Ochrana osobních údajů v kontextu audiovizuálních záznamů

Bc. Jakub Němec

Diplomová práce
2021

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva

Akademický rok: 2020/2021

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Jakub Němec**
Osobní číslo:	**L19389**
Studijní program:	**N1032A020002 Bezpečnost společnosti**
Studijní obor:	**Ochrana obyvatelstva**
Forma studia:	**Prezenční**
Téma práce:	**Ochrana osobních údajů v kontextu audiovizuálních záznamů**

Zásady pro vypracování

1. Zpracujte literární rešerši vztahující se k dané problematice s důrazem na monografie.
2. Analyzujte současnou právní úpravu ochrany osobních údajů v kontextu pořizování audiovizuálních záznamů.
3. Analyzujte právní aspekty implementace kamerových systémů do vybraného objektu.
4. Vytvořte prostorový model vybraného objektu.
5. Na základě vytvořeného prostorového modelu navrhněte řešení implementace kamerových systémů do vybraného objektu v souladu s platnými zákony České republiky.

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. SHARMA, Sanjay. *Data Privacy and GDPR Handbook*. Hoboken: Wiley, 2020. ISBN 978-1119594246.
2. WRAY, Darren. *The little book of GDPR*. United States: Independently published, 2017. ISBN 978-1522021148.
3. ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. ISBN 9788075541529.

Další odborná literatura dle doporučení vedoucího diplomové práce.

Vedoucí diplomové práce: **Ing. Petr Svoboda, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání diplomové práce: **1. prosince 2020**
Termín odevzdání diplomové práce: **14. května 2021**

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2020

PROHLÁŠENÍ AUTORA
DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 25. 7. 2021

Jméno a příjmení studenta: Bc. Jakub Němec

…….
podpis studenta

ABSTRAKT

Tato práce je zaměřena na problematiku ochrany osobních údajů v kontextu audiovizuálních záznamů. V teoretické části se práce věnuje definici základních pojmů a výčtu právních dokumentů a předpisů. Dále je popsán vývoj ochrany osobních údajů v České republice a ve světě. Na závěr teoretické části je definována ochrana osobních údajů v kontextu audiovizuálních záznamů. Z praktického hlediska práce vysvětluje základní zásady pro správný provoz kamerových systémů a jejich implementace do modelů domů s názornou ukázkou možného umístění kamer. V další části se práce věnuje dotazníkovému šetření, které zjišťuje pohled obyvatelstva na problematiku ochrany osobních údajů a kamerových systémů. V poslední kapitole práce je navržena interaktivní prezentace pro lepší orientaci v dané problematice a doporučeny programy pro snadnější pořízení kamerového systému.

Klíčová slova: GDPR, kamerové systémy, model ochrana, osobní údaje, soukromí

ABSTRACT

This work is focused on the issue of personal data protection in the context of audiovisual recordings. The theoretical part deals with the definition of basic concepts and a list of legal documents and regulations. Furthermore, the development of personal data protection in the Czech Republic and in the world is described. At the end of the theoretical part, the protection of personal data in the context of audiovisual recordings is defined. From a practical point of view, the work explains the basic principles for the proper operation of camera systems and their implementation in house models with a clear example of the possible location of cameras. In the next part, the work is devoted to a questionnaire survey, which finds out the view of the population on the issue of personal data protection and camera systems. In the last chapter, an interactive presentation is proposed for better orientation in the issue and recommended programs for easier acquisition of a camera system.

Keywords: camera systems, GDPR, model, personal data, privacy, protection

Rád bych poděkoval svému vedoucímu Ing. Petru Svobodovi Ph.D. za cenné rady, jeho ochotu a věnovaný čas. Velké díky patří také mé rodině za možnost studovat a jejich podporu po celou dobu studia. A na konec chci poděkovat všem svým přátelům, za pomoc během psaní této závěrečné práce, za motivaci a cenné životní zkušenosti a hlavně za krásné roky studia strávených v Uherském Hradišti.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Problematika ochrany osobních údajů je součást života každého člověka pohybujícího se v moderním světě. Města jsou plná kamerových systémů, které dohlížejí na veřejné prostranství, na většině dnešních rodinných domů je instalována kamera pro zajištění bezpečí a dohledu nad pozemkem, v obchodech je člověk obklopen informačními cedulemi upozorňující na kamerové systémy, které zaznamenávají dění v daném prostou. Kamerové systémy a ochrana osobních údajů jsou dvojicí pojmů, které nás každý den potkávají a my s nimi musíme umět správně naložit. Je tedy důležité se v problematice ochrany osobních údajů vyznat a vědět jaké jsou práva a povinnosti ať už obyčejných lidí, co se prochází po veřejném prostranství, anebo správců zpracovávající obří množství informací získaných z kamer.

Ochrana osobních údajů je v dnešní době často zmiňovaným pojmem a řešením témat týkajících se této problematiky se nevyhne prakticky žádný moderní člověk. Ochranu osobních údajů je potřeba řešit především z pohledu kamerových systémů, jejichž špatná instalace, zasahuje do citlivého soukromí ostatních lidí. Bohužel se v dnešní době setkáváme i s případy, kdy je takovéto protiprávní jednání úmyslné a získané záznamy z kamer jsou zneužívány například k vydírání. Téma ochrany osobních údajů je sice často diskutovaná v odborné společnosti, je ovšem potřeba o ní zvýšit povědomí především v laické části obyvatelstva.

V době, ve které žijeme, patří právo na ochranu osobních údajů při jejich zpracování mezi základní práva člověka a jeho zajištění je jedním z atributů právního státu. Toto právo, které je imanentní součástí práva na ochranu soukromí, se postupem času vyvíjelo do současné podoby. Postupem času vyvstala nutnost chránit nejen soukromí jako celek, ale v jeho rámci poskytnout zvláštní ochranu také dotčeným fyzickým osobám pří zpracování jejich osobních údajů, neboť zpracování osobních údajů začalo výrazně negativně zasahovat do soukromí člověka. Stále složitější a provázanější život lidí si žádal zpracování osobních údajů čím dál častěji a ve větším rozsahu, což je děje dodnes. Aktuální způsob života většiny obyvatel se neobejde bez využívání moderních zařízení, které často lidem ulehčují život a rozhodování ovšem za cenu omezení práva na jejich soukromí a často značně velkého využívání jejich osobních údajů. Samozřejmě je potřeba si svá práva na ochranu osobních údajů a soukromí potřeba chránit, a proto je nutné zvýšit povědomí o této problematice a zlepšit vědomosti obyvatelstva v tomto směru, aby často nedocházelo k nevědomému poskytování osobních údajů.

CÍL PRÁCE A POUŽITÉ METODY

Hlavní cíle

Hlavním cílem práce je analyzovat a objektivně shrnout stav problematiky ochrany osobních údajů, a to především v kontextu audiovizuálních záznamů.

Vedlejší cíle

Vedlejšími cíli práce je provést rešerši současného stavu ochrany osobních údajů v kontextu audiovizuálních záznamů. Dále objektivně shrnout pravidla týkající se problematiky osobních údajů a kamerových systémů a prakticky znázornit správné umístění monitorovacích zařízení. Dalším důležitým cílem práce je zjistit četnost nainstalovaných kamerových systémů na rodinných a bytových domech a následně analyzovat vztah obyvatelstva k problematice ochrany osobních údajů a úroveň znalostí v dané problematice u těchto respondentů. Mezi poslední vedlejší cíl práce patří navrhnutí opatření ke zlepšení znalostí a povědomí obyvatelstva o problematice ochrany osobních údajů v kontextu audiovizuálních záznamů.

Použité metody:

- **Analýza –** této metody bylo využito k rozboru právních dokumentů týkající se dané problematiky a při zkoumání vztahu obyvatelstva k problematice ochrany osobních údajů v kontextu audiovizuálních záznamů.
- **Syntéza –** díky této metodě byla provedena sumarizace informací získaných z právních dokumentů v oblasti ochrany osobních údajů k následnému využití při praktickém znázornění možného umístění kamerových systému na domech.
- **Komparace –** v práci bylo nutné porovnat několik právních dokumentů, a to především občanský zákoník a Obecné nařízení o ochraně osobních údajů (GDPR). Na základě porovnání došlo k získání informací potřebných pro správnou instalaci nastavení kamer na domech.
- **Explanace –** metoda byla použita především pro vysvětlení, jakým způsobem může být kamerový systém nainstalován a jaké náležitosti musí monitorování splňovat.
- **Modelování –** pro názorné zobrazení možných míst vhodných k instalaci kamerových systémů byly vytvořeny dva modely domu, a to rodinného a bytového.

- **Dotazování –** bylo využito k získání reálných informací o vztahu obyvatelstva k problematice ochrany osobních údajů v kontextu audiovizuálních záznamů.
- **Indukce a dedukce –** těmito metodami byly zpracovány informace a data z dotazníkového šetření a bylo tak vyvozeno, jaký postoj mají uživatelé kamerových systému vzhledem k ochraně osobních údajů a soukromí druhých osob. Dále bylo zjištěno, zda si jsou obyvatelé vědomi možného narušení ochrany osobních údajů a vlastního soukromí, a to především prostřednictvím kamerových systémů.
- **Sběr dat a informací** – těchto metod bylo v práci využito nejvíce, a to jak v teoretické části práce, tak i praktické.

I. TEORETICKÁ ČÁST

1 NÁZVOSLOVÍ A PRÁVNÍ DOKUMENTY

V základě je potřeba si vysvětlit některé důležité pojmy, které se týkají problematiky ochrany osobních údajů. Dalším důležitým bodem je seznámení s právními dokumenty, které tuto oblast ochrany upravují a definují její podstatu.

1.1 Základní pojmy

Níže jsou vypsány nejdůležitější základní pojmy, které se týkají oblasti ochrany osobních údajů. Velká část těchto pojmů je vysvětlená přímo v Obecném nařízení o ochraně osobních údajů. Mimo tyto pojmy, existují ještě další, které souvisí s danou problematikou a je potřeba si je definovat.

1.1.1 Výčet definic v Obecné nařízení o ochraně osobních údajů

Obecné nařízení obsahuje v čl. 4 výčet definic, se kterými je pro účely dalšího výkladu vhodné se seznámit, jelikož ovlivňují samotnou aplikaci Obecného nařízení (např. pojem osobní údaj, zpracování), ale i aplikaci některých povinností (např. definice porušení zabezpečení osobních údajů). Pro účely Obecného nařízení se rozumí:

- *„**osobními údaji**" veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů"); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, 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 osoby;*
- *„**zpracováním**" jakákoliv operace nebo soubor operací, které jsou prováděny s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení;". Je uváděn správný překlad definice, protože v českém překladu je pojem zpracování přeložen chybně;*
- *„**omezením zpracování**" označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu;*

- *„**evidencí**" jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska;*
- *„**správcem**" fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Evropské unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení;*
- *„**zpracovatelem**" fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce;*
- *„**příjemcem**" 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. Avšak orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu, se za příjemce nepovažuji; zpracování těchto osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany údajů pro dané účely zpracování;*
- *„**třetí stranou**" 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;*
- *„**souhlasem**" subjektu údajů jakýkoliv svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů;*
- *„**porušením zabezpečení osobních údajů**" porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů; „genetickými údaji" 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;*

- *„**biometrickými údaji**" osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, např. zobrazení obličeje nebo daktyloskopické údaje;*
- *„**relevantní a odůvodněnou námitkou**" námitka vůči návrhu rozhodnutí za účelem posouzení, zda došlo k porušení Obecného nařízení, nebo zda je zamýšlený úkon v souvislosti se správcem či zpracovatelem v souladu s Obecným nařízením, která jasně dokazuje významnost rizik vyplývajících z návrhu rozhodnutí, pokud jde o základní práva a svobody subjektů údajů, případně volný pohyb osobních údajů v rámci Evropské unie* (Nařízení Evropského parlamentu a rady, 2016/679).

1.1.2 Výčet ostatních definic

Bezpečnost

„Stav, kdy je systém schopen odolávat známým a předvídatelným vnějším a vnitřním hrozbám, které mohou negativně působit proti jednotlivým prvkům (případně celému systému) tak, aby byla zachována struktura systému, jeho stabilita, spolehlivost a chování v souladu s cílovostí. Je to tedy míra stability systému a jeho primární a sekundární adaptace.“ (Ministerstvo vnitra, 2019).

Informační bezpečnost

Jedná se ochranu informací ve všech jejich formách a po celý jejich životní cyklus – během jejich vzniku, zpracování, ukládání, přenosu a likvidace (Jirásek, Novák, Požár, 2015).

Citlivé osobní údaje

Citlivé osobní údaje jsou speciální kategorií podle obecného nařízení o ochraně osobních údajů (dále jen „GDPR“), která zahrnuje údaje o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém vyznání, členství v odborech, o zdravotním stavu, sexuální orientaci a trestních deliktech či pravomocném odsouzení osob. Tyto údaje mohou subjekt údajů samy o osobě poškodit ve společnosti, v zaměstnání, ve škole či mohou zapříčinit jeho diskriminaci. Do kategorie citlivých údajů GDPR nově zahrnuje genetické a biometrické údaje. Zpracování citlivých osobních údajů podléhá mnohem přísnějšímu režimu, než je tomu u obecných údajů (Citlivé osobní údaje, 2019).

1.2 Právní předpisy a dokumenty

Problematice ochrany osobních údajů se věnuje mnoho právních dokumentů.

Nejčastěji se jedná o zákony, ale existuje i mnoho nařízení:

- úmluva o ochraně lidských práv a základních svobod;
- zákon č. 89/2012 Sb., občanský zákoník;
- ePrivacy Regulation neboli nařízení o soukromí a elektronických komunikacích;
- sdělení č. 115/2001 Sb., m. s. Sdělení Ministerstva zahraničních věcí o přijetí Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat;
- zákon č. 110/2019 Sb., o zpracování osobních údajů;
- nařízení EU 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (Obecné nařízení o ochraně osobních údajů);
- směrnice Evropského parlamentu a rady (EU) 2016/680 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV, tzv. trestněprávní směrnice;
- listina základních práv a svobod, 2/1993 Sb;
- zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti);
- zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.

2 OCHRANA OSOBNÍCH ÚDAJŮ

Ochrana osobních údajů je v právních dokumentech zakotvená již delší dobu. V poslední době je její vývoj čím dál znatelnější a ochrana osobních údajů se tak stává jednou z věcí, se kterou se člověk setkává prakticky každý den.

2.1 Vývoj ochrany osobních údajů

V dnešní době je právo na ochranu osobních údajů základním právem každého člověka. Toto právo se postupem času vyvíjelo společně s moderní společností, a to jak v České republice, tak v celém světě. K jeho rozvoji dochází stále a každý den se stává důležitějším. Jak se toto právo historicky vyvíjelo bude popsáno níže.

2.1.1 Světový a evropský vývoj a stav

Prvním celosvětově významným mezinárodním dokumentem zaručujícím právo na soukromí byla Všeobecná deklarace lidských práv, přijatá v San Francisku v roce 1948 Valným shromážděním Organizace spojených národů. Tato deklarace v čl. 12 stanovovala mimo jiné zákaz vystavovat kohokoliv svévolnému zasahování do korespondence a soukromého života. Obdobně jako Všeobecná deklarace lidských práv zaručovala v čl. 8 právo na respektování rodinného a soukromého života Evropská úmluva o ochraně lidských práv a základních svobod sjednaná v roce 1950 v Římě. Tyto dva mezinárodní dokumenty deklarovaly právo na ochranu soukromí obecně, ale nevěnovaly se blíže právu na ochranu osobních údajů při jejich zpracování, které bylo v době přijetí těchto dokumentů přirozenou součástí práva na ochranu soukromí, protože okolnosti prozatím nenutily tuto oblast zvlášť vyčlenit. V průběhu několika let docházelo ke komplexnímu rozvoji společnosti včetně rozvoje automatizovaných prostředků, které byly postupně stále více využívány ke zpracování osobních údajů, vyvstala nutnost na tuto skutečnost speciálně reagovat, a tedy začít chápat ochranu osobních údajů při jejich zpracování jako samostatnou právní oblast, která zasluhuje zvláštní právní pozornost. V 70. a. 80. letech 20. století byly v některých zemích západní Evropy přijaty první vnitrostátní předpisy stanovující ochranu fyzickým osobám a pravidla při zpracování osobních údajů, a to především u států Rakousko, Francie, Lucembursko nebo Norsko. Například Španělsko, Portugalsko a Rakousko zase v této době zakotvily právo na ochranu osobních údajů dokonce i ústavně (Sharma, 2020).

Ačkoliv se při vyčleňování práva na ochranu osobních údajů při jejich zpracování jednalo o delší kontinuální časový proces, lze alespoň neformálně označit 28. leden 1981, kdy došlo k přijetí Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat (č. 115/2001 Sb. m. s.), za den, kdy se právo na ochranu osobních údajů při jejich zpracování osamostatnilo jako zvláštní část práva na ochranu soukromí. Tato úmluva, zkráceně nazývána jako Úmluva č. 108 definovala pojmy jako osobní údaj, automatizované zpracování nebo správce, zároveň vymezilo zvláštní skupiny údajů, stanovila zásady zpracování osobních údajů, nutnost osobní údaje zabezpečit a další hlediska týkající se automatizovaného zpracování. Za osobní údaj byla v Úmluvě č. 108 považována **jakákoliv informace týkající se identifikované, nebo identifikovatelné osoby (subjektu údajů). Tato definice osobního údaje po obsahové stránce přetrvává dodnes a nic na ní nemění ani Obecné nařízení**. Od přijetí úmluvy č. 108 nebylo po obsahové stránce nutné měnit ani pojmy správce či zpracování. Úmluvou č. 108 byly kladeny požadavky na kvalitu údajů a na to, aby byly získány a zpracovány poctivě s ohledem na legitimní účel a účelu přiměřeně. Součástí úmluvy bylo i ustanovení o nutnosti osobní údaje řádné zabezpečit. Úmluvou č. 108 byly položeny základy ochrany osobních údajů při jejich zpracování, na kterých stavěly další evropské dokumenty. Na počest přijetí Úmluvy č. 108, jakožto dokumentu s historickým významem, je považován **den 28. ledna za mezinárodní den ochrany osobních údajů** (Sharma, 2020).

Vývoj společnosti, především té západní, se v 80. a 90. letech 20. století ubíral mílovými kroky, svět se vlivem moderních dopravních prostředků neustále „zmenšoval", informace, včetně osobních údajů, se začaly v čím dál větším rozsahu zpracovávat automatizovaně, novými prostředky a nastalá nutnost předávat osobní údaje do třetích zemí byla jednou z projevů počínající globalizace. V evropském prostoru i s ohledem na fungování Evropské unie založené na volném pohybu osob, zboží a služeb (a s tím spojného pohybu osobních údajů) nastala potřeba rámcově sjednotit pravidla pro zpracování osobních údajů a jejich předávání do jiných států. Jednotlivé vnitrostátní právní úpravy, které byly přijímány v některých západoevropských zemích, již přestaly postačovat (Sharma, 2020).

Vyvstala tak nutnost regulovat zpracování osobních údajů takovým právním instrumentem, který by ochranu osobních údajů při jejich zpracování podrobně upravil jako celek, reflektoval by technologický vývoj od přijetí Úmluvy č. 108 a zároveň by právní úpravu v evropském prostoru alespoň částečné sjednotil. Tímto právním instrumentem se stala směrnice Evropské unie, konkrétně Směrnice Evropského parlamentu 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. V mnohém se inspirovala Úmluvou č. 108 a zároveň pojímala zpracování osobních údajů komplexně, jelikož se vztahovala jak na částečně nebo plné automatizované zpracování, tak nově i na neautomatizované zpracování osobních údajů. Ve Směrnici 95/46/ES se objevila i práva subjektu údajů, tj. pilíř současné právní úpravy v Evropské unii. Směrnice 95/46/ES tak je příkladem, jak vývoj společnosti a zejména využívaných při zpracování osobních údajů ovlivnil i výběr nového prostředků právního instrumentu pro regulaci zpracování osobních údajů v evropském prostoru. Pro směrnici, jakožto právní akt Evropské unie, je primárně charakterizující její harmonizační účinek na právní řády jednotlivých zemí Evropské unie, protože stanovuje členským státům Evropské unie, **čeho mají dosáhnout ve svých vnitrostátních řádech.** Nestanovuje však práva a povinnosti subjektům vnitrostátního práva přímo. Jednotlivým státům Evropské unie tedy vznikla povinnost přijmout do svých právních řádů adekvátní právní předpisy, které by odpovídaly požadavkům kladeným Směrnicí 95/46/ES. Je neoddiskutovatelné, že Směrnici 95/46/ES se v základních parametrech podařilo sjednotit právní rámec ochrany osobních údajů v evropském prostoru, nicméně jednotlivé státy si její provedení mnohdy vysvětlily po svém a v některých, a to i podstatných, ohledech se od sebe lišily (Žůrek, 2018; Sharma, 2020).

V prvním desetiletí nového milénia započal překotný vývoj počítačové techniky, rozvoj internetu a sociálních sítí, což s sebou přineslo nové obtíže při aplikaci vnitrostátních zákonů. Byla tedy potřeba jejich novelizace, protože tyto zákony původně vycházející z již postupně zastarávající Směrnice 95/46/ES, při jejímž koncipování nikdo nemohl přepokládat tak rapidní vývoj zásadně ovlivňující zpracování osobních údajů, nemohly by v měnícím se světě bez jejich změny obstát. Zároveň musela být vzata v potaz rozšiřující se globalizace a související vzrůstající tlak na efektivní zajišťování ochrany osobních údajů při přeshraničním zpracování a vytvoření odpovídajících mechanismů ochrany fyzických osob. Muselo tak dojít k revizi všech právních norem týkající se ochrany osobních údajů v evropském prostoru. Tato revize nastala po roce 2010. Na základě zkušeností se Směrnicí 95/46/ES, která harmonizaci zajistila jen v základních otázkách a částečně, bylo nově pro revizi právního rámce zpracování osobních údajů použito nařízení Evropské unie, které se od směrnice Evropské unie liší tím, že přímo stanovuje povinnosti a přiznává práva přímo jeho adresátům, kterými jsou především jednotlivé vnitrostátní subjekty, nikoliv primárně státy k provedení vnitrostátních legislativních opatření. Zjednodušeně řečeno, nařízení

Evropské unie nahrazuje vnitrostátní právní předpis a analogicky jej lze z pohledu jeho adresátů označuje za obdobu zákona. **Nařízení Evropské unie** tak logicky má, oproti směrnici, větší sjednocující účinek, jelikož jeho pravidla jsou **přímo aplikovatelná na adresáty ve všech státech Evropské unie**. Použitím Nařízení Evropského parlamentu a Rady (EU) č. 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), se stanovenou účinností od 25. května 2018 je další etapou, resp. reakcí na vývoj lidského společenství a souvisejícího zpracování osobních údajů. Právě použití nařízení Evropské unie je v tomto kontextu revoluční, protože dosud nikdy nebylo nařízení Evropské unie použito pro úpravu tak širokého komplexů vztahů, a to ani těch, které vznikají při zpracování osobních údajů, resp. se přímo netýkalo i stovek milionů subjektů údajů, kterým Obecné nařízení přiznává přímo vykonavatelná práva vůči správcům osobních údajů. V tomto ohledu jsme účinností Obecného nařízení vstoupili do nové doby nejen v oblasti ochrany osobních údajů při jejich zpracování, ale i jako občané České republiky, jelikož poprvé v daleko větší míře aplikujeme přímo evropský předpis namísto zákona (Žůrek, 2018; Sharma, 2020).

2.1.2 Vývoj a stav v České republice

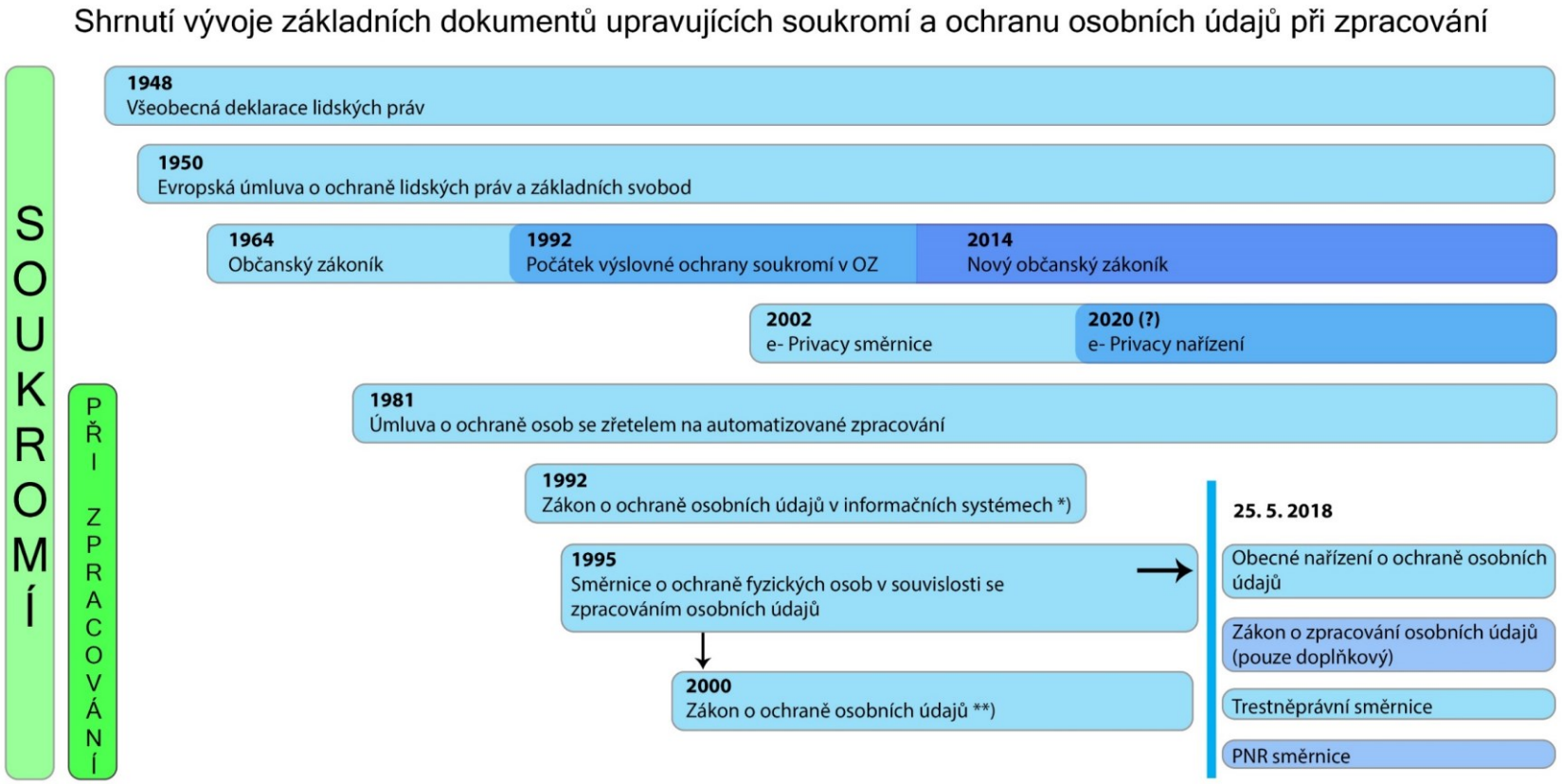
V prostředí České republiky, začala být ochrana osobních údajů při jejich zpracování samostatně řešena až přijetím zákona č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech, který upravoval pouze zpracování osobních údajů v informačních systémech. Nejednalo se o komplexní zákon, který by se vztahoval i na osobní údaje zpracovávané v papírových evidencích. Navíc nikdy nebyly zřízeny v tomto zákoně předpokládané orgány dozoru (Žůrek, 2018; Sharma, 2020).

Na poli ochrany osobních údajů při jejich zpracování neměla Česká republika až do roku 2000 plnohodnotný zákon, který by pro zpracování osobních údajů na zákonné úrovni prováděl čl. 10 odst. 3 Listiny základních práv a svobod, jelikož zákon o ochraně osobních údajů v informačních systémech se vztahoval pouze na informační systémy a neřešil ochranu osobních údajů při jejich zpracování komplexně, tj. nevztahoval se na zpracování prostřednictvím evidence, tak jak už se vztahovala Směrnice 95/46/ES. O plnohodnotné ochraně osobních údajů při jejich zpracování v České republice lze hovořit až od 1. června 2000, a to díky zákonu č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, kterým byl zároveň zřízen Úřad pro ochranu osobních údajů jako dozorový úřad nad dodržováním povinností stanovených při zpracování osobních údajů. Aby mohla Česká

republika vstoupit do Evropské unie musela naplnit i podmínky v oblasti ochrany osobních údajů. V roce 2004 byl zákon o ochraně osobních údajů významněji novelizován v souvislosti s nutností transponovat (realizovat na zákonné úrovni) Směrnici 95/46/ES. Obecným nařízením měl být zákon o ochraně osobních údajů zrušen, neboť nově již odpovídající práva a povinnosti upravuje od 25. května 2018 právě zmíněné Obecné nařízení, které převzalo hmotněprávní roli zákona o ochraně osobních údajů (Sharma, 2020).

Zároveň měl být s účinností Obecného nařízení účinný tzv. adaptační zákon, jehož funkcí je především připravit český právní řád na „dopad" Obecného nařízení, tj. předpisu, který byl přijat mimo sféru českého zákonodárství, a je tedy nutné právní řád na účinnost Obecného nařízení adaptovat. Česká republika musela rovněž na zákonné bázi ustanovit dozorový úřad, včetně jeho organizace. Tím zůstane Úřad pro ochranu osobních údajů. A jelikož výsledkem celkové revize ochrany osobních údajů v evropském prostoru není jen Obecné nařízení, ale i již zmíněná trestněprávní Směrnice 2016/680, která ze své povahy musí být transponována do českého právního řádu, mělo by tak být učiněno též v adaptačním zákoně. Co se týká vztahu Obecného nařízení a adaptačního zákona, jde o vztah doplňkový. Nejde již o svébytný zákon stanovující v celém rozsahu práva a povinnosti, jakým byl původní zákon o ochraně osobních údajů (Žůrek, 2018; Sharma, 2020).

Právní předpisy upravující ochranu osobních údajů při jejich zpracování částečně zajišťují i ochranu soukromí. Jde však o dílčí ochranu soukromí a nelze je chápat tak, že na jejich základě se lze dovolávat obecné ochrany soukromí. Soukromí je v nejširším slova smyslu chráněno zákonem č. 89/2012 Sb., občanský zákoník, a to konkrétně § 81 odst. 2, který stanovuje, že ochrany požívají zejména život a důstojnost člověka, jeho zdraví a právo žít v příznivém životním prostředí, jeho vážnost, čest, soukromí a jeho projevy osobní povahy (Žůrek, 2018; Sharma, 2020) .



Obrázek 1 – Vývoj základních dokumentů [Zdroj: Žůrek, 2018 s. 22 - upraveno]

3 PRÁVNÍ DOKUMENTY UPRAVUJÍCÍ OCHRANU OSOBNÍCH ÚDAJŮ

Ochrana osobních údajů je zakotvena v mnoha právních dokumentech. Z hlediska ochrany osobních údajů v kontextu audiovizuálních záznamů se však nachází v několika základních dokumentech. V této kapitole bude přesně vypsáno, jaká část těchto dokumentů se dané problematice věnuje a upravuje jí.

3.1 Listina základních práv a svobod

Základ právní úpravy ochrany osobních údajů lze najit i v samotných základech právního řádů České republiky, a to právě v Listině základních práv a svobod. Ochrana osobních údajů je v ní zakotvena právě jako jedna ze základních lidských práv každého subjektu práva. Články 7 a 10 jsou právě těmi, které se věnují problematice ochrany osobních údajů. Článek 7 v odstavci 1 Listiny základnách práv a svobod určuje, že nedotknutelnost osoby a jejího soukromí je zaručena (Šolc, 2015).

To jsou ústavní mantinely, kterým se chtě nechtě musí celá řada právních předpisů zabývajících se různými oblastmi lidského života podvolit a být s nimi v souladu. Podobně jako většina ostatních základních práv a svobod ale mohou být také omezeny, a to konkrétně na základě ustanovení tohoto článku a vždy jenom v takových případech, kdy to zákon (jako jakýsi prováděcí předpis takového „omezení“) stanoví. To nejdůležitější z ochrany osobních údajů se však nachází v desátém článku Listiny základních práv a svobod, a to přesněji v odstavcích 1,2 a 3 (Šolc, 2015).

Článek 10

(1) *Každý má právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno.*

(2) *Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.*

(3) *Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě* (ČESKO, 1993).

3.2 Občanský zákoník

Základnou ochrany osobnosti je hned po Listině základních práv a svobod zákon č. 89/2012 Sb., občanský zákoník, který je zároveň hlavním soukromoprávním kodexem u nás. Z pohledu občanského zákoníku je ochrana osobnosti člověka systematicky rozdělena do jednotlivých pododdílů na ochranu podoby a soukromí, ochranu duševní a tělesné integrity člověka, včetně práv člověka zadrženého proti jeho vůli ve zdravotnickém zařízení, otázek nakládání s odňatými částmi lidského těla a ochrany těla člověka po jeho smrti. Ale spadá sem zcela nepochybně taktéž i ochrana jména člověka (Šolc, 2015).

Ochraně osobních údajů svědčí z velké části i ochrana podoby člověka, protože právě zachycení jeho podoby může za určitých okolností vést k jeho identifikaci a k neblahým důsledkům s tím spojeným, a to v podstatě i kdykoliv v budoucnu (Šolc, 2015).

Občanský zákoník se ochraně osobních údajů věnuje především v oddílu 6, který nese název Ochrana člověka. Tento oddíl má celkem 6 pododdílů z niž ochrana osobních údajů se řeší především v prvních dvou pododdílech. Tyto částí nesou název Obecná ustanovení a Podoba a soukromí.

Oddíl 6

Osobnost člověka

Pododdíl 1

Obecná ustanovení

§ 81

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

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

§ 82

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

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

§ 83

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

(2) *Po smrti člověka se právnická osoba může domáhat, aby od neoprávněného zásahu bylo upuštěno a aby byly odstraněny jeho následky* (ČESKO, 2012).

Pododdíl 2

Podoba a soukromí

§ 84

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

§ 85

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

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

§ 86

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

§ 87

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

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

§ 88

(1) *Svolení není třeba, pokud se podobizna nebo zvukový či obrazový záznam pořídí nebo použijí k výkonu nebo ochraně jiných práv nebo právem chráněných zájmů jiných osob.*

(2) *Svolení není třeba ani v případě, když se podobizna, písemnost osobní povahy nebo zvukový či obrazový záznam pořídí nebo použijí na základě zákona k úřednímu účelu nebo v případě, že někdo veřejně vystoupí v záležitosti veřejného zájmu.*

§ 89

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

§ 90

Zákonný důvod k zásahu do soukromí jiného nebo k použití jeho podobizny, písemnosti osobní povahy nebo zvukového či obrazového záznamu nesmí být využit nepřiměřeným způsobem v rozporu s oprávněnými zájmy člověka (ČESKO, 2012).

V této části zákona se tedy říká, že zachytit jakýmkoliv způsobem (např. fotoaparátem nebo videokamerou) podobu člověka tak, že zobrazením je možné určit jeho totožnost, a to jedině s podmínkou, že k tomu dojde s jeho vlastním svolením. Toto pravidlo se uplatňuje nejenom v soukromí člověka, ale i na veřejnosti. Je ale potřeba, aby na daném zachycení podoby člověka jej bylo možné identifikovat, v opačném případě postrádá platnost (Švestka, Dvořák a Fiala, 2014).

I u následného rozšiřování podoby člověka opět platí, že je k tomu nutné jeho svolení. Svolením k vyobrazení své podoby za okolností, z nichž je zřejmé, že bude zároveň docházet k šíření tohoto vyobrazení, uděluje člověk podle § 85 odst. 2 zákona zároveň i souhlas k rozmnožování a rozšiřování této své podobizny, a to obvyklým způsobem, jak je mohl vzhledem k okolnostem, za kterých svolení uděloval, rozumně předpokládat. Výjimkou k tomuto pravidlu, kdy svolení zaznamenávaného jedince potřeba není, je podle § 88 Občanského zákoníku případ, kdy se podobizna nebo zvukový či obrazový záznam **pořídí nebo použije k výkonu nebo k ochraně jiných práv** (např. jako důkaz v soudním řízení) nebo **právem chráněných zájmů jiných osob** (Bartík a Janečková, 2012).

Oproti dřívější právní úpravě je nyní pojetí této výjimky širší, akcentován je nově zájem na řádném uplatnění soukromých práv. Svolení dále není potřeba, když se podobizna,

písemnost osobní povahy nebo zvukový či obrazový záznam pořídí nebo použijí na základě zákona k úřednímu účelu nebo v případě, že někdo veřejně vystoupí v záležitosti veřejného zájmu (např. na veřejnosti přístupném jednání zastupitelstva obce) (Lavický, 2015).

Stejně tak není svolení dle § 89 potřeba, má-li být podobizna, zvukový nebo obrazový záznam **pořízen nebo přiměřeným způsobem použit k vědeckému nebo k uměleckému účelu a rovněž tak pro tiskové, rozhlasové, televizní nebo jiné obdobné zpravodajství** (jedná se o tzv. zákonné licence omezení ochrany osobnosti). Od těchto výjimek není možno se jakkoliv odchýlit. Všechny tyto zákonné důvody umožňující zásah do soukromí člověka nebo k použití jeho podobizny, písemnosti osobní povahy nebo zvukového či obrazového záznamu, ale podle § 90 Občanského zákoníku nesmí být využity nepřiměřeným způsobem, který by byl v rozporu s oprávněnými zájmy člověka (Bartík a Janečková 2012).

V tomto smyslu se jedná o takové zájmy člověka, na kterých je třeba s ohledem na požadavek zajištění elementární úcty k jeho důstojnosti a jeho osobnosti za všech okolností bezpodmínečně trvat a které jsou za všech okolností nedotknutelné (Lavický, 2015).

3.3 Evropská úmluva o ochraně lidských práv a základních svobod

Úmluva o ochraně lidských práv a základních svobod, zkráceně Evropská úmluva o lidských právech, je nejdůležitější lidskoprávní úmluvou sjednanou v rámci Rady Evropy a základem regionální mezinárodněprávní ochrany lidských práv v Evropě. Byla podepsána v Římě dne 4. listopadu 1950 (Šolc, 2015).

Československo bylo roku 1992 vůbec prvním státem střední a východní Evropy, který se stal stranou Úmluvy (úmluva byla ratifikována 18. března 1992 a publikována pod č. 209/1992 Sb.) (Šolc, 2015).

Již zde lze najít základy právní úpravy ochrany osobních údajů. Úmluva o ochraně lidských práv a základních svobod zaručuje mnoho práv, jako například svobodu projevu či právo na život, ale z hlediska problematiky ochrany osobních údajů Úmluva o ochraně lidských práv a základních svobod zajišťuje lidem právo na respektování soukromého a rodinného života, tedy článek 8 (Šolc, 2015).

Článek 8 - Právo na respektování rodinného a soukromého života

„1. Každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence.

2. Státní orgán nemůže do výkonu tohoto práva zasahovat kromě případů, kdy je to v souladu se zákonem a nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných" (Ministerstvo zahraničních věcí, 1992).

Znění prvního odstavce lze tedy jednoduše aplikovat na problematiku ochrany osobních údajů, stačí si postupně tento první odstavec rozebrat. V případě, že by někdo například pořizoval videozáznam či fotografie, který bych značně zasahoval do našeho soukromí, jíž by porušoval toto základní právo a jednal by tak protiprávně. V kontextu tohoto práva, lze uvést i problematiku dronů s kamerami, které tuto část Evropské úmluvy o ochraně lidských práv a základních svobod velice lehce poruší, když například pořizují videozáznam nad naší domem.

3.4 Trestněprávní směrnice

Tato směrnice reaguje na specifickou povahu policejní a justiční spolupráce v trestněprávních věcech a obsahuje zvláštní pravidla pro ochranu osobních údajů a volný pohyb osobních údajů v této oblasti, která je vyňata z působnosti GDPR.

Dále se také věnuje jak přeshraničnímu, tak vnitrostátnímu zpracování osobních údajů příslušnými orgány členských států za účelem vymáhání práva, pod který se řadí prevence, vyšetřování, odhalování a stíhání trestných činů, anebo výkonu trestů jakož i ochrana a předcházení ohrožení veřejné bezpečnosti. Jejím hlavním cílem je chránit právo jednotlivců na ochranu vlastních osobních údajů a zároveň zaručit vysokou úroveň právě veřejné bezpečnosti (Trestněprávní směrnice, © 2018; Nařízení Evropského parlamentu a rady (EU) 2016/679, 2016).

Naopak se nevztahuje na zpracování osobních údajů prováděné při výkonu činností, které nespadají do oblasti působnosti práva Unie či zpracování prováděné orgány, institucemi a jinými subjekty Unie (Trestněprávní směrnice, © 2018; Nařízení Evropského parlamentu a rady (EU) 2016/679, 2016).

Mezi obsah směrnice patří například stanovení řady zásad pro zpracování a shromažďování osobních údajů, mimo jiné povinnost členských států zajistit, aby byly osobní údaje zpracovávány zákonným a korektním způsobem a způsobem, který zajistí jejich náležité zabezpečení, shromažďovány pro určité, výslovně vyjádřené a legitimní účely, aby nebyly

nepřiměřené ve vztahu k účelu, pro který jsou zpracovávány a aby byly přesné a v případě potřeby aktualizované (Trestněprávní směrnice, © 2018; Nařízení Evropského parlamentu a rady (EU) 2016/679, 2016).

Zpracování osobních údajů je dle této směrnice legální, pouze pokud je nezbytné ke splnění úkolů prováděných příslušnými orgány pro účely prevence, vyšetřování, odhalování a stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení a v rozsahu pro tyto účely nezbytném a pokud má základ v právu Unie nebo členského státu (Trestněprávní směrnice, © 2018; Nařízení Evropského parlamentu a rady (EU) 2016/679, 2016).

Dále směrnice ukládá členským státům povinnost určit přiměřené lhůty pro vymazání osobních údajů nebo pro pravidelné přezkoumání potřeby uložení osobních údajů. Co do délky lhůt mají národní zákonodárci volnost, měli by však zohlednit jak maximální dobu pro skladování osobních údajů, tak i potřebu pravidelně prověřit, zda je nutné příslušné údaje uchovávat (Trestněprávní směrnice, © 2018; Nařízení Evropského parlamentu a rady (EU) 2016/679, 2016).

Mezi další témata, kterými se směrnice zabývá, je například zpracování zvláštních kategorií osobních údajů, tedy genetických údajů, biometrických údajů, údajů o zdravotním stavu nebo údajů o sexuálním životě či sexuální orientaci, či těch které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filosofickém přesvědčení nebo členství v odborech, které je umožněno pouze po kumulativním splnění podmínek nezbytnosti a existence vhodné záruky práv a svobod subjektu údajů a pokud to unijní či národní právní úprava umožňuje. Cílem zpracování je ochrana životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby, nebo pokud tyto osobní údaje subjekt údajů zjevně zveřejnil (Trestněprávní směrnice, © 2018; Nařízení Evropského parlamentu a rady (EU) 2016/679, 2016).

Členské státy jsou dle této směrnice mimo jiné povinny zřídit nezávislý dozorový úřad (ÚOOÚ) s vyšetřovací, nápravnou a poradní pravomocí a s pravomocí upozornit na porušení předpisů přijatých na základě této směrnice justiční orgány, a pokud je to vhodné, zahájit soudní řízení nebo se do něj jinak zapojit (Trestněprávní směrnice, © 2018; Nařízení Evropského parlamentu a rady (EU) 2016/679, 2016).

Trestněprávní směrnice nahrazuje Rámcové rozhodnutí Rady 2008/977/SVV, které se věnovalo pouze zpracování osobních údajů přenesených nebo uveřejněných mezi

členskými státy navzájem. Vzhledem ke zvolené formě tohoto pramenu práva je vyžadována její implementace do právních řádů členských států, jednotlivé právní úpravy se od sebe tedy mohou lišit (Trestněprávní směrnice, © 2018; Nařízení Evropského parlamentu a rady (EU) 2016/679, 2016).

3.5 Zákon o zpracování osobních údajů

Zákon č. 110/2019 Sb., o zpracování osobních údajů je následníkem předchozího zákona o ochraně osobních údajů s číslem 101/2000 Sb., který byl právě výše zmíněným zákonem zrušen. Samotný zákon č. 110/ 2019 Sb. je brán jako tak zvaný Adaptační zákon upřesňující Obecné nařízení o ochraně osobních údajů (nařízení GDPR). Vejitím Adaptačního zákona v účinnost bylo do českého právního řádu zakotveno několik desítek ustanovení, jejichž cílem je upřesnit práva a povinnosti vyplývající z Nařízení GDPR (Nový zákon o zpracování osobních údajů, © 2019).

Je nutné uvést, že dikce nařízení GDPR umožňuje členským státům úpravu některých právních institutů vnitrostátní legislativou, přičemž dává rovněž možnost upřesnit či jinak rozvést již v nařízení GDPR zakotvená ustanovení, čímž umožňuje zákonodárci odchýlit se od obecné úpravy a přijmout určité národní výjimky, které jsou lépe uzpůsobeny konkrétnímu právnímu prostředí. Adaptační zákon je tedy výsledkem snahy o zpřesnění vnitrostátní právní úpravy v oblasti ochrany osobních údajů. nařízení GDPR, jakožto přímo použitelný právní předpis, bude i nadále aplikováno, avšak již ve světle výjimek a upřesnění stanovených novým Adaptačním zákonem (Nový zákon o zpracování osobních údajů, © 2019).

Mezi hlavní změny, které Adaptační zákon zavádí je například:

- upřesnění věkové hranice u dětí, které jsou způsobilé k udělení souhlasu se zpracováním osobních údajů,
- upřesnění informační povinnosti správce osobních údajů, zpracovávajícího osobní údaje na základě zákonné povinnosti nebo ve veřejném zájmu či při výkonu veřejné moci,
- zmírňuje povinnost správce stanovenou v článku 35 Nařízení GDPR, která spočívá v povinnosti vypracovat posouzení vlivu na ochranu osobních údajů v případě pravděpodobnosti rizika při systematickém a rozsáhlém zpracování osobních údajů,

- specifikuje zpracování osobních údajů na základě novinářské, akademické, umělecké, nebo literární licence a posuzování přiměřenosti takového zpracování (Žůrek, 2018).

3.6 Obecné nařízení o ochraně osobních údajů

Obecné nařízení o ochraně osobních údajů, je jedním ze základních právních norem přímo upravující zpracování osobních údajů, a to právě z hlediska pořizování audiovizuálních záznamů.

Důmyslnost tohoto dokumentu se odráží zejména v novém pojetí odpovědnosti správce za zajištění a dokládání souladu zpracování s Obecným nařízením, v rámci, kterého přináší Obecné nařízení nové standardizované nástroje např. v podobě kodexů chování či osvědčení nebo povinnosti vést záznamy o činnostech zpracování, jejichž účelem je napomoci správci zajistit a doložit soulad zpracování s Obecným nařízením. Mezi další významné změny týkající se činností pro zajišťováni souladu zpracování s Obecným nařízením je pro některé správce i pověřenec pro ochranu osobních údajů (Rafajová a Váryová, 2019).

Další změnou v Obecném nařízení je propracovanější pojetí přístupu založeného na riziku, v rámci, něhož je rozlišováno riziko zpracování, které je u každého správce jiné, a od tohoto rizika se následně odvíjejí adekvátní povinnosti správce. To tedy znamená že, Obecné nařízení odráží rozdílnost rizika u každého správce a podle rizika zpracování daného správce mu stanovuje méně či více povinností (Nulíček, 2017).

3.6.1 Struktura Obecného nařízení

Skládá se ze dvou částí, a sice z Preambule a vlastního (normativního) textu stanovující práva a povinnosti, tak jak je již obvyklé i u formy zákona (Nulíček, 2017).

Preambuli, kterou tvoří tzv. recitály (očíslované odstavce 1 až 173), lze označit za výklad normotvůrce, protože obsahuje důvody přijetí Obecného nařízení a jednotlivých povinností, práv či nových institutů, někdy i návody, jak je chápat (Žůrek, 2018).

Pro zajímavost Směrnice 95/46/ES obsahovala 9 968 slov, resp. 68 315 znaků (včetně mezer). Zákon o ochraně osobních údajů obsahoval 8 112 slov, resp. 54 101 znaků (včetně mezer). Obecné nařízení, včetně Preambule, obsahuje 45 609 slov, resp. 310 656 znaků (včetně mezer). Zde jde tedy přesně vidět, o jak propracovaný dokument se jedná (Rafajová a Váryová, 2019).

Druhá část, kterou již tvoří vlastní text Obecného nařízení, stanovuje pravidla pro zpracování osobních údajů, tedy text podobný zákonu (s tím rozdílem, že je členěn na články (1 až 99), nikoliv paragrafy) a bude tedy stěžejní při uplatňování Obecného nařízení (Nulíček, 2017).

Pro úspěšnou komplexní profesní práci s vlastním textem Obecného nařízení je nutné pracovat i s jednotlivými recitály, protože některé z nich jsou poměrně zásadní pro výklad některých článků a institutů a dá se říci, že pokud se jich některý recitál týká, pak je nutné k němu při výkladu přihlížet. Jejich přečtení a alespoň orientační znalost velmi usnadní vytvoření si celkového obrázku o Obecném nařízení a jeho správné aplikaci (Žůrek, 2018; Wray, 2017).

3.6.2 Nové pojetí odpovědnosti správce a přístup založený na riziku

Obecné nařízení představuje novou etapu v pojetí ochrany osobních údajů na evropském kontinentu a dá se říci, že i celosvětově, vzhledem k tomu, že jeho působností budou dotčeni i někteří správci usídlení mimo evropský kontinent. Pokud zpracovávají osobní údaje subjektu údajů nacházejících se v Evropské unii v souvislosti s nabídkou zboží nebo služeb nebo v souvislosti s monitorováním jejich chování, dochází-li k němu v rámci Evropské unie (viz čl. 3 odst. 2 Obecného nařízení).

Jednotlivá ustanovení Obecného nařízení nelze chápat izolovaně, ale je nutné je chápat v souvislostech jako celek, zejména pokud jde o princip odpovědnosti a přístup založený na riziku, jelikož tyto dva prvky se prolínají Obecným nařízením a současně představují jednu z nejvýraznějších kvalitativních změn oproti Směrnici 95/46/ES, resp. zákonu o ochraně osobních údajů (Žůrek, 2018).

3.6.3 Princip odpovědnosti správce

Odpovědnost správce za zpracování osobních údajů není novinkou, protože správce byl podle zákona o ochraně osobních údajů odpovědný za jím prováděné zpracování osobních údajů. Tak tomu je i za účinnosti Obecného nařízení (Žůrek, 2018).

Nově Obecné nařízení rozvíjí princip odpovědnosti správce za zpracování tím, že nejen výslovně stanovuje odpovědnost správce za dodržení povinností vyplývajících z Obecného nařízení, ale zároveň mu stanovuje povinnost být schopen soulad doložit (Žůrek, 2018).

Konkrétně podle čl. 24 odst. 1 Obecného nařízení je povinností správce, aby s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob zavedl vhodná technická

a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s Obecným nařízením. Tato opatření musí být podle potřeby revidována a aktualizována (Rafajová a Váryová 2019).

Obdobně je princip odpovědnosti správce stanoven v čl. 5 odst. 2 Obecného nařízení, ve kterém je stanovena odpovědnost správce za dodržení zásad zpracování stanovených v odstavci 1 zmíněného ustanovení, a zároveň je stanovena povinnost být schopen toto dodržení souladu doložit (Žůrek, 2018).

Na nově pojatý princip odpovědnosti navazují nové standardizované nástroje, prostřednictvím kterých bude správcům umožněno prokazovat soulad zpracování. Těmito nástroji jsou především záznamy o činnostech zpracování, kodexy chování či možnost získání osvědčení, pověřenec pro ochranu osobních údajů. Tyto nástroje však nebudou samospasné, jelikož prokazování souladu zpracování je nutné považovat za kontinuální činnost spočívající v plnění celého Obecného nařízení, nikoliv pouze jedné dílčí povinnosti, navíc např. kodexy chování či osvědčení představují dobrovolnou možnost (Žůrek, 2018).

Správce bude soulad dokládat i řádným plněním práv subjektu údajů. (např. poskytováním informací apod.), spoluprací s dozorovým úřadem atd. Vždy půjde o komplex činností, nikoliv o jednu izolovanou činnost, např. pouze přihlášení ke kodexu chování, když kodexy chování jsou navíc, jak již bylo zmíněno, založeny na dobrovolné bázi stejně jako získání osvědčení. Dosáhnout souladu zpracování napomůže i respektování principu *data protection by design*, což znamená nutnost počítat s nastavením adekvátní ochrany osobních údajů již od návrhu činností představujících zpracování osobních údajů (Žůrek, 2018; Wray, 2017).

Každý správce musí dokládat soulad zpracování se zásadami zpracování, resp. s Obecným nařízením svým způsobem i s ohledem na povahu, rozsah, kontext a účel zpracování, které provádí (Žůrek, 2018).

Zajišťování a dokládání souladu zpracování se zásadami zpracování, potažmo s Obecným nařízením, není jednorázový stav v minulosti, ale kontinuální proces v přítomnosti, který spočívá v plnění povinností kladených Obecným nařízením na správce. Pro úspěšné zvládnutí tohoto procesu je stěžejní tzv. mapování zpracování, při kterém správce zjišťuje, co vlastně s osobními údaji dělá a proč, vyhodnocuje rizika, zabezpečení, porovnává tyto informace s povinnostmi kladenými Obecným nařízením a zjištěné negativní rozdíly mezi aktuálním stavem a stavem žádoucím uvádí do souladu. Mapování může být podkladem

i pro vypracování, záznamů o činnostech zpracování, které mohou být větším správcům velmi užitečné, aby se vůbec orientovali ve zpracování, jež provádí, a pro zjištění, jaké povinnosti s ohledem na přístup založený na riziku se na ně vztahují (Žůrek, 2018; Wray, 2017).

3.6.4 Přístup založený na riziku

Pojetím, na němž je vedle principu odpovědnosti Obecné nařízení postaveno, přístup založený na riziku, který se nově promítá i v přijetí některých nových povinností, resp. institutů, přičemž jejich aplikace je vázána pouze určitý druh rizikovosti zpracování osobních údajů. Některé povinnosti tak nedotýkají některých správců, a sice tehdy, není-li zpracování osobních údajů, které provádějí, rizikové pro práva a svobody subjektů údajů (Rafajová a Váryová, 2019).

Přístup založený na riziku obecně znamená povinnost správce a zpracovatele s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování a možným rizikům přijmout adekvátní technická a organizační opatření za účelem zajištění zabezpečení osobních údajů odpovídající riziku, které dané zpracování pro subjekty údajů představuje. Analogicky lze přirovnat k zajištění bezpečnosti a ochrany zdraví při práci, jejíž míra je odvozována od charakteru činností zaměstnavatele (Žůrek, 2018; Wray, 2017).

Tento přístup je logický, jelikož každé zpracování bude pro subjekty údajů rozdílně rizikové a nelze stanovit jednotnou hranici zabezpečení pro všechny správce. V tomto pojetí byl přístup založený na riziku de facto uplatňován i ve Směrnici 95/46/ES, resp. zákoně o ochraně osobních údajů (Žůrek, 2018; Rafajová a Váryová, 2019).

Obecné nařízení přístup založený na riziku dále rozpracovává a přidává jeho nové pojetí, které spočívá v aplikaci některých povinností, a to pouze v případech, představuje-li dané zpracování vyšší riziko pro subjekty údajů. Jinými slovy, čím vyšší riziko zpracování pro subjekty údajů, tím více povinností pro správce (Žůrek, 2018; Rafajová a Váryová, 2019).

Pojetí přístupu založeného na riziku zpracování se odráží zejména u nových institutů, jako je např. vedeni záznamů o činnostech zpracování, posuzování vlivu na ochranu osobních údajů, předchozí konzultace s dozorovým úřadem a jmenování pověřence. Tyto povinnosti se podle podmínek jejich aplikace vesměs uplatňují právě u zpracování, které je rizikové nebo vysoce rizikové pro práva a svobody subjektu údajů. S rizikem se pracuje i u povinností ohlašovat případy porušení zabezpečení ochrany osobních údajů dozorovému úřadu, resp.

oznamovat je subjektu údajů, u kterých je však riziko pro práva a svobody subjektu údajů posuzováno ve vztahu k danému bezpečnostnímu incidentu (Žůrek, 2018; Wray, 2017).

Byt' se riziko může posuzovat v různých situacích (tj. při zpracování jako takovém nebo při bezpečnostním incidentu), jde vždy o jednu kategorii rizika, přičemž se poměřuje riziko pro práva a svobody subjektu údajů. Přístup založený na riziku do určité míry diverzifikuje správce podle rizikovosti zpracování osobních údajů, které provádí, na základě čehož mu pak jsou stanoveny dodatečné povinnosti. Mnoho správců právě s ohledem na minimální riziko, které jejich zpracování představuje pro subjekty údajů, nebude zbytečně nuceno plnit povinnosti, jejichž plnění by s ohledem na nerizikovost zpracování bylo neadekvátní vyžadovat. Obecné nařízení je z hlediska dopadu nových povinností, které nebyly součástí Směrnice 95/46/ES, resp. zákona o ochraně osobních údajů, významné především pro správce zpracovávající osobní údaje způsobem, který již představuje riziko pro práva a svobody fyzických osob (Žůrek, 2018).

Jelikož správci často zpracovávají různé kategorie subjektů údajů a tomu odpovídající různé kategorie osobních údajů, může riziko představovat pouze některé zpracování a jiné už nikoliv. Například zpracování osobních údajů pro pracovněprávní účely nepředstavuje obecně riziko, ovšem pokud by správce zároveň provozoval systém jízdného v hromadné městské dopravě zpracovávající osobní údaje cestujících, tímto zpracováním by se již kvalifikoval do rizikového zpracování, a pokud by např. začal v rámci systému jízdného zavádět nové prostředky např. párování předplaceného časového kupónu s platební kartou, jednalo by se již o situaci, kdy by musel provést tzv. posouzení vlivu na ochranu osobních údajů a přijmout adekvátní (zvýšené) prvky ochrany. Obdobně by bylo nutné postupovat i v případě, kdy by správce provozoval např. biometrický docházkový systém, který by představoval zpracování zvláštní kategorie osobních údajů (Žůrek, 2018; Rafajová a Váryová, 2019).

S rozšířením pojetí přístupu založeného na riziku souvisí **i zrušení oznamovací povinnosti**, která byla správcům stanovena v § 16 odst. 1 zákona o ochraně osobních údajů. Obecné nařízení tuto povinnost původně stanovenou ve Směrnici 95/46/ES nepřevzalo, neboť její roli plní nové instituty postavené na přístupu založeném na riziku (záznamy o činnostech zpracování či posouzení vlivu na ochranu osobních údajů, předchozí konzultace nebo pověřenec pro ochranu osobních údajů) (Rafajová a Váryová 2019; Wray, 2017).

4 OCHRANA OSOBNÍCH ÚDAJŮ V KONTEXTU AUDIOVIZUÁLNÍCH ZÁZNAMŮ

V obecném pojetí je problematika ochrany osobních údajů velice rozsáhlým tématem. V této kapitole bude ovšem řešena především v kontextu audiovizuálních záznamů, tedy jak ochrana osobních údajů souvisí s provozem kamerových systémů a celkově, jak je řešena z hlediska poskytování audiovizuálních záznamů.

4.1 Funkce ochrany podle občanského zákoníku

O tom, zda někdo svým jednáním narušuje vaše právo na ochranu soukromí a podoby, rozhoduje především to, zda k takovému jednání dal svolení, respektive zda vůči němu nedal jasně najevo svůj nesouhlas (Mates, 2019).

Svolení podle občanského zákoníku ovšem nelze zaměňovat se souhlasem, jak jej používá GDPR, totiž se souhlasem jako jedním z právních titulů pro zpracovávání osobních údajů, který musí naplňovat poměrně přísná kritéria. Zákoník je v tomto ohledu méně formální a jako svolení se bude počítat jakékoliv svobodné a vážné vyjádření vůle, ze kterého vyplývá, že se zachycením své podoby nemá člověk problém. Udělit svolení tak můžeme třeba i mlčky tím, že se proti pořízení záznamu neohradíme. Automaticky tak umožňujete i jeho šíření. To však musí být provedeno obvyklým a předvídatelným způsobem, což zákoník nijak blíže nespecifikuje, a tento pojem je tak ponechán k výkladu dle konkrétních okolností. V obou případech máte právo svůj souhlas odvolat a domáhat se smazání fotografie či jejího stažení, pokud už došlo k jejímu rozšíření (Mates, 2019).

Jako příklad činností mimo režim regulace GDPR lze uvést oslavu narozenin či jinou událost, na které se sejde skupina přátel. Pokud hosté vědí o tom, že jsou fotografováni, a nijak se vůči tomu neohradí, lze jejich souhlas vztáhnout i na následné zveřejnění fotek v rámci oslavencova profilu na sociální síti, jelikož to je v dnešní době takřka „standardní postup“ (Mates, 2019).

Zcela jiná situace by ovšem nastala tehdy, pokud vyfotíme osobu, která na večírku třeba usnula v nějakém nelichotivém stavu. V případě, že takovou fotografii navíc bez svolení zveřejníte na internetu, jednáte protizákonně a poškozený se na vás může domáhat mj. odškodnění prostřednictvím žaloby na ochranu osobnosti. Přičemž otevřenost, propojenost a nekontrolovatelnost internetu může významně přispět k závažnosti takto

způsobených následků. Zásadní poškození reputace se pak může mimo jiné projevit i ve výši odškodnění přiznaného soudem (Mates 2019).

Stejný princip můžeme aplikovat například na koncerty nebo jiné veřejné akce. Fotografie tančících a bavících se lidí může být zveřejněna, zatímco snímek, který by zachycoval například viditelně opilého účastníka akce, může zadělat tomu, kdo jej zveřejnil, na problémy (Mates ,2019).

4.2 Rozdíl mezi zákonem o ochraně osobních údajů a GDPR

Zákon o ochraně osobních údajů už dříve nařizoval, aby provozovatelé kamerových systémů o monitorování daného prostoru informovali všechny osoby do něj vstupující, stejně jako o právním titulu pro zpracování těchto údajů. Dále bylo nutné zabezpečit zpracovávané údaje proti jejich možnému zneužití a dbát na ochranu soukromí monitorovaných osob. GDPR vyžaduje to samé, takže výrazné změny oproti stávající právní úpravě ohledně kamerových systémů zde nejsou. Stejně jako dříve, je i dnes podle tohoto nařízení vždy primárně odpovědný správce, například družstvo, společenství vlastníků jednotek či zaměstnavatel, který rozhodl o provozování kamerového systému. Správce musí s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob zavést vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto nařízením (Srovnání nařízení GDPR a zákona o ochraně osobních údajů, 2021).

Podle základní zásady, která ovšem platí už dnes, musí být osobní údaje ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem. Tento princip GDPR označuje jako „zákonnost, korektnost a transparentnost“. Podle nařízení je zpracování osobních údajů zákonné, pouze pokud je splněna nejméně jedna z podmínek uváděných v článku 6. To znamená, že subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů:

a) *„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;*

b) *zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;*

c) *zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;*

d) *zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;*

e) *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"* (Nařízení Evropského parlamentu a rady (EU) 2016/679, 2016).

4.2.1 Souhlas s poskytováním záznamů

Běžně je zákonnost ošetřena udělením souhlasu subjektu se zpracováním osobních údajů. V případě zpracování údajů kamerovými systémy by se ovšem tento titul velmi těžko dodržoval. Proto bude možné zpracovávat údaje bez souhlasu na základě podmínky zpracování, které je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany. Souhlas se zpracováním osobních údajů je jen jednou z možností zákonného zpracování osobních údajů, nikoliv jedinou. Ne vždy se souhlas vyžaduje. Naopak se v praxi vyskytují nadbytečné žádosti o udělení souhlasu v situaci, kdy je zpracování zákonné z jiného důvodu. Takové nadbytečně vyžadované souhlasy dokonce Úřad pro ochranu osobních údajů považuje za porušení zákona. Zároveň je ale potřeba upozornit, že při pořizování kamerových záznamů nezbytných pro účely oprávněných zájmů příslušného správce či třetí strany nesmí být zasahováno do základních práv a svobod osob, tedy nesmí být nadměrně zasahováno do soukromí osob a musí jít o monitoring přiměřený účelu, který se jeho použitím sleduje (Srovnání nařízení GDPR a zákona o ochraně osobních údajů, 2021).

Při použití kamerových systémů ke sledování osob a záznamů těchto osob platí, že musí být nezbytné pro naplnění konkrétního účelu a musí být přiměřené vzhledem k okolnostem a k ochraně soukromí těchto osob. Vždy je třeba maximálně respektovat soukromí a oprávněné zájmy osob, například nakupujících v obchodě. Co se týká kamerových záznamů na pracovišti, ani v tomto případě není třeba žádat zaměstnance o souhlas s umístěním kamer, protože se bude jednat o zpracování osobních údajů na základě oprávněného zájmu zaměstnavatele. Zaměstnanci ale musí být o umístění kamerového systému informováni (Srovnání nařízení GDPR a zákona o ochraně osobních údajů, 2021).

Podle § 316 zákoníku práce nesměl zaměstnavatel bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci. Jestliže je u zaměstnavatele dán závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele, který odůvodňuje zavedení kontrolních mechanismů, je zaměstnavatel povinen přímo informovat zaměstnance o rozsahu kontroly a o způsobech jejího provádění (Srovnání nařízení GDPR a zákona o ochraně osobních údajů, 2021).

Novými povinnostmi, které nařízení GDPR provozovatelům kamerových systémů přinesl je zvýšený rozsah poskytovaných informací, vedení záznamů o činnosti a povinnost ohlášení porušení zabezpečení či úniku dat (Srovnání nařízení GDPR a zákona o ochraně osobních údajů, 2021).

4.2.2 Rozsah poskytovaných informací

V praxi se zaměňuje povinnost informovat subjekt údajů o zpracování osobních údajů se souhlasem ke zpracování osobních údajů. Jak podle zákona o ochraně osobních údajů, tak podle GDPR je třeba při zpracování osobních údajů postupovat transparentně, tedy poskytnout vhodným způsobem subjektu údajů informace zejména o tom, kdo a jaké osobní údaje zpracovává, k jakému účelu a zda je dále předává třetím osobám a kdo má k osobním údajům přístup. Podle článku 12 je správce povinen přijmout vhodná opatření, aby poskytl subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků potřebné informace. Informace je možno poskytnout písemně, ale i jinými prostředky elektronické formy. Pokud si to subjekt údajů vyžádá, mohou být v určitých situacích informace poskytnuty i ústně (Srovnání nařízení GDPR a zákona o ochraně osobních údajů, 2021).

Rozsah informační povinnosti upravují články 13 a 14. Mimo jiné je nutné subjektu údajů vhodným způsobem sdělit:

a) totožnost a kontaktní údaje na správce a jeho případného zástupce;

b) kontaktní údaje na pověřence pro ochranu osobních údajů (pokud byl zřízen);

c) účel zpracování (u kamerových systémů například sledování vymezených prostor);

d) právní základ pro zpracování (u kamerových systémů sdělení, že zpracování probíhá podle čl. 6 odst. 1 písm. f) GDPR, kdy souhlas subjektu údajů není třeba, jelikož zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, a že se tomu děje tak, aby byly chráněny zájmy a základní práva a svobody subjektu údajů);

e) přesné vymezení oněch oprávněných zájmů správce či třetích osob, které je nezbytné kamerovým systémem chránit (například ostraha objektu, ochrana majetku);

f) informaci o délce uchování kamerového záznamu.

Provozovatelé musí zajistit, aby informační tabulky o provozu kamerového systému byly dobře viditelné při každém vstupu nebo vjezdu osob do monitorovaných míst. Vedle toho musí být subjekt údajů poučen o svých právech. V praxi je tedy nutné rozlišovat mezi souhlasem a informací. Informaci musí subjekt údajů obdržet vždy.

Správce systému proto musí subjektu údajů poskytnout další informace, jsou-li nezbytné pro zajištění spravedlivého a transparentního zpracování ve vztahu k subjektu údajů:

1. *„doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby;*
2. *oprávněné zájmy správce nebo třetí strany v případě, že je zpracování založeno na čl. 6 odst. 1 písm. f);*
3. *existence práva požadovat od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz anebo omezení zpracování a práva vznést námitku proti zpracování, jakož i práva na přenositelnost údajů;*
4. *pokud je zpracování založeno na souhlasu, existence práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním;*
5. *existence práva podat stížnost u dozorového úřadu;*
6. *zdroj, ze kterého osobní údaje pocházejí“* (Nařízení Evropského parlamentu a rady (EU) 2016/679, 2016).

4.2.3 Vedení záznamů o činnosti

Vedení záznamů je jakousi náhradou za zrušení registrační povinnosti podle zákona o ochraně osobních údajů. Protože se provoz kamerového systému nedá považovat

za příležitostné zpracování, měl by se každý provozovatel takového systému na tuto novou povinnost včas připravit. Nařízení obsahuje celou samostatnou část, která se zabezpečení dat a povinností správce věnuje.

Záznamy obsahují všechny tyto informace:

1. *„jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů;*
2. *účely zpracování;*
3. *popis kategorií subjektů údajů a kategorií osobních údajů;*
4. *kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích;*
5. *informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a v případě předání podle čl. 49 odst. 1 druhého pododstavce doložení vhodných záruk;*
6. *je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů;*
7. *je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1“* (Nařízení Evropského parlamentu a rady (EU) 2016/679, 2016).

Záznamy se vyhotovují písemně, a to počítaje i elektronickou formu. Správce, zpracovatel nebo případný zástupce správce nebo zpracovatele poskytne záznamy na požádání dozorového úřadu.

4.2.4 Povinnost ohlášení porušení zabezpečení či úniku dat

Pokud jde o ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu, autoři nařízení očekávají, že jakékoli porušení zabezpečení správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí dozorovému úřadu, **ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob.** Tato nová povinnost se na provozovatele kamerového systému bude určitě vztahovat, tudíž je nutné, aby dbali v maximální míře na bezpečné zpracování těchto záznamů (Hlídání areálu kamerovým systémem, 2017).

4.3 Definice audiovizuálních záznamů v kontextu ochrany osobních údajů

V Obecném nařízení o ochraně osobních údajů nenajdeme přímo zmínku o audiovizuálních záznamech, tedy o videích natočených kamerami, fotografiích a zvukových nahrávkách. Všechny tyto druhy audiovizuálních záznamů se skrývají pod pojmem biometrické údaje. Ve smyslu čl. 4 bod 14 nařízení GDPR se za biometrické údaje považují osobní údaje, které jsou výsledkem zvláštního technického zpracování (týkající se fyzických, fyziologických nebo behaviorálních charakteristických znaků fyzické osoby) a které umožňují nebo potvrzují jedinečnou identifikaci fyzické osoby, jako například vyobrazení obličeje. Je poměrně časté, že celková zachycená podobizna dotyčné osoby na kamerovém záznamu v sobě kombinuje vícero informací. Běžně se získává například vyobrazení obličeje, celé postavy dotknuté osoby včetně jejích specifických znaků (např. kulhavá chůze, tetování). K těmto údajům se přidávají další údaje, a to minimálně v rozsahu, že v určitém čase byla dotyčná osoba na monitorovaném místě. V závěru je tedy možné jednoznačně identifikovat konkrétní fyzickou osobu (Calde, 2018).

S ohledem na rychlý technologický pokrok a stále častější zavádění složitých kamerových systémů ve světě lze očekávat tento trend i v podmínkách České republiky. Vzhledem k tomu, že získaný kamerových záznam je velmi citlivým materiálem, který může být zneužit více způsoby, tak jeho zpracovávání představuje pro práva dotčených osob vysoké riziko. Uvedené zařízení podporuje i trend technologického vývoje a nutnost přípravy náležitého právního rámce na masové rozšíření takových kamerových systémů v podmínkách České republiky tak, aby mohly být práva a svobody dotčených osob náležitě chráněny (Facial Recognition ©, 2020).

Je nutné doplnit, že v některých zemích Evropské unie fungují i samostatné orgány, zabývající se problematikou kamer a monitorování prostorů. Ve Spojeném království je tím Surveillance Camera Commissioner, jehož úloha je poskytovat stanoviska, pokyny a šířit informace o povinnostech při provozování kamerových systémů. (Calde, 2018).

Vzhledem k početnosti kamerových systémů a dříve zmíněného technologického pokroku je možné zastávat názor, že takové orgány minimálně v podobě pracovních skupin poskytujících pokyny by měli být vytvořené v každém evropském státě. To by mohlo zvýšit uvědomělost provozovatelů kamerových systémů při jejich provozu a zlepšit tak úroveň ochrany práv dotknutých osob (Calde, 2018).

4.4 Možnosti identifikace osob

Možnost jednoznačně identifikovat osobu na kamerovém záznamu, závisí na technických možností kamery, nastavení snímaní kamer, její rozlišení, úhel záběru a dalších faktorech. Kamerový systém může snímat statický záznam, dynamický záznam se zvukem anebo bez zvuku. Dále může kamerový systém automaticky přidružovat informace k snímanému obrazu, jako například teplotu dotknuté osoby a čas. Stále častějším typem monitorování, hlavně veřejných prostorů je monitorování s automatickým rozpoznáváním tváře tzv. Facial Recognition (Bojkovic, Milovanovic, 2019).

V dnešní době je již celkem běžné a nikomu už nepřijde natolik divné, že obce a města na veřejných prostranstvích instalují kamery a vytváří tak propojené kamerové systémy monitorující dění v celých částí obcí a měst. Je i už dost časté, že jsou v městech nainstalované kamery s automatickým rozeznáváním tváře, a dokonce jsou i tyto systémy vybaveny sledováním zájmových objektů, při kterém je zadán do systému požadavek na sledování určité osoby či automobilu. A pokud kamerový systém zaznamená a rozpozná žádaný objekt či osobu, upozorní na to obsluhu kamerových systému. Osoba obsluhující, tak může přímo před sebou vidět kam daná osoba jde, čí kam zajíždí hledaný automobil. Systémy s automatickým rozpoznáváním tváře jsou již často využívány i v domácích podmínkách. Tyto kamerové systémy jsou využívány k hlídání příslušných pozemků u rodinných domů, které nejsou veřejné. Na takovéto zpracování osobních údajů se obyčejně ve smyslu čl. 2 ods. 2 písm. c) nařízení GDPR ve spojitosti s recitálem 18 nařízení GDPR právní úprava GDPR nevztahuje (Bojkovic, Milovanovic, 2019).

5 DÍLČÍ ZÁVĚR TEORETICKÉ ČÁSTI

Teoretická část měla především za úkol vysvětlit základní pojmy a uvést základní informace potřebné k porozumění problematiky ochrany osobních údajů z hlediska audiovizuálních záznamů. Pomocí odborné literatury, a především Obecného nařízení o ochraně osobních údajů bylo vysvětleno několik základních pojmů, které je potřeba znát pro orientaci v problematice ochrany osobních údajů. Dále byly vypsány hlavní právní dokumenty týkající se ochrany osobních údajů. Hlavní část teoretické části se věnovala vývoji ochrany osobních údajů. V této kapitole byl pospán vývoj jak v Evropské unii, tak v České republice. Poslední kapitola se věnovala charakteristice právních dokumentů věnující se ochraně osobních údajů. Tyto dokumenty byly obecně popsány a následně znázorněny v jakých částech dokument řeší přímo problematiku ochrany osobních údajů z hlediska audiovizuálních záznamů.

II. PRAKTICKÁ ČÁST

6 KAMEROVÉ SYSTÉMY A GDPR

Obecné nařízení o ochraně osobních údajů je hlavním a aktuálně platným dokumentem, který se přímo týká problematiky kamerových systému a celkové pořizování audiovizuálních záznamů. Jaké zásady, práva a povinnosti má člověk při kontaktu s kamerovými systémy bude popsáno níže v této kapitole.

6.1 Základní zásady provozování kamerového systému

Provoz kamerového systému stejně jako každé jiné nakládání s osobními údaji se musí uskutečňovat v souladu se základními zásadami ochrany osobních údajů. Těmi jsou ve smyslu č.1. 5 odst. 1 nařízení GDPR:

1. zásada zákonnosti, spravedlnosti a transparentnosti;
2. zásada omezení účelu;
3. zásada minimalizace údajů;
4. zásada správnosti;
5. zásada minimalizace uchovávání;
6. zásada integrity a důvěrnosti.

Při plánování provozu kamerového systému je provozovatel povinen nastavit kamerový systém z technické stránky tak, aby jeho provoz byl v souladu s uvedenými zásadami. Stejně všechny související procesy, při kterých dochází ke zpracovávání osobních údajů, musí být nastaveny v souladu s těmito zásadami.

Při úplném zahájení prací na zavedení provozu kamerového systému by si měl provozovatel odpovědět, proč chce provozovat kamerový systém.

Typickými důvody bývají například:

- ochrana majetku;
- ochrana zdraví;
- ochrana bezpečnosti a prevence kriminality;
- sledování pracovního výkonu zaměstnanců;
- zajištění veřejného pořádku v obci / městě;
- usnadnění poskytnutí služby.

Po definování primárního důvodu zavedení kamerového monitorování si provozovatel určí, zda je to skutečně nezbytné k dosažení stanoveného cíle. Provozovatel musí rozlišit, zda je schopen dosáhnout svůj určený cíl pouze zavedením provozu kamerového systému, nebo je schopen uvedený cíl prosadit i jiným způsobem méně zasahujícím do práv dotčených osob (Solove, 2020).

Příklad: Společnost provozující autoservis potřebuje vyřešit problém stížnosti zákazníků na kvalitu jimi provedených oprav aut. Zákazníci autoservisu si mnohdy stěžují neoprávněně, a to s cílem získat slevu z konečné ceny opravy auta klamem o původním stavu vozidla, obsahu kufru, příp. stížnosti na délku trvání prací automechanika. Při řešení stížností zákazníků dochází ke konfliktu tvrzení automechaniky a zákazníků. Autoservis potřebuje nějakým způsobem získat údaje o kvalitě prací automechaniků v dílně tak, aby mohli být poskytnuty i zákazníkům v případě, že nejsou zákazníci přímo přítomni u celé opravě vozidla. Jediným objektivním řešením je zavedení kamerového systému v dílně tak, aby kamery snímaly celý průběh opravy vozidla. Kamerový systém by tak plnil několik funkcí – získával by při nejmenším materiál pro případ stížnosti zákazníka na kvalitu opravy, či délku prací. Uvedeného není z objektivního hlediska možné docílit jinak než provozem kamerového systému.

Po určení důvodu pro provoz kamerového systému a jeho oprávněnosti si může provozovatel správně zvolit právní základ pro zpracování osobních údajů. Ve smyslu zásady legality musí provozovatel zpracovávat osobní údaje zákonně, což znamená, že má dodržovat právní předpisy, nemá postupovat nezákonně a protiprávně. Provozovatel by měl i ve smyslu zásady spravedlnosti a transparentnosti postupovat takříkajíc celkově "fér". Z tohoto důvodu musí provozovatel disponovat právním základem pro zpracování osobních údajů. Dokud by neměl provozovatel právní základ pro zpracování osobních údajů, není zákonný provoz kamerového systému možný. Může jím být některý ze šesti právních základů uvedených v čl. 6 odst. 1 nařízení GDPR. "Při kamerových systémech je nejčastějším právním základem tzv. Oprávněný zájem ve smyslu čl. 6 odst. 1

Právní základy zpracování osobních údajů podle čl. 6 odst. 1 nařízení GDPR:

1. zpracování je zákonné pouze tehdy a pouze v tom rozsahu, když je špinění alespoň jedna z těchto, podmínek:

a) dotyčná osoba vyjádřila souhlas se zpracováním svých osobních údajů na jeden nebo více konkrétní účely;

b) zpracování je nezbytné pro plnění smlouvy, jejíž …….

1. *písm. f) nařízení GDPR (dále jen oprávněný zájem). Méně častým je tzv. souhlas dotčené osoby dle čl. 6 odst. 1 písm. a) nařízení GDPR (dále jen souhlas)* (Nařízení Evropského parlamentu a rady (EU) 2016/679, 2016).

6.1.1 Podoba člověka

Podoba člověka je významným projevem osobní povahy představovaným především souhrnem opticky vnímatelných charakteristik člověka, které umožňují jeho individualizaci, resp. identifikaci, představují tedy to, jak se člověk vzhledově jeví navenek. (Podmínky zachycení a šíření podoby člověka prostřednictvím fotografie, © 2020).

Nejedná se ovšem nutně pouze o vizuální podobu, není tedy důležité, jakými smysly můžeme podobu člověka vnímat. V úvahu proto přichází také např. vjem hmatový u nevidomých osob. V užším smyslu zahrnuje podoba člověka ztvárnění obličeje, v širším smyslu celkový vzhled člověka. Tvoří ji proto jakákoli složka vzhledu tělesné schránky člověka. Podoba člověka ovšem nezahrnuje pouze to, co je možné vnímat prvotně lidskými smysly, ale řadíme sem i jakékoli zobrazení těla člověka. Na tomto místě lze jmenovat např. zobrazení těla za pomoci dostupných technických prostředků, jako je např. rentgenový či ultrazvukový prostředek. Mezi významné znaky, na základě, kterých je možné seznat podobu člověka, pak zejména patří tvarová specifika, zvláštnosti pigmentace, geneticky podmíněné zvláštnosti, následky úrazů či chorob, tetování, piercing, účes, znaky stařeckých změn apod (Podmínky zachycení a šíření podoby člověka prostřednictvím fotografie, © 2020).

Od podoby člověka je nutné odlišovat jeho podobiznu. V případě podobizny se jedná o jeden ze způsobů zobrazení člověka, a není proto předmětem absolutního osobnostního práva podle občanského zákoníku. K takovému zobrazení může dojít také prostřednictvím fotografie. Proto vždy, pokud má být na fotografii zachycena podoba osoby, je nutné mít na zřeteli úpravu v občanském zákoníku, která reguluje práva k podobě člověka. Samotná fotografie pak může být předmětem některého z práv duševního vlastnictví.. Je však nutné si uvědomit rozdíl mezi podobou člověka a zachycením jeho podoby prostřednictvím fotografie. Pořízení takové fotografie či její šíření je ovlivněno právě tím, že zasahuje do práv k podobě člověka. Fotografie zde vystupuje pouze jako hmotný nosič, na němž je zachycena podoba člověka (Podmínky zachycení a šíření podoby člověka prostřednictvím fotografie, © 2020).

6.1.2 Právo na podobu člověka

Právo na podobu člověka vzniká narozením každé fyzické osoby. V pozitivním smyslu se jedná o oprávnění subjektu zachytit svou podobu, jakož i udělovat jiným svolení k jejímu zachycení. V negativním smyslu se pak bude jednat o právo bránit se proti neoprávněnému zachycení podoby a jejímu neoprávněnému rozšiřování ze strany jiného subjektu. Stručně řečeno, obsahem práva na podobu člověka je zejména užívací a dispoziční oprávnění ve vztahu k zachycení podoby člověka. Předmětem práva na podobu je potom individualizovaná podoba člověka jako jedna z významných hodnot osobnosti jednotlivce. Pokud je obsahem práva na podobu užívací a dispoziční oprávnění ve vztahu k zachycení podoby fyzické osoby, pak obsahem práva k podobizně je užívací a dispoziční právo subjektu ve vztahu k ní. Podmínkou uplatnění práva na podobu je, že osoba je na základě zobrazení identifikovatelná (Podmínky zachycení a šíření podoby člověka prostřednictvím fotografie, © 2020).

6.2 Soukromé užívání kamer

Hlídá-li osoba svůj soukromý pozemek kamerovým systémem se záznamem, který však může zachytit i podobu dalších osob, nastane okamžik, kdy se už jedná o systematickou činnost, a tím pádem o zpracování osobních údajů. Nicméně pokud tak činí v rámci své osobní potřeby, jedná se o výše zmiňovanou výjimku z aplikace GDPR (Soukromé užívání kamer, 2019).

V této souvislosti je ale potřeba upozornit, že je nutné vyvarovat se nepřiměřeně rozsáhlého monitorování veřejných prostranství v okolí nemovitosti, například ulice vedoucí kolem domu či sousedova pozemku, což by mohlo způsobit nepoužitelnost této výjimky (Soukromé užívání kamer, 2019).

Jiná situace nastane v případě používání kamer v automobilech či na helmách motocyklistů nebo sportovců. Režimu GDPR se zcela vyhneme, jedná-li se o nahodilé používání kamery pouze v rámci určité volnočasové aktivity pro naši osobní potřebu, například při závodech. V takové situaci se nebude vůbec jednat o zpracování osobních údajů. Pokud se provozuje ve vozidle kamera, která trvale zaznamenává okolní provoz, je potřeba dát si pozor. Jelikož dochází k systematickému zaznamenávání velkého množství registračních značek a obličejů ostatních řidičů a kolemjdoucích, pod režim GDPR tato činnost spadá. Nicméně, takový druh zpracovávání GDPR umožňuje na základě právního titulu, kterým je nezbytnost pro ochranu vašich oprávněných zájmů. Pokud tedy využíváme kameru v autě pro ochranu

svých oprávněných zájmů, jako je například zisk důkazu při dopravní nehodě atd. neporušujeme tím tak GDPR (Soukromé užívání kamer, 2019).

Nesmíme zapomínat na to, že monitorovaný prostor by měl být zřetelně označen a zpracovávaná data zabezpečena proti možnému zneužití. Odpovědnost za správné označení nese správce. Dalším důležitým bodem je dodržení **korektnosti, zákonnosti a transparentnosti** při zpracovávání osobních údajů. Aby bylo zpracování osobních údajů zákonné, musí být splněna nejméně jedna z podmínek uvedených v této podkapitole. Není zde dokonce zapotřebí obdržet souhlas monitorovaných osob. Tento titul by byl těžko splnitelný, nicméně musí být dodržována základní pravidla. Mezi ta patří nezbytnost pro naplnění účelu užívání kamer a přiměřenost k ochraně soukromí monitorovaných osob (Kamerové systémy, 2017).

Mezi nové povinnosti se s příchodem GDPR byl zařazen **rozsah poskytovaných informací**, vedení záznamů o činnosti a neméně důležitá oznamovací povinnost při úniku dat. Vždy je důležité informovat transparentně, stručně a srozumitelně subjekt údajů. Subjekt musí být též informován o kontaktních údajích na správce, pověřence pro ochranu osobních údajů, o účelu zpracování údajů, právním základu pro zpracování údajů a informaci o délce uchování kamerového záznamu (Kamerové systémy, 2017).

Nová povinnost **vedení záznamů** nahrazuje registrační povinnost dle zákona o ochraně osobních údajů. U záznamů je důležité obsáhnout kontaktní údaje na správce, účely zpracování záznamů, popis kategorií osobních údajů, příjemce údajů, ale také plánované lhůty pro výmaz. Záznamy musí být vyhotoveny písemně a správce je povinen je na požádání poskytnout dozorovému úřadu (Kamerové systémy, 2017).

Nakonec se také nesmí zapomenout na **ohlašovací povinnost**. Jakékoliv porušení zabezpečení osobních údajů má být ohlášeno dozorovému orgánu bez zbytečného odkladu, pokud možno do 72 hodin od okamžiku, kdy se správce o problému dozvěděl (Kamerové systémy, 2017).

7 INSTALACE KAMEROVÝCH SYSTÉMŮ

Existuje mnoho typů kamerových systémů a mnoho druhů zařízení, které dokáží zaznamenávat dění ať již v interiéru či exteriéru. Tyto kamerové systémy jsou využívány k hlídání jak soukromých, tak veřejných prostorů a majetku. Níže bude popsáno, jak by měly tyto kamerové systémy být instalovány a jakým způsobem nastaveny, tak aby byl zajištěn správný provoz a nebylo narušováno soukromí ostatních osob.

7.1 Instalace kamerových systémů pro dohled nad rodinnými domy

Na většině rodinných domů, můžeme dnes najít velice moderní kamerové systémy, jejíž pořizovací cena se může pohybovat již kolem tisíce korun. Pořídit si tak v dnešní domě velice kvalitní kamerový systém není vůbec složité, a i jeho instalace je poměrně snadná. Kde však bývá problém, je správné nastavení záběru kamer.

Musí být tedy dodrženo několik základních pravidel. Tím nejdůležitějším je, že musí být monitorován pouze vlastní pozemek, a nikoliv dění na cizím pozemku, či veřejném prostranství. Sledování cizího pozemku je v jakémkoliv případě jednoznačně protiprávním jednáním. Nikdy nesmí být zasaženo do soukromí cizího člověka a nesmíme například monitorovat dění na sousedově zahradě a podobně.

Aby byl provoz kamerového systému v souladu se všemi právními normami, je důležité znát jejich znění a kameru podle nich nastavit. Nejjednodušším způsobem, jak se vyhnout problémům například s Obecným nařízením o ochraně osobních údajů, je stanovit si takové podmínky zaznamenávání prostoru kamerami, aby se na nás daná nařízení nevztahovala. Toho můžeme využít podle článku 2, věcné působnosti:

Článek 2

Věcná působnost

2. *Toto nařízení se nevztahuje na zpracování osobních údajů prováděné:*

   c) *fyzickou osobou v průběhu výlučně osobních či domácích činností;*

Budeme-li tedy provozovat náš kamerový systém pouze na našem pozemku a budeme sledovat pouze denní u nás doma, nemusíme se starat o jakákoliv nařízení GDPR.

7.2 Instalace kamerových systémů pro dohled nad bytovými domy

Z hlediska umístění kamerových systémů do bytových domů je potřeba si prvotně ujasnit, kdo daný kamerový systém instaluje. Nejčastěji kamerové zařízení instaluje vlastník bytového domu za účelem kontroly společných prostorů.

Při pořizování záznamů dění v těchto prostorech dochází ke zpracování osobních údajů a musí se postupovat tak, aby vše probíhalo dle daných právních norem. Jak správně zaznamenávat dění v bytových domech se dá shrnout v několika bodech:

1. Jako první je potřeba si uvědomit, z jakého důvodu chceme instalovat kamery a provádět dozor nad prostory v bytovém domě. Nejčastější důvodem je ochrana života a zdraví, ochrana majetku, prevence před vandalismem. Potřebnost kamerového systému musí každý, kdo kamerový systém hodlá provozovat, pečlivě uvážit a v případě potřeby musí být schopen doložit potřebnost a užitečnost kamerového systému. Provozovatel kamerového systému v bytovém domě je i v průběhu provozu povinen kdykoliv prokázat, že kamerový systém jako prostředek k ochraně majetku a osob ve zvolené lokalitě je s ohledem na jistý zásah do soukromí osob řešením proporcionálním, a to zejména ve vztahu k požadavkům na bezpečnost.
2. Další bodem při zpracovávání osobní údaje prostřednictvím kamerových zařízení je posouzení poměru mezi hodnotami, které mají být chráněny, na jedné straně (např. ochrana života a zdraví, ochrana majetku), a hodnotami, do kterých bude zasaženo, na straně druhé (ochrana soukromí). Každý, kdo hodlá instalovat a provozovat kamerový systém, musí posoudit, zda je zvolený prostředek (kamerový systém) způsobilý a potřebný k dosažení cíle (např. odradit či následně odhalit pachatele krádeže apod.) a vhodně jej kombinovat s dalšími prostředky (např. zamykání dveří, mříže apod.) tak, aby zvolené řešení nepřiměřeně nezasahovalo do práva na soukromí všech lidí, kteří se v prostorách bytového domu mohou pohybovat.
3. Při stanovení prostředků a způsobu zpracování osobních údajů (tj. při nastavení kamerového systému), je nutné přihlédnout k povaze prostor, které mají být sledovány, a to zejména k tomu, zda tyto prostory jsou obvykle průchozí nebo pouze příležitostně navštěvovány, anebo zda slouží jako bezprostřední přístup k bytům, v nichž obyvatelé domu mají nárok na nejvyšší míru soukromí.

4. Dále je si potřeba uvědomit povahu sledovaných prostorů. Veřejná místa, jako jsou sklepy, půdy a vchody do nich, garáže, kočárkárny, kolárny, prostory dopisních schránek, vnější plášť budovy (a jeho bezprostřední okolí), obvykle nevyvolává z hlediska zásad účelného a přiměřeného zpracování údajů zásadní problémy, a proto lze v těchto prostorách kameru instalovat, aniž by byl nutný souhlas vlastníků či nájemníků (pozn. posuzováno z hlediska GDPR). V obdobném režimu jsou obvykle také vstupní dveře do domu, vstupní chodby k výtahům a schodištím i výtahy a schodiště. Ve všech prostorách je třeba dbát na pečlivé nastavení kamerového systému, zejména úhlu záběru kamery ve vztahu k celkovému rozsahu snímaných prostor tak, aby současně, bez dalšího výslovného posouzení dle odstavce 3, nebyla snímána jiná místa, v nichž by sledováním bylo více zasaženo soukromí obyvatel či návštěvníků domu.
5. Na co si dát pozor při instalací kamer v bytových domech jsou vchodové dveře do jednotlivých bytů. jedná o prostory, jejichž záběry mohou podstatně více vypovídat o soukromém životě obyvatel domu. Provozováním kamerového systému zaměřeného na konkrétní byty může docházet k závažným zásahům do práva na ochranu soukromého a osobního života a lze jej uskutečnit jen ve výjimečných a odůvodněných případech, a to se souhlasem obyvatel dotčených bytů.
6. Z praxe je známo, že provoz kamerového systému nelze založit na souhlasu se zpracováním osobních údajů získaného od všech obyvatel a návštěvníků domu, tento souhlas lze totiž následně kdykoliv odvolat a přináší problémy nejen v případě časté změny nájemníků nebo majitelů bytů apod., ale také nezletilých osob. Potřebným souhlasem není ani „souhlas většiny“, tj. usnesení společenství vlastníků jednotek či družstva k realizaci kamerového projektu, jedná se toliko o faktor zdůvodňující potřebnost kamerového systému.
7. V dalším bodě je potřeba si dát pozor na dobu uchovávání získaných záznamů. Tato doba musí být stanovena tak, aby nepřesáhla dobu potřebnou k tomu, aby incident zaznamenaný kamerou bylo možno dále prošetřit a zajistit další nezbytné informace potřebné například k předání záznamu příslušným orgánům či pojišťovně. Takovou dobou je obvykle nejvýše 7 dnů, v případě příležitostně navštěvovaných prostor uvedených v odstavci 5 pak až 14 dnů. V odůvodněných případech může správce dobu prodloužit.

8. Často opomíjeným krokem při zpracovávání osobních údajů prostřednictvím kamerových systémů je, že se zapomíná na povinnost informovat dotčené osoby o možném zpracování jejích osobních údajů. Může tak být provedeno například prostřednictvím schůze shromáždění společenství vlastníků jednotek a následným vyvěšením nebo rozesláním informace o zpracování všem obyvatelům domu, a to ještě před zahájením zpracování. Informační povinnost vůči obyvatelům domu je nutno plnit v plném rozsahu požadovaném zákonem, neboť tento okruh subjektů údajů je správci předem znám, a ten má tak možnost bez zbytečného odkladu informovat ještě před zahájením shromažďování údajů. Uvedené platí i v případě nových obyvatel domu, kteří se do něj přistěhují již po instalaci a spuštění kamerového systému.
9. V bytovém domě se ovšem pohybují i osoby, které do bytového domu budou přicházet nepravidelně, resp. nepředvídatelně, je správce povinen splnit informační povinnost alespoň umístěním informačních tabulek u všech vstupů do sledovaných prostor (vč. vstupu do výtahu). Informační tabulka musí obsahovat alespoň informaci, že prostor je sledován kamerovým systémem, musí zde být uveden správce – provozovatel kamerového systému, resp. kontaktní osoba nebo sdělení, kde bude subjektu údajů poskytnuta (např. v písemné podobě) kompletní informace o zpracování v rozsahu požadovaném zákonem.

Obrázek 2 – Příklad informační tabule

o provozu kamerového systému

(Zdroj: Informační tabule, 2021)

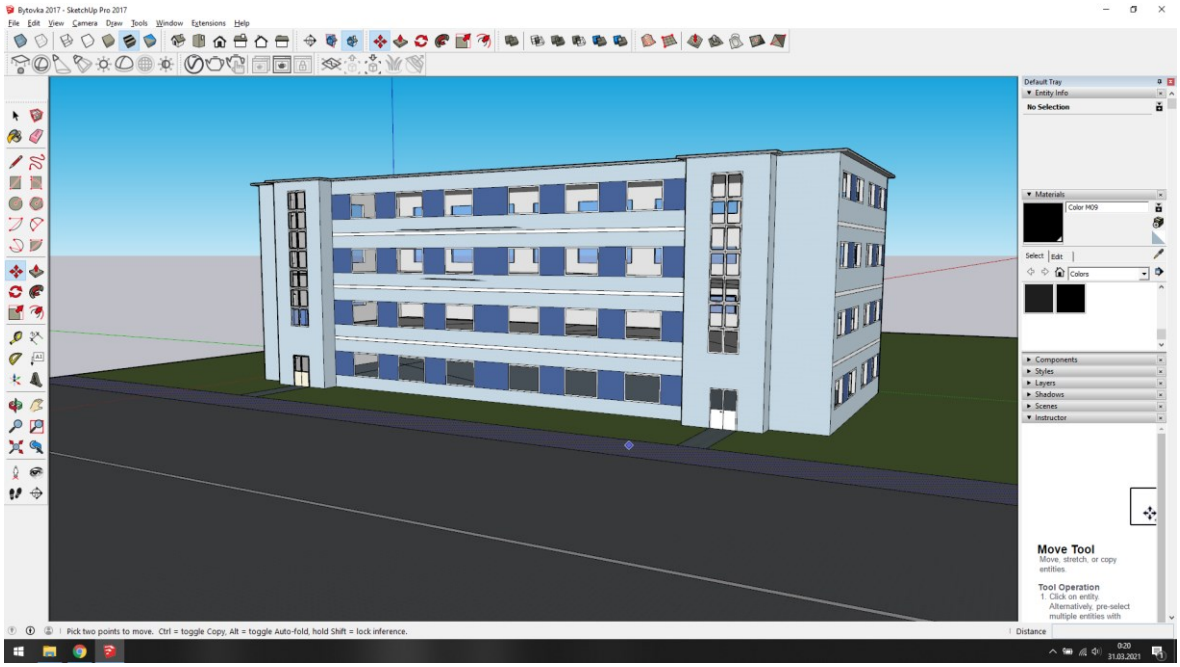
10. Kamerový systém není nutno registrovat u Úřadu pro ochranu osobních údajů. Dnem 25. května 2018 nabylo účinnosti obecné nařízení (GDPR), které již podobnou registrační povinnost neukládá. Místo registrace má v souvislosti s provozováním kamerového záznamu správce povinnost vést záznamy o činnostech zpracování.

11. Je nutno určit úzký okruh osob, jež mají k zařízení přístup a jimž jediným jsou známa hesla, dále vymezit případy, kdy tyto osoby mohou k záznamům přistupovat (většinou jen případy podezření z konkrétní trestné činnosti či přestupku a škody na majetku) a stanovit kompetence a postup, jak s nimi mohou nakládat, včetně způsobu a dokumentování předání části záznamu dalším osobám (orgánům činným v trestním řízení, obecní policii, pojišťovně). Všechny přístupy k záznamům a operace s kamerovými záznamy musí být evidovány („logovány“), aby bylo zřejmé, kdo, kdy a z jakého důvodu do záznamů nahlížel. Nelze tedy libovolně přistupovat ke kamerovému systému a jeho záznamům (a manipulovat s nimi) mimo stanovený bezpečnostní režim, bez důvodu prověření konkrétního incidentu. Správce je povinen přijmout a dokumentovat řadu bezpečnostních opatření (Stanovisko č. 1/2016, 2016).

8 PRAKTICKÉ MODELY ZOBRAZENÍ NEJLEPŠÍHO UMÍSTĚNÍ KAMER

V předchozích kapitolách bylo uvedeno, co vše je potřeba dodržet pro správnou instalaci kamerových systémů, a jak by měl probíhat dohled nad budovami.

Tyto informace si je potřeba znázornit i prakticky. Tomu se věnuje následující kapitola, ve které bylo díky grafickému programu SketchUp vytvořen 3D model rodinného domu a v následující podkapitole i bytového domu. Při vytváření těchto modelů bylo vycházeno z reálných budov. Z hlediska typu instalovaných kamer se předpokládá umístění zařízení vybavené záznamem, tedy možností ukládat natočené video, či vyfocené fotky na nějakém uložišti.



Obrázek 3 – Průběh vytváření modelu bytového domu
(Zdroj: SketchUp, vytvořeno autorem)

8.1 Praktické znázornění umístění kamer u rodinného domu

Jak již bylo zmíněno, následující kapitola se bude věnovat grafickému znázornění možného provedení instalace kamerových systémů.

Na obrázku č. 4 lze vidět hotový model reálného rodinného domu, na kterém bylo v programu umístěno několik kamer.

Obrázek 4 - Finální podoba modelu rodinného domu
(Zdroj: SketchUp, vytvořeno autorem)

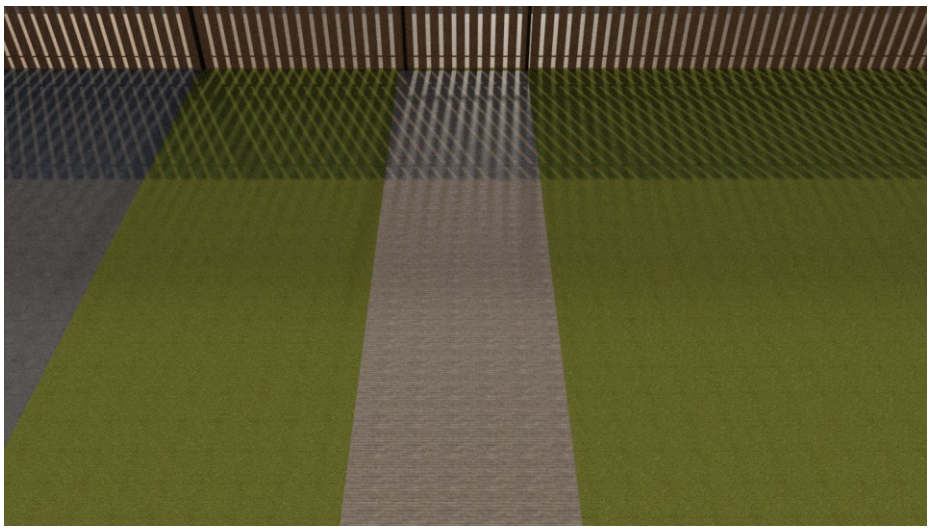
Z praktického hlediska je potřeba kamery umísťovat, tak aby zaznamenávaly co největší plochu našeho hlídaného prostoru, či objektu. Omezujícím faktorem je zde rozsah záběru kamery. Kamera nesmí zabírat dění na cizím pozemku, a ani na veřejném prostranství.

Jedno z nejdůležitějších míst, které je potřeba u rodinného domu hlídat je příchodová cesta. Kameru je nejlepší umístit přímo nad vchodové dveře a sklonit jí tak, aby záběr končil poblíž branky a dřevěného plotu, jako na obrázku č. 5.

Obrázek 5 – Zaznamenávaný úsek kamery nad vchodem
(Zdroj: SketchUp, vytvořeno autorem)

Zde je důležité se vyvarovat zaznamenávání dění na veřejném prostranství, tedy v tomto případě na chodníku před domem. Kameru by bylo možné ještě posunout více směrem ke garážovým vratům, aby byl zajištěn i monitoring příjezdové cesty.

Výhled z kamery nad vchodem by mohl vypadat následovně, jak jde vidět na obrázku č. 6.



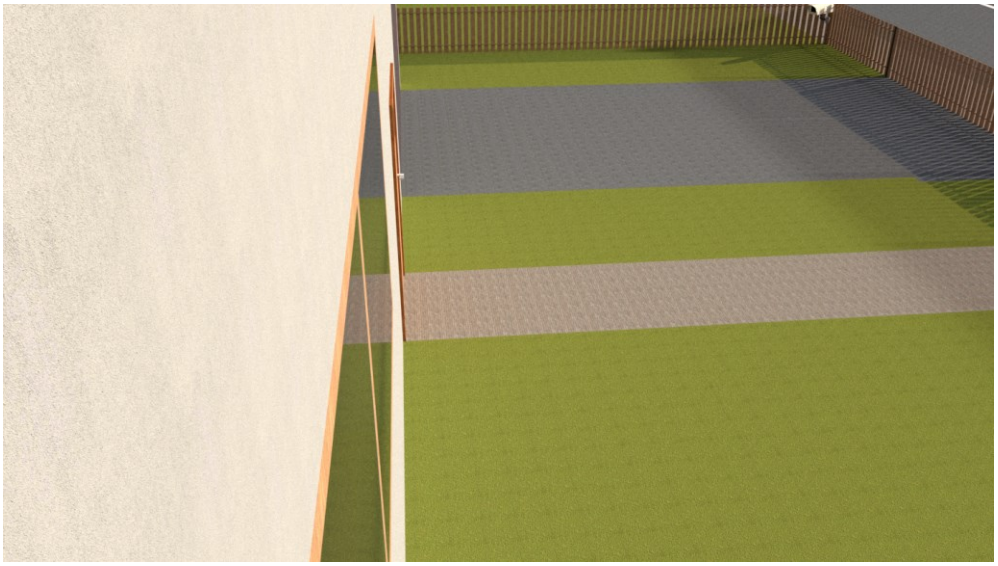
Obrázek 6 – Výhled z kamery umístěné nad vchodem
(Zdroj: SketchUp, vytvořeno autorem)

Dalším možným místem pro ideální umístění kamery by mohl být levý roh domu. Zde by kamera měla zabírat jak příchodovou cestu, tak příjezdovou. Oproti předchozímu umístění kamery je zde možnost sledovat částečně vstupní dveře a garážová vrata.

Obrázek 7 – Zaznamenávaný úsek kamery na levém rohu
(Zdroj: SketchUp, vytvořeno autorem)

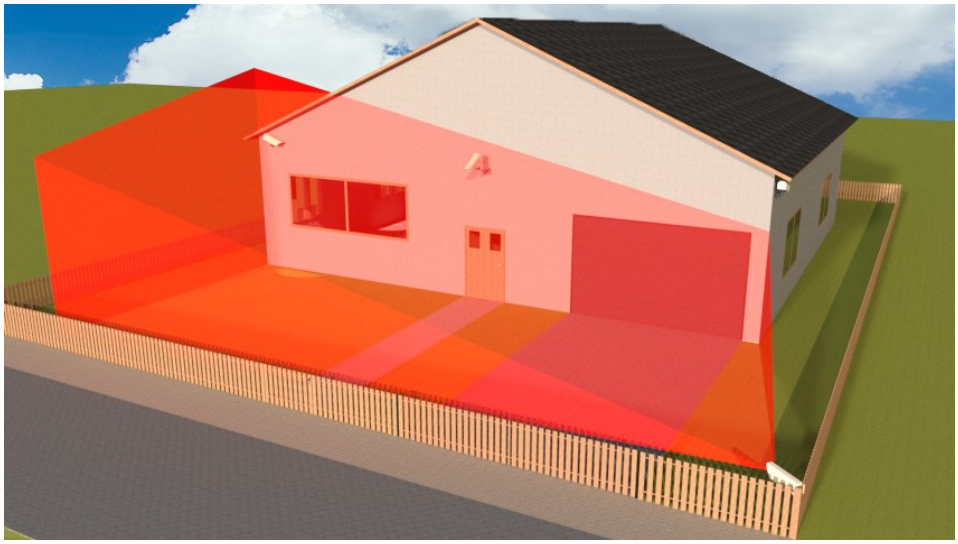
Opět je důležité dbát na dostatečný sklon kamery a zajistit, aby záběr kamery nepřesáhl plot na našem pozemku a nebylo zaznamenáváno dění na veřejném prostranství, či sousedově pozemku.

Na obrázku č. 8 jde již vidět, jak by vypadal výsledný záznam. Díky tomuto záběru máme dostatečně pokrytý sledovaný prostor před domem a zároveň nedochází k narušování soukromí osob pohybujících se okolo domu.



Obrázek 8 – Výhled z kamery umístěné na levém rohu
(Zdroj: SketchUp, vytvořeno autorem)

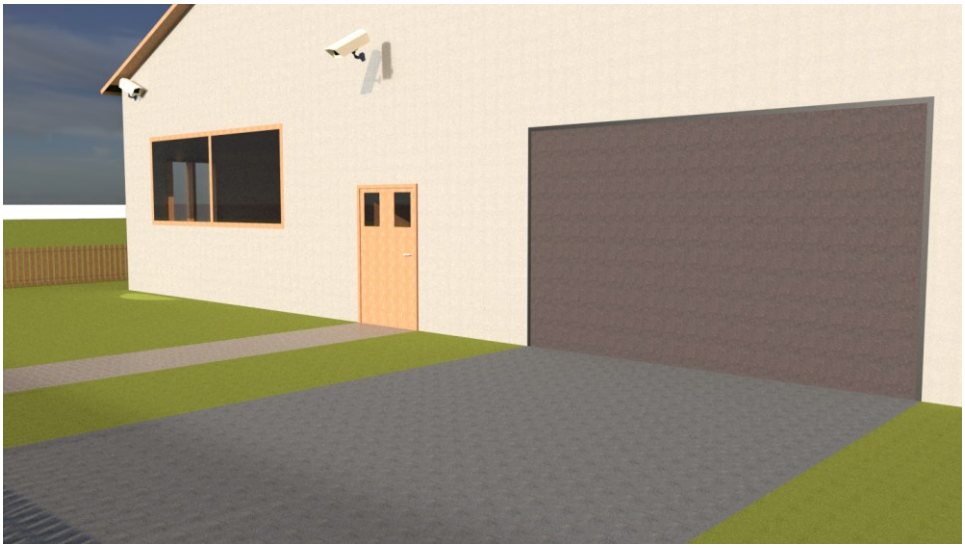
Kdybychom chtěli mít co nejlepší výhled na vstupní dveře a garážová vrata, případně okna, je ideálním řešením následující umístění kamery na obrázku č. 9. Kameru je navíc možné umístit pod úroveň plotu. Tím tak dojde k částečnému schování kamery.



Obrázek 9 – Zaznamenávaný úsek kamery umístěné v rohu pozemku
(Zdroj: SketchUp, vytvořeno autorem)

Jak jde vidět na obrázku č. 10, díky této kameře je možné dobře dohlížet na dění kolem garáže, vstupních dveří a oken.

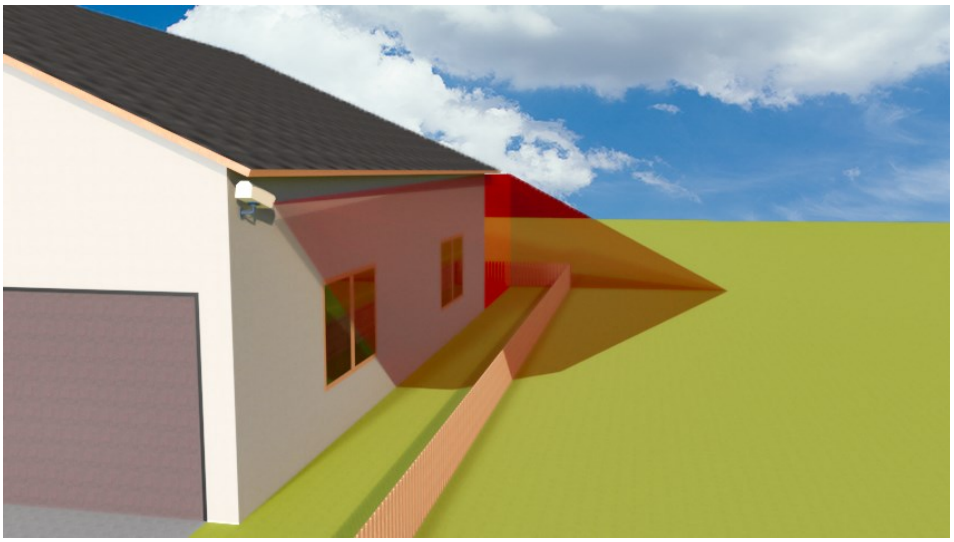
Další velkou výhodou tohoto umístění kamery je, že je naprosto vyloučena možnost monitorování dění na veřejném prostranství a nemůže tak dojít k porušení soukromí lidí na ulici.



Obrázek 10 – Výhled z kamery umístěné v rohu pozemku
(Zdroj: SketchUp, vytvořeno autorem)

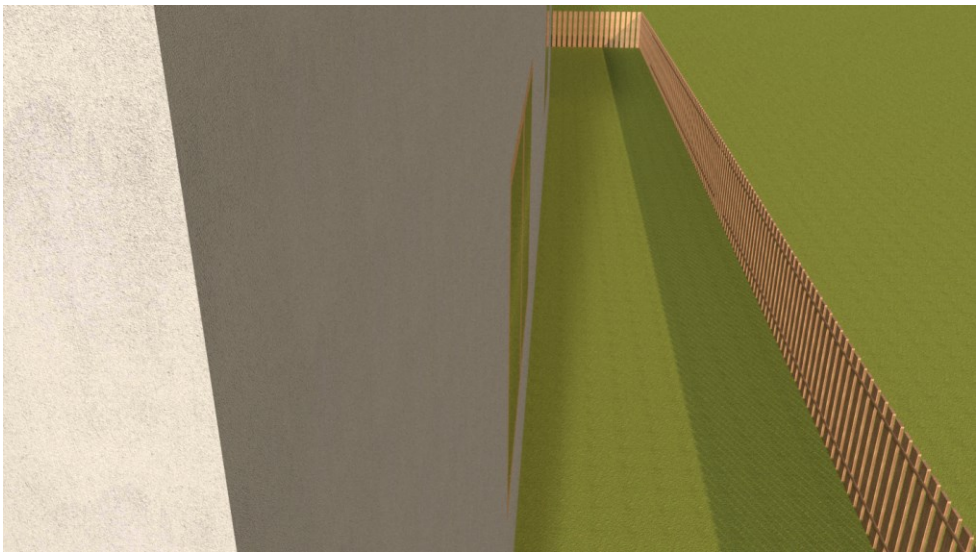
Rodinné domy je ovšem také důležité hlídat i z ostatních stran než jen předních. V případě možného pokusu vniknutí cizí osoby do domu za jakýmkoliv protiprávním důvodem je právě

velice pravděpodobné, že bude využito jiných vchodů než těch z předních stran domů. Co se týká bočních stran domů, je zde především riziko vniknutí zlodějů do domu přes okno. V případě následného umístění kamery na roh domu by mohl být ten to prostor pokryt a majitel domů by měl přehled nad děním v této části rodinného domu.



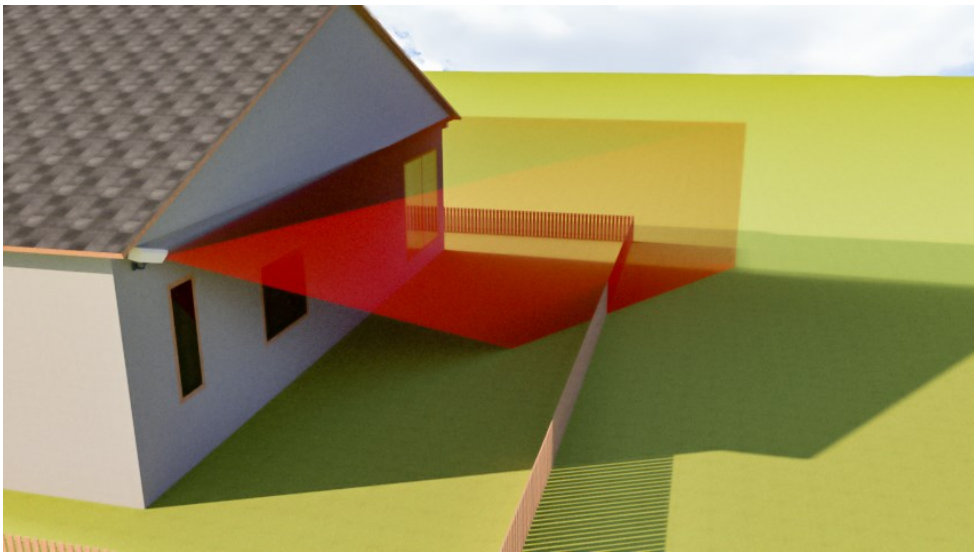
Obrázek 11 – Zaznamenávaný úsek kamery umístěné na pravém rohu domu
(Zdroj: SketchUp, vytvořeno autorem)

Následný výhled z kamery zabírá co největší část boční strany domu a plotu a je tak zajištěný monitoring daného prostoru. Snímání místa za plotem je potřeba omezit na co nejmenší míru a zajistit, aby případné cizí osoby nacházející se mimo náš pozemek nebyly zaznamenávaný a nedocházelo tak k porušování ochrany osobních údajů a soukromí.



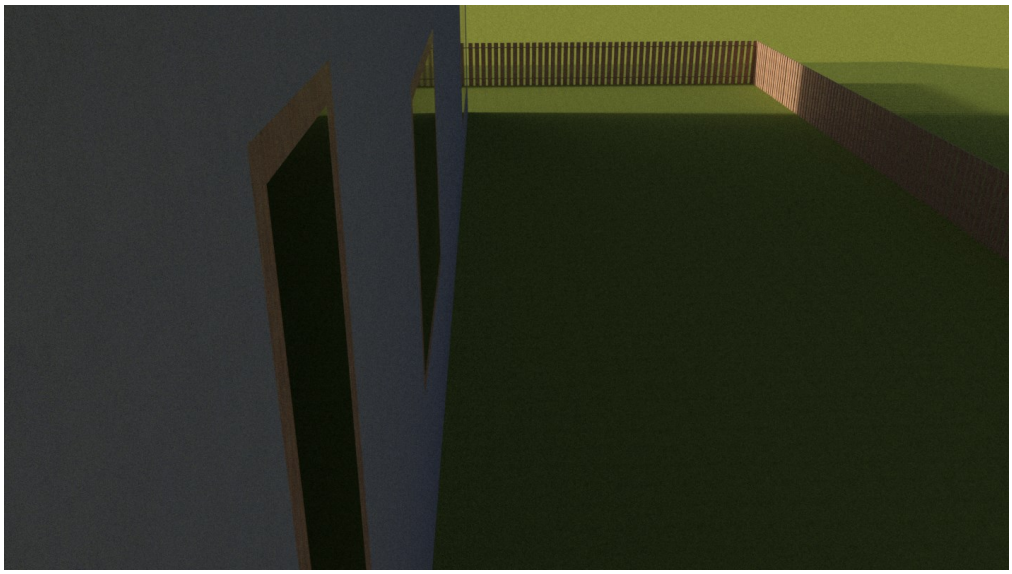
Obrázek 12 – Výhled z kamery umístěné na pravém rohu domu
(Zdroj: SketchUp, vytvořeno autorem)

Největší pravděpodobnost vniknutí cizí osoby do domu je ovšem přes zadní stranu domu, která je kryta od veřejného prostranství ze přední strany domu a je tak minimální šance, že by byla tato osoba vyrušena při neoprávněném vstupu do domu. Jedná se tedy o jedno z nejdůležitějších míst, kde je možné umísit kameru.



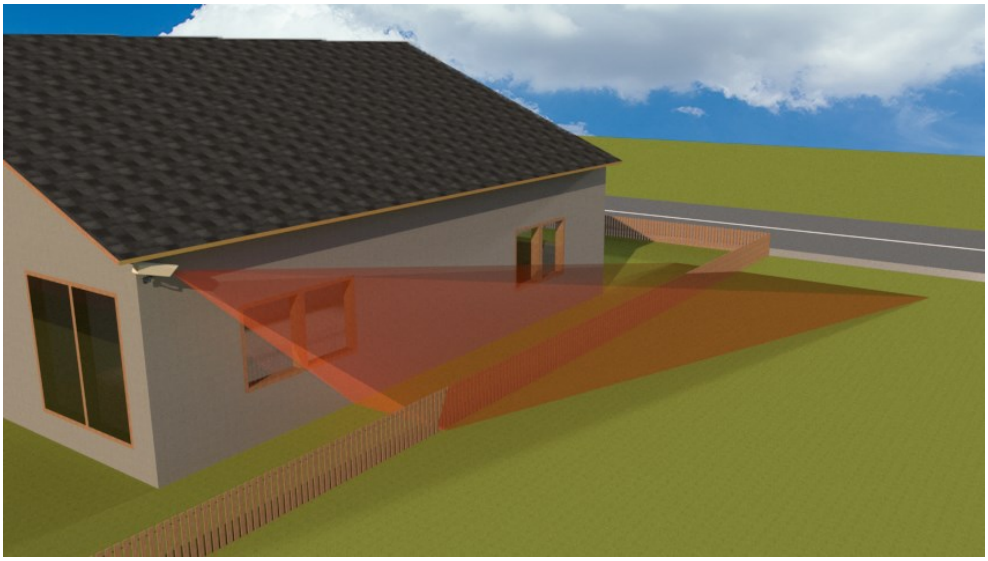
Obrázek 13 – Zaznamenávaný úsek kamery umístěné na zadní straně domu
(Zdroj: SketchUp, vytvořeno autorem)

Výsledný záznam plně pokryje oblast zadního vchodu i oken a dojde tak k dostatečnému dohledu nad tímto rizikovým prostorem. Zároveň je i zde potřeba věnovat pozornost možnému omezení zaznamenávaného prostoru kvůli zamezení snímání cizího pozemku.



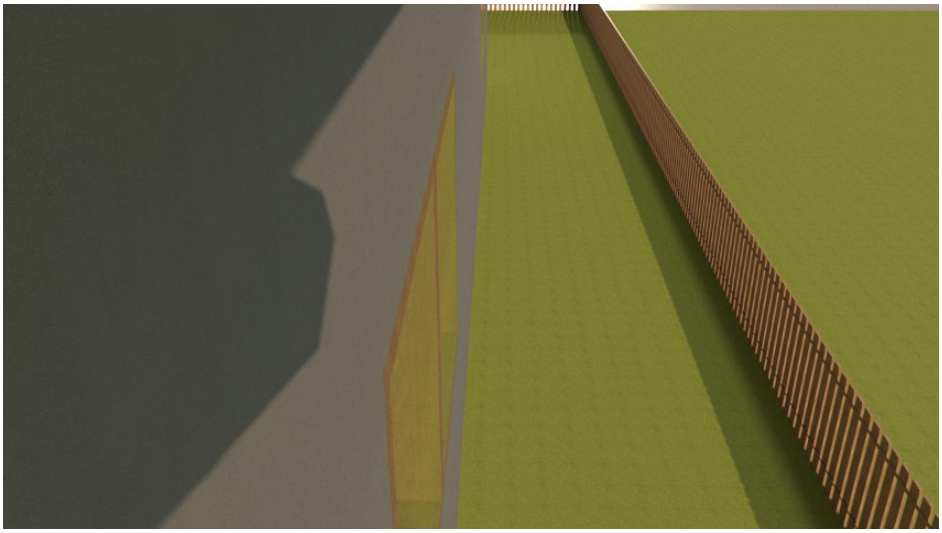
Obrázek 14 – Výhled z kamery umístěné na zadní straně domu
(Zdroj: SketchUp, vytvořeno autorem)

Poslední vhodnou pozicí pro umístění kamery je boční strana domu. Zde by mohla záběr kamery směřovat k veřejné silniční komunikaci. Z hlediska zabezpečení se jedná o dobrou pozici pro kameru, ale zároveň je zde největší pravděpodobnost porušení ochrany osobních údajů a soukromí cizích osob pohybujících se na veřejném prostranství.



Obrázek 15 – Zaznamenávaný úsek kamery umístěné na levé straně domu
(Zdroj: SketchUp, vytvořeno autorem)

Kvůli výše zmíněnému riziku je proto potřeba omezit snímaní kamery pouze na náš pozemek a vyhnout se monitorování dění na veřejném prostranství. Tímto prostranstvím se zde rozumí především chodník před domem. Poskytovat záznamy s děním na tomto místě by bylo porušením ochrany osobních údajů a soukromí osob, vyskytujících se na tomto místě.



Obrázek 16 – Výhled z kamery umístěné na levé straně domu
(Zdroj: SketchUp, vytvořeno autorem)

8.2 Praktické znázornění umístění kamer u bytového domu

V přechozí kapitole bylo znázorněno na vytvořeném modelu rodinného domu ideální varianty umístění kamer. Ale s kamerovými systémy se můžeme setkat i u bytových domech. Zde se jedná především o dohled nad venkovními prostory. Stejně jako u rodinného domu, i zde bylo při tvorbě modelu vycházeno z reálného bytového domu.

Na následujícím obrázku lze vidět již hotový model domu na kterém bylo umístěno 6 kamer. Jedná se se především o dohled nad vchodem, příchodovou cestou a okolí bytového domu. Opět je důležité dodržet zaznamenávaný prostor na hranici našeho pozemku.

Obrázek 17 – Výsledný model bytového domu

(Zdroj: SketchUp, vytvořeno autorem)

Instalovat kamerový systém na bytový dům muže pouze majitel bytového domu, nebo odborná firma na žádost majitele domu. Zpracování osobních údajů je z hlediska GDPR možné, a to přesně díky článku 6, kde je zmíněno, že zpracování je zákonné, pouze pokud je splněna podmínka aspoň jedna z následujících podmínek:

a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;
b) 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;
c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;

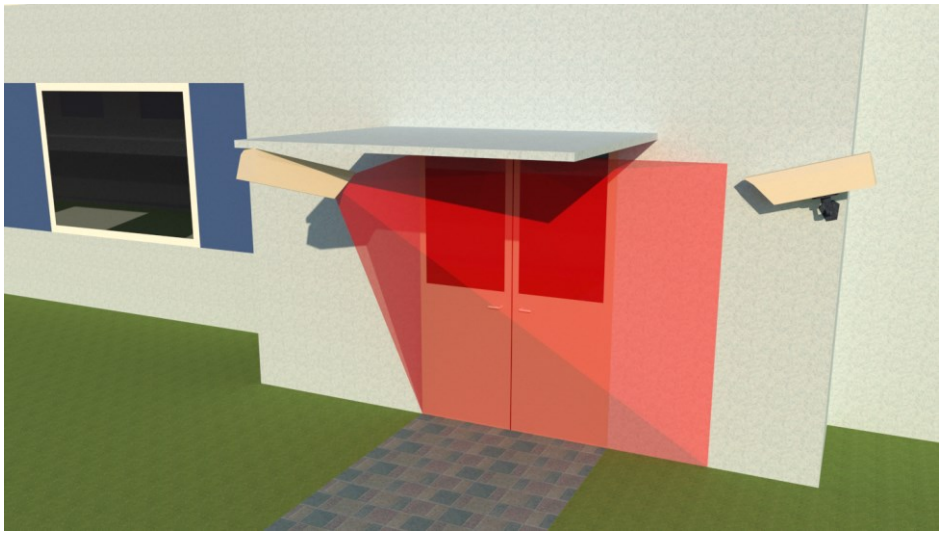
d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;
e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;
f) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce 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.

Z hlediska těchto podmínek by majitel bytového domu mohl využít podmínky první a získat písemný souhlas o možnosti zpracovat osobních údaje všech lidí bydlících v domě. Problém nastává ve chvíli, kdy se v bytovém domě začnou pohybovat osoby, které v domě nebydlí, například návštěva některých obyvatel domu. Druhým negativem písemných souhlasů je, že jsou kdykoliv odvolatelné. Může tak kdykoliv dojít k odvolaní písemného souhlasu a zaznamenávání se stane tím pádem protiprávním.

Ideálním případem je tedy využití podmínek, kdy je zpracování důležité pro ochranu životně důležitých zájmů, či pro ochranu oprávněných zájmů příslušného správce či třetí strany.

Dále je nutné splnit informační povinnost a před monitorované prostory umístit cedule s informací, že je daný prostor monitorován.

Na obrázku č. 18 lze již vidět první z možných míst, kam je možné umístit kameru. Při tomto umístění dojde k monitorování hlavních vstupních dveří. V blízkosti těchto vstupních dveří se často nachází poštovní schránky či zvonky. Umístění kamerového systémů je tedy pro dohled nad tímto místem klíčový.

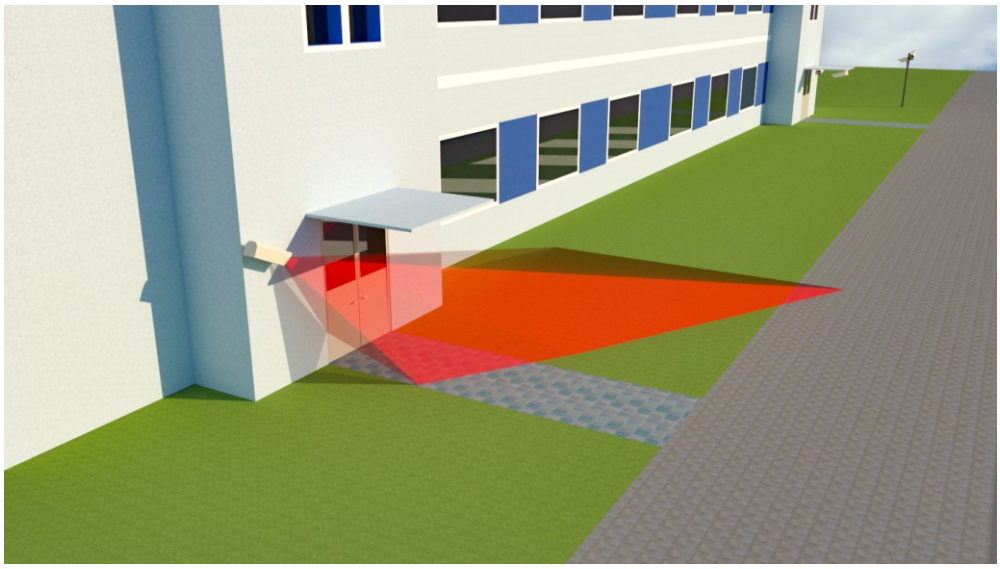


Obrázek 18 – Zaznamenávaný úsek kamery umístěné nad vchodem
(Zdroj: SketchUp, vytvořeno autorem)

Na tomto záznamu jsou monitorovány pouze osoby bydlící přímo v bytové domě a zároveň se pohybující ve společných prostorách domu. Kamery mohou samozřejmě zachytit i cizí lidi, kteří nebydlí v tomto domě, ovšem pokud byla splněna informační povinnost a tito lidé jsou předem správně upozorněními, že vstupují do monitorovaného místa, tak lze tento provoz kamerového systému považovat za správný.

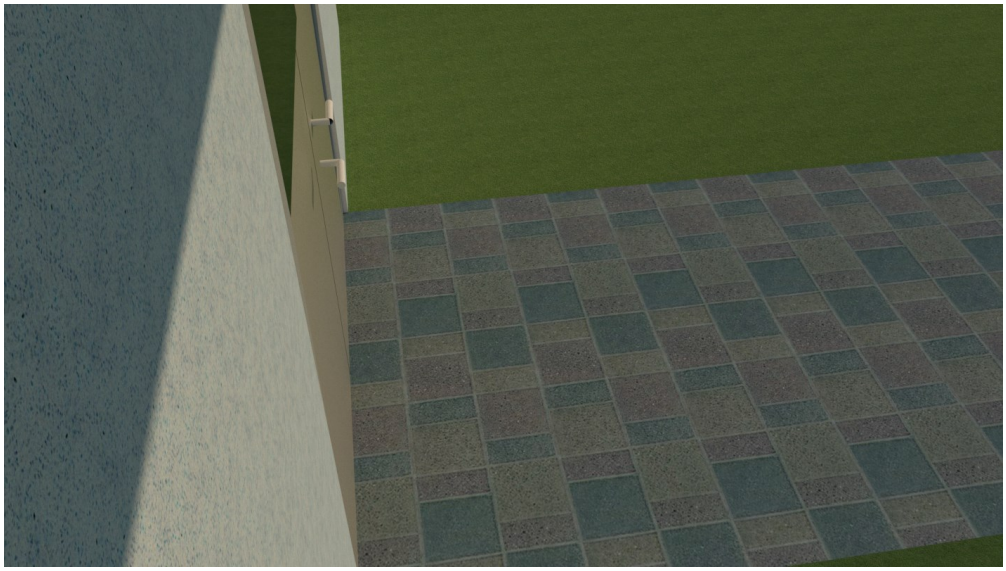
Obrázek 19 – Výhled z kamery umístěné nad vchodem
(Zdroj: SketchUp, vytvořeno autorem)

Další variantou by bylo umístění kamery na stejném místě, ale otočenou směrem do ulice. Zde by došlo k lepšímu monitorování dění v blízkosti bytového domu.



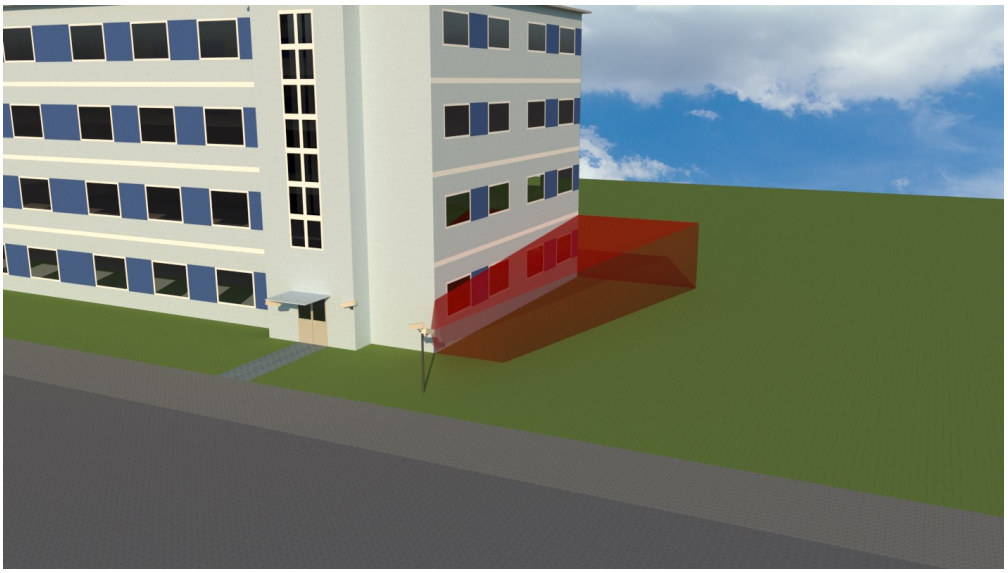
Obrázek 20 – Zaznamenávaný úsek kamery umístěné nad vchodem
(Zdroj: SketchUp, vytvořeno autorem)

Takto by vypadal výsledný záznam. Vstup o domu je kontrolován a zároveň je zamezeno monitoringu veřejného prostranství, tedy chodníku před domem. Je-li bytový dům vybaven dvěma vchody, je možné umístit takto kamery nad každý vchod.



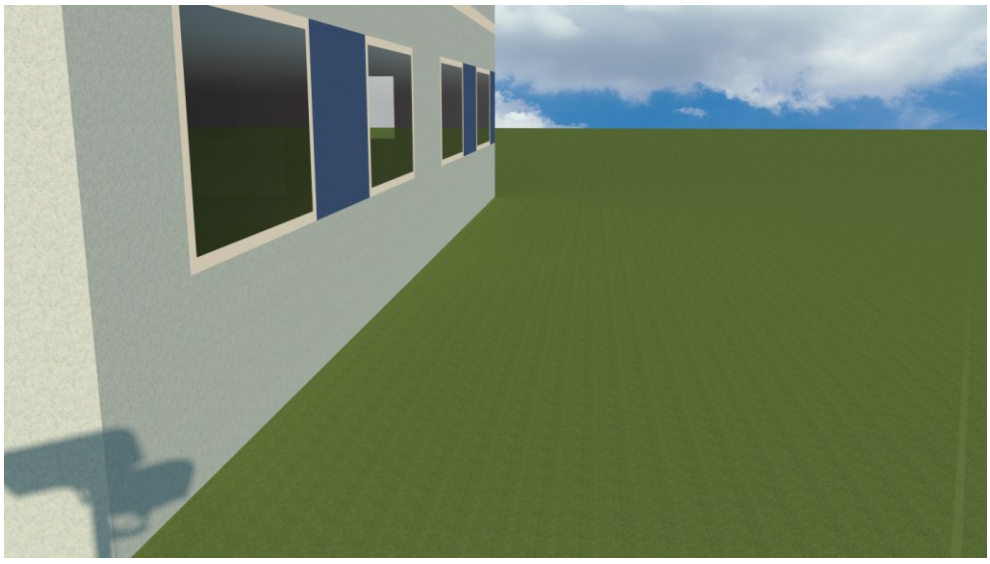
Obrázek 21 – Výhled z kamery umístěné nad vchodem
(Zdroj: SketchUp, vytvořeno autorem)

Další variantou, jak by se dalo okolí bytového domu monitorovat je, že se kamera umístí na jeden z rohu domu, ideálně na stožár, jak je zobrazeno na obrázku níže.



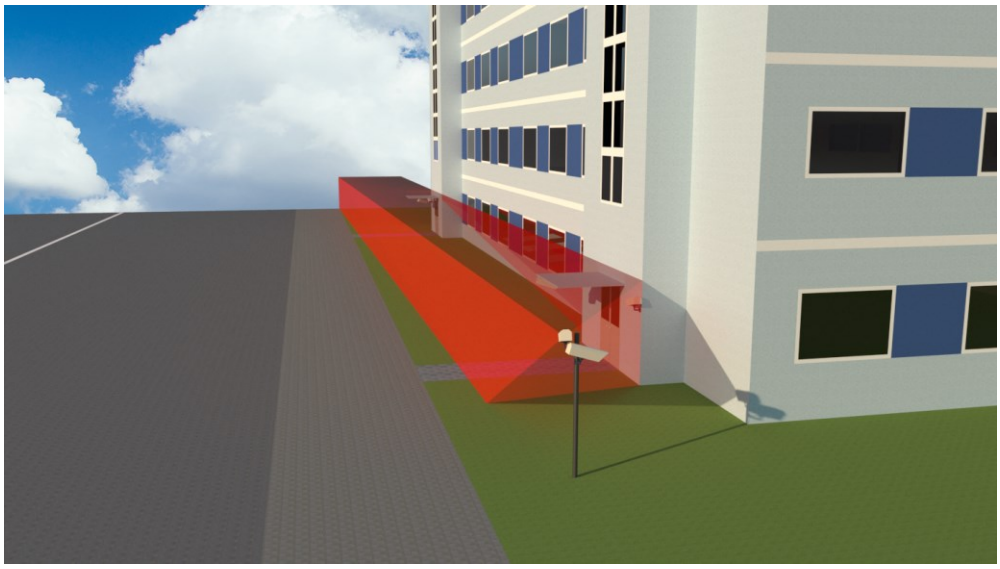
Obrázek 22 – Zaznamenávaný úsek kamery umístěné na rohu
(Zdroj: SketchUp, vytvořeno autorem)

První kamera umístěna na stožáru zaznamenává především boční stranu bytového domu, kde se mohou pohybovat cizí osoby bez možného vyrušení z veřejného prostranství.



Obrázek 23 – Výhled z kamery umístěné na rohu
(Zdroj: SketchUp, vytvořeno autorem)

Druhá kamera umístěna na stožáru, na rohu domu by byla výhodná především kvůli umožnění dohledu nad oběma vchody a zároveň okny v přízemí.



Obrázek 24 – Zaznamenávaný úsek kamery na rohu domu
(Zdroj: SketchUp, vytvořeno autorem)

Takto by vypadal výsledný záznam. Oba vchody jsou monitorovány a je pokryt velký prostor okolo domu. Zaznamenávání dění na veřejném prostranství je zde také zamezeno.

Obrázek 25 – Výhled z kamery umístěné na rohu domu
(zdroj: SketchUp, vytvořeno autorem)

9 ANALÝZA VZTAHU OBYVATELSTVA K PROBLEMATICE OCHRANY OSOBNÍCH ÚDAJŮ

Rozšířenost kamerových systému je v dnešní době obrovská a prakticky na každém domě lze umístit zařízení schopné pořizovat audiovizuální záznamy. Většina obyvatelstva je s touto skutečností seznámena. Ke zjištění, zda lidé znají své práva a povinnosti při pořizování audiovizuálních záznamů, a jak si dokáží chránit svoje soukromí, bude níže využito dotazníkového šetření, díky kterému bude získáno velké množství reálných informací.

9.1 Stanovení výzkumných otázek a hypotéz

Před analýzou vztahu obyvatelstva k problematice ochrany osobních údajů je potřeba si stanovit hranice zkoumaného problému. Tedy je potřeba si uvědomit, co od dotazníkového šetření očekáváme a jaké jsou předpoklady výsledku. Ke stanovení rozsahu a hranic zkoumaného problému slouží definování výzkumného problému, výzkumných otázek a hypotéz.

Pro přesné vymezení, co chceme zkoumat je potřeba si stanovit výzkumný problém.

Výzkumný problém

Porušování ochrany osobních údajů a soukromí prostřednictvím kamerových systémů.

Výzkumné otázky

- Jak dochází k porušení ochrany osobních údajů a soukromí v kontextu audiovizuálních záznamů?
- Proč dochází k porušení ochrany osobních údajů a soukromí v kontextu audiovizuálních záznamů?
- Kdo porušuje ochranu osobních údajů a soukromí v kontextu audiovizuálních záznamů?
- Kdo může být obětí porušení ochrany osobních údajů?
- Jaký je vztah obyvatelstva k problematice ochrany osobních údajů?
- Jaké jsou znalosti obyvatelstva v oblasti ochrany osobních údajů?

Výzkumnými otázkami dané téma lze lépe popsat a následně z nich vyvodit jisté hypotézy.

Hypotézy

Hypotézu můžeme označit jako předpoklad současného stavu. Snažíme se ji výzkumem ověřit – tedy zamítnout nebo nezamítnout. Zde byly stanoveny následující hypotézy:

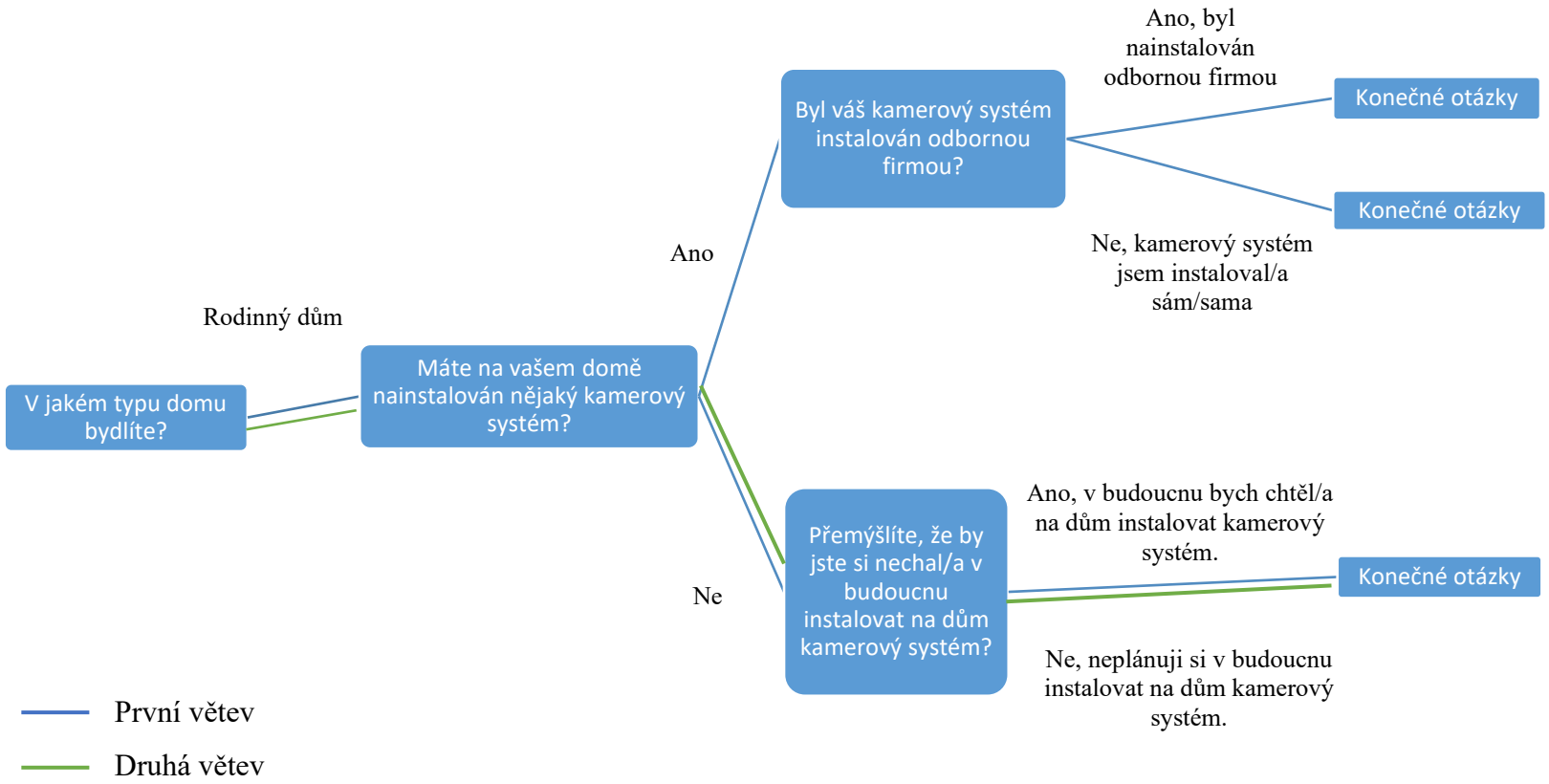
1. K porušení ochrany osobních údajů dochází při špatné instalaci kamerového systému.
2. K porušení ochrany osobních údajů dochází především v bytových domech.
3. Lidé s nižší znalostí problematiky ochrany osobních údajů, jsou více optimističtí vůči možnému narušení jejich soukromí.
4. Na mnoha domech jsou instalovány kamerové systémy lidmi s nízkou znalostí problematiky ochrany osobních údajů.

9.2 Dotazníkové šetření

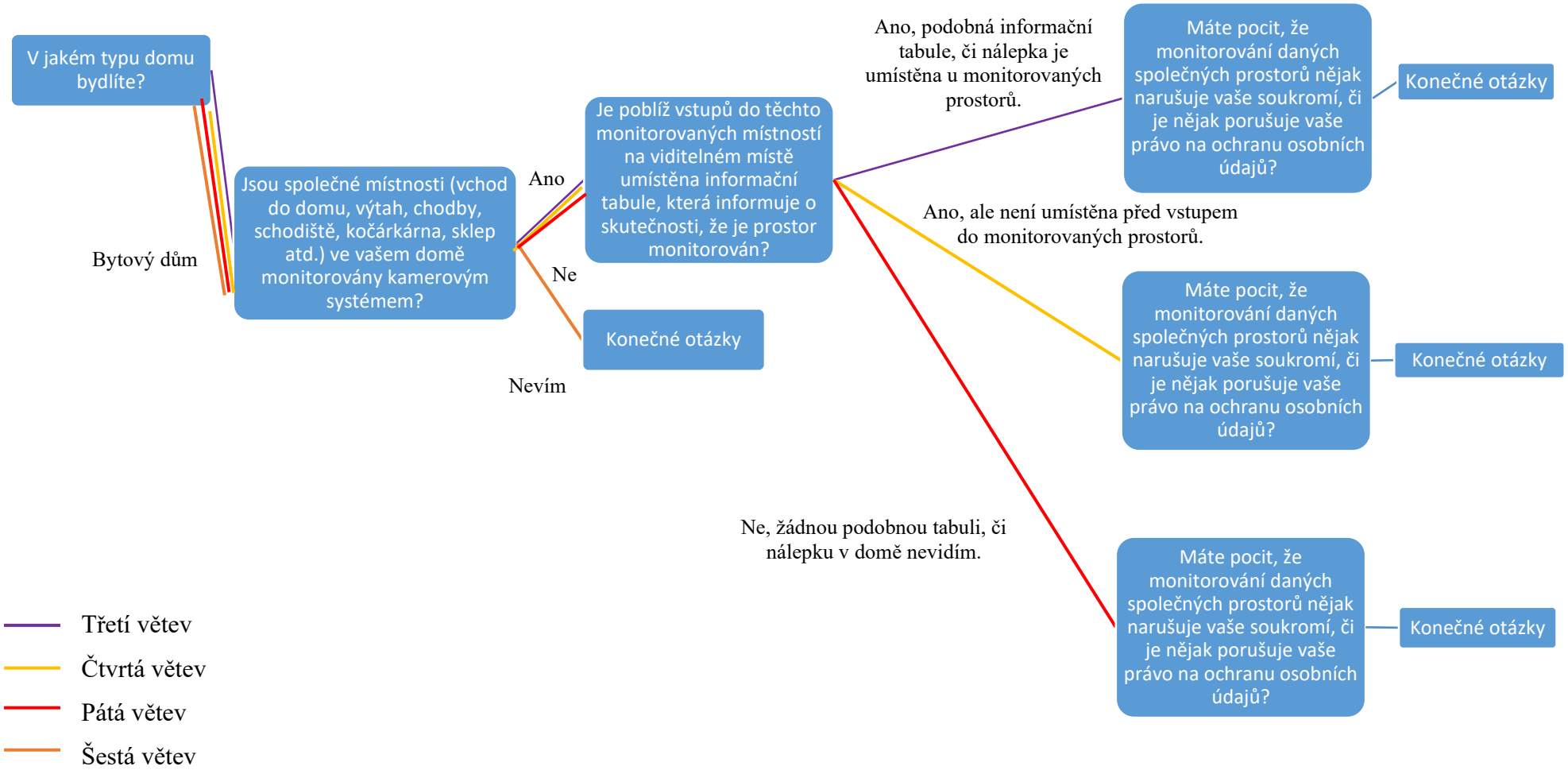
Součástí praktické části je i dotazník. Tento dotazník, byl vytvořen s cílem analyzovat vztah obyvatelstva k problematice ochrany osobních údajů v kontextu audiovizuálních záznamů. Mezi další cíle lze zařadit i snahu zjistit kolik kamerových systému je pravděpodobně špatně naistalováno a může tak porušovat soukromý cizích osob. Samotný dotazník má složitější strukturu. Je vytvořen v několika úrovních a pro získání co nejkvalitnějších odpovědí jsou respondenti rozdělení dle jejich odpovědí a dále vedení dotazníkem na rozdílné otázky. Tyto specifické otázky mají za cíl získat co nejlepší informace o aktuální vztahu jednotlivých respondentů k problematice ochrany osobních údajů v kontextu audiovizuálních záznamů.

Pro lepší pochopení struktury dotazníku, je rozdělen na šest odvětví, jak lze vidět na obrázku č. 26 a 27, vycházejících z první otázky. Samotný dotazník byl vytvořený přes on-line aplikaci Formuláře Google. Jeho vyplňování probíhalo on-line, a to právě skrze tuto aplikaci. Tento dotazník byl distribuován pomocí sociálních sítí. Respondentem mohl být kdokoliv, kdo měl zájem tento dotazník vyplnit. Samotný dotazník je rozdělen do několika úrovní. První otázku měli všichni respondenti společnou, k dalším otázkám se rozdělili dle jejich odpovědí. Na tento dotazník odpovídalo 100 respondentů. Níže budou vypsány a zobrazeny otázky a grafy výsledů získaných z dotazníku. Následně je každá otázka okomentována a vyhodnocena každá odpověď.

9.3 Struktura a obsah dotazníku



Obrázek 26 – Schéma rozdělení dotazníků podle odpovědí, větev rodinného domu (Zdroj: Vlastní)



Obrázek 27 - Schéma rozdělení dotazníků podle odpovědí, větev bytového domu (Zdroj: Vlastní)

První větev

Otázka:

- V jakém typu domu bydlíte?
- Máte na vašem domě nainstalován nějaký kamerový systém?
- Byl váš kamerový systém instalován odbornou firmou?
- Konečné otázky.

Odpověď: Rodinný dům

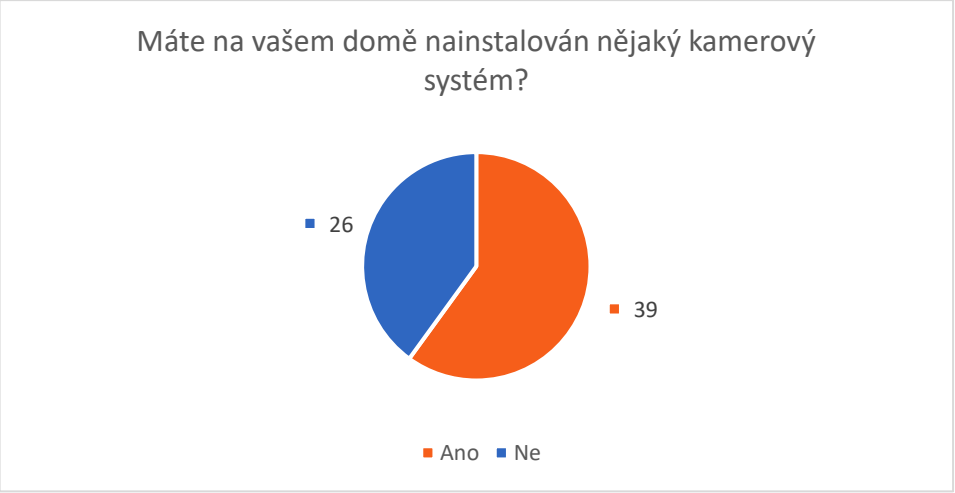
Graf 1 Graf odpovědí na první otázku (Zdroj: Vlastní)

První otázka je pro všechny odvětví stejná. Na tomto dotazu začínal každý respondent a dále se již rozdělovali podle odpovědí. Sto respondentů se zde rozdělilo do dalších větví dotazníků.

První otázka měla za úkol rozdělit respondenty na dvě skupiny, těch, co bydlí v rodinném domě a těch so žijí v bytovém domě. Z této získané informace bylo dále vycházeno a vztahovaly se k ní výsledky odpovědí na další otázky. 65 % respondentů odpovědělo, že žijí v rodinném domě a 35 % v domě bytovém. Početně se tedy jedná o 65 lidí v rodinném domě a 35 v bytovém domě.

Z této první otázky se bude dále pokračovat na další, a to podle odpovědi. První větev, kterou mohl být respondent veden pokračuje po odpovědi na první otázku, že žije v rodinném domě.

Odpověď: Ano



Graf 2 - Graf odpovědí na druhou otázku (Zdroj: Vlastní)

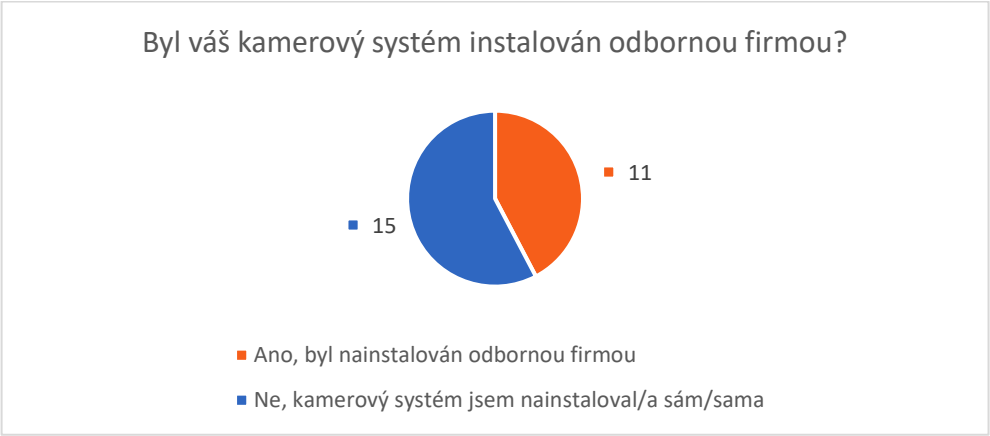
Tato otázka sloužila pro zjištění, jakým směrem je potřeba dále respondenta vést. Zda je možné se ho ptát na detaily ohledně kamerových systémů v jeho okolí, či nikoliv.

Díky této otázce byl také zjištěn poměr domů s nainstalovaných a nenainstalovaným kamerových systémem. Tedy jak moc lidé využívají možnost instalovat si na dům kamerové systémy.

Po rozdělení respondentů první otázkou zde odpovídalo 65 lidí z nichž 60 % (39 lidí) nemá na domě nainstalovaný kamerový systém a 40 % (26 lidí) má nainstalováno.

Dále se pokračuje ve větví odpovědí Ano.

Odpověď: Ano, byl nainstalován odbornou firmou



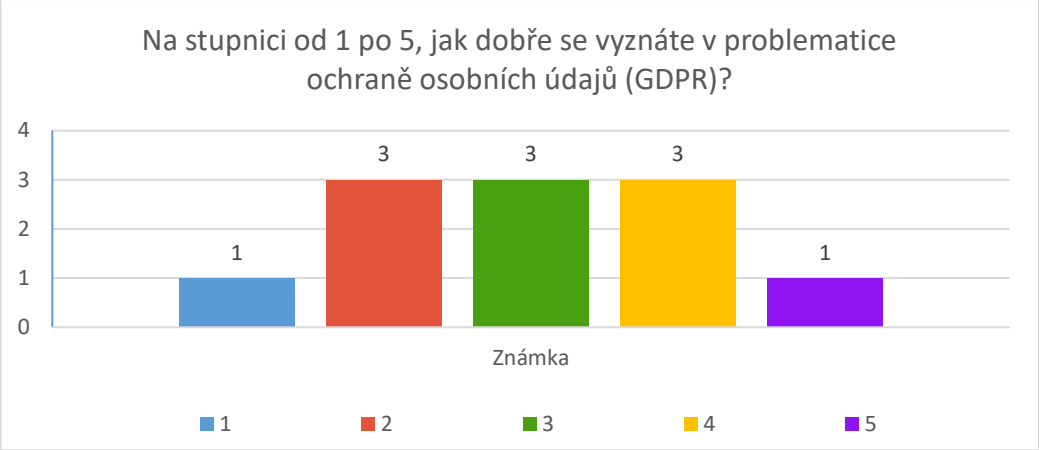
Graf 3 - Graf odpovědí na třetí otázku (Zdroj: Vlastní)

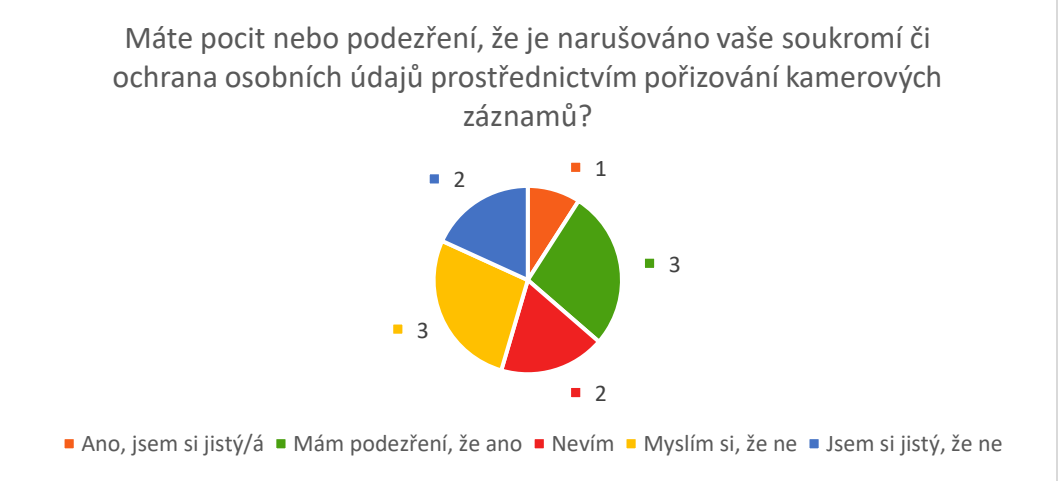
Pokud respondent odpověděl na přechozí otázku ano, tedy že má na rodinném domě nainstalovaný kamerový systém, dostal se k otázce, zda byl jeho kamerový systém

nainstalován odbornou firmou. K této variantě dotazníku se dostalo 26 respondentů z nichž 15 odpovědělo, že si instalovalo kamerový systém samo a 9 lidí si nechalo instalovat kamerový systém odbornou firmou, kde se dá tedy předpokládat, že bylo dodrženo všech náležitostí spojených s dodržením ochrany osobních údajů.

Význam této otázky je především ten, aby bylo zjištěno, kolik nainstalovaných kamerových systémů je potencionálně špatných a porušují ochranu osobních údajů. Pro toto zjištění, je ovšem potřeba dalších otázek, aby byla zjištěna úroveň znalostí lidí, kteří instalovali daný kamerový systém. Tomu se bude věnovat následující otázka. Po této otázce už jen zbývá dvojice posledních.

Konečné otázky první větve





Graf 4 - Grafy odpovědí na konečné otázky č. 1 (Zdroj: Vlastní)

Tyto dva dotazy jsou vždy stejné a jsou umístěny vždy na konci každé větve dotazníku. První otázka má za úkol zjistit jaká je znalost ochrany osobních údajů daného respondenta a druhá otázka zase zjišťuje vztah lidí k ochraně osobních údajů a ke zjištění, zda mají pocit, že je jejích soukromí narušováno.

Na první otázku se odpovídalo podle stupnice. Čím nižší číslo, tím nižší znalosti ohledně ochrany osobních údajů.

Z 11 možných respondentů byl jeden se znalostmi na nízké úrovni (1 bod) a jeden na nejvyšší (5 bodů). Průměrně se tedy znalost pohybuje na známce 3, tedy průměrná znalost problematiky.

Další otázka zjišťovala, zda mají respondenti pocit nebo podezření, že je jejich soukromí narušováno prostřednictvím kamerových systémů. Odpovídalo se formou výběru jedné možnosti z pěti možných. Pouze jeden člověk si je jistý, že je jeho soukromí narušováno a dva mají jistotu, že není. Dá se tedy konstatovat, že se lidé spíše necítí ohrožení.

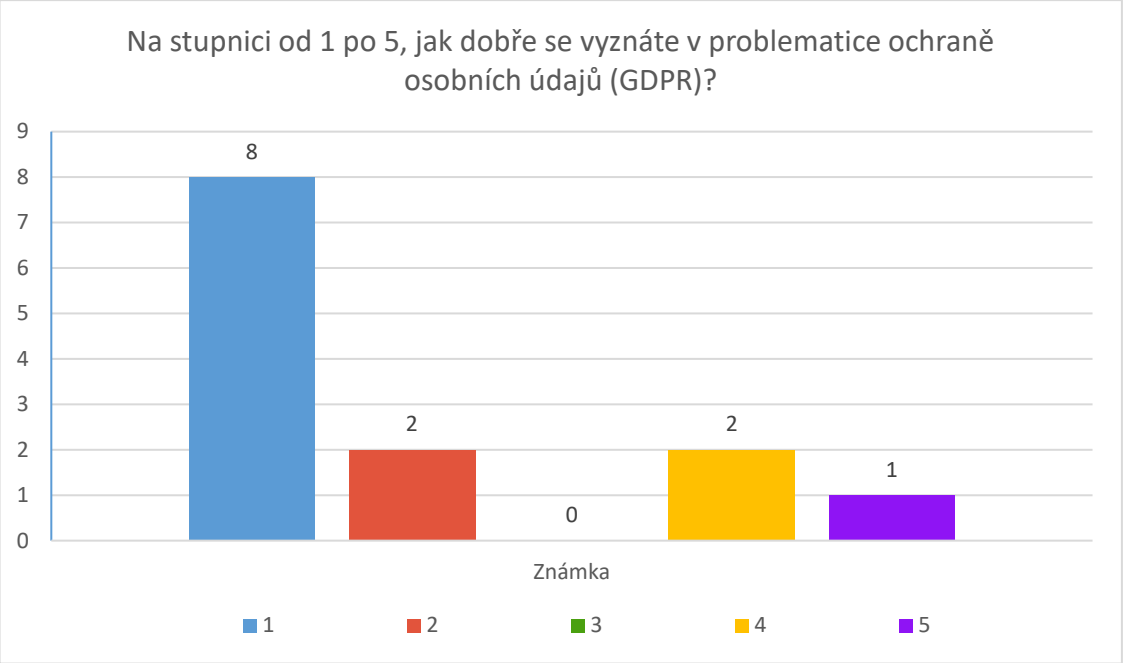
Pokud někdo v předchozí otázce, zda byl jeho kamerový systém instalován odbornou firmou, odpověděl, že ne a instaloval si kamerový systém sám, odpovídal na následující dvojicí otázek.

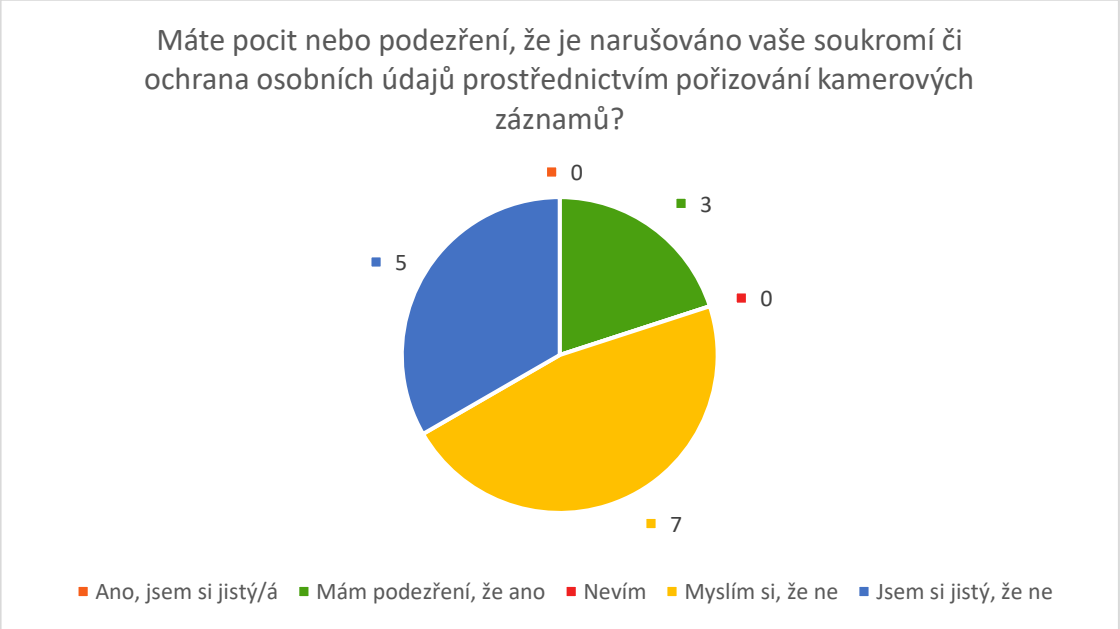
Odpověď: Ne, kamerový systém jsem instaloval/a sám/sama

Na tyto otázky odpovídalo 15 lidí, který si podle předchozí odpovědi instalovali kamerový systém sami. Průměrně se znalost problematiky pohybuje na přibližné hodnotě 2.3, tedy spíše podprůměrné znalosti. Ve spojitosti s přechozí otázkou se dá konstatovat, že existuje vetší pravděpodobnost špatného nainstalování kamerových systémů.

Lidé, kteří bydlí v rodinném domě a nainstalovali si na dům sami kamerový systém, odpovídali i na otázku týkající se pocitu porušování jejich soukromí. Z výsledku této otázky lze zjistit spíše negativnější postoj k možnému pocitu porušování ochrany osobních údajů těchto lidí.

Konečné otázky první větve





Graf 5 - Grafy odpovědí na konečné otázky č. 2 (Zdroj: Vlastní)

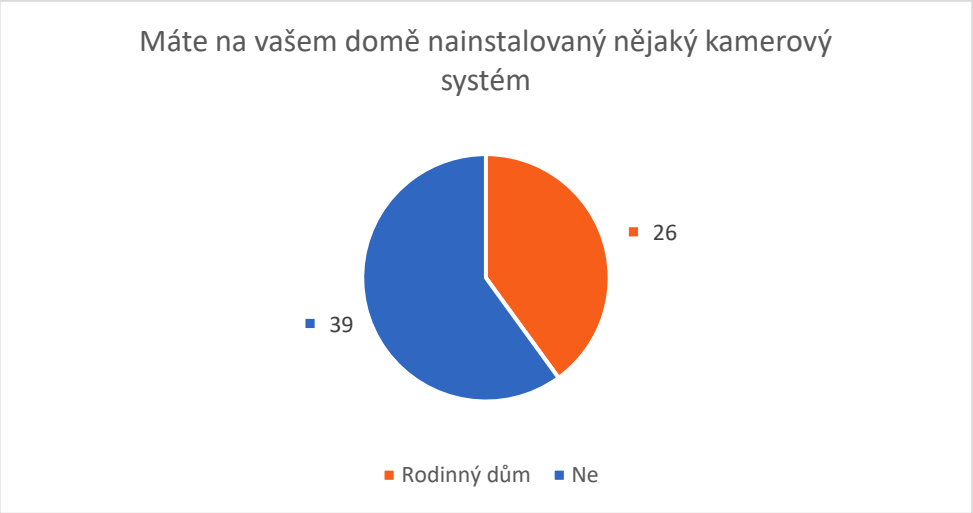
Druhá větev

Se stejnými dvěma, prvními otázkami následuje druhá větev dotazníku. Postup je stejný, jako v první větvi. Sto lidí odpovědělo na první otázku. Na otázku, zda mají na jejich domě instalován kamerový systém odpovídalo 65 lidí. Pozitivní odpověď byla rozebrána výše v první větvi. Nyní následuje rozbor odpovědí lidí, kteří odpovídali na tuto otázku negativně, tedy, že nemají na domě kamerový systém.

Otázka:

- V jakém typu domu bydlíte?
- Máte na vašem domě nainstalován nějaký kamerový systém?
- Přemýšlíte, že byste si nechal/a v budoucnu instalovat na dům kamerový systém?
- Konečné otázky.

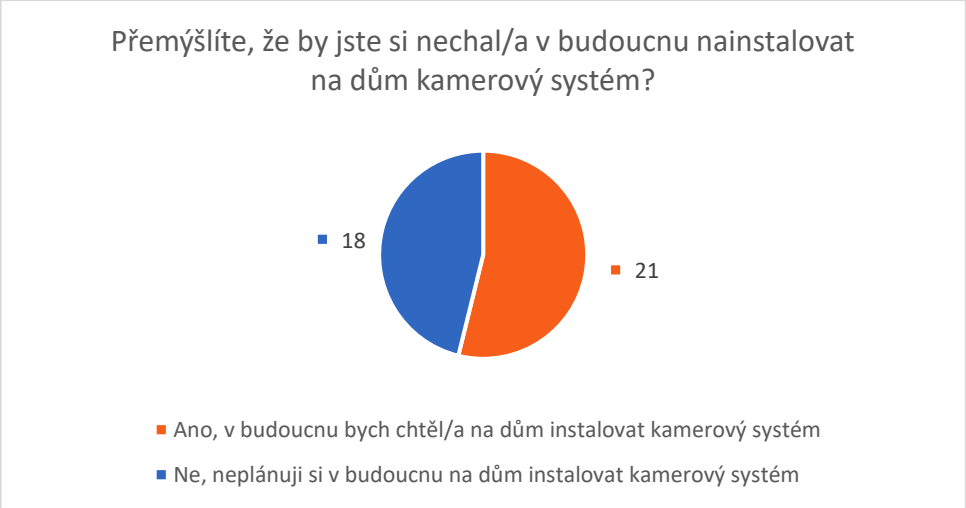
Odpověď: Ne



Graf 6 - Graf odpovědí na první otázku (Zdroj: Vlastní)

Jak již bylo zmíněno v přechozím odvětví dotazníku odpověď ano dalo 40 % (26 lidí). Nyní budou rozebrány odpovědi 39 lidí co nemá nainstalováno na domě kamerový systém.

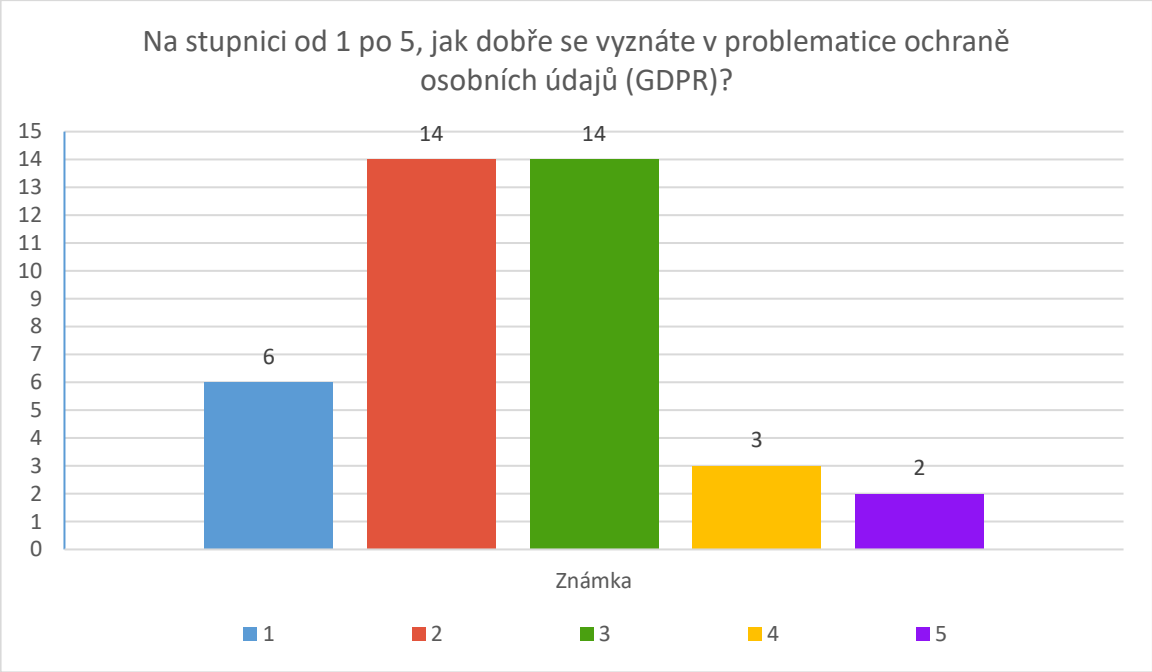
Odpověď: Ne



Graf 7 - Graf odpovědí na druhou otázku (Zdroj: Vlastní)

Respondenti, kteří nemají na domě instalován kamerový systém byli dále tázáni, zda by si nechali v budoucnosti na dům nainstalovat kamerový systém. 18 lidí by si nenechalo na dům instalovat kamerový systém a 21 naopak nechali. Ke zjištění, zda k tomu mají dostatečné znalost sloužila následující otázka.

Konečné otázky druhé větve



Graf 8 – Grafy odpovědi na konečné otázky č. 3 (Zdroj: Vlastní)

39 lidí odpovídalo na konečné otázky a v první části byla zjištěna průměrná hodnota znalosti kolem čísla 2.5, tedy průměrné znalosti. Což je poměrně dobrý základ pro lidi, co si chtějí v budoucnosti instalovat kamerový systém na dům.

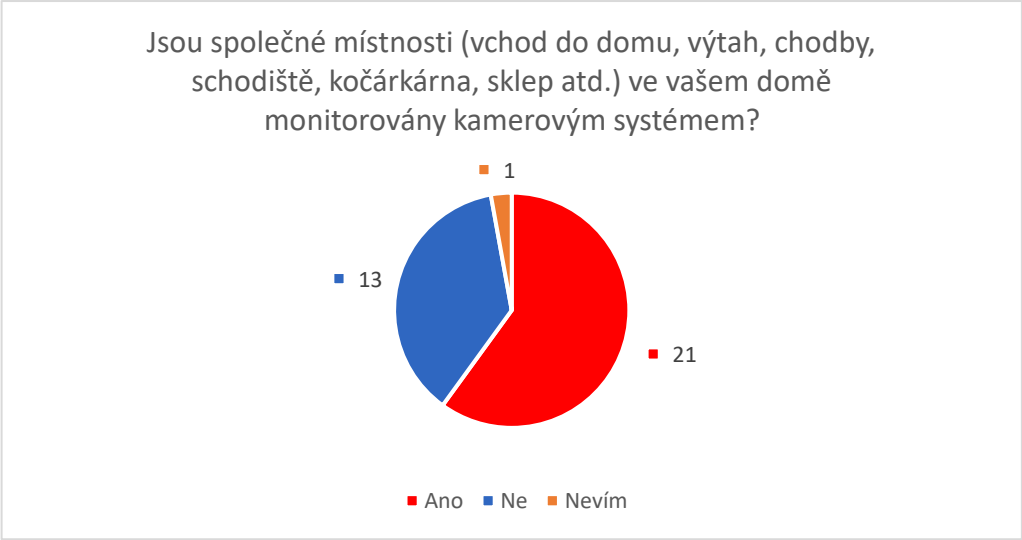
Druhá část, věnující se pocitu narušování soukromí vyšla na střední míře podezření.

Třetí větev

Otázka:

- V jakém typu domu bydlíte?
- Jsou společné místnosti (vchod do domu, výtah, chodby, schodiště, kočárkárna, sklep atd.) ve vašem domě monitorovány kamerovým systémem?
- Je poblíž vstupů do těchto monitorovaných místností na viditelném místě umístěna informační tabule, která informuje o skutečnosti, že je prostor monitorován?
- Máte pocit, že monitorování daných společných prostorů nějak narušuje vaše soukromí, či je nějak porušuje vaše právo na ochranu osobních údajů?
- Konečné otázky.

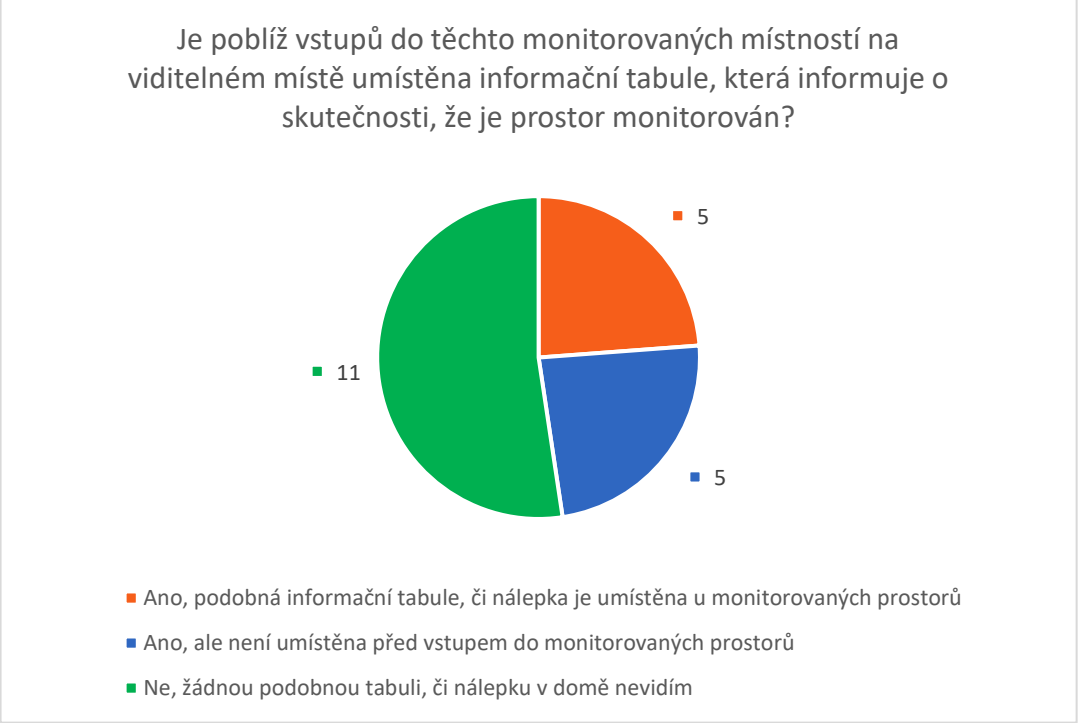
Odpověď: Ano



Graf 9 - Graf odpovědí na druhou otázku (Zdroj: Vlastní)

Po oddělení respondentů bydlících v bytovém domě, byly následně tázání na dotaz, týkající se přítomnosti kamerových systémů v jejich domě. Z 35 lidí 21 lidí uvedlo, že v jejich domě jsou přítomny kamery. 13 lidí v bytovém domě kamerový systém nezaznamenalo a zbylí jeden člověk si není jistý.

Odpověď: Ano, podobná informační tabule, či nálepka je umístěna u monitorovaných prostorů.



Graf 10 - Graf odpovědí na třetí otázku (Zdroj: Vlastní)

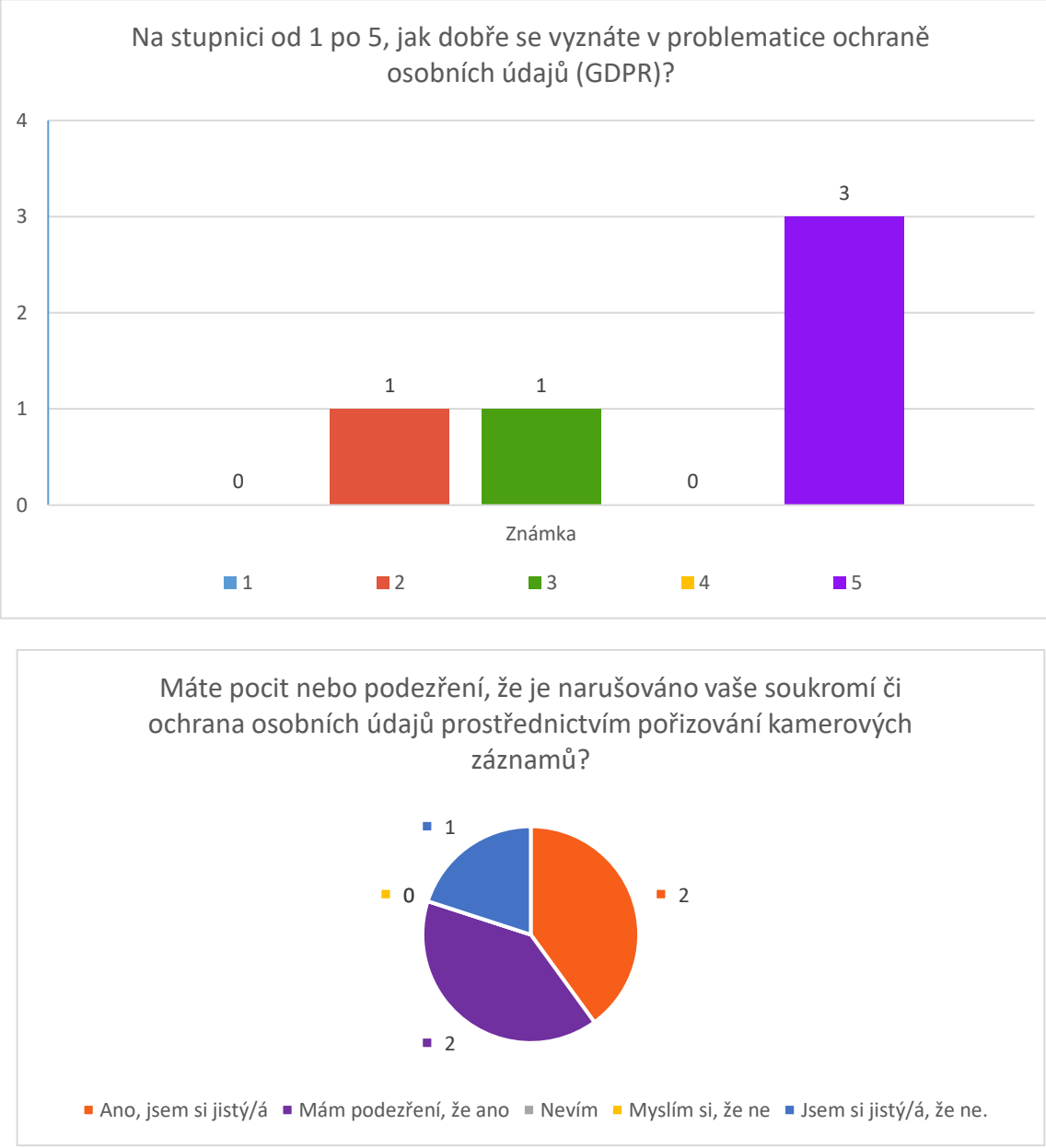
Tato otázka sloužila pro zjištění, zda majitel bytového domu splnil informační povinnost a na viditelném místě vystavil ceduli informující přicházející osoby na přítomnost kamerových systémů.

5 lidí odpovědělo, že daná tabule je umístěna je umístěna u monitorovaných prostorů, což je správná varianta. Dalších 5 lidí uvedlo, že tabule je umístěna v bytovém domě, ale není správně umístěna. Nejčastější chybou je, že tuto ceduli správci umísťují již v prostoru, který je monitorován a člověk se tak o jeho existenci dozví pozdě. Poslední variantou odpovědi je, že žádná informační tabule není poblíž monitorovaných prostorů umístěna. Bohužel, tato odpověď má největší počet odpovědí, tedy 11. Zde lze tedy konstatovat, že vetší část správců kamerových systémů v bytových domech nesplňují informační povinnost.

Konečné otázky třetí větve

V návaznosti na přechozí otázku byla vytvořena otázka zjištující, zda lidé mají pocit, že je v jejich domě kamerový systém porušující ochranu osobních údajů. Na tuto otázku odpovídalo 5 lidí, kteří v přechozí otázce odpověděli, že je poblíž monitorovaných prostorů

správně vystavena informační tabule. I přes správné splnění všech povinností správce mají tito lidé spíše pocit, že je jejich soukromí narušováno.



Graf 11 - Grafy odpovědí na konečné otázky č. 4 (Zdroj: Vlastní)

Opět na konec následovaly koncové otázky zjišťující úroveň znalostí problematiky GDPR a úroveň podezření na poručování ochrany osobních údajů. Výsledný průměr je na vysoké úrovni, což může znamenat, že může doopravdy docházet k narušování soukromí v bytových domech. O tom vypovídá i další část konečných otázek, kdy respondenti odpovídali, že mají spíše pocit, že je jejich soukromí narušováno, a to nejen v jejich domech, ale i kdekoliv jinde.

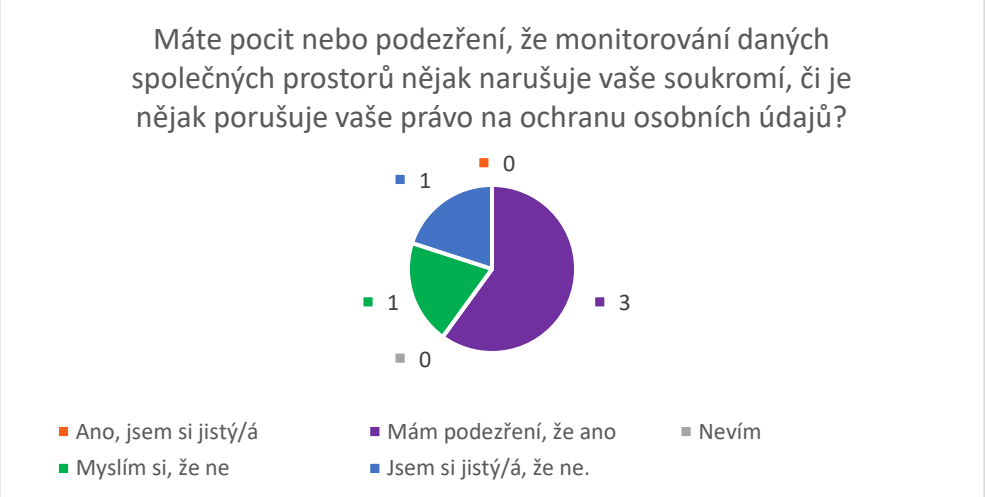
Čtvrtá větev

Jak bylo zmíněno výše, následující větve mají společná základ, takže dále bude rozebíraná rovnou otázka týkající se pocitu, zda monitorování společných prostorů v bytovém domě narušuje jejich soukromí. Předpokládá se tedy, že na předchozí otázky bolo zodpovězeno, že žijí v bytovém domě, jejich společné prostory jsou monitorovány a informační tabule je umístěna na jiném místě, než by správně měla být.

Otázka:

- V jakém typu domu bydlíte?
- Jsou společné místnosti (vchod do domu, výtah, chodby, schodiště, kočárkárna, sklep atd.) ve vašem domě monitorovány kamerovým systémem?
- Je poblíž vstupů do těchto monitorovaných místností na viditelném místě umístěna informační tabule, která informuje o skutečnosti, že je prostor monitorován?
- Máte pocit, že monitorování daných společných prostorů nějak narušuje vaše soukromí, či je nějak porušuje vaše právo na ochranu osobních údajů?
- Konečné otázky.

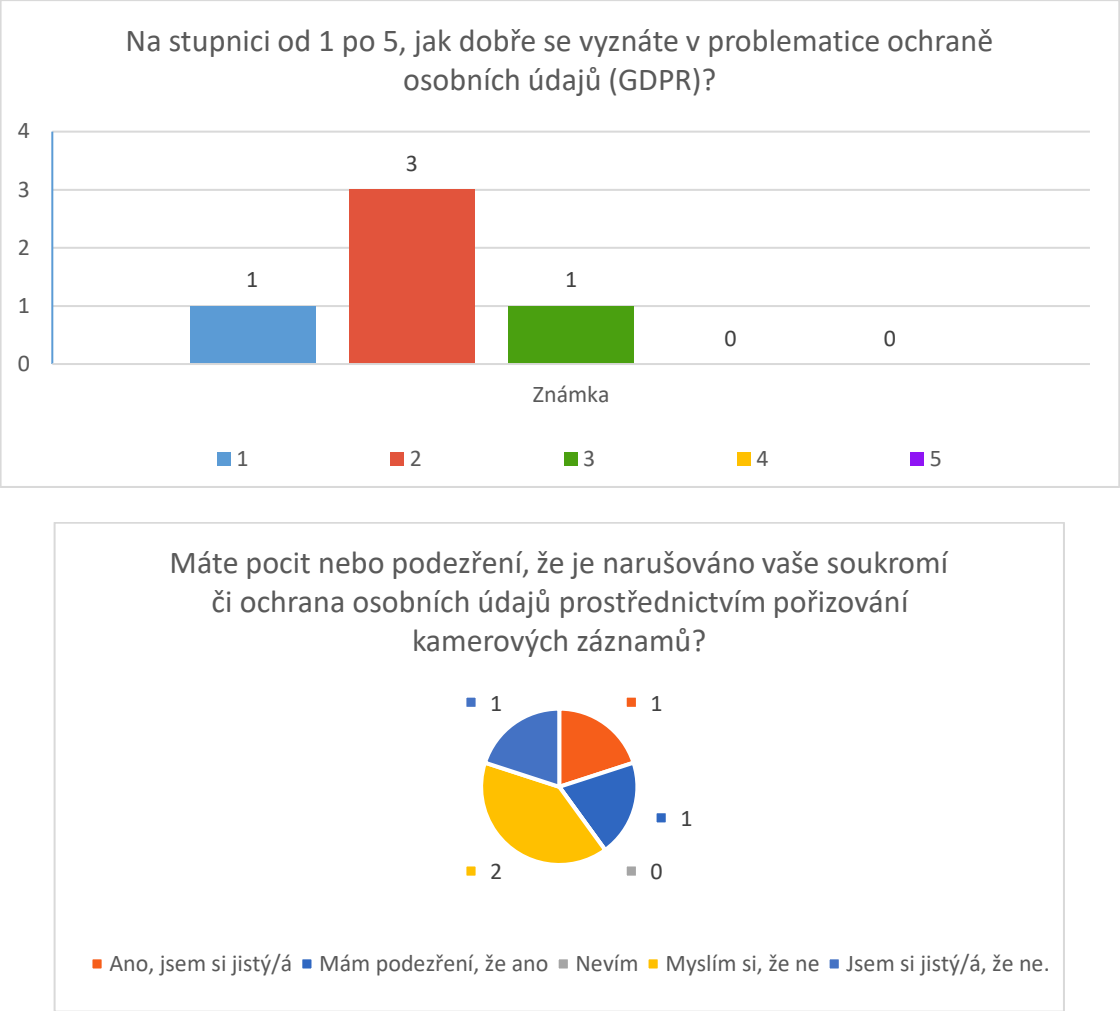
Odpověď: Ano, ale není umístěna před vstupem do monitorovaných prostorů.



Graf 12 - Graf odpovědí na čtvrtou otázku (Zdroj: Vlastní)

Na tuto odpověď došlo 5 lidí a celkově se dá konstatovat, že vztah těchto lidí k pocitu narušovaní soukromí je spíše neutrální.

Konečné otázky čtvrté větve



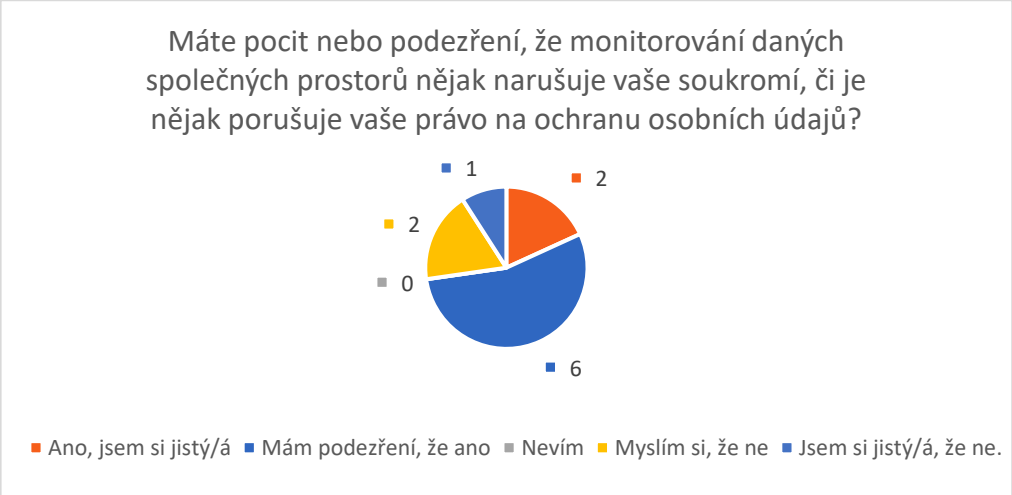
Graf 13 - Grafy odpovědí na konečné otázky č. 5 (Zdroj: Vlastní)

Opět následovala dvojice konečných otázek, z nichž první část týkající se znalostí GDPR vyšla spíš podprůměrně a druhá část týkající se pocitu porušování soukromí vyšla spíše negativně, takže tito lidé mají poct, že je jejich soukromí v bezpečí.

Pátá větev

Stejně jako přechozí větev i zde se rovnou pokračuje od otázky, zda je poblíž vstupů do monitorovaných prostorů umístěna informační tabule, na kterou tentokrát respondenti odpovídali, že žádnou tabuli v okolí nevidí, i když je na jejich bytovém domě umístěn kamerový systém. Tuto odpověď označilo 11 lidí.

Odpověď: Ne, žádnou podobnou tabuli, či nálepku v domě nevidím.

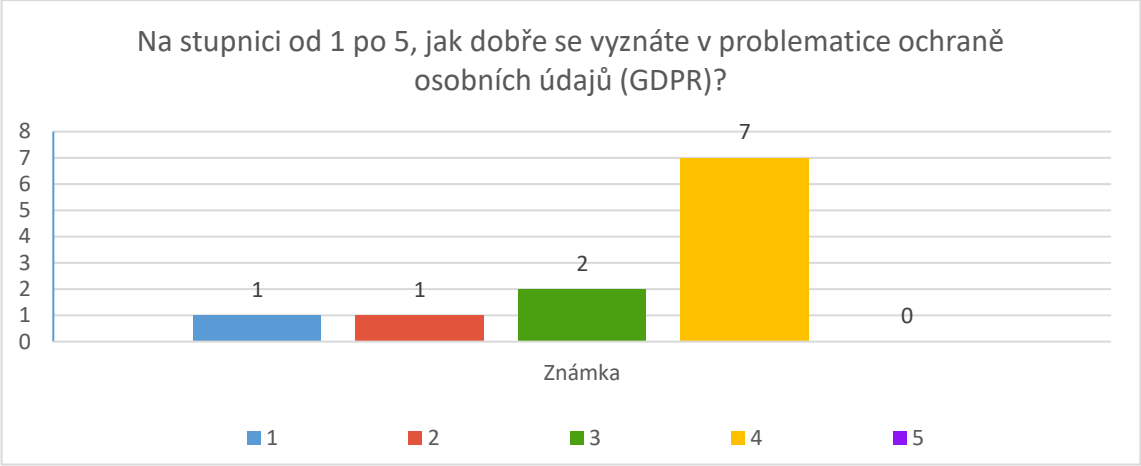


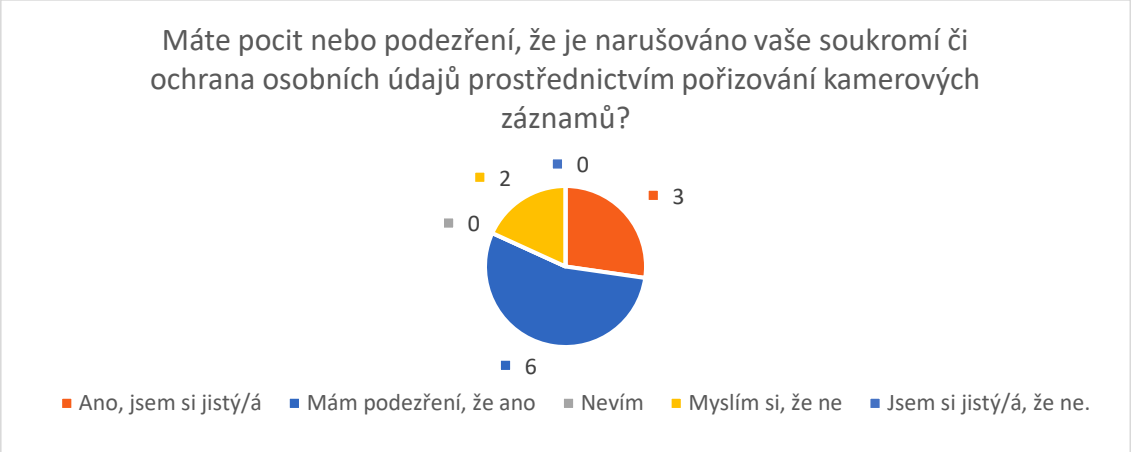
Graf 14 - Graf odpovědí na čtvrtou otázku (Zdroj: Vlastní)

Těchto 11 lidí dále pokračovalo na otázku, zda mají pocit, že je jejich soukromí narušováno.

A podle očekávání, většina respondentů potvrdlo, že mají opravdu pocit narušování jejich soukromí prostřednictvím kamer.

Konečné otázky páté větve





Graf 15 - Grafy odpovědí na konečné otázky č. 6 (Zdroj: Vlastní)

Dále 11 respondentů pokračovalo na konečné otázky, kde bylo zjištěno, že mají poměrně dobrou znalost GDPR a opět se potvrdilo, že je jejich soukromí opravdu narušováno a dochází tak pravděpodobně k porušování ochrany osobních údajů, a to nejen v jejich domě.

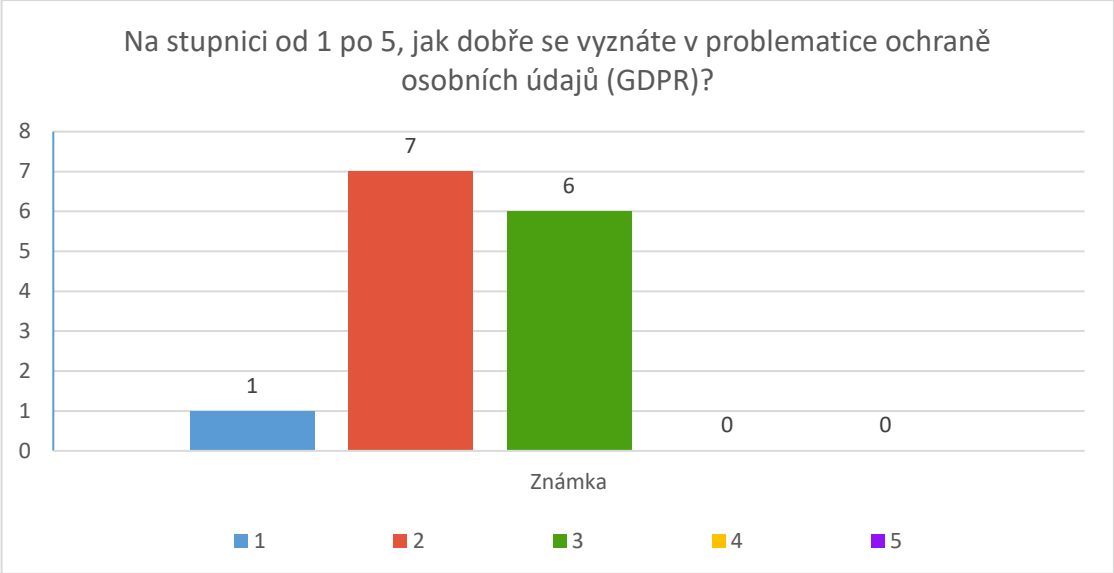
Šestá větev

Poslední šestá větev má s ostatními opět společných pár otázek, a to přesněji první dvě z nichž na první odpověděli že žijí v bytovém domě a buď v jejich domě není kamerový systém, nebo o něm neví. Odtud pokračovali přímo na končené otázky.

Otázka:

- V jakém typu domu bydlíte?
- Jsou společné místnosti (vchod do domu, výtah, chodby, schodiště, kočárkárna, sklep atd.) ve vašem domě monitorovány kamerovým systémem?
- Konečné otázky.

Odpověď: Ne, nebo nevím



Graf 16- Grafy odpovědí na konečné otázky č. 7 (Zdroj: Vlastní)

Znalost problematiky ochrany osobních údajů u těchto lidí byla spíše podprůměrná. Druhá část otázky vypověděla, že těchto 14 lidí má pocit, že je jejich soukromí narušováno.

Získané odpovědi na výzkumné otázky

Jak dochází k porušení ochrany osobních údajů a soukromí kontextu audiovizuálních záznamů?

- Díky dotazníku bylo zjištěno, že jednou z možných variant, jak dochází k porušování ochrany osobních údajů je, že nejsou správně nebo vůbec vystaveny informační

cedule v bytových domech, informujících o přítomnosti kamerového systému se záznamem.

Proč dochází k porušení ochrany osobních údajů a soukromí v kontextu audiovizuálních záznamů?

- K porušení s největší pravděpodobností dochází kvůli nízké znalosti problematiky GDPR a ochrany soukromí.

Kdo porušuje ochranu osobních údajů a soukromí v kontextu audiovizuálních záznamů?

- Vždy se jedná o majitele domu, či správce. Většinou se jedná o lidi s nižší znalostí problematiky ochrany osobních údajů.

Kdo může být obětí porušení ochrany osobních údajů?

- Z hlediska rodinných domů to nejčastěji bývají obyvatelé sousedních domů, či kolemjdoucí a z hlediska bytových domů jsou většinou obětí právě obyvatelé daného domu.

Jaký je vztah obyvatelstva k problematice ochrany osobních údajů?

- Je evidentní, že lidé, co se více zajímají o problematiku ochrany osobních údajů mají větší povědomí o tomto možném riziku a snaží se získat více informací. Ale lidé s nižší znalostí ochrany osobních údajů, nemají k tomuto tématu příliš dobrý vztah.

Jaké jsou znalosti obyvatelstva v oblasti ochrany osobních údajů?

- Z dotazníku vychází, že znalost a tím pádem zájem o problematiky ochrany osobních údajů je poměrně na malé úrovni.

Ověření hypotéz

1. K porušení ochrany osobních údajů dochází při špatné instalaci kamerového systému.

Z dotazníku byla tato hypotéza potvrzena. Kromě toho byla zjištěna i příčina, a to špatná informovanost obyvatelstva o přítomnosti kamerového systému.

2. K porušení ochrany osobních údajů dochází především v bytových domech.

Podle výsledků byla tato hypotéza potvrzena, jelikož se vyskytl poměrně vysoký počet lidí, co není vůbec seznámeno s tím, že se v jejich přítomnosti monitorují společné prostory.

3. Lidé s nižší znalostí problematiky ochrany osobních údajů, jsou více optimističtí vůči možnému narušení jejich soukromí.

I tato hypotéza byla potvrzena. Čím nižší byla znalost problematiky GDPR, tím více se následně objevovaly odpovědi vypovídající o pocitu bezpečí, z hlediska možného porušení ochrany osobních údajů.

4. Na mnoha domech jsou instalovány kamerové systémy lidmi s nízkou znalostí problematiky ochrany osobních údajů.

Z hlediska dotazníku, bylo zaznamenáno několik případů, kdy bylo nainstalováno několik kamerových systémů na dům lidmi s nízkou znalostí dané problematiky, ale naštěstí je většina kamer instalovaných na domě, umístěna odbornou firmou.

10 NÁVRHY PRO LEPŠÍ ORIENTACI V PROBLEMATICE OCHRANY OSOBNÍCH ÚDAJŮ Z HLEDISKA INSTALACE KAMEROVÝCH SYSTÉMŮ

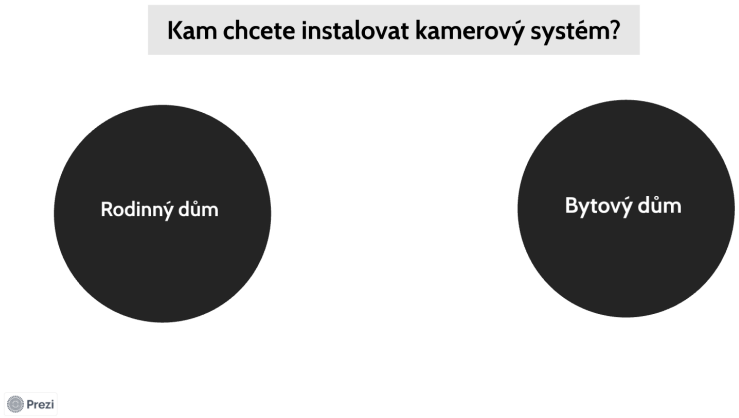
Na základě dat a informací získaných z dotazníkového šetření vyplývá, že porušení ochrany osobních údajů a soukromí prostřednictvím kamerových systémů je způsobeno především nízkou znalostí daných právních norem a celkově minimálním povědomím o dané problematice, a to jak u majitelů kamerových systémů, tak i ostatních lidí, kteří si ani neuvědomují možný zásah do jejich bezpečí osobních údajů a soukromí z hlediska kamerových systémů.

K možnému zlepšení této situace by mohlo dojít vytvořením interaktivní prezentace[1], která by majitelům kamerových systémů radila, jak mají jejich zařízení umístit a nastavit, aby byl provoz těchto kamer naprosto správný a z právního hlediska nepostihnutelný.

10.1 Interaktivní prezentace

K prvotnímu seznámení obyvatelstva s právními aspekty provozování kamerových systémů by mohla dobře sloužit interaktivní prezentace. Tato prezentace by měla uživatele postupně provést možnými variantami umístění kamerových systémů, a hlavně seznámit s právními aspekty pro správné provozování těchto kamerových systémů. Stěžejní částí prezentace by byla praktická ukázka možného umístění kamerových systémů s komentářem a rady, jak správně tato zařízení nastavit. Primárním výsledkem shlédnutí této prezentace by měl být především zisk uživatele základních informací o správném umístění kamerových systémů a doporučení možného umístění kamer. Sekundárním výsledkem by bylo zejména také získaní základní orientace v problematice ochrany osobních údajů a soukromí. Obsah celé prezentace je součástí přílohy P I: Náhled interaktivní prezentace.

[1] Odkaz na prezentaci: https://prezi.com/view/4SVGi4UXHappyvxdacAg/



Obrázek 28 – Náhled interaktivní prezentace (Zdroj: Prezi, vytvořeno autorem)

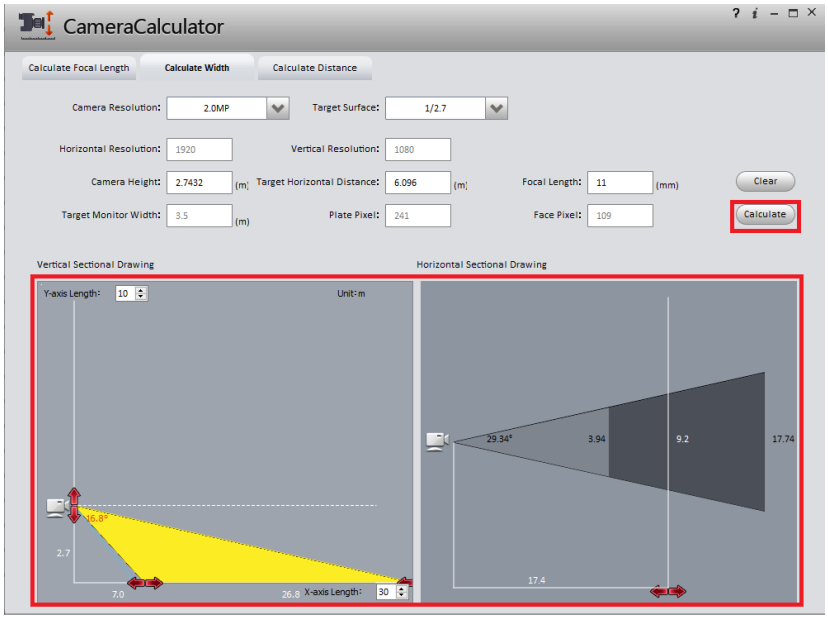
Obrázek výše již znázorňuje, jak by mohla vypadat první strana prezentace. Jako první by si uživatel vybral, na jaký typ domu chce kamerový systém instalovat. Dle jeho volby by byl dále přesměrován na názorné video, kde mu bude již prezentováno a prakticky znázorněno, kam lze umístit kamery a na co si dát pozor.

Takováto prezentace by se mohla stát účinným nástrojem a pomocníkem pro všechny majitele kamerových systému, v případě, že by potřebovali získat znalosti v dané problematice a zvýšit své povědomí o ochraně osobních údajů a soukromí. Výše zmíněný návrh prezentace je pouze koncept, který názorně zobrazuje možnost, jakou by mohla být orientace v problematice ochrany osobních údajů zlepšena.

10.2 Využití softwarových programů při výběru kamer

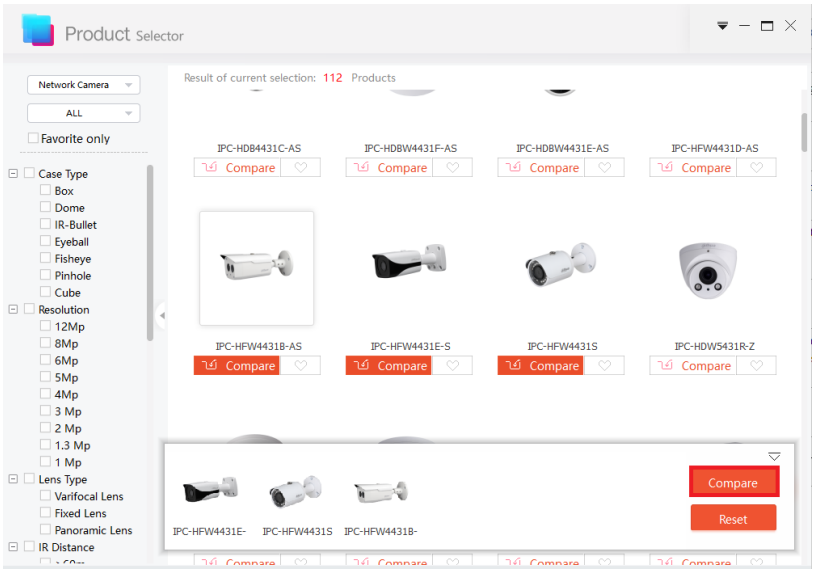
Další možností, jak lze pomoct potencionálním majitelům kamerových systémů je nabídka možného využití různých softwarů, které dokáží uživatele provést celým procesem instalace kamer, a to už od samotného začátku, kdy je důležité správně vybrat typ kamery. Jedno z možných softwarových vybavení nabízí například firma Dahua. Tato firma nabízí několik základních i pokročilých programů, které pomáhají zákazníkovi již od samotného výběru kamery až po finální nastavení kamer.

Jako první uživatel může sáhnout po programu Camera Calculator. Tento program pomáhá vybrat správné místo na instalaci kamer.



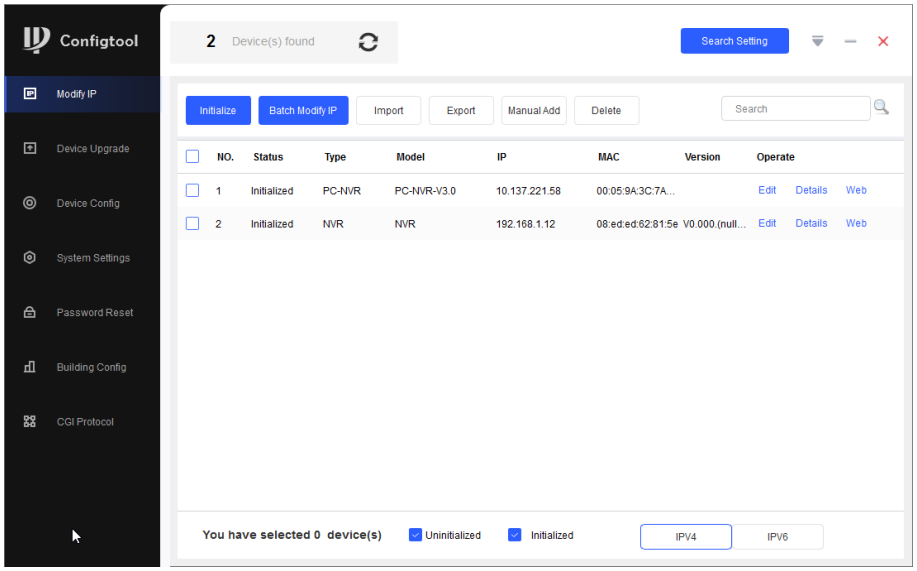
Obrázek 29 – Software Camera Calculator (Zdroj: Camera Calculator, 2021)

Když je známo, jak správně a na jaké místo lze umístit kameru, je možné využít další program, a to Product Selector, který na základě výše získaných informací z programu Camera Calculator dokáže vybrat vhodný typy kamer, které lze na určitá místa instalovat.



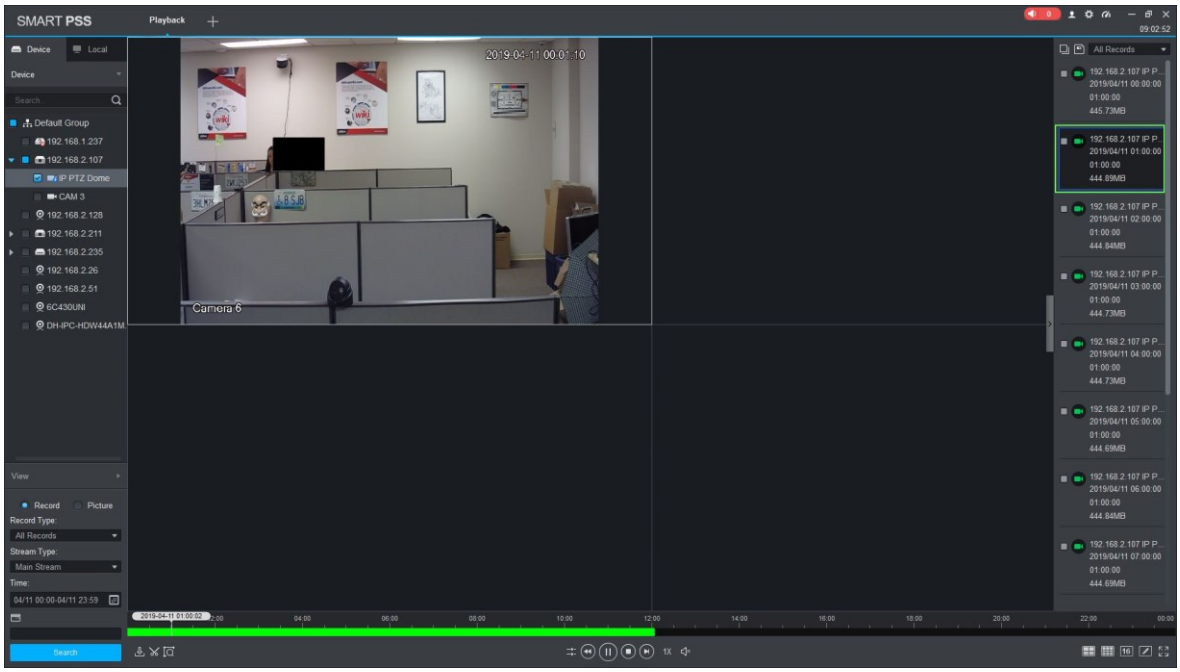
Obrázek 30 – Software Product Selector (Zdroj: Product Selector, 2021)

Jeden z dalších programů, jaký lze využít při nastavování kamer je ConfigTool, který přehledně provádí uživatele při prvotním nastavení kamery. Díky tomuto programu dojde k bezpečnému a lehkému nastavení daných kamerových systémů.



Obrázek 31 – Software Confing Tool (Zdroj: Confing Tool, 2021)

Ve finální fázi uživatel potřebuje již poslední program a to takový, který umožňuje obsluhovat kamery a sledovat monitorovaný prostor. Smart PSS je možným softwarem pro obsluhu kamer a práci s uloženými záznamy.



Obrázek 32 – Software Smart PSS (Zdroj: Smart PSS, 2021)

Existuje mnoho programů a programových balíčků, který nabízejí většinou samotní výrobci kamerových systémů. Tyto programy jsou ve většině případě zdarma a jejich použití je pouze na uživatelích. Díky těmto softwarům je majitel kamerových systémů postupně proveden od úplného začátku, kdy vybírá vhodnou kameru až po finální nastavení kamer.

ZÁVĚR

V současnosti je rozsah zpracovávaných informací o jedinci mnohonásobně rozsáhlejší, než jak bylo vůbec možné si představit ještě před několika desítkami let. Zároveň je i snadnější díky dostupnějším technologiím. Součástí našeho každodenního života se staly kamerové systémy, automatizované prostředky umožňující v několika sekundách provádět různé druhy zpracovatelských operací, které by dříve zabraly dny či by vůbec nebyly reálné možné. Samozřejmostí je internet umožňující jedním kliknutím zaslat osobní údaje na druhý konec světa nebo je zpřístupnit. Všechny tyto moderní prostředky však představují i velké riziko pro osobní údaje a soukromí člověka.

Jak bylo několikrát zmíněno v diplomové práci, hlavním nedostatkem v dané problematice je nízká úroveň znalostí obyvatelstva ochrany osobních údajů a s ní souvisejících právních norem. Pro odstranění tohoto nedostatku by bylo třeba vytvořit dostatečné množství různých edukačních prostředků, které by dokázaly předávat potřebné informace danému obyvatelstvu a zvýšit tak povědomí o této problematice.

V teoretické části práce definuje základní pojmy a právní dokumenty týkající se problematiky ochrany osobních údajů, což je pro seznámení a pochopení daného tématu potřebné. Dále byla ochrana osobních údajů vložena do kontextu audiovizuálních záznamů a bylo vysvětleno jaká je její funkce ve spojitosti s kamerovými systémy.

V praktické části práce jako první vysvětluje, jaké jsou zásady při instalaci kamerových systémů a co je potřeba dodržet, aby byl provoz těchto kamerových systémů bezchybný a v souladu s danými právními dokumenty. Hlavní částí práce je implementace těchto zásad a pravidel do praktického modelu domů. Zde bylo využito potřebných programů pro vytvoření modelů, na kterých bylo názorně ukázáno možné umístění kamerových systémů. Při tvorbě modelů bylo vycházeno z reálných budov, takže toto zjednodušené zobrazení reality by mělo být věrohodné a zároveň podle zásad modelů, dostatečné z hlediska potřebných informací pro praktické zobrazení daných zásad instalace kamer. Další částí práce byla analýza vztahu obyvatelstva k problematice ochrany osobních údajů. K tomu bylo využito dotazníkového šetření, jehož struktura byla vytvořena speciálně pro separaci jednotlivých respondentů podle jejich odpovědí. Tím bylo získáno mnoho reálných informací, které odpověděli na předem stanovené výzkumné otázky a hypotézy. Na závěr bylo v práci navrhnuto opatření pro zlepšení orientace obyvatelstva v této

problematice a vytvořena interaktivní prezentace, která pomáhá uživateli vybrat nejlepší umístění pro jeho kamerový systém.

Cílem práce bylo objektivně shrnout a prakticky znázornit náležitosti týkající se problematiky osobních údajů a kamerových systémů. Cíl práce byl splněn.

SEZNAM POUŽITÉ LITERATURY

Elektronické zdroje

Automatické rozpoznávání obličeje, 2020. *Cncenter.cz* [online]. Praha, [cit. 2021-6-18]. Dostupné z: https://img.cncenter.cz/img/11/full/6169429_smirovaci-technologie-v0.jpg?v=0

Camera Calculator [online]. Chang-čou, 2021 [cit. 2021-7-16]. Dostupné z: https://dahuawiki.com/File:Camercalc5.png

Config Tool [online]. Chang-čou, 2021 [cit. 2021-7-16]. Dostupné z: https://dahuawiki.com/images/8/89/Config4.05.png

ČESKO, 1992. Usnesení předsednictva České národní rady ze dne 16. prosince 1992 o vyhlášení listiny základních práv a svobod jako součásti ústavního pořádku České republiky. Dostupné také z: https://www.zakonyprolidi.cz/cs/1993-2

ČESKO, 2012. Zákon č. 89/2012 Sb. Občanský zákoník. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2012-89

Drony – hrozba pro okolí, 2021. *Česká justice* [online]. Praha, [cit. 2021-6-18]. Dostupné z: https://www.ceska-justice.cz/2016/01/uoou-budme-bdeli-drony-mohou-byt-hrozbou-pro-soukromi-majetek-i-informace/

Epravo, 2018. *Trestněprávní směrnice*. [online]. Praha [cit. 2021-02-28]. Dostupné z: https://www.epravo.cz/top/clanky/trestnepravni-smernice-jako-doplneni-obecneho-narizeni-na-ochranu-osobnich-udaju-108013.html

Facial Recognition, 2020. *The Guardian* [online]. London [cit. 2021-04-08]. Dostupné z: https://www.theguardian.com/technology/2019/aug/16/privacy-campaigners-uk-facial-recognition-epidemic

GDPR, 2019. *Citlivé osobní údaje*, [online]. Praha [cit. 2019-05-04]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/citlive-osobni-udaje/

Hlídání areálu kamerovým systémem, 2017. *Podnikatel.cz* [online]. Praha, [cit. 2021-6-18]. Dostupné z: https://www.podnikatel.cz/clanky/hlidate-areal-sve-firmy-a-pracoviste-kamerami-pak-vas-cekaji-nove-povinnosti/?utm_source=newsletter-html-d&utm_medium=text&utm_campaign=2017-08-11

Informační tabule, 2021. *CCB.cz* [online]. Praha. [cit. 2021-7-13]. Dostupné z: https://www.ccb.cz/images_aqua/2018/kveten/Infotabulka_1821x.jpg

Kamerové systémy, 2017. *GDPR.cz* [online]. Praha. [cit. 2021-7-15]. Dostupné z: https://www.gdpr.cz/blog/kamerove-systemy-v-soucinnosti-s-gdpr/

Ministerstvo vnitra. *Bezpečnost,* 2019. [online]. Praha [cit. 2021-03-02]. Dostupné z: https://www.mvcr.cz/clanek/pojmy-bezpecnost.aspx

MINISTERSTVO ZAHRANIČNÍCH VĚCÍ. Sdělení č. 209 ze dne 18. března 1992 federálního ministerstva zahraničních věcí o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících Dostupné také z: https://www.zakonyprolidi.cz/cs/1992-209

Nařízení Evropského parlamentu a rady (EU) 2016/679, 2016. *O ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES.* Dostupné z: https://www.mpo.cz/assets/cz/podnikani/ochrana-osobnich-udaju-gdpr/gdpr-dokumenty/2017/11/Narizeni-EU-2016679_GDPR.pdf

Nový zákon o zpracování osobních údajů, 2019. Epravo [online]. Praha, 2019 [cit. 2021-02-27]. Dostupné z: https://www.epravo.cz/top/clanky/novy-zakon-o-zpracovani-osobnich-udaju-109312.html

Podmínky zachycení a šíření podoby člověka prostřednictvím fotografie, 2020. Právní prostor [online]. Praha [cit. 2021-02-27]. Dostupné z: https://www.pravniprostor.cz/clanky/obcanske-pravo/podminky-zachyceni-sireni-podoby-cloveka-prostrednictvim-fotografie

Pravidla létání s drony, 2021. *RCProfi* [online]. Praha, [cit. 2021-6-18]. Dostupné z: https://www.rcprofi.cz/poradna/pravidla-letani-s-drony-v-cr

Product Selector [online]. Chang-čou, 2021 [cit. 2021-7-16]. Dostupné z: https://dahuawiki.com/images/2/25/Product_Selector4.png

Smart PSS [online]. Chang-čou, 2021 [cit. 2021-7-16]. Dostupné z: https://dahuawiki.com/images/2/24/Playback_SmartPSS_-_6.jpg

Soukromé užívání kamer, 2019, *GDPR.cz* [online]. Praha. [cit. 2021-7-13]. Dostupné z: https://www.gdpr.cz/blog/fotky/

Srovnání nařízení GDPR a zákona o ochraně osobních údajů. *OOU.cz* [online]. Praha, 2021 [cit. 2021-7-16]. Dostupné z: http://www.oou.cz/gdpr/srovnaniGDPR

Stanovisko č. 1/2016, 2016. *Úřad pro ochranu osobních údajů* [online]. Praha. [cit. 2021-7-13]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=38408

TRIMBLE NAVIGATION. SketchUp, 2019. [software]. 2019 [cit. 2021-7-16]. Dostupné z: https://www.sketchup.com/

Tištěné zdroje

BARTÍK, Václav a Eva JANEČKOVÁ, 2012. Ochrana osobních údajů: z pohledu zvláštních právních úprav k 1.8.2012. Olomouc: ANAG. ISBN 978-80-7263-749-2.

BOJKOVIC, Zoran a Dragorad MILOVANOVIC, 2019. *The Biometric Computing*. Boca Raton: Chapman and Hall/CRC. ISBN 9781351013437.

CALDE, Alan, 2018. *EU GDPR a Pocket Guide*. 2. vydání. New York: Itgp. ISBN 9781787780644.

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR, 2015. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze. ISBN 978-80-7251-436-6.

LAVICKÝ, Petr, 2015. Občanský zákoník: komentář. Praha: C.H. Beck. Velké komentáře. ISBN 978-80-7400-529-9.

MATES, Pavel. *Ochrana osobnosti, soukromí a osobních údajů*. Praha: Leges, 2019. ISBN 978-80-7502-346-9.

NULÍČEK, Michal, 2017. *GDPR – obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer. Praktický komentář. ISBN 978-80-7552-765-3.

RAFAJOVÁ, Monika a Lucia VÁRYOVÁ, 2019. *Biometrické osobné údaje podľa GDPR: (biometrický podpis, kamerový systém)*. Praha: Leges. Teoretik. ISBN 978-80-7502-433-6.

SHARMA, Sanjay. 2020. *Data Privacy and GDPR Handbook*. Hoboken: Wiley. ISBN 978-1119594246.

SOLOVE, Daniel, 2020. *EU Data Protection and the GDPR*. New York: Aspen Publ. ISBN 9781543832631.

ŠOLC, Martin, 2015. *Ochrana osobních údajů.* Praha. Rigorózní práce. Univerzita Karlova v Praze, Právnická fakulta, Katedra správního práva a správní vědy.

ŠVESTKA, Jiří, Jan DVOŘÁK a Josef FIALA, 2014. Občanský zákoník: komentář. Praha: Wolters Kluwer ČR. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-370-8.

VOIGT, P. BUSSCHE, A, 2017. *The EU General Data Protection Regulation (GDPR). A practical Guide*. Cham, Švýcarsko: Springer. *ISBN 978-3-319-57959-7*

WRAY, 2017. Darren. *The little book of GDPR*. United States: Independently published, 2017. ISBN 978-1522021148.

ŽŮREK, Jiří, 2018. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG. ISBN 978-80-7554-152-9.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

§	Paragraf
č.	Číslo
čl.	Článek
EU	Evropská unie
GDPR	Obecné nařízení o ochraně osobních údajů (General Data Protection Regulation)
mj.	Mimo jiné
např.	Například
Resp.	Respektive
Sb. m. s.	Sbírka mezinárodních smluv
SVV	Rada pro spravedlnost a vnitřní věci
ÚOOÚ	Úřad pro ochranu osobních údajů

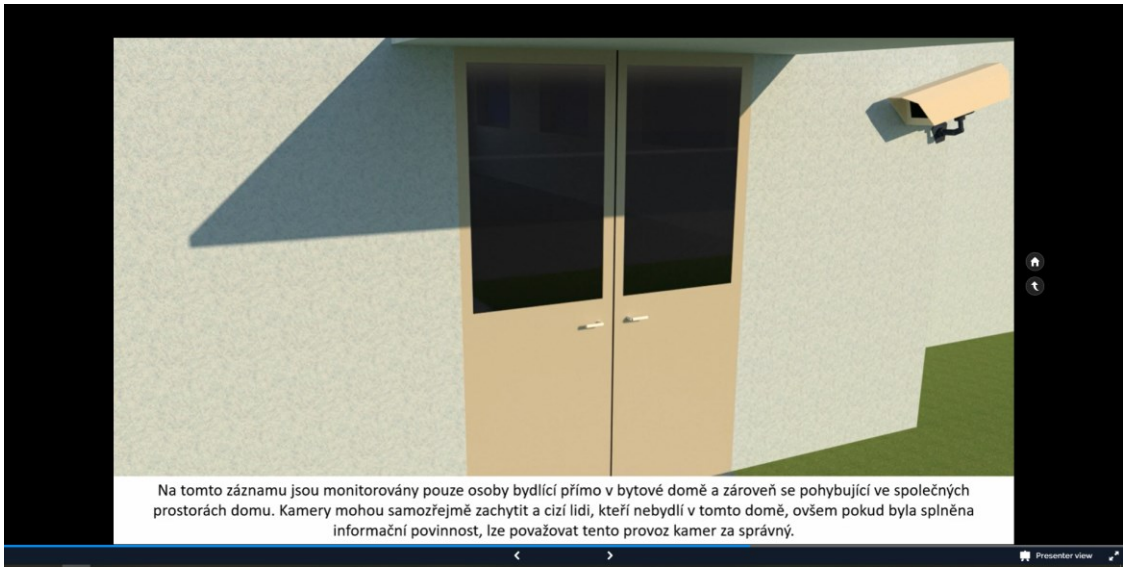
SEZNAM OBRÁZKŮ

SEZNAM PŘÍLOH

PŘÍLOHA P I: NÁHLED INTERAKTIVNÍ PREZENTACE

Při instlaci kamer k dohledu nad bytovým domem, je potřeba dbát na několi pravidel.

Prezi



(Zdroj: Prezi, vytvořeno autorem)

PŘÍLOHA P II: DOTAZNÍK

Seznam otázek a odpovědí:

- V jakém typu domu bydlíte?
    - Rodinný dům
    - Bytový dům
- Máte na vašem domě nainstalován nějaký kamerový systém?
    - Ano
    - Ne
- Byl váš kamerový systém instalován odbornou firmou?
    - Ano, byl instalován odbornou firmou
    - Ne, kamerový systém jsem instaloval/a sám/sama
- Přemýšlíte, že byste si nechal/a v budoucnu instalovat na dům kamerový systém?
    - Ano, v budoucnu bych chtěl/a na dům instalovat kamerový systém.
    - Ne, neplánuji si v budoucnu instalovat na dům kamerový systém.
- Jsou společné místnosti (vchod do domu, výtah, chodby, schodiště, kočárkárna, sklep atd.) ve vašem domě monitorovány kamerovým systémem?
    - Ano
    - Ne
    - Nevím
- Je poblíž vstupů do těchto monitorovaných místností na viditelném místě umístěna informační tabule, která informuje o skutečnosti, že je prostor monitorován?
    - Ano, podobná informační tabule, či nálepka je umístěna u monitorovaných prostorů.
    - Ano, ale není umístěna před vstupem do monitorovaných prostorů.
    - Ne, žádnou podobnou tabuli, či nálepku v domě nevidím.
- Máte pocit, že monitorování daných společných prostorů nějak narušuje vaše soukromí, či je nějak porušuje vaše právo na ochranu osobních údajů?

    - Ano, jsem si jistý/á
    - Mám podezření, že ano
    - Nevím
    - Myslím si, že ne
    - Jsem si jistý/á, že ne.

Každá větev dotazníků je zakončena dvojicí otázek **(konečné otázky):**

- Na stupnici od 1 po 5, jak dobře se vyznáte v problematice ochraně osobních údajů (GDPR)?
    - 1 - V problematice GDPR se vůbec nevyznám
    - 5 - Problematiku GDPR znám velice dobře a vyznám se v ní
- Máte pocit nebo podezření, že je narušováno vaše soukromí, či ochrana osobních údajů prostřednictvím pořizování kamerových záznamů? (Například, že někdo nelegálně sleduje prostřednictvím kamer dění na veřejném místě, či dění na soukromém pozemku někoho jiného).
    - Ano, jsem si jistý/á
    - Mám podezření, že ano
    - Nevím
    - Myslím si, že ne
    - Jsem si jistý/á, že ne