práce je orgánem státní správy, jehož úkolem je kontrolovat dodržování povinností plynoucích z pracovněprávních předpisů včetně předpisů o bezpečnosti a ochraně zdraví při provádění pracovní činnosti. Je to orgán ochrany pracovních vztahů. Hlavním cílem činností Státního úřadu inspekce práce je nikoliv

[133] „pravidelným pracovištěm rozumí místo dohodnuté se zaměstnancem, a není-li takové místo dohodnuto, je pravidelným pracovištěm místo výkonu práce sjednané v pracovní smlouvě." VYSOKAJOVÁ, Margerita. Komentář k § 34 zák. č. 262/2006 Sb. [Náležitosti pracovní smlouvy] ASPI [databáze] ASPI stav k 15.3.2012 [cit. 2012-03-21]

[134] § 316 odst. 1 z. č. 262/2006 Sb. zákoníku práce, ve znění pozdějších předpisů: „Zaměstnanci nesmějí bez souhlasu zaměstnavatele užívat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele včetně výpočetní techniky ani jeho telekomunikační zařízení. Dodržování zákazu podle věty první je zaměstnavatel oprávněn přiměřeným způsobem kontrolovat."

[135] § 316 odst. 2 z. č. 262/2006 Sb. zákoníku práce, ve znění pozdějších předpisů: „Zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci."

[136] „zvláštní povinnost" není nikde v judikatuře definována. Pro představu je vhodné si představit pracoviště, kde se manipuluje s vysokými hodnotami, kde je zvýšené riziko ohrožení chráněných hodnot, nebo kde je zvýšené riziko pracovních úrazů. JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 54

[137] Tamtéž.

represe, ale prevence, tedy předcházení negativních jevů a situací na pracovišti. Státní úřad inspekce práce však nemá žádnou pravomoc k ukládání správně právních sankcí při porušení práva zaměstnanců na ochranu soukromí.[138]

Pokud orgán inspekce dojde k závěru, že instalace kamerového systému na pracovišti neodpovídá zákonným podmínkám, pak je oprávněn zrealizovat kontrolu, a je-li to důvodné, uložit opatření k nápravě, spočívající v zákazu monitoringu či jeho omezení jen na určitá místa, a určit, kde jsou zákonem daná pravidla porušena. Dál má úřad oprávnění uložená opatření kontrolovat. Ve zmíněné organizaci kontroly však existuje mezera, a to ve fázi, kdy zaměstnavatel neplní nebo odmítá plnit uložená opatření. Orgán inspekce práce totiž nemá nikde v zákonné úpravě udělenou pravomoc k vymáhání uložené sankce. Jediné, co v takovém případě zaměstnanci zbývá, pokud je dle jeho názoru neprávem monitorován na pracovišti, je podání občanskoprávní žaloby.[139]

Základním problémem přezkoumávání výše uvedeným úřadem z hlediska kamerových systémů, je tvrzení zaměstnavatele, že právě pracovní činnosti na jeho pracovišti mají zvláštní povahu, a proto je bez pochyby oprávněn k užívání kamerového systému. Zaměstnavatelé mají za to, že sledování na pracovišti je účelné z hlediska zjišťování, zda zaměstnanci důsledně plní své pracovní povinnosti a dodržují pracovní dobu. Zároveň z hlediska kontroly pohybu návštěvníků v prostorách pracovního objektu z důvodu ochrany majetku. Avšak i na pracovišti je třeba dodržovat určitou míru soukromí.[140]

„…I kdyby bylo možno souhlasit s názorem soudu prvního stupně, že kancelář vedoucího odboru dopravy a silničního hospodářství v budově Městského úřadu Rychnova nad Kněžnou je veřejným prostorem, protože je v ní vykonávána veřejná moc, pak z toho nelze vyvodit, že by kdokoliv na místě výkonu státní služby postrádal soukromí. I když je kvalita (resp. rozsah) tohoto soukromí zcela nepochybně jiná než na jiných místech, přesto nelze akceptovat názor, že vůbec neexistuje, resp. že vůbec nepožívá ochrany čl. 8 Úmluvy[141], což přiměřeně platí i pro osoby, které v takových

[138] Státní úřad inspekce práce, Základní údaje, 5. března 2012, dostupné na http://www.suip.cz/o-nas/zakladni-udaje/
[139] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505,str. 56
[140] Tamtéž, str. 52-56
[141] Čl. 8 ECHR garantuje právo každého na respektování jeho soukromého a rodinného života, obydlí a korespondence s tím, že orgány státu mohou do výkonu tohoto práva zasahovat jen v případě, kdy je to

prostorech vykonávají státní službu. Lze naopak poukázat na to, že ochrana soukromí obecně všech zaměstnanců je nyní zákonodárcem na úrovni podústavního práva výslovně zakotvena v § 316 odst. 2 zákoníku práce. …Veřejné prostory, v nichž se vykonává veřejná moc, by tedy bylo možné soustavně monitorovat jen v legitimním zájmu a při vědomí všech dotčených osob. …Skryté sledování orgány veřejné moci je proto s ohledem na shora uvedené základní právo na ochranu soukromí možné vždy jen v legitimním zájmu a na základě zákona.“[142]

Může nastat situace, kdy zaměstnavatel, nejistý si svým právem na monitorování zaměstnanců či naplněním zmíněné podmínky spočívající ve zvláštní povaze činnosti zaměstnance, začlení do pracovní smlouvy požadavek, aby zaměstnavatel udělil souhlas s monitorováním svého pohybu na pracovišti. Zaměstnanec udělí souhlas nejpravděpodobněji ze strachu ze ztráty pracovního místa. Taková cesta je však v rozporu se samotnými základními lidskými právy a svobodami, která jsou nezadatelná, nezcizitelná, nepromlčitelná a nezrušitelná. To znamená, že nikomu nemohou být odpírána, stejně tak se jich nikdo nemůže vzdát. V této konkrétní problematice by se zaměstnanec předem vzdával práva na ochranu soukromí na pracovišti, což je nepřípustné. [143]

„Podle § 4 písm. n) zákona o ochraně osobních údajů je souhlasem subjektu údajů svobodný a vědomý projev vůle, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů. Souhlas se zpracováním osobních údajů je tedy projevem vůle subjektu údajů (jednostranným právním úkonem), a ne dvoustrannou smlouvou mezi správcem a subjektem údajů. Již z tohoto důvodu lze uvést, že zařazení souhlasu se zpracováním osobních údajů do smluvního ujednání je nevhodné a pro subjekt údajů matoucí, neboť s vlastním smluvním ujednáním nemá nic společného. Naopak, subjekt údajů nad rámec vlastního smluvního vztahu souhlasí, aby správce použil jeho osobní údaje za stanoveným účelem. Z toho vyplývá, že souhlas se zpracováním osobních údajů nemůže a nesmí být podmínkou, která by sama o sobě znemožňovala (v případě

---

v souladu se zákonem a nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, předcházením nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných.

[142] II.ÚS 2806/08, 5.března 2012, dostupné na http://nalus.usoud.cz/Search/ResultDetail.aspx?id=64936&pos=1&cnt=1&typ=result

[143] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 55

jeho neudělení) uzavření smluvního vztahu, neboť osobní údaje nemohou být vedle peněz dalším platidlem za poskytnutou službu nebo zboží.“[144]

5.1. Případová studie v českém právním řádu

„Firma prováděla kamerové sledování celého areálu firmy, tedy dílen a provozu, kde byla zajišťována výrobní činnost. Záznamy byly uchovávány po dobu jednoho týdne, vyhodnocovány managementem a na základě jejich vyhodnocení byla přijímána i nápravná opatření směřovaná proti jednotlivým zaměstnancům. Jednalo se např. o napomenutí zaměstnance pro porušení pracovní kázně s odůvodněním, že pracovník při noční směně vypnul technologické zařízení, spal a nepracoval. Tento pracovník následně podal stížnost pro využívání kamerového systému.“[145]

Podíváme-li se na uvedený případ z pohledu zákoníku práce, respektive povinností zaměstnavatele dle § 302 [146], § 101 odst. 1[147] a § 248 odst. 2[148], je kontrola pracovní činnosti, organizování pracovní náplně, zabezpečování ochrany zdraví při práci a také ochrana majetku (vlastníka podniku i samotných zaměstnanců) bezpochyby možným účelem pro zpracování osobních údajů.

V uvedeném případu však nebyla řádně splněna informační povinnost správce, jak při svém přezkumu zjistil Úřad. Zaměstnanci byli o provozu kamerového systému v objektu informováni pouze tabulkou s nápisem: „Prostory jsou monitorovány

[144] Úřad pro ochranu osobních údajů, Stanovisko č. 2/2011, 5. březen 2012, dostupné na http://www.uoou.cz/files/stanovisko_2011_2.pdf

[145] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 76 – Ilustrační případ č. 1

[146] Vedoucí zaměstnanci jsou dále povinni
a) řídit a kontrolovat práci podřízených zaměstnanců a hodnotit jejich pracovní výkonnost a pracovní výsledky,
b) co nejlépe organizovat práci,
c) vytvářet příznivé pracovní podmínky a zajišťovat bezpečnost a ochranu zdraví při práci,
f) zabezpečovat dodržování právních a vnitřních předpisů,
g) zabezpečovat přijetí opatření k ochraně majetku zaměstnavatele.
§ 302 písm. a), b), c), f), g) z. č. 262/2006 Sb. zákoník práce, ve znění pozdějších předpisů

[147] (1) Zaměstnavatel je povinen zajistit bezpečnost a ochranu zdraví zaměstnanců při práci s ohledem na rizika možného ohrožení jejich života a zdraví, která se týkají výkonu práce (dále jen "rizika").
§ 101 odst. 1 z. č. 262/2006 Sb. zákoník práce, ve znění pozdějších předpisů

[148] (2) Zaměstnavatel je z důvodu ochrany majetku oprávněn v nezbytném rozsahu provádět kontrolu věcí, které zaměstnanci k němu vnášejí nebo od něho odnášejí, popřípadě provádět prohlídky zaměstnanců. Při kontrole a prohlídce podle věty první musí být dodržena ochrana osobnosti. Osobní prohlídku může provádět pouze fyzická osoba stejného pohlaví.
§ 248 odst. 2 z. č. 262/2006 Sb. zákoník práce, ve znění pozdějších předpisů

kamerovým systémem“. To by však znamenalo, že kamery nepořizují záznam (šlo by o sledování online), a nedocházelo by ke zpracování osobních údajů. Zde však záznam pořizován byl a o zpracovávání osobních údajů se tedy jednalo. Výše uvedený text na tabulce však byl zcela nedostatečný, neboť ke splnění informační povinnosti by muselo být zaměstnancům sděleno, nejen kdo osobní údaje zpracovává a jaké k tomu využívá prostředky (v případě kamerového systému je toto zřejmé), ale také za jakým účelem osobní údaje shromažďuje, jak dlouho je uchovává před jejich likvidací a kde je případně možné záznam se osobními údaji shlédnout. Úřad pro ochranu osobních údajů v tomto případě shledal porušení zákona. Zajímavé je porovnat výše uvedený spor s jiným případem, kdy majitel podniku nainstaloval kamerový systém v kanceláři pokladní za účelem ochrany majetku. Systém spouštěl současně s uzamčením objektu a aktivací alarmu, tedy v době, kdy se po prostorách objektu žádný zaměstnanec nepohyboval. Kamerový systém tedy nebyl zřízen pro účely sledování zaměstnanců při jejich pracovní činnosti. Ve spolupráci s Policií ČR byl vyhodnocen videozáznam, ze kterého byla odhalena pachatelka, bývalá manželka majitele podniku, která se následně k činu doznala. Ač byl kamerový systém provozován se záznamem a jednalo by se o zpracování osobních údajů, byl provozován pro ochranu majetku a v uzavřeném prostoru bez možnosti přístupu osob, nebylo v tomto případě Úřadem shledáno porušení zákona na ochranu osobních údajů ani zákoníku práce.[149]

Pokud má tedy zaměstnanec důvodné podezření, že zaměstnavatel narušuje jeho soukromí monitorováním, o jehož rozsahu a způsobu jej dostatečně neinformoval nebo k němuž mu neposkytl souhlas, a to svobodně, vážně, určitě a srozumitelně, nebo že zaměstnavatel, přestože splnil všechny povinnosti správce, monitoruje zaměstnance i na místech a v době, kdy nevykonávají práci, je oprávněn se u zaměstnavatele domáhat upuštění od jeho jednání, anebo přímo, i bez jednání se zaměstnavatelem, podat stížnost k Úřadu pro ochranu osobních údajů. [150] Toto tvrzení je však v rozporu s novelizací zákona č. 439/2004 Sb., která ustanovení o možnosti podání stížnosti k Úřadu poškozeným zaměstnancem ze zákona vyjmula; litera zákona tedy podání stížnosti k Úřadu jednotlivcem odmítá.[151]

[149] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 76 – 77 – Ilustrační případ č. 2
[150] Užij si svá práva.cz, Sledování na pracovišti, 21.březen 2012, dostupné na http://www.uzijsisoukromi.cz/sledovani-na-pracovisti/
[151] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 75

Na otázku, jaký právní účinek má podle § 21 odst. 1, respektive odst. 3 zákona o ochraně osobních údajů[152] podání stížnosti poškozeným zaměstnancem k Úřadu, zda se jedná o stížnost, nebo pouze o podnět, tedy zda se Úřad stížností zabývat musí, nebo zda je podaná stížnost pouze podnětem pro zahájení šetření ex offo, odpovídá rozhodnutí Nejvyššího správního soudu[153]. Dle jeho judikatury je podnětem, čímž je rozuměno takové podání ke správnímu orgánu, které nezakládá právo úspěšně se domáhat žalobou na ochranu proti nečinnosti správního orgánu; je tedy pouze podnětem k zahájení řízení ex offo.[154] Spornou situaci řeší fakt, že po novele zákona byl vyškrtnut odstavec 3 § 21, který uváděl: „*Nevyhoví-li správce nebo zpracovatel žádosti subjektu údajů podle odstavce 1, má subjekt údajů právo obrátit se přímo na Úřad.“* Dříve tedy byla dána aktivní legitimace zaměstnance, po novelizaci zákonem č. 439/2004 Sb. byla však možnost podání stížnosti jednotlivcem odejmuta.[155]

5.2. Komparace se situací ve Velké Británii

Britská úprava též omezuje užívání kamerového systému na pracovišti k monitorování zaměstnanců jejich zaměstnavateli ve smyslu DPA 1998. Ze znění tohoto zákona vyplývá, že stejně jako v české právní úpravě, i ve Spojeném království je nutné získat souhlas od zaměstnance ke zpracovávání jeho osobních údajů, získaných kontrolou jeho telefonních hovorů, e-mailové schránky a monitorováním jeho pohybu po pracovišti prostřednictvím kamerového systému. Tento prostředek zpracování osobních údajů byl

[152] **(1)** Každý subjekt údajů, který zjistí nebo se domnívá, že správce nebo zpracovatel provádí zpracování jeho osobních údajů, které je v rozporu s ochranou soukromého a osobního života subjektu údajů nebo v rozporu se zákonem, zejména jsou-li osobní údaje nepřesné s ohledem na účel jejich zpracování, může

a) požádat správce nebo zpracovatele o vysvětlení,
b) požadovat, aby správce nebo zpracovatel odstranil takto vzniklý stav. Zejména se může jednat o blokování, provedení opravy, doplnění nebo likvidaci osobních údajů.

§ 21 odst. 1 z. č. 101/2000 Sb. o ochraně osobních údajů o změně některých zákonů, ve znění pozdějších předpisů

[153] Nejvyšší správní soud, 4 Ans 6/2006 – 162, Původní nebo upravené texty pro ASPI [Rozsudek] ASPI [databáze] ASPI stav k 15.3. 2012 [cit. 2012-03-21]

[154] Tamtéž

[155] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 75

zaveden pro účely kontroly plnění povinností zaměstnanců. Je však nutno stále dbát na ustanovení čl. 8 EÚLP upravující právo na soukromí.[156]

Pokud zaměstnanci dají souhlas ke zpracování svých osobních údajů zaměstnavatelem, respektive správcem osobních údajů, pak důvodně očekávají, že jejich údaje budou zpracovávány pouze pro stanovené účely a pouze správcem, jemuž souhlas udělili. Britská judikatura pro tuto problematiku uvádí případ Douglas v. Hello [2001][157], kde bylo deklarováno porušení důvěry subjektu osobních údajů.[158]

Michael Douglas a Catherine Zeta-Jones uzavřeli smlouvu s časopisem OK!, podle které časopis získal exkluzivní práva na publikaci snímků z jejich svatby. Nikdo jiný nebyl oprávněn na zmíněné svatbě pořizovat jakýkoliv záznam. Zaměstnanci svatební agentury podepsali smlouvu, kde se zavázali, že na svatbě nebudou pořizovat žádné záznamy. Hostům byly při vstupu zabavovány fotoaparáty, kamery a jiné přístroje pořizující záznam. Přesto jeden ze zaměstnanců magazínu Hello bez povolení k pořízení jakéhokoliv vizuálního obrazu pořídil ze svatby záznam, který později publikoval. Následně bylo vydavatelství Hello obviněno z porušení důvěry.[159]

Soud posuzoval kolizi mezi právem na svobodu projevu dle Human Right Act 1998 a čl. 8 EÚLP deklarující právo na respektování soukromého a rodinného života a dospěl k závěru, že dle britského práva v rámci svobody projevu lze užít takto získaného záznamu, přestože nebylo uděleno žádné předchozí povolení, ale jen v případě, že o tom informuje subjekt údajů. Zákon umožňuje i výjimku, kdy není třeba splnit uvedenou informační povinnost, ale pouze v případě, existují-li dostatečné důvody, proč by subjekt údajů neměl být informován. Takovým důvodem může být veřejný zájem.

[156] NOUWT, Sjaak. Reasonable Expectations of Privacy?: Eleven country reports on camera surveillance and workplace privacy (Information Technology and Law Series). The Hague: T.M.C. Asser Press, 2005. ISBN 9789067041980, str. 105-106

[157] 5RB, Douglas v Hello! Ltd **Case Reference** [2001] QB 967; [2001] 2 WLR 992; [2001] 2 All ER 289; [2001] EMLR 199; [2001] FSR 732 **Court** Court of Appeal, 25.března 2012, dostupné na http://www.bailii.org/ew/cases/EWCA/Civ/2000/353.html

[158] NOUWT, Sjaak. Reasonable Expectations of Privacy?: Eleven country reports on camera surveillance and workplace privacy (Information Technology and Law Series). The Hague: T.M.C. Asser Press, 2005. ISBN 9789067041980, str. 105-106

[159] 5RB, Douglas v Hello! Ltd **Case Reference** [2001] QB 967; [2001] 2 WLR 992; [2001] 2 All ER 289; [2001] EMLR 199; [2001] FSR 732 **Court** Court of Appeal, 25.března 2012, dostupné na http://www.bailii.org/ew/cases/EWCA/Civ/2000/353.html

V případu Douglas v. Hello [2001] soud rozhodl, že z důvodu velkého zájmu o záznamy ze svatebního obřadu a popularity aktérů, není možné striktně zamítnout ustanovení o svobodě projevu. [160]

Dá-li tedy zaměstnanec souhlas ke zpracování svých osobních údajů získaných prostřednictvím kamerového systému na pracovišti, o kterém je dostatečně informován, měl by mít právo očekávat, že jeho údaje budou použity jen ke stanoveným účelům správce, tedy ke kontrole jeho pracovní činnosti. Vyvstane-li však veřejný zájem, například stane-li se vnitřní dění v některé společnosti mediálně žádané, pak se může stát, že osobní údaje subjektů budou zpracovány dalším správcem. To v českém právním řádu není přípustné.

[160] 5RB, Douglas v Hello! Ltd **Case Reference** [2001] QB 967; [2001] 2 WLR 992; [2001] 2 All ER 289; [2001] EMLR 199; [2001] FSR 732 **Court** Court of Appeal, 25.března 2012, dostupné na http://www.bailii.org/ew/cases/EWCA/Civ/2000/353.html

6. Kamerové systémy ve zdravotnických zařízeních

Kamerové systémy ve zdravotnictví jsou instalovány tam, kde je vyžadován trvalý dohled nad pacienty pro účely jejich léčby, jako například na jednotkách intenzivní péče. I zde je však nutno posuzovat nezbytnost, oprávněnost a míru ingerence do soukromí osob. Je totiž nepochybné, že hospitalizace na nemocničním lůžku je záležitost na výsost soukromá.[161]

„Každý má právo na ochranu zdraví. Občané mají na základě veřejného pojištění právo na bezplatnou zdravotní péči a na zdravotní pomůcky za podmínek, které stanoví zákon.“[162]

Na základě této ústavní úpravy zákonodárce stanovil, v zákoně č. 48/1997 Sb., o veřejném zdravotním pojištění a o změně a doplnění některých souvisejících zákonů, ve znění pozdějších předpisů, podmínky, za kterých je poskytována bezplatná zdravotní péče, a na co všechno má pacient v jejím rámci nárok. I zde jsou uvedeny prostředky zdravotnické techniky, mezi které patří i monitorovací a kamerové systémy.[163]

Ve vyhlášce Ministerstva zdravotnictví č. 221/2010 Sb. jsou uvedeny požadavky na věcné a technické vybavení jednotlivých typů zdravotnických zařízení. Pro některá oddělení vyhláška jasně stanoví povinnost sledovat pacienty a ukládá zřízení místnosti pro sledování pacientů.

„Požadavky na věcné a technické vybavení zdravotnických zařízení jednodenní péče na lůžku

1. *základní provozní prostory zdravotnického zařízení jsou:*
   e) místnost pro sledování pacientů po zákroku“[164]

Je tedy evidentní, že některá oddělení ze své podstaty vyžadují vizuální kontrolu pacientů, a to v operativním dosahu pracoviště sester. Vyhláška však nestanoví, zda musí být vizuální kontrola přímá, tedy očním kontaktem. Pak lze požadavek vizuální kontroly splnit i prostřednictvím instalace kamerového systému, jehož obrazovky budou

[161] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 50
[162] Čl. 31 Listiny základních práv a svobod
[163] KLÍMA, Karel. Ústavní právo. 3. rozšířené vydání. Plzeň: Aleš Čeněk, s.r.o., 2006. ISBN 80-7380-000-4, str. 365
[164] Vyhláška Ministerstva zdravotnictví č. 221/2010 Sb. Příloha č. 3, str. 2598

umístěny právě na zmíněném pracovišti sester. I tento způsob plnění zákonného požadavku na provádění vizuálního dohledu nad pacienty však musí být realizován v určitých mezích, aby byla zachována jistá míra soukromí pacientů.[165]

Při řešení užívání kamerového systému ve zdravotnických zařízeních se setkáme s kolizí dvou základních práv garantovaných Listinou, a to práva na soukromí obsažené v čl. 10[166] a práva na ochranu zdraví včleněné do čl. 31Listiny.[167] Ústavní soud deklaroval[168], že aby mohla být dána přednost základního práva či svobody před ochranou soukromí, musí se jejich vzájemný stav nejprve důkladně posoudit. [169] Nutnou podmínku pro řešení střetu dvou základních práv ustanovuje čl. 4 odst. 4 Listiny[170], a to omezení jednoho z práv, aniž by bylo zneužito jeho účelu, a zároveň minimalizovat zásah jednoho práva či svobody do druhého. Ústavní soud pro posuzování možnosti omezení základního práva stanovil podmínky, při jejichž splnění má jedno ze základních práv či svobod přednost[171]:

„První podmínkou je jejich vzájemné poměřování, druhou je požadavek šetření podstaty a smyslu omezovaného základního práva resp. svobody (čl. 4 odst. 4 Listiny základních práv a svobod).

Vzájemné poměřování ve vzájemné kolizi stojících základních práv a svobod spočívá v následujících kritériích:

---

[165] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 51

[166] zákon č. 2/1993 Sb., Listina základních práv a svobod, čl. 10
(1) Každý má právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno.
(2) Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.
(3) Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.

[167] zákon č. 2/1993 Sb., Listina základních práv a svobod, čl. 31
Každý má právo na ochranu zdraví. Občané mají na základě veřejného pojištění právo na bezplatnou zdravotní péči a na zdravotní pomůcky za podmínek, které stanoví zákon.

[168] Pl. ÚS 4/94

[169] „K omezení základních práv či svobod, i když jejich ústavní úprava omezení nepředpokládá, může dojít v případě jejich kolize. V těchto situacích je nutné stanovit podmínky, za splnění kterých má prioritu jedno základní právo či svoboda, a za splnění kterých jiné. Základní je v této souvislosti maxima, podle které základní právo či svobodu lze omezit pouze v zájmu jiného základního práva či svobody.“ (Pl. ÚS 4/94)

[170] zákon č. 2/1993 Sb., Listina základních práv a svobod, čl. 4
(4) Při používání ustanovení o mezích základních práv a svobod musí být šetřeno jejich podstaty a smyslu. Taková omezení nesmějí být zneužívána k jiným účelům, než pro které byla stanovena.

[171] Ústavní soud (ÚS), Pl. ÚS 4/94 – Nález (ÚS) [Práva obviněného v trestním řízení (214/1994 Sb.)] ASPI [databáze] ASPI stav k 15.3.2012 [cit. 2012-03-15]

Prvním je kritérium vhodnosti, tj. odpověď na otázku, zdali institut, omezující určité základní právo, umožňuje dosáhnout sledovaný cíl (ochranu jiného základního práva)…

Druhým kritériem poměřování základních práv a svobod je kritérium potřebnosti, spočívající v porovnávání legislativního prostředku, omezujícího základní právo resp. svobodu, s jinými opatřeními, umožňujícími dosáhnout stejného cíle, avšak nedotýkajícího se základních práv a svobod…

Třetím kritériem je porovnání závažnosti obou v kolizi stojících základních práv…"[172]

Zásah do soukromí je tedy legitimní, je-li zájem chráněný jiným základním právem či svobodou natolik závažný, že před ochranou soukromí dostane určitou přednost. Z toho celého lze tedy dovodit, že kamerové systémy používané ve zdravotnictví jsou z důvodu naléhavého zájmu na co nejkvalitnější péči o pacienta legální. Nicméně o monitoringu by měl být pacient informován.[173]

6.1. Případová studie v českém právním řádu

„Vedení nemocnice rozhodlo instalovat kamerový systém, který byl tvořen 10 stacionárními kamerami umístěnými u všech vstupů do nemocnice, na chodbách, v čekárnách, na dvoře a heliportu. Záznam z kamerového systému byl uchováván po dobu 5 dnů a subjekty údajů byly o jeho použití informovány piktogramy a informačními tabulemi."[174]

Zdravotnická zařízení jako účel instalace a užívání kamerových systémů uvádějí bezpečnostní důvody, ochranu práv a svobod osob, ochranu majetku, odvrácení vandalismu a dále prevenci kriminality. Dalším důvodem je preventivní ochrana personálu před bezdomovci, kteří se do zdravotnických zařízení často uchylují a neoprávněně se zde zdržují. Dalším důvodem je ochrana před agresivními pacienty a

[172] Ústavní soud (ÚS), Pl. ÚS 4/94 – Nález (ÚS) [Práva obviněného v trestním řízení (214/1994 Sb.)] ASPI [databáze] ASPI stav k 15.3.2012 [cit. 2012-03-15]
[173] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 52
[174] Tamtéž, str. 96-97 – ilustrační případ č. 1

osobami pod vlivem alkoholu či návykových látek, a to především v nočních hodinách v prostorách ambulancí.[175]

Zde však vyvstává otázka, kdy je potřebné instalovat kamerové systémy se záznamem (půjde o zpracování osobních údajů, bude tedy třeba splnit zákonné podmínky pro ochranu soukromí sledovaných osob a subjektů osobních údajů) a kdy postačí pouhý online monitoring, tedy sledování kamer bez pořizování záznamu.

V případě, kdy *„se nemocnice rozhodla instalovat kamerový systém se záznamem, který obsahoval 30 kamer umístěných u vjezdů a výjezdů z areálu, vstupů do budov, na parkovištích a vstupů na oddělení. Takto pořizované záznamy byly uchovávány po dobu nejdéle 2 kalendářních dnů a systém byl registrován u Úřadu.“*[176] *a d*eklarovaným účelem pro instalaci těchto kamer byla tedy ochrana majetku, Úřad kamerový systém schválil, jelikož pro stanovený účel byly zvolené prostředky přiměřené. Pro kontrolu osob, které mohly spáchat trestný čin krádeže nebo se dopustit jakékoli formy vandalismu podle úřadu stačí sledování vchodů do objektu. Z takových záznamů je možno identifikovat danou osobu a později použít jako důkaz. Nicméně je k zamyšlení, jak je možné prokázat příčinnou souvislost mezi spáchaným činem a osobou natočenou na záznamu, pokud není nijak dovozeno, že daný subjekt opravdu spáchal předmětný delikt. Dojde-li ke krádeži nebo poškození majetku zdravotnického zařízení či přítomných osob, není tak možno příčinnou souvislost ani časově doložit. Nabízí se pak možnost důkazu pomocí svědectví některé z přítomných osob, pak ovšem pořizování záznamu kamerovým systémem pozbývá své důležitosti.

Nicméně dle názoru Úřadu, aplikovaného na uvedený případ, je instalace kamerových systémů u vchodů do budov zcela v souladu se zákonem, a to právě proto, že pořízený záznam je pouze v řádech několika sekund a nedosahuje takové kvality, aby mohl být ze strany pacientů považován za zpracování citlivých údajů dle § 9 zákona o ochraně osobních údajů.[177] Celková míra zásahu do soukromí subjektů údajů nijak zvlášť neporušuje jejich práva.[178]

---

[175] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 89

[176] Tamtéž, str. 98

[177] Citlivé údaje je možné zpracovávat, jen jestliže

a) subjekt údajů dal ke zpracování výslovný souhlas. 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. Existenci souhlasu subjektu údajů se zpracováním osobních údajů musí být správce

Vrátíme-li se k prvnímu případu, tedy instalaci kamerového systému jak u vstupů do zdravotnického zařízení, tak i na chodbách a v čekárnách, budeme nuceni řešit otázku soukromí pacientů. *„Listina základních práv a svobod ve svém čl. 7 upravuje obecný princip a taktéž princip duševní.“*[179] Fyzické osoby vstupující do zdravotnických zařízení s cílem léčby svých zdravotních problémů mnohdy bývají velice citlivé na informace, které při zdravotní prohlídce podávají. Často považují za choulostivou informaci už samotný fakt, že se k léčbě ve zdravotnickém zařízení uchýlili, a to zejména v případech onemocnění, vypovídajících o jejich chování v soukromém životě. Proto při úniku takové informace můžeme hovořit o porušování práva na ochranu soukromí. Instalace kamerových systémů na chodbách a v čekárnách, za účelem ochrany majetku před odcizením a poškozováním, zajištění bezpečnosti a ochrany zdraví osob, je shromažďováním osobních údajů o přítomných subjektech. Nadměrně zasahuje do soukromí jednotlivců a podle Úřadu překračuje limity dané § 10 zákona o ochraně osobních údajů. Dále není dán souhlas dalších subjektů údajů, tedy u pouhých návštěvníků zařízení.[180]

Celý problém s kamerovými systémy se záznamem na chodbách, v čekárnách a jiných místech velmi frekventovaně navštěvovaných lze snadno vyřešit monitorováním bez záznamu. Tímto způsobem lze i nadále kontrolovat dění v budově a zároveň nezpracovávat osobní údaje. Nutno podotknout, že v praxi dochází k situaci, kdy jsou prostory sledovány jak online zařízením, aby mohly být operativně řešeny případné incidenční situace, tak zároveň kamerovým systémem se záznamem, a to s odůvodněním, aby byly shromážděny důkazy pro případné šetření Policie ČR. Takové

---

schopen prokázat po celou dobu zpracování. Správce je povinen předem subjekt údajů poučit o jeho právech podle § 12 a 21,

b) je to nezbytné v zájmu zachování života nebo zdraví subjektu údajů nebo jiné osoby nebo odvrácení bezprostředního závažného nebezpečí hrozícího jejich majetku, pokud není možno jeho souhlas získat zejména z důvodů fyzické, duševní či právní nezpůsobilosti, v případě, že je nezvěstný nebo z jiných podobných důvodů. Správce musí ukončit zpracování údajů, jakmile pominou uvedené důvody, a údaje musí zlikvidovat, ledaže by subjekt údajů dal k dalšímu zpracování souhlas,

c) se jedná o zpracování při poskytování zdravotních služeb, ochrany veřejného zdraví, zdravotního pojištění a výkon státní správy v oblasti zdravotnictví podle zvláštního zákona15) nebo se jedná o posuzování zdravotního stavu v jiných případech stanovených zvláštním zákonem,15a)

§ 9 z. č. 101/2000 Sb. o ochraně osobních údajů o změně některých zákonů, ve znění pozdějších předpisů

[178] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 89

[179] KLÍMA, Karel. Ústavní právo. 3. rozšířené vydání. Plzeň: Aleš Čeněk, s.r.o., 2006. ISBN 80-7380-000-4, str. 282

[180] Česká stomatologická komora, Použití kamerového systému v čekárně zdravotnického zařízení, 21.března 2012, dostupné na http://www.dent.cz/detail-text.php?id_strana=27&id_text=182

řešení je však nepřiměřené stanovenému účelu a je bráno jako nadměrný zásah do soukromí jak pacientů, tak i zaměstnanců (viz kap. 5 kamerové systémy na pracovišti).

6.2. Komparace se situací ve Velké Británii

Ve Velké Británii je právo limitující kamerové systémy spojeno především s ochranou soukromí, ochranou lidské důstojnosti a porušováním lidské důvěry. Poslední zmíněná ochrana je myšlena v tom smyslu, že pokud subjekt někde dobrovolně poskytne své osobní údaje s důvěrou, že nebudou zneužity, má právo očekávat, že se tak nestane. Tento problém je příhodný porovnat právě s problematikou instalace kamerových systémů ve zdravotnických zařízeních, kde pacienti dobrovolně podávají své osobní údaje s důvěrou, že jich nebude nijak zneužito.

O případ porušení důvěry se jednalo v britském případu Campbell v. MGM [2004][181], kdy byla Naomi Campbell vyfotografována, jak vychází z protidrogové léčebny. Tato fotografie byla později publikována spolu s titulkem „Naomi: Jsem závislá na drogách.“, a to včetně zveřejnění počtu sezení, kterých se zúčastnila.[182]

I když se v uvedeném případě jedná o pořízení fotografie prostřednictvím fotoaparátu, principy tohoto případu jsou plně aplikovatelné i na porušení zákonných ustanovení pro kamerové systémy, a to z toho důvodu, že se v obou případech jedná o pořízení záznamu, možnou identifikaci subjektu osobních údajů a následné zpracování dat.

Paní Campbell se nechala zapsat na protidrogovou léčbu, kde při zápisu do programu musela uvést své osobní údaje. Podle DPA 1998 důvodně předpokládala, že s jejími osobními údaji nebude nijak protizákonně nakládáno a nebudou tedy zneužity. Když byla následně vyfotografována, jak vychází z léčebného zařízení, byla díky tomuto záznamu podle svých fyziologických znaků identifikována, stejně jako by tomu mohlo být při pořízení záznamu kamerovým systémem. Pořízením dodatečných informací o počtu sezení, kterých se zúčastnila, tedy potvrzením, že léčebnu navštívila opravdu ze zdravotních důvodů a nikoliv například s cílem podpořit místní pacienty svou přítomností a psychickou podporou, došlo ke zneužití osobních údajů. Soud deklaroval

[181] 5RB, Campbell v MGN Ltd (HL) **Case Reference** [2004] UKHL 22; [2004] 2 AC 457; [2004] 2 WLR 1232; [2004] EMLR 247 **Court** House of Lords, 24března 2012, dostupné na http://www.5rb.com/case/Campbell-v-MGN-Ltd-(HL)
[182] Tamtéž.

porušení ustanovení DPA 1998, porušení čl. 8 EÚLP, upravující právo na soukromí a rodinný život. Došlo však ke kolizi s čl. 10 EÚLP, upravujícím svobodu projevu. Právo na svobodu projevu zde porušovalo právo na ochranu cti a podporovalo únik důvěrných informací.[183]

Je tedy zjevné, že došlo ke zneužití vizuálního záznamu, stejně jako by tomu bylo, kdyby fotografie byla pořízena z kamerového systému. Podobné je to v českém právním řádu, kde je právní úprava pro užívání kamerových systémů koncipována tak, aby soukromí pacientů ve zdravotnických zařízeních bylo co nejvíce chráněno a důvěrné informace o jejich zdravotním stavu nebo o tom, že s jejím zdravotním stavem je v něco v nepořádku, nebyla nikomu neoprávněnému zveřejněna a tím nebyl porušen zákon na ochranu osobních údajů.

[183] 5RB, Campbell v MGN Ltd (HL) Case Reference [2004] UKHL 22; [2004] 2 AC 457; [2004] 2 WLR 1232; [2004] EMLR 247 Court House of Lords, 24března 2012, dostupné na http://www.5rb.com/case/Campbell-v-MGN-Ltd-(HL)

7. Kamerové systémy ve školských zařízení

Školským zařízením máme na mysli součást výchově vzdělávacího zařízení, poskytujícího školské služby a státem uznané vzdělávání a s tím související zájmové studium (školský ústav umělecké výroby, státní jazyková škola), školské zotavovací zařízení (škola v přírodě, středisko pro volný čas dětí a mládeže, školní družina, školní klub, školní knihovna, domov mládeže) a dále také zařízení ústavní a ochranné výchovy (diagnostický ústav, dětský domov, dětský domov se školou, výchovný ústav, středisko výchovné péče).[184]

Instalace kamerových systémů ve školských zařízeních je odůvodnitelná, stejně jako instalace na jiných místech, ochranou majetku místního zařízení a zajištěním bezpečností zaměstnanců a studentů. Dle § 29 odst. 2 z. č. 561/2004 Sb. o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon), ve znění pozdějších předpisů (dále jen školský zákon) [185] lze kamerový systém zahrnout do výkonu povinností školy jako možný prostředek k plnění povinností stanovených zákonem a k zajištění bezpečnosti a ochrany zdraví dětí, žáků a studentů. § 30 odst. 1 školského zákona.[186] dále stanoví, že ředitel školy vydává školní řád, kde je upraven provoz a vnitřní režim školy, práva a povinnosti studentů a jejich zákonných zástupců a pracovníků školy a stanoveny podmínky zajištění bezpečnosti a ochrany zdraví dětí, žáků a studentů, stejně tak jako zacházení s majetkem školy a školským zařízením. Nezbytným ustanovením pro účely zákona o ochraně osobních údajů a pro možnost

[184] *Právnický slovník*. 2. rozšířené vydání. Praha: C. H. Beck, 2001. ISBN 80-7179-740-5, str. 1021-1022

[185] (2) Školy a školská zařízení zajišťují bezpečnost a ochranu zdraví dětí, žáků a studentů při vzdělávání a s ním přímo souvisejících činnostech a při poskytování školských služeb a poskytují žákům a studentům nezbytné informace k zajištění bezpečnosti a ochrany zdraví. Ministerstvo stanoví vyhláškou opatření k zajištění bezpečnosti a ochrany zdraví dětí, žáků a studentů při vzdělávání ve školách a školských zařízeních a při činnostech s ním souvisejících.
§ 29 odst. 2 z. č. 561/2004 o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon), ve znění pozdějších předpisů

[186] Školní řád, vnitřní řád a stipendijní řád
(1) Ředitel školy vydá školní řád; ředitel školského zařízení vnitřní řád. Školní řád a vnitřní řád upravuje
a) podrobnosti k výkonu práv a povinností dětí, žáků, studentů a jejich zákonných zástupců ve škole nebo školském zařízení a podrobnosti o pravidlech vzájemných vztahů s pedagogickými pracovníky,
b) provoz a vnitřní režim školy nebo školského zařízení,
c) podmínky zajištění bezpečnosti a ochrany zdraví dětí, žáků nebo studentů a jejich ochrany před sociálně patologickými jevy a před projevy diskriminace, nepřátelství nebo násilí,
d) podmínky zacházení s majetkem školy nebo školského zařízení ze strany dětí, žáků a studentů.
§ 30 odst. 1 z. č. 561/2004 o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon), ve znění pozdějších předpisů

instalace kamerového systému je § 30 odst. 3 školského zákona[187], ukládající povinnost seznámit studenty a zaměstnance se školním řádem a případně s provozem kamerového systému.[188] U kamerových systémů ve školských zařízeních je také nezbytné přihlédnout k faktu, že neexistuje zvláštní právní úprava pro provozování kamerových systémů. Je tedy nutné dodržovat ustanovení zákona o ochraně osobních údajů a zároveň není (při splnění zákonných povinností) dle vyjádření Úřadu důvod, proč by školské zařízení nemohlo instalaci kamerového systému pro své potřeby užít.[189]

7.1. Případová studie v českém právním řádu

Škola provozovala ve své budově kamerový systém se záznamovým zařízením snímající chodby školy s tím, že se v přízemí budovy nacházel i soukromí byt. Důvodem rozhodnutí ředitele školy pro instalaci kamerového zařízení byly negativní zkušenosti s dřívějšími drobnými krádežemi, které však ale ani nebyly ohlášeny policejním orgánům. Na základě podnětu byla zahájena kontrola dodržování povinností stanovených zákonem na ochranu osobních údajů, a to příslušným Úřadem pro ochranu osobních údajů, který ve svém rozhodnutí došel k závěru, že bylo porušeno hned několika podmínek stanovených zákonem.[190]

Jako účel provozování kamerového systému byla uvedena ochrana života a zdraví studentů a pedagogů, ochrana majetku a prevence drobné kriminality, tedy ochrana před krádežemi a zamezení zneužívání prostor školy učiteli k soukromým účelům. Podle ředitele školy měl stanovený účel pouze preventivní charakter. Dle rozhodnutí Úřadu a posléze i Městského soudu v Praze je takovéto sledování nepřiměřeným zásahem do soukromí sledovaných osob. Pro účely zajištění majetku školy bylo dostatečné užít kamerových systémů v době, kdy se v budově školy nenachází žádná osoba, čímž by byl naplněn účel potřeby dohledu a zároveň by nedocházelo ke zpracování osobních

[187] (3) Školní řád nebo vnitřní řád zveřejní ředitel na přístupném místě ve škole nebo školském zařízení, prokazatelným způsobem s ním seznámí zaměstnance, žáky a studenty školy nebo školského zařízení a informuje o jeho vydání a obsahu zákonné zástupce nezletilých dětí a žáků.
§ 30 odst. 3 z. č. 561/2004 Sb. o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon), ve znění pozdějších předpisů
[188] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 112-114
[189] Vyjádření a doporučení ÚOOU k možnosti instalovat kamerový systém v prostorách školy, 23.března 2012, dostupné na http://www.uoou.cz/files/vyjadreni_a_doporuceni_uoou.pdf
[190] Rozsudek Městského soudu v Praze, sp. zn. 11 Ca 298/2008 – 47, 23.března 2012, dostupné na http://www.uoou.cz/files/judik_rozsudek_ms_-_hotel.pdf

údajů. Přes den je majetek školy naopak sledován a kontrolován místními zaměstnanci a pedagogy, kteří se po budově školy neustále pohybují. Co se týká ochrany života a zdraví studentů, na ty v rámci své pracovní náplně dohlížejí přítomní pedagogové, což je alternativní a dostačující prostředek dohledu ve školském zařízení. Možnost užití kamerového systému pro stanovený účel by bylo příhodné pro kontrolu před zneužíváním prostor školy k soukromým účelům. V takovém případě by měl být kamerový systém zapnut v době, kdy se v budově nepohybují žádné osoby, a nešlo by tedy o zpracovávání osobních údajů a případný záznam o zneužití prostor školy by byl brán jako důkaz o neoprávněného vniknutí[191]. Provozovatel však namítl, že zákon ani předpisy komunitárního práva neupravují konkrétně použití kamerových systémů. Soud při posuzování případu vyloučil možnou výjimku podle § 5 odst. 2 písm. e) zákona o ochraně osobních údajů a nezbytnost zpracování osobních údajů pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby. Nesmíme totiž zapomenout na ústavně zaručené právo na ochranu soukromí, nedotknutelnost osoby dle čl. 7 Listiny, ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním informací o své osobě dle čl. 10 odst. 3 Listiny. Na straně druhé Listina ve svém čl. 11 odst. 1 deklaruje právo vlastnit majetek a právo jej chránit. Dochází tedy ke střetu dvou zájmů, které řeší již zmíněný nález Ústavního soudu ČR, č.j. IV. ÚS 154/97. Soud označil v tomto případě vyzdvižení práva na ochranu majetku za bezdůvodné, nepřípustné a především: *„…neproporcionální ve vztahu ke konkrétnímu veřejnému zájmu, který má žalobce údajně prosazovat a nemůže tak jít o legitimní omezení.“*[192]

Dále provozovatel kamerového systému s odvoláním na § 5 odst. 1 písm. e) zákona o ochraně osobních údajů namítal, že žádný zákon a ani předpis komunitárního práva neupravuje délku uchování záznamu. Proto si stanovil vlastní lhůtu pro zpracování osobních údajů, a to 14 dní, jež mu přijde adekvátní. To ale Úřad označil za naprosto nepřiměřené stanovenému cíli, a sice proto, že získané záznamy je nedůvodné uchovávat dobu delší než tři dny, během kterých lze případný vandalismus, drobné krádeže či nepřípustné chování v budově školy odhalit a použít jako důkaz.[193]

„… ke zpracování záznamů pořízených kamerami dojde pouze v případě oznámení krádeže, kdy bude příslušný záznam předán Policii České republiky. Záznamy bývají

[191] § 208 z. č. 40/2009 trestní zákoník, ve znění pozdějších předpisů
[192] Rozsudek Městského soudu v Praze, sp. zn. 11 Ca 298/2008 – 47, 23.března 2012, dostupné na http://www.uoou.cz/files/judik_rozsudek_ms_-_hotel.pdf
[193] Tamtéž.

uchovávány po dobu od 24hodin po dobu 3 dnů, jen v době prázdnin a víkendů se předpokládá doba delší.“[194]

Nedostatkem dle Úřadu bylo plnění informační povinnosti, kterou provozovatel řešil prostřednictvím informačních tabulek, na nichž bylo napsáno: „Prostor této chodby je monitorován kamerovým systémem.“ Jak soud později poznamenal, touto tabulkou nebylo subjektům údajů sděleno v jakém rozsahu, pro jaký účel, kdo a jakým způsobem je bude zpracovávat a komu mohou být osobní údaje zpřístupněny. Provozovatel se hájil argumentem, že o instalovaném kamerovém systému byli informováni zaměstnanci školského zařízení a ti měli dále informovat své žáky a jejich zákonné zástupce. V této argumentaci je však očividná mezera v aplikaci na třetí osoby, které vstoupí do budovy školy a také především na obyvatele bytu, nacházející se v přízemí. Ti nejenže nebyli informováni o provozu sledovacího zařízení, ale především neudělili souhlas ke zpracování svých osobních údajů.[195]

Souhlas subjektů osobních údajů byl dalším konstatovaným nedostatkem. Souhlas od zaměstnanců byl doložen na základě písemných prohlášení zaměstnanců školy. Souhlas od obyvatel zmíněného bytu získán nebyl. Otázkou zůstává souhlas místních studentů.

Směrnice číslo 95/46/ES uvádí:

„(12) vzhledem k tomu, že zásady ochrany se musí vztahovat na veškerá zpracování osobních údajů kteroukoli osobou,“[196]

Neexistuje žádné zvláštní ustanovení, upravující podávání souhlasu nezletilými, ale dle směrnice je zjevné, že i nezletilí jsou subjekty údajů, na něž se stanovené povinnosti správce vztahují. Diskutabilní je zákonný požadavek zastoupení nezletilého zákonným zástupcem, rozsah možnosti zastoupení nezletilého zákonným zástupcem a různá úroveň vyspělosti subjektů.

[194] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 102
[195] Rozsudek Městského soudu v Praze, sp. zn. 11 Ca 298/2008 – 47, 23.března 2012, dostupné na http://www.uoou.cz/files/judik_rozsudek_ms_-_hotel.pdf
[196] Evropský Parlament a Rada, Směrnice č. 95/46/ES [o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů] ASPI [databáze] ASPI stav k 15.3.2012 [cit. 2012-03-23]

Se školním řádem se, dle vlastních zkušeností, studenti seznamují na začátku školního roku, kdy jim jsou jednotlivé body přečteny, potažmo tedy i informace o existenci kamerového systému, seznámení studentů je podepsáno jako souhlas s jeho jednotlivými body a jako závazek k jeho plnění. Zároveň však v praxi není dána možnost školní řád nepodepsat. Otázkou je, od kterého ročníku je student oprávněn za sebe takto rozhodovat (když plnou právní subjektivitu získává až dosažením plnoletosti) a do kterého věku by za studenta měl podpis poskytnout jeho zákonný zástupce například na třídních schůzkách. Podrobnější úpravu neupřesňuje ani unijní právo, které stanoví:

„(17) pro účely této směrnice by měl mít souhlas uživatele nebo účastníka, bez ohledu na to, zda účastník je fyzická či právnická osoba, stejný význam jako souhlas subjektu údajů definovaný a dále upřesněný ve směrnici 95/46/ES. Souhlas může být udělen jakýmkoli vhodným způsobem, který umožňuje vyjádřit svobodně poskytnutý, zvláštní a informovaný projev vůle uživatele, včetně označení zaškrtnutím políčka při návštěvě webové stránky na internetu;“[197]

Další skutečností, v rozporu se zákonnými podmínkami, byla opožděná registrace kamerového systému u Úřadu, respektive správce podal žádost na registraci až následně po spuštění kamerového systému.[198]

Soud tedy rozhodl, že žaloba podaná školským zařízením proti rozhodnutí Úřadu se zamítá, a to z důvodu porušení zákonných podmínek podle zákona o ochraně osobních údajů[199], a uznal finanční sankci uloženou Úřadem v souladu s § 45 odst. 4 zákona o ochraně osobních údajů.

[197] Evropský Parlament a Rada, Směrnice č. 2002/58/ES [o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích] ASPI [databáze] ASPI stav k 15.3.2012 [cit. 2012-03-23]

[198] Rozsudek Městského soudu v Praze, sp. zn. 11 Ca 298/2008 – 47, 23.března 2012, dostupné na http://www.uoou.cz/files/judik_rozsudek_ms_-_hotel.pdf

[199] Soud shledal porušení § 5 odst. 1 písm. d). e), odst. 2; § 11 odst. 1; §16; § 45 odst. 1 písm. c), d), e), f), i) zákona č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů

7.2. Komparace se situací ve Velké Británii

K užívání kamerových systémů ve školách ve Spojeném království se vyjádřila Unie pro pedagogické pracovníky ve Velké Británii (ATL). Ta uznává, že užívání kamerových systémů ve školách se stalo nedílnou součástí ústavů. Zdůrazňuje, že instalace a následné užívaní kamerových systémů musí šetřit práva subjektů osobních údajů a být provozovány striktně s cílem naplnění předem stanoveného účelu. [200]

Dle ATL by bylo nepravdivé říci, že kamerové systémy ve školách nemají žádné opodstatnění. Ve Velké Británii posilují dozor nad žáky, kontrolují jejich chování, stejně jako chování pedagogů daného zařízení a v neposlední řadě dohlíží na majetek školy. Jsou však stále zóny s vysokou mírou soukromí jako toalety a šatny, kde kamerové systémy nemají co dělat. [201]

ATL se ohrazuje především proti přehrávání nashromážděných snímků jiným orgánům nebo rodičům, a to především těch záznamů, které jsou pořízeny v učebnách nebo jiných prostorech určených k vyučování. V těchto prostorech je očekávána velká míra soukromí, a když musí být záznam z těchto míst pořizován, mělo by se nakládat se získanými údaji velmi opatrně. [202]

Nabízí se aplikace již zmíněného případu Douglas v. Hello [2001] (viz. podkapitola 4.2.), který uvádí, že pro veřejný zájem a vysokou publicitu lze dát přednost právu na informace před právem na soukromí a vloženou důvěru správci osobních údajů. Zamyslíme-li se nad možností, že má rodič důvodné podezření, že je jeho dítě šikanováno nebo snad fyzicky napadáno, ať už spolužáky nebo pedagogem, pak v takovém případě by byl dán dostatečný důvod, aby byly záznamy rodičům poskytnuty, a to už jen z důvodu, že rodič je zákonným zástupcem nezletilé osoby. Ze stejného důvodu by pak měl mít zájem shlédnout záznam i jiný orgán, příslušný k řešení takové problematiky.

Je však otázkou, zda by bylo vhodné takovou situaci medializovat. Nezletilá osoba se nachází v procesu duševního vývoje a jakýkoliv nepřiměřený zásah do její psychiky by

[200] ATL, Use of CCTV surveillance in schools, 25.března 2012, dostupné na http://www.atl.org.uk/policy-and-campaigns/policies/CCTV-policy.asp

[201] Tamtéž.

[202] ATL, Use of CCTV surveillance in schools, 25.března 2012, dostupné na http://www.atl.org.uk/policy-and-campaigns/policies/CCTV-policy.asp

ji mohl negativně ovlivnit. Z tohoto důvodu ATL klade důraz na správu údajů a především na ochranu před únikem nashromážděných informací. ATL podporuje zásadu, že by každé školské zařízení mělo pověřit speciálního pracovníka, zodpovědného za správu získaných údajů, který bude každoročně vydávat písemnou zprávu o nashromážděných údajích a o užívání kamerového systému. [203]

[203] ATL, Use of CCTV surveillance in schools, 25.března 2012, dostupné na http://www.atl.org.uk/policy-and-campaigns/policies/CCTV-policy.asp

8. Kamerové systémy instalované pro soukromé účely

Kamerový monitoring instalovaný pro soukromé účely je systém, který instalují soukromé subjekty u vchodů svých domů, na schránky, ve výtahových kabinkách obytných domů, do dvorů, průjezdů či sklepů. V tomto případě je velmi podstatné dbát ustanovení zákona, jelikož v obytných domech vlastníci či nájemníci, respektive obyvatelé očekávají vysokou míru soukromí.

Při instalaci kamerového systému na rodinném domu je nutno dbát úpravy § 127 odst. 1 občanského zákoníku, obsahující tzv. generální klauzuli sousedského práva. Jedná se o práva a povinnosti jednotlivých vlastníků pozemků nebo staveb, kteří se výkonem svých práv mohou navzájem ovlivňovat. Ustanovení občanského zákoníku ukládá každému vlastníku pozemku:

„…vlastník věci se musí zdržet všeho, čím by nad míru přiměřenou poměrům obtěžoval jiného (má se na mysli vlastníka)nebo čím by vážně ohrožoval výkon jeho práv.“[204]

Jinak řečeno práva jednoho končí tam, kde začínají práva druhého.

V rámci problematiky kamerových systémů je vhodné zmínit pojem „obtěžování pohledem“, který řešil ve svém rozhodnutí Nejvyšší soud[205]. Je-li některá z kamer instalována tak, že zabírá byť jen část sousedního domu nebo pozemku, lze hovořit o imateriální imisi[206] nazvané „obtěžování pohledem“. Zde Nejvyšší soud uvádí, že obtěžování pohledem lze za imisi považovat pouze výjimečně a to až po důkladném posouzení věci s přihlédnutím k oprávněným zájmům obou stran. Imisí je míněno až tehdy, je- li závažným způsobem porušováno soukromí vlastníka sousední nemovitosti.[207]

Dle jiného judikátu Nejvyššího soudu:

„Těm, kdo mají faktickou možnost nahlížet do cizích oken nelze zpravidla uložit, aby provedli taková opatření, kterými by tuto možnost vyloučili. Proto je na tom,, kdo se cítí

[204] FIALa, Josef a kol. Komentář k §127 odst. 1 zák. č. 40/1964 Sb. [omezení vlastnického práva-sousedské právo] ASPI [databáze] ASPI stav k 15.3. 2012 [cit. 2012-03-24]
[205] Nejvyšší soud (NS) ČR, 22 Cdo 1150/99 – Rozhodnutí (RC) [Sousedská práva a obtěžování pohledem jako imise] ASPI [databáze] ASPI stav k 15.3. 2012 [cit. 2012-03-24]
[206] Imise jsou neoprávněné zásahy do práv sousedního vlastníka pozemku. Imateriální rušivou imisí je například vytváření nadměrného hluku. FIALa, Josef a kol. Komentář k §127 odst. 1 zák. č. 40/1964 Sb. [omezení vlastnického práva-sousedské právo] ASPI [databáze] ASPI stav k 15.3. 2012 [cit. 2012-03-24]
[207] Nejvyšší soud (NS) ČR, 22 Cdo 1150/99 – Rozhodnutí (RC) [Sousedská práva a obtěžování pohledem jako imise] ASPI [databáze] ASPI stav k 15.3. 2012 [cit. 2012-03-24]

být obtěžován pohledem, aby provedl opatření, která by tomuto obtěžování zabránila. Obtěžování pohledem je imisí proti které právo poskytuje ochranu jen v případě, jde-li o mimořádnou situaci a zvlášť závažné a soustavné narušování soukromí vlastníka nebo uživatele sousední nemovitosti.“[208]

Při užívání kamerového systému v obytných domech, tedy domech o více bytech, přístupných ze společného prostoru, společným hlavním vstupem, vlastníci bytových domů obvykle trvají na skutečnosti, že ohledně možnosti instalace kamerových systémů se na ně vztahuje ustanovení § 5 odst. 2 písm. a) a e) zákona o ochraně osobních údajů, tedy ustanovení o zpracování osobních údajů, nezbytné pro plnění povinnosti správce. Dále i možnost zpracování osobních údajů z důvodu nezbytnosti pro ochranu práv a právem chráněných zájmů správce.[209]

Nařízení vlády č. 371/2004 Sb., kterým se vydávají vzorové stanovy společenství vlastníků jednotek, je správa bytového domu vymezena jako činnost, zahrnující údržbu společných částí domu, opravy částí domu, administrativní operace, stejně jako správa svěřeného majetku s péčí řádného hospodáře.[210]

Správci bytového domu pak často pro své účely instalují kamerové systémy s detekcí pohybu. Tyto systémy v obytných domech lze často připojit do místního rozvodu TV, takže každý obyvatel daného domu může pozorovat dění zaznamenávané kamerovým systémem.[211] Je tedy otázkou, do jaké míry je ještě akceptovatelné užívání kamerových systémů v obytných domech, kde obyvatelé důvodně očekávají nejvyšší míru soukromí. Kde jinde, než na místě, kterému říkají domov, by měli soukromí očekávat. Bude tedy záležet na místě, kde je kamera umístěna respektive jaké prostory snímá.

Podle názoru ESLP by bylo příliš restriktivní považovat za prostory, kde by měla fyzická osoba právo na soukromí, pouze místa, kde může žít svůj soukromí život, myšleno prostory bytu. Nebylo by legitimní uznat názor, že v prostorech vně bytu se již nejedná o soukromí. I tam se o soukromí jedná, ač míra toho soukromí je nižší. Proto se v praxi rozdělují místa obytného domu na dvě skupiny:

[208] Nejvyšší soud (NS) ČR, sp. zn. 22 Cdo 1629/99 – Rozhodnutí [Omezení práv vlastníka (sousedská práva) a nahlížení do oken] ASPI [databáze] ASPI stav k 15.3. 2012 [cit. 2012-03-24]
[209] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 79
[210] Vláda České republiky, Nařízení č. 371/2004 Sb. [Nařízení vlády České republiky, kterým se vydávají vzorové stanovy společenství vlastníků jednotek] ASPI [databáze] ASPI stav k 15.3. 2012 [cit. 2012-3-24]
[211] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 79

- První skupina zahrnuje prostory, neurčené k soukromému životu, jako půda, sklep, jejich vchody, kočárkárna, kolárna, místo pro dopisní schránky, a proto se zde neočekává zásah do soukromí. Na těchto místech by bylo možné aplikovat výjimku dle § 5 odst. 2 písm. e) zákona o ochraně osobních údajů, tedy možnost zpracování osobních údajů bez souhlasu subjektů a to z důvodu ochrany práv a právem chráněných zájmů správce. Pouze však v případě, že takové zpracování osobních údajů nebude v rozporu s právem na ochranu soukromí a soukromého života.
- Druhou skupinou jsou chodby, výtahy, schodiště, vchodové dveře do budovy, vchodové dveře do bytů, kde je očekávaná vysoká míra soukromí a jsou úzce spjaty se soukromím životem lidí obývajících obytný dům. Instalace kamerového systému vyžaduje souhlas subjektů údajů a to všech obyvatel domu. Vlastníci bytových domů však z praxe argumentují, že získání trvalého souhlasu je téměř nemožné například z důvodu časté výměny nájemníků nebo dlouhodobé nepřítomnosti některých vlastníků. [212]

8.1. Případová studie v českém právním řádu

Majitel bytového domu nainstaloval čtyři kamery, z nichž tři snímaly společné prostory a jedna z nich snímala vstup do společného bytového prostoru. Kamerami tedy byla zaznamenána každá osoba, která vstoupila do bytového domu, nebo jej opustila. Majitel bytového domu nainstaloval kamerový systém především z toho důvodu, že v minulosti docházelo k častému vloupání do objektu, útokům na majetek, a osobním útokům na členy družstva a správce. Žádný z těchto útoků však nebyl policií došetřen, trestní stíhání nebylo zahájeno z důvodu neprokazatelnosti těchto útoků. [213]

Úřad pro ochranu osobních údajů zavedení uvedeného kamerového systému v obytném domě ve svém rozhodnutí označil za protizákonné. Jako důvod uvedl, že nelze dát v tomto případě přednost právu vlastnit majetek a právu na jeho ochranu, byť je to ústavně zaručené právo podle čl. 11 Listiny, před právem na ochranu

[212] JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505, str. 81-84
[213] Rozsudek Městského soudu v Praze, sp. zn. 7 Ca 204/2005 – 49, 25.března 2012, dostupné na http://www.uoou.cz/files/judik_07.pdf

soukromí, dle čl. 8 EÚLP a ve smyslu čl. 7 Listiny. Dle nálezu Ústavního soudu (sp. zn. Pl. ÚS 4/94) se musí po důkladném šetření jednotlivých práv dát přednost tomu, které v daném případě požívá větší důležitosti.

Úřad také namítal, že správce nezískal od všech nájemníků souhlas ke zpracování jejich osobních údajů. Argument majitele nemovitosti, že v jeho případě se na něj vztahuje výjimka dle § 5 odst. 2 písm. e) zákona o ochraně osobních údajů a osobní údaje pořízené jím instalovaným kamerovým systém nejsou osobními údaji ve smyslu § 4 písm. a) zákona o ochraně osobních údajů[214]. Dle správce identifikace z pořízených záznamů není možná. V tomto případě, i kdyby úřad přijal argument, že samotný vizuální záznam není pro identifikaci dostačující, ač pro fyziologické znaky dostačující je, nelze opomenout, že majitel domu nechal nainstalovat i speciální dveře, které byly otvírané na čip. Každý čip obsahuje unikátní kód, se kterým lze ztotožnit osobu, která tento čip užívá a tedy která dveře otevřela. Následně tato osoba byla zaznamenána nahrávacím zařízením. Není pochyb o tom, že jde o zpracování osobních údajů a pořizování osobních údajů ve znění ustanovení § 4 písm. a) zákona o ochraně osobních údajů.[215]

Soud následně uvedl, že: *„ pokud by monitorování prostor domu mělo sloužit především ochraně majetku, pak by museli všichni uživatelé bytů (bez ohledu, zda jsou nájemci, či členové družstva) s takovým monitorováním souhlasit, neboť tím jsou zachycovány a zpracovávány jejich osobní údaje.“*[216] Kamerový systém v bytovém domě označil za nezákonný.

8.2. Komparace se situací ve Velké Británii

[214] a) osobním údajem jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu, §4 písm. a) z. č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů

[215] Rozsudek Městského soudu v Praze, sp. zn. 7 Ca 204/2005 – 49, 25.března 2012, dostupné na http://www.uoou.cz/files/judik_07.pdf

[216] Tamtéž.

V roce 2009 se v britských médiích objevila informace o instalaci kamerových systémů přímo v soukromých domech a bytech.[217] Tato sledovací zařízení neměla sledovat vstupní prostory, či prostory společné všem obyvatelům domu, jako jsou chodby, sklepy či výtahy. Tyto systémy ale byly určeny pro monitorování soukromého života obyvatel určených bytů. Tedy jasně narušují čl. 8 EÚLP o právu na ochranu soukromí. Jejich účel byl jasně vymezen jako kontrola výchovy dětí sociálně slabých či asociálních rodin.[218]

Tento nápad vyšel z kanceláře ministra pro dětská práva Eda Ballse, který jako důvod monitorování takových rodin odůvodňuje tím, že děti vyrůstající ve stabilnějších rodinách se v budoucnu méně uchylují k drogám a kriminální činnost. V tomto duchu byl projekt pojmenován „Sin bins for worst families“, v překladu kontejner hříchu pro nejhorší rodiny. Funkcí instalovaných kamerových systémů má být doslova sledování, zda si děti píší své úkoly, zda jim rodiče servírují zdravé jídlo, zda chodí včas spát. Dalo by se tedy spíše konstatovat, že kamery mají sledovat řádnou péči rodičů o své děti. Podle tohoto programu každý rok budou děti a jejich rodiče sepisovat „smlouvu o chování, ve které bude stanoveno, které povinnosti se musí plnit.[219]

Již v roce 2009 bylo nainstalováno 2000 takových kamer, shromažďujících osobní údaje o soukromí rodin označených jako asociální. Kamery zaznamenávají osobní údaje 24 hodin denně. Pro stejné účely byl zřízen i speciální policejní orgán, který náhodnými prohlídkami kontroluje vytipované rodiny. [220]

Takovýto zásah do ústavně zaručeného práva na soukromí dle ať už dle čl. 8 EÚLP nebo DPA 1998 porušuje všechna možná ustanovení o soukromí subjektů osobních údajích a to jak rodičů, tak dětí. Je sice stanoveno, že účelem kamerového sledování je dohlížet na rodičovskou výchovu avšak v bytech probíhají i jiné činnosti, které jsou kamerami sledovány. Například bude natočena jakákoliv návštěva. Taková osoba už ale

[217] EXPRESS.co.uk, SIN BINS FOR WORST FAMILIES, 25.března, dostupné na http://www.express.co.uk/posts/view/115736/Sin-bins-for-worst-families
[218] Zvědavec, V Británii chtějí umístit CCTV kamery do soukromých domů a bytů, 25.března 2012, dostupné na http://www.zvedavec.org/komentare/2009/08/3251-v-britanii-chteji-umistit-cctv-kamery-do-soukromych-domu-a-bytu.htm
[219] Tamtéž.
[220] EXPRESS.co.uk, SIN BINS FOR WORST FAMILIES, 25.března, dostupné na http://www.express.co.uk/posts/view/115736/Sin-bins-for-worst-families

s programem monitorování asociálních rodin nemá nic společného a nemá tedy důvod zásah do svého práva na soukromí strpět.

Na povážlivou je také otázka, proč, když má vláda důvodné podezření, že rodiče zanedbávají svou péči, neodebere dítě z jejich výchovy a neumístí do jiné pro něj nejvhodnější náhradní péče, tak jak to v českém právní řádu řeší z. č. 94/1963 Sb. o rodině ve znění pozdějších předpisů.

9. Závěr

Právní úprava používání kamerových systému je značně nedostatečná. Základním právním předpisem upravující problematiku instalace a užívání kamerových systémů je zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

Ten však neupravuje v žádné své části výlučně kamerové systémy. Zákon upravuje jednotlivé povinnosti správce osobních údajů a je tedy aplikovatelný pouze na kamerové systémy se záznamem.

Kamerovým systémům bez záznamu se tak dostává neomezené libovůle. Mohou být instalovány kdekoliv a kýmkoliv. Nemusí být nikde registrovány a nejsou ani žádnou autoritou kontrolovány. Dle mého názoru je velmi zarážející, že zákonodárce nepovažuje tento stav za nežádoucí. Je pravda, že podle dikce zákona o ochraně osobních údajů u kamerových systémů bez záznamu ke zpracování osobních údajů nedochází. Při jejich provozu je však zachycený obraz přenášen na centrální místo, kde je kontrolován pověřenou osobou, a ta tím pádem výkonem své práce, tedy sledováním projekce, zasahuje do soukromí monitorovaných osob.

Ohledně aplikace zákona o ochraně osobních údajů na kamerové systémy se záznamem vyvstává celá škála nejistot. Zákon je koncipován velmi obecně, aby byl aplikovatelný na všechny způsoby zpracovávání osobních údajů za použití jakýchkoli prostředků. Nemyslím si, že by se užívání různých druhů prostředků dalo paušalizovat.

S velmi obecnou a nedostačující právní úpravou pak souvisí i způsob řešení sporných situací. Ve správní organizaci České republiky vzniknul pro tuto problematiku Úřad pro ochranu osobních údajů. Zde se každý budoucí správce osobních údajů musí registrovat za současného splnění všech zákonných požadavků. Obecnost zákona je řešena Úřadem, který je pověřen prošetřením jednotlivých žádostí o registraci. Ve vyjádřeních samotného úřadu nalezneme, že Úřad prozkoumává u každého případu soulad se zákonem s přihlédnutím ke konkrétním okolnostem. Zde dochází k problému s obecnou právní úpravou. Není zřetelně jasné, zda jsou aplikovatelné výjimky či nikoliv. Není jasně určena doba pro zpracování osobních údajů. Není jasně stanoveno, v jakých prostorách je ještě vhodné narušovat soukromí a kde už takový zásah nepřichází

v úvahu. Na jedné straně tak dochází ke snaze obcházet zákon, na straně druhé je zde nedostatek právní jistoty.

Úřad pro ochranu osobních údajů tedy vystupuje jako registrátor a zároveň kontrolor. Úřad vydává správní rozhodnutí, v nichž uvádí nedostatky určitého kamerového systému a požadavky k nápravě. Dále ukládá finanční sankce. Sám o sobě však nedisponuje žádnou autoritou, kterou by byl oprávněn uložené požadavky a sankce vymáhat. Děje se tak prostřednictvím soudní žaloby. Proti rozhodnutí soudu je možno podat kasační stížnost. V případě, kdy jsou narušena práva na ochranu soukromí některého ze subjektu osobních údajů, podává tento subjekt občanskoprávní žalobu, chce-li se domoci finanční náhrady za jemu způsobenou újmu.

V porovnání s britským systémem, kde působí obdobný úřad nazvaný ICO, je český úřad pro ochranu osobních údajů pouhým indikátorem problémů. ICO disponuje vlastní vymáhací mocí na sankce, které uloží. Jeho agenda se skládá především z vyhledávání problémů v oblasti osobních údajů, které pak předkládá soudům. Na rozdíl od českého Úřadu však nefiguruje před soudem jako strana sporu.

Co se týče samotné právní úpravy kamerových systémů ve Velké Británii, není ale co vychvalovat. Nelze mluvit o žádné právní jistotě ani konkrétně stanovených hranicích. Celá situace kamerových systémů je navíc dost netransparentní a před veřejností se britská vláda snaží leccos utajit. Například zavedení projektu The Internet Eyes a jeho registrace u ICO je jedna velká záhada, kterou neodhalilo ani BBC, respektive v příhodnou dobu o problematice začalo mlčet. Na pováženou je program „Sin bins worst families“, který hraničí pomalu s vězeňským dohledem. Porovnám-li ho s dohledem pomocí elektronických náramků, je kamerové sledování soukromého života v asociálních rodinách mnohem horší. Zajímavé je, že i zde média mlčí.

Má původní domněnka, že Velká Británie jako průkopník masové instalace kamerových systémů vlastní dostatečně propracovanou právní úpravu a že by se od ní mohli ostatní země inspirovat, byla mylná. Britská právní úprava je obdobná jako v českém právním řádu, který se s velkou pravděpodobností právě britskou úpravou inspiroval. Ve Velké Británii také dochází k porušování základních lidských práv a svobod a až zarážejícím způsobem to místní vládě prochází.

Závěrem bych chtěla shrnout, že užívání kamerových systémů, a to ať už se záznamem nebo bez záznamu, akutně vyžaduje speciální právní úpravu, která se bude zabývat výlučně provozováním kamerových systémů a bude co nejvíce konkretizovat hranice jejich užívání.

Seznam použitých zdrojů

Odborná literatura a monografie

BARTÍK, Václav, Janečková, Eva. Zákon o ochraně osobních údajů s komentářem. 1. vyd. Olomouc: ANAG, 2010. ISBN 978-80-7263-613-6.

JANEČKOVÁ, Eva,. Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 9788072018505.

KLÍMA, Karel. Ústavní právo. 3. rozšířené vydání. Plzeň: Aleš Čeněk, s.r.o., 2006. ISBN 80-7380-000-4.

NOUWT, Sjaak. Reasonable Expectations of Privacy?: Eleven country reports on camera surveillance and workplace privacy (Information Technology and Law Series). The Hague: T.M.C. Asser Press, 2005. ISBN 9789067041980.

NOVÁK, Daniel. *Problémy ochrany soukromí a osobních údajů v právu EU*. Brno, 2010/2011. Disertační práce. Právnická fakulta Masarykovy univerzity.

Právnický slovník. 2. rozšířené vydání. Praha: C. H. Beck, 2001. ISBN 80-7179-740-5.

VERMAN ROMESH. *Distance Education In Technological Age*. Pvt. Ltd.: Anmol Publications, 2005. ISBN 8126122102.

Internetové zdroje

5RB, http://www.5rb.com/

Ministerstvo vnitra České republiky, *Aktualizované stanovisko k provozování kamerových systémů obecní policií* –právní stav ke dni 10. října 2011, 18.března 2012, dostupné na http://www.google.com/cse?cx=015489265366623571386%3Aizzrwg3bmqm&q=kamerov%C3%A9+syst%C3%A9my&ok.x=0&ok.y=0&ok=ok#gsc.tab=0&gsc.q=kamerov%C3%A9%20syst%C3%A9my&gsc.page=1

A Study of CCTV at Harvard, *Legislation*, 17.března 2012, dostupné na http://www.eecs.harvard.edu/cs199r/fp/JanaRachel.pdf

ATL, *Use of CCTV surveillance in schools*, 25.března 2012, dostupné na http://www.atl.org.uk/policy-and-campaigns/policies/CCTV-policy.asp

BBC New, *Public to monitor CCTV from home*, 21.března 2012, dostupné na http://news.bbc.co.uk/2/hi/uk_news/england/london/8293784.stm

British and Irish Legal Information Institute, http://www.bailii.org/

Česká stomatologická komora, *Použití kamerového systému v čekárně zdravotnického zařízení*, 21.března 2012, dostupné na http://www.dent.cz/detail-text.php?id_strana=27&id_text=182

EXPRESS.co.uk, *SIN BINS FOR WORST FAMILIES*, 25.března, dostupné na http://www.express.co.uk/posts/view/115736/Sin-bins-for-worst-families

ICO, *About the ICO*, 24.března 2012, dostupné na http://www.ico.gov.uk/about_us.aspx

IDNES.cz ,*Plzeňská městská kamera sledovala byt, ne křižovatku* [online]. 2007, 16.BŘEZNA 2012, dostupné z: http://zpravy.idnes.cz/plzenska-mestska-kamera-sledovala-byt-ne-krizovatku-pcf-/domaci.aspx?c=A070801_144158_domaci_hos

Iuridicum Remedium, *Pracovní skupina podle článku 29 směrnice (dále jen WP 29)*, 15. Března 2012, dostupné na www.iure.org/15/pracovní-skupina-podle-clanku-29-smernice-dale-jen-wp29

Lupacz, *Sledování odstartovalo. Je to bezpečnostní průšvih*, 21.března 2012, dostupné na http://www.lupa.cz/clanky/sledovani-londynanu-zacalo-bezpecnostni-prusvih/

NALUS, http://nalus.usoud.cz/

European Commission, http://ec.europa.eu/

Europena Commission, *Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance*, 12.března 2012, dostupné na http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp89_en.pdf

Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance, *G) Additional Requirements*,14.března 2012, dostupné na http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp89_en.pdf

Policejní akademie České republiky, *Právo na soukromí*, 28. února 2012; dostupné na http://www.polac.cz/g2/view.php?katedry/kspd/pril9.ppt

Státní úřad inspekce práce, *Základní údaje*, 5. března 2012, dostupné na http://www.suip.cz/o-nas/zakladni-udaje/

Úřad pro ochranu osobních údajů, http://www.uoou.cz/

Úřad pro ochranu osobních údajů, Komentář k Zásadám provozování kamerového systému z hlediska zákona o ochraně osobních údajů, 26. února 2012; dostupné na

http://www.uoou.cz/uoou.aspx?menu=14&loc=328#kamery

Úřad pro ochranu osobních údajů; *Stanovisko č. 4/2004 ke zpracování osobních údajů prostředky kamerového sledování*; 27.února 2012; dostupné na http://www.uoou.cz/uoou.aspx?menu=50&submenu=52&loc=83#pp3

Úřad pro ochranu osobních údajů, *Stanovisko č. 1/2006*, 10.březen 2012, dostupné na http://www.uoou.cz/files/stanovisko_2006_1.pdf

Úřad pro ochranu osobních údajů, *Stanovisko č. 2/2008*, 13.březen 2012, dostupné na http://www.uoou.cz/files/stanovisko_2008_2.pdf

Úřad pro ochranu osobních údajů, *Vyjádření a doporučení ÚOOU k možnosti instalovat kamerový systém v prostorách školy*, 23.března 2012, dostupné na http://www.uoou.cz/files/vyjadreni_a_doporuceni_uoou.pdf

Užij si svá práva.cz, *Sledování na pracovišti*, 21.březen 2012, dostupné na http://www.uzijsisoukromi.cz/sledovani-na-pracovisti/

Užij si svá práva.cz, *Veřejné kamerové systémy*, 18.března 2012, dostupné na http://www.uzijsisoukromi.cz/verejne-kamerove-systemy/

Zvědavec, V *Británii chtějí umístit CCTV kamery do soukromých domů a bytů*, 25.března 2012, dostupné na http://www.zvedavec.org/komentare/2009/08/3251-v-britanii-chteji-umistit-cctv-kamery-do-soukromych-domu-a-bytu.htm

Databáze

Evropský Parlament a Rada, Směrnice č. 95/46/ES [o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů] ASPI [databáze] ASPI stav k 15.3.2012 [cit. 2012-03-23]

Evropský Parlament a Rada, Směrnice č. 2002/58/ES [o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích] ASPI [databáze] ASPI stav k 15.3.2012 [cit. 2012-03-23]

FIALa, Josef a kol. Komentář k §127 odst. 1 zák. č. 40/1964 Sb. [omezení vlastnického práva-sousedské právo] ASPI [databáze] ASPI stav k 15.3. 2012 [cit. 2012-03-24]

FIALA, Josef. Komentář k §433 zák. č. 40/1964 Sb. [Odpovědnost za vnesené a odložené věci] ASPI [databáze]. ASPI stav k 15.3.2012 [cit. 2012-03-19]

Nejvyšší soud (NS) ČR, 3 Tdo 593/2009 – Usnesení [Důkaz] ASPI [databáze]. ASPI stav k 15.3.2012 [cit. 2012-03-18]

Nejvyšší správní soud, 4 Ans 6/2006 – 162, Původní nebo upravené texty pro ASPI [Rozsudek] ASPI [databáze] ASPI stav k 15.3. 2012 [cit. 2012-03-21]

Nejvyšší soud (NS) ČR, 8 Tdo 682/2009 – Usnesení [K trestnému činu výtržnictví – místo veřejnosti přístupné (§202)] ASPI [databáze] ASPI stav k 15.3.2012 [2012-03-18]

Nejvyšší soud (NS) ČR, 22 Cdo 1150/99 – Rozhodnutí (RC) [Sousedská práva a obtěžování pohledem jako imise] ASPI [databáze] ASPI stav k 15.3. 2012 [cit. 2012-03-24]

Nejvyšší správní soud (NSS), sp. zn. 9 As 34/2008 – 68 - Rozsudek [Ochrana osobních údajů: zpracovatel osobních údajů] ASPI [databáze] ASPI stav k 15.3.2012 [cit. 2012-03-15]
Nejvyšší státní zástupce, Výkladové stanovisko NSZ (Vykls)[Vykls 10/2003 K zákonnosti umístění audio-vizuálních prostředků ve školských zařízení vykonávajících ústavní výchovu a ochranou výchovu] ASPI [databáze] ASPI stav k 15.3.2012 [cit. 2012-03-15]

Ústavní soud (ÚS), IV. ÚS 154/97 – Nález (ÚS) [Lidská důstojnost, osobní čest, dobrá pověst] ASPI [databáze] ASPI stav k 15.3.2012 [cit. 2012-03-21]

Ústavní soud (ÚS), Pl. ÚS 4/94 – Nález (ÚS) [Práva obviněného v trestním řízení (214/1994 Sb.)] ASPI [databáze] ASPI stav k 15.3.2012 [cit. 2012-03-15]

Vláda České republiky, Nařízení č. 371/2004 Sb. [Nařízení vlády České republiky, kterým se vydávají vzorové stanovy společenství vlastníků jednotek] ASPI [databáze] ASPI stav k 15.3. 2012 [cit. 2012-3-24]

VYSOKAJOVÁ, Margerita. Komentář k § 34 zák. č. 262/2006 Sb. [Náležitosti pracovní smlouvy] ASPI [databáze] ASPI stav k 15.3.2012 [cit. 2012-03-21]

Seznam použitých právních předpisů

z. č. 2/1993 Sb., Listina základních práv a svobod

z. č. 40/1964 občanský zákoník, ve znění pozdějších předpisů

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

z. č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů

z. č. 128/2000 Sb. o obcích (obecní zřízení), ve znění pozdějších předpisů

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

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

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

z. č. 40/2009 trestní zákoník, ve znění pozdějších předpisů
Vyhláška Ministerstva zdravotnictví č. 221/2010 Sb. Příloha č. 3

Evropská úmluvy o ochraně lidských práv a základních svobod ze dne 4. listopadu 1950

Směrnice 95/46/ES

The Data Protection Act 1998 (DPA)
The Human Right Act 1998

Soudní judikatura a správní rozhodnutí

Nález Ústavního soudu, Pl. ÚS 4/94

Nález Ústavního soudu, II.ÚS 2806/08

Rozsudek Městského soudu v Praze, sp. zn. 7 Ca 204/2005 – 49

Rozsudek Městského soudu v Praze, sp. zn. 11 Ca 298/2008 – 47

Rozsudek Městského soudu v Praze, sp. zn. 11 Ca 433/2008-89

Campbell v MGN Ltd (HL) Case Reference [2004] UKHL 22; [2004] 2 AC 457; [2004] 2 WLR 1232; [2004] EMLR 247 Court House of Lords

Douglas v Hello! Ltd Case Reference [2001] QB 967; [2001] 2 WLR 992; [2001] 2 All ER 289; [2001] EMLR 199; [2001] FSR 732 Court Court of Appeal

England and Wales Court of Appeal (Civil Division) Decisions, Wood and Commissioner of Plolice for the Metropolis, Case No: C1/2008/1466

European Court of Human Rights, CASE OF PECK v. THE UNITED KINGDOM, Application no. 44647/98

Rozhodnutí Úřadu pro ochranu osobních údajů, zn. REG – 1218/08

Rozhodnutí Úřadu pro ochranu osobních údajů, zn. VER-2041/08-28,

Seznam zkratek

ICO	Information Commissioner´ s Office
DPA	The Data Prorotection Act 1998
EÚLP	Evropská úmluva o ochraně lidských práv a základních Svobodách
Úřad	Úřad pro ochranu osobních údajů
WP 29	The Data Protection Working Party
MDKS	městské dohlížecí kamerové systémy
DPA	The Data Protection Act 1998
Rada	Bretwood Borough Council
ATL	The Education Union
ESLP	Evropský soud pro lidská práva

Resumé

This diploma work deals with the issues related to the use and legal framework for the use of video surveillance systems. Video surveillance systems were first used in the 1970s in Great Britain to protect embassies, airports, banks, prisons, i.e. objects that had been until then under constant surveillance by the employees. In the 1990s video surveillance systems were gradually used for monitoring of public spaces, publically accessible premises and later also for private use.

Extensive use of video surveillance systems for processing personal data logically requires proper legal framework. However, due to the short history of this technology the existing legislation is very general and not thoroughly elaborated. The situation is not aided by the fact that the technology develops faster than the lawmakers can react.

The basic legal framework for processing personal data within the Czech legislation is the Personal Data Protection Act No. 101/2000 Col. But also the Civil Code contains provisions on the protection of personality rights and, of course, the basic human rights and liberties protected by the Declaration of Human Rights must be respected as well.

The oversight authority in the Czech Republic is the Office for Personal Data Protection. Every administrator of personal data must register with this administrative body in order to be permitted to process personal data. Analogous agency in Great Britain is the ICO. The difference is that unlike Czech Office for Personal Data Protection the ICO has the authority to enforce the rectifications and sanctions it imposes.

In conclusion we observe that the legal framework for video surveillance systems in the Czech Republic, as well as in Great Britain, is insufficient due to the non-existence of a special law, which would address specifically video surveillance systems.