Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra práva

Diplomová práce

Používání kamerových systémů a ochrana osobnosti

Bc. Aneta Kašpárková

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Aneta Kašpárková

Podnikání a administrativa

Název práce

Používání kamerových systémů a ochrana osobnosti

Název anglicky

The use of CCTV systems and protection of personality

Cíle práce

Cílem práce je analýza právní úpravy kamerových systémů a právní úpravy ochrany osobnosti, srovnání režimů právní regulace provozu kamerového systému se záznamem a bez záznamu a identifikace rozdílů mezi nimi. Dílčím cílem je na příkladu kamerového systému v bytových domech (za použití metody statistické a kvalitativního výzkumu) zjistit, jakým způsobem jsou jeho obyvatelé a návštěvníci chráněni před shromažďováním osobních údajů, a zda je kamerový systém provozován v souladu s platnými právními předpisy, tento vztah vyhodnotit a zaujmout právní názor.

Metodika

V teoretické části diplomové práce bude použita zejména analýza platné právní úpravy ČR a EU, která se věnuje ochraně osobnosti a používání kamerových systémů. Dále bude použita metoda komparace porovnávající kamerové systémy se záznamem a bez záznamu.

V praktické části diplomové práce bude použita metoda statistická, která zachycuje vývoj kriminality v bytových domech, a dále bude použita metoda řízeného rozhovoru s provozovatelem kamerových systémů v bytových domech. Na závěr bude použita metoda syntézy k vyhodnocení jednotlivých zjištění.

Doporučený rozsah práce

60-80

Klíčová slova

Ochrana osobnosti, ochrana osobních údajů, kamerové systémy, osobní údaje, citlivé údaje, správce osobních údajů, ochrana soukromí, Úřad pro ochranu osobních údajů, zákon o ochraně osobních údajů

Doporučené zdroje informací

BARTÍK, V. JANEČKOVÁ, E., Kamerové systémy v praxi. Praha: Linde, 2011. ISBN 978-80-7201-850-5

Data Protection and Privacy: JurisdictionalComparisons. Sweet& Maxwell, 2012. ISBN 978-1-908230-14-3

KUČEROVÁ, A. Zákon o ochraně osobních údajů. Komentář. Praha: C. H. Beck, 2012. ISBN 978-80-7179-226-0

MATOUŠOVÁ, M., HEJLÍK, L. Osobní údaje a jejich ochrana. 2. Doplněné a aktualizované vydání. Praha: ASPI, 2008. ISBN 978-80-7357-322-5

NOVÁK, D. Zákon o ochraně osobních údajů a předpisy související. Komentář. Praha: WoltersKluwer, 2015. ISBN 978-80-7478-665-5

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

ŠVESTKA, J., DVOŘÁK, J., FIALA, J. Občanský zákoník. Komentář. Svazek I (§ 1-654). Praha: WoltersKluwer, 2014. ISBN 978-80-7478-370-8

ŠVESTKA, J. Občanský zákoník. Komentář. Svazek VI (§ 2521 až § 3081). Praha: WoltersKluwer, 2014. ISBN 978-80-7478-369-2

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

Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů

Předběžný termín obhajoby

2018/19 ZS – PEF (únor 2019)

Vedoucí práce

JUDr. Jitka Mráčková, CSc.

Garantující pracoviště

Katedra práva

Elektronicky schváleno dne 27. 11. 2017

JUDr. Jana Borská, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 28. 11. 2017

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 29. 11. 2018

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Používání kamerových systémů a ochrana osobnosti" jsem vypracovala samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autorka uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušila autorská práva třetích osob.

V Praze dne 29. 11. 2018 _____

Poděkování

Ráda bych touto cestou poděkovala paní JUDr. Jitce Mráčkové, CSc. za cenné připomínky, rady, ochotu a odborné vedení, které mi pomohly při zpracování této práce. Dále bych ráda poděkovala firmě Siemens, s. r. o., za odbornou konzultaci a panu Bc. Jiřímu Svobodovi za poskytnutý rozhovor. Dále děkuji všem, kteří mě po celou dobu studií podporovali.

Používání kamerových systémů a ochrana osobnosti

Abstrakt

Diplomová práce „Používání kamerových systémů a ochrana osobnosti“ se zabývá používáním kamerových systémů a v souvislosti s ním spojenou ochranou osobnosti. Zaměřuje se na analýzu právní úpravy používání kamerových systémů, na kterou lze nahlížet z hlediska právní úpravy ochrany osobnosti, zabývající se především ochranou soukromí, a z hlediska nové právní úpravy ochrany osobních údajů. Pozornost je věnována především zásadním změnám a úpravě zcela nových práv a povinností, které byly s účinností Obecného nařízení o ochraně osobních údajů zavedeny. Dále jsou v práci porovnány režimy právní regulace provozu kamerového systému se záznamem a bez záznamu a identifikace rozdílů mezi nimi. Vlastní práce je zaměřena na problematiku provozování kamerových systémů v bytových domech z pohledu současné běžné praxe a s ohledem na dodržování platných právních předpisů - konkrétněji na právní hlediska plynoucí z používání kamerových systémů v bytových domech, rovněž jsou uvedeny příklady z praxe. Práce je zakončena stručným seznámením s navrhovanou budoucí právní úpravou ochrany osobních údajů, tzv. adaptační zákon.

Klíčová slova: ochrana osobnosti, ochrana osobních údajů, ochrana soukromí, kamerové systémy, osobní údaje, zvláštní kategorie osobních údajů, soukromí, správce osobních údajů, zpracování osobních údajů

The use of CCTV systems and protection of personality

Abstract

The thesis „The use of CCTV systems and protection of personality" deals with the use of CCTV systems and related protection of personality. The thesis focuses on the analysis of the legislation of the use of CCTV systems from two points of view: the legislation of personality protection (especially protection of privacy) and the new legislation of protection of personal data. Attention is paid mainly to major changes and changes of completely new rights and obligations introduced by the General Data Protection Regulation. In the thesis there are also compared the modes of legal regulation of the CCTV system with recording and without recording and identification of the differences between them. The practical part of the thesis is focused on the issue of operation of the CCTV systems in apartment houses from the point of view of current practice and with respect to the valid legislation – specifically on the legal aspects following from the use of CCTV systems in the apartment houses. There are also given examples from the practice in the thesis. The thesis is ended with the brief introduction of the proposed future legislation on the protection of personal data (an adaptation law).

Keywords: protection of personality, protection of personal data, privacy protection, CCTV systems, personal data, special categories of personal data, privacy, controller of personal data, processing of personal data

Obsah

Seznam obrázků

Seznam tabulek

Seznam grafů

Seznam použitých zkratek

atd.	a tak dále
apod.	a podobně
BYOD	Bring Your Own Device
CCTV	Closed Circuit TeleVision
ČR	Česká republika
ČSÚ	Český statistický úřad
DVR	Digital Video Recorder
EU	Evropská unie
ES	Evropská společenství
GDPR	General Data Protection Regulation (Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
IoT	Internet of Things
IP	IP address
LAN	Local Area Network
Listina	Listina základní práv a svobod (ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů)
mj.	mimo jiné
např.	například
OZ	Občanský zákoník (zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů)
OZO	Obecný zákoník občanský (č. 946/1811 Sb. z. s., ve znění pozdějších předpisů)
PoE	Power over Ethernet
příp.	případně
resp.	respektive
SVJ	Společenství vlastníků jednotek
TCP	Transmission Control Protocol
tzv.	takzvaný, takzvaně
ÚOOÚ	Úřad pro ochranu osobních údajů
Ústava	Ústava České Republiky (ústavní zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpisů)
Vykls	Výkladové stanovisko
ZoOU	Zákon o ochraně osobních údajů (zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů)

1 Úvod

„Zavádění kamerových systémů v průběhu posledního desetiletí nabylo na popularitě a snadno tak můžeme nabýt dojmu, že jsme sledováni na každém kroku. Zdá se, že bez toho, abychom byli všetečným okem pozorováni, nemůžeme projít bytovým domem k našim dveřím, jet výtahem, nakoupit v obchodě, zajít si k lékaři, ubytovat se v hotelu, chodit do práce, vyřídit záležitost na úřadě a někdy i jen projet křižovatku. Kamerové systémy jsou všudypřítomné. Někteří z nás kamery již nevnímají a berou je jako běžnou součást našich životů, jiní se však třeba občas pozastaví nad umístěním určité kamery či důvody, proč je kamerový systém na určitém místě instalován.“[1]

Úkolem mé diplomové práce je analyzovat právní úpravu používání kamerových systémů a v souvislosti s ní spojenou právní úpravu ochrany osobnosti. Na právní úpravu kamerových systémů lze nahlížet ze dvou hledisek. Prvním hlediskem je ochrana osobnosti, zabývající se především ochranou soukromí a druhým je ochrana osobních údajů. První ustanovení týkající se ochrany osobnosti na českém území lze nalézt už v Obecném zákoníku občanském č. 946/1811 Sb. zák. soud. (dále jen „OZO“), ovšem ucelená právní úprava ochrany osobnosti byla zakotvena až v občanském zákoníku z roku 1964. Tehdejší občanský zákoník prošel několika novelizacemi a až v roce 2012 byl přijat nový občanský zákoník č. 89/2012 Sb. (dále jen „OZ“). V legislativě České republiky (dále jen „ČR“) je ochrana osobnosti zakotvena také v ústavním zákoně č. 1/1993 Sb., Ústava České republiky (dále jen „Ústava“) a v ústavním zákoně č. 2/1993 Sb., Listina základních práv a svobod (dále jen „Listina“). V roce 2000 byl přijat vlastní zákon týkající se ochrany osobních údajů, a to zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (dále jen „ZoOU“) vycházející ze Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „Směrnice 95/46/ES“). Protože právní rámec, založený na Směrnici 95/46/ES, přestal odpovídat současné době a také nebylo dosaženo požadované míry sjednocení právní úpravy v jednotlivých zemích Evropské unie (dále jen „EU“), bylo v roce 2016 schváleno obecné nařízení o ochraně osobních údajů (angl. General Data Protection Regulation) (dále jen „GDPR“), jehož cílem je výrazné zvýšení ochrany osobních dat občanů ve všech státech EU. Plným názvem Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a

[1] CHWISTKOVÁ, K., Náš život před kamerou aneb Kamerové systémy v praxi [online]. 2016 [cit. 2018-11-07]. Dostupné z: http://www.hajduk.cz/nas-zivot-pred-kamerou-aneb-kamerove-systemy-v-praxi/

o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) nabylo účinnosti 25. května 2018 a v českém právním prostředí tak z velké části nahradilo právní úpravu obsaženou v ZoOU.

Práce je rozdělena na dvě části – teoretická východiska a vlastní práce. V první části jsou vysvětleny některé základní pojmy, které jsou nezbytné k lepšímu pochopení dané problematiky. Dále je definován kamerový systém, princip jeho fungování a srovnání režimů právní regulace provozu kamerového systému se záznamem a bez záznamu a identifikace rozdílů mezi nimi. Také jsou nastíněny náklady na fungování kamerových systémů. Následuje analýza platné právní úpravy používání kamerových systémů a s ní spojená analýza ochrany osobnosti podle OZ, ochrany osobních údajů a ochrany zvláštních kategorií osobních údajů podle GDPR (zejména analýza práv a povinností při zpracování těchto údajů).

Kamerové systémy jsou zaváděny především za účelem ochrany majetku a bezpečnosti osob, což jsou i časté důvody pro umístění kamerových systémů v bytových domech. Kamerový systém však není jediným účinným opatřením, jak majetek nebo osoby chránit. V řadě případů tak kamerové systémy nahrazují nedostatky v mechanickém nebo elektronickém zabezpečení. Jde o prostředek nepochybně účinný, ale zároveň také velmi agresivní vůči soukromí osob. Druhá část práce je věnována kamerovým systémům v bytových domech, jelikož k závažným zásahům do soukromého a osobního života osob dochází nejčastěji právě v okolí našich domovů. Vlastní práce se zaměřuje především na provozování kamerových systémů v souladu s platnými právními předpisy. Každý, kdo hodlá kamerový systém provozovat, musí nejprve jeho potřebnost pečlivě uvážit, proto se v této části práce zaměřuji na důvody pro zavedení kamerových systémů v bytových domech, na umístění kamerových systémů v bytových domech (kamerový systém nelze instalovat kdekoli v prostorách bytového domu), dále na právní hlediska plynoucí z používání kamerových systémů v bytových domech, a v neposlední řadě také na náklady, tedy na kolik nás provozování kamerového systému včetně jeho pořízení vyjde. Vlastní práce je obohacena o rozhovor s obyvatelem bytového domu, ve kterém je kamerový systém se záznamem instalován.

Celou práci poté zakončuji vyhodnocením jednotlivých zjištění a stručným seznámením s navrhovanou budoucí právní úpravou, tzv. adaptační zákon, jehož návrh se nyní nachází v legislativním procesu. Po jeho schválení tak bude spolu s GDPR upravovat ochranu osobních údajů na našem území.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem diplomové práce je analýza právní úpravy používání kamerových systémů a v souvislosti s ní spojená analýza právní úpravy ochrany osobnosti, jejíž součástí je i nástin vývoje ochrany osobnosti v občanském zákoníku. V souvislosti s používáním kamerových systémů se práce zaměřuje na zásadní změny a úpravy zcela nových práv a povinností, které byly s účinností GDPR zavedeny. Dalším cílem je srovnání režimů právní regulace provozu kamerového systému se záznamem a bez záznamu a identifikace rozdílů mezi nimi.

Cílem praktické části je na příkladech kamerových systémů v bytových domech zjistit, jakým způsobem jsou obyvatelé a návštěvníci domu chráněni před shromažďováním osobních údajů, a za jakých podmínek je kamerový systém v bytovém domě provozován v souladu s platnými právními předpisy a vyhodnotit tento vztah. Praktická část je doplněna o rozhovor s obyvatelem bytového domu, který zjišťuje, s jakými problémy či nedostatky se provozovatelé kamerového systému v bytových domech musí v praxi vypořádat. Práce je zakončena stručným seznámením s navrhovanou budoucí právní úpravou, tzv. adaptační zákon.

2.2 Metodika

Diplomová práce je rozdělena na teoretickou a praktickou část. U první, teoretické části, metodika zpracování spočívala ve shromažďování studijních materiálů, jejich následném pečlivém prostudování a dalším zpracování poznatků tímto způsobem získaných. K získání adekvátních dat byly využity také četné aktuální internetové zdroje, jelikož problematika používání kamerových systémů není v odborné literatuře příliš zastoupena a navíc prochází neustálým vývojem. První část práce je věnována výkladu pojmů, které úzce souvisí s používáním kamerových systémů, zde byla použita metoda výkladu práva. Dále byl použit systematický výklad práva pro rozbor legislativy pro analyzování platné právní úpravy, která se věnuje ochraně osobnosti a používání kamerových systémů. Kromě vymezení právních předpisů, především ústavních zákonů, a to zákona č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpisů, a zákona č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů, byl zejména analyzován zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, a zvláště velký důraz byl kladen na Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

U systematického rozboru Nařízení Evropského parlamentu a Rady (EU) 2016/679 byla použita i metoda historická, jež nám ukázala vývoj této legislativy. Pomocí této metody byl nastíněn i vývoj ochrany osobnosti v občanském zákoníku. Dále byla použita metoda komparace porovnávající režimy právní regulace provozu kamerového systému se záznamem a bez záznamu.

V praktické části je užita metoda analýzy kamerových systémů v bytových domech, konkrétněji jeho provozování, kde je kladen důraz zejména na jeho umístění, a právních hledisek plynoucích z jeho používání. Dále byla použita metoda statistická, která zachycuje vývoj kriminality v bytových domech, jakožto jeden z hlavních důvodů pro zavedení kamerových systémů v bytových domech. Pro vyhodnocení situace provozování kamerových systémů v bytových domech z pohledu současné běžné praxe a s ohledem na dodržování platných právních předpisů byla použita metoda kvalitativního sociologického výzkumu. Rozhovor je polostrukturovaný, který též *„bývá nazýván řízený. Přesto, že si pro takový rozhovor připravujeme soubor otázek, označuje se také rozhovor s návodem; bývá považován za optimální způsob získávání dat.“*[2] Respondentem je obyvatel bytového domu, ve kterém je kamerový systém provozován. Pro vyhodnocení jednotlivých zjištění je užita metoda syntézy.

[2] SEDLÁKOVÁ, R., Výzkum médií: nejužívanější metody a techniky, str. 211

3 Teoretická východiska

3.1 Úvodem

„Jedním z fenoménů současné doby je snaha zabezpečit ochranu své osoby, rodiny, majetku, zdraví apod. prostřednictvím maximálního využití technologií umožňujících monitorovat pohyb kolem nás.“[3]

Nejprve je nutno si vysvětlit několik základních pojmů. Prvním z pojmů je kamerový systém, dále osobní údaj a zvláštní kategorie osobních údajů, koho lze považovat za správce osobních údajů a co vše obnáší zpracování osobních údajů a nakonec pojem soukromí.

3.2 Základní pojmy

3.2.1 Kamerový systém

Za kamerový systém lze považovat *„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.“*[4]

Kamerové systémy se mohou skládat ze statických i otočných kamer a mohou pracovat buď v automatickém režimu, nebo mohou být ovládány např. ostrahou objektu. S dostatečnými přístupovými právy se může uživatel do systému nejen vzdáleně připojit a sledovat obrazy z živých kamer, ale sledovat i záznam nebo celé zařízení ovládat.

3.2.2 Osobní údaj

Za osobní údaje lze považovat veškeré informace o fyzické osobě[5] (dále jen „subjekt údajů“), kterou je možné identifikovat ať už přímo či nepřímo pomocí určitých identifikátorů[6].[7] Oproti definici osobních údajů, uvedené ve Směrnici 95/46/ES a následně i v ZoOU, došlo v GDPR

[3] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Na aktuální téma – Archiv. Komentář k Zásadám provozování kamerového systému z hlediska zákona o ochraně osobních údajů [online]. In: uoou.cz, Leden 2006 [cit. 2018-02-27]. Dostupný z: https://www.uoou.cz/vismo/zobraz_dok.asp?id_ktg=1103&p1=1103#kamery

[4] BARTÍK, V., JANEČKOVÁ, E., Kamerové systémy v praxi, str. 19

[5] identifikované nebo identifikovatelné

[6] Podle čl. 4 odst. 1) GDPR jsou identifikátory např. *„jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osob.“*

[7] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 4 odst. 1). [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679

k rozšíření výčtu identifikátorů, podle kterých lze subjekt údajů přímo či nepřímo identifikovat. Zejména se jedná o jméno, lokační údaje, síťový identifikátor a genetický prvek fyzické osoby.[8] Přidání lokačního údaje či síťového identifikátoru fyzické osoby do explicitního výčtu osobních údajů je především důsledkem obrovského technologického pokroku od roku 1995.

Za obecné osobní údaje jsou považovány jméno, pohlaví, věk, datum narození, osobní stav, ale i IP adresa či fotografický záznam.

3.2.3 Zvláštní kategorie osobních údajů

Podle čl. 9 odst. 1 GDPR zvláštní kategorie osobních údajů zahrnuje osobní údaje, „*které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.*“[9]

I zde je ve výčtu osobních údajů, které zvláštní kategorie údajů obsahují, patrný rozdíl mezi Směrnicí 95/46/ES a GDPR. GDPR nově vymezuje zpracování genetických údajů[10], biometrických údajů[11] za účelem jedinečné identifikace subjektu údajů a údajů o sexuální orientaci fyzické osoby explicitně. Směrnice 95/46/ES výčet takových údajů neobsahovala.[12] Možná právě proto, že před třiadvaceti lety nebyly běžně dostupné technologie, které genetické a biometrické údaje dokázaly zpracovat (např. čtečky na otisk prstu, detekce obličeje apod.).

Rozdíl je i mezi GDPR a ZoOU, ve kterém byly zvláštní kategorie osobních údajů nazývány jako citlivé údaje. Mezi výčtem citlivých údajů a výčtem osobních údajů obsažených ve zvláštních kategoriích osobních údajů lze nalézt následující rozdíly. Tak např. GDPR mezi zvláštní kategorie osobních údajů nezařazuje osobní údaj vypovídající o národnostním původu, naopak ale ZoOU již zahrnoval genetické údaje a biometrické údaje, které umožňují přímou identifikaci nebo autentizaci

[8] JANEČKOVÁ, E., GDPR. Praktická příručka implementace, str. 2

[9] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 9 odst. 1. [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679

[10] Podle čl. 4 odst. 13) GDPR se genetickými údaji rozumí *„osobní údaje týkající se zděděných nebo získaných genetických znaků fyzické osoby, které poskytují jedinečné informace o její fyziologii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotčené fyzické osoby.“*

[11] Podle čl. 4 odst. 14) GDPR se biometrickými údaji rozumí *„osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci.“*

[12] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů [online]. Čl. 8 odst. 1. [cit. 2018-02-27]. Dostupná z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679

fyzických osob.[13] Dále ZoOU za citlivý údaj považoval i údaj o odsouzení za trestný čin, GDPR tento údaj sice nepovažuje explicitně za zvláštní kategorii osobních údajů, ale upravuje jej samostatně ustanovení čl. 10 GDPR.[14]

3.2.4 Správce osobních údajů

Správcem osobních údajů může být každý subjekt[15], který buď sám anebo společně s jinými určuje účely a prostředky zpracování osobních údajů.[16] Definici správce GDPR převzalo ze Směrnice 95/46/ES takřka v nezměněné formě. Odlišnost ve vymezení tohoto pojmu nalézt pouze v ZoOU, který správce definoval jako *„každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj.“*[17] Správce tedy odpovídá za dodržení zásad zpracování, za dodržování povinností upravených GDPR a za zabezpečení údajů.

3.2.5 Zpracování osobních údajů

Za zpracování osobních údajů lze považovat jakoukoliv operaci, soubor operací s osobními údaji, ale i soubory osobních údajů, které jsou prováděny bez pomoci či s pomocí automatizovaných postupů. Ke zpracování osobních údajů tedy dochází např. shromažďováním, zaznamenáváním, uspořádáním, strukturováním, ukládáním, přizpůsobením nebo pozměněním, vyhledáváním, nahlédnutím, použitím, zpřístupněním přenosem, šířením nebo jakýmkoliv jiným zpřístupněním, seřazením či zkombinováním, omezením, výmazem anebo zničením.[18] Vymezení pojmu zpracování osobních údajů v GDPR je oproti Směrnici 95/46/ES a ZoOU opět rozšířeno o některé další operace s osobními údaji, a to zejména o strukturování a nahlédnutí.[19]

[13] viz ust. § 4 písm. b) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů
[14] ŽŮREK, Jiří. Praktický průvodce GDPR, str. 54 a 55
[15] Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt.
[16] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 4 odst. 7). [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679
[17] JANEČKOVÁ, E., GDPR. Praktická příručka implementace, str. 2
[18] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 4 odst. 2). [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679
[19] JANEČKOVÁ, E., GDPR. Praktická příručka implementace, str. 2

Zpracování je zákonné pouze tehdy je-li v odpovídajícím rozsahu splněna nejméně jedna z podmínek v GDPR uvedených.[20] Podmínky zákonného zpracování, které GDPR stanovuje, ve větším rozsahu odpovídají zásadám pro oprávněné zpracování údajů[21] ze Směrnice 95/46/ES. Za zmínku stojí podmínka/zásada udělení souhlasu se zpracováním osobních údajů subjektem údajů, kdy ve Směrnici 95/46/ES bylo explicitně vymezeno, že zpracování osobních údajů může být provedeno pouze pokud *„subjekt údajů nezpochybnitelně udělil souhlas.“*[22] V GDPR slovo *„nezpochybnitelně“* u vymezení této podmínky již nenajdeme, a dalo by se říci, že jej nahrazují ustanovení čl. 7 GDPR o podmínkách vyjádření souhlasu, mezi které mj. patří právě i doložení udělení souhlasu subjektu údajů o zpracování jeho osobních údajů, což se za nezpochybnitelné považovat dá.[23]

3.2.6 Soukromí

Soukromí fyzické osoby její nedotknutelnost a ochrana, patří mezi základní lidská práva a svobody. *„Výrazy „soukromí“ nebo „soukromý“ jsou v právním myšlení nejčastěji spojovány s něčím, co patří pouze fyzické osobě, člověku. Ve vědomí lidí je „soukromé spojováno s něčím, „do čeho nikomu nic není“. Nemusí se ale vždy jednat o majetkové hodnoty. Často může „soukromí“ zahrnovat chování a jednání člověka představující určitou intimní sféru jeho života, kterou si člověk nepřeje zveřejňovat.“*[24]

Na soukromí lze nahlížet ze dvou rovin. *„Jednak je to ochrana proti úniku informací o intimní sféře na veřejnost a jednak ochrana ve vztahu k veřejné kontrole státní moci. Je to ona sféra života člověka, do které bez výslovného dovolení zákona ani toho, koho se týká, nikdo*

[20] Podle čl. 6 odst. 1 GDPR těmito podmínkami jsou *„subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů, zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů, zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje, zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby, zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce, zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.“*

[21] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů [online]. Čl. 7. [cit. 2018-02-27]. Dostupná z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679

[22] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů [online]. Čl. 7 písm. a). [cit. 2018-02-27]. Dostupná z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679

[23] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 7 odst. 1. [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679

[24] PLECITÝ, V., Problematika ochrany osob a majetku z pohledu soukromého a veřejného práva, str. 11

(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.“[25] Z výše uvedeného vyplývá, že zásahy ze zákonných důvodů jsou do soukromí povoleny, ovšem tyto zásahy se musí řídit zásadami přiměřenosti a lze je tedy uskutečnit pouze v takové míře, která soukromí postihuje co nejméně a je schopna ještě zajistit naplnění sledovaného cíle.

V právní teorii se lze setkat i s přístupem dle něhož *„lze právo na ochranu osobního soukromí vymezit jako právo fyzické osoby rozhodnout podle vlastního uvážení zda, popř. v jakém rozsahu a jakým způsobem mají být skutečnosti jejího osobního soukromí zpřístupněny jiným a zároveň se bránit proti neoprávněným zásahům do této sféry ze strany jiných osob s rovným právním postavením.“*[26] Podle názoru Ústavního soudu však toto zúžené pojetí nerespektuje, že soukromý život musí do určité míry zahrnovat i právo na vytváření a rozvíjení vztahu s dalšími lidskými bytostmi. Kromě práva určit, komu budou zpřístupněny určité údaje a možnosti bránit se proti neoprávněným zásahům do intimní sféry, zahrnuje právo na soukromí také závazek státu zajistit respektování tohoto práva.

3.2.7 Závěr

Na začátku bylo nutné si vyložit platnou právní úpravu, která je účinná poměrně krátce, ale nijak významně se neliší od té předchozí. Bylo nutné si vysvětlit, že kamerový systém lze chápat jako automaticky provozovaný stálý technický systém, který umožnuje pořizovat a uchovávat zvukové, obrazové či jiné záznamy ze sledovaných míst, a že se skládá ze statických či otočných kamer, které jsou buďto ovládány člověkem anebo pracují automaticky (viz 3.2.1). Dále pak, co se rozumí osobním údaji - že se jedná o veškeré informace o subjektu údajů, který lze identifikovat přímo či nepřímo pomocí určitých identifikátorů či zvláštních prvků. Vzhledem k rychlému vývoji technologií se nově do výčtu identifikátorů řadí také lokační údaje a síťový identifikátor fyzické osoby a mezi zvláštní prvky pak prvek genetický (viz 3.2.2).

Oproti Směrnici 95/46/ES nově zahrnuje GDPR do zvláštní kategorie osobních údajů údaj o sexuální orientaci fyzické osoby a za účelem identifikace fyzické osoby i zpracování genetických údajů a biometrických údajů. V porovnání s osobními údaji zahrnutými ve zvláštních kategoriích osobních údajů v GDPR s citlivými údaji vymezenými v ZoOU došlo také k některým změnám.

[25] BARTÍK, V., JANEČKOVÁ, E., Kamerové systémy v praxi, str. 12
[26] KNAP, K., ŠVESTKA, J., JEHLIČKA, O., PAVLÍK, P., PLECITÝ, V., Ochrana osobnosti, str. 288

GDPR mezi zvláštní kategorie osobních údajů již nezařazuje osobní údaj vypovídající o národnostním původu a údaj o odsouzení za trestný čin (viz 3.2.3). Bylo nutné si také objasnit, že správcem osobních údajů se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který určuje účely a prostředky zpracování osobních údajů, a že zodpovídá za dodržování zásad zpracování osobních údajů, za dodržování svých povinností a za zabezpečení osobních údajů (viz 3.2.4).

Jakákoliv operace, soubor operací s osobními údaji nebo soubory osobních údajů, které jsou prováděny pomocí či bez pomoci automatizovaných postupů, a to pouze pokud jsou zároveň v odpovídajícím rozsahu splněny i podmínky uvedené v GDPR, lze považovat za zákonné zpracování osobních údajů (viz 3.2.5).

Nedotknutelnost a ochrana soukromí fyzické osoby patří mezi základní lidská práva a svobody. Tudíž do soukromí jakožto do osobní oblasti člověka nelze bez jeho dovolení s výjimkou případů výslovně GDPR stanovených zasahovat ani nahlížet ani pořizovat obrazové záznamy apod. Zároveň má člověk právo rozhodnout podle svého uvážení, zda a v jakém rozsahu a jakým způsobem mají být skutečnosti jeho soukromí zpřístupněny jiným (viz 3.2.6).

3.3 Východiska pro používání kamerových systémů

3.3.1 Kamerový systém

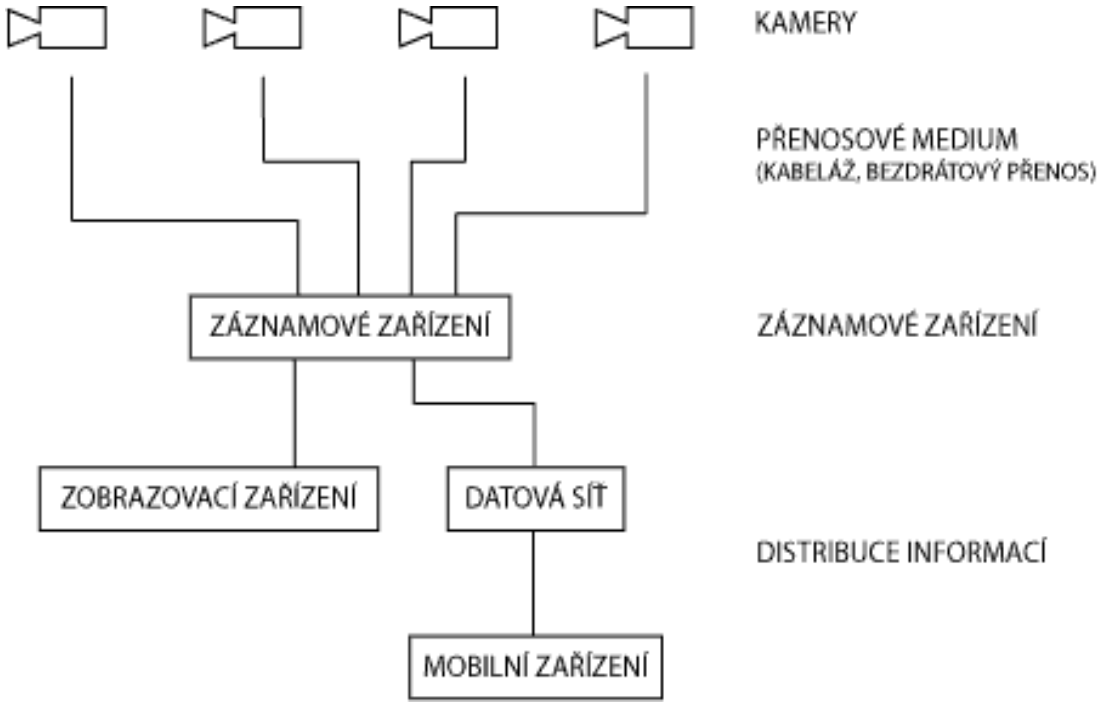
Kamerové systémy, které definuje kapitola 3.2.1, jsou jednou z forem ochrany majetku a osob a slouží k monitorování venkovních prostranství i míst uvnitř budov. Umožňují kontrolu a monitorování oblasti střeženého prostoru a také zajišťují přenos těchto informací do stanoviště obsluhy, kde je pořízený záznam dále zpracováván. Způsobů, jak uchovávat záznamy z kamerových systémů, je celá řada - od zastaralejší formy v podobě videokazet až po moderní formy digitalizace a zálohování dat pomocí počítačových technologií. V ČR funguje na 21 tisíc kamerových systémů.

3.3.1.1 Fungování kamerových systémů

Jedná se o soustavu prvků, pomocí kterých můžeme zaznamenávat, nebo zobrazovat snímané objekty. Dle schématu na obr. č. 1 je kamerový systém rozdělen do čtyř úrovní – samostatné kamery (kamerové body), přenosové medium mezi kamerou a záznamovým zařízením[27], záznamové zařízení a distribuce informací.

[27] U analogových systémů jde o koaxiální kabel, u IP systémů je signál přenášen přes síť LAN, dalším přenosovým médiem může být radiový přenos.

Obrázek č. 1 - Princip kamerových systémů



Zdroj: Princip CCTV, dostupné z: http://www.ladinn.cz/ostatni/technika/kamerovy_system.html

Požadovaná scéna je snímána kamerami. Data, která kamery pořídí, je nutné dopravit na další prvek systému, tím může být úložiště, kde můžeme záznamy pro pozdější potřebu po určitou dobu uchovávat. Existují ale i systémy, kde nemusí být na uložení dat kladen důraz a výstup z kamer je odesílán přímo na zobrazovací zařízení a dále se nearchivuje. Pomocí různých řídících softwarových nástrojů lze například rozpoznávat tváře, či automatizovat čtení státní poznávací značky. V počátcích vývoje kamerových systémů byly kamery pouze analogové, ovšem v dnešní době se nejčastěji používají IP digitální kamery. Kamerové systémy lze tedy rozdělit do dvou základních skupin:

1) CCTV (analogové)
2) IP (digitální)

„Princip fungování kamerového systému je u analogových i IP systémů podobný. Liší se pouze jen v použitých technologiích a přenosových médiích.“[28]

[28] NOVÁK, V., Kamerový systém. In: Ladinn.cz [online]. Tišnov: ELKOV elektro, 2014 [cit. 2018-01-16]. Dostupný z: http://www.ladinn.cz/ostatni/technika/kamerovy_system.html

3.3.1.1.1 Analogové kamerové systémy (CCTV)

Kamerový systém CCTV (z anglického **C**losed **C**ircuit **T**ele**V**ision) znamená „uzavřený televizní okruh“ a jedná se o označení analogových kamerových systémů. V České republice se ale označení CCTV používá pro kamerové systémy obecně.

„Analogový systém se skládá z kamery, která je spojena se záznamovým zařízením pomocí koaxiálního kabelu. Záznamové zařízení se označuje zkratkou DVR (Digital Video Recorder). Toto zařízení jde většinou připojit do sítě LAN a pomocí programu či webového prohlížeče k němu vzdáleně přistupovat.“[29]

„I přesto, že jsou analogové systémy postupně vytlačovány digitálními, jsou stále hojně používaným typem kamerových systémů především vzhledem k jejich ceně a také dostačující kvalitě obrazu. Jejich další výhodou je velmi nízká poruchovost a jednoduchost celého systému.“[30] Naopak největším úskalím těchto systémů je způsob vyhledávání záznamu na pásce, například pokud chceme dohledat konkrétní událost.

3.3.1.1.2 IP (digitální) kamerové systémy

Jedná se o novější a modernější variantu kamerového systému. *„Systém využívá jako přenosové médium mezi kamerami a záznamovým zařízením počítačovou IP síť.“*[31] Princip snímání obrazu u IP kamer je stejný jako u kamer analogových, liší se pouze ve výstupním signálu kamery, který je z analogového převeden na signál digitální. *„Obraz snímaný IP kamerou je přímo v IP kameře prostřednictvím zabudovaného web serveru zkomprimován, převeden na datový tok a zakódován do TCP paketů, které jsou dále šířeny do datové sítě LAN a případně i do internetu. Protokol pro přenos videosignálu z IP kamery vyžaduje zabezpečení přenášených dat (obvykle jménem a heslem) a pro připojení na danou IP kameru je tedy nutné znát tyto přihlašovací údaje.“*[32] Každá IP kamera má svou webovou stránku, pomocí které je možné nastavit a sledovat obraz kamery, a svou jedinečnou IP adresu, na kterou se lze pomocí běžného internetového prohlížeče nebo pomocí klientského softwaru připojit.

[29] NOVÁK, V., Kamerový systém. In: Ladinn.cz [online]. Tišnov: ELKOV elektro, 2014 [cit. 2018-01-16]. Dostupný z: http://www.ladinn.cz/ostatni/technika/kamerovy_system.html
[30] NOVÁK, V., Kamerový systém. In: Ladinn.cz [online]. Tišnov: ELKOV elektro, 2014 [cit. 2018-01-16]. Dostupný z: http://www.ladinn.cz/ostatni/technika/kamerovy_system.html
[31] NOVÁK, V., Kamerový systém. In: Ladinn.cz [online]. Tišnov: ELKOV elektro, 2014 [cit. 2018-01-16]. Dostupný z: http://www.ladinn.cz/ostatni/technika/kamerovy_system.html
[32] Elnika.cz: IP systémy [online]. Praha: Elnika plus, s. r. o. [cit. 2018-02-10]. Dostupné z: https://www.elnika.cz/cz/podpora/pruvodce-kamerovym-systemem/ip-systemy/

Hlavní a tedy největší výhodou IP kamerových systémů je přenos obrazu z jakéhokoli místa na světě pomocí internetové sítě. Tato výhoda, ale zároveň představuje větší riziko, jelikož bezdrátové sítě mají oproti těm kabelovým velkou nevýhodu z hlediska bezpečnosti. Bezdrátové sítě jsou zranitelnější, protože k narušení jejich bezpečnosti stačí být jen v dosahu signálu vysílače. I přesto, že před neautorizovanými úniky dat jsou bezdrátové sítě chráněny mj. pomocí šifrování, které je neustále vyvíjeno, ke kybernetickým útokům často dochází.

Dalšími výhodami jsou možnost použití stávající počítačové sítě, snadnější manipulace se záznamem, snadné ovládaní a snadné zálohování záznamu.

3.3.1.2 Kamerový systém bez záznamu a se záznamem

3.3.1.2.1 Úvodem

Z právního hlediska rozlišujeme dva základní druhy kamerových systémů. A to kamerový systém bez záznamu (tedy bez nahrávání) a kamerový systém se záznamem (tedy s nahráváním a archivací obrazového záznamu po určitou dobu).

3.3.1.2.2 Kamerové systémy bez záznamu

Kamerové systémy bez záznamu lze označit za kamerové systémy (kamerové sledování), při nichž není využíván záznam a ani není instalováno záznamové zařízení, a jedná se tak pouze o on-line přenos obrazu. Lze tedy živě sledovat snímaný prostor na monitoru, ovšem bez možnosti zpětného přehrání. Z tohoto důvodu se na tyto systémy GDPR nevztahuje[33] a lze se řídit pouze obecnými předpisy na ochranu osobnosti, zejména Ústavou, Listinou a OZ. V řadě případů je tak obtížné na otázku možnosti či legality provozovat kamerové systémy bez záznamu jednoznačně odpovědět.

Například ve výkladovém stanovisku Nejvyššího státního zastupitelství pořadové č. 10/2003 je uvedeno, že *„pouhé zrakové a sluchové pozorování, které ani není zaznamenáváno, není právem upraveno a považuje se za samozřejmé, že v zařízeních s určitou koncentrací osob je nutné provádět sluchovou a zvukovou kontrolu chování osob, a to vždy s intenzitou odpovídající povaze věci, že z hlediska práva není žádný rozdíl v tom, je-li takto sledován cestující na pohyblivých schodech v metru, nebo dítě ve výchovném ústavu, že ani v jednom případě takové sledování samo o sobě*

[33] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 4 odst. 2). [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679

nenarušuje ani jeho obydlí, ani soukromí[34]*, ani dobré jméno atd. a zejména neporušuje míru jeho svobody pohybu nebo jiného počínání: ta totiž zůstává vždy stejná, jako kdyby zde sledování vůbec nebylo, protože míra svobody počínání jedince v konkrétní situaci je věcí jen hmotného práva a nikoliv věcí intenzity kontroly.“*[35]

Kamery nesmějí sledovat prostory, kde lidé vykonávají ryze soukromé záležitosti, jako jsou toalety, koupelny, šatny a další místa, kde ani lidé neočekávají, že mohou být sledováni. Zároveň musí být o tom, že je snímaný prostor monitorován, náležitě informováni. Pokud není pořizován obrazový záznam, není ani nutný souhlas osob s monitorováním prostoru.[36]

„Nicméně kamerové systémy bez záznamu jsou v současné době spíše minoritní záležitostí, protože mají-li být účinné, vyžadují neustálou obsluhu sledující monitory, neumožňují využití pro zpětné prokázání událostí, které se v prostoru odehrály, cena záznamového zařízení je dnes již jen malou položkou v celkové ceně kamerového systému.“[37]

Kamerové systémy bez záznamu lze využít například v objektu, kde se nachází stálá služba, ostraha areálu či budovy. Systém jí tak umožňuje sledovat více míst současně a tím případně i redukovat počet pracovníků ostrahy.

3.3.1.2.3 Kamerové systémy se záznamem

Kamerové systémy, při jejichž využívání je pořizován záznam, naopak podléhají zvláštnímu způsobu regulace a posuzování a mají tak svá specifika. Oprávněnost zřídit a provozovat kamerový systém se záznamem je odvozována ze dvou základních hledisek. *„Pro orgány veřejné moci je takovým základem zákonné zmocnění, resp. oprávnění. Bez takového zmocnění by je totiž ani zřídit a provozovat nemohly. Na rozdíl od soukromých subjektů, které mohou činit vše, co není zákonem zakázáno.“*[38]

U kamerových systémů vybavených zařízením, které pořizuje záznam, se jedná o zpracování osobních údajů se vším, co tato skutečnost přináší. *„Provozování kamerového systému je tedy považováno za zpracování osobních údajů, pokud je vedle kamerového sledování prováděn záznam*

[34] Pojem soukromí zahrnuje jednak ochranu proti úniku informací o intimní sféře na veřejnost a jednak ochranu ve vztahu k veřejné kontrole státní moci.
[35] Vykls poř. č. 10/2003 Sb., k zákonnosti umístění audio-vizuálních prostředků ve školských zařízeních vykonávajících ústavní výchovu a ochrannou výchovu, Dostupné v systému ASPI. ID: LIT23204CZ.
[36] KUČEROVÁ, A., NOVÁKOVÁ, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D., Zákon o ochraně osobních údajů, str. 89 až 94
[37] Kamerová technika.cz: Kamerové systémy a zákony [online]. Brno: KamerováTechnika.cz, 2018 [cit. 2018-02-27]. Dostupné z: http://kamerovatechnika.cz/legislativa.html
[38] Stanovisko č. 1/2006 - Provozování kamerového systému z hlediska zákona o ochraně osobních údajů [online]. In: uoou.cz, Leden 2006 [cit. 2018-02-27]. Dostupné z: https://www.uoou.cz/files/stanovisko_2006_1.pdf

pořizovaných záběrů, nebo jsou v záznamovém zařízení uchovávány informace a zároveň účelem pořizovaných záznamů, případně vybraných informací, je jejich využití k identifikaci fyzických osob v souvislosti s určitým jednáním.“[39] V praxi se obvykle jedná o

a) zpracování nezbytné pro splnění úkolu prováděného při výkonu veřejné služby; v těchto případech je třeba dbát ustanovení příslušného právního předpisu nařizujícího, resp. upravujícího zvláštní podmínky kamerového sledování,
b) zpracování nezbytné pro účely oprávněných zájmů správce.[40]

Jak již bylo řečeno v kapitole 3.2.2, obrazové či zvukové údaje uchovávané v záznamovém zařízení, jsou osobními údaji za předpokladu, že na základě těchto záznamů lze přímo či nepřímo identifikovat konkrétní subjekt údajů.[41] „*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.“*[42] Identifikátory umožňující příslušnou osobu spojit s určitým jednáním, které je na snímku zachyceno, pak tvoří osobní údaj.

3.3.1.3 Náklady na fungování kamerových systémů

Cenu na pořízení kamerového systému lze rozdělit do několika položek

1) Dohledové pracoviště – jedná se o místnost pro umístění dohledového centra vybavená příslušným nábytkem, konektivitou, zabezpečením vstupu apod.
2) Pořízení serveru, dohledového pultu s monitory a záznamového zařízení pro připojení všech kamer
3) Kamerový bod – digitální kamera (pohyblivá, možnost Zoom či detekce obličeje, vysoké krytí IP65[43] pro venkovní instalaci), včetně instalace a napojení na centrální server
4) Záložní generátor elektrického proudu
5) Ostatní náklady – dodávka kabelových rozvodů, montáž zařízení, materiálová a rozpočtová rezerva, kamerové zkoušky před instalací, oživení, programování, připojení a konfigurace sítě LAN, doprava, inženýring

[39] BARTÍK, V., JANEČKOVÁ, E., Kamerové systémy v praxi, str. 19
[40] Stanovisko č. 1/2016 – K umístění kamerových systémů v bytových domech [online]. In: uoou.cz, Leden 2016 [cit. 2018-03-27]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=29566
[41] viz kapitola 3.2.2 této práce
[42] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ: K provozování kamerových systémů [online]. In: uoou.cz, 2018 [cit. 2018-10-25]. Dostupné z: https://www.uoou.cz/k-nbsp-provozovani-kamerovych-systemu/d-29535/p1=1099
[43] Stupeň krytí dle normy ČSN EN 60529 Stupně ochrany krytem, která u IP65 značí zcela prachotěsnou ochranu před cizími předměty a ochranu vůči tryskající vodě.

Vyčíslení jednotlivých položek naleznete v tabulce č. 1.[44]

Tabulka č. 1 - Cenová kalkulace pořízení kamerového systému

Položka		Cena celkem v Kč
Dohledové pracoviště		**150.000,-**
Pořízení serveru		**360.000,-**
	Server	*60.000,-*
	Dohledový pult s monitory	*200.000,-*
	Záznamové zařízení	*100.000,-*
Kamerový bod		**100.000 – 130.000,-**
Záložní generátor		**85.000,-**
Ostatní		**155.000,-**
	Dodávka kabelových rozvodů	*100.000,-*
	Montáž zařízení	*30.000,-*
	Materiálová a rozpočtová rezerva	*15.000,-*
	Kamerové zkoušky před instalací	*10.000,-*

Zdroj: vlastní zpracování na základě poskytnutých dat od Siemens, s.r.o

Jak je z tabulky č. 1 patrné, pořízení kamerového systému není vůbec levnou záležitostí. Pořízení kamerového systému nás vyjde zhruba na 1 – 1,5 milion korun českých. Navíc cena vzrůstá s počtem instalovaných kamer (kamerových bodů). Proto je vždy nutné myslet dopředu, kolik bude do budoucna v systému kamer, jinak kapacita základny nemusí stačit vzrůstajícímu počtu připojených kamerových bodů.

Co se týče samotné obsluhy kamerového systému, tyto systémy pracují převážně v autonomním provozu tzv. „patrol systému“[45], kde dozor probíhá v režimu občasné obsluhy. Náklady na zaměstnance, kteří tuto obsluhu zajišťují, činí ročně zhruba 150.000,- Kč.

[44] Přibližná cenová kalkulace pro kamerový systém (základna (dohledové pracoviště, pořízení serveru) + 10 kamerových bodů).
[45] Patrol systém neboli kontrola hlídkou, která je určena převážně pro objekty, kde není stálá ostraha, ani stálý provoz, se z ekonomických důvodů používají patroly hlídkou.

3.3.2 Závěr

Za kamerové sledování lze považovat využití dostupných technických prostředků ke snímání a generování obrazu, přenosu obrazu a zobrazení obrazu, případně obrazu společně i se zvukem (např. CCTV, tzv. fotopasti, webkamery apod.) (viz 3.3.1).

Základní rozdíl mezi IP digitálním a analogovým kamerovým systémem je v použité technologii výstupního videa. U klasických analogových kamer je výstup obrazu veden koaxiálním kabelem do záznamového zařízení (DVR) nebo monitoru, kdežto IP digitální kamery umožňují po připojení do počítačové sítě přenášet nejen obraz, ale i třeba obousměrný zvuk, na libovolné místo. IP kamery tak můžeme nejen sledovat odkudkoli ze světa, ale také je plnohodnotně nastavit a naprogramovat přes libovolný internetový prohlížeč. Zjevný rozdíl je také u výstupního obrazu, který je většinou u IP digitálních kamer detailnější, ostřejší a věrohodnější, jelikož mají několikanásobně větší rozlišení než kamery analogové. Z tohoto důvodu je také IP digitální kamerový systém nejvíce využíván především tam, kde jsou požadovány výborné rozlišovací schopnosti, příkladem může být snímání SPZ při vjezdu do areálu nebo identifikace osob. Naopak tam, kde není potřeba vysokého rozlišení, a kde celý systém má plnit spíše funkci přehledovou, například monitorování vstupu do budovy, je využíván kamerový systém analogový (viz 3.3.1.1).

Dále kamerové systémy rozlišujeme na kamerové systémy bez záznamu a se záznamem. Pokud se příslušná osoba rozhodne pro instalaci kamerového systému bez záznamu, nedopadají na ni ustanovení GDPR, navíc po administrativní stránce je jeho instalace jednodušší. Co však respektovat musí, je právo sledovaných osob na respektování soukromého a rodinného života. Zároveň osoby pohybující se v prostoru snímaném kamerami musí být o existenci kamerového systému informováni (viz 3.3.1.2.2).

Naopak kamerové systémy se záznamem jsou mj. podrobeny regulaci GDPR, jelikož provozování takového systému je považováno za zpracování osobních údajů. Podle GDPR se záznamy pořízené kamerami, ať obrazové, zvukové či kombinace těchto dvou, považují za osobní údaj, pokud lze na základě takto pořízeného záznamu identifikovat ať už přímo či nepřímo konkrétní osobu (viz 3.3.1.2.3). Za zpracování osobních údajů primárně odpovídá správce, který musí dodržovat určené povinnosti a musí být také schopen toto dodržení souladu doložit (viz 3.2.4).

Náklady na fungování kamerového systému jako takového vůbec nejsou levnou záležitostí. Samotné pořízení kamerového systému, jež zahrnuje zřízení dohledového pracoviště, pořízení serveru, kamery, záložní generátor a ostatní náklady spojené s instalací celého systému, vyjde více jak na 1 milion korun českých. Navíc nesmíme opomenout také na náklady na zaměstnance, kteří ať už pravidelně či občasně obsluhu kamerového systému zajišťují (viz 3.3.1.3).

3.4 Ochrana osobnosti a ochrana osobních údajů a zvláštních kategorií osobních údajů

3.4.1 Úvodem

Ochranu osobnosti na našem území upravuje především Ústava, Listina a OZ, naopak ochrana osobních údajů a ochrana zvláštních kategorií osobních údajů je již plně obsažena v novém nařízení GDPR.

3.4.2 Ochrana osobnosti

3.4.2.1 Vývoj ochrany osobnosti v občanském zákoníku

Pro české země měl velký význam císařský patent JGS Nr. 946/1811, který byl do československého práva přejat tzv. recepčním zákonem č. 11/1918 Sb., o zřízení samostatného státu československého. Tento císařský patent v české právní praxi označovaný jako OZO výslovnou právní úpravu osobnosti neobsahoval, ale je možné v něm nalézt několik ustanovení, která se ochrany osobnosti týkají. O osobnostních právech pojednává jeho díl prvý, např. v ustanovení § 16 OZO má každý člověk „*vrozená, již rozumem poznatelná práva, a nutno je tudíž považovati za osobu*“[46], a ustanovení § 43 OZO poskytuje výslovně ochranu pouze dílčímu osobnostnímu právu na jméno (příp. krycí jméno, tzv. pseudonym)[47]. OZO byl několikrát novelizován a na českém území platil až do 31. prosince 1950, kdy byl nahrazen zákonem č. 141/1950 Sb., občanský zákoník. Zákon č. 218/1926 Sb., o původském právu k dílům literárním, uměleckým a fotografickým (o právu autorském) obsahoval ochranu dílčího osobnostního práva k vlastní podobizně, práva k dopisům, deníkům a jiným písemnostem osobní povahy. I tento zákon 1. ledna 1954 nahradil zákon nový, a to zákon č. 115/1953 Sb., o právu autorském (autorský zákon).

Jak z výše uvedeného vyplývá, upravena byla pouze některá dílčí osobnostní práva, a to navíc v několika různých právních předpisech (např. právo na jméno upravoval občanský zákoník, právo na podobiznu a na osobní písemnosti upravoval autorský zákon). K ucelení právní úpravy ochrany osobnosti došlo až s novým občanským zákoníkem č. 40/1964 Sb., který poprvé ve svých ustanoveních (§ 11 až § 16) zakotvil obecnou úpravu všeobecného osobnostního práva, a v jeho rámci úpravu jednotlivých dílčích osobnostních práv včetně právních prostředků ochrany.[48]

[46] viz ust. § 16 Obecný zákoník občanský č. 946/1811 Sb. z. s., ve znění pozdějších předpisů
[47] viz ust. § 43 Obecný zákoník občanský č. 946/1811 Sb. z. s., ve znění pozdějších předpisů
[48] KNAP, K., ŠVESTKA, J., JEHLIČKA, O., PAVLÍK, P., PLECITÝ, V., Ochrana osobnosti, str. 53

Právní úprava ochrany osobnosti v občanském zákoníku z roku 1964 přetrvala až do roku 1989, kdy v souvislosti s celkovým přerodem společnosti a s dodržováním základních lidských práv nastala nová etapa ochrany osobnosti. *„Dosavadní občanský zákoník odpovídající potřebám administrativně direktivního systému se stal po roce 1989 do značné míry nepoužitelný.“*[49] Od čistě materialistické koncepce socialistického práva bylo v návaznosti na přijetí Ústavy a Listiny opuštěno a při výkladu právních norem byl kladen důraz na přirozená subjektivní práva člověka.[50] V rámci novelizace občanského zákoníku č. 40/1964 Sb., byl přijat zákon č. 87/1990 Sb., kterým se mění a doplňuje občanský zákoník - který rozšířil prostředky ochrany o *„právo na náhradu nemajetkové újmy v penězích“*[51], a zákon č. 509/1991 Sb., kterým se mění, doplňuje a upravuje občanský zákoník.[52] Občanskoprávní úpravu začaly doplňovat i další specifické právní úpravy (a to např. v oblasti zdravotnictví, v oblasti tisku a médií, v pracovní oblasti atd.), a mj. byl přijat zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

V roce 2012 došlo k přijetí OZ (nového občanského zákoníku č. 89/2012 Sb.), jehož *„zásady na kterých je vybudován, jsou v celku identické s těmi, na jejichž základě byla již v období po listopadu 1989 vykládána ochrana osobnosti.“*[53]

3.4.2.2 Ochrana osobnosti podle OZ

Jak již bylo výše zmíněno, z hlediska právní úpravy ochrany osobnosti nelze opomenout ani dva nejdůležitější předpisy, kterými jsou Ústava a Listina. V Ústavě se hned v Preambuli můžeme setkat s hodnotami jako *„lidská důstojnost“, „svoboda“, „úcta k lidským právům“* atd., které jsou dále rozpracovány v Listině, jenž je také součástí ústavního pořádku ČR.[54] Obě obsahují základní práva každého člověka. V rozporu s těmito dvěma nejvyššími právními předpisy tak nesmějí být žádné právní normy.

Dalším významným obecným předpisem je OZ, který rozvádí základní práva obsažená v Listině a v mezinárodních paktech a úmluvách o lidských právech. Základní zásady soukromého práva jsou zakotveny v § 3 odst. 2 OZ, kde je uvedeno, že každý má právo na ochranu svého života

[49] KADLECOVÁ M., SCHELLE, K., VESELÁ, R., VLČEK, E., Vývoj českého soukromého práva, edice právní dějiny
[50] MELZER, F., TÉGL, P., a kol., Občanský zákoník – velký komentář, str. 506
[51] viz ust. § 13 zákona č. 87/1990 Sb., kterým se mění a doplňuje zákon č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů
[52] KNAP, K., ŠVESTKA, J., JEHLIČKA, O., PAVLÍK, P., PLECITÝ, V., Ochrana osobnosti, str. 39
[53] ŠVESTKA, J., DVOŘÁK, J., FIALA, J., Občanský zákoník. Komentář. Svazek I., str. 310
[54] Preambule ústavního zákona č. 1/1993 Sb. ve znění ústavního zákona č. 347/1997 Sb., 300/2000 Sb., 448/2001 Sb., 395/2001 Sb., 515/2002 Sb., 319/2009 Sb., 71/2012 Sb. a 98/2013 Sb.

a zdraví, jakož i svobody, cti, důstojnosti a soukromí.[55] *„Je zcela jasně patrné, že tato východiska jsou neodlučitelně spjata s fenoménem osobnosti člověka.“*[56] Právo na ochranu osobnosti je ovšem zaručeno již na ústavní úrovni, tudíž se naskytuje otázka, zda jeho ukotvení v OZ již není zbytečné. Tuto úvahu by umocňoval i fakt a jak je výše zmíněno, žádná právní norma nesmí být v rozporu s Ústavou a Listinou. Tato osobnostní práva jsou pro zákonodárce ovšem tak důležitá, že je OZ znovu opakuje a dále rozvádí. Navíc Ústava nemůže dopodrobna rozvádět všechna práva - k tomu jsou určeny další právní předpisy, jako např. níže zmíněný OZ.

Podle ustanovení § 81 odst. 1 OZ je osobnost člověka chráněna včetně všech jeho přirozených práv a každý je povinen ctít svobodné rozhodnutí člověka žít podle svého.[57] Demonstrativní výčet[58] některých chráněných hodnot osobnosti člověka pak připojuje ustanovení § 81 odst. 2 OZ.[59] Člověk, jehož osobnost byla dotčena, má právo se podle ustanovení § 82 odst. 1 OZ domáhat toho, aby mu bylo od neoprávněného zásahu upuštěno anebo aby byl odstraněn jeho následek.[60] Je-li předpokladem vzniku sankce za porušení existence konkrétního zásahu do osobnosti člověka, musí být tento zásah shledán buď jako neoprávněný (tj. v rozporu s objektivním právem), anebo jako oprávněný (v tomto případě z hlediska práva na ochranu osobnosti nesankcionovaný).[61] *„Přitom bude nutno ověřovat, zda dotčený člověk k zásahu do své osobnosti případně nesvolil, nebo zda takový zásah výslovně dovoluje zákon, resp. zda k zásahu došlo výkonem subjektivního práva, případně při plnění zákonem uložené právní povinnosti.“*[62]

Jako jedna z významných hodnot osobnosti člověka je uváděno právo na podobu.[63] To lze, jako jednu z definičních a identifikačních složek jeho osobnosti podle ustanovení § 84 OZ, zachytit jakýmkoliv způsobem tak, aby podle zobrazení bylo možné určit její totožnost, pouze s jeho svolením[64].[65] *„Zachycení podoby člověka technickými prostředky i jen v latentní formě může značně znesnadňovat naplňování § 84, a to především u zachycení podoby člověka, k níž došlo necíleným*

[55] viz ust. § 3 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
[56] ŠVESTKA, J., DVOŘÁK, J., FIALA, J., Občanský zákoník. Komentář. Svazek I., str. 307
[57] viz ust. § 81 odst. 1 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
[58] Právo člověka na život, na zdraví a na právo žít v příznivém životním prostředí, dále právo na důstojnost člověka, jeho vážnost a čest, právo na soukromí a právo na ochranu jeho projevů osobní povahy.
[59] viz ust. § 81 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
[60] viz ust. § 82 odst. 1 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
[61] ŠVESTKA, J., DVOŘÁK, J., FIALA, J., Občanský zákoník. Komentář. Svazek I., str. 317
[62] ŠVESTKA, J., DVOŘÁK, J., FIALA, J., Občanský zákoník. Komentář. Svazek I., str. 317
[63] Obsahem práva na podobu se rozumí užívací a dispoziční právo subjektu ve vtahu k zachycení jeho podoby.
[64] viz ust. § 84 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
[65] Protože zachycení podoby člověka bývá často spjato s jejím následným rozšiřováním, bývá mnohdy souhlas se zachycením podoby člověka a souhlas s jejím šířením udělován současně.

způsobem.“[66] Z toho je patrné, že § 84 OZ má význam především v souvislosti s úpravou práva k podobizně[67], resp. k obrazovému snímku, případně k obrazovému záznamu.[68]

Čl. 7 odst. 1 Listiny stanovuje, že je zaručena nedotknutelnost osoby a jejího soukromí a že může být omezena jen v případech stanoveným zákonem.[69] *„Této zásadě odpovídá § 86, který uvádí, že nikdo nesmí zasáhnout do soukromí jiného, nemá-li k tomu zákonný důvod. Tímto zákonným důvodem bude především příslušné svolení udělené člověkem. Přitom ani takové svolení nemůže umožňovat zásah, který by byl v rozporu s oprávněnými zájmy člověka na ochranu jeho osobnosti (§ 90).“*[70]

„Právo na soukromí člověka bývá definováno jako právo rozhodnout podle vlastního uvážení, zda, v jakém rozsahu a jakým způsobem mají být skutečnosti jeho osobního soukromí zpřístupněny jiným, a zároveň se bránit proti neoprávněným zásahům do této sféry ze strany jiných osob.“[71] Bez svolení člověka nelze narušit jeho soukromé prostory, sledovat jeho soukromý život, pořizovat o jeho soukromém životě zvukový nebo obrazový záznam, využívat takové či jiné záznamy pořízené o soukromém životě člověka třetí osobou, a takové záznamy o jeho soukromém životě šířit.[72] *„Ve stejném rozsahu, jako tomu je u soukromých prostor člověka, u sledování jeho soukromého života nebo u pořizování zvukových nebo obrazových záznamů, jsou při jejich využívání třetí osobou nebo v případě možnosti takové záznamy o jeho soukromém životě šířit chráněny i jeho soukromé písemnosti osobní povahy*[73]*.“*[74]

Podle § 87 odst. 1 OZ může člověk, který svolil k použití písemnosti osobní povahy, podobizny nebo zvukového či obrazového záznamu jeho se týkajícího nebo jeho projevů osobní povahy, své svolení odvolat.[75]

---

[66] ŠVESTKA, J., DVOŘÁK, J., FIALA, J., Občanský zákoník. Komentář. Svazek I., str. 325
[67] Právo k podobizně je právo, jehož předmětem je podobizna, tj. hmotné zachycení podoby člověka. Obsahem práva k podobizně a k obrazovému snímku je užívací a dispoziční právo subjektu ve vztahu k podobizně. Právo na podobu vzniká již narozením člověka, naopak právo k podobizně teprve okamžikem, kdy je podoba zachycená na podobizně již individualizovatelná.
[68] ŠVESTKA, J., DVOŘÁK, J., FIALA, J., Občanský zákoník. Komentář. Svazek I., str. 326
[69] viz čl. 7 odst. 1 ústavního zákona č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů
[70] ŠVESTKA, J., DVOŘÁK, J., FIALA, J., Občanský zákoník. Komentář. Svazek I., str. 328
[71] ŠVESTKA, J., DVOŘÁK, J., FIALA, J., Občanský zákoník. Komentář. Svazek I., str. 328
[72] ŠVESTKA, J., DVOŘÁK, J., FIALA, J., Občanský zákoník. Komentář. Svazek I., str. 328
[73] Obsahem tohoto práva je dispoziční právo člověka k chráněnému statku. Zároveň jsou upraveny i předpoklady zákonné licence k jeho užití a současně i vymezení jejích limitů.
[74] ŠVESTKA, J., DVOŘÁK, J., FIALA, J., Občanský zákoník. Komentář. Svazek I., str. 329
[75] viz § 84 odst. 1 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů

Jak již bylo řečeno, ochrana osobnosti člověka je zakotvena i v tzv. mezinárodních paktech a úmluvách, zejména v evropských zemích se ochranou osobních údajů zabývá Úmluva o ochraně osob se zřetelem na automatizované zpracování dat (tzv. Úmluva č. 108).[76]

3.4.3 Ochrana osobních údajů a ochrana zvláštních kategorií osobních údajů

3.4.3.1 Historie ochrany osobních údajů z hlediska GDPR

Prvním větším milníkem byl rok 1981, kdy došlo k podpisu smlouvy o ochraně osob s ohledem na automatické zpracování osobních údajů.[77] Roku 1995 vstoupila v platnost Evropská směrnice o ochraně osobních údajů známá jako Směrnice 95/46/ES. Tato směrnice byla vytvořena jako základní prvek ochrany soukromí v rámci EU a práva v oblasti lidských práv. *„Směrnice o ochraně osobních údajů existuje již dvacet let. Stanovuje minimální standard zákona o ochraně údajů v členských státech EU. Česká Republika v roce 2000 přijala vlastní zákon týkající se ochrany osobních údajů.“*[78] V roce 2009 pak Evropská komise zahájila konferenci věnovanou využití a ochraně osobních údajů a zkoumání nových úkolů týkajících se ochrany soukromí. Na základě této konference byl zveřejněn dokument *„Budoucnost soukromí“*, který zdůrazňoval, *„že úroveň ochrany osobních údajů v rámci EU lze zvýšit lepším uplatňováním stávajících zásad a legislativy v oblasti ochrany osobních údajů v praxi a postupnou modernizací právního rámce.“*[79] V následujících letech pak Evropská komise stanovila strategii, jak chránit údaje jednotlivců ve všech oblastech (včetně vymáhání práv), přijala návrh komplexnějšího přístupu k ochraně osobních údajů a na začátku roku 2012 navrhla komplexní reformu pravidel EU ochrany osobních údajů za účelem posílení práv, zejména v online prostředí. Jelikož každý členský stát EU upravoval ve svých národních právních předpisech ochranu osobních údajů jinak, a úprava byla minimální, chtěla Evropská komise zavést takové nařízení, které by bylo přímo aplikovatelné ve všech členských státech EU a národním právním předpisům nadřazené. Zhruba po třech letech došlo v květnu 2015 k zahájení tzv. *„trialogu“*[80], jehož cílem bylo uzavření dohody o GDPR. V roce 2016 Evropská unie přijala GDPR, které je platné ve všech 28 členských státech a Islandu, Norsku a

[76] Úmluva Rady Evropy č. 108 ze dne 28. ledna 1981 o ochraně osob se zřetelem na automatizované zpracování osobních dat, vyhlášená pod č. 115/2001 Sb. m. s., která pro ČR nabyla účinnosti dne 1. listopadu 2001, a kterou doplňuje dodatkový protokol Rady Evropy z 8. listopadu 2001 č. 181 k úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat o orgánech dozoru a toku dat přes hranice, vyhlášený pod č. 29/2005 Sb. m. s., který pro ČR nabyl účinnosti dne 1. července 2004.
[77] Byla podepsána jako Úmluva Rady Evropy č. 108.
[78] NEZMAR, L., GDPR: Praktický průvodce implementací, str. 14
[79] NEZMAR, L., GDPR: Praktický průvodce implementací, str. 15
[80] Původně dialogická diskuse, do níž se zapojuje třetí neutrální osoba, která se snaží usnadnit dohodu mezi účastníky jednání či konfliktu.

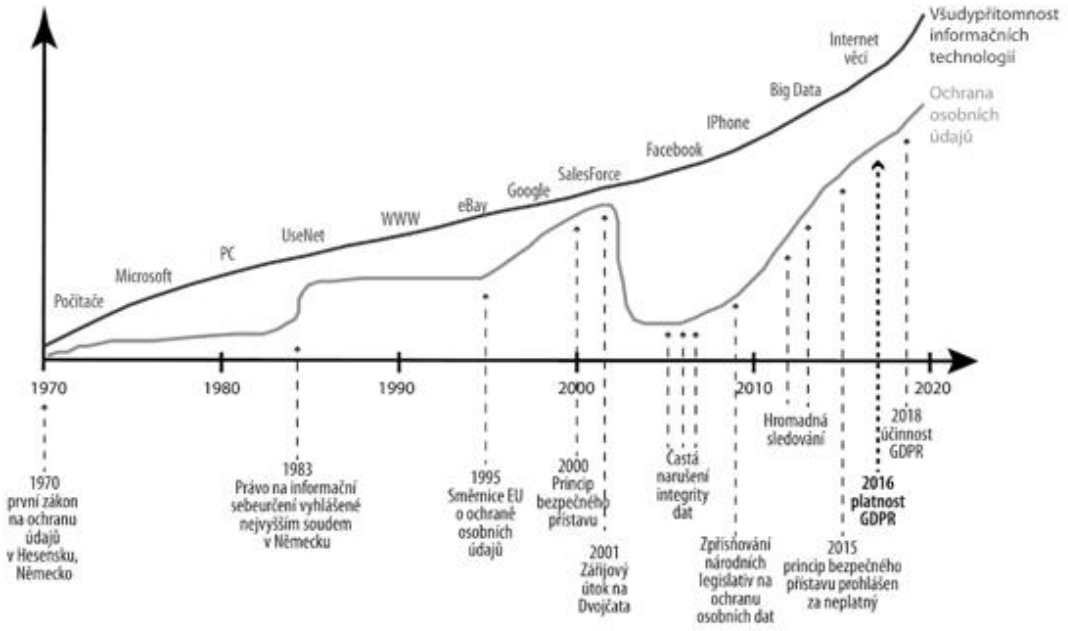
Lichtenštejnsku. V účinnost GDPR vstoupilo 25. května 2018[81] a nahradilo tak v českém právním prostředí ZoOU (respektive jeho podstatou část). V souvislosti s nutností adaptovat český právní řád na GDPR vyvstala nutnost *„upravit některé dílčí aspekty nezbytné k dotvoření celého rámce ochrany osobních údajů na zákonné úrovni.“*[82] GDPR totiž umožňuje, aby se členský stát v jím definovaných případech od jeho úpravy odchýlil, a zároveň stanovuje, že některé aspekty mají být ve vnitrostátním právu členského státu upraveny. ZoOU tak bude zcela zrušen až s účinností adaptačního zákona. GDPR je v současné době nejkomplexnějším nařízením chránící soukromí občanů.

3.4.3.2 Důvody pro přijetí GDPR

„Za potřebou aktualizace stojí zejména technologický a společenský vývoj.“[83] GDPR vychází z původní Směrnice 95/46/ES[84], která začala platit v roce 1995, kdy neexistovaly různé sociální sítě, cloudová úložiště a ani řada dalších technologií. Vývoj technologií je vždy rychlejší než vývoj právních norem, což dokazuje i obr. č. 2. Důležitá je však reakční doba právního systému na technologické změny. Přestože GDPR začalo platit až od tohoto roku, již nyní se ví, že za technologickým pokrokem zaostává minimálně o pět let, a tudíž nepočítá s některými problémy.[85] Automatizované zpracování dat v budoucnosti bylo zohledněno pouze v Úmluvě Rady Evropy č. 108.

[81] NEZMAR, L., GDPR: Praktický průvodce implementací, str. 14 až 18
[82] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ: Základní příručka k GDPR [online]. In: uoou.cz [cit. 2018-10-12]. Dostupná z: https://www.uoou.cz/zakladni%2Dprirucka%2Dk%2Dgdpr/ds-4744/p1=4744
[83] POMAIZLOVÁ, K., FÜRSTOVÁ, M., GDPR – revoluce, nebo rozvedení stávajícího? [online]. In: Bulletin advokacie, str. 16 [cit. 2018-10-12]. Dostupné z: http://www.bulletin-advokacie.cz/assets/zdroje/casopis/2016/BA_9_2017_web.pdf
[84] Viz recitál 9 GDPR *„Ačkoliv cíle a zásady směrnice 95/46/ES nadále platí, nezabránilo to roztříštěnosti v provádění ochrany údajů v celé Unii, právní nejistotě ani rozšířenému pocitu veřejnosti, že v souvislosti s ochranou fyzických osob existují značná rizika, zejména pokud jde o činnosti prováděné online.“*
[85] Jimiž jsou internet věcí (IoT), big data analýz či BYOD, což je praxe, kdy si zaměstnanci nosí do práce vlastní počítač nebo mobil.

Obrázek č. 2 - Vývoj technologií v porovnání s vývojem legislativy



Zdroj: NEZMAR, L., GDPR: Praktický průvodce implementací, str. 15

„*Dalším důvodem pro přijetí nového nařízení byla zjištění, že tajné služby některých států mimo evropský prostor v minulosti hojně shromažďovaly údaje o občanech EU. S ohledem na rozdíly vnímání osobní svobody a odpovědnosti jednotlivce mezi Evropou a jinými státy tak bylo nutné stanovit jasná pravidla ochrany našich práv.*“[86] GDPR jakožto nový právní rámec ochrany osobních údajů má za cíl co nejvíce hájit práva občanů EU proti neoprávněnému zacházení s jejich daty. Charakteristická pro GDPR je i jeho univerzální použitelnost ve všech státech EU (a Islandu, Norsku a Lichtenštejnsku), jejímž výsledkem je sjednocení právní úpravy. Tudíž jednotná pravidla pro zpracování osobních údajů platí ve všech státech EU včetně třech vyjmenovaných v předchozí větě.[87]

Forma směrnice[88] pro právní úpravu ochrany osobních údajů na evropské úrovni se z pohledu dnešních zkušeností jevila jako nešťastná volba, proto byla pro novou právní úpravu GDPR zvolena forma nařízení, jelikož *„dává v něm obsaženým pravidlům celounijní platnost.*

[86] ŠKORNIČKOVÁ, E., Proč potřebuje Evropa lepší ochranu osobních dat [online]. In: gdpr.cz [cit. 2018-11-02]. Dostupné z: https://www.gdpr.cz/gdpr/proc/
[87] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ: Základní příručka k GDPR [online]. In: uoou.cz [cit. 2018-10-12]. Dostupná z: https://www.uoou.cz/zakladni%2Dprirucka%2Dk%2Dgdpr/ds-4744/p1=4744
[88] Směrnice je legislativní akt EU, který členským státům určuje, aby dosáhly konkrétního cíle, aniž by diktovala, jakými prostředky daného cíle dosáhnout. Směrnice obvykle poskytují prostor členským státům pro to, aby přijala daná pravidla podle svého právního řádu.

Přímá použitelnost či lépe řečeno účinnost a také závaznost GDPR ve všech členských státech EU bez nutnosti ho do jednotlivých národních právních řádů transponovat si klade za cíl právní úpravu sjednotit a nastolit nové podmínky pro všechny společnosti, které působí v rámci EU.“[89]

3.4.3.3 Základní zásady ochrany osobních údajů

Jak v OZ tak v GDPR byly převzaty z ústavních principů základní zásady, které jsou v obou předpisech společné. Propojenost mezi oběma právními předpisy lze nalézt mj. především v zásadě zákonnosti zpracování[90].

GDPR a OZ se shodují hned v hlavním požadavku pro zákonné zpracování, kterým podle GDPR je splnění nejméně jedné z podmínek v něm uvedených, neboli podle OZ jinak řečeno *„nikdo nesmí zasáhnout do soukromí jiného, nemá-li k tomu, zákonný důvod.“*[91]

Dalším příkladem je souhlas subjektu údajů se zpracováním svých osobních údajů[92], kterému v OZ odpovídá § 84, který uvádí že *„zachytit jakýmkoliv způsobem podobu člověka, je možné jen s jeho svolením“*[93], a dále podle § 85 je možné jen s jeho svolením podobu rozšiřovat.[94]

Zpracování, které je *„nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby“*[95], se prolíná s § 88 odst. 1 OZ, který uvádí, že *„svolení není třeba, pokud se podobizna nebo zvukový či obrazový záznam pořídí nebo použijí k výkonu nebo ochraně jiných práv nebo právem chráněných zájmů jiných osob.“*[96] Zároveň podle § 88 odst. 2 OZ není třeba svolení, pořídí se nebo použijí se podobizna nebo obrazový či zvukový záznam *„na základě zákona k úřednímu účelu nebo v případě, že někdo veřejně vystoupí v záležitosti veřejného zájmu.“*[97]

[89] POMAIZLOVÁ, K., FÜRSTOVÁ, M., GDPR – revoluce, nebo rozvedení stávajícího? [online]. In: Bulletin advokacie, str. 16 [cit. 2018-10-12]. Dostupné z: http://www.bulletin-advokacie.cz/assets/zdroje/casopis/2016/BA_9_2017_web.pdf
[90] viz kapitola 3.2.5 této práce
[91] viz ust. § 86 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
[92] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 6 odst. 1 písm. a). [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679
[93] viz ust. § 84 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
[94] viz ust. § 85 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
[95] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 6 odst. 1 písm. d). [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679
[96] viz ust. § 88 odst. 1 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
[97] viz ust. § 88 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů

Zde dochází opět k propojení s GDPR, které také povoluje zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci.[98]

A v neposlední řadě příklad zpracování, které je *„nezbytné pro účely oprávněných zájmů správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů“*[99], v zásadě upravuje i § 90 OZ, podle kterého zákonný důvod zásahu nesmí být využit nepřiměřeným způsobem v rozporu s oprávněnými zájmy člověk.[100]

Lze tedy říci, že základní zásady a principy obsažené v OZ, GDPR převzalo a detailněji je rozpracovává a zpřesňuje - představují tak nástavbu spočívající v dodatečných nových povinnostech. GDPR je založeno na dvou (nových) přístupech, a to

- na principu odpovědnosti správce za dodržení zásad zpracování[101]
- na principu rizika

„Principem rizika se myslí to, že správce od samého počátku zpracování osobních údajů musí brát v úvahu rozsah, kontext, povahu a účel zpracování a zároveň průběžně přihlížet k možným rizikům.“[102] Ke všem těmto okolnostem musí být přizpůsobeno zabezpečení osobních údajů.

Zásady a pravidla ochrany subjektů údajů v souvislosti se zpracováním jejich osobních údajů by měla respektovat jejich základní práva a svobody, zejména právo na ochranu osobních údajů.[103]

Podle ustanovení čl. 5 GDPR jsou základními zásadami zpracování osobních údajů

- zákonnost,[104]
- korektnost a transparentnost,[105]

[98] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 6 odst. 1 písm. e). [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679

[99] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 6 odst. 1 písm. f). [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679

[100] viz ust. § 90 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů

[101] Včetně schopnosti toto dodržení souladu doložit, např. prostřednictvím kodexu, osvědčení, certifikace nebo vedení záznamů o činnostech zpracování.

[102] POMAIZLOVÁ, K., FÜRSTOVÁ, M., GDPR – revoluce, nebo rozvedení stávajícího? [online]. In: Bulletin advokacie, str. 17 [cit. 2018-10-12]. Dostupné z: http://www.bulletin-advokacie.cz/assets/zdroje/casopis/2016/BA_9_2017_web.pdf

[103] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Recitál 2. [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679

[104] Požadavek na zákonnost je podrobněji rozveden v čl. 6 GDPR a v kapitole 3.2.5 této práce.

[105] Základem pro zpracování osobních údajů musí být min. jeden právní důvod a transparentnost.

- účelové omezení,[106]
- minimalizace údajů,[107]
- přesnost,[108]
- omezení uložení,[109]
- integrita a důvěrnost,[110]
- odpovědnost správce.[111]

Všechny výše zmíněné zásady až na poslední uvedenou byly obsaženy také v ustanoveních Směrnice 95/46/ES[112] a především rovněž v ZoOU.[113]

3.4.3.4 Souhlas se zpracováním osobních údajů

Souhlas subjektu údajů byl podle úpravy ZoOU jednou se základních zásad zpracování osobních údajů, *„a to proto, že zpracováním osobních údajů dochází k zásahu do soukromí jejich nositele.“*[114] GDPR základní parametry souhlasu nemění, ale rozšiřuje požadavky. Ovšem podstatným rozdílem je *„že zatímco podle zákona o ochraně osobních údajů byl souhlas prvotním základem pro zpracování osobních údajů a až posléze byly stanoveny výjimky, kdy mohly údaje být zpracovány bez souhlasu, Nařízení výlučné postavení souhlasu nezná a staví jej na stejnou úroveň jako jiné důvody pro zpracování osobních údajů.“*[115] Jelikož zpracování na základě souhlasu je jedním z nejkomplikovanějších důvodů vzhledem k jeho odvolatelnosti, GDPR doporučuje nejprve hledat a zvážit některý z jiných zákonných důvodů uvedených v kapitole 3.2.5, a až v případě, že žádný není, žádat souhlas.

---

[106] Viz čl. 5 odst. 1 písm. b) GDPR, který stanovuje, že osobní údaje musí být *„shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný.“*
[107] Viz čl. 5 odst. 1 písm. c) GDPR, který stanovuje, že osobní údaje musí být „*přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány.“*
[108] Viz čl. 5 odst. 1 písm. d) GDPR, který kromě požadavku na přesnost, zmiňuje osobní údaje, které *„v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny.“*
[109] Viz čl. 5 odst. 1 písm. e) GDPR stanovující požadavek na uložení osobních údajů pouze na dobu nezbytně nutnou pro účely zpracování.
[110] Viz čl. 5 odst. 1 písm. f) GDPR, který povoluje zpracování osobních údajů pouze „*způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením.“*
[111] Viz čl. 5 odst. 2 GDPR, který správci osobních údajů stanovuje odpovědnost za dodržování zásad zpracování, které musí být schopen doložit.
[112] Zejména v čl. 6 Směrnice 95/46/ES.
[113] viz ust. § 5 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů
[114] JANEČKOVÁ, E., GDPR. Praktická příručka implementace, str. 12
[115] JANEČKOVÁ, E., GDPR. Praktická příručka implementace, str. 12

Čl. 4 odst. 11 GDPR definuje souhlas jako *„svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů.“*[116] Recitál 32 GDPR rozšiřuje tuto definici, a říká, že souhlas by měl být dán jednoznačným potvrzením, které je vyjádřením výše zmíněného, a to v podobě písemného prohlášení, i účinného elektronicky, nebo ústního prohlášení.[117]

„Nařízení zároveň upozorňuje na známou poučku, že mlčení neznamená souhlas.“[118] Souhlas by se měl vztahovat na veškeré činnosti zpracování osobních údajů pro stejný nebo stejné účely, tudíž jestliže má zpracování více účelů, měl by být udělen pro všechny.

GDPR také odstraňuje v ČR velmi rozšířený nešvar, a to, že souhlas je jednostranným právním úkonem, ale bývá součástí dvoustranných právních aktů, nejčastěji smluv. GDPR totiž požaduje, aby *„pokud je souhlas subjektu údajů vyjádřen písmenným prohlášením, které se týká rovněž jiných skutečností, byla žádost o vyjádření souhlasu předložena způsobem, který je od těchto jiných skutečností jasně odlišitelný a je srozumitelný a snadno přístupný za použití jasných a jednoduchých jazykových prostředků.“*[119]

Podle čl. 7 odst. 3 GDPR je také výslovně stanovena odvolatelnost souhlasu se zpracováním osobních údajů.[120] V praxi to znamená, že *„všechny operace zpracování dat, které byly založeny na tomto souhlasu a probíhaly před jeho odvoláním, zůstávají zákonné, ale správce musí zastavit dotčené zpracovatelské činnosti. Neexistuje-li jiný právní důvod opravňující ke zpracování dat, měl by je správce smazat nebo anonymizovat.“*[121]

Probíhá-li zpracování osobních údajů založené na souhlasu podle ZoOU, není nutné, aby subjekt údajů svůj souhlas udělil znovu, způsob udělení souhlasu musí být ovšem v souladu s GDPR.

---

[116] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 4 odst. 11). [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679

[117] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Recitál 32. [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679

[118] JANEČKOVÁ, E., GDPR. Praktická příručka implementace, str. 14

[119] JANEČKOVÁ, E., GDPR. Praktická příručka implementace, str. 14

[120] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 7 odst. 3. [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679

[121] JANEČKOVÁ, E., GDPR. Praktická příručka implementace, str. 14

3.4.3.5 Práva a povinnosti při zpracování osobních údajů

3.4.3.5.1 Úvodem

Jak z kapitoly 3.4.3.3 vyplývá, práva a povinnosti přímo vyplývající z GDPR, nahradily práva a povinnosti obsažené ve Směrnici 95/46/ES a zároveň i v ZoOU. Správcům a zpracovatelům jsou při ochraně osobních údajů ukládány především povinnosti, zatímco subjektům údajů jsou dána práva.

3.4.3.5.2 Povinnosti při zpracování osobních údajů

GDPR stanovuje povinnosti správce poněkud obecněji. V podstatě se jedná o zásady zpracování osobních údajů[122] a pak jednu hlavní povinnost správce, a to zpracovávat osobní údaje v souladu s těmito zásadami.[123]

Jak již bylo řečeno, jakékoliv zpracování osobních údajů by mělo být prováděno zákonným a transparentním způsobem. Základním předpokladem při zpracování osobních údajů je zásada zákonnosti. Ta stanovuje, že *„zpracování se vždy děje za určitým účelem a právní důvod musí daný účel pokrývat. Účel zpracování tak ovlivňuje právní důvod zpracování. Nelze tedy stanovit nelegitimní účel.“*[124] Za transparentní způsob zpracování osobních údajů je možné považovat otevřené zpracování osobních údajů, bez zatajování důvodů, proč je potřeba osobní údaje zpracovávat, a také plnění informační povinnosti vůči subjektům údajů.[125] S transparentností se také úzce pojí princip odpovědnosti[126], jelikož *„transparentnost má vést k uvědomění si, že zpracování osobních údajů může zasáhnout a více či méně zasahuje do života fyzických osob a v důsledku nedostatečné ochrany může mít na tyto osoby (negativní) dopad.“*[127]

[122] viz kapitola 3.4.3.3 této práce
[123] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 5 odst. 2. [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679
[124] ŽŮREK, Jiří. Praktický průvodce GDPR, str. 67
[125] POMAIZLOVÁ, K., FÜRSTOVÁ, M., GDPR – revoluce, nebo rozvedení stávajícího? [online]. In: Bulletin advokacie, str. 18 [cit. 2018-10-12]. Dostupné z: http://www.bulletin-advokacie.cz/assets/zdroje/casopis/2016/BA_9_2017_web.pdf
[126] Obsahem odpovědnosti správce je povinnost zavedení, revidování a případné aktualizování vhodných technických a organizačních opatření, aby správce osobních údajů zajistil a také byl schopen doložit zpracování osobních údajů v souladu s GDPR.
[127] POMAIZLOVÁ, K., FÜRSTOVÁ, M., GDPR – revoluce, nebo rozvedení stávajícího? [online]. In: Bulletin advokacie, str. 18 [cit. 2018-10-12]. Dostupné z: http://www.bulletin-advokacie.cz/assets/zdroje/casopis/2016/BA_9_2017_web.pdf

Povinností správce je tedy zajistit, aby subjektu údajů poskytl stručným, transparentním, srozumitelným a snadno přístupným způsobem[128], veškeré potřebné informace o zpracování jeho osobních údajů[129], jako je identifikace správce a jeho případného zástupce, účel a právní základ zpracování[130], příjemce osobních údajů[131], úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci a případně také informace o době uložení osobních údajů, o právu na přístup k osobním údajům, možnost podat stížnost u dozorového orgánu, možnost odvolat udělený souhlas, o právu na opravu, omezení zpracování či výmaz atd. Poskytuje-li osobní informace přímo subjekt údajů, správce jej s příslušnými informacemi obeznámí v okamžiku získání osobních údajů.

Mezi nové povinnosti stanovené GDPR patří vedení záznamů o činnostech, rozsah poskytovaných informací a neméně důležitá oznamovací povinnost při úniku dat.

3.4.3.5.2.1 Vedení záznamů o činnostech

Povinnost vést záznamy o činnostech částečně nahrazuje zrušenou registrační povinnost[132]. Jedná se v podstatě o podrobný popis zpracování osobních údajů, který umožní správci, ale i dozorovému úřadu získat dokonalý přehled. Záznamy musí být vyhotoveny písemně a na požádání je správce povinen záznamy příslušnému dozorovému úřadu poskytnout. Přesný obsah těchto záznamů nařizuje GDPR[133].

[128] Za použití jasných a jednoduchých jazykových prostředků.
[129] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 12. [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679
[130] Včetně oprávněných zájmů správce viz čl. 6 odst. 1 písm. f) GDPR.
[131] Podle ust. čl. 4 GDPR se příjemcem osobních údajů rozumí *„fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoliv.“*
[132] viz ust. § 16 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů
[133] V čl. 30 odst. 1 GDPR stanovuje, že tyto záznamy musí obsahovat *„jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů; účely zpracování; popis kategorií subjektů údajů a kategorií osobních údajů; kategorie příjemců, kterým bylo nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích; informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace; je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů; je-li to možné, obecný popis technických a organizačních bezpečnostních opatření.“*

Protože ne všichni správcové jsou schopni vést tuto agendu, mohou ji přenést na zpracovatele[134]. *„Vést záznamy o činnostech zpracování nedoléhá na podnik nebo organizaci zaměstnávající méně než 250 osob, ledaže zpracování, které provádí, pravděpodobně představuje riziko pro práva a svobody subjektů údajů, zpracování není příležitostné, nebo zahrnuje zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech.“*[135]

3.4.3.5.2.2 Povinnost zabezpečení a hlášení bezpečnostních incidentů

Další povinností je mj. i povinnost zabezpečit zpracování osobních údajů, které je již obsaženo v základních zásadách.[136] Týkají se jí především zásada integrity a důvěrnosti a zásada odpovědnosti. Podle čl. 32 odst. 1 GDPR má správce povinnost zavést s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob vhodná technická a organizační opatření[137], aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s GDPR. *„Aby správce mohl doložit soulad s tímto nařízením, měl by přijmout vnitřní koncepce a zavést opatření, která dodržují zejména zásady záměrné a standardní ochrany osobních údajů.“*[138] Tato opatření by mohla spočívat např. v minimalizaci zpracování osobních údajů, pseudonymizaci[139] osobních údajů, transparentnosti, příp. subjektům údajů umožnit monitorovat zpracování osobních údajů a správcům umožnit vytvářet a zlepšovat bezpečnostní prvky.

[134] Podle ust. čl. 4 GDPR je zpracovatelem „*fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.“*
[135] ŠKORNIČKOVÁ, E., Záznamy o činnostech zpracování [online]. In: gdpr.cz [cit. 2018-11-01]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/zaznamy-o-cinnostech-zpracovani/
[136] viz kapitola 3.4.3.3 této práce
[137] Tyto opatření mají zajistit nejen bezpečnost zpracování a samotných údajů, ale také dodržování dalších povinností, jako je například minimalizace osobních údajů.
[138] JANEČKOVÁ, E., GDPR. Praktická příručka implementace, str. 30
[139] Pseudonymizací se podle ust. čl. 4 GDPR rozumí *“zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě.“* Příkladem pseudonymizace jsou například údaje kódované pomocí klíče.

Správce nebo zpracovatel by měli také v zájmu zachování bezpečnosti posoudit rizika spojená se zpracováním osobních údajů[140] a přijmout tak opatření ke zmírnění těchto rizik, např. šifrováním.[141] GDPR však neukládá povinnost použít pro zabezpečení zpracování některých specifických opatření. Šifrování je uvedeno jako jedno z vhodných opatření.

Za porušení zabezpečení osobních údajů podle GDPR (stejně tak tomu bylo i v ZoOU) lze považovat náhodné nebo protiprávní zničení, ztrátu, změnu nebo neoprávněné poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů. *„Porušením zabezpečení je tedy jak jednání nahodilé, tak úmyslné.“*[142] Porušení lze rozdělit do tří kategorií

- porušení důvěrnosti[143]
- porušení dostupnosti[144]
- porušení integrity[145]

Nově je formulována povinnost ohlašovat případy porušení zabezpečení osobních údajů.[146] První povinnost při vzniku bezpečnostního incidentu vzniká směrem k Úřadu pro ochranu osobních údajů (dále jen „ÚOOÚ“) jakožto dozorovému úřadu. Správce musí bez zbytečného odkladu (pokud možno do 72 hodin od okamžiku, kdy se o porušení zabezpečení dozvěděl) jakékoliv porušení zabezpečení osobních údajů ohlásit příslušenému dozorovému úřadu, „*ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko a práva a svobody fyzických osob.*“[147] V této souvislosti půjde nepochybně o možný únik dat ze systému nebo nějaké jiné vážné porušení zásady zabezpečení dat.

Vzhledem k tomu, že GDPR v mnoha ohledech kopíruje Směrnici 95/46/ES a ZoOU, povinnost zabezpečit osobní údaje není zas až takovou novinkou, pouze GDPR stanovuje tuto povinnost šířeji a precizněji, a od správce vyžaduje mnohem větší aktivitu.

---

[140] Mezi rizika zpracování osobních údajů podle recitálu 83 GDPR lze zařadit *„náhodné nebo protiprávní zničení, ztrát, pozměnění, neoprávněné zpřístupnění nebo zpřístupnění předaných, uložených nebo jiným způsobem zpracovaných osobních údajů, které by mohly zejména vést k fyzické, hmotné nebo nehmotné újmě.“*

[141] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Recitál 83. [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679

[142] JANEČKOVÁ, E., GDPR. Praktická příručka implementace, str. 33

[143] V případě neoprávněného nebo náhodného poskytnutí nebo zpřístupnění osobních údajů.

[144] V případě neoprávněné nebo náhodné ztráty přístupu nebo zničení osobních údajů.

[145] V případě neoprávněného nebo náhodného pozměnění osobních údajů.

[146] V ČR je tato povinnost již zakotvena v zákoně č. 127/2005 Sb., o elektrických komunikacích a o změně některých souvisejících zákonů (zákon o elektrických komunikacích), ve znění pozdějších předpisů

[147] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 33 odst. 1. [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679

3.4.3.5.2.3 Posouzení vlivu

Nakonec je třeba zmínit i posouzení vlivu na ochranu osobních údajů. Tato povinnost vzniká ve chvíli, kdy je pravděpodobné, že určitý druh zpracování (zejména jsou-li využity nové technologie) bude mít za následek vysoké riziko pro práva a svobody subjektu údajů. Posouzení vlivu provede správce vždy před zahájením zpracování[148] a je nutné zejména v případech, kdy je prováděno *„systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování včetně profilování“*[149], dále pokud se jedná o rozsáhlé zpracování zvláštních kategorií údajů[150], anebo pokud se jedná o rozsáhlé systematické monitorování veřejně přístupných prostorů.[151]

3.4.3.5.3 Práva při zpracování osobních údajů

GDPR výrazně posiluje práva subjektů údajů. Konkrétně v ustanoveních čl. 12 až 22 GDPR stanovuje subjektům údajů tyto práva

a) informace a přístup k osobním údajům – jedná se o práva ke všem údajům, které má správce o subjektu údajů k dispozici, tj. i k tzv. nestrukturovaným údajům.[152]
b) právo na přístup k osobním údajům[153] – kdy *„subjekt údajů má právo na to, aby mu správce potvrdil, zda zpracovává jeho osobní údaje, a pokud ano, má právo získat přístup k nim a k informacím, které se tohoto zpracování týkají.“*[154]

[148] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 35. [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679

[149] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 35 odst. 3 písm. a). [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679

[150] viz kapitola 3.2.3 této práce

[151] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 35 odst. 3. [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679

[152] Tyto údaje mohou tvořit přílohy e-mailů nebo mohou být uloženy na různých interních a externích úložištích.

[153] Příkladem práv na přístup je informace o zdravotním stavu subjektu a přístup k údajům v jeho zdravotní dokumentaci.

[154] POMAIZLOVÁ, K., FÜRSTOVÁ, M., GDPR – revoluce, nebo rozvedení stávajícího? [online]. In: Bulletin advokacie, str. 18 [cit. 2018-10-12]. Dostupné z: http://www.bulletin-advokacie.cz/assets/zdroje/casopis/2016/BA_9_2017_web.pdf

c) právo na opravu – je provedením zásady správnosti. Subjekt údajů má právo, aby jeho nepřesné či neúplné údaje, které se ho týkají, byly bez zbytečného odkladu správcem opraveny.[155]

d) právo na výmaz – subjekt údajů má *„právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají.“*[156] Naopak i správce má povinnost bez zbytečného odkladu osobní údaje vymazat v případě je-li dán jeden z důvodů v GDPR uvedených.[157]

e) právo na omezení zpracování – subjekt údajů má podle čl. 18 odst. 1 GDPR právo, aby v taxativně vyjmenovaných případech[158] správce omezil zpracování[159] jeho osobních údajů.[160] Tato skutečnost omezení musí být v systému jasně vyznačena.

f) právo na oznamovací povinnost - se týká opravy osobních údajů, výmazu osobních údajů anebo omezení zpracování.[161]

g) právo na přenositelnost údajů – subjekt údajů má *„právo získat bezplatně své osobní údaje, které poskytl správci, a také právo tyto údaje bez omezení předat jinému správci.“*[162]

Podmínky, za kterých subjekt údajů toto právo nabývá, nalezneme v ustanovení čl. 20 GDPR. Těmito podmínkami jsou, jedná-li se o osobní údaje poskytnuté subjektem údajů,

[155] JANEČKOVÁ, E., GDPR. Praktická příručka implementace, str. 22

[156] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 17 odst. 1. [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679

[157] Podle čl. 17 odst. 1 GDPR jsou těmito důvody *„osobní údaje již nejsou potřebné pro účel, pro který byly shromažďovány nebo zpracovávány; subjekt údajů odvolá souhlas, pokud je zpracování založeno na souhlasu a neexistuje žádný další právní důvod pro zpracování; subjekt údajů vznese námitku proti zpracování z důvodu oprávněných zájmů správce osobních údajů; osobní údaje byly zpracovány protiprávně; pokud není dán rodičovský souhlas se zpracováním osobních údajů dětí a právní povinnost stanovená právem Unie nebo členským státem.“*

[158] Podle ust. čl. 18 GDPR *„Subjekt údajů popírá přesnost osobních údajů, a to na dobu potřebnou k tomu, aby správce mohl přesnost osobních údajů ověřit; zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o mezení jejich použití; správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právní nároků nebo subjekt údajů vznesl námitku proti zpracování podle čl. 21 odst. 1 obecného nařízení o ochraně osobních údajů, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu údajů.“*

[159] Zpracování lze omezit např. dočasným přesunem vybraných údajů do jiného systému zpracování, znepřístupněním vybraných osobních údajů uživatelům nebo dočasným odstraněním zveřejněných údajů z internetových stránek.

[160] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 18 odst. 1. [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679

[161] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 19 odst. 1. [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679

[162] POMAIZLOVÁ, K., FÜRSTOVÁ, M., GDPR – revoluce, nebo rozvedení stávajícího? [online]. In: Bulletin advokacie, str. 20 [cit. 2018-10-12]. Dostupné také z: http://www.bulletin-advokacie.cz/assets/zdroje/casopis/2016/BA_9_2017_web.pdf

dále jsou-li tyto osobní údaje zpracovávány automatizovaně, dochází-li k jejich zpracování pro konkrétní účely, anebo pokud subjekt údajů udělil se zpracováním osobních údajů souhlas.[163] *„Přenositelnost údajů je zcela nové právo vytvořené EU k podpoře konkurence na digitálním trhu.“*[164]

h) právo vznést námitku – subjektu údajů má kdykoli možnost vznést námitku nejen proti zpracování jeho osobních údajů pro účely přímého marketingu[165], ale i proti zpracovávání prováděné pověřeným správcem ve veřejném zájmu nebo výkonu veřejnému moci, nebo pro účely oprávněných zájmů správce či třetí strany[166].[167]

i) právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování[168], včetně profilování[169]

[163] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 20 odst. 1. [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679

[164] POMAIZLOVÁ, K., FÜRSTOVÁ, M., GDPR – revoluce, nebo rozvedení stávajícího? [online]. In: Bulletin advokacie, str. 20 [cit. 2018-10-12]. Dostupné také z: http://www.bulletin-advokacie.cz/assets/zdroje/casopis/2016/BA_9_2017_web.pdf

[165] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 21 odst. 2. [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679

[166] Podle ust. čl. 4 GDPR se třetí stranou rozumí *„fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, jež je oprávněna ke zpracování osobních údajů.“*

[167] POMAIZLOVÁ, K., FÜRSTOVÁ, M., GDPR – revoluce, nebo rozvedení stávajícího? [online]. In: Bulletin advokacie, str. 21 [cit. 2018-10-12]. Dostupné také z: http://www.bulletin-advokacie.cz/assets/zdroje/casopis/2016/BA_9_2017_web.pdf

[168] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 22 odst. 1. [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679

[169] Profilováním se podle ust. čl. 4 GDPR rozumí *„jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu.“*

3.4.3.6 Práva a povinnosti při zpracování zvláštních kategorií osobních údajů

Zpracování zvláštních kategorií osobních údajů podléhá mnohem přísnějšímu režimu, než tomu je u údajů obecných. Jak již bylo řečeno v kapitole 3.2.3, pod zvláštní kategorii osobních údajů spadají údaje, které mohou subjekt údajů samy o sobě poškodit (ve společnosti, v zaměstnání, ve škole) či mohou zapříčinit jeho diskriminaci, a proto se zpracování těchto údajů zakazuje[170] (ovšem existují případy, kdy je jejich zpracování povoleno[171]).

3.4.3.7 Sankce

„Vzhledem k tomu, že Nařízení obsahuje mnoho povinností, které přinesou správcům a zpracovatelům zvýšené náklady a nutnost upravit do této chvíle běžné činnosti, hrozí, že nebudou tyto povinnosti plnit zcela dobrovolně. Nařízení proto obsahuje i sankční ustanovení.“[172]

Správci a zpracovatelé osobních údajů se tak s účinností GDPR dostali pod větší drobnohled a dodržování jak nových, příp. upřesněných, tak i existujících pravidel je kontrolováno intenzivněji, zejména ze strany ÚOOÚ. Horní hranicí pro uložení pokuty je 20 000 000 euro nebo, jedná-li se o podnik[173] 4 % z celosvětového obratu podle toho, co je vyšší. [174]

---

[170] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 9 odst. 1. [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679

[171] Těmi podle čl. 9 odst. 2 GDPR jsou „*pokud subjekt údajů udělil výslovný souhlas se zpracováním těchto osobních údajů pro jeden nebo více stanovených účelů; je-li zpracování nezbytné pro účely plnění povinností a výkon zvláštních práv správce nebo subjektu údajů v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a sociální ochrany; je-li zpracování nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas; zpracování se provádí v rámci svých oprávněných činností a s vhodnými zárukami nadace, sdružení nebo jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle; zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů; zpracování je nezbytné z důvodu významného veřejného zájmu na základě práva Unie nebo členského státu, které je přiměřené sledovanému cíli; zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče či léčby nebo řízení systémů a služeb zdravotní nebo sociální péče; zpracování je nezbytné z důvodů veřejného zájmu v oblasti veřejného zdraví, jako je ochrana před vážnými přeshraničními zdravotními hrozbami nebo zajištění přísných norem kvality a bezpečnosti zdravotní péče a léčivých přípravků nebo zdravotnických prostředků; zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely.“*

[172] JANEČKOVÁ, E., GDPR. Praktická příručka implementace, str. 103

[173] Týká pouze podniku definovaného v článku 4 odst. 18 GDPR *(jakákoli fyzická nebo právnická osoba vykonávající hospodářskou činnost bez ohledu na její právní formu, včetně osobních společností nebo sdružení, která běžně vykonávají hospodářskou činnost).*

[174] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 83. [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679

„*Vedle možnosti soudní i mimosoudní ochrany v případě porušení práv při zpracování osobních údajů tak definuje GDPR v čl. 83 podmínky pro ukládání správních pokut.*“[175] Výše pokuty závisí na řadě faktorů (např. na povaze, závažnosti a délce porušování, na počtu poškozených subjektů a míře škody, na krocích podniknutých správcem či zpracovatelem ke zmírnění škod, na kategorii osobních údajů dotčenou porušením a na řadě dalších).[176]

3.4.4 Závěr

Na českém území platil do roku 1950 OZO, ve které je možné nalézt první ustanovení o ochraně osobnosti. OZO poskytoval výslovně ochranu pouze dílčímu osobnostnímu právu na jméno. Ochrana dalších dílčích osobnostních práv byla pak roztříštěna do různých právních předpisů (např. právo k vlastní podobizně a k osobním písemnostem upravoval autorský zákon). K ucelení právní úpravy ochrany osobnosti došlo až s přijetím občanském zákoníku č. 40/1964 Sb., ve kterém přetrvala právní úprava ochrany osobnosti až do roku 1989. Poté v souvislosti s přechodem socialismu ke kapitalismu na českém území byl občanský zákoník několikrát novelizován, např. byly rozšířeny prostředky ochrany o peněžité zadostiučinění. Občanskoprávní úpravu pak postupně začaly rozšiřovat i další specifické právní úpravy (zejména v oblasti zdravotnictví, v oblasti médií, tisku atd.). V roce 2012 byl přijat nový občanský zákoník (OZ), který je dosud platný (viz 3.4.2.1).

Ochranu osobnosti tedy upravuje OZ, který dále rozvádí základní práva obsažená v Ústavě, Listině a dalších úmluvách o lidských právech. Osobnost člověka je chráněna včetně všech jeho přirozených práv, mezi které patří zejména právo na život a na zdraví člověka, právo žít v příznivém životním prostředí, právo na důstojnost, vážnost a čest člověka a právo na ochranu projevů osobní povahy člověka a právo na ochranu soukromého života, které mj. zahrnuje i právo člověka se rozhodnout podle vlastního uvážení, zda, v jakém rozsahu a jakým způsobem mají být skutečnosti jeho osobního soukromí zpřístupněny jiným. Pokud bude osobnost člověka jakýmkoli způsobem dotčena, má právo se domáhat upuštění neoprávněného zásahu a příp. odstranění jeho následků (viz 3.4.2.2). Jednou z významných hodnot osobnosti člověka je i právo na podobu a s ním související právo na podobiznu. Narušení soukromých prostor člověka, sledování jeho soukromého

[175] POMAIZLOVÁ, K., FÜRSTOVÁ, M., GDPR – revoluce, nebo rozvedení stávajícího? [online]. In: Bulletin advokacie, str. 24 [cit. 2018-10-12]. Dostupné také z: http://www.bulletin-advokacie.cz/assets/zdroje/casopis/2016/BA_9_2017_web.pdf

[176] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 83 odst. 2. [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679

života, pořizování zvukových či obrazových záznamů o jeho soukromém životě, příp. šíření těchto záznamů nebo jejich pořizování třetí osobou lze pouze se souhlasem člověka (viz 3.4.2.2).

Naopak ochranu osobních údajů a ochranu zvláštních kategorií osobních údajů upravuje GDPR (viz 3.4.3). Počátek historického vývoje ochrany osobních údajů z hlediska GDPR lze datovat od roku 1981, kdy byla podepsána smlouva o ochraně osob s ohledem na automatické zpracování osobních údajů. Důležitější ovšem byl rok 1995, kdy byla jako základní prvek ochrany soukromí v rámci EU a práva v oblasti lidských práv vytvořena evropská směrnice o ochraně osobních údajů (Směrnice 95/46/ES). V roce 2000 pak přijala Česká republika vlastní zákon (ZoOU) týkající se ochrany osobních údajů. ZoOU a Směrnice 95/46/ES byly 25. května 2018 nahrazeny GDPR. Nařízení je přímo aplikovatelné a nadřazené národním právním předpisům a je tak v současné době nejkomplexnějším nařízením chránící soukromí občanů. ZoOU jako takový ovšem zcela zanikne až s účinností adaptačního zákona, který teprve bude přijat (viz 3.4.3.1). Mezi hlavní důvody pro přijetí GDPR patří zejména technologický pokrok, neomezené shromažďování údajů o občanech EU ostatními mimo evropskými státy, a neucelená a minimální úprava, vzhledem k tomu, že si každý členský stát ve svých národních předpisech ochranu osobních údajů upravoval jinak (viz 3.4.3.2).

Jak OZ tak GDPR převzaly z ústavních principů základní zásady, které tak jsou v obou předpisech společné. GDPR tyto zásady pouze zpřesňuje a detailněji rozpracovává. GDPR je založeno na principu odpovědnosti správce za dodržení zásad zpracování a na principu rizika. Mezi základní zásady zpracování osobních údajů patří zákonnost, korektnost, transparentnost, účelové omezení, minimalizace údajů, přesnost, omezení uložení, integrita a důvěrnost (viz 3.4.3.3). Zpracovávat osobní údaje zákonně lze i mj. na základě souhlasu subjektu údajů. Ovšem vzhledem k jeho odvolatelnosti se doporučuje hledat nejdříve jiný zákonný důvod pro zpracování osobních údajů, a až v případě, že žádný není, žádat o souhlas. Jedná se tak o jeden z nejkomplikovanějších možných důvodů zpracování. Souhlas by se měl vztahovat na činnosti zpracování osobních údajů, které mají stejné účely zpracování, v opačném případě je nutné udělit souhlas pro každý účel zpracování. Udělený souhlas lze kdykoliv odvolat (viz 3.4.3.4).

Mezi povinnosti správce při zpracování osobních údajů tedy patří zejména povinnost zpracovávat osobní údaje v souladu se základními zásadami. GDPR také upravuje rozsah poskytovaných informací, které musí být přiměřené a relevantní. Důležité také je, aby byla zpracovávána data nezbytná pro daný účel (viz 3.4.3.5.2).

Novými povinnostmi správce jsou povinnost vést záznamy o činnosti, které musí být vyhotoveny písemně (viz 3.4.3.5.2.1), dále povinnost zabezpečit zpracování osobních údajů a

hlášení bezpečnostních incidentů a povinnost posouzení vlivu na ochranu osobních údajů. Při porušení zabezpečení zpracování osobních údajů se rozlišuje, zda došlo k porušení důvěrnosti, dostupnosti anebo k porušení integrity. Jakékoli porušení zabezpečení je nutno bez zbytečného odkladu hlásit dozorovému úřadu (viz 3.4.3.5.2.2). Pokud je pravděpodobné, že zpracování osobních údajů vzhledem k povaze, rozsahu, kontextu a účelům bude mít za následek vysoké riziko pro práva a svobody fyzických osob, musí správce před zahájením zpracování provést posouzení vlivu. Posouzení vlivu se týká především automatizovaného zpracování včetně profilování, rozsáhlého zpracování zvláštních kategorií osobních údajů a rozsáhlého systematického monitorování veřejných prostorů (viz 3.4.3.5.2.3).

Výrazné posílení práv subjektů je jedním z největších dopadů GDPR. Těmito právy jsou právo na přístup k osobním údajům, jejich opravu nebo výmaz, dále právo na omezení zpracování, právo na přenositelnost údajů, právo vznést námitku a také právo nebýt předmětem žádného rozhodnutí založeného pouze na automatizovaném zpracování (viz 3.4.3.5.3).

Zvláštní kategorie osobních údajů zahrnuje takové osobní údaje, které jsou z hlediska základních práv a svobod svou povahou obzvláště citlivé a proto zasluhují zvláštní ochranu. Proto by tyto údaje neměly být zpracovávány, pokud není udělen souhlas subjektu údajů nebo pokud je subjekt údajů sám nezveřejnil, dále pak pokud není zpracování nezbytné pro účely plnění povinností a výkon zvláštních práv správce nebo subjektu údajů anebo pokud není zpracování nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby, případně další (viz 3.4.3.6). Dojde-li k porušení či nedodržení některé z povinností, které GDPR stanovuje, hrozí provozovatelům mj. vysoké pokuty, jejichž výše závisí na řadě faktorů (viz 3.4.3.7).

3.5 Právní úprava používání kamerových systémů

3.5.1 Úvodem

„Provoz kamer je neoddělitelně spjat s ochranou soukromí v nejširším slova smyslu, tak jak je soukromí chráněno v občanském zákoníku. Kamerové systémy (tj. kamery, které používá např. zaměstnavatel, prodejce, SVJ, družstvo atd.) současně zahrnují i zpracování osobních údajů.“[177]

Každý, kdo chce kamerový systém instalovat a je-li jeho záměrem snímat a uchovávat záznamy sledovaných míst, ve kterých se pohybují i další fyzické osoby, si musí určit účel a prostředky zpracování dat. Zároveň jeho záměr musí být legitimní a musí znát, jaké povinnosti je

[177] ŽŮREK, J., Praktický průvodce GDPR., str. 215

třeba zajistit a dodržovat ve vztahu k jiným subjektům. Dále také musí zvážit, zda je zavedení kamerového systému opravdu nezbytné a zda by tedy nepostačovalo jiné řešení. Protože takováto úvaha může nejen eliminovat možné budoucí střety s právem, ale navíc může přinést i nemalou finanční úsporu.

3.5.2 Používání kamerových systémů z hlediska právních úprav

3.5.2.1 Používání kamerových systémů z hlediska právní úpravy ochrany osobnosti

Instalováním kamerového systému vzniká kolize mezi právem na ochranu majetku a bezpečnosti osob (např. u bytových domů mezi právem majitelů bytových domů na ochranu vlastnictví[178]) a právy subjektu údajů na soukromí[179], právy na ochranu před neschváleným pořizováním a shromažďováním obrazových záznamů[180] a právy na ochranu před neoprávněným zpracováním osobních údajů[181].[182]

Jelikož se jedná o ústavně chráněná lidská práva, je nutno v případě kolize mezi nimi využít standartní test proporcionality.[183]

Prvním kritériem v testu proporcionality je hledisko vhodnosti, *„jehož cílem je posouzení způsobilosti zvoleného prostředku dosáhnout sledovaného účelu.“*[184] Druhým kritériem je hledisko potřebnosti neboli hledisko minimalizace zásahu, *„které sleduje analýzu plurality možných prostředků způsobilých dosáhnout sledovaného účelu, z nichž je pak zapotřebí zvolit takový prostředek, který ústavně chráněnou hodnotu omezuje v míře nejmenší.“*[185] Posledním třetím kritériem je hledisko poměřování, *„tj. porovnávání závažnosti v kolizi stojících základních práv, a to i vzhledem k akceptované hierarchii hodnot.“*[186] A právě v případě kolize těchto práv, může dojít k omezení základních práv či svobod, i když jejich omezení ústavní úprava vůbec nepředpokládá.

[178] viz ust. čl. 11 ústavního zákona č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů
[179] viz kapitola 3.4.2 této práce
[180] viz kapitola 3.4.2 této práce
[181] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 6. [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679
[182] Tyto tři práva jsou i ústavně garantována v čl. 7 odst. 1 a čl. 10 odst. 2 a 3 Listiny.
[183] BARTÍK, V. JANEČKOVÁ, E., Kamerové systémy v praxi, str. 80
[184] BARTÍK, V. JANEČKOVÁ, E., Kamerové systémy v praxi, str. 80
[185] BARTÍK, V. JANEČKOVÁ, E., Kamerové systémy v praxi, str. 81
[186] BARTÍK, V. JANEČKOVÁ, E., Kamerové systémy v praxi, str. 81

Aby nedocházelo k porušování práva na ochranu osobnosti[187], nesmí snímání kamerovými systémy se záznamem nadměrně zasahovat do osobní sféry sledovaných osob[188]. *„Porušením soukromí by došlo také k porušení čl. 8 odst. 1 Úmluvy o lidských právech a základních svobodách[189], která je dle čl. 10 ústavního zákona č. 1/1993 Sb., Ústava České republiky, součástí právního řádu a má přednost před zákony.“*[190]

3.5.2.2 Používání kamerových systémů z hlediska nové právní úpravy (GDPR)

Pokud byly z hlediska fungování kamerových systémů naplněny podmínky ZoOU, též naplňují i velkou část povinností uvedených v GDPR.

Nejprve je nutné si objasnit na jaké kamerové systémy se GDPR vlastně vztahuje. Z kapitoly 3.3.1.2.2 již víme, že GDPR se vztahuje na všechny kamerové systémy, které pořizují záznam. Dále jsou to kamerové systémy, které identifikují fyzické osoby ve veřejném prostoru[191], a nakonec kamerové systémy patřící právnickým osobám[192], včetně bytových družstev a SVJ.[193]

„Provoz kamerového systému musí být v každém případě pečlivě zvážen k daným okolnostem a ochrana soukromí by již měla být zahrnuta v jeho návrhu, čemuž musí odpovídat i vhodně zvolená technika.“[194]

3.5.2.2.1 Právní důvody zpracování

„Problematika možné kolize užití kamerového systému s principy ochrany osobních údajů je v současné době často a hlasitě diskutovaným námětem.“[195] V této souvislosti je nezbytné odpovědět na to, kdy lze kamerový systém považovat za systém zpracovávající osobní údaje, a kdy tomu tak není, a kdy se zpracovávaná informace považuje za osobní údaj, příp. zvláštní kategorii osobních údajů, a kdy tomu tak není.

---

[187] viz kapitola 3.4.2 této práce

[188] Jak již bylo řečeno v kapitole 3.3.1.2.2, není možné umístit kamerový systém do prostor toalet, sprch, převlékáren apod.

[189] Podle čl. 8 odst. 1 Úmluvy o lidských právech a základních svobodách *„má každý právo na respektování svého soukromého a rodinného života, obydlí a korespondence.“*

[190] BARTÍK, V. JANEČKOVÁ, E., Kamerové systémy v praxi, str. 81

[191] GDPR se netýká počítacích kamer, které dodávají pouze statistiky o počtu průchozích osob, rovněž mnohých termálních a přehledových kamer nebo starých analogových kamer, které kvůli nízkému rozlišení neposkytují prakticky žádné použitelné osobní informace.

[192] Na soukromou osobu, která si chce pomocí kamerového systému chránit svůj dům a bezprostřední prostor před ním, se vztahuje OZ, nikoli GDPR.

[193] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. K provozování kamerových systémů [online]. In: uoou.cz, 2018 [cit. 2018-10-25]. Dostupné z: https://www.uoou.cz/k-nbsp-provozovani-kamerovych-systemu/d-29535/p1=1099

[194] ŽŮREK, J., Praktický průvodce GDPR, str. 215

[195] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Na aktuální téma – Archiv. Komentář k Zásadám provozování kamerového systému z hlediska zákona o ochraně osobních údajů [online]. In: uoou.cz, Leden 2006 [cit. 2018-02-27]. Dostupný z: https://www.uoou.cz/vismo/zobraz_dok.asp?id_ktg=1103&p1=1103#kamery

Jak již bylo řečeno v kapitole 3.3.1.2.2, o zpracování osobních údajů se jedná, je-li kamerový systém vybaven záznamovým zařízením zaměřeným na monitorování fyzických osob a jsou-li pořizované záznamy používány k identifikaci fyzických osob v souvislosti s určitým jednáním. Ke zpracování tak musí mít správce právní důvod[196], který *„představuje oprávnění zpracovávat osobní údaje i prostřednictvím kamerového systému“*[197]. V rámci GDPR tak připadají pro provozování kamerových systémů v úvahu de facto pouze dva právní důvody[198] (také viz kapitola 3.3.1.2.3).

„Pokud správce, kterému svědčí některé prostory zaznamenávat kamerou na základě zákona, chce zaznamenávat i jiné prostory, nebo jde o správce, kterému žádná zákonná norma nestanovuje povinnost provozovat kamerový systém[199]*, může v úvahu připadat právní důvod nezbytnost zpracování pro účely oprávněných zájmů správce.“*[200] Tímto zájmem může být např. typická ochrana majetku. A základním předpokladem tohoto právního důvodu musí být právě jeho nezbytnost zpracování osobních údajů ve vztahu k účelu. *„Zároveň se musí jednat o takovou situaci, kdy objektivně převáží zájem správce na sledování určitého prostoru před právem na ochranu soukromí člověka“*[201], neboli jinak řečeno je třeba provést test proporcionality.[202]

Provozování kamerových systémů a jejich instalace je tedy oprávněná pouze, je-li sledovaný účel legitimní a nelze jej dosáhnout jinými běžnými prostředky. Zároveň kamerový systém nelze instalovat na každém místě. Prostory, v nichž je monitorování pro ochranu majetku, zdraví či života lidí nezbytné, musí být správcem voleny pečlivě. Protože pouze v takovém případě se lze vyhnout např. demontáži protizákonně umístěného kamerového systému, což může ušetřit nemalé finanční prostředky. Dále by měl správce volit *„takové technické řešení, aby pokud možno při dosažení účelu provozování kamerového systému co nejméně zasahoval lidem do soukromí (např. vhodně směřovat kamery), roli může hrát i výběr samotného zařízení.“*[203]

I odpověď na druhou otázku, kdy zpracovávanou informaci lze považovat za osobní údaj, nalezneme již v kapitole 3.3.1.2.2. Ze které lze tedy vyvodit, že prvotní záznamy fyzických osob

[196] viz kapitola 3.2.5 této práce
[197] ŽŮREK, J., Praktický průvodce GDPR, str. 216
[198] Koncipovat provozování kamerového systému na základě souhlasu nemá v žádném případě cenu, protože se nikdy nezaručí 100% souhlas všech osob. Navíc se jedná o právní důvod nestálý, protože souhlas lze odvolat.
[199] Povinnost provozovat kamerový systém vyplívá ze zákona č. 186/2016 Sb., o hazardních hrách, zákona č. 307/2013 Sb., o povinném značení lihu, zákona č. 181/2014 Sb., o kybernetické bezpečnosti, resp. vyhlášce č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatření a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti.
[200] ŽŮREK, J., Praktický průvodce GDPR, str. 217
[201] ŽŮREK, J., Praktický průvodce GDPR, str. 217
[202] viz kapitola 3.5.2.1 této práce
[203] ŽŮREK, J., Praktický průvodce GDPR, str. 217

uchovávané v rámci provozovaného kamerového systému samy o sobě jen velmi těžko umožní jednoznačně a bez dalších údajů identifikovat určitý nebo určitelný subjekt údajů. *„Nicméně na druhou stranu je nepochybné, že každý záběr zachycující znaky umožňující odlišení fyzické osoby od jiné vytváří ze záběru minimálně potencionální osobní údaj a jako s takovým by s ním mělo být nakládáno.“*[204] Těžko tak můžeme vyloučit, že by nemohlo dojít k identifikaci příslušné osoby kdykoliv v budoucnu, což je i důvodem toho, proč k pořizování záznamů vůbec dochází. Dá se říci, že se jedná o jistou presumpci dalšího využívání těchto záběrů, protože pokud by tyto záběry neměly být nijak využívány, celé záznamové zařízení by tak postrádalo jakýkoli smysl. Z výše uvedeného je tedy nezbytné stanovit také účel uchování záznamů z kamerových systémů, který se bezpochyby odvozuje od jejich využitelnosti.

V rámci této otázky je třeba také upřesnit, do jaké míry se v souvislosti se záznamy kamerových systémů jedná o zvláštní kategorii osobních údajů, jejichž výčet je uveden v kapitole 3.2.3.

3.5.2.2.2 Zabezpečení kamerového systému a záznamu

V rámci návrhu kamerového systému, musí správce řešit i jeho zabezpečení, včetně prostor, kde bude záznamové zařízení umístěno. Zároveň musí zabezpečení kamerového systému odpovídat v čl. 25 GDPR stanoveným podmínkám záměrné a standartní ochrany osobních údajů[205], a také podmínkám zabezpečení osobních údajů stanovených čl. 32 GDPR.[206] Záznamové zařízení musí správce umístit především tak, aby bylo zabezpečeno proti neoprávněnému přístupu. Šifrování záznamů nutné není, ale v rámci zabezpečení musí být vyřešena všechna přístupová práva a především logování, aby bylo zřejmé, jaký uživatel se na daný záznam díval příp. s ním jakkoliv nakládal.[207]

[204] BARTÍK, V. JANEČKOVÁ, E., Kamerové systémy v praxi, str. 20 až 21
[205] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 25. [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679
[206] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 23. [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679
[207] ŽŮREK, J., Praktický průvodce GDPR, str. 218

Jak je již uvedeno v kapitole 3.4.3.5.2.2 v případě, že by k porušení zabezpečení kamerového systému došlo, vztahovala by se na správce nebo provozovatele povinnost ohlásit jej ÚOOÚ[208] potažmo subjektu údajů[209].

3.5.2.2.3 Informační povinnost

GDPR stanovuje určité informace, které musí správce subjektu údajů poskytnout v závislosti na tom, zda získal osobní údaje přímo od subjektu údajů či nikoliv.[210] *„V případě kamerového systému se bude jednat o osobní údaje, které byly získány od subjektu údajů, byť jde o velmi hraniční případ a na první pohled tomu tak být nemusí.“*[211]

Každý správce musí zvolit informování, které musí být účelné a to i s ohledem na charakter osob, které může kamerový systém zachytit (např. rozesláním e-mailu, v papírové podobě, vylepením piktogramů, zveřejněním na internetu či intranetu).[212]

„Nedílnou součástí kamerového systému musí být řádné splnění informační povinnosti s přihlédnutím ke specifikům, které kamerový systém přináší.“[213] Na sledovaný prostor by měla upozorňovat minimálně informační tabulka, která musí obsahovat alespoň informaci, že je prostor kamerovým systémem monitorován, musí zde být uveden správce příp. provozovatel kamerového systému, resp. kontaktní osoba nebo sdělení, kde budou na žádost subjektu údajů poskytnuty všechny informace, které GDPR stanovuje.[214]

Tyto písemné informace lze doplnit jednoduchými a názornými obrázky viz obr. č. 3.

Obrázek č. 3 - Informace ohledně kamerového systému formou piktogramu[215]

PROSTOR JE STŘEŽEN KAMEROVÝM SYSTÉMEM
SE ZÁZNAMEM
Z důvodu bezpečnosti a prevence kriminality

Správcem zpracování je: ……..
Podrobnější informace o kamerovém sytému je možné získat na hlavní vrátnici nebo na tel. …...…… nebo e-mailu ……..… nebo na www……

Obrázek: vlastní zpracování

[208] Pokud by incident představoval riziko pro subjekt údajů.
[209] Pokud by incident představoval vysoké riziko pro subjekt údajů.
[210] viz kapitola 3.4.3.5.2 této práce
[211] ŽŮREK, J., Praktický průvodce GDPR, str. 218
[212] ŽŮREK, J., Praktický průvodce GDPR, str. 218
[213] ŽŮREK, J., Praktický průvodce GDPR, str. 218
[214] viz kapitola 3.4.3.5.2 této práce
[215] Měl by být poskytnut alespoň jeden kontakt.

Součástí informace musí být také uvedeny účely, za jakými jsou záznamy pořizovány, zpravidla se jedná o ochranu majetku správce, života a zdraví osob prostřednictvím stálého kamerového systému.

Plnění informační povinnosti je jednou z povinností spadajících do kategorie práv subjektu údajů, ovšem by neměly být opomíjeny ani další jeho práva uvedeny v kapitole 3.4.3.5.2. Subjekt údajů tak v případě kamerového systému může uplatňovat například právo na přístup k osobním údajům a v rámci něj na základě čl. 15 odst. 3 GDPR požadovat kopii zpracovávaných osobních údajů.[216]

K informační povinnosti, resp. transparentnosti kamerového systému je nutné také zmínit to, *„že v praxi pramení mnoho stížností na kamerový systém z jeho přezíravé instalace provozovatelem (SVJ, družstvo, zaměstnavatel), který se rozhodne kamerový systém začít provozovat bez náležité konzultace se zainteresovanými stranami (vlastníky, nájemníky) či bez řádné a spravedlivé informace pro zaměstnance.“*[217]

3.5.2.2.4 Záznamy o činnostech zpracování, nakládání s nimi a doba jejich archivace

S provozováním kamerových systémů souvisí také povinnost vedení záznamů o činnostech zpracování. Z povinnosti vést tyto záznamy jsou vyloučeny podniky nebo organizace, které zaměstnávají méně než 250 osob[218].[219] Jelikož provozování kamerových systémů zpravidla představuje riziko pro práva a svobody fyzických osob, a navíc takovéto zpracování není příležitostné, musí provozovatelé kamerových systémů tyto záznamy o zpracování činnosti vést.[220] Řádné nakládání se záznamy a adekvátní doba jejich uchování jsou pro celkové zajištění souladu kamerových systémů nezbytné a odvíjejí se od účelu zpracování.

„Záznamy z kamerového systému by měly být využívány pouze v odůvodněných případech, tj. když nastane incident, který naplňuje účel pořízení kamerového systému.“[221] Záznam lze

[216] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 15 odst. 3. [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679

[217] ŽŮREK, J., Praktický průvodce GDPR, str. 219

[218] Ledaže podle čl. 30 odst. 5 GDPR *„zpracování, které provádí, pravděpodobně představuje riziko pro práva a svobody subjektů údajů, zpracování není příležitostné, nebo zahrnuje zpracování zvláštních kategorií osobních údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.“*

[219] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 30 odst. 5. [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679

[220] ŽŮREK, J., Praktický průvodce GDPR, str. 220

[221] ŽŮREK, J., Praktický průvodce GDPR, str. 220

poskytnout pouze v případě, je-li zachycen vážný incident např. krádež, a to primárně Policii České republiky, která má mj. i zákonné oprávnění audiovizuální záznamy zveřejňovat, příp. jiným orgánům, včetně pojišťovny atd. *„Správce by se měl vyvarovat umísťování záznamů na internet s rychlými soudy o tom, že zachycená osoba je zloděj atd.“*[222]

Osobní údaje by měly být uchovávány po dobu nezbytně nutnou (omezenou na minimum)[223]. Rovněž se doba uchování záznamů odvíjí od stanoveného účelu, což odpovídá zásadě omezení uložení.[224] V závislosti na situaci každého konkrétního provozovatele kamerového systému, se jedná o dobu v řádech několika dnů až týdnů, která musí být v případě potřeby provozovatelem zdůvodněna a obhájena. Po uplynutí této doby by měl být záznam automaticky smazán[225].[226]

3.5.2.2.5 Další konsekvence kamerového systému

Pokud jde o povinnost jmenovat pověřence pro ochranu osobních údajů ve smyslu ustanovení čl. 37 GDPR *„není z důvodu běžného provozování kamerového systému v mezích shora uvedených (tj. SVJ, družstva, zaměstnavatelé – ochrana nemovitosti, pozemku, výrobních prostředků) nutné jmenovat pověřence.“*[227] Další otázkou může být plnění povinnosti posouzení vlivu na ochranu osobních údajů[228], kterou obvykle výše zmiňovaní provádět nebudou muset. Samozřejmě pouze v případě, pokud by se nejednalo o rozsáhlé systematické monitorování veřejně přístupných prostor[229], pak by nutnost provést posouzení vlivu nastala.

Obě dvě povinnosti by se tak vztahovaly např. na bezpečnostní agenturu provozující kamerové systémy v nákupních centrech, kde je rozsáhlé pravidelné a systematické monitorování vyžadováno.

---

[222] ŽŮREK, J., Praktický průvodce GDPR, str. 220

[223] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Recitál 39. [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679

[224] viz kapitola 3.4.3.3 této práce

[225] Je-li zachycen vážný incident, který se řeší nebo vyžaduje další řešení, bude daná sekvence pro tyto účely uchována po delší dobu.

[226] ŽŮREK, J., Praktický průvodce GDPR, str. 221

[227] ŽŮREK, J., Praktický průvodce GDPR, str. 222

[228] viz kapitola 3.4.3.5.2.3 této práce

[229] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Čl. 35 odst. 3 písm. c). [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679

3.5.2.3 Používání kamerových systémů z hlediska právní úpravy ostatních mezinárodních smluv

Právní rámec, založený na Směrnici 95/46/ES, přestal současné době odpovídat. Vzhledem k technologickému vývoji především prostředky (např. výpočetní technika), které jsou při zpracování osobních údajů využívány. Zpracování je sice daleko komplexnější, než bylo před několika desítkami let, ale zároveň se stalo pro práva a svobody subjektů údajů rizikovější. Proto bylo přikročeno k revizi právního rámce ochrany osobních údajů a tuto směrnici nahradilo GDPR. Zároveň touto směrnicí nebyla v jednotlivých zemích EU dosažena požadovaná míra sjednocení právní úpravy, což činilo problémy správcům působících ve více zemích. *„Cílem obecného nařízení je tedy přizpůsobení právního rámce ochrany osobních údajů dnešní době, dosažení větší jednoty právního rámce ve všech zemích, na které dopadá, posílení práv subjektů údajů a v neposlední řadě je snahou dosáhnout sjednoceného výkladu obecného nařízení a dozoru jednotlivými dozorovými úřady.“*[230]

Mezi další mezinárodní právní nástroje lze zařadit:

a) Evropskou úmluvu o ochraně lidských práv a základních svobod[231]
b) Úmluvu Rady Evropy č. 108/1981 o ochraně jednotlivců se zřetelem na automatizované zpracování osobních dat
c) Listinu základních práv Evropské unie[232]

3.5.2.4 Závěr

Na právní úpravu používání kamerových systémů lze nahlížet z několika hledisek. První z nich je používání kamerových systémů z hlediska právní úpravy ochrany osobnosti. Instalováním kamerového systému dochází totiž ke kolizi hned několika práv, zejména se jedná o rozpor mezi právem na ochranu majetku a bezpečnosti osob a ústavními právy subjektu údajů na soukromí, právy na ochranu před neschváleným pořizováním a shromažďováním obrazových záznamů a právy na ochranu před neoprávněným zpracováním osobních údajů. V tomto případě je pak nutné uplatnit test proporcionality (viz 3.5.2.1).

Druhým hlediskem je pak používání kamerových systémů z hlediska nové právní úpravy GDPR, které se vtahuje pouze na kamerové systémy, které slouží k identifikaci osob, zejména

[230] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Základní příručka k GDPR [online]. In: uoou.cz [cit. 2018-10-12]. Dostupná z: https://www.uoou.cz/zakladni%2Dprirucka%2Dk%2Dgdpr/ds-4744/p1=4744
[231] Ochrana soukromí je obsažena v čl. 8 Úmluvy o lidských právech.
[232] Ochrana soukromého a rodinného života, obydlí a korespondence je obsažena v čl. 7 Listiny základních práv Evropské unie, ochranu osobních údajů upravuje č. 8 Listiny základních práv Evropské unie.

ve veřejném prostoru, dále na kamerové systémy pořizující záznam a kamerové systémy patřící právnickým osobám, zejména provozuje-li kamerový systém bytové družstvo či SVJ (viz 3.5.2.2). Zde se můžeme také setkat s problematikou možného rozporu, a to mezi používáním kamerových systémů a principy ochrany osobních údajů. Proto je důležité si vyjasnit, kdy je kamerový systém považován za systém zpracovávající osobní údaje, a především kdy je zpracovávaná informace považována za osobní údaj a kdy za zvláštní kategorii osobních údajů. Ke zpracování osobních údajů dochází vždy, když je kamerový systém vybaven záznamovým zařízením (viz 3.3.1.2.3) anebo jsou-li pořizované záznamy používány k identifikaci fyzických osob (viz 3.5.2.2.1). Navíc k takovému zpracování musí mít správce právní důvod, za který z hlediska kamerových systémů lze považovat pouze zpracování nezbytné pro splnění právní povinnosti správce, která se na něj vztahuje anebo pokud je zpracování nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany (viz 3.3.1.2.3 a 3.5.2.2.1). Instalovat a provozovat kamerový systém lze tedy pouze, je-li sledovaný účel legitimní. Navíc nelze monitorovat všechny prostory, proto umístění kamerového systému musí být uváženo pečlivě, tak aby kamery zasahovaly lidem co nejméně do soukromí (viz 3.5.2.2.1).

Za osobní údaj je považována taková informace obsažená v záznamech z kamerových systémů pomocí, které lze identifikovat konkrétní fyzickou osobu (viz 3.3.1.2.3). Jelikož k identifikaci může dojít i v budoucnu, musí být stanoven kromě účelu zpracování také účel uchování těchto záznamů, kde záznam může být např. důkazem o trestné činnosti nebo o způsobení škody (viz 3.5.2.2.1). V případě kdyby při snímání či zpracování docházelo také k ukládání a/nebo porovnávání např. některých biometrických charakteristik subjektu údajů (obličejové charakteristiky, biometrické charakteristiky chůze, systém identifikace lidských tváří apod.), pak by se jednalo zpracování zvláštních kategorií osobních údajů (viz 3.5.2.2.1).

Při provozování kamerového systému musí správce dbát i na jeho zabezpečení včetně záznamového zařízení, a to podle podmínek záměrné a standartní ochrany osobních údajů a podmínek zabezpečení osobních údajů, např. pomocí šifrování (viz 3.5.2.2.2). Nedílnou součástí kamerového systému je také plnění informační povinnosti, zejména v prostorách, které jsou kamerovým systémem sledovány, a to nejen pomocí informačních tabulek, ale i např. zveřejněním na internetu. Kromě informační povinnost, jež spadá zároveň i do kategorie práv subjektu údajů, nelze opomenout ani další práva, které může subjekt údajů kdykoliv vůči správci uplatnit (viz 3.5.2.2.3). Vzhledem k tomu, že kamerové sledování představuje riziko pro práva a svobody fyzických osob musí provozovatelé kamerových systémů vést záznamy o činnostech zpracování osobních údajů, jejichž řádné nakládání s nimi a adekvátní doba jejich uchování se odvíjí od účelu

zpracování. To znamená, že záznamy z kamerového systému lze poskytnout příslušnému orgánu pouze v odůvodněných případech (např. při krádeži), a doba, po kterou smějí být záznamy uchovány, by měla být omezena na nezbytné minimum. A po uplynutí této doby by mělo dojít k automatickému smazání záznamu (viz 3.5.2.2.4). V souvislosti s provozováním kamerového systému vyvstaly i některé další otázky týkající se povinnosti jmenování pověřence pro ochranu osobních údajů, která se v případě běžného provozování kamerového systému na provozovatele nevztahuje, stejně tak jako povinnost posouzení vlivu na ochranu osobních údajů (viz 3.5.2.2.5).

I když GDPR představuje nový právní rámec ochrany osobních údajů v evropském prostoru, je třeba se v mezinárodním měřítku řídit i ostatními evropskými předpisy, mezi které patří zejména Evropská úmluva o lidských právech a základních svobodách, Úmluva o ochraně jednotlivců se zřetelem na automatizované zpracování osobních dat a Listina základních práv EU (viz 3.5.2.3).

4 Vlastní práce

4.1 Úvodem

Nový právní rámec na ochranu osobních údajů (GDPR) vznikl s cílem maximálně hájit práva občanů EU proti neoprávněnému zacházení s jejich osobními údaji a daty. Tato regulace se dotkla i činnosti členů Společenství vlastníků jednotek (dále jen „SVJ“) a členů bytových družstev. Konkrétně se jedná například o právo na přístup k osobním údajům, právo na opravu nepřesných údajů, právo na výmaz (tzv. „právo být zapomenut“) nebo právo vznést námitku proti zpracování osobních údajů.

4.2 Kamerové systémy v bytových domech

Instalace kamerového systému v bytovém domě je zřejmě nejošemetnější, co se provozování kamerových systémů týče, ačkoli právě instalace kamer v bytových domech je od roku 2016 na vzestupu.[233] Podle ÚOOÚ po celé ČR fungují kamerové systémy v téměř čtyřiceti tisících bytových domů. Jen v Praze hlídají kamerové systémy bezpečnost zhruba ve 40 % bytových domech.

Častými důvody pro umístění kamerových systémů v bytových domech jsou ochrana života a zdraví, ochrana majetku a prevence před vandalismem. Každý, kdo hodlá kamerový systém provozovat, musí nejprve jeho potřebnost pečlivě uvážit, neboť jeho povinností je jako budoucího správce osobních údajů stanovit legitimní účel zpracování osobních údajů tak, aby v případě potřeby byl schopen potřebnost a užitečnost kamerového systému doložit (viz 3.5.2.2.1).

Jednou se základních otázek zpracování osobních údajů prostřednictvím kamerových systémů v bytových domech je posouzení poměru mezi hodnotami, které mají být chráněny (ochrana života a zdraví, ochrana majetku) a hodnotami, do kterých bude zasaženo (ochrana soukromí).

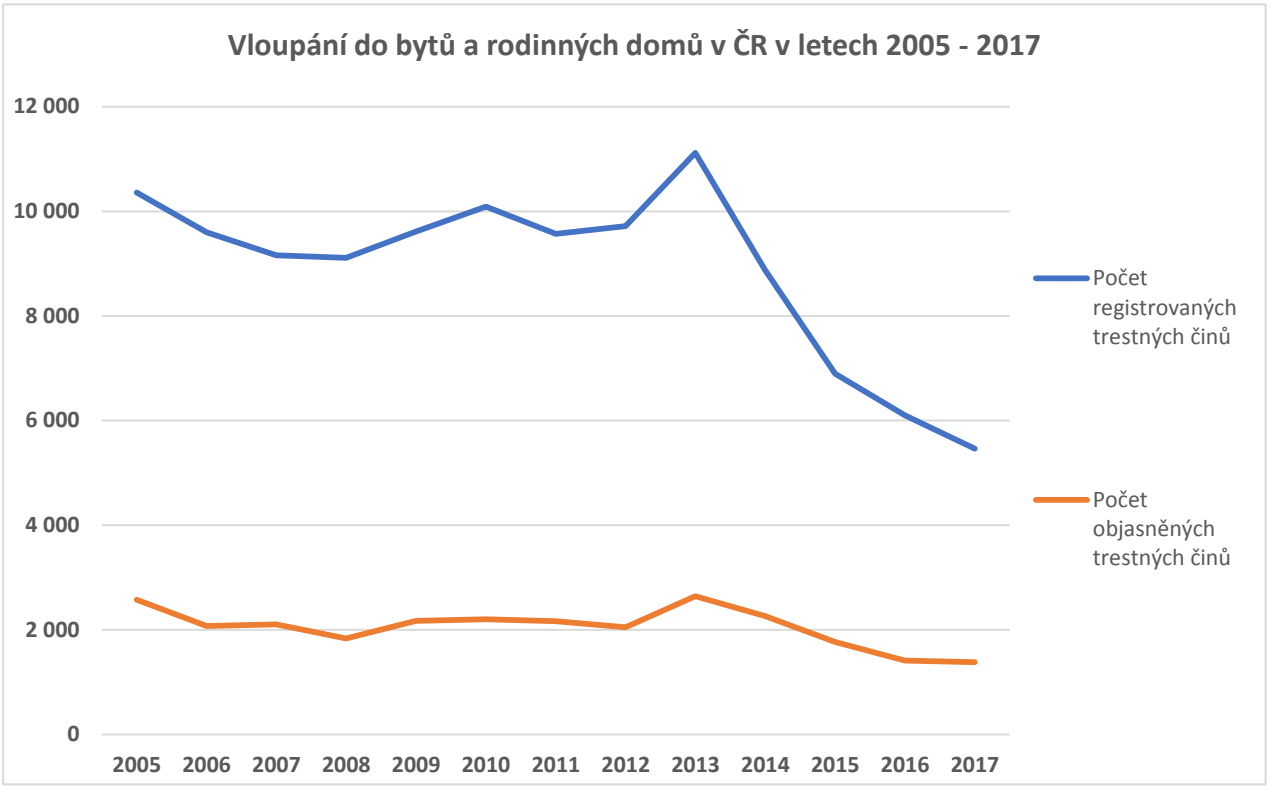
[233] Od ledna 2016 je možné sledovat také vstupní dveře do domu, vstupní chodby k výtahům a schodištím a i výtahy a schodiště.

4.2.1 Provozování kamerových systémů v bytových domech

4.2.1.1 Důvody pro zavedení kamerových systémů v bytových domech

Majetková kriminalita, zejména vloupání do bytů trápí občany řadu let. Graf č. 1 zobrazuje počet vloupání do bytů a rodinných domů v ČR za posledních 12 let. Jak je z grafu patrné počet registrovaných trestných činů vloupání v roce 2013 dosáhl svého dosavadního maxima, tedy více jak 11 tisíc registrovaných trestních činů vloupání. Lze se domnívat, že na tento výkyv mohla mít podstatný vliv částečná amnestie, kterou vyhlásil tehdejší prezident ČR Václav Klaus. Vzhledem k této skutečnosti lze předpokládat, že zájem o zabezpečení svých domovů rostl. Tím lze vysvětlit i následný rapidní pokles, kdy počet registrovaných trestných činů během čtyř let klesl zhruba na polovinu. Pokles mohl být způsoben právě i zvyšující se oblibou chránit svůj majetek, život a zdraví kamerovým systém. Naopak počet objasněných trestných činů vloupání se po celé roky nijak významně nezměnil, ba naopak má klesající tendenci.

Graf č. 1 - Vloupání do bytů a rodinných domů v ČR v letech 2005 - 2017

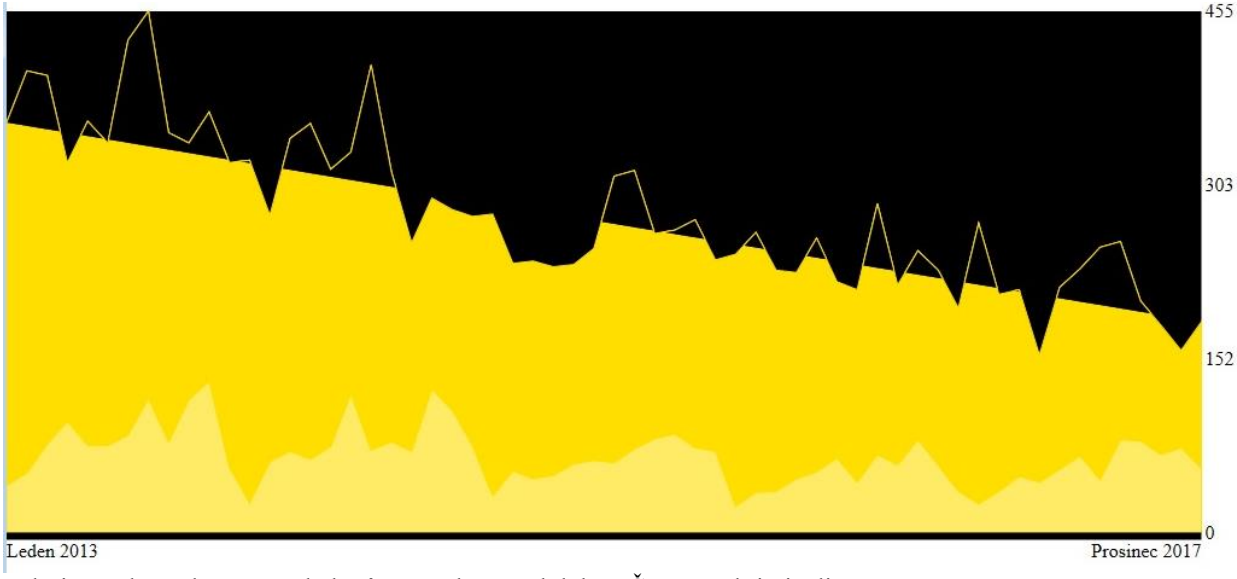


graf: vlastní zpracování, zdroj dat: Kriminalita - trestné činy, ČSÚ

Podrobnější informace nalezneme na obr. č. 4 a 5. Na obr. č. 4 jsou porovnány počty zjištěných (registrovaných) skutků[234] (znázorněno tmavě žlutou barvou) a objasněných skutků[235] (znázorněno světle žlutou barvou) a na obr. č. 5 je pro srovnání mezi jednotlivými obvodními odděleními použit index kriminality[236], jehož hodnoty ilustruje intenzita barvy.[237]

Obr. č. 4 zobrazuje krádeže vloupáním do bytů v ČR v letech 2013–2017 a obr. č. 5 zobrazuje krádeže vloupáním do bytů v loňském roce dle obvodních oddělení Policie ČR.

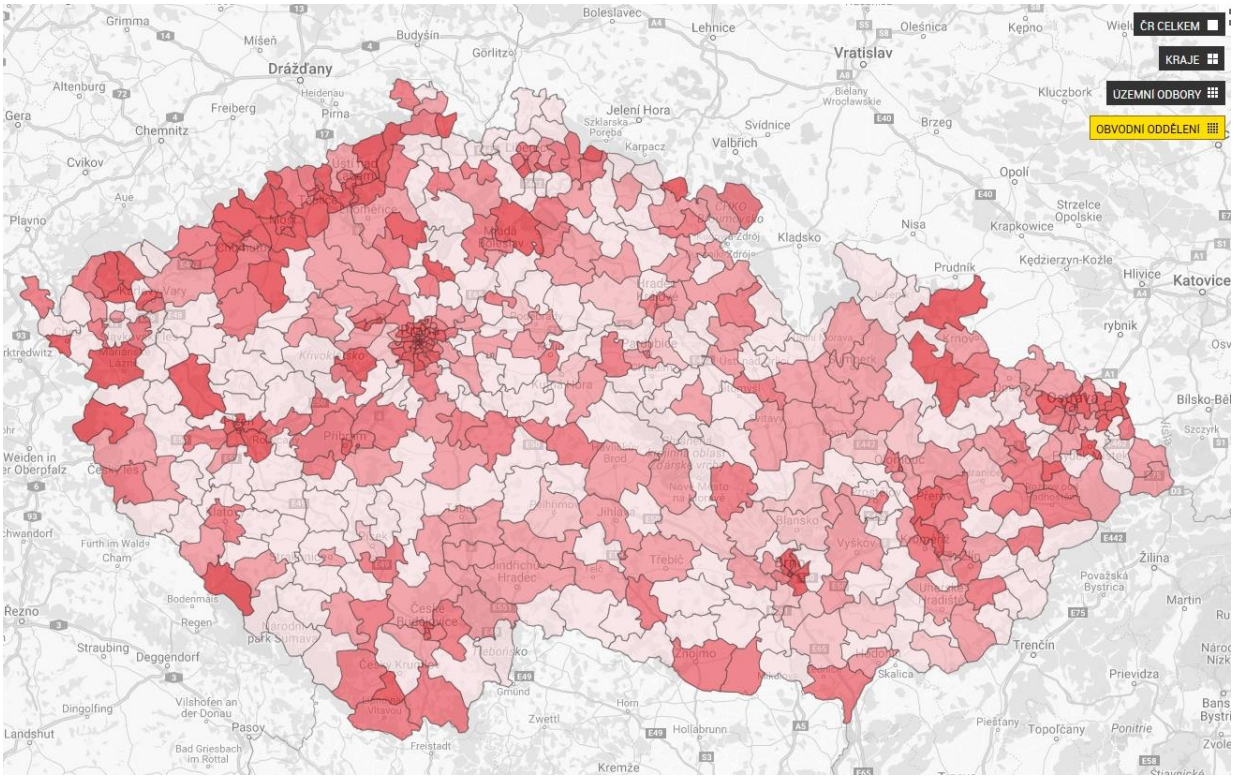
Obrázek č. 4 - Krádeže vloupáním do bytů v ČR v letech 2013 - 2017



Zdroj: Krádeže vloupáním do bytů ve zvoleném období v ČR, mapakriminality.cz

[234] Vykázaný trestný čin, kde bylo zahájeno trestní řízení ve sledovaném období a je ukončen (určitým způsobem) nebo neukončen.
[235] Registrovaný skutek, u kterého byl zjištěn (a vykázán) alespoň jeden známý pachatel a zároveň je skutek ukončen ve sledovaném období nebo zároveň je skutek ukončen ve sledovaném období, ale trestní řízení bylo zahájeno před začátkem sledovaného období.
[236] Počet zjištěných skutků za zvolené období, přepočtený na 10 000 obyvatel.
[237] Čím je barva sytější, tím vyšší je index kriminality, což znamená vyšší počet trestných činů.

Obrázek č. 5 - Krádeže vloupáním do bytů dle obvodních oddělení v roce 2017



Zdroj: Krádeže vloupáním do bytů ve zvoleném období v ČR, mapakriminality.cz

Bezpečnost obydlí může do určité míry ovlivnit každý občan tím, že bude dodržovat základní organizační opatření, jimiž jsou například řádné uzamykání, zajištění přízemních a sklepních oken, zvýšení odolnosti domovních dveří, upravené a přehledné prostranství před domem či dostatečné osvětlení společných prostor (chodby, sklepy) i osvětlení před domem. Celkovou bezpečnost bytového domu řádově zvyšuje i zabezpečení jednotlivých bytů. Častým problémem je ale i poškozování majetku ve společném vlastnictví. Nejčastěji se jedná o poškozené zámky, poničené (počmárané nebo posprejované) omítky a malby, zničené schránky nebo poničené výtahy, u kterých se škody mohou vyšplhat až do desítek tisíc korun. Ničení majetku však lze zamezit a právě z těchto důvodů jsou čím dál častěji kamerové systémy instalovány.

Kamery mají také psychologický efekt. V případě, kdy pachatel vidí, že v objektu jsou kamery naistalovány, může ho to odradit. Z tohoto důvodu se lze často setkávat i s tzv. atrapami či maketami bezpečnostních kamer.

4.2.1.2 Umístění kamerových systémů v bytových domech

V bytovém domě lze rozlišit dvě základní skupiny prostor, v nichž je možné vzhledem k míře soukromí kamerový systém nainstalovat (viz 3.5.2.2.1). Od tohoto rozdělení se pak odvíjí i míra souhlasu obyvatel domu (tj. lidé, kteří jsou majiteli, nájemci nebo podnájemci bytových jednotek nebo bytů v domě a kteří v bytě opravdu bydlí) (viz 3.4.3.4), a přirozeně i práva a povinnosti při zpracování osobních údajů uvedené v kapitole 3.4.3.5.

První skupinou jsou prostory, které nejsou určeny k soukromému životu obyvatel domu, a monitorování těchto prostor (tj. půdy, sklepy, vchody na půdu a do sklepa, výtahů[238], kočárkáren, koláren, prostor dopisních schránek, vnější opláštění budov a jeho bezprostřední okolí apod.) v zásadě do soukromí zasahuje v přiměřené míře a tudíž nevyvolává zásadní problémy. Umístění kamer v těchto prostorách je tedy možné bez souhlasu subjektu údajů.

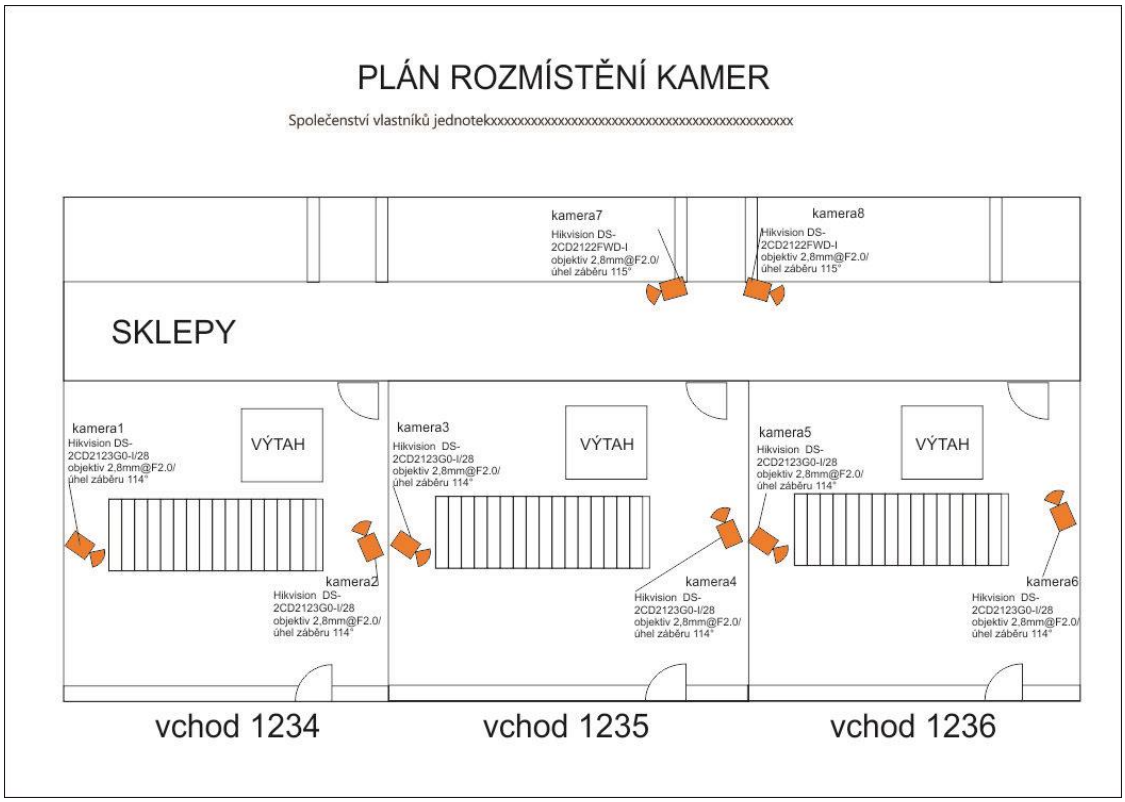
Druhou skupinou jsou prostory, kde obyvatelé domu požívají vyšší míru soukromí, jelikož tyto prostory jsou ze své podstaty spjaty s jejich soukromým a osobním životem (tj. chodby, schodiště, vchodové dveře do objektů, vchodové dveře do bytů apod.). Dochází zde ke shromažďování různých informací o soukromém životě obyvatel domu, jako například kdy, s kým, či „v jaké stavu“ přicházejí nebo odcházejí z domu, a to včetně jejich návštěv. Proto je v těchto prostorách k instalaci kamerového systému nutný souhlas všech obyvatel domu, tedy nejen vlastníků bytů, nájemníků či členů družstva, ale i všech dalších osob, které v domě bydlí. Jelikož souhlas musí být poskytnut v každém okamžiku všemi výše zmíněnými obyvateli domu, může v případě časté změny nájemníků nebo majitelů bytů (ale i nezletilých osob) nastat problém. Navíc jak je uvedeno v kapitole 3.4.3.4 souhlas se zpracováním osobních údajů může subjekt údajů za určitých podmínek odvolat. Z čehož vyplývá, že zpracování osobních údajů založené na souhlasu by bylo dobré praktikovat pouze v bytových domech s menším počtem bytů. I přesto je v případě kamerových systémů v bytových domech udělení souhlasu subjektů údajů nejfrekventovanější.

Při nastavení kamerového systému (tj. při stanovení prostředků a způsobu zpracování osobních údajů) je nutné přihlédnout k povaze prostor, které mají být sledovány, a to zejména k tomu, zda jsou tyto prostory obvykle průchozí nebo pouze příležitostně navštěvovány, anebo zda slouží jako bezprostřední přístup k bytům. Důležité je také samotné nastavení úhlu záběru kamery, a to ve vtahu k celkovému rozsahu snímaných prostor tak, aby současně nebyla snímána i jiná místa,

[238] Podle názorů vlastníků bytů, kteří jsou toho názoru, že výtahy a přístupové trasy jsou nedílnou součástí společných prostor bytových objektů, a že je nelze z těchto společných prostor vyjmout, byl prostor výtahů zařazen do skupiny první, a je tedy možné do něj kamerový systém instalovat již bez souhlasu.

v nichž by sledováním docházelo k zasažení soukromí obyvatel či návštěvníků domu (viz 3.5.2.1). Každý bytový dům by měl mít vypracován svůj plán rozmístění kamer (viz obr. č. 6).

Obrázek č. 6 - Plán rozmístění kamer v bytovém domě



Zdroj: Kamerové a zabezpečovací systémy. Dostupné online z: http://www.chran.cz/kamery-do-bytovych-domu/

V případě kamerového sledování vchodových dveří do bytů tak může docházet k závažným zásahům do práva na ochranu soukromého a osobního života, zde jednoznačně převažuje právo na ochranu osobnosti. Ve výjimečných a odůvodněných případech lze sledovat i tyto prostory ovšem pouze výhradně se souhlasem obyvatel dotčených bytů.

Pokud by provozovatelé kamerových systémů chtěli zabírat veřejné prostranství, např. parkoviště před bytovým domem, musí být kamery nastaveny tak, aby zabíraly jen úsek nezbytný v souvislosti s účelem zpracování, tedy s ochranou majetku. Rovněž v tomto případě musí být splněna informační povinnost podle kapitoly 3.5.2.2.

Jak již bylo řečeno v kapitole 3.5.2.2.2 i záznamové zařízení musí být umístěno na bezpečném místě (tj. samostatná a uzamykatelná místnost) a musí být také vnitřně zabezpečeno (tj. hesla, určený okruh osob, jež má přístup k zařízení a zná hesla, a ostatní prostředky nutné k překonání zabezpečení). Kromě záznamového zařízení musí být zabezpečeny také prostředky, které přenášejí obraz nebo data. Jsou známy případy, kdy správci projevují zájem instalovat

záznamové zařízení v bytě člena bytového družstva nebo SVJ na jeho osobním počítači bez adekvátních prvků počítačové bezpečnosti nebo instalovat záznamové zařízení jiným obdobným způsobem, jež nesplňuje zákonné podmínky zabezpečení zpracování osobních údajů. V případě, když není jiná možnost, nebo v případě, kdy by umístění záznamového zařízení v samostatné místnosti bylo spojeno s nepřiměřeně vysokými náklady (vzhledem k poměrům správce), teprve tehdy je možné umístit zařízení i v bytě člena bytového družstva nebo SVJ. Ovšem musí být zakódováno nebo zabezpečeno jiným podobným opatřením, které umožňuje přístup k záznamům a do místnosti, ve kterém se zařízení nachází, pouze úzké skupině osob, která je k tomu na základě rozhodnutí SVJ nebo bytového družstva oprávněna a nikoli už třeba jejím rodinným příslušníkům (viz 3.5.2.2.2).

4.2.2 Náklady na provozování kamerových systémů v bytových domech

Náklady na provozování kamerových systémů se u jednotlivých bytových domů liší. V kapitole 3.3.1.3 byly nastíněny hrubé náklady na pořízení a provozování kamerového systému, ovšem vždy záleží na velikosti domu, počtu vchodů a míst, kam chceme kamery umístit. Za považované minimum jsou čtyři kamery, umístěné zpravidla u vstupního vchodu, vchodu do sklepa, u schránek a ve výtahu. Přičemž s každou další kamerou se sice snižuje výskyt slepých míst (míst, kam kamery nevidí), ale zároveň se zvyšuje pravděpodobnost, že bude zasaženo soukromí obyvatel či návštěvníků domu.

Uvažujeme-li o bytovém domě s třemi předními a třemi zadními vchody, monitoringem garáží, kde budou umístěny 3 kamery, a monitoringem společných a sklepních prostor, na které budou dohlížet také 3 kamery, vejdeme se do 12 kamer pro celý bytový dům. Cena za jeden kamerový bod (čili jednu kameru) je stanovena na 20.000,- Kč a za záznamové zařízení, které pokryje všech 12 kamer a plus navíc je počítáno i s rezervou pro dalších 5 kamer v případě budoucího rozšíření kamerového systému, zaplatíme okolo 100.000,- Kč.[239] Připojení kamer do sítě LAN, pokud se dostaneme do vzdálenosti 95 m na kameru, PoE[240] a s tím související aktivní prvky se pohybují v řádu 15.000 – 25.000,- Kč. Sečteme-li všechny položky a přičteme cenu za instalaci (bez kabeláže) a oživení systému, vyjde nás pořízení kamerového systému pro tento bytový dům zhruba na 350.000 – 400.000,- Kč. Kromě výše zmíněných nákladů za pořízení kamerového

[239] V ceně jsou zahrnuty i potřebné utility pro lokální i vzdálený dohled.
[240] PoE (Power over Ethernet) je napájení po datovém síťovém kabelu, bez nutnosti přivést napájecí napětí k přístroji dalším samostatným kabelem.

systému musíme také počítat s pravidelnými provozními náklady, které se měsíčně pohybují v rozmezí 1.500 – 2.000,- Kč.

Zpravidla u nově postavených bytových domů jsou také důležité tzv. přístupové systémy, kde je u vchodu vstup na čip nebo biometrický systém (otisk prstu). Jejich výhodou je, že např. při ztrátě čipu, ho lze pouze odhlásit ze systému a nikdo už jej nezneužije, na rozdíl od klíčů, kde je případně nutné měnit celý zámek. Součástí přístupových systémů bývá i kamera s náhledem vchodu pro kontrolu „kdo zvoní“. V těchto případech by se dalo na první pohled říci, že zde kamerový systém není potřeba, ale z praxe je známo, že 80 % lidí otevře hned na první zazvonění bez kontroly, kdo u vchodu je, a bez kontrolní otázky. Podvodníci se často hlásí jako sociální pracovníci. Lidský faktor je tedy nesmírně důležitý.

4.2.3 Právní hlediska plynoucí z používání kamerových systémů v bytových domech

Jak již bylo řečeno v kapitole 3.5.2.2, podmínky pro provozování kamerového systému se od května 2018 řídí zcela novým právním předpisem GDPR a nijak významně se od předchozí právní úpravy neliší. Ovšem pro lepší pochopení pravidel, zejména tedy nových povinností správce či provozovatele kamerových systémů v bytových domech vyplývající z GDPR, si dovolím předestřít nejprve krátké shrnutí jednotlivých kroků, které musel učinit každý provozovatel nebo správce v souladu se ZoOU (tj. do 28. 5. 2018):

1) zpracování osobních údajů zaregistrovat u ÚOOÚ (tato povinnost byla přijetím GDPR zrušena),
2) prostřednictvím informačních tabulek informovat všechny osoby vstupující do monitorovaného prostoru,
3) zároveň informovat všechny osoby, které v bytovém domě bydlí o právním důvodu[241] zpracování jejich osobních údajů,
4) zabezpečit zpracovávání osobních údajů proti jejich možnému zneužití,
5) a dbát při provozování kamerového systému na ochranu soukromí monitorovaných osob.[242]

Pokud provozovatel kamerového systému dbal na všechny shora uvedené zásady a doporučení, které byly ÚOOÚ vydány, pak by se měl bez problémů vypořádat i s podmínkami GDPR. Zásadní změnou prošla pouze registrační povinnost, která dnem účinnosti GDPR byla ukončena

[241] Souhlas nebo právní důvod dle zákona. Více viz kapitola 3.2.5 a 3.4.3.4 této práce.
[242] viz zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů

(viz 3.4.3.5.2.1).

Každý správce nebo zpracovatel[243] musí dodržet určitá pravidla pro zpracování osobních údajů uvedená v kapitole 3.4.3.5.2, která by měla ochránit subjekt údajů před nezákonným zpracováním jeho osobních dat. Jak již bylo řečeno v kapitole 3.4.3.4, zákonnost je běžně ošetřena udělením souhlasu subjektu se zpracováním osobních údajů. Nicméně u zpracování údajů kamerovými systémy by se toto těžko dodržovalo, proto lze zpracovávat osobní údaje i bez souhlasu, na základě oprávněného zájmu vlastníka bytu (ochrana majetku a zdraví), ovšem musí být dodržována základní pravidla. Mezi ta patří v kapitole 3.5.2.2.1 uvedená nezbytnost pro naplnění účelu užívání kamer a přiměřenost k ochraně soukromí monitorovaných subjektů. Obzvláště je třeba rozlišit míru soukromí při umisťování kamer v jednotlivých prostorech bytového domu (viz 3.5.2.1).

Jak uvádí kapitola 3.5.2.2.4 související povinností s provozováním kamerového systému je nutnost vyhotovit záznamy o činnostech zpracování. Ty se vyhotovují písemně, v to počítaje i elektronickou formu a možný vzor takového záznamu o zpracování lze nalézt v příloze č. 1. Jedním z údajů, které mj. záznam obsahuje, je i lhůta pro výmaz. U bytových domů je uváděna doba potřebná k prošetření incidentu a zjištění dalších nezbytných informací pro příslušené orgány či pojišťovny 3 až 10 dní, v případě příležitostně navštěvovaných prostor až 14 dnů (v případech uvedených v kapitole 3.5.2.2.4 může správce tuto dobu prodloužit). Záznamy z kamer jsou v bytových domech ve většině případů uchovávány v časových smyčkách, tzn., že po uplynutí stanovené doby uchování záznamu dochází k automatickému přepisu záznamů ve smyčce.[244] Lze se setkat i s případy, kdy k automatickému přepisu záznamů dochází až při naplnění kapacity záznamového zařízení. V tomto případě je možné snížit kapacitu záznamového zařízení natolik, aby byla splněna potřebná doba uchování záznamů, a zároveň aby nebyla překročena (viz 3.5.2.2.4).

Co zůstává neměnné, je informační povinnost, kterou blíže specifikuje kapitola 3.5.2.2.3. Správce tedy odpovídá za to, že každý subjekt údajů musí být o užití kamerového systému v bytovém domě informován, ať už se jedná o obyvatele domu (člen družstva nebo SVJ) nebo další osoby (návštěvník), které do bytového domu přichází nepravidelně, resp. nepředvídatelně. U obyvatel domu lze splnit informační povinnost například prostřednictvím shromáždění SVJ a následným vyvěšením nebo rozesláním informace o zpracování všem obyvatelům domu, a to před

[243] U bytových domů lze zapojit i externího zpracovatele. Tím bývá nejčastěji správní firma, ale může to být případně i bezpečnostní agentura. Smlouva mezi tímto „externistou“ a SVJ nebo bytovým družstvem musí obsahovat mnoho konkrétních náležitostí a záruk.

[244] Kromě účelu zpracování záleží i na velikosti místa na disku a počtu snímajících kamer.

zahájením zpracování. To platí i v případě nových obyvatel domu, kteří se do domu přistěhují již po instalaci a spuštění kamerového systému. V případě návštěvníků je nutné splnit informační povinnost alespoň umístěním informačních tabulek. Důležité je, aby informace o monitorování objektu byly uvedeny na přehledných místech, tj. u vstupů/vjezdů včetně vstupu do výtahu. Tudíž má-li bytový dům více než jeden vchod/vjezd, musí být tato informace umístěna na všech těchto místech. Současně je dobré umístit doplňující informace na domovní nástěnku či elektronickou informační desku. Informační tabulky pak musí obsahovat všechny informace uvedené v kapitole 3.5.2.2.3.

Jako praktický příklad lze uvést kamery instalované v suterénních (sklepních) prostorech za účelem kontroly vstupu a pobytu neoprávněných osob jejich nežádoucích aktivit. Nejedná se tak o značný zásah do soukromého a osobního života, protože do sklepních prostor vstupují subjekty údajů pouze nepravidelně a málo často jak již bylo řečeno v kapitole 4.2.1.2. Navíc nejsou tyto prostory zpravidla průchozí, tj. neslouží pro vstup do dalších částí domů, kam by musely subjekty nezbytně vstupovat. A proti vstupu neoprávněných osob do domů jsou u vstupu chráněny uzamykatelnými mřížemi nebo dveřmi. Na základě těchto skutečností lze na předmětné zpracování kamerových záznamů aplikovat výjimku, kdy je zpracování nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany (viz 3.5.2.2.1).

Beze změny zůstala i primární odpovědnost správce (družstvo nebo SVJ), který rozhodl o provozování kamerového systému, jehož jedním z hlavních povinností je i nadále v kapitole 3.5.2.2.2 uvedené zabezpečení provozu kamerového systému a jeho datového úložiště proti neoprávněnému přístupu. Správce by měl zajistit mimo uvedené v kapitole 3.4.3.5.2.2 také další technická a organizační bezpečností opatření, což zahrnuje např. řízený přístup k datům, školení oprávněných osob, vedení záznamů o předání nahrávek oprávněným orgánům a osobám nebo například i zabezpečení samotných kamer například pomocí bezpečnostních krytů. Zásada zabezpečení zpracování osobních údajů ve svém důsledku přináší zvýšení tlak jak na provozovatele systému, tak na dodavatele a servisní společnosti, které se zabývají údržbou CCTV.

Na provozovatele kamerového systému v bytových domech se také vztahuje ohlašovací povinnost uvedená v kapitole 3.4.3.5.2.2. Což v praxi neznamená, že se vše musí okamžitě hlásit dozorovému úřadu, ale musí být zdokumentované veškeré případy porušení zabezpečení osobních údajů. Správce vždy uvede skutečnosti, které se daného porušení týkají, jeho účinky ale i přijatá nápravná opatření. Důležité je vyhodnotit, jaký by porušení mohlo mít dopad do osobnostní sféry jednotlivých osob.

Naopak provozovatelů kamerového systému v bytových domech se nebude týkat povinnost posouzení vlivu na ochranu osobních údajů (viz 3.5.2.2.5), jelikož vnitřní prostory v domě nejsou považovány za prostory veřejně přístupné, jako jsou např. obchodní centra nebo kamery na ulicích.

V případě porušení či nezavedení některých z podmínek GDPR hrozí provozovatelům kamerových systémů vysoké pokuty, jejichž výše je uvedena v kapitole 3.4.3.7. Ovšem mnohem větší dopad by porušením těchto podmínek mohl nastat v případě trestního řízení. Protože pokud by byl kamerový záznam pořízen neoprávněně, nejenže by v trestním řízení byl jako důkaz vyřazen, ale navíc by pachatel mohl podat trestní oznámení pro neoprávněné snímání jeho osoby. Jelikož se v našem právním systému i usvědčený pachatel může bránit tím, že byl sledován protiprávně, když zrovna dům vykrádal. V praxi jsou tak známy i případy, kdy pachatel vysoudil odškodnění.

4.3 Řízený rozhovor

V rámci praktické části byly zjišťovány názory obyvatel bytového domu, ve kterém je kamerový systém instalován a provozován. Otázky byly zaměřeny především na zabezpečení bytového domu, na to zda je kamerový systém provozován v souladu s platnými právními předpisy a v neposlední řadě na znalost práv obyvatel monitorovaného bytového domu jakožto subjekt údajů.

Dotazovaný respondent bydlí v bytovém domě, který byl postaven zhruba před sedmi lety, a lze ho tedy považovat za novostavbu. Jedná se o čtyřpatrový bytový dům, ve kterém se nachází 14 bytových jednotek, výtah, vstupní hala a suterén, ve kterém je garáž, sklepy a technické místnosti. Součástí bytového domu je společná zahrada a čtyři parkovací místa před domem. Právní forma bytového domu je SVJ.

Tazatel: Jak je Váš bytový dům zabezpečen? (mechanické nebo elektronické zabezpečení)

Respondent: Co se týče mechanického zabezpečení, všechny vstupní dveře jsou zabezpečeny zámkem, vrata do garáže se otevírají/zavírají pomocí dálkového ovládání a okna v 1. NP jsou opatřena venkovními roletami, které plní mimo jiné i funkci bezpečnostní. Elektronické zabezpečení zajišťuje kamerový systém, který monitoruje všechny vchody/východy (viz obr. č. 7), vstupní halu, garážová stání a parkovací stání před domem. A světla u vchodů/východů jsou na pohyblivá čidla.

Obrázek č. 7 - Umístění kamer v bytovém domě

Zdroj: obrázek poskytnut respondentem

Tazatel: Jsou ve Vašem bytovém domě umístěny kamery i na jiných místech, které jste výše nezmiňoval? Víte celkový počet kamer ve Vašem bytovém domě?

Respondent: Kameru vlastně máme ještě u vchodu do domu, takže je vidět, kdo zvoní. Celkový počet bych odhadl na pět kamer v celém domě (včetně té u vchodu do domu).

Tazatel: Zabírá některá z kamer veřejné prostranství okolo Vašeho domu?

Respondent: Ano, jak již bylo řečeno parkovací stání před domem.

Tazatel: Jedná se o parkovací stání vyhrazená pro obyvatele či návštěvníky Vašeho domu, nebo se jedná o veřejná parkovací stání?

Respondent: Tato parkovací stání (celkem čtyři) jsou vyhrazena pouze pro náš dům.

Tazatel: Máte kamerový systém se záznamem či bez záznamu?

Respondent: Jedná se o kamerový systém se záznamem. Kamery zaznamenávají v pravidelných 24 hodinových smyčkách.

Tazatel: Máte v rámci kamerového systému nějaké atrapy/makety kamer?
Respondent: Nemáme, všechny kamery jsou plně v provozu.

Tazatel: Jsou známy nějaké události spojené s narušením zabezpečení Vašeho bytového domu? (vandalismus, kriminalita)
Respondent: Vykradení vozidla před domem. Vozidlo bylo zaparkované na ulici v těsné blízkosti domu.

Tazatel: Výše jste zmiňoval, že kamerový systém monitoruje i prostranství před domem, konkrétně parkovací stání. Zachytily kamery tuto událost?
Respondent: Ano, ale zjistili jsme, že neoprávněně.

Tazatel: Pomohl záznam z Vašich kamer k vyřešení případu, příp. dopadnout pachatele?
Respondent: Nakonec ne, jelikož bylo zjištěno, že kamera zabírala větší úhel, než bylo pro její účely nezbytné. V tomto případě jsme tak na základě rady od právníka záznam z kamer před Policií ČR zatajili. Předešli jsme tak případné žalobě ze strany pachatele, bohužel na úkor vyřešení krádeže.

Tazatel: Bylo provedeno nezbytné nápravné opatření?
Respondent: Ano, neprodleně.

Tazatel: Kdo je provozovatelem kamerového systému ve Vašem domě?
Respondent: Naše SVJ.

Tazatel: Kdo je správcem kamerového systému ve Vašem domě?
Respondent: Domnívám se, že tři členové výboru. SVJ jim k tomu udělilo oprávnění.

Tazatel: Za jakým účelem je provozován kamerový systém ve Vašem domě?
Respondent: Předpokládám, že primárně ochrana majetku, jelikož záznamy jsou používány pouze v případě trestné činnosti. Jiný důvod jsem nezažil.

Tazatel: Jsou Vám známé měsíční náklady na provozování Vašeho kamerového systému?
Respondent: Není mi známo, ale jedná se jen o náklady na roční servis.

Tazatel: Víte, kde je umístěno záznamové zařízení?

Respondent: Ano, záznamové zařízení se nachází v suterénu domu, který je přístupný pouze na klíč. Navíc je zařízení ještě umístěno v uzamykatelné skříince viz obr. č. 8, od které mají klíče pouze k tomu pověřené osoby, tedy správcové.

Obrázek č. 8 - Umístění záznamového zařízení v bytovém domě

Zdroj: obrázek poskytnut respondentem

Tazatel: Došlo někdy u Vás k narušení zabezpečení osobních údajů?

Respondent: Nejsem si vědom.

Tazatel: Jakým způsobem je splněna informační povinnost ve Vašem domě?

Respondent: Na dveřích při vstupu do domu jsou umístěny informační tabulky. (viz obr. č. 9)

Obrázek č. 9 - Informační tabulka o monitorování prostoru kamerovým systémem

Zdroj: obrázek poskytnut respondentem

Tazatel: Byly jste jako obyvatelé domu informování prostřednictvím shromáždění, příp. rozesláním informace o provozování kamerového systému ve Vašem domě a tedy i o zpracování osobních údajů?

Respondent: Do domu jsme se přestěhovali teprve před dvěma lety, ale myslím, že informační e-mail nebo informace o provozování kamerového systému při koupi bytu určitě proběhla.

Tazatel: Pocítili jste nějakou změnu (příp. jakou) co se kamerového systému týče ve Vašem domě s účinností GDPR, tedy od 25. května 2018?

Respondent: Na domovní nástěnce bylo vyvěšeno obecné poučení o souhlasu se zpracováním osobních údajů. (viz příloha č. 2)

Tazatel: Udělili jste souhlas se zpracováním osobních údajů ve Vašem bytovém domě?

Respondent: Ano, byl udělen písemný souhlas všech obyvatel domu.

Tazatel: Znáte svá práva při zpracování osobních údajů? Jaká?

Respondent: Určitě mám právo na přístup k mým osobním údajům a určitou manipulaci s nimi, případně zažádat o vymazání mých osobních údajů pokud už nejsou potřebné. Pak bych měl mít právo souhlasit či nesouhlasit se zpracováním osobních údajů.

Tazatel: Znáte lhůtu pro výmaz neboli dobu archivace záznamů u Vašeho kamerového systému?

Respondent: Neznám.

4.3.1 Závěr z řízeného rozhovoru

Z poskytnutých odpovědí je patrné, že zmiňovaný bytový dům je kromě mechanického zabezpečení zabezpečen také elektronicky, prostřednictvím kamerového systému, který si spravuje a provozuje samo SVJ. Kamerový systém uchovává záznamy, které kamery pořizují v pravidelných 24 hodinových smyčkách. Celkem v tomto bytovém domě je umístěno pět kamer, včetně té, která je umístěna v přístupovém zařízení. Dále jsou kamery umístěny jak v prostorách (tj. vchod do sklepa, garážová a venkovní parkovací stání vyhrazená pro obyvatele a návštěvníky domu), kde není potřebný souhlas subjektu údajů, tak ale i u vchodů do domu a vstupní hale, kde souhlas všech

obyvatel domu nutný je.[245] Ve všech zmíněných prostorách k zákonnému zpracování osobních údajů dochází, protože SVJ obdrželo písemný souhlas od všech obyvatelů domu. O potřebnosti a dobrovolnosti souhlasu o zpracování osobních údajů byly obyvatelé domu informováni mj. prostřednictvím vyvěšeného obecného poučení o tomto souhlasu na domovní nástěnce.

Kamerový systém je v bytovém domě provozován primárně za účelem ochrany majetku, jelikož záznamy byly vždy použity pouze v případě trestné činnosti. Došlo zde ovšem k pochybení v nastavení kamery, která monitoruje venkovní prostředí. Nastavení úhlu záběru této kamery nebylo nezbytné v souvislosti s účelem zpracování tohoto bytového domu. Proto při vyšetřování trestné činnosti vloupání do vozidla v těsné blízkosti domu, nemohl být záznam, který kamera zachytila, použit, jelikož by se jednalo o neoprávněné pořízení tohoto záznamu a na SVJ by mohlo být pachatelem podáno trestní oznámení. Po tomto zjištění SVJ neprodleně provedlo nápravné opatření tak, aby se podobná situaci již neopakovala. Dle mého názoru se bohužel nejedná o jediný případ v ČR, jelikož ze svého okolí znám několik bytových domů, u kterých se domnívám, že jejich kamery monitorující blízké venkovní prostředí nejsou nastaveny tak, aby zabíraly jen úsek k tomu nezbytný. Na druhou stranu přesně takovéto případy porušení pravidel provozování kamerových systémů mohou právě snižovat procento objasněných trestních případů, jejichž počet je velmi nízký a navíc stále klesá, jak je vidět i na obr. č. 4.[246]

Kamerový systém v tomto domě spravují tři členové výboru, kteří k tomu byli SVJ oprávněni. Ti jako jediní mají také přístup k záznamovému zařízení, které je umístěno v suterénu domu, kde je navíc ještě uzamčeno v průhledné schránce k tomu určené. Respondent také potvrdil, že si není vědom, že by někdy k narušení zabezpečení osobních údajů došlo. Lze tedy konstatovat, že SVJ svědomitě plní povinnost zabezpečení záznamového zařízení proti neoprávněnému přístupu a očividně zatím nemuseli porušení zabezpečení osobních údajů ohlašovat.

Za ne zcela uspokojivé by se dalo považovat splnění informační povinnosti, která v tomto bytovém domě sice splněna je, ale ne v požadovaném rozsahu. U obyvatel domu byla informační povinnost splněna zajisté prostřednictvím shromáždění a následným rozesláním informace o zpracování, která je rozesílána vždy i nově přistěhovalým, což potvrdil i respondent. Ovšem na splnění informační povinnosti uvnitř domu je ještě co vylepšovat. Jak je vidět na obr. č. 9 informační tabulka je umístěna na vchodových dveřích, nelze ji tedy přehlédnout. Obsahuje informaci o sledování prostoru kamerovým systémem doplněnou o názorný piktogram, není zde ovšem uveden správce ani provozovatel, resp. kontaktní osoba nebo sdělení, kde by v případě

[245] viz kapitola 4.2.1.2 této práce
[246] viz kapitola 4.2.1.1 této práce

zájmu byly poskytnuty požadované informace, a není uveden ani účel pořizování záznamu, natož informace zda je vůbec provozován kamerový systém se záznamem či bez záznamu. V tomto případě bych doporučila umístit další informační tabulku se všemi těmito povinnými náležitostmi na domovní nástěnku, pokud tak již není už učiněno.

Alarmující je i neznalost práv subjektu údajů. Dotazovaný respondent ve své odpovědi uvedl pouze tři práva z devíti možných. Lze tedy předpokládat podobnou neznalost i u ostatních obyvatel bytového domu, ne-li u většiny subjektů údajů na našem území celkem. Toto zjištění mě vede k závěru, že vzhledem k neúplné znalosti všech práv při zpracování osobních informací, může docházet k jejich zneužívání. Zejména tím, že ti co svá práva neznají, je také nikdy nevyužijí a na tento fakt by právě mohl případně někdo spoléhat. Nulová informovanost u respondenta je také u délky lhůty pro výmaz. Dle mého názoru by obyvatelé domu jakožto subjekty údajů měli znát dobu, po kterou budou záznamy s nimi uchovávány, neboli za jak dlouho budou vymazány. Zde lze ovšem těžko soudit, kdo je za neinformovanost zodpovědný, může se totiž jednat pouze o nezájem ze strany obyvatel.

5 Výsledky a diskuse

5.1 Teoretická východiska

V teoretické části je analyzována právní úprava kamerových systémů a v souvislosti s ní právní úprava ochrany osobnosti. Jsou zde vymezeny pojmy, které souvisí s používáním kamerových systémů. Za kamerový systém lze považovat soustavu prvků, pomocí kterých můžeme zaznamenávat nebo zobrazovat snímané objekty. Po technické stránce rozdělujeme kamerové systémy do dvou skupin – analogové a digitální, jejichž princip fungování se liší pouze v použitých technologií a přenosových médiích (viz 3.3.1.1). Po stránce legislativní rozlišujeme také dva druhy kamerových systémů, a to kamerový systém se záznamem a bez záznamu. Zde je rozdíl v právních předpisech, kterými se musí řídit (viz 3.3.1.2). U kamerového systému bez záznamu se lze řídit pouze obecnými předpisy na ochranu osobnosti (Ústava, Listina a OZ) a GDPR se na tento druh kamerových systémů nevztahuje (viz 3.3.1.2.2). Naopak kamerové systémy se záznamem jsou mj. regulaci GDPR podrobeny, jelikož při jejich provozování dochází ke zpracování osobních údajů (viz 3.3.1.2.3). Pořízení kamerového systému vyjde zhruba na 1 milion korun českých, ke kterému ovšem musíme přičíst i pravidelné průběžné náklady na servis či obsluhu (viz 3.3.1.3). Je tedy otázkou zda tento dnes, dá se říci nejpoužívanější zabezpečovací systém, je vůbec účelný a není zbytečně nadužíván. Za úvahu stojí skutečnost, že z hlediska zabezpečení kamerové systémy ve své podstatě nahrazují chyby lidského faktoru. Tudíž kdyby se snížila chybovost lidského faktoru, nemusely by být vynakládány tak vysoké částky za zabezpečení pomocí kamerového systému. Vždyť přeci zamykání je stále tou nejbezpečnější ochranou. Bohužel se ale nacházíme v době, kdy se snažíme co nejvíce svých činností zautomatizovat tak, abychom museli udělat co nejméně. Proto dle mého názoru raději zaplatíme horentní sumy za různé bezpečnostní systémy, než abychom např. pravidelně zamykali.

První zmínky o ochraně osobnosti na českém území lze nalézt už v OZO z roku 1811, ovšem ucelenou právní úpravu o ochraně osobnosti upravoval až od roku 1965 občanský zákoník č. 40/1964 Sb., který byl nahrazen až v roce 2012 současným OZ (viz 3.4.2.1). Od roku 1993 právní úpravu ochrany osobnosti můžeme mj. nalézt ve dvou základních ústavních zákonech. Občanský zákoník tak pouze rozvádí základní práva obsažená v Ústavě, Listině a příp. dalších mezinárodních úmluvách o lidských právech. Podle OZ má každý právo na ochranu svého života a zdraví, ale i svobody, cti, důstojnosti a soukromí, a byla-li jeho osobnost dotčena, má právo se domáhat upouštění neoprávněného zásahu anebo přímo odstranění jeho následku. Významnou hodnotou ochrany osobnosti je právo na podobu, jakožto na jednu z identifikačních složek osobnosti člověka,

které má význam především v souvislosti s právem k podobizně neboli k obrazovému snímku či záznamu (viz 3.4.2.2). Nedotknutelnost člověka a jeho soukromí může být omezena pouze v případě stanoveným zákonem, a v žádném případě nesmí být bez jeho svolení narušeno. Svůj souhlas může každý navíc podle OZ kdykoli odvolat (viz 3.4.2.2).

Počátky historie ochrany osobních údajů z hlediska GDPR lze datovat od roku 1981, ačkoliv za zmínku stojí až rok 1995, kdy vstoupila v platnost Evropská Směrnice 95/46/ES. ČR pak o pět let později přijala vlastní zákon (ZoOU) týkající se ochrany osobních údajů (viz 3.4.3.1). Jelikož vývoj technologií není přímo úměrný vývoji právních norem a technologický pokrok nelze zastavit, musela být po více jak dvaceti letech směrnice aktualizována a také vzhledem k požadavku EU, která chtěla zavést nařízení přímo aplikovatelné ve všech členských státech EU (viz 3.4.3.1), bylo v roce 2016 přijato Nařízení Evropského parlamentu a Rady (EU) 2016/679 neboli GDPR, které nabylo účinnosti 25. května 2018. Jelikož GDPR je přímo použitelné a má tedy přednost před ZoOU, probíhá novelizace tohoto národního předpisu, který bude v budoucnu nahrazen tzv. adaptačním zákonem (viz 3.4.3.1). Mezi hlavní důvody přijetí GDPR lze zařadit zejména technologický a společenský vývoj, zamezení neoprávněnému zacházení s osobními údaji občanů EU a minimální neucelená právní úprava (viz 3.4.3.2.).

Jak v OZ tak v GDPR jsou převzaty z ústavních principů základní zásady, které jsou v obou předpisech společné. GDPR tyto zásady pouze zpřesňuje a detailněji rozpracovává. Jedná se především o zásady zákonného zpracování, jejichž výklad v GDPR se ve své podstatě shoduje s ustanoveními v OZ (viz 3.4.3.3). Jedním ze zákonných důvodů zpracování osobních údajů je i velmi často používaný souhlas, i přestože se jedná o jeden z nejkomplikovanějších důvodů, a to vzhledem k jeho snadné odvolatelnosti. Proto GDPR pro zpracování osobních údajů doporučuje nejprve hledat jiný zákonný důvod (viz 3.2.5) a souhlas vyžadovat až v posledním možném případě (viz 3.4.3.4).

Práva a povinnosti při zpracování osobních údajů obsažené v ZoOU nahradila práva a povinnosti stanovené GDPR. Nejedná se ovšem o velké rozdíly, pouze povinnosti správce jsou GDPR stanoveny obecněji (viz 3.4.3.5.2) a práva subjektů byla výrazně posílena (viz 3.4.3.5.3).

Mezi povinnost správce patří zejména jedna hlavní, a to dodržování zásad zpracování osobních údajů (viz 3.4.3.3), mezi nové povinnosti pak patří povinné vedení záznamů o činnostech zpracování, které částečně nahrazuje zrušenou registrační povinnost (viz 3.4.3.5.2.1), dále pak povinnost zabezpečit vhodnými technickými a organizačními opatřeními zpracování osobních údajů včetně záznamového zařízení a povinnost jeho porušení bez zbytečného odkladu hlásit příslušnému dozorovému úřadu (porušit lze důvěrnost, dostupnost a integritu) (viz 3.4.3.5.2.2). Poslední novou

povinností je posouzení vlivu na ochranu osobních údajů, kterou musí správce provést vždy, když je pravděpodobné, že zpracování pomocí zejména nových technologií bude mít za následek vysoké riziko pro práva a svobody subjektu údajů (viz 3.4.3.5.2.3). Při nedodržení některých z těchto povinností, mohou správcům a provozovatelům kamerových systémů hrozit pokuty až do výše 20 milionů eur (viz 3.4.3.7).

Za práva subjektu údajů lze považovat právo na informace a přístup k osobním údajům, právo na opravu, omezení zpracování anebo výmaz osobních údajů, právo na oznamovací povinnost, právo vznést námitku proti zpracování a v poslední řadě právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování (viz 3.4.3.5.3). Pro zpracování zvláštních kategorií osobních údajů platí stejné práva a povinnosti, pokud je ovšem vzhledem k jejich citlivosti, zpracování vůbec povoleno (viz 3.4.3.6).

Instalováním kamerového systému dochází ke střetu mezi právem ochrany majetku a bezpečnosti osob a právy subjektu údajů na soukromí, právy na ochranu před neschváleným pořizováním shromažďováním obrazových záznamů a právy na ochranu před neoprávněným zpracováním osobních údajů. V případě kolize těchto ústavních práv je nutno využít testu proporcionality, jehož kritérii jsou hledisko vhodnosti, hledisko potřebnosti a hledisko poměřování. Aby nebylo narušeno soukromí, nesmí kamerové snímání nadměrně zasahovat do osobnostní sféry sledovaných osob (viz 3.5.2.1).

GDPR se kromě kamerových systémů se záznamem vztahuje také na kamerové systémy právnických osob a na kamerové systémy ve veřejném prostoru, které pořizují záznam za účelem identifikace osob (viz 3.5.2.2). Možná kolize může nastat i mezi principy ochrany osobních údajů jak podle OZ tak podle GDPR a užití kamerového systému. Proto je nutné si nejprve vyjasnit, v jakém případě lze považovat kamerový systém za systém, který zpracovává osobní údaje, a kdy lze zpracovávané informace považovat za osobní údaj (viz 3.5.2.2). Z hlediska právních důvodů lze kamerové systémy používat pouze, pokud je zpracování nezbytné pro splnění právní povinnosti správce anebo pokud je zpracování nezbytné pro účely oprávněných zájmů správce či třetí strany (viz 3.3.1.2.3 a 3.4.3.3). Je-li sledovaný účel legitimní, lze kamerový systém instalovat a provozovat. Umístění kamerového systému musí být pak pečlivě zváženo, protože nelze jej instalovat na každém místě (viz 3.5.2).

Správce při provozování kamerového systému musí dbát také na jeho bezpečnost, zejména tedy na bezpečnost zpracování osobních údajů a bezpečnost osobních údajů jako takových (viz 3.5.2.2.2). Dále musí vůči subjektům údajů splnit informační povinnost a musí být připraven na eventualitu, že subjekt údajů může kdykoli uplatnit svá práva (viz 3.5.2.2.3). Správce také je

povinen vést záznamy o činnostech zpracování. Samotné kamerové záznamy pak mohou být poskytnuty příslušným orgánům pouze v odůvodněných případech a smí být uchovány pouze po dobu nezbytně nutnou, která se odvíjí od účelu zpracování. Po uplynutí této doby by měly být záznamy automaticky smazány (viz 3.5.2.2.4). Povinnost jmenovat pověřence pro ochranu osobních údajů a povinnost posouzení vlivu na ochranu osobních údajů se v případě běžného provozování kamerového systému na provozovatele nevztahuje (viz 3.5.2.2.5). Z mezinárodního hlediska je pak třeba se řídit mj. i ostatními evropskými předpisy (viz 3.5.2.3).

5.2 Východiska z vlastní práce

Nový OZ nabyl účinnosti 1. ledna 2014, GDPR je účinné od 25. května 2018 a nepřineslo v rámci provozování kamerových systémů žádné výrazné změny, a tak pokud byly naplněny podmínky ZoOU, též z velké části splňují i pravidla stanovené OZ nebo GDPR.

V téměř čtyřiceti tisících bytových domech po celé ČR jsou provozovány kamerové systémy (viz 4.2). Přičemž mezi nejčastějšími důvody pořízení kamerového systému do bytového domu patří ochrana proti majetkové kriminalitě a vandalismu, a ochrana života a zdraví obyvatel domu (viz 4.2.1.1). Jak je z dostupných statistik známo, i přestože počet registrovaných trestních činů krádeží vloupáním od roku 2013 klesá, na počtu z nich objasněných to nic nemění, naopak jejich počet také klesá. Lze se tedy domnívat, že pokles může být způsobem právě zvyšující se oblibou zabezpečovat si svůj majetek kamerovým systémem, který má zároveň i psychologický efekt (viz 4.2.1.1). Takže paradoxně i když se kamerový systém teoreticky zdá být méně výhodným než ostatní způsoby zabezpečení (zamykání, přístup do domu na elektrický čip nebo čipovou kartu, příp. otisk prstu), je z praktického hlediska poměrně účinným prvkem (má výraznou preventivní funkci).

Z hlediska kamerových systémů se v bytovém domě rozlišují dvě základní skupiny prostor. První skupinou jsou prostory, které nejsou k soukromému životu obyvatel domu určeny, a souhlas s monitorováním těchto prostor potřeba není. Druhou skupinou jsou naopak prostory, které jsou ve vyšší míře se soukromým a osobním životem obyvatel domu spjaty, a proto musí být k jejich monitorování udělen souhlas každého obyvatele domu, včetně nezletilých osob či nově přistěhovalých (viz 4.2.1.2). Proto je vždy nutné k povaze prostor, které mají být sledovány, přihlédnout, jelikož při špatném nastavení kamerového systému (zejména úhlu záběru kamer), může docházet k narušení soukromí. Za takovéto protiprávní sledování může být na provozovatele kamerového systému podána žaloba anebo v lepším případě udělena vysoká pokuta (viz 4.2.3). Výše zmíněné platí zejména v případě monitorování veřejného prostranství, např. parkovacích stání před domem (viz 4.2.1.2). Zabezpečení provozu kamerového systému a jeho záznamového zařízení

proti neoprávněnému přístupu je jednou z hlavních povinností správce nebo provozovatele. Ten by měl kamerový systém zabezpečit všemi dostupnými opatřeními, což zahrnuje nejen bezpečnostní opatření technická (tj. bezpečnostní kryty kamer, umístění záznamového zařízení do uzamykatelného prostoru, šifrování dat), ale i organizační (tj. školení oprávněných osob, řízený přístup k datům, vedení záznamů o předání nahrávek oprávněným orgánům) (viz 4.2.1.2 a 4.2.3).

Cenová kalkulace kamerového systému demonstrována na konkrétním bytovém domě prokázala, že pořízení kompletního kamerového systému včetně instalace a oživení systému vychází řádově na statisíce korun českých, přičemž s každou další přidanou kamerou se cena zvyšuje, zvlášť když při prvotní instalaci kamerového systému není o případném budoucím rozšíření uvažováno. Cenu za pořízení kamerového systému může také zvyšovat instalace a používání stále modernějších technologií, např. kamery v přístupových systémech či vstup na biometrický údaj (otisk prstu). Kromě nákladů za pořízení kamerového systému musíme také uvažovat o pravidelných nákladech (zpravidla měsíčních) na jeho provoz, zejména servis, příp. obsluhu. Tyto náklady se pak pohybují v rozmezí mezi 1.000 - 2.000,- Kč (viz 4.2.2).

Každý správce musí mj. dodržovat určitá pravidla stanovená GDPR pro zpracování osobních údajů a obzvláště musí při instalaci kamer rozlišit míru soukromí v jednotlivých prostorech bytového domu (viz 4.2.1.2). O činnostech zpracování osobních údajů musí vyhotovovat písemné záznamy, které obsahují mj. i lhůtu pro výmaz, u které musí být uvedena doba ve dnech, po kterou jsou záznamy uchovány, rovněž odůvodnění této doby zpracování a následný způsob likvidace těchto záznamů. U bytových domů se doporučená doba uchování pohybuje okolo sedmi dnů, jelikož převážná většina kamerových systémů v bytových domech funguje na principu časové smyčky, což znamená, že po uplynutí stanovené doby dochází k automatickému přepisu záznamů. V případě zachycení nějakého incidentu výše zmíněné neplatí a záznam je uchován po dobu nebytně nutnou k jeho vyšetření (viz 4.3.2). Neměnná zůstává i informační povinnost vůči obyvatelům a návštěvníkům domu, došlo pouze k rozšíření informací, které musí být uvedeny na informačních tabulkách (viz 3.5.1.2.3). Nově na provozovatele kamerového systému v bytových domech spadá ohlašovací povinnost v případě úniku dat (viz 4.3.2), a naopak se jich netýká povinnost posouzení vlivu na ochranu osobních údajů a povinnost jmenovat pověřence pro ochranu osobních údajů (viz 3.5.2.2.5).

V rámci řízeného rozhovoru bylo zjištěno několik závažných pochybení ze strany provozovatele bytového domu, ve kterém dotazovaný respondent žije, a několik dalších drobných nedostatků. Závažné pochybení bylo zjištěno v již několikrát zmiňovaném a především velmi sporném nastavení úhlu záběru kamer, které sledují venkovní prostranství. V daném případě byl

upřednostněn zájem provozovatele před případnými tahanicemi z neoprávněného sledování na úkor objasnění trestného činu krádeže. Drobné nedostatky byly zjištěny v případě informační povinnosti, kdy dle mého názoru nebyly zcela aktualizovány informační tabulky tak, aby splňovaly požadavky GDPR. Trochu znepokojující zjištění vyplynulo i z odpovědí na otázky zaměřené na znalost práv subjektu údajů. Dotazovaný respondent potvrdil znalost pouze tří z devíti možných práv. Podobná neznalost se dle mého názoru dá očekávat i u ostatních subjektů údajů, což může mít negativní dopad při zpracování osobních údajů, zejména jedná-li se o zneužívání neznalosti práv. Jelikož se dá předpokládat, že pokud práva nejsou subjektu známa, pravděpodobně jich nikdy nevyužije (viz 4.3).

V současné době se v legislativním procesu nachází návrh českého adaptačního zákona, který bude přijat právě v souvislosti s přímou použitelností nařízení GDPR, a který bude upravovat některé dílčí záležitosti nutné k dotvoření celého právního rámce ochrany osobních údajů na vnitrostátní úrovni (viz 3.4.3.1).

5.3 Návrh adaptačního zákona k GDPR

Jak již bylo v kapitole 3.4.2.1 řečeno ZoOU, jakožto obecný právní předpis ochrany osobních údajů v ČR, byl v květnu 2018 nahrazen GDPR, a protože GDPR poskytuje členským státům určitý prostor ke stanovení vlastních pravidel, tak i zatím chybějícím českým „adaptačním“ zákonem. Ve většině evropských zemí zákonodárci adaptační zákony ke GDPR před nebo těsně po jeho účinnosti schválili, ovšem jak už je u nás letitým zvykem, naši zákonodárci schválit klíčovou normu včas nestihli. To, že ČR nemá adaptační zákon přijatý, ovšem na platnosti GDPR nic nemění, jelikož GDPR je přímo použitelné a to i bez přijatých národních prováděcích předpisů. Pouze české právnické i fyzické osoby se musí od začátku řídit GDPR v jeho základní, nejtvrdší podobě. I přes přímou aplikovatelnost GDPR, je tedy nezbytné stávající právní předpis ZoOU upravit zásadním způsobem. Rozhodovalo se mezi novelizací nebo přípravou zcela nového předpisu, a nakonec byl 18. srpna 2017 zveřejněn zcela nový návrh zákona o ochraně osobních údajů (tj. adaptační zákon) i návrh změn dotčených zákonů. Gestorem implementace je Ministerstvo vnitra. Návrh adaptačního zákona se nyní nachází v legislativním procesu, konkrétně ve třetím čtení a veřejnosti je již dostupný.

Návrh adaptačního zákona upravuje především ta ustanovení, ve kterých je dána členským státům při volbě vhodné právní úpravy možnost vlastního uvážení. Mezi nejzásadnější změny v kontextu s ochranou osobních údajů lze považovat problematiku přestupků uvedenou také v kapitole 3.4.2.7, kde v návrhu adaptačního zákona došlo k razantnímu snížení sankcí (horní

hranici pokuty pro orgány veřejné moci stanovuje ve výši 10 milionů korun českých a pro podnikatelské subjekty až do výše 20 milionů korun). Další změny se pak z hlediska ochrany osobních údajů týkají výjimek pro média a pro vědu, výzkum či statistické účely a pro správu vlastních zájmů. Také vzhledem ke zrušení registrační povinnosti (viz kapitola 3.4.3.5.2.1) by v rámci ÚOOÚ měly postupně zaniknout registry zpracování osobních údajů.[247]

6 Závěr

V průběhu posledního desetiletí se zavádění kamerových systémů stalo doslova fenoménem. Jedná se především o maximální využití dostupných technologií, které umožnují monitorovat pohyb kolem nás, a zajištují tak ochranu majetku, osob a zdraví (viz 3.3.1).

Kamerový systém je definován jako automaticky provozovaný stálý technický systém, který umožňuje pořizovat a uchovávat obrazové a zvukové záznamy (viz 3.2.1). V počátcích vývoje byly kamerové systémy pouze analogové, ovšem postupně byly a jsou vytlačovány IP kamerami. Princip fungování mezi nimi je velmi podobný a liší se pouze v použitých technologiích a přenosových médiích (viz 3.3.1.1). Dále rozlišujeme kamerový systém bez záznamu a kamerový systém se záznamem. Z pohledu zákona je ale mezi nimi zásadní rozdíl, zejména v předpisech, kterými se jejich instalace a provozování řídí (viz 3.3.1.2). Kamerový systém bez záznamu je v praxi využíván jen výjimečně, jelikož připojení a odpojení záznamu ke kamerovému systému je v dnešní době už poměrně jednoduchou záležitostí. Pořízení a následné provozování kamerového systému ovšem není vůbec levnou záležitostí, i vzhledem k tomu, že do určité míry nahrazuje selhání lidského faktoru.

Ochranu osobnosti v ČR upravuje zejména občanský zákoník, který rozvádí základní práva obsažená v ústavních zákonech. Osobnost člověka je tedy chráněna včetně všech jeho přirozených práv, které mj. zahrnují i právo člověka se podle svého uvážení rozhodnout, zda a v jakém rozsahu či jakým způsobem mají být skutečnosti jeho osobního soukromí zpřístupněny jiným. Z čehož vyplývá, že jakékoli narušení soukromých prostor člověka, sledování a pořizování zvukových či obrazových záznamů o jeho soukromém životě lze provádět pouze s jeho souhlasem (viz 3.4.2).

Naopak ochranu osobních údajů upravuje nově GDPR, které tak po více jak dvaceti letech nahradilo dosavadní evropskou Směrnici 95/46/ES a podstatnou část ZoOU. GDPR je tak

[247] Rozdílová tabulka návrhu právního předpisu s předpisy EU [online]. In: Aplikace ODok, 2018 [cit. 2018-11-21]. Dostupná z: https://apps.odok.cz/veklep-detail?p_p_id=material_WAR_odokkpl&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=3&_material_WAR_odokkpl_pid=KORNAQCDZPW5&tab=detail

v současnosti nejkomplexnějším nařízením chránící soukromí občanů EU, jehož hlavním cílem je maximálně hájit práva občanů EU zejména proti neoprávněnému zacházení s jejich osobními údaji (viz 3.4.2.1).

Při instalaci a následném zprovoznění kamerového systému je třeba dbát na příslušná ustanovení OZ (viz 3.5.2.1) a GDPR (viz 3.5.2.2), přihlédnout by se však mělo také na právní názory a stanoviska dozorového úřadu - ÚOOÚ. GDPR základní zásady zpracování osobních údajů či základní pojmy nijak nemění (naopak se ve většině shoduje s OZ) a ani nerozšiřuje svoji působnost oproti předešlé právní úpravě, pouze pro některá zpracování, resp. subjekty, klade vyšší nároky při zpracování osobních údajů (viz 3.4.3.3) a výrazně posiluje práva subjektů údajů (viz 3.4.3.5.3). Pokud jde o stanovení práv a povinností, tak není mezi nařízením a zákonem de facto rozdíl (3.4.3.5). Jednou ze základních zásad je mj. i souhlas subjektu údajů (viz 3.4.3.4). Nikoli překvapivým faktem nadále je, že není vždy nutné vyžadovat po monitorovaných osobách jejich souhlas s tím, aby mohly být natáčeny. Stejný princip má i OZ v ustanoveních § 84 – § 88, proto může zpracování probíhat i bez souhlasu, pokud je to nezbytné pro účely oprávněných zájmů správce či třetí strany (viz 3.4.2). Hlavní povinností správce je tedy dodržovat základní zásady (viz 3.4.3.3) a další (nové) povinnosti (viz 3.4.3.5.2) Za nedodržení nebo porušení některé z povinností můžou být správci nebo provozovatelé sankciováni.

Kamerové sledování nesmí nadměrně zasahovat do soukromí monitorovaných osob, jelikož pak může docházet a mnohdy i dochází k rozporu hned několika práv (viz 3.5.2.1). Kamerový systém nelze umístit na každém místě, proto každá kamera musí být nainstalována a „zacílena“ dle podmínek OZ a GDPR (viz 3.5.2). Navíc je jeho instalace a provoz možný pouze je-li sledovaný účel legitimní (viz 3.5.2.2.1). Jelikož možná kolize může nastat i mezi právy užití kamerového systému a principy ochrany osobních údajů, musí být vyjasněno, jaké kamery GDPR podléhají, kdy se jedná o systém zpracovávající osobní údaje, a kdy se ze zpracovávané informace stává osobní údaje příp. zvláštní kategorie osobních údajů (viz 3.5.2.2). Subjekt údajů může vůči správci kdykoli uplatnit svá práva a správce na tuto eventualitu musí být připraven (např. tím, že dokáže soulad zpracování jeho osobních údajů s účelem zpracování, příp. dokáže subjektu údajů sdělit veškeré požadované informace).

Mezi nejčastějšími důvody instalace a provozování kamerového systému v bytových domech je zejména ochrana proti majetkové kriminalitě a vandalismu. Jedná se zřejmě o prvek účinný, protože dle statistik počet trestných činů krádeží vloupáním do bytů klesá (viz 4.2.1.1). V bytovém domě pak z hlediska provozování kamerového systému a z hlediska míry soukromí rozlišujeme dvě skupiny prostor, podle nichž je odvozena také míra souhlasu, a je tedy vždy nutné

k povaze prostor při instalaci kamerového systému přihlédnout (viz 4.2.1.2). Cenu za pořízení a provoz, která se i v případě bytových domů pohybuje ve výši statisíců, zvyšuje každé další rozšíření systému a také instalace modernějších technologií (viz 4.2.2). Je na každém, zda a do jaké míry bude selhání lidského faktoru nahrazovat předraženým bezpečnostním zabezpečením.

Pravidla, které musí správci kamerových systémů v bytových domech dodržovat, se nijak neliší od výše zmíněných práv a povinností ukládaných při provozování kamerových systémů jako takových (a také viz 4.2.3).

Na základě řízeného rozhovoru bylo zjištěno několik pochybení ze strany provozovatele bytového domu, ve kterém dotazovaný respondent žije. Jednalo se zejména o špatné nastavení úhlu kamery snímající venkovní prostranství v blízkosti domu (docházelo k neoprávněnému sledování) a drobné nedostatky v plnění informační povinnosti. Vzhledem k povaze těchto pochybení lze usoudit, že se rozhodně nejedná o jediný bytový dům, který se s takovými problémy může potýkat. Bohužel jsou tyto skutečnosti odhaleny až v případě, když se vážnější incident skutečně stane, což může jeho vyšetřování nejen znesnadnit, ale dokonce může být ještě proti provozovateli vzneseno obvinění za neoprávněné sledování a shromažďování osobních údajů. Za znepokojující lze považovat i neznalost subjektu údajů ohledně všech svých práv (viz 4.3).

Celý právní rámec bude navíc dotvářet adaptační zákon, jehož obsahem budou i drobné (povolené) odchylky či zvláštní úpravy k GDPR. Zejména se bude jednat o razantní snížení sankcí v případě porušení či nedodržení některých z povinností a z hlediska ochrany osobních údajů o změny v podobě výjimek pro média, vědu, výzkum, statistické účely a pro správu vlastních zájmů. Bude se tedy jednat pouze o doplňkový zákon k obecnému nařízení, dotvářející komplexní úpravu ochrany osobních údajů při jejich zpracování. Návrh adaptačního zákona je již v legislativním procesu (viz 5.3).

7 Seznam použitých zdrojů

7.1 Literární zdroje

BARTÍK, Václav, JANEČKOVÁ, Eva. *Kamerové systémy v praxi*. Praha: Linde, 2011, 240 s. ISBN 978-80-7201-850-5

JANEČKOVÁ, Eva. *GDPR. Praktická příručka implementace.* Praha: Wolters Kluwer ČR, a. s., 2018, s. 136. ISBN 978-80-7552-248-1

KADLECOVÁ, Marta, SCHELLE, Karel, VESELÁ, Renata, VLČEK, Eduard. V*ývoj českého soukromého práva, edice právní dějiny.* Praha: Eurolex Boheia, s. r. o., 2004, s. 213. ISBN 80-86432-83-1

KNAP, Karel, ŠVESTKA, Jiří, JEHLIČKA, Oldřich, PAVLÍK, Pavel, PLECITÝ, Vladimír. *Ochrana osobnosti podle občanského práva.* 4. podstatně přepracované a doplněné vydání. Praha: Linde Praha, 2004, 440 s. ISBN 80-7201-484-6

KUČEROVÁ, Alena, NOVÁKOVÁ, Ludmila, FOLDOVÁ, Vanda, NONNEMANN, František, POSPÍŠIL, Daniel. *Zákon o ochraně osobních údajů.* Komentář. 1. Vydání. Praha: C. H. Beck, 2012, 536 s. ISBN 978-80-7179-226-0

MATOUŠKOVÁ, Miroslava, HEJLÍK, Ladislav. *Osobní údaje a jejich ochrana*. 2. doplněné a aktualizované vydání. Praha: ASPI, 2008. ISBN 978-80-7357-322-5

MELZER, Filip, TÉGL, Petr, a kol. *Občanský zákoník – velký komentář. Svazek I (§ 1 – 117).* Praha: Leges, s. r. o., 2013, 720 s. ISBN 978-80-8757-673-1

NEZMAR, Luděk. *GDPR: Praktický průvodce implementací*. Praha: Grada Publishing, a.s., 2017, 304 s. ISBN 978-80-271-0668-4

PLECITÝ, Vladimír. *Problematika ochrany osob a majetku z pohledu soukromého a veřejného práva.* Vyd. 1. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2010, 139 s. ISBN 978-80-7380-247-9

POMAIZLOVÁ, Karin, FÜRSTOVÁ, Monika. *GDPR – revoluce, nebo rozvedení stávajícího?* In: Bulletin advokacie. Praha: Česká advokátní komora, 2017, roč. 2017, č. 9, 90 s. ISSN 1210-6348 [online]. [cit. 2018-02-27]. Dostupné také z: http://www.bulletin-advokacie.cz/assets/zdroje/casopis/2016/BA_9_2017_web.pdf

SEDLÁKOVÁ, Renáta. *Výzkum médií: nejužívanější metody a techniky*. Praha: Grada, 2015, Žurnalistika a komunikace, 544 s. ISBN 978-80-247-3568-9

ŠVESTKA, Jiří, DVOŘÁK, Jan, FIALA, Josef. *Občanský zákoník. Komentář. Svazek I (§ 1 – 654).* Praha: Wolters Kluwer ČR, a. s., 2014, 1736 s. ISBN 978-80-7478-370-8

ŽŮREK, Jiří. *Praktický průvodce GDPR*. 2. aktualizované vydání. Praha: ANAG, 2018, 344 s. ISBN 978-80-7554-152-9

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. [cit. 2018-02-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1542210767963&uri=CELEX:32016R0679

Obecný zákoník občanský č. 946/1811 Sb. z. s., ve znění pozdějších předpisů

Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů [online]. [cit. 2018-02-27]. Dostupná z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:31995L0046&from=CS

Ústavní zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpisů

Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů

Vykls poř. č. 10/2003 Sb., k zákonnosti umístění audio-vizuálních prostředků ve školských zařízení vykonávajících ústavní výchovu a ochranou výchovu. Dostupné v systému ASPI, 2012, ID: LIT23204CZ

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

Zákon č. 87/1990 Sb., kterým se mění a doplňuje zákon č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů

Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů

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

7.2 Internetové zdroje

ČESKÝ STATISTICKÝ ÚŘAD. Kriminalita – trestné činy. Statistiky [online]. In: czso.cz, 2018 [cit. 2018-11-11]. Dostupné z: https://vdb.czso.cz/vdbvo2/faces/cs/index.jsf?page=vystup-objekt-parametry&z=T&f=TABULKA&katalog=31008&pvo=KRI05&sp=A&evo=v104_%21_KRI05-H-6065_1&str=v32

Elnika.cz: IP systémy [online]. Praha: Elnika plus, s. r. o. [cit. 2018-02-10]. Dostupné z: https://www.elnika.cz/cz/podpora/pruvodce-kamerovym-systemem/ip-systemy/

CHWISTKOVÁ, Karla. Náš život před kamerou aneb Kamerové systémy v praxi [online]. 2016 [cit. 2018-11-07]. Dostupné z: http://www.hajduk.cz/nas-zivot-pred-kamerou-aneb-kamerove-systemy-v-praxi/

Kamerové a zabezpečovací systémy [online]. [cit. 2018-11-05]. Dostupné z: http://www.chran.cz/kamery-do-bytovych-domu/

Kamerová technika.cz: Kamerové systémy a zákony [online]. Brno: KamerováTechnika.cz, 2018 [cit. 2018-02-27]. Dostupné z: http://kamerovatechnika.cz/legislativa.html

NOVÁK, Vladimír. Kamerový systém. In: Ladinn [online]. Tišnov: ELKOV elektro, 2014 [cit. 2018-01-16]. Dostupný z: http://www.ladinn.cz/ostatni/technika/kamerovy_system.html

OCHRANA OSOBNÍCH ÚDAJŮ. Srovnání nařízení GDPR a zákona o ochraně osobních údajů [online]. [cit. 2018-11-03]. Dostupné z: http://www.oou.cz/gdpr/srovnaniGDPR

Rozdílová tabulka návrhu právního předpisu s předpisy EU. In: Aplikace ODok [online]. 2018 [cit. 2018-11-21]. Dostupná z: https://apps.odok.cz/veklep-detail?p_p_id=material_WAR_odokkpl&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=3&_material_WAR_odokkpl_pid=KORNAQCDZPW5&tab=detail

Stanovisko č. 1/2006 - Provozování kamerového systému z hlediska zákona o ochraně osobních údajů [online]. In: uoou.cz, Leden 2006 [cit. 2018-02-27]. Dostupné z: https://www.uoou.cz/files/stanovisko_2006_1.pdf

Stanovisko č. 1/2016 – K umístění kamerových systémů v bytových domech [online]. In: uoou.cz, Leden 2016 [cit. 2018-03-27]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=29566

ŠKORNIČKOVÁ, Eva. Citlivé osobní údaje [online]. In: gdpr.cz [cit. 2018-10-10]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/citlive-osobni-udaje/

ŠKORNIČKOVÁ, Eva. Proč potřebuje Evropa lepší ochranu osobních dat [online]. In: gdpr.cz [cit. 2018-11-02]. Dostupné z: https://www.gdpr.cz/gdpr/proc/

ŠKORNIČKOVÁ, Eva. Záznamy o činnostech zpracování [online]. In: gdpr.cz [cit. 2018-11-01]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/zaznamy-o-cinnostech-zpracovani/

ŠKORNIČKOVÁ, Eva. GDPR a kamerové systémy [online]. In: gdpr.cz [cit. 2018-11-03]. Dostupné z: https://www.gdpr.cz/blog/gdpr-a-kamerove-systemy/

TAHOTNÁ, Lucie. Kamerové systémy z hlediska ochrany osobních údajů [online]. In: epravo.cz, 2017 [cit. 2018-10-25]. Dostupné z: https://www.epravo.cz/top/clanky/kamerove-systemy-z-hlediska-ochrany-osobnich-udaju-106300.html?mail

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Na aktuální téma – Archiv. Komentář k Zásadám provozování kamerového systému z hlediska zákona o ochraně osobních údajů [online]. In: uoou.cz, Leden 2006 [cit. 2018-02-27]. Dostupný z: https://www.uoou.cz/vismo/zobraz_dok.asp?id_ktg=1103&p1=1103#kamery

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. K provozování kamerových systémů [online]. In: uoou.cz, 2018 [cit. 2018-10-25]. Dostupné z: https://www.uoou.cz/k-nbsp-provozovani-kamerovych-systemu/d-29535/p1=1099

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Základní příručka k GDPR [online]. In: uoou.cz [cit. 2018-10-12]. Dostupná z: https://www.uoou.cz/zakladni%2Dprirucka%2Dk%2Dgdpr/ds-4744/p1=4744

8 Přílohy

8.1 Příloha č. 1

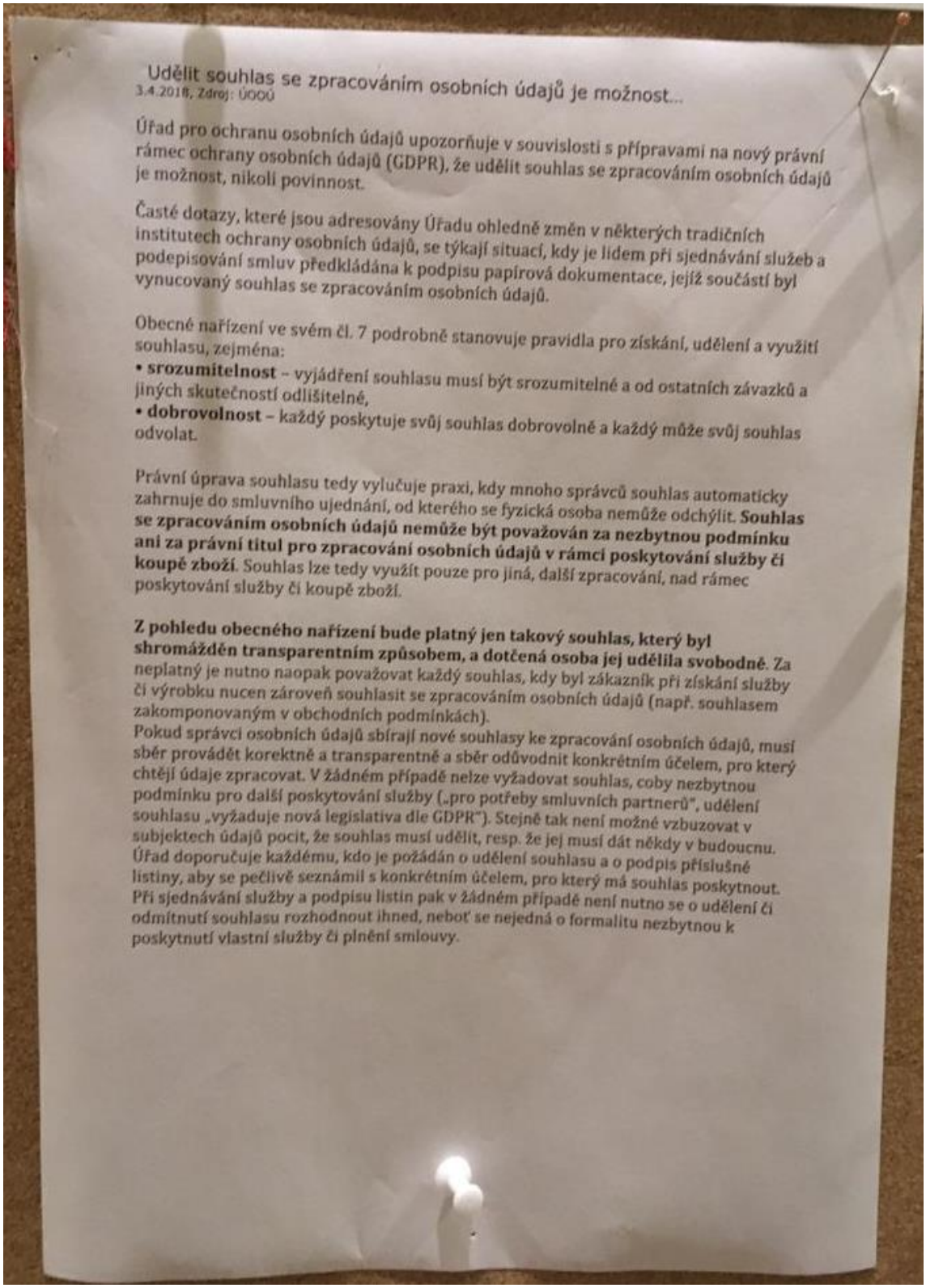
Příloha č. 1 - Záznam o zpracování (možný vzor)

ZÁZNAM O ZPRACOVÁNÍ č. ..... (kamerový systém)	
Správce	*Název společnosti, adresa sídla společnosti, identifikační číslo a kontaktní osoba či jméno případně jmenovaného pověřence.* Společnost XYZ s.r.o. Bezejmená ulice 1234, 100 00 Praha IČ: 123456789 Kontaktní osoba: Josef Chytrý
Účel zpracování	*Zákonný účel pro nasazení kamerového systému.* Ochrana majetku správce a ochrana života a zdraví osob pohybujících se ve sledovaném prostoru.
Právní důvod	Oprávněné zájmy správce a třetích stran *(čl. 6 odst. 1 písm. f)*
Popis kategorií subjektů údajů	*Skupiny osob pohybující v monitorovaném prostoru.* Zákazníci, zaměstnanci a další osoby vstupující do monitorovaného prostoru *(návštěvy, dodavatelé)*.
Popis kategorií osobních údajů	Vizuální, případně zvukové *(pokud využíváte)*, identifikační údaje ve formě kamerového záznamu.
Informace poskytované subjektům údajů	*Způsoby upozornění na instalovaný kamerový systém a způsob seznámení zaměstnanců s jeho existencí.* Na používání kamerového systému upozorňují piktogramy, které jsou umístěny na vstupu do zaznamenávaného prostoru. Piktogramy obsahují vedle symbolu kamery také slovní upozornění na monitoring prostoru, identifikaci správce údajů a sdělení, kde lze získat další, podrobnější informace.
Příjemci osobních údajů	*Veškeré pravděpodobné instituce či osoby, které mohou obdržet pořízený kamerový záznam.* Zákazníci Zaměstnanci Další osoby vstupující do monitorovaného prostoru *(návštěvy, dodavatelé)* Subjekt údajů, vyžadující informace o zpracovaných údajích. V odůvodněných případech organy činné v trestním řízení Jiné zainteresované subjekty pro naplnění účelu zpracování *(pojišťovna)*. Nejsou plánovaní příjemci údajů mimo země EU.

Lhůta pro výmaz	*Doba pořizování záznamu ve dnech včetně jejich následného způsobu likvidace. Rovněž odůvodnění této doby zpracování.* Doba uchování záznamu je 7 dní. Následně dochází k jejich automatické likvidaci. Doba uchování osobních údajů je přiměřená vzhledem k účelu jejich zpracování. Řešený zachycený incident je uchován po nezbytnou dobu.
Technická a organizační opatření	*Veškerá dostupná opatření, které jsou využívány pro zabezpečení kamerových záznamů. Podrobnější informace je možné také uvést ve „Vnitřním předpise o provozu kamerového systému", která by měla být přílohou tohoto záznamu.* Bezpečnostní kryt kamery Šifrovaný přenos dat Šifrovaná uložiště dat Řízení přístupu k datům Školení oprávněných osob Vedení předávacích protokolů třetím osobám
Počet zapojených kamer	*Počet instalovaných kamer v dané lokalitě.* 8
Objekt umístění kamer	*Název a adresa sledované lokality včetně slovního popisu rozmístění kamer. K záznamu rovněž dodat formou přílohy schéma rozmístění kamer.* Prodejna XXXXXX na adrese YYYYY Prodejní prostory včetně vstupních míst a skladové prostory. Viz. příloha tohoto záznamu.
Režim kamer	*Časový harmonogram a způsob pořizování kamerového záznamu. Tedy zda se jedná o nepřetržité nahrávání (24/7) nebo zda je záznam pořizován například pouze v pracovní době. Rovněž uvést, zda se jedná o prostý záznam bez využití analytiky typů softwarové porovnání biometrických údajů a jiných či zda je tato video analytika využívána.* Nepřetržitý, tj. v režimu 24/7. *(alternativně např. uvést záznam v provozní době, záznam mimo provozní dobu atd.)* Jedná se o prostý záznam bez využití analytiky typu softwarové porovnání biometrických údajů a jiných.
Zpracovatel	Nevyužívá se *(pokud by se využíval, tak jej identifikovat)*

8.2 Příloha č. 2

Příloha č. 2 - Obecné poučení o udělení souhlasu vyvěšené na domovní nástěnce v bytovém domě



Udělit souhlas se zpracováním osobních údajů je možnost...
3.4.2018, Zdroj: ÚOOÚ

Úřad pro ochranu osobních údajů upozorňuje v souvislosti s přípravami na nový právní rámec ochrany osobních údajů (GDPR), že udělit souhlas se zpracováním osobních údajů je možnost, nikoli povinnost.

Časté dotazy, které jsou adresovány Úřadu ohledně změn v některých tradičních institutech ochrany osobních údajů, se týkají situací, kdy je lidem při sjednávání služeb a podepisování smluv předkládána k podpisu papírová dokumentace, jejíž součástí byl vynucovaný souhlas se zpracováním osobních údajů.

Obecné nařízení ve svém čl. 7 podrobně stanovuje pravidla pro získání, udělení a využití souhlasu, zejména:
• **srozumitelnost** – vyjádření souhlasu musí být srozumitelné a od ostatních závazků a jiných skutečností odlišitelné,
• **dobrovolnost** – každý poskytuje svůj souhlas dobrovolně a každý může svůj souhlas odvolat.

Právní úprava souhlasu tedy vylučuje praxi, kdy mnoho správců souhlas automaticky zahrnuje do smluvního ujednání, od kterého se fyzická osoba nemůže odchýlit. **Souhlas se zpracováním osobních údajů nemůže být považován za nezbytnou podmínku ani za právní titul pro zpracování osobních údajů v rámci poskytování služby či koupě zboží**. Souhlas lze tedy využít pouze pro jiná, další zpracování, nad rámec poskytování služby či koupě zboží.

Z pohledu obecného nařízení bude platný jen takový souhlas, který byl shromážděn transparentním způsobem, a dotčená osoba jej udělila svobodně. Za neplatný je nutno naopak považovat každý souhlas, kdy byl zákazník při získání služby či výrobku nucen zároveň souhlasit se zpracováním osobních údajů (např. souhlasem zakomponovaným v obchodních podmínkách).
Pokud správci osobních údajů sbírají nové souhlasy ke zpracování osobních údajů, musí sběr provádět korektně a transparentně a sběr odůvodnit konkrétním účelem, pro který chtějí údaje zpracovat. V žádném případě nelze vyžadovat souhlas, coby nezbytnou podmínku pro další poskytování služby („pro potřeby smluvních partnerů", udělení souhlasu „vyžaduje nová legislativa dle GDPR"). Stejně tak není možné vzbuzovat v subjektech údajů pocit, že souhlas musí udělit, resp. že jej musí dát někdy v budoucnu. Úřad doporučuje každému, kdo je požádán o udělení souhlasu a o podpis příslušné listiny, aby se pečlivě seznámil s konkrétním účelem, pro který má souhlas poskytnout. Při sjednávání služby a podpisu listin pak v žádném případě není nutno se o udělení či odmítnutí souhlasu rozhodnout ihned, neboť se nejedná o formalitu nezbytnou k poskytnutí vlastní služby či plnění smlouvy.